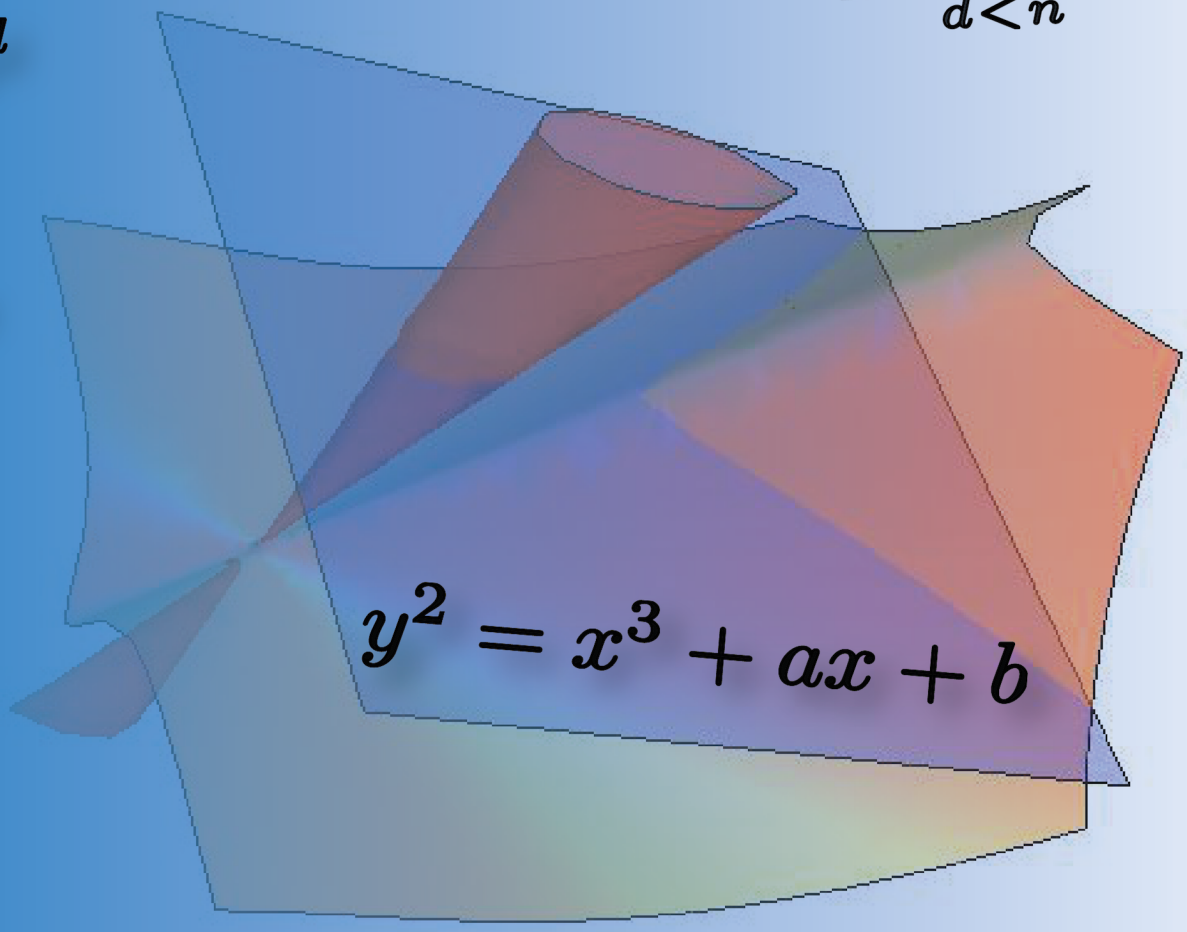
Πεπερασμένα Σώματα & Κρυπτογραφία

$$\Phi_n(x) = \frac{x^n - 1}{\prod_{\substack{d|n \\ d<n}} \Phi_d(x)}$$

$$\begin{matrix} \mathbb{F}_{p^d} \\ | \\ \mathbb{F}_p \end{matrix}$$



Γιάννης Αντωνιάδης
Αριστείδης Κοντογεώργης

Ελληνικά Ακαδημαϊκά Ηλεκτρονικά Συγγράμματα και Βοηθήματα
www.kallipos.gr

HEALLINK
Σύνδεσμος Ελληνικών Ακαδημαϊκών Βιβλιοθηκών

Ευρωπαϊκή Ένωση
Ευρωπαϊκό Κοινωνικό Ταμείο

ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ
ΕΚΠΑΙΔΕΥΣΗ ΚΑΙ ΔΙΑ ΒΙΟΥ ΜΑΘΗΣΗ
επένδυση στην κοινωνία της γνώσης
ΥΠΟΥΡΓΕΙΟ ΠΑΙΔΕΙΑΣ ΚΑΙ ΘΡΗΣΚΕΥΜΑΤΩΝ
ΕΙΔΙΚΗ ΥΠΗΡΕΣΙΑ ΔΙΑΧΕΙΡΙΣΗΣ

ΕΣΠΑ 2007-2013
ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΩΝΙΚΟ ΤΑΜΕΙΟ

Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

Πεπερασμένα Σώματα και Κρυπτογραφία

Συγγραφή
Ιωάννης Αντωνιάδης
Αριστείδης Κοντογεώργης

Κριτικός αναγνώστης
Δημήτριος Δεριζιώτης

Συντελεστές Έκδοσης
ΓΛΩΣΣΙΚΗ ΕΠΙΜΕΛΕΙΑ: Δημήτριος Καλλιάρας
ΓΡΑΦΙΣΤΙΚΗ ΕΠΙΜΕΛΕΙΑ: Αριστείδης Κοντογεώργης
ΤΕΧΝΙΚΗ ΕΠΕΞΕΡΓΑΣΙΑ: Αριστείδης Κοντογεώργης

ISBN: 978-618-82124-6-6
Έκδοση 1.2 13/6/2016

Σύνδεσμος Ελληνικών Ακαδημαϊκών Βιβλιοθηκών
Εθνικό Μετσόβιο Πολυτεχνείο
Ηρώων Πολυτεχνείου 9, 15780 Ζωγράφου

http://www.kallipos.gr

Αφιερώνεται στις μητέρες μας, Κατερίνα και Μαρία.

Εισαγωγή

Η Θεωρία Αριθμών μπορεί να διδαχτεί με στοιχειώδη τρόπο, ειδικότερα αν η διδασκαλία της γίνει σε ένα αρχικό στάδιο. Η διδακτική αυτή προσέγγιση είναι χρήσιμη, γιατί εισάγει τον φοιτητή σε έννοιες οι οποίες μπορεί να χρησιμοποιηθούν στη συνέχεια, προκειμένου να γίνουν καλύτερα κατανοητές περισσότερο αφηρημένες αλγεβρικές έννοιες.

Σε αυτό το βιβλίο (το οποίο απευθύνεται σε φοιτητές που έχουν ήδη παρακολουθήσει ένα πρώτο μάθημα άλγεβρας) θα ακολουθήσουμε μια προσέγγιση η οποία χρησιμοποιεί περισσότερο προχωρημένες αλγεβρικές έννοιες προκειμένου να δώσουμε συντομότερες και περισσότερο κομψές αποδείξεις. Αν και γίνεται προσπάθεια να υπάρξει ορισμός κάθε αλγεβρικής έννοιας που χρησιμοποιούμε, ο αναγνώστης θα μπορούσε και θα έπρεπε να ανατρέξει σε ένα βιβλίο αφηρημένης άλγεβρας για περισσότερες πληροφορίες.

Η φιλοσοφία αυτής της διδασκαλίας βοηθάει στο να μπορέσει ο φοιτητής να κατανοήσει τη σημασία αλγεβρικών εννοιών και να δει την εισαγωγική Θεωρία Αριθμών από μια διαφορετική οπτική γωνία. Άλλωστε, τα προβλήματα της Θεωρίας Αριθμών ήταν μια από τις κινητήριες δυνάμεις για την ανάπτυξη της αφηρημένης Άλγεβρας.

Οι κλάσεις υπολοίπων $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ ακέραιων αριθμών modulo έναν πρώτο p αποτελούν παραδείγματα από πεπερασμένα σώματα. Τα πεπερασμένα σώματα όμως δεν περιορίζονται στα σώματα $\mathbb{F}_p$, αλλά επεκτείνονται και στις αλγεβρικές επεκτάσεις τους. Αναπτύσσουμε λοιπόν και τη θεωρία επεκτάσεων σωμάτων, ενώ παρουσιάζουμε και στοιχεία από τη Θεωρία Galois. Ιδιαίτερη έμφαση δίνεται στις n-στές ρίζες της μονάδας και στην κατασκευή των κυκλοτομικών πολυωνύμων.

Στο πέμπτο κεφάλαιο ορίζουμε βασικούς αλγορίθμους κρυπτογράφησης, ενώ στο επόμενο κεφάλαιο αναφέρονται οι αλγόριθμοι ανοιχτού κλειδιού. Αυτοί οι αλγόριθμοι δείχνουν την ανάγκη λύσης προβλημάτων όπως η παραγοντοποίηση ακέραιων αλλά και το πρόβλημα του διακριτού λογαρίθμου.

Το κεφάλαιο 7 αποτελεί μια εισαγωγή στη Θεωρία των ελλειπτικών καμπυλών οι οποίες βρίσκουν εφαρμογή και στο επόμενο κεφάλαιο όπου περιγράφονται αλγόριθμοι παραγοντοποίησης.

Τέλος στο τελευταίο κεφάλαιο δίνουμε μερικά στοιχεία σχετικά με την κατασκευή ελλειπτικών καμπυλών με εκ των προτέρων γνωστή τάξη. Η κατασκευή αυτή είναι απαραίτητη προκειμένου να κατασκευάσουμε κρυπτοσυστήματα βασισμένα στις ελλειπτικές καμπύλες τα οποία να είναι ανθεκτικά στις γνωστές επιθέσεις.

Η παραπάνω θεωρία απαιτεί ευχέρεια στην εκτέλεση υπολογισμών, οπότε το βιβλίο είναι γεμάτο με παραδείγματα βασισμένο στο ανοιχτού κώδικα λογισμικό sage, ενώ στις ηλεκτρονικές εκδόσεις του

βιβλίου (epub, pdf) ο χρήστης μεταφέρεται σε online διαδραστική εκτέλεση του προγράμματος προκειμένου να πειραματιστεί.

Θα θέλαμε να ευχαριστήσουμε θερμά τον κριτικό αναγνώστη, ομότιμο Καθηγητή του τμήματος Μαθηματικών του ΕΚΠΑ, κ. Δεριζιώτη, για τις εύστοχες και εποικοδομητικές παρατηρήσεις του. Επίσης πολλές ευχαριστίες στον γλωσσικό επιμελητή-φιλόλογο, κ. Δημήτρη Καλλιάρα, για όλες τις διορθώσεις του.

Περιεχόμενα

Κατάλογος σχημάτων

Κατάλογος πινάκων

1

Στοιχειώδης Θεωρία Αριθμών

1.1. Θεωρία αριθμών στους ακέραιους

Σε αυτό το κεφάλαιο θα δούμε μερικές βασικές ιδιότητες των ακέραιων αριθμών σχετικά με τη διαίρεση. Ο αναγνώστης θα μπορούσε να συμβουλευτεί ένα βιβλίο θεωρίας αριθμών για περισσότερες πληροφορίες όπως τα (Αντωνιάδης και Κοντογεώργης 2015), (Λάκκης 1990) ή το (Stein 2008).

1.1.1 Θεώρημα:
Έστω $a, b \in \mathbb{Z}$ *με* $b \neq 0$. *Υπάρχουν μονοσήμαντα ορισμένα* $p, q \in \mathbb{Z}$ *ώστε*

$$a = bq + r,$$

με $0 \leqslant r < |b|$.

Απόδειξη: Θα υποθέσουμε για απλότητα ότι $b > 0$. Θεωρούμε το σύνολο

$$M = \{a - bt : t \in \mathbb{Z}, a - bt > 0\}.$$

Παρατηρούμε ότι το σύνολο M είναι ένα μη κενό σύνολο φυσικών άρα έχει ένα ελάχιστο στοιχείο r. Το στοιχείο αυτό θα είναι το υπόλοιπο της διαίρεσης, ενώ το $q = t$ στο οποίο αντιστοιχεί το r, θα είναι το πηλίκο. Είναι σαφές ότι $0 \leqslant r < b$, γιατί διαφορετικά θα μπορούσαμε να αφαιρέσουμε ακόμα ένα b και να καταλήξουμε σε ένα ακόμα μικρότερο στοιχείο του M, άτοπο.

Για τη μοναδικότητα θεωρούμε δύο διαφορετικές γραφές του a ως

$$a = bq_1 + r_1, a = bq_2 + r_2$$

τις οποίες και αφαιρούμε για να πάρουμε:

$$b(q_1 - q_2) = r_2 - r_1,$$

ενώ

$$-b < r_2 - r_1 < b \Rightarrow -1 < q_1 - q_2 < 1$$

άρα, αφού τα $q_1 - q_2$ είναι ακέραιοι, έχουμε ότι $q_1 = q_2$ άρα και $r_1 = r_2$.

Η περίπτωση $b < 0$ ανάγεται στην περίπτωση $b > 0$ πολλαπλασιάζοντας με -1.

1.1.2 Ορισμός:
Για $a, b \in \mathbb{Z}$ *θα λέμε ότι ο* a *διαιρεί τον* b *και θα γράφουμε* $a \mid b$ *αν και μόνο υπάρχει ακέραιος αριθμός* c *ώστε* $b = ca$. *Ισοδύναμα, το υπόλοιπο της διαίρεσης του* b *με* a *θα πρέπει να είναι ίσο με* 0.

1.1.1. Ιδιότητες διαίρεσης.

1. Αν $a \mid b$ και $a \mid c$, τότε για κάθε $x, y \in \mathbb{Z}$ $a \mid xa + yb$.
2. Αν $a \mid b$ και $b \mid c$, τότε $a \mid c$.
3. Αν $a \mid b$ και $b \mid c$, τότε $a = \pm b$.

1.1.3 Ορισμός:
Ένας φυσικός αριθμός $p > 1$ *θα λέγεται πρώτος αν οι μόνοι θετικοί διαιρέτες του είναι ο εαυτός του και η μονάδα.*

1.1.4 Θεώρημα:
Κάθε θετικός ακέραιος γράφεται ως γινόμενο πρώτων.

Απόδειξη Ας υποθέσουμε ότι το σύνολο των φυσικών αριθμών A που δεν γράφονται ως γινόμενο πρώτων είναι μη κενό. Τότε το σύνολο αυτό έχει ένα ελάχιστο στοιχείο n.

Αν είναι ήδη πρώτος, τότε γράφεται ως γινόμενο πρώτων με τετριμμένο τρόπο, άρα δεν θα μπορούσε να είναι στοιχείο του συνόλου M. Αν δεν είναι πρώτος τότε γράφεται ως γινόμενο

$$n = a \cdot b,$$

όπου τα a, b είναι μη τετριμμένοι διαιρέτες του n, οπότε $1 \leqslant a, b < n$. Όμως, αφού το n είναι το ελάχιστο στοιχείο του M, θα έχουμε ότι $a, b \notin M$ και, συνεπώς, τα a, b θα αναλύονται σε γινόμενο πρώτων. Συνεπώς, το ίδιο θα συμβαίνει για το n, άτοπο.

1.1.5 Θεώρημα:
Ευκλείδη Υπάρχουν άπειροι πρώτοι.

Απόδειξη: Έστω ότι υπήρχαν πεπερασμένοι το πλήθος πρώτοι

$$\{p_1, p_2, \ldots, p_N\}.$$

Τότε, το γινόμενό τους

$$S = p_1 \cdot p_2 \cdots p_N$$

θα ήταν ένας φυσικός αριθμός. Ο αριθμός $S + 1$ θα έπρεπε να έχει έναν πρώτο διαιρέτη p, ο οποίος θα ήταν ένας παράγοντας του S. Αφού $p \mid S + 1$ και $p \mid S$, θα έχουμε ότι $p \mid 1$, άτοπο.

1.1.6 Ορισμός:
Θεωρούμε τους ακέραιους a, b. *Θα ονομάζουμε μέγιστο κοινό διαιρέτη των* a, b *και θα τον συμβολίζουμε με* (a, b), *έναν φυσικό αριθμό* d *ο οποίος ικανοποιεί:*

1. $d \mid a$ *και* $d \mid b$
2. *Αν* $\delta \mid a$ *και* $\delta \mid b$ *τότε* $\delta \mid d$.

Για τους $a, b \in \mathbb{Z}$ θεωρούμε το σύνολο

$$A = \{xa + yb > 0, \text{ με } x, y \in \mathbb{Z}\} \subset \mathbb{N}.$$

Το σύνολο αυτό έχει ένα ελάχιστο στοιχείο, το οποίο ταυτίζεται με τον μέγιστο κοινό διαιρέτη των a, b.

Πράγματι, αν το $n = x_0a + y_0b$ είναι το ελάχιστο στοιχείο του A, τότε

$$n = \pi a + \upsilon \text{ με } 0 \leqslant \upsilon < a.$$

Στην περίπτωση που $\upsilon > 0$ θα είχαμε:

$$n - \pi a = x_0a + y_0b - \pi a = (x_0 - \pi)a + y_0b = \upsilon > 0,$$

δηλαδή το $n - \pi a$ είναι στοιχείο του A γνήσια μικρότερο του ελαχίστου n. Άρα $\upsilon = 0$ και $a \mid n$. Με όμοιο τρόπο $b \mid n$. Τέλος, αν δ είναι ένας άλλος κοινός διαιρέτης των a, b, τότε αυτός θα πρέπει να διαιρεί και το $n = x_0a + y_0b$.

Αποδείξαμε παραπάνω ότι ο μέγιστος κοινός διαιρέτης δύο ακέραιων a, b γράφεται ως $\mathbb{Z}$-γραμμικός συνδυασμός των a, b. Θα δούμε έναν αποτελεσματικό τρόπο εύρεσης των αριθμών $x_0, y_0 \in \mathbb{Z}$ ώστε $(a, b) = x_0a + y_0b$, όταν θα μιλήσουμε για τον αλγόριθμο του Ευκλείδη.

1.1.7 Πρόταση:
Αν ένας πρώτος αριθμός $p \mid ab$, *τότε* $p \mid a$ *είτε* $p \mid b$.

Απόδειξη: Αν $p \mid a$ τότε η απόδειξη έχει τελειώσει. Αν όχι τότε $(a, p) = 1$ συνεπώς υπάρχουν $x, y \in \mathbb{Z}$ με $xa + yp = 1$. Πολλαπλασιάζουμε με b και έχουμε

$$ab + ypb = b,$$

από όπου προκύπτει το ζητούμενο, αφού ο p διαιρεί και τους δύο προσθετέους.

1.1.8 Θεώρημα:
Η ανάλυση ενός ακέραιου αριθμού σε γινόμενο πρώτων παραγόντων είναι μονοσήμαντη αν δεν ληφθεί υπόψη η σειρά των παραγόντων.

Απόδειξη: Ας υποθέσουμε ότι

$$a = \pm p_1^{\nu_1} \cdots p_r^{\nu_r} = \pm q_1^{\nu_1} \cdots q_s^{\nu_s}$$

είναι δύο διαφορετικές αναλύσεις του n ως γινόμενο πρώτων. Επιπλέον, ας υποθέσουμε ότι $r \leqslant s$. Ο πρώτος p_1 διαιρεί το γινόμενο $q_1^{\nu_1} \cdots q_s^{\nu_s}$ άρα ο p_1 διαιρεί κάποιον q_i, και συνεπώς ταυτίζεται με αυτόν. Στην παραπάνω ισότητα διαγράφουμε τους p_1 και q_1 και συνεχίζουμε μέχρι να εξαντληθούν οι

πρώτοι στο αριστερό μέρος. Επειδή το γινόμενο πρώτων δεν μπορεί να είναι μονάδα, ταυτόχρονα θα εξαντληθούν οι πρώτοι και στο δεξί μέρος, οπότε προκύπτει το ζητούμενο.

1.1.9 Πρόταση:
Αν $a = p_1^{\nu_1} \cdots p_r^{\nu_r}$ *και* $b = p_1^{\mu_1} \cdots p_r^{\mu_r}$ *είναι οι αναλύσεις των* a, b *σε γινόμενο πρώτων παραγόντων τότε*

$$(a, b) = p_1^{\min\{\nu_1,\mu_1\}} \cdots p_r^{\min\{\nu_r,\mu_r\}}.$$

Μπορούμε να ορίσουμε τους πρώτους αριθμούς ως εξής:

```
sage: P = Primes(); P
Set of all prime numbers: 2, 3, 5, 7, ...
sage: P.cardinality()
+Infinity
```

Αν θέλουμε να πάρουμε τον n-οστό πρώτο δίνουμε

```
sage: P = Primes()
sage: P.next(10^20)
100000000000000000039
```

Ενώ μπορούμε να παραγοντοποιήσουμε ως εξής:

```
sage:factor(28397492387492387429387)
13 * 2551 * 856300467011198849
```

Μπορούμε να ελέγξουμε αν ένας αριθμός είναι πρώτος

```
sage: 856300467011198849 in P
True
```

Interactive

1.1.2. Γραμμικές Ισοδυναμίες mod m.

1.1.10 Ορισμός:
Θα λέμε ότι οι αριθμοί a, b *είναι ισοδύναμοι modulo* m *και θα το συμβολίζουμε με*

$$a \equiv b \bmod m$$

αν και μόνο αν $m \mid b - a$.

Η σχέση $\equiv$ είναι μια σχέση ισοδυναμίας δηλαδή ικανοποιεί:

1. $a \equiv a \bmod m$
2. $a \equiv b \bmod m \Leftrightarrow b \equiv a \bmod m$
3. Αν $a \equiv b \bmod m$ και $b \equiv c \bmod m$, τότε $a \equiv c \bmod m$.

1.1.11 Πρόταση:
Δύο αριθμοί είναι ισοδύναμοι modulo m *αν και μόνο αν έχουν το ίδιο υπόλοιπο όταν διαιρεθούν με* m.

Απόδειξη: Γράφουμε $a = \pi_a m + u_a$ και $b = \pi_b m + u_b$. Παρατηρούμε ότι $b - a = m(\pi_b - \pi_a) + u_b - u_a$, άρα $m \mid b - a$ αν και μόνο αν $m \mid (u_b - u_a)$. Όμως, $0 \leqslant u_a, u_b < m$, συνεπώς $-m < u_b - u_a < m$. Άρα $m \mid u_b - u_a$ αν και μόνο αν $u_b = u_a$.

1.1.12 Πρόταση:
Ισχύει ότι αν $a \equiv a' \bmod m$ *και* $b \equiv b' \bmod m$, *τότε*

- $a + b \equiv a' + b' \bmod m$
- $a \cdot b \equiv a' \cdot b' \bmod m$

Απόδειξη: Γράφουμε $a = a' + km$, $b = b' + lm$ από όπου έχουμε

$$a + b = a' + b' + m(k + l)$$

και

$$a \cdot b = (a' + km)(b' + lm) = a' \cdot b' + m(a'l + b'k) + klm^2.$$

Το σύνολο των κλάσεων ισοδυναμίας της σχέσης $\equiv$ εφοδιάζεται με τη δομή αντιμεταθετικού δακτυλίου. Είναι δε ισόμορφο με τον δακτύλιο $\mathbb{Z}/m\mathbb{Z}$, των ακέραιων modulo το κύριο ιδεώδες $m\mathbb{Z}$.

Θα δούμε πώς μπορούμε να κάνουμε κάνουμε πράξεις στο πρόγραμμα sage:

```
sage:Mod(10,3)+Mod(2,3)
0
sage:p=P.next(10^10)
sage:Mod(2^(p-1),p)
1
```

Interactive

1.1.3. Ο αλγόριθμος του Ευκλείδη. Ο αλγόριθμος του Ευκλείδη είναι μια διαδικασία η οποία δέχεται ως είσοδο δύο ακέραιους αριθμούς και όταν ολοκληρωθεί δίνει τον μέγιστο κοινό τους διαιρέτη. Θεωρητικά, για τον υπολογισμό του μέγιστου κοινού διαιρέτη θα μπορούσε να χρησιμοποιηθεί η παραγοντοποίηση των αριθμών. Η μέθοδος αυτή όμως δεν είναι καλή, ιδιαίτερα όταν οι αριθμοί που

έχουμε να διαχειριστούμε είναι πολύ μεγάλοι αφού, όπως θα δούμε στη συνέχεια, η παραγοντοποίηση είναι μια ακριβή διαδικασία.

Ξεκινάμε με τους αριθμούς $a, b \in \mathbb{Z}$ και εκτελούμε τη διαίρεση με πηλίκο και υπόλοιπο.

$$a = \pi_1 b + u_1, \qquad 0 \leqslant u_1 < |b|$$

Παρατηρούμε ότι $(a, b) = (b, u_1)$ (γιατί;). Στη συνέχεια υπολογίζουμε

$$b = \pi_2 u_1 + u_2 \qquad 0 \leqslant u_2 < u_1.$$

Και πάλι έχουμε $(a, b) = (b, u_1) = (u_1, u_2)$. Συνεχίζουμε με αυτόν τον τρόπο, σχηματίζοντας μια ακολουθία υπολοίπων

$$|b| > u_1 > u_2 > \cdots > u_n > \cdots$$

Είναι σαφές ότι μετά από πεπερασμένα το πλήθος βήματα ($|b|$ το πολύ!) η ακολουθία αυτή θα μηδενιστεί. Ο μέγιστος κοινός διαιρέτης θα είναι ο τελευταίος μη μηδενικός όρος της ακολουθίας αυτής.

$$12839 = 7 \cdot 1728 + 743$$
$$1728 = 2 \cdot 743 + 242$$
$$743 = 3 \cdot 242 + 17$$
$$242 = 14 \cdot 17 + 4$$
$$17 = 4 \cdot 4 + 1$$
$$4 = 4 \cdot 1 + 0$$

Μπορούμε εκτελώντας ανάποδα τον αλγόριθμο του Ευκλείδη να υπολογίσουμε $x, y \in \mathbb{Z}$ ώστε $ax + by = (a, b)$.

Για παράδειγμα

$$1 = 17 - 4 \cdot 4 = 17 - 4(242 - 14 \cdot 17) = 57 \cdot 15 - 4 \cdot 242$$
$$= (743 - 3 \cdot 242)57 - 4 \cdot 242 = 57 \cdot 743 - 175 \cdot 242 =$$
$$= 57 \cdot 743 - 175(1728 - 2 \cdot 743) = 407 \cdot 743 - 175 \cdot 1728 =$$
$$= 407(12839 - 7 \cdot 1728) - 175 \cdot 1728 = 407 \cdot 12839 - 3024 \cdot 1728.$$

Δηλαδή υπολογίσαμε ότι $x = 407$ και $y = -3024$ και για την επιλογή αυτών των αριθμών έχουμε

$$(12839, 1728) = 1 = 407 \cdot 12839 - 3024 \cdot 1728.$$

Μπορούμε να υπολογίσουμε το παραπάνω στο sage ως

```
d,u,v = xgcd(12839,1728);d;u;v
1
407
-3024
```

και να επαληθεύσουμε το αποτέλεσμα

```
d == u*12839 + v*1728
True
```

Interactive

1.1.4. Το Θεώρημα του Κινέζου. Το παρακάτω θεώρημα δίνει μια φυσιολογική διάσπαση του δακτυλίου των ακέραιων modulo m.

1.1.13 Θεώρημα:
Έστω $m = \prod_{i=1}^{n} m_i$ η γραφή ενός φυσικού αριθμού ως γινόμενο αριθμών m_i που είναι ανά δύο πρώτοι μεταξύ τους. Οι παρακάτω δακτύλιοι είναι ισόμορφοι:

$$\frac{\mathbb{Z}}{m\mathbb{Z}} = \prod_{i=1}^{n} \frac{\mathbb{Z}}{m_i\mathbb{Z}}.$$

Απόδειξη: Θεωρούμε τον ομομορφισμό δακτυλίων

$$\psi : \frac{\mathbb{Z}}{m\mathbb{Z}} \longrightarrow \prod_{i=1}^{n} \frac{\mathbb{Z}}{m_i\mathbb{Z}},$$

$$x \bmod m \mapsto (x \bmod m_1, \ldots, x \bmod m_n).$$

Παρατηρούμε ότι $\ker(\psi) = \{0\}$. Πράγματι, αν ένας αριθμός x διαιρείται από τους πρώτους μεταξύ τους αριθμούς m_i, τότε διαιρείται και από τον m. Άρα η συνάρτηση ψ είναι 1-1. Επειδή οι δακτύλιοι έχουν τον ίδιο πληθάριθμο, η συνάρτηση ψ είναι αναγκαστικά και επί.

Παραδοσιακά στα μαθήματα Θεωρίας Αριθμών το παραπάνω θεώρημα εκφράζεται ως εξής: Το σύστημα γραμμικών ισοδυναμίων $(m_i, m_j) = 1$ για $i \neq j$, $m = m_1 \cdots m_n$

$$x \equiv x_1 \bmod m_1$$
$$x \equiv x_2 \bmod m_2$$
$$\vdots$$
$$x \equiv x_n \bmod m_n$$

έχει μοναδική λύση $\bmod m$.

1.1.14 Πρόταση:
Η λύση στο πρόβλημα ισοδυναμιών του Κινέζου υπολογίζεται ως εξής: Υπολογίζουμε τον αριθμό $m = m_1 \cdots m_n$, αλλά και τους αριθμούς $M_i = \frac{m}{m_i}$. Εξ υποθέσεως $(M_i, m_i) = 1$, οπότε υπολογίζουμε μια λύση b_i της εξίσωσης

$$M_i y \equiv 1 \bmod m_i$$

Το

$$x_0 = \sum_{i=1}^{n} x_i M_i b_i$$

είναι μια λύση του συστήματος.

Απόδειξη Αρκεί να θεωρήσουμε το x_0 modulo m_i και να παρατηρήσουμε ότι οι προσθετέοι $x_j M_j b_j$ για $i \neq j$ μηδενίζονται, ενώ ο $x_i M_j b_j \equiv x_i \mathrm{mod} m$.

Παράδειγμα Να λυθεί το σύστημα:

$$x \equiv 3 \mathrm{mod} 5$$

$$x \equiv 3 \mathrm{mod} 7$$

$$x \equiv 8 \mathrm{mod} 9$$

Λύση Υπολογίζουμε $m = 5 \cdot 7 \cdot 9 = 315$, $M_1 = 63$, $_2 = 45$ και $M_3 = 35$. Οι ισοτιμίες $M_i x \equiv 1 \mathrm{mod} m_i$, $i = 1, 2, 3$ γράφονται $63x \equiv 1 \mathrm{mod} 5$, $45x \equiv 1 \mathrm{mod} 7$ και $35x \equiv 1 \mathrm{mod} 9$ και έχουν λύσεις $b_1 \equiv 2 \mathrm{mod} 5$, $b_2 \equiv 5 \mathrm{mod} 7$ και $b_3 \equiv 8 \mathrm{mod} 9$ αντίστοιχα. Επομένως, η μοναδική λύση του αρχικού συστήματος είναι

$$x_0 \equiv (a_1 M_1 b_1 + a_2 M_2 b_2 + a_3 M_3 b_3) \mathrm{mod} 315$$

δηλαδή $x_0 = 143 \mathrm{mod} 315$.

Για να λύσουμε το παραπάνω πρόβλημα στο sage δίνουμε

```
sage:CRT_list([3,3,8], [5,7,9])
143
```

Interactive

1.1.5. Αντιστρέψιμα στοιχεία modulo m..

1.1.5.1. *Η εξίσωση* $ax \equiv b mod m$.. Παρατηρούμε ότι αναγκαία συνθήκη για να έχει λύση η εξίσωση

$$ax \equiv b \mathrm{mod} m$$

είναι $(a, m) \mid b$. Η συνθήκη αυτή είναι και ικανή αφού μπορούμε να βρούμε ακέραιους $x, y \in \mathbb{Z}$ ώστε

$$ax + by = (a, b).$$

Άρα, αν $(a, b) \mid b$, τότε $\frac{m}{(a,b)} \in \mathbb{Z}$ και συνεπώς

$$ax\frac{m}{(a,b)} + by\frac{m}{(a,b)} = \frac{m}{(a,b)}(a, b) = m,$$

όπου τα $X := x\frac{m}{(a,b)}$ και $Y := y\frac{m}{(a,b)}$ αποτελούν λύσεις. Αποδείξαμε ότι

1.1.15 Πρόταση:
η εξίσωση $ax + by = d$ *έχει λύσεις αν και μόνο αν* $(a, b) \mid m$.

1.1.5.2. *Αντιστρέψιμα στοιχεία modulo* m.. Η αντιστρεψιμότητα του στοιχείου $a \mathrm{mod} m$ είναι ισοδύναμη με την υπάρξη λύσης της εξίσωσης $ax \equiv 1 \mathrm{mod} m$. Άρα με βάση την προηγούμενη πρόταση καταλήγουμε στην

1.1.16 Πρόταση:
Τα αντιστρέψιμα στοιχεία $\mathrm{mod}\,m$ *είναι αυτά τα οποία έχουν μέγιστο κοινό διαιρέτη* $(m, a) = 1$.

Ας υπολογίσουμε τον αντίστροφο του $10 \mathrm{mod} 13$

```
sage:Mod(10,13)^(-1)
4
```

Interactive

1.1.5.3. *Πλήθος αντιστρέψιμων στοιχείων modulo* m.. Θα συμβολίζουμε με $\phi(m)$ το πλήθος των στοιχείων $0 \leqslant a < m$ που είναι πρώτα προς τον m, δηλαδή

$$\phi(m) = \mid a \in \mathbb{Z} : 0 \leqslant a < m, (a, m) = 1 \mid .$$

Παρατηρούμε ότι αν ο p είναι πρώτος, τότε

$$\phi(p) = p - 1.$$

Ομοίως, στο σύνολο $0 \leqslant a \leqslant p^t$ υπάρχουν p^{t-1} αριθμοί που διαιρούνται με p, αφού αυτοί είναι της μορφής $x = pa'$, και $0 \leqslant a < p^t$, αν και μόνο αν $0 \leqslant a' < p^{t-1}$. Συνεπώς

$$\phi(p^t) = p^t - p^{t-1}.$$

Για να υπολογισουμε την τιμή του ϕ σε σύνθετους αριθμούς χρειαζόμαστε την παρακάτω

1.1.17 Πρόταση:
Αν $(m, n) = 1$ *τότε ισχύει* $\phi(m \cdot n) = \phi(m)\phi(n)$.

Απόδειξη: Παρατηρούμε ότι η συνάρτηση ϕ ταυτίζεται με την τάξη της ομάδας των μονάδων $U(\mathbb{Z}/m\mathbb{Z})$ του δακτυλίου $\mathbb{Z}/m\mathbb{Z}$. Το θεώρημα του Κινέζου εξασφαλίζει ότι

$$U\left(\frac{\mathbb{Z}}{m\mathbb{Z}}\right) = \prod_{i=1}^{n} U\left(\frac{\mathbb{Z}}{m_i\mathbb{Z}}\right).$$

Από την παραπάνω σχέση προκύπτει το ζητούμενο αποτέλεσμα.

1.1.18 Πρόταση:
Για κάθε $a \in \mathbb{Z}$, $(a, m) = 1$ *ισχυεί ότι*

$$a^{\phi(m)} \equiv 1 \mathrm{mod} m.$$

Απόδειξη: Η τάξη κάθε στοιχείου στην ομάδα $U(\mathbb{Z}/m\mathbb{Z})$ είναι διαιρέτης της τάξης της ομάδας που είναι ίση με $\phi(m)$. Το αποτέλεσμα έπεται.

Ας υπολογίσουμε λίγο με τη συνάρτηση του Euler. Θα την υπολογίσουμε με δύο τρόπους για τον $n = 2015$. Η συνάρτηση prime divisors επιστρέφει ως λίστα τους πρώτους διαιρέτες του n. Παρατηρήστε τη σύνταξη της εντολής prod που διατρέχει τους πρώτους διαιρέτες του n. Η συνάρτηση euler_phi είναι η ενσωματωμένη συνάρτηση του sage.

```
sage:n=2015
sage:prime_divisors(n)
[5, 13, 31]
sage:phi = n*prod([1 - 1/p for p in prime_divisors(n)]); phi
1440
sage:euler_phi(n)
1440
```

Interactive

1.1.6. Αριθμητικές Συναρτήσεις.

1.1.19 Ορισμός:
Μία συνάρτηση $f : \mathbb{N} \to \mathbb{C}$ *θα λέγεται αριθμητική συνάρτηση.*

Ενδιαφέρουσες αριθμητικές συναρτήσεις είναι οι παρακάτω:

1. $d(n) =$ ο αριθμός των (θετικών) διαιρετών του n.
2. $\sigma(n) =$ το άθροισμα των θετικών διαιρετών του n.
3. $\phi(n) =$ ο αριθμός των θετικών ακέραιων $\leqslant n$ που είναι πρώτοι προς τον n.
4. $\nu(n) =$ ο αριθμός των διακεκριμένων πρώτων παραγόντων του n
5. $\Omega(n) =$ ο αριθμός των πρώτων παραγόντων του n
6. $\mu(n) = \begin{cases} 0 & \text{αν ένα τετράγωνο διαιρεί τον } n \\ (-1)^{\nu(n)} & \text{αν ο } n \text{ είναι ελεύθερος τετραγώνου} \end{cases}$

Η $\phi(n)$ λέγεται συνάρτηση του Euler και η $\mu(n)$ συνάρτηση του Möbius.

1.1.20 Θεώρημα:
Θεωρούμε τον φυσικό $n > 1$ *με ανάλυση* $n = \prod_{i=1}^{r} p_i^{a_i}$, $a_i > 0$. *Τότε*

$$d(n) = \prod_{i=1}^{r} (a_i + 1).$$

Απόδειξη Κάθε διαιρέτης του n θα έχει μια παράσταση της μορφής

$$m = p_1^{\ell_1} p_2^{\ell_2} \dots p_r^{\ell_r},$$

όπου $0 \leqslant \ell_i \leqslant a_i$. Μάλιστα, κάθε διαιρέτης του n εμφανίζεται ακριβώς μία φορά στις παραστάσεις της παραπάνω μορφής. Επειδή δε κάθε ℓ_i έχει $a_i + 1$ δυνατότητες, το πλήθος $d(n)$ δίνεται από τον παραπάνω τύπο.

Παρατήρησεις:

1. Η $d(n)$ μπορεί να γραφεί και ως $d(n) = \sum_{d|n} 1$.
2. Ισχύει $d(nm) = d(n)d(m)$ για όλους τους φυσικούς n, m με $(n, m) = 1$.

Θεωρούμε την ποσότητα $\sigma(n)$ η οποία εξ ορισμού γράφεται ως

$$\sigma(n) = \sum_{d|n} d.$$

Παρατηρούμε ότι όταν το d διατρέχει τους διαιρέτες του n το ίδιο κάνει και το n/d, συνεπώς μπορούμε να γράψουμε:

$$\sigma(n) = \sum_{d|n} \frac{n}{d} = n \sum_{d|n} \frac{1}{d},$$

δηλαδή καταλήγουμε σε έναν τύπο για το άθροισμα των αντιστρόφων των διαιρετών του n:

$$\frac{\sigma(n)}{n} = \sum_{d|n} \frac{1}{d}.$$

1.1.21 Πρόταση:
Αν $(a, b) = 1$, *τότε*

$$\sigma(ab) = \sigma(a)\sigma(b).$$

Απόδειξη Παρατηρούμε ότι

$$\sigma(ab) = \sum_{d|ab} d = \sum_{d_1|a, d_2|b} d_1 d_2 = \left(\sum_{d_1|a} d_1 \right) \left(\sum_{d_2|b} d_2 \right) = \sigma(a)\sigma(b).$$

1.1.22 Πρόταση:
Αν $n = \prod_{i=1}^{r} p_i^{a_i}$, *τότε*

$$\sigma(n) = \prod_{i=1}^{r} \frac{p_i^{a_i+1} - 1}{p_i - 1}.$$

Απόδειξη Υπολογίζουμε ότι

$$\sigma(p_i^{a_i}) = 1 + p_i + p_i^2 + \cdots + p_i^{a_i} = \frac{p_i^{a_i+1} - 1}{p_i - 1}.$$

Το ζητούμενο προκύπτει από την ιδιότητα

$$\sigma(n) = \prod_{i=1}^{r} \sigma(p_i^{a_i}).$$

1.1.23 Ορισμός:
Μια αριθμητική συνάρτηση f *θα λέγεται πολλαπλασιαστική όταν:*

1. *Υπάρχει* $n_0 \in \mathbb{N}$ *ώστε* $f(n_0) \neq 0$
2. *Αν* $(m,n) = 1$ *τότε* $f(mn) = f(m)f(n)$.

1.1.24 Θεώρημα:
Αν η f *είναι πολλαπλασιαστική, τότε και η* g *που ορίζεται ως*

$$g(n) = \sum_{d|n} f(d)$$

είναι επίσης πολλαπλασιαστική.

Απόδειξη Αν $(m,n) = 1$, όταν το d_1 διατρέχει τους διαιρέτες του m και το d_2 διατρέχει τους διαιρέτες του n, τότε το $d_1 d_2$ θα διατρέχει τους διαιρέτες του mn. Συνεπώς

$$g(mn) = \sum_{d|mn} f(d) = \sum_{d_1|m, d_2|n} f(d_1 d_2) =$$

$$= \sum_{d_1|m, d_2|n} f(d_1)f(d_2) =$$

$$= \sum_{d_1|m} f(d_1) \sum_{d_2|m} f(d_2) = g(m)g(n).$$

Παρατήρηση Θα μπορούσαμε να αποδείξουμε ότι οι συναρτήσεις d, σ είναι πολλαπλασιαστικές παρατηρώντας ότι οι συναρτήσεις $f_1(n) = 1$ και $f_2(n) = n$ είναι πολλαπλασιαστικές και κάνοντας χρήση της παραπάνω πρότασης.

Η συνάρτηση του Möbius είναι πολλαπλασιαστική αφού η τιμή της σε ένα πρώτο είναι $-1 \neq 0$ και αν $(n,m) = 1$ τότε $\mu(nm) = \mu(n)\mu(m)$. Το τελευταίο ισχύει, διότι αν κάποιος από τους δύο αριθμούς διαιρείται με το τετράγωνο ακέραιου, τότε $\mu(n)\mu(m) = 0 = \mu(nm)$, ενώ αν $m = p_1 \cdots p_\mu$, $n = q_1 \cdots q_s$ με $p_i \neq p_j$ και $q_i \neq q_j$ για $i \neq j$ και αφού $(n,m) = 1$ έχουμε

$$\mu(nm) = (-1)^{\mu+s} = (-1)^\mu (-1)^s = \mu(m)\mu(n).$$

1.1.25 Θεώρημα:
Έστω $n \prod_{i=1}^r p_i^{n_i}$ *η ανάλυση ενός φυσικού σε πρώτους παράγοντες. Αν η* f *είναι πολλαπλασιαστική, τότε*

1.

$$\sum_{d|n} f(d) = \prod_{i=1}^{r} \left(1 + f(p_i) + \cdots + f(p_i^{n_i})\right)$$

2.
$$\sum_{d|n} \mu(d)f(d) = \prod_{i=1}^{r}(1 - f(p_i)).$$

Απόδειξη Υπολογίζουμε ότι

$$\sum_{d|n} f(d) = \sum_{m_1,\ldots,m_r=0}^{n_1,\ldots,n_r} f(p_1^{m_1})f(p_2^{m_2})\cdots f(p_r^{m_r}) =$$

$$\sum_{m_1=0}^{n_1} f(p_1^{m_1}) \sum_{m_2}^{n_2} f(p_2^{m_2}) \cdots \sum_{m_r=0}^{n_r} f(p_r^{m_r})$$

από όπου προκύπτει η πρώτη σχέση.

Η δεύτερη σχέση είναι συνέπεια της πρώτης, αρκεί να παρατηρήσουμε ότι το γινόμενο δύο πολλαπλασιαστικών συναρτήσεων είναι πολλαπλασιαστικό και ότι

$$f(p^i)\mu(p^i) = 0 \text{ αν } i \geqslant 2,$$

ενώ

$$f(p)\mu(p) = -f(p).$$

Παρατήρηση Ισχύει ότι

$$\sum_{d|n} \mu(d) = \begin{cases} 0 & \text{αν } n > 1 \\ 1 & \text{αν } n = 1 \end{cases}.$$

1.1.26 Θεώρημα:
Έστω f, g *αριθμητικές συναρτήσεις. Οι παρακάτω προτάσεις είναι ισοδύναμες:*

1. $g(n) = \sum_{d|n} f(d)$
2. $f(n) = \sum_{d|n} \mu(n/d)g(d)$

Απόδειξη Θα αποδείξουμε πρώτα ότι $1 \Rightarrow 2$. Υπολογίζουμε

$$\sum_{d|n} \mu(n/d)g(d) = \sum_{d|n} \mu(n/d) \sum_{t|d} f(t) = \sum_{t|d|n} \mu(n/d)f(t)$$

Παρατηρούμε ότι το t διατρέχει όλους τους διαιρέτες του n, ενώ το d διατρέχει όλους τους διαιρέτες του n για τους οποίους ισχύει $t \mid d$. Αυτό είναι ισοδύναμο με $\frac{n}{d} \mid \frac{n}{t}$. Θέτουμε $d' := n/d$. Ισχύει:

$$\sum_{t|d|n} \mu(n/d)f(t) = \sum_{t|n} \sum_{\frac{n}{d}|\frac{n}{t}} \mu(n/d) = \sum_{t|n} f(t) \sum_{d'|\frac{n}{t}} \mu(d')$$

$$= f(n).$$

Θα δείξουμε τώρα ότι $2 \Rightarrow 1$. Έχουμε

$$\sum_{d|n} f(d) = \sum_{d|n} \sum_{t|d} \mu(d/t)g(t) =$$

$$= \sum_{t|n} g(t) \sum_{\frac{n}{d}|\frac{n}{t}} \mu(d/t) =$$

$$\sum_{t|n} g(t) \sum_{d'|\frac{n}{t}} \mu\left(\frac{n}{d't}\right) =$$

$$\sum_{t|n} g(t)\epsilon(n/t) = g(n).$$

Με χρήση του νόμου αντιστροφής μπορούμε να αποδείξουμε

1.1.27 Πρόταση:
Αν η αριθμητική συνάρτηση $g(n)$ *είναι πολλαπλασιαστική και*

$$g(n) = \sum_{d|n} f(d)$$

για $n \geqslant 1$, *τότε και η* f *είναι πολλαπλασιαστική.*

Απόδειξη Αφού $g(n) = \sum_{d|n} f(d)$ έχουμε ότι

$$f(n) = \sum_{d|n} \mu(d)g(n/d).$$

1.1.28 Θεώρημα:
Για κάθε θετικό ακέραιο, ισχύει

$$n = \sum_{d|n} \phi(d).$$

Απόδειξη Σε κάθε διαιρέτη d του n αντιστοιχίζουμε όλους τους ακέραιους τους μικρότερους ή ίσους του n, των οποίων ο μέγιστος κοινός διαιρέτης με τον n είναι ακριβώς d. Προφανώς κάθε ακέραιος $\leqslant n$ αντιστοιχεί σε ακριβώς έναν d.

Σε κάποιον d αντιστοιχούν ακριβώς εκείνοι από τους

$$d, 2d, \ldots, kd, \ldots, (n/d)d$$

για τους οποίους ισχύει $(kd, n) = d$, δηλαδή οι ακέραιοι για τους οποίους $(k, n/d) = 1$ και $k \leqslant n/d$. Σύμφωνα με τον ορισμό της συνάρτησης του Euler το πλήθος αυτών είναι $\phi(n/d)$. Αν τους προσθέσουμε θα πρέπει να βρούμε n δηλαδή:

$$n = \sum_{d|n} \phi(n/d) = \sum_{d|n} \phi(d).$$

Ας πιστοποιήσουμε τον παραπάνω τύπο στο sage

```
sage:n=24
     divisors(n)
[1, 2, 3, 4, 6, 8, 12, 24]
```

```
4 sage:sum([euler_phi(d) for d in divisors(n)])
5 24
```

Interactive

Παρατήρηση

1. Αφού η συνάρτηση $n \mapsto n$ είναι πολλαπλασιαστική και η συνάρτηση ϕ είναι.
2. Για κάθε θετικό ακέραιο n ισχύει

$$\phi(n) = n \sum_{d|n} \frac{\mu(d)}{d}.$$

Πράγματι αρκεί να γράψουμε

$$\phi(n) = \sum_{d|n} \mu(n/d)g(d) = \sum_{d|n} \mu(d)g(n/d) = \sum_{d|n} \frac{n\mu(d)}{d} = n \sum_{d|n} \frac{\mu(d)}{d}.$$

Παρατήρηση Αν έχουμε δύο αριθμητικές συναρτήσεις f, g, τότε σχηματίζουμε τη συνέλιξη Dirichlet η οποία ορίζεται ως

$$f * g = \sum_{d|n} f(d)g\left(\frac{n}{d}\right).$$

Η παραπάνω πράξη είναι προσεταιριστική

$$(f * g) * h = f * (g * h)$$

επιμεριστική ως προς την πρόσθεση

$$f * g = g * f$$

έχει ένα ουδέτερο στοιχείο το ϵ που ορίζεται ως

$$\epsilon(1) = \begin{cases} 1 & \text{αν } n = 1 \\ 0 & \text{αν } n \neq 1 \end{cases},$$

και για κάθε συνάρτηση f με $f(1) \neq 0$ υπάρχει g ώστε $f * g = \epsilon$.

1.1.29 Ορισμός:
Για μία αριθμητική συνάρτηση ορίζουμε μία σειρά Dirichlet

$$DG(f; s) = \sum_{n=1}^{\infty} \frac{f(n)}{n^s},$$

η οποία ορίζει μια μιγαδική συνάρτηση για όλα τα $s \in \mathbb{C}$ στα οποία συγκλίνει.

Ο πολλαπλασιασμός Dirichlet είναι συμβατός με τις σειρές Dirichlet σαν οι σειρές Dirichlet να ήταν ένας μετασχηματισμός Fourier:

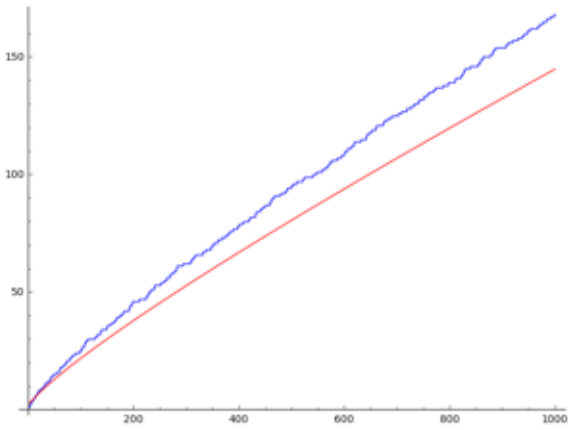
$$DG(f; s)DG(g; s) = DG(f * g; s).$$

1.1.7. Το θεώρημα των πρώτων αριθμών. Το θεώρημα των πρώτων αριθμών καθορίζει την ασυμπτωτική κατανομή των πρώτων αριθμών, δηλαδή μία περιγραφή του πώς οι πρώτοι αριθμοί κατανέμονται ανάμεσα στους θετικούς αριθμούς. Το θεώρημα αυτό μας περιγράφει μεταξύ άλλων πόσο πιθανό είναι αν επιλέξουμε έναν αριθμό μικρότερο του x να είναι ο αριθμός αυτός πρώτος.

Θεωρούμε τη συνάρτηση $\pi(x)$ η οποία μετράει πόσοι πρώτοι αριθμοί είναι μικρότεροι του x, δηλαδή

$$\pi(x) = \#\{p \in \mathbb{N} : p \leqslant x, p \text{ πρώτος}\}.$$

```
sage:prime_pi(123456789)
7027260
```



Σχήμα 1.1. Γραφική παράσταση της $\pi(x)$ (μπλέ) και της $x/\log(x)$ (κόκκινο) μέχρι το 1000

1.1.30 Θεώρημα:
Η συνάρηση $\pi(x)$ είναι ασυμπτωτική στη συνάρτηση $x/\log(x)$, δηλαδή

$$\lim_{x\to\infty} \frac{\pi(x)}{x/\log(x)} = 1.$$

Η απόδειξη του παραπάνω θεωρήματος είναι εκτός του σκοπού αυτού του βιβλίου.

Ασκήσεις

1. Θεωρούμε το πολυώνυμο με συντελεστές από το $\mathbb{Z}$ της μορφής
$$f(x) = \sum_{i=0}^{n} a_i x^i.$$
Δείξτε ότι αν το $f(x)$ έχει ρητή ρίζα $q = a/b$ $(a, b) = 1$, τότε $b \mid a_n$ και $a \mid a_0$. Να δείξετε ότι οι αριθμοί $\sqrt[13]{3}$ και $\sqrt[3]{5}$ δεν είναι ρητοί.
2. Να αποδειχτεί ότι ο αριθμός $100m + n$ διαιρείται δια του 7, αν ο αριθμός $2m + n$ διαιρείται δια του 7.
3. Να αποδειχτεί ότι ένας αριθμός διαιρείται διά του 3 ή του 9, αν το άθροισμα των ψηφίων του διαιρείται δια του 3 ή του 9, αντίστοιχα.

4. Να αποδειχτεί ότι ο αριθμός $3n^2+1$, $n \in \mathbb{N}$, δεν μπορεί να είναι το τετράγωνο ενός φυσικού αριθμού.
5. Αν για τους φυσικούς αριθμούς m, n ισχύει $m < n$ να αποδειχτεί ότι $2^{2^m}+1$ διαιρεί το $2^{2^n}-1$.
6. Να αποδειχτεί ότι για κάθε φυσικό αριθμό $n > 0$ ισχύει ότι το 10 δεν διαιρεί το $(n-1)!+1$.
7. Να αποδειχτεί ότι ο αριθμός $2^{4n+2}+1$ δεν είναι πρώτος για $n \geqslant 1$.
8. Να αποδειχτεί ότι ο αριθμός n^4+4 δεν είναι πρώτος για $n \geqslant 1$.
9. Αν p_n συμβολίζει τον n-οστό πρώτο αριθμό, να αποδειχτεί ότι $p_{n-1} \geqslant n+2$ για $n \geqslant 5$.
10. Πότε ο αριθμός $(p-1)!+1$ είναι δύναμη του p, όπου p πρώτος αριθμός;
11. Να βρεθεί ο μέγιστος κοινός διαιρέτης των αριθμών 625 και 231 και να εκφραστεί ως γραμμικός συνδυασμός με συντελεστές ακέραιους των παραπάνω αριθμών.
12. Να αποδειχτεί ότι το γινόμενο τεσσάρων διαδοχικών αριθμών διαιρείται διά του 24.
13. Να αποδειχτεί ότι για κάθε φυσικό αριθμό n ισχύει
$$\sum_{d|n} \frac{\mu^2(d)}{\phi(d)} = \frac{n}{\phi(n)}.$$
14. Να αποδειχτεί ότι για κάθε φυσικό αριθμό n ισχύει
$$\sum_{d|n} \mu(d)\phi(d) = \prod_{p|n}(2-p).$$
15. Να βρεθεί το πλήθος και το άθροισμα των φυσικών διαιρετών του 1440.
16. Να αποδειχτεί ότι για κάθε ακέραιο αριθμό a ισχύει
$$a^2 \equiv 0 \text{ ή } 1 \text{ ή } 4 \bmod 8.$$
17. Αν p, q είναι πρώτοι αριθμοί διαφορετικοί μεταξύ τους, να αποδειχτεί ότι
$$p^{q-1}+q^{p-1} \equiv 1 \bmod pq.$$
18. Αν για τον ακέραιο αριθμό a και για τον φυσικό αριθμό m ισχύει $(a,m)=1$ και $(a-1,m)=1$, να αποδειχτεί ότι ισχύει:
$$1+a+a^2+\cdots+a^{\phi(m)-1} \equiv 0 \bmod m.$$
19. Αν $0 < s < p$, όπου p πρώτος αριθμός, να αποδειχτεί ότι ισχύει
$$(s-1)!(p-s)!+(-1)^{s-1} \equiv 0 \bmod p.$$
20. Να λυθεί το σύστημα
$$x \equiv 3 \bmod 25, x \equiv 1 \bmod 27, x \equiv 4 \bmod 11.$$

Βιβλιογραφία

Stein, W. 2008. *Elementary Number Theory: Primes, Congruences, and Secrets: A Computational Approach*. Undergraduate Texts in Mathematics. Springer New York. https://books.google.gr/books?id=5hYd0yX4mrMC.

Αντωνιάδης, Ι., και Α. Κοντογεώργης. 2015. *Θεωρία Αριθμών Και Εφαρμογές*. Εκδόσεις Κάλλιπος.

Λάκκης, Κ. 1990. *Θεωρία Αριθμών*. Εκδόσεις Ζήτη.

2

Στοιχεία Θεωρίας Δακτυλίων

2.1. Βασικοί ορισμοί

Στο πρώτο κεφάλαιο είδαμε βασικά στοιχεία της αριθμητικής του δακτυλίου των ακέραιων $\mathbb{Z}$. Θα δούμε ότι είναι χρήσιμο να αντικαταστήσουμε τον δακτύλιο $\mathbb{Z}$ με έναν γενικότερο δακτύλιο R.

Ο άνθρωπος σκέφτεται αφαιρετικά. Μία από τις πρώτες αφαιρέσεις που μαθαίνει κανείς είναι αυτή των φυσικών αριθμών. Η έννοια του αριθμού 3 εκφράζει τον πληθικό αριθμό ενός συνόλου και είναι ανεξάρτητη από τη φύση των στοιχείων που περιέχει το σύνολο με 3 το πλήθος στοιχεία. Το επόμενο βήμα είναι να απομονώσουμε τις πράξεις από τη φύση των συνόλων στα οποία αναφέρονται και να μελετήσουμε τις ιδιότητες των πράξεων από μόνες τους.

Ξεκινάμε να δώσουμε μερικούς ορισμούς. Για περισσότερες πληροφορίες ο αναγνώστης μπορεί να συμβολευτεί ένα οποιοδήποτε βιβλίο άλγεβρας, όπως το (Βάρσος et al. 2012), (Fraleigh 2011).

2.1.1 Ορισμός:
Ένας αντιμεταθετικός δακτύλιος R *με μονάδιαίο είναι ένα σύνολο* R *εφοδιασμένο με δύο πράξεις*

$$+ : R \times R \to R$$

$$(x, y) \mapsto x + y$$

και

$$\cdot : R \times R \to R$$

$$(x, y) \mapsto x \cdot y,$$

οι οποίες ικανοποιούν (για κάθε $x, y, z \in R$*):*

$$x + (y + z) = (x + y) + z$$

$$x \cdot (y \cdot z) = (x \cdot y) \cdot z$$

$$x(y + z) = xy + xz$$

Επιπλέον, απαιτούμε να υπάρχουν στοιχεία $1, 0 \in R$, $1 \neq 0$, *ώστε*

$$0 + x = 0 \quad 1x = x$$

και για κάθε στοιχείο $x \in R$ *απαιτούμε να υπάρχει ένα στοιχείο* $-x \in R$ *ώστε* $x + (-x) = 0$.

$$x \cdot y = y \cdot x$$

Παραδείγματα

1. Ο δακτύλιος $\mathbb{Z}$ των ακέραιων αριθμών εφοδιασμένος με τις συνηθισμένες πράξεις είναι αντιμεταθετικός δακτύλιος με μονάδα.
2. Ο δακτύλιος των πολυωνύμων $R[x]$ με συντελεστές από έναν αντιμεταθετικό δακτύλιο R αποτελεί αντιμεταθετικό δακτύλιο με μοναδιαίο. Για παράδειγμα, μπορούμε να θεωρήσουμε τον δακτύλιο $\mathbb{Z}[x]$, αλλά και να συνεχίσουμε επαγωγικά για να ορίζουμε τον δακτύλιο

$$\mathbb{Z}[x, y] = \mathbb{Z}[x][y].$$

Σε έναν δακτύλιο R θέλουμε να δημιουργήσουμε δακτύλιους πηλίκο ως προς κατάλληλες σχέσεις ισοδυναμίας. Για να το επιτύχουμε χρειαζόμαστε την έννοια του ιδεώδους:

2.1.2 Ορισμός:
Ένα υποσύνολο $I \neq \emptyset$ *του δακτύλιου* R *είναι ιδεώδες αν για κάθε* $x, y \in I$ *ισχύει*

$$x - y \in I$$

και αν για κάθε $x \in I$ *και* $r \in R$ *ισχύει*

$$rx \in I$$

Παράδειγμα Αν επιλέξουμε ένα στοιχείο $f \in R$ μπορούμε να θεωρήσουμε το ιδεώδες fR που αποτελείται από όλα τα πολλαπλάσια του f. Ιδεώδη αυτής της μορφής θα λέγονται *κύρια*.

Θα αποδείξουμε στη συνέχεια ότι κάθε ιδεώδες των δακτυλίων $\mathbb{Z}$ και $\mathbb{F}[x]$, όπου $\mathbb{F}$ είναι σώμα, είναι κύριο. Αντιθέτως στον δακτύλιο $\mathbb{F}[x, y]$ το ιδεώδες $\langle x, y\rangle$ που παράγεται από τα x, y δεν είναι κύριο.

Παρατήρηση Από τις ιδιότητες του δακτυλίου είναι άμεσο ότι $0 \cdot a = 0$. Πράγματι
$0 \cdot a = (0 + 0)a = 0 \cdot a + 0 \cdot a$ άρα $0 \cdot a = 0$.
Ένας αντιμεταθετικός δακτύλιος με μοναδιαίο θα λέγεται ακέραια περιοχή αν και μόνο αν
$x \cdot y = 0$ συνεπάγεται $x = 0$ ή $y = 0$.

Παράδειγμα Ο δακτύλιος $\mathbb{Z}$ είναι ακέραια περιοχή. Αντιθέτως, ο δακτύλιος $\mathbb{Z}/6\mathbb{Z}$ δεν είναι ακέραια περιοχή, αφού $2 \neq 0$ και $3 \neq 0$ όμως $2 \cdot 3 \equiv 0 \mathrm{mod} p$.

2.1.3 Ορισμός:
Μια ακέραια περιοχή θα λέγεται περιοχή κύριων ιδεωδών όταν κάθε ιδεώδες της είναι κύριο.

2.1.4 Ορισμός:
Ένα σύνολο G *θα λέγεται ομάδα αν είναι εφοδιασμένο με μία πράξη*

$$\cdot : G \times G \to G$$
$$(g, g') \mapsto gg'$$

ώστε για κάθε g_1, g_2, g_3 *να ισχύουν*

$$g_1(g_2g_3) = (g_1g_2)g_3$$

Υπάρχει στοιχείο $e \in G$ *ώστε για κάθε* $g \in G$

$$eg = ge = g$$

Για κάθε στοιχείο $g \in G$ *υπάρχει* $g^{-1} \in G$ *ώστε*

$$gg^{-1} = g^{-1}g = e$$

Αν επιπλέον για κάθε $g, g' \in G$ *ισχύει*

$$gg' = g'g$$

τότε η ομάδα λέγεται αντιμεταθετική ή αβελιανή.

Παράδειγματα

1. Η πράξη $+$ σε κάθε δακτύλιο R δίνει στον R δομή αβελιανής ομάδας.
2. Σε κάθε δακτύλιο R μπορούμε να ορίσουμε την *ομάδα των μονάδων*

$U(R) = \{x \in R$ για τα οποία υπάρχει $x^{-1} \in R$ ώστε $xx^{-1} = 1\}$.

Παρατηρούμε ότι $U(\mathbb{Z}) = \{\pm 1\}$. Επίσης $U(\mathbb{R}[x]) = \mathbb{R}^*$. Τέλος ιδιαίτερα ενδιαφέρουσα είναι η δομή της ομάδας $U\big((\mathbb{Z}/n\mathbb{Z})^*\big)$ η οποία έχει $\phi(n)$ το πλήθος στοιχεία.

2.1.5 Ορισμός:
Ένας αντιμεταθετικός δακτύλιος R *με μοναδιαίο στοιχείο* 1_R *για τον οποίο ισχύει* $U(R) = R - \{0\}$ *θα λέγεται σώμα.*

Παρατήρηση Αν ένα ιδεώδες I περιέχει ένα στοιχείο του $U(R)$, τότε $I = R$. Πράγματι, ένα τέτοιο ιδεώδες περιέχει το 1 του R και συνεπώς όλο τον δακτύλιο. Αυτό έχει ως συνέπεια ότι κάθε ιδεώδες ενός σώματος είναι ή μηδενικό ή όλος ο δακτύλιος R.

Παρατήρηση Το $\mathbb{Z}$ είναι ακέραια περιοχή αλλά όχι σώμα. Αν όμως έχουμε μια πεπερασμένη ακέραια περιοχή, τότε αναγκαστικά αυτή είναι σώμα. Πράγματι γράφουμε όλα τα στοιχεία της στη μορφή $a_1 = 0, a_2 = 1, \ldots, a_n$. Θεωρούμε στη συνέχεια ένα μη μηδενικό στοιχείο $a \in R$ και πολλάπλασιάζουμε κάθε στοιχείο με a. Τα στοιχεία

$$aa_1 = 0, aa_2, \ldots, aa_n$$

είναι ανά δύο διαφορετικά, αφού, αν $aa_i = aa_j$, τότε $a(a_i - a_j) = 0$ άρα αφού έχουμε ακέραια περιοχή και $a \neq 0$ θα έχουμε $a_i = a_j$. Άρα με τον πολλαπλασιασμό με a παίρνουμε κάθε στοιχείο του δακτυλίου R, άρα για κάποιο a_i θα πάρουμε $aa_i = 1$.

2.2. Δακτύλιος πηλίκο

Όπως ακριβώς κάναμε στους δακτυλίους $\mathbb{Z}/m\mathbb{Z}$ ορίζουμε για ένα ιδεώδες I τη σχέση ισοδυναμίας

$$a \sim b \Leftrightarrow b - a \in I.$$

Το ότι το παραπάνω είναι μια σχέση ισοδυναμίας είναι άμεσο από τις ιδιότητες του ιδεώδους. Ως μια σχέση ισοδυναμίας χωρίζει τον δακτύλιο σε μια ξένη ένωση κλάσεων ισοδυναμίας. Το σύνολο πηλίκο R/I αποτελείται από αυτές τις κλάσεις ισοδυναμίας.

Ένα τυχαίο στοιχείο του R/I αποτελείται από στοιχεία της μορφής

$$a + I = \{a + i, i \in I\},$$

ενώ εξ ορισμού $a + I = b + I$ αν και μόνο αν $a = b + i$ για κάποιο $i \in I$.

Θα δείξουμε ότι το R/I μπορεί να εφοδιαστεί με δομή δακτυλίου. Πράγματι, ορίζουμε το άθροισμα των κλάσεων

$$(a + I) + (b + I) = (a + b) + I$$
$$(a + I)(b + I) = ab + I.$$

Οι παραπάνω πράξεις ορίστηκαν με βάση τους αντιπροσώπους των κλάσεων. Θα πρέπει να δείξουμε ότι είναι καλά ορισμένες, δηλαδή ανεξάρτητες των αντιπροσώπων που ορίζουν μια κλάση. Πράγματι, ας υποθέσουμε ότι $a + I = a' + I$ και $b + I = b' + I$, δηλαδή $a' = a + x$, $b' = b + y$ για κάποια στοιχεία $x, y \in I$. Θα πρέπει να δείξουμε ότι $a + b \sim a' + b'$ και ότι $ab \sim a'b'$. Πράγματι, το πρώτο ισχύει αφού $a' + b' = a + b + x + y$ και $x + y \in I$. Για το δεύτερο έχουμε

$$a'b' = (a + x)(b + y) = ab + xb + xy + ay,$$

και το ζητούμενο ισχύει αφού από τις ιδιότητες του ιδεώδους $xb + xy + ay \in I$.

Από τη στιγμή που έχουμε δείξει ότι οι πράξεις είναι καλά ορισμένες οι υπόλοιπες ιδιότητες του δακτυλίου κληρονομούνται από αυτές του R.

Η μονάδα του δακτυλίου R/I είναι το στοιχείο $1 + I$ ενώ το μηδενικό είναι το στοιχείο $0 + I$.

2.3. Ομομορφισμοί δακτυλίων

Μία συνάρτηση $\phi : R \to S$ θα λέγεται ομομορφισμός δακτυλίων αν για κάθε $x, y \in R$

$$\phi(x + y) = \phi(x) + \phi(y)$$

και

$$\phi(xy) = \phi(x)\phi(y).$$

Ένας ομομορφισμός που είναι *επί* θα λέγεται επιμορφισμός, ένας ομορφισμός που είναι *1-1* θα λέγεται μονομορφισμός και ένας μονομορφισμός που είναι ταυτόχρονα και επιμορφισμός θα λέγεται ισομορφισμός.

2.3.1 Ορισμός:
Θα ονομάζουμε πυρήνα ένος ομομορφισμού και θα το συμβολίζουμε με $ker(\phi)$ *το σύνολο:*

$$ker(\phi) = \{x \in R : \phi(x) = 0\}.$$

Θα ονομάζουμε εικόνα ενός ομομορφισμού τον υποδακτύλιο του S *που αποτελείται από τα στοιχεία* y *για τα οποία υπάρχει* $x \in R$ *ώστε* $y = \phi(x)$. *Την εικόνα θα τη συμβολίζουμε με* $Im(\phi)$.

Παρατήρησεις

1. Ο πυρήνας ενός ομορφισμού είναι ιδεώδες του δακτυλίου R.
2. Ένας ομομορφισμός ϕ είναι μονομορφισμός αν και μόνο αν $\ker\phi = \{0\}$.
3. Εξ ορισμού η συνάρτηση
$$\pi : R \to R/I$$
$$x \mapsto x + I$$
είναι επιμορφισμός.

2.3.2 Θεώρημα:
Θεωρούμε έναν ομομορφισμό $\phi : R \to S$ *δακτυλίων. Υπάρχει μονομορφισμός*
$$\overline{\phi} : R/ker\phi \to Im(\phi) \subset S$$
ο οποίος ικανοποιεί επιπλέον $\overline{\phi} \circ \pi = \phi$. *Οι δακτύλιοι* $R/ker(\phi)$ *και* $Im(\phi)$ *είναι ισόμορφοι.*

Απόδειξη: Θεωρούμε το σύνολο R/I το οποίο αποτελείται από τις κλάσεις $x + \ker(\phi)$. Ορίζουμε
$$\overline{\phi}(x + I) = \phi(x).$$
Η συνάρτηση αυτή, αν είναι καλά ορισμένη, είναι ομομορφισμός και ικανοποιεί εκ κατασκευής την ιδιότητα $\overline{\phi} \circ \pi = \phi$.

Χρειάζεται να αποδείξουμε ότι είναι καλά ορισμένη γιατί την ορίσαμε με βάση τον αντιπρόσωπο της κλάσης και πρέπει να δείξουμε ότι είναι ανεξάρτητη του αντιπροσώπου.

Όμως, αν $x + \ker(\phi) = y + \ker(\phi)$, τότε $x = y + h$, όπου $h \in \ker(\phi)$. Άρα
$$\phi(x) = \phi(x + h) = \phi(x) + \phi(h) = \phi(x).$$

Τέλος, για να δείξουμε ότι η ϕ είναι μονομορφισμός παρατηρούμε ότι
$$\ker(\overline{\phi}) = \{x + \ker(\phi) : \phi(x) = 0\}$$
και αυτό σημαίνει ότι $x \in \ker\phi$, δηλαδή ο πυρήνας της $\overline{\phi}$ είναι το μηδενικό στοιχείο του δακτυλίου $R/\ker(\phi)$. □

Για τις ανάγκες αυτού του μαθήματος θα χρειαστούμε τους δακτυλίους $\mathbb{Z}$ και $\mathbb{F}[x]$, όπου το F είναι ένα σώμα. Οι δακτύλιοι αυτοί μοιράζονται πολλές ιδιότητες και οι ομοιότητές τους ήταν μία από τις κινητήριες δυνάμεις στην ανάπτυξη της θεωρίας αριθμών και της αριθμητικής γεωμετρίας

Και στους δύο δακτυλίους υπάρχει ένα θεώρημα διαίρεσης με πηλίκο και υπόλοιπο.

2.4. Πολυώνυμα

2.4.1 Ορισμός:
Θεωρούμε την ακέραια περιοχή R. *Ορίζουμε τον δακτύλιο* $R[x]$ *να έχει ως στοιχεία του τα πολυώνυμα, δηλαδή πεπερασμένα αθροίσματα*
$$f(x) = \sum_{\nu=0}^{n} a_\nu x^n,$$

όπου $a_\nu \in R$. *Το μεγαλύτερο* ν *ώστε* $a_\nu \neq 0$ *ονομάζεται βαθμός του πολυωνύμου και θα το συμβολίζουμε με* $deg(f)$.
Το άθροισμα δύο πολυωνύμων $f(t) = \sum_{\nu=0}^{n} a_\nu x^n$ *και* $g(t) = \sum_{\nu=0}^{m} b_\nu x^n$ *το ορίζουμε ως*

$$f(t) + g(t) = \sum_{\nu=0}^{n} (a_\nu + b_\nu) x^n,$$

όπου αν $n < m$ *θέσαμε* $a\nu = 0$ *για τα* $\nu > n$.
Το γινόμενο δύο πολυωνύμων ορίζεται ως εξής:

$$f(t) \cdot g(t) = \sum_{\nu=0}^{n} \sum_{\mu=0}^{m} a_\nu b_\mu x^{\nu+\mu}$$
$$= \sum_{\nu=0}^{n+m} \sum_{\mu=0}^{n+m} a_\nu b_{n+m-\mu} x^\nu$$

Με $\mathbb{F}$ θα συμβολίζουμε ένα σώμα. Η συνάρτηση βαθμού

$$deg : \mathbb{F}[x] - \{0\} \to \mathbb{N},$$

ικανοποιεί

$$deg(f + g) \leqslant \max(deg(f), deg(g))$$
$$deg(fg) = deg(f) + def(g).$$

Παρατηρήστε ότι δεν ορίζουμε τον βαθμό του μηδενικού πολυωνύμου.

2.4.2 Θεώρημα:

1. *Για κάθε δύο στοιχεία* $a, b \in \mathbb{Z}$ *υπάρχουν στοιχεία* $\pi, u \in \mathbb{Z}$ *ώστε* $a = b\pi + u$ *με* $0 \leqslant u < |b|$.
2. *Για κάθε δύο στοιχεία* $a, b \in \mathbb{F}[x]$ *υπάρχουν στοιχεία* $\pi, u \in \mathbb{F}[x]$ *ώστε* $a = b\pi + u$ *με* $u = 0$ *ή* 0 *deg*$u <$ *deg*(b).

Άμεση εφαρμογή του παραπάνω Θεωρήματος είναι το

2.4.3 Θεώρημα:
Κάθε ιδεώδες του δακτυλίου $\mathbb{Z}$ *ή* $\mathbb{F}[x]$ *είναι κύριο.*

Απόδειξη Αν έχουμε ένα ιδεώδες του $\mathbb{Z}$ το οποίο είναι μη μηδενικό, τότε έχει ένα στοιχείο που είναι θετικό. Θεωρούμε το ελάχιστο στοιχείο n του μη κενού συνόλου των θετικών στοιχείων του ιδεώδους I. Κάθε στοιχείο a του I είναι πολλαπλάσιο του n. Αυτό γιατί αν γράψουμε το τυχαίο στοιχείο $a \in I$ ως

$$a = \pi n + u, 0 \leqslant u < n,$$

τότε το $u \in I$ και συνεπώς είναι μηδενικό, αλλιώς το n δεν θα ήταν το ελάχιστο θετικό στοιχείο του ιδεώδους.

Στην περίπτωση που το δεν είναι μηδενικό ιδεώδες του δακτυλίου $\mathbb{F}[x]$ θα έχει ένα στοιχείο g ελαχίστου βαθμού. Κάθε στοιχείο $a \in I$ είναι αναγκαστικά πολλαπλάσιο του g. Σε διαφορετική περίπτωση γράφουμε

$$a = g\pi + u, \deg(u) < \deg(g)$$

και αφού το $u \in I$, καταλήγουμε σε άτοπο (το g κατασκευάστηκε να είναι ελαχίστου βαθμού στο ιδεώδες). □

2.4.1. Ανάγωγα Πολυώνυμα Κριτήρια Αναγωγισιμότητας.

2.4.4 Ορισμός:
Έστω R μια ακέραια περιοχή. Ένα πολυώνυμο $f \in R[x]$ θα λέγεται ανάγωγο αν δεν μπορεί να διασπαστεί ως γινόμενο δύο πολυωνύμων $f = gh$ με $deg(g), deg(h) \geqslant 1$.

Παρατήρησεις:

1. Το πολυώνυμο f είναι ανάγωγο αν και μόνο αν το ιδεώδες $fR[x]$ είναι πρώτο.
2. Στην περίπτωση που το R είναι σώμα το πολυώνυμο f είναι ανάγωγο αν και μόνο αν το πηλίκο $R[x]/fR[x]$ είναι σώμα.
3. Η έννοια της αναγωγισιμότητας εξαρτάται από το σώμα ή τον δακτύλιο συντελεστών. Έτσι το πολυώνυμο $x^2 + 1$ είναι ανάγωγο στον δακτύλιο $\mathbb{R}[x]$ αλλά όχι στον $\mathbb{C}[x]$.

2.4.5 Πρόταση:
Ας υποθέσουμε ότι έχουμε ένα ανάγωγο πολυώνυμο $f \in \mathbb{F}[x]$, και το $\mathbb{F}$ είναι σώμα. Τότε ο δακτύλιος πηλίκο $\mathbb{F}[x]/f\mathbb{F}[x]$ είναι ένα σώμα που περιέχει το σώμα $\mathbb{F}$ στο οποίο το πολυώνυμο f έχει μία ρίζα.

Απόδειξη Αφού το πολυώνυμο f είναι ανάγωγο, το πηλίκο $K := \mathbb{F}[x]/f\mathbb{F}[x]$ είναι σώμα. Το σώμα $\mathbb{F}$ μπορεί να θεωρηθεί ως υπόσωμα του σώματος K αφού κάθε στοιχείο $a \in \mathbb{F}$ μπορεί να θεωρηθεί ως το σταθερό πολυώνυμο.

Στον πολυωνυμικό δακτύλιο $\mathbb{F}[x]$ εισαγάγουμε τη μεταβλητή x και όλες τις πολυωνυμικές της εκφράσεις. Τέλος, στο πηλίκο επιβάλλουμε εξ' ορισμού τον μηδενισμό του $f(x)$, δηλαδή επιβάλλουμε στο x να είναι ρίζα του πολυωνύμου f. □

Παράδειγμα Θεωρούμε το ανάγωγο πολυώνυμο $f(x) = x^2 + 1 \in \mathbb{R}[x]$. Πράγματι το πολυώνυμο αυτό είναι ανάγωγο αφού είναι βαθμού 2 και δεν έχει πραγματικές ρίζες. Ο δακτύλιος πηλίκο $\mathbb{R}[x]/\langle x^2 + 1\rangle$ είναι εξ ορισμού το σώμα των μιγαδικών αριθμών.

2.4.1.1. *Κριτήρια Αναγωγισιμότητας.*

2.4.6 Πρόταση:
Ένα πολυώνυμο βαθμού 2 ή 3 στο $\mathbb{F}[x]$, όπου $\mathbb{F}$ σώμα, δεν είναι ανάγωγο αν και μόνο έχει μία τουλάχιστον ρίζα.

ΑπόδειξηΗ ύπαρξη ρίζας ρ του πολυωνύμου f είναι ισοδύναμη με το ότι $(x - \rho) \mid f$, άρα, αν ένα οποιουδήποτε βαθμού $\geqslant 2$ πολυώνυμο έχει ρίζα, τότε δεν μπορεί να είναι ανάγωγο. Αντιστρόφως, ένα πολυώνυμο βαθμού αν διασπάται, τότε θα είναι γινόμενο δύο πολυωνύμων βαθμού 1 και αν ένα

πολυώνυμο βαθμού 3 τότε θα είναι γινόμενο ή τριών πολυωνύμων βαθμού 1 ή ενός πολυωνύμου βαθμού ένα και ενός πολυωνύμου βαθμού 2. Σε κάθε περίπτωση η ύπαρξη παράγοντα βαθμού ένα εξασφαλίζει την ύπαρξη ρίζας.

Παρατήρηση Μπορεί ένα πολυώνυμο στο $\mathbb{F}[x]$ βαθμού $\geqslant 4$ χωρίς να έχει ρίζες στο $\mathbb{F}$ να μην είναι ανάγωγο. Για παράδειγμα στο $\mathbb{Q}[x]$ μπορούμε να θεωρήσουμε το $(x^2+1)(x^2-2)$.

Στην περίπτωση που θεωρούμε πολυώνυμα στο $\mathbb{Q}[x]$ ισχύει το παρακάτω θεώρημα, γνωστό και ως *λήμμα του Gauss*:

2.4.7 Θεώρημα:
Ας θεωρήσουμε ένα πολυώνυμο $f(x) \in \mathbb{Z}[x]$ βαθμού μεγαλύτερου του μηδενός. Αν το f είναι ανάγωγο στο $\mathbb{Z}[x]$ τότε είναι ανάγωγο και στον $\mathbb{Q}[x]$. Επίσης, αν ο μέγιστος κοινός διαιρέτης των συντελεστών του f είναι μονάδα και το f είναι ανάγωγο στο $\mathbb{Q}[x]$, τότε είναι ανάγωγο και στο $\mathbb{Z}[x]$.

Απόδειξη Ένα πολυώνυμο $f(x) \in \mathbb{Z}[x]$ της μορφής

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n$$

θα λέγεται *πρωταρχικό* αν ο μέγιστος κοινός διαιρέτης των συντελεστών του είναι 1. Προφανώς κάθε πολυώνυμο είναι γινόμενο ενός πρωταρχικού πολυωνύμου και ενός στοιχείου του $\mathbb{Z}$.

Παρατηρούμε ότι το γινόμενο δύο πρωταρχικών πολυωνύμων $f, g \in \mathbb{Z}[x]$ είναι πρωταρχικό πολυώνυμο. Πράγματι, αν ο μέγιστος κοινός διαιρέτης των συντελεστών του γινομένου $f \cdot g$ δεν ήταν ένα, τότε θα υπήρχε ένας πρώτος p που θα τον διαιρούσε. Αυτό σημαίνει ότι το πολυώνυμο $f \cdot g$ θα ήταν 0 στον δακτύλιο $\mathbb{Z}/p\mathbb{Z}[x]$. Ο τελευταίος δακτύλιος όμως είναι δακτύλιος πολυωνύμων πάνω από ένα σώμα, άρα είναι ακέραια περιοχή. Συνεπώς ή όλοι οι συντελεστές του f θα είναι 0 modulo p ή όλοι οι συντελεστές του g θα είναι 0 modulo p. Και οι δύο δυνατότητες είναι αδύνατες, αφού ξεκινήσαμε από πρωταρχικά πολυώνυμα.

Ας υποθέσουμε ότι ένα μη σταθερό $f \in \mathbb{Z}[x]$ αναλύεται σε γινόμενο πολυώνυμων στον $\mathbb{Q}[x]$, δηλαδή

$$f = h_1 \cdot h_2, \quad h_1, h_2 \in \mathbb{Q}[x].$$

Πολλαπλασιάζοντας με έναν μεγάλο ακέραιο d (για παράδειγμα με το ελάχιστο κοινό πολλαπλάσιο των παρονομαστών όλων των συντελεστών) μπορούμε να έχουμε ότι:

$$d \cdot f = h_1' \cdot h_2',$$

όπου τα $h_1', h_2' \in \mathbb{Z}$. Τα πολυώνυμα h_i' τα γράφουμε στη μορφή $h_i' = d_i h_i''$, όπου $d_i \in \mathbb{Z}$ και τα h_i'' είναι πρωταρχικά πολυώνυμα. Επειδή το $h_1'' \cdot h_2''$ είναι πρωταρχικό πολυώνυμο, έχουμε ότι $d = d_1 d_2$ και $f = h_1'' h_2''$ το οποίο είναι άτοπο.

Το αντίστροφο είναι προφανές. □

Το επόμενο κριτήριο είναι γνωστό ως κριτήριο Eisenstein

2.4.8 Θεώρημα:
Έστω p πρώτος. Υποθέτουμε ότι το

$$f(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$$

Σχήμα 2.1. G. Eisenstein 1823-1852, Το παρόν έργο αποτελεί κοινό κτήμα (public domain). Πηγή: Wikimedia Commons

είναι τέτοιο ώστε $a_n \neq 0$, $p \mid a_i$ *για όλα τα* $i = 0, \ldots, n-1$ *και ο* p *δεν διαιρεί τα* a_n, *ενώ ο* p^2 *δεν διαιρεί το* a_0. *Τότε το* $f(x)$ *είναι ανάγωγο στο* $\mathbb{Q}[x]$.

Απόδειξη Σύμφωνα με το λήμμα του Gauss αρκεί να δείξουμε ότι το f δεν αναλύεται ως γινόμενο πολυωνύμων με βαθμούς μεγαλύτερους της μονάδας στον δακτύλιο $\mathbb{Z}[x]$.

Ας υποθέσουμε ότι είχαμε μια γραφή

$$f(x) = (b_t x^t + \cdots b_1 x + b_0)(c_s x^s + \cdots + c_1 x + c_0),$$

όπου $b_t c_s \neq 0$ και $b_\nu, c_\mu \in \mathbb{Z}$.

Αφού p^2 δεν διαιρεί το $a_0 = b_0 c_0$, είναι σαφές ότι το p δεν μπορεί να διαιρεί και το b_0 και το c_0. Ας υποθέσουμε ότι ο p διαιρεί το c_0 και ότι δεν διαιρεί το b_0. Με τον ίδιο τρόπο βλέπουμε ότι αφού ο p δεν διαιρεί το a_n έχουμε ότι ο p δεν διαιρεί το b_t και ο p δεν διαιρεί το c_s. Έστω c_r η μικρότερη τιμή ώστε ο p να μην διαιρεί το c_r. Υπολογίζουμε

$$a_r = b_0 c_r + b_1 c_{r-1} + \cdots + b_{r-i} c_i + \cdots + b_r c_0$$

για κάποιο $0 \leqslant i < r$. Στον παραπάνω τύπο τα $c_{r-1}, \ldots, c_i$ είναι διαιρετά με p όπως και το a_r είναι διαιρετό με p. Όμως το $b_0 c_r$ δεν είναι,άτοπο. □

Παραδείγματα

1. Το πολυώνυμο $x^2 - a$ όσο το a δεν είναι τετράγωνο είναι ανάγωγο στο $\mathbb{Q}[x]$. Πράγματι, αφού το a δεν είναι τετράγωνο υπάρχει $p \mid a$ και ο p^2 δεν διαιρεί το a. Το ζητούμενο προκύπτει από το κριτήριο του Eisenstein.
2. Το πολυώνυμο $x^{2015} + 4x + 2$ είναι ανάγωγο στο $\mathbb{Q}[x]$, όπως βλέπουμε με χρήση του κριτηρίου του Eisenstein για $p = 2$.
3. Έστω p πρώτος. Το πολυώνυμο
$$\Phi_p(x) := x^{p-1} + x^{p-2} + \cdots + x + 1$$
είναι ανάγωγο στο $\mathbb{Q}[x]$.

Παρατηρούμε ότι ένα πολυώνυμο $f(x)$ είναι ανάγωγο αν και μόνο αν το $f(x+1)$ είναι ανάγωγο. Θεωρούμε λοιπόν το πολυώνυμο

$$\Phi_p(x+1) = \frac{(x+1)^p - 1}{(x+1) - 1} = \sum_{\nu=1}^{p} \binom{p}{\nu} x^{\nu-1}$$

το οποίο πληρεί τις προϋποθέσεις του κριτηρίου του Eisenstein.

```
sage:Phi=cyclotomic_polynomial(105,'x');Phi
x^48 + x^47 + x^46 - x^43 - x^42 - 2*x^41 - x^40 -x^39 + x^36
+x^35 +x^34 + x^33 + x^32 + x^31 - x^28 - x^26 - x^24 - x^22
- x^20 + x^17 +x^16 + x^15 + x^14 + x^13 + x^12 - x^9 - x^8
- 2*x^7 - x^6 - x^5 + x^2 +x + 1
sage:Phi.is_irreducible()
True
```

Interactive

2.4.2. Χαρακτηριστική δακτυλίου. Παρατήρηση Αν ένα σύνολο Σ παράγει τον δακτύλιο R και δεν υπάρχουν αλγεβρικές σχέσεις μεταξύ των στοιχείων του Σ, δηλαδή κάθε στοιχείο του R μπορεί να γραφεί με μοναδικό τρόπο ως αποτέλεσμα των δύο πράξεων του δακτυλίου με πράξεις μεταξύ των στοιχείων του Σ, τότε κάθε συνάρτηση $\phi : \Sigma \to S$ μπορεί να επεκταθεί σε ομομορφισμό $\phi : R \to S$.

Περισσότερο συγκεκριμένα ένας μη μηδενικός ομομορφισμός $\mathbb{Z} \to S$ προσδιορίζεται μονοσήμαντα αν γνωρίζουμε το $\phi(1)$ το οποίο στην περίπτωση που ο S είναι ακέραια περιοχή δεν μπορεί να είναι άλλο από το μοναδιαίο του S. Πράγματι

$$\phi(1_{\mathbb{Z}}) = \phi(1_{\mathbb{Z}} \cdot 1_{\mathbb{Z}}) = \phi(1_{\mathbb{Z}})\phi(1_{\mathbb{Z}})$$

Δηλαδή

$$\phi(1_{\mathbb{Z}})(1_S - \phi(1_{\mathbb{Z}})) = 0$$

από όπου προκύπτει το ζητούμενο.

2.4.9 Ορισμός:

Έστω S δακτύλιος αντιμεταθετικός με μοναδιαίο θεωρούμε τον ομομορφισμό

$$\phi : \mathbb{Z} \to S$$

$$1_{\mathbb{Z}} \mapsto 1_S.$$

Ο πυρήνας είναι ένα κύριο ιδεωδές του $\mathbb{Z}$, δηλαδή $ker(\phi) = n\mathbb{Z}$. Τον αριθμό n θα τον λέμε χαρακτηριστική του δακτυλίου S.

Παρατηρήσεις:

1. Αν ο πυρήνας του ϕ είναι μηδενικός, τότε ο δακτύλιος S έχει χαρακτηριστική 0 και σε αυτή την περίπτωση ο δακτύλιος S είναι άπειρος.
2. Από το θεώρημα ισομορφισμού ο $\mathbb{Z}/n\mathbb{Z}$ είναι ένας υποδακτύλιος του S. Αν ο S είναι ακέραια περιοχή, τότε αναγκαστικά n είναι πρώτος αριθμός.
3. Κάθε πεπερασμένο σώμα περιέχει το $\mathbb{Z}/p\mathbb{Z}$ για κάποιο πρώτο p ως υπόσωμα.

2.4.10 Ορισμός:
Ένα ιδεώδες P του δακτυλίου R θα λέγεται πρώτο αν και μόνο αν για κάθε $a, b \in R$ $ab \in P$ συνεπάγεται $a \in P$ είτε $b \in P$.
Το ιδεώδες M θα λέγεται μέγιστο αν κάθε ιδεώδες I του R ώστε $M \subset I$ επιβάλλει $I = R$ ή $I = M$.

2.4.11 Θεώρημα:
Ένα ιδεώδες P είναι πρώτο αν και μόνο αν ο δακτύλιος R/P είναι ακέραια περιοχή.

Απόδειξη Θεωρούμε το γινόμενο $(a + P)(b + P) = ab + P$. Παρατηρούμε ότι $ab \in P$ είναι ισοδύναμο με το $ab + P = 0_{R/P}$ είναι 0 στον δακτύλιο R/P. Ομοίως $a + P = 0_{R/P}$ (αντίστοιχα $b + P = 0_{R/P}$) είναι ισοδύναμο με $a \in P$ (αντίστοιχα $b \in P$). Το ζητούμενο είναι σαφές από τον ορισμό της ακέραιας περιοχής. □

2.4.12 Θεώρημα:
Ένα ιδεώδες M είναι μέγιστο αν και μόνο αν ο δακτύλιος R/M είναι σώμα.

Απόδειξη Ας υποθέσουμε ότι το M είναι ένα μέγιστο ιδεώδες. Η κλάση $x + M$ είναι μη μηδενική κλάση αν και μόνο αν $x \notin M$. Σε αυτή την περίπτωση το ιδεώδες $M + xR$, που παράγεται από τα στοιχεία του M και το x είναι ένα ιδεώδες που περιέχει γνήσια το M.

Στην περίπτωση που το M είναι μέγιστο το $M + xR$ είναι όλος ο δακτύλιος R άρα το μοναδιαίο 1_R του δακτυλίου γράφεται ως $1_R = m + xa$ για κάποια στοιχεία $m \in M$ και $a \in R$. Αυτό όμως σημαίνει ότι $(a + M)(x + M) = 1 + M$, άρα η τυχαία μη μηδενική κλάση $x + M$ είναι αντιστρέψιμη και το R/M είναι σώμα.

Αντιστρόφως, έστω ότι R/M είναι σώμα. Αν το M περιέχεται γνήσια σε ένα ιδεώδες I, τότε το I περιέχει ένα στοιχείο $x \notin M$, και συνεπώς η κλάση $x + M$ είναι αντιστρέψιμη, δηλαδή υπάρχει $a \in R$ ώστε $(x + M)(a + M) = 1 + M$. Η τελευταία σχέση είναι ισοδύναμη με το ότι $xa = 1_R + m$ για κάποιο στοιχείο $m \in M$. Τότε όμως το $1_R = xa - m$ είναι στοιχείο του I και συνεπώς $I = R$. □

Παρατηρήσεις

1. Το ιδεώδες $p\mathbb{Z}$ για p πρώτο αριθμό είναι πρώτο και μέγιστο ιδεώδες του $\mathbb{Z}$.
2. Αν f είναι ένα ανάγωγο πολυώνυμο του $\mathbb{F}[x]$, τότε το ιδεώδες $f(x)\mathbb{F}[x]$ είναι και πρώτο και μέγιστο.
3. Το μηδενικό ιδεώδες είναι πρώτο αν και μόνο αν ο δακτύλιος R είναι ακέραια περιοχή.
4. Κάθε μέγιστο ιδεώδες είναι πρώτο.
5. Υπάρχουν πρώτα ιδεώδη που δεν είναι μέγιστα όπως το $p\mathbb{Z}[x] \subset \mathbb{Z}[x]$ ή το $x\mathbb{F}[x, y] \subset \mathbb{F}[x, y]$.

2.4.3. Γεωμετρική Θεώρηση. Η θεωρία των δακτυλίων είναι ένας από τους συνδετικούς κρίκους ανάμεσα στην Άλγεβρα και τη Γεωμετρία. Πράγματι, έγινε αρκετά νωρίς σαφές από την σκοπιά της Αλγεβρικής Γεωμετρίας ότι πολλές γεωμετρικές ιδιότητες ενός γεωμετρικού αντικειμένου αντανακλώνται στην άλγεβρα των συναρτήσεων που ορίζονται πάνω από το γεωμετρικό αντικείμενο. Ανάλογα αποτελέσματα υπήρξαν και στην ανάλυση, όπως το θεώρημα των Gelfand-Naimark. Η ιδέα αυτή γενικεύτηκε και χρησιμοποιήθηκε κατόπιν ως εργαλείο επίλυσης προβλημάτων και της Θεωρίας αριθμών από τον A. Grothendieck.

Σχήμα 2.2. A. Grothendieck 1970, Το παρόν έργο αποτελεί κοινό κτήμα (public domain). Πηγή: Wikimedia Commons

Ας προσπαθήσουμε να εξηγήσουμε μερικές από τις ιδέες αυτές σε όσο γίνεται περισσότερο απλή γλώσσα:

Ο δακτύλιος των πολυωνύμων μίας μεταβλητής πάνω από το σώμα των μιγαδικών συναρτήσεων $R := \mathbb{C}[x]$ είναι μια φυσιολογική κλάση συναρτήσεων πάνω στο μιγαδικό επίπεδο. Σε κάθε σημείο a του επιπέδου μπορούμε να θεωρήσουμε ένα μέγιστο ιδεώδες του R, το m_a το οποίο ορίζεται ως

$$m_a = \{f \in R : f(a) = 0\}$$

(Άσκηση: Δείξτε ότι όντως είναι ένα μέγιστο ιδεώδες) Το ιδεώδες αυτό είναι κύριο και παράγεται από το $(x-a)$. Επιπλέον είναι σαφές ότι η τιμή του πολυωνύμου f στο σημείο a δεν είναι τίποτε άλλο από την κλάση υπολοίπων της $f \bmod m_a$ στον δακτύλιο R/m_a.

Πράγματι, αν κάνουμε τη διαίρεση της f με το $x-a$ το υπόλοιπο θα είναι μια σταθερά:

$$f(x) = (x-a)g(x) + \nu(x),\ \deg\nu(x) < \deg(x-1) = 1.$$

Το υπόλοιπο είναι σαφώς ένας αντιπρόσωπος της κλάσης $f \bmod m_a$ και επιπλέον είναι ίσο με $f(a)$ όπως εύκολα παρατηρούμε τοποθετώντας το a στην παραπάνω εξίσωση της διαίρεσης.

Παρατηρούμε ότι έχουμε μία 1-1 και επί αντιστοιχία

$$\{\text{Μέγιστα Ιδεώδη του} R\} \longrightarrow \{\text{σημεία του} \mathbb{C}\}$$

Σε παρόμοια συμπεράσματα θα καταλήγαμε αν για R θεωρούσαμε τον δακτύλιο των ολόμορφων ή απειροδιαφορισίμων συναρτήσεων. Αυτό που θα άλλαζε θα ήταν το θεώρημα της διαίρεσης το οποίο θα έπρεπε να αναπτύξουμε και να αποδείξουμε.

Θα μπορούσαμε να αλλάξουμε το σώμα σε ένα διαφορετικό όπως το $\mathbb{Q}$ ή ένα πεπερασμένο σώμα $\mathbb{F}_p$ ακολουθώντας την προτροπή του A. Weil (να κάνουμε γεωμετρία πάνω από οποιοδήποτε σώμα). Σε αυτή την περίπτωση θα οδηγούμασταν στο να εξετάζουμε τα σημεία του γεωμετρικού αντικειμένου πάνω από το σώμα.

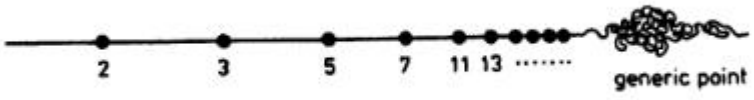
Σχήμα 2.3. A. Weil (μαζί με την αδελφή του Simone σε εκδρομή στο Βέλγιο). Το παρόν έργο αποτελεί κοινό κτήμα (public domain) λόγω παρέλευσης 70 ετών από τον θάνατο του δημιουργού. Πηγή: Apprenticeship of a Mathematician, Courtesy of Sylvie Weil.

Τι θα συμβεί όμως αν αντί για τον δακτύλιο $\mathbb{C}[x]$ θεωρούσαμε έναν άλλο δακτύλιο με αριθμητική σημασία όπως το $\mathbb{Z}$ ή το $\mathbb{Z}[x]$; Θα υπήρχε ένα γεωμετρικό αντικείμενο του οποίο το $\mathbb{Z}$ να ήταν ο φυσιολογικός δακτύλιος συναρτήσεων; Σύμφωνα με τις ιδέες του Grothendick το αντικείμενο αυτό είναι το σύνολο των πρώτων ιδεωδών του δακτυλίου το οποίο θα το συμβολίζουμε με $\mathrm{Spec}(R)$. Για παράδειγμα, όταν $R = \mathbb{Z}$ το σύνολο των πρώτων ιδεωδών δεν είναι άλλο από τους πρώτους αριθμούς, ενώ όταν $R = \mathbb{Z}[x]$ το σύνολο των πρώτων ιδεωδών αποτελείται από τα κύρια ιδεώδη $p\mathbb{Z}[x]$ όπου p πρώτος, τα κύρια ιδεώδη $f\mathbb{Z}[x]$, όπου f ανάγωγο πολυώνυμο αλλά και από τα ιδεώδη $\langle p, f\rangle$ που παράγονται από έναν πρώτο αριθμό p και ένα ανάγωγο πολυώνυμο. Μάλιστα στην περίπτωση που το πολυώνυμο

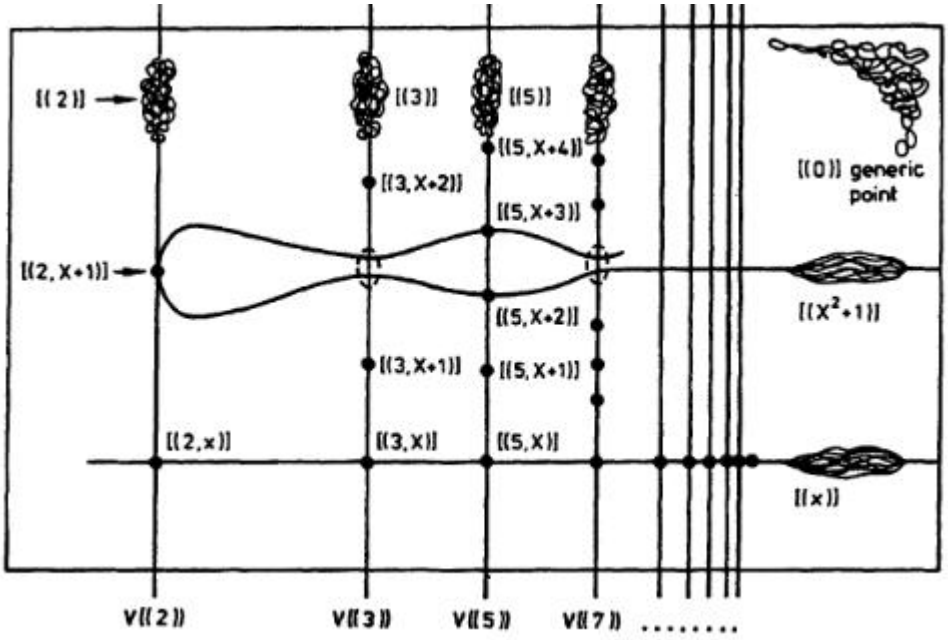
f παραμένει ανάγωγο mod p το ιδεώδες $\langle p, f\rangle$ είναι μέγιστο αφού

$$\frac{\mathbb{Z}[x]}{\langle p, f\rangle} \cong \frac{\mathbb{F}_p[x]}{f(x)\mathbb{F}_p}$$

το οποίο είναι σώμα. Η πρώτη γραφική παράσταση αυτών των ιδεών εμφανίστηκε πιθανότατα στο σκίτσο του D. Mumford στο κόκκινο βιβλίο των πολλαπλοτήτων και σχημάτων (Mumford 1999), τη δεκαετία του 70.



Σχήμα 2.4. Πρώτα ιδεώδη των ακέραιων



Σχήμα 2.5. Πρώτα ιδεώδη των πολυωνύμων με συντελεστές ακέραιους

Το πρόβλημα κατά πόσο ένα ανάγωγο πολυώνυμο του $\mathbb{Z}[x]$ παραμένει ανάγωγο αν το θεωρήσουμε modulo p και πώς αναλύεται αν δεν είναι ανάγωγο είναι ένα πρόβλημα θεμελιώδους σημασίας για τη Θεωρία Αριθμών που έχει τις αρχές του στον τετραγωνικό νόμο αντιστροφής του Gauss.

Ας δούμε τώρα πώς ένα στοιχείο του δακτυλίου μπορεί να θεωρηθεί ως συνάρτηση πάνω στο σύνολο των πρώτων ιδεωδών:

$$P \mapsto f(P) = f \bmod P \in R/P.$$

Αν ο δακτύλιος $R = \mathbb{F}[x]$ είναι ένας δακτύλιος πολυωνύμων πάνω από ένα σώμα, τότε η τιμή της συνάρτησης ανήκει πάντα στο σώμα $\mathbb{F} = R/P$ το οποίο είναι κοινό για όλα τα πρώτα ιδεώδη του R.

Στην περίπτωση που $R = \mathbb{Z}$ υπάρχει μια διαφορά. Τα στοιχεία του δακτυλίου δίνουν τιμές σε διαφορετικά σώματα. Έτσι το $3 \in \mathbb{Z}$ στο (σημείο)-πρώτο ιδεώδες $7\mathbb{Z}$ δίνει την τιμή $3 \bmod 7$ η οποία

ανήκει στο σώμα με 7 στοιχεία ενώ στο (σημείο)-πρώτο ιδεώδες $5\mathbb{Z}$ δίνει την τιμή 3 αλλά στο σώμα με 5 στοιχεία.

Οι ιδέες αυτές έδωσαν τεράστια ώθηση στα Μαθηματικά και στην Θεωρία Αριθμών αφού πρόσθεσαν μια γεωμετρική ενόραση των αριθμητικών εννοιών και επέτρεψαν να ορίσουμε πλήρως γεωμετρικά αντικείμενα όπως ο εφαπτόμενος χώρος, η παραγώγιση κλπ.

Βιβλιογραφία

Fraleigh, J.B. 2011. *Εισαγωγή Στην Άλγεβρα*. Πανεπιστημιακές Εκδόσεις Κρήτης.

Mumford, D. 1999. *The Red Book of Varieties and Schemes: Includes the Michigan Lectures (1974) on Curves and Their Jacobians*. Lecture Notes in Mathematics. Springer. https://books.google.gr/books?id=K1hFauNsmR4C.

Βάρσος, Δ., Δ. Δεριζιώτης, Ι. Εμμανουήλ, Μ. Μαλιάκας, και Ο. Ταλέλλη. 2012. *Μια Εισαγωγή Στην Άλγεβρα*. Σοφία Α. Ε.

3

Νόμος τετραγωνικής Αντιστροφής

3.1. Εισαγωγικά στοιχεία για λύσεις τετραγωνικών εξισώσεων

Είδαμε προηγουμένως ότι μας ενδιαφέρει πότε ένα ανάγωγο πολυώνυμο $f \in \mathbb{Z}[x]$ παραμένει ανάγωγο modulo p. Ένα ενδιαφέρον πρόβλημα είναι να χαρακτηρίσουμε τους πρώτους για τους οποίους αλλάζει συμπεριφορά η αναγωγισιμότητα modulo p. Για τετραγωνικά πολυώνυμα αυτό είναι ισοδύναμο με το αν η διακρίνουσα είναι τετράγωνο ή όχι. Ενώ λοιπόν για πραγματικά πολυώνυμα με συντελεστές πραγματικούς αυτό είναι σαφές (τετράγωνα δεν είναι οι αρνητικοί αριθμοί) σε ένα σώμα όπως το $\mathbb{Z}/p\mathbb{Z}$ τα πράγματα είναι περισσότερο πολύπλοκα. Το εργαλείο που χαρακτηρίζει για ποιους πρώτους ο ακέραιος $a \in \mathbb{Z}$ είναι τετράγωνο ή όχι ονομάζεται νόμος της τετραγωνικής αντιστροφής. Περισσότερα στοιχεία σχετικά με τον νόμο αντιστροφής και τις γενικεύσεις του ο αναγνώστης μπορεί να αναζητήσει στα (Λάκκης 1990), (Αντωνιάδης and Κοντογεώργης 2015) και στο (Lemmermeyer 2000).

Υποθέτουμε ότι θέλουμε να λύσουμε την τετραγωνική ισοδυναμία

$$ax^2 + bx + c \equiv 0 \mathrm{mod} m,$$

με $a, b, c \in \mathbb{Z}$, $m \in \mathbb{N}$, $m > 1$. Η λύση εξαρτάται από τη λύση ισοδυναμιών της μορφής

$$ax^2 + bx + c \equiv 0 \mathrm{mod} p^s,$$

όπου p πρώτος οι οποίες ανάγονται σε ισοδυναμίες της μορφής

$$ax^2 + bx + c \equiv 0 \mathrm{mod} p.$$

Για μικρές τιμές του p ισοδυναμίες της παραπάνω μορφής μπορούν να λυθούν με τη μέθοδο της δοκιμής και της επιτυχίας. Για μεγάλο p χρειάζεται μια νέα ιδέα. Υποθέτουμε ότι p είναι περιττός πρώτος και $(a, p) = 1$. Εργαζόμαστε λοιπόν στο σώμα $\mathbb{Z}/p\mathbb{Z}$ και επιλύουμε την τετραγωνική εξίσωση με τον ίδιο τρόπο όπως θα κάνουμε στο σώμα των πραγματικών ή μιγαδικών αριθμών. Πράγματι, αφού $(2, p) = 1$ οι λύσεις της

$$ax^2 + bx + c \equiv 0 \mathrm{mod} p$$

είναι ισοδύναμες προς τις λύσεις της ισοδυναμίας

$$4a^2x^2 + 4abx + 4ac \equiv \mathrm{mod} p$$

δηλαδή της

$$(2ax + b)^2 \equiv (b^2 - 4ac) \mathrm{mod} p$$

Η τελευταία ισοδυναμία μπορεί να λυθεί τότε και μόνο τότε όταν μπορούμε να βρούμε κάποιον ακέραιο x_0 ο οποίος να είναι λύση της ισοδυναμίας

$$2ax + b \equiv y_0 \mathrm{mod} p$$

και y_0 μια λύση της ισοδυναμίας της

$$y^2 \equiv (b^2 - 4ac) \mathrm{mod} p$$

Αφού $(2a, p) = 1$ η πρώτη ισοδυναμία έχει πάντα λύση. Το αρχικό πρόβλημα λοιπόν ανάγεται στη λύση ισοδυναμιών της μορφής

$$y^2 \equiv a \mathrm{mod} p$$

Αν $a \equiv 0 \mathrm{mod} p$, τότε η προηγούμενη ισοδυναμία έχει λύση. Θα εξετάσουμε την περίπτωση p δεν διαιρεί το a.

Σε ότι ακολουθεί, ο αριθμός p θα είναι ένας περιττός πρώτος.

3.2. Τετραγωνικά υπόλοιπα

3.2.1 Ορισμός:
Έστω p ένας πρώτος αριθμός. Ένας ακέραιος a που δεν είναι πολλαπλάσιο του p, είναι τετραγωνικό υπόλοιπο του p αν ο a είναι τετράγωνο κάποιου αριθμού mod$p$. Αν ο a δεν είναι τετράγωνο κάποιου αριθμού mod$p$ τότε λέγεται τετραγωνικό μη-υπόλοιπο mod$p$.

Με άλλα λόγια ο a είναι τετραγωνικό υπόλοιπο αν η εξίσωση

$$x^2 \equiv a \mathrm{mod} p$$

έχει λύση.

Θα μπορούσαμε (όταν ο πρώτος p είναι μικρός) να υπολογίσουμε όλα τα τετράγωνα και στη συνέχεια να δούμε αν το a είναι τετραγωνικό υπόλοιπο ή όχι.

Έτσι για $p = 5$ υπολογίζουμε ότι

x	0	1	2	3	4
x^2	0	1	4	4	4

Αν το a είναι ή όχι τετραγωνικό υπόλοιπο εξαρτάται από την κλάση του $a \mathrm{mod} p$.

Ορίζουμε την απεικόνιση:

$$\psi : (\mathbb{Z}/p\mathbb{Z})^* \to \{\pm 1\}$$
$$\psi : a \mapsto \left(\frac{a}{p}\right)$$

Η ποσότητα $\left(\frac{a}{p}\right)$ ονομάζεται *σύμβολο του Legendre* και είναι ίση με 1 αν το a είναι τετραγωνικό υπόλοιπο και -1 αν το a δεν είναι τετραγωνικό υπόλοιπο $\mathrm{mod} p$. Για χάρη συντομίας του συμβολισμού ορίζουμε και

$$\left(\frac{a}{p}\right) = 0$$

στην περίπτωση που $a \equiv 0 \mathrm{mod} p$. Η τελευταία γενίκευση είναι γνωστή στη βιβλιογραφία ως το *σύμβολο του Kronecker*.

Η παραπάνω απεικόνιση είναι ομομορφισμός ομάδων, το οποίο ισοδυναμεί με το ότι ισχύει:

$$\left(\frac{a\beta}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{\beta}{p}\right).$$

Πράγματι θα δείξουμε στη συνέχεια ότι η $(\mathbb{Z}/p\mathbb{Z})^* = \mathbb{F}^*$ είναι μία κυκλική ομάδα, άρα υπάρχει g ώστε η $(\mathbb{Z}/p\mathbb{Z})$ να είναι της μορφής:

$$\left\{g, g^2, \ldots, g^{(p-1)/2}, g^{(p+1)/2}, \ldots, g^{p-1} = 1\right\}$$

Αφού ο $p-1$ είναι άρτιος, τα τετράγωνα των στοιχείων του $(\mathbb{Z}/p\mathbb{Z})^*$ είναι τα

$$g^2, g^4, \ldots, g^{(p-1)/2\cdot 2} = 1, g^{p+1} = g^2, \ldots, g^{2(2(p-1))},$$

το οποίο σημαίνει ότι τα τέλεια τετράγωνα του $(\mathbb{Z}/p\mathbb{Z})^*$ είναι τα g^i με i : άρτιος και τα μη τέλεια τετράγωνα είναι τα g^i με i: περιττός. Αυτό σημαίνει ότι η ψ είναι ομομορφισμός καθώς: το άθροισμα δύο περιττών είναι άρτιος, το άθροισμα δύο άρτιων είναι άρτιος και το άθροισμα ενός περιττού με έναν άρτιο είναι περιττό.

Παρατηρούμε ότι ο πυρήνας της ψ είναι τα $g \in (\mathbb{Z}/p\mathbb{Z})^*$ για τα οποία ισχύει ότι $\psi(a) = 1$, δηλάδη τα τετραγωνικά υπόλοιπα του p.

Ένα βασικό εργαλείο στον υπολογισμό του συμβόλου του Legendre είναι ο *τετραγωνικός νόμος αντιστροφής* ο οποίος έχει την παρακάτω μορφή:

3.2.2 Θεώρημα:
Έστω p, q δύο περιττοί, πρώτοι αριθμοί. Τότε ισχύει

$$\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\left(\frac{q}{p}\right)$$

Επίσης,

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} \text{ και } \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

Θα δώσουμε σε λίγο μια απόδειξη του παραπάνω θεωρήματος.

3.2.3 Πρόταση:
Ισχύει ότι

$$\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} mod\, p,$$

δηλαδή

$$\left(\frac{a}{p}\right) = 1 \iff a^{\frac{p-1}{2}} \equiv 1 mod\, p$$

Απόδειξη Ισχύει ότι $\left(\frac{a}{p}\right) = \pm 1$ και $a^{p-1} \equiv 1 \mathrm{mod} p$, οπότε $a^{\frac{p-1}{2}} \equiv \pm 1 \mathrm{mod} p$. Η απεικόνιση

$$\phi : (\mathbb{Z}/p\mathbb{Z})^* \to (\mathbb{Z}/p\mathbb{Z})^*$$

με

$$\phi(a) = a^{\frac{p-1}{2}}$$

είναι ένας ομομορφισμός ομάδων.

Με βάση το σύμβολο του Legendre ορίσαμε την απεικόνιση $\psi(a) = \left(\frac{a}{p}\right)$. Αν $a \in \ker\psi$, τότε $a = b^2$ για κάποιο $b \in (\mathbb{Z}/p\mathbb{Z})^*$ οπότε

$$\phi(a) = a^{(p-1)/2} = (b^2)^{(p-1)/2} = b^{p-1} = 1.$$

Κατά συνέπεια είναι $\ker\psi \subseteq \ker\phi$. Θα δείξουμε ότι $\ker\psi = \ker\phi$. Ο $\ker\psi$ έχει δείκτη 2 στο $\mathbb{Z}/p\mathbb{Z}^*$. Εφόσον ο πυρήνας ενός ομομορφισμού είναι ομάδα από μόνος του και η τάξη μιας υποομάδας διαιρεί την τάξη της ομάδας, θα ισχύει είτε ότι $\ker\phi = \ker\psi$ ή $\phi = 1$. Αν $\phi = 1$ το πολυώνυμο $x^{(p-1)/2} - 1$ έχει $p-1$ ρίζες στο σώμα $\mathbb{Z}/p\mathbb{Z}$ το οποίο είναι άτοπο. Κατά συνέπεια ισχύει ότι $\ker\phi = \ker\psi$.

3.3. Αθροίσματα Gauss

3.3.1. m-ρίζες της μονάδας. Υπενθυμίζουμε ότι όλες οι m-ρίζες της μονάδας είναι της μορφής

$$\zeta_m = \cos(2\pi k/m) + i\sin(2\pi ik/m) = \exp(2\pi ik/m),$$

όπου $i^2 = -1$ και $0 \leqslant k \leqslant m-1$, $k, m \in \mathbb{N}$.

Οι m ρίζες της μονάδας είναι δυνάμεις μίας *πρωταρχικής* ρίζας η οποία είναι της μορφής

$$\zeta_m = \cos(2\pi k/m) + i\sin(2\pi ik/m),$$

με $(k, m) = 1$.

Ας υποθέσουμε ότι $m = p$ πρώτος αριθμός. Τότε η εξίσωση ορισμού της p-ρίζας της μονάδας διασπάται ως

$$x^p - 1 = (x-1)(x^{p-1} + x^{p-1} + \cdots + x + 1)$$

και δείξαμε χρησιμοποιώντας το κριτήριο του Eisenstein ότι το πολυώνυμο

$$(x^{p-1} + x^{p-1} + \cdots + x + 1)$$

είναι ένα ανάγωγο πολυώνυμο του $\mathbb{Q}[x]$.

Οι n-ρίζες της μονάδας ανήκουν στο λεγόμενο κυκλοτομικό σώμα αριθμών το οποίο ορίζεται ως το σώμα

$$\mathbb{Q}[\zeta_n] = \mathbb{Q}[x]/\Phi_n(x)$$

όπου $\Phi_n(x)$ είναι ένα ελάχιστο ανάγωγο πολυώνυμο του $\mathbb{Q}[x]$ που μηδενίζεται σε μία n-στή ρίζα της μονάδας. Ένα τέτοιο πολυώνυμο ορίζεται γενικότερα ως εξής: Θεωρούμε έναν αριθμό $a \in \mathbb{C}$ και τον ομορφισμό δακτυλίων

$$\phi : \mathbb{Q}[x] \to \mathbb{C}$$
$$f \mapsto f(a)$$

Ο πυρήνας είναι ένα ιδεώδες του δακτυλίου $\mathbb{Q}[x]$ και επειδή τα ιδεώδη του $\mathbb{Q}[x]$ είναι όλα κύρια, είναι της μορφής $\ker(\phi) = \Phi_n(x)\mathbb{Q}[x]$. Η εύρεση του ανάγωγου πολυωνύμου είναι ένα ενδιαφέρον πρόβλημα. Στην περίπτωση $n = p$, όπου p είναι ένας πρώτος αριθμός, το κυκλοτομικό πολυώνυμο είναι το

$$\Phi_p(x) = 1 + x + \cdots + x^{p-1}$$

που υπολογίσαμε παραπάνω. Θα επανέλθουμε αργότερα στον υπολογισμό του κυκλοτομικού πολυωνύμου για γενικό n.

Ας παρατηρήσουμε ακόμα ότι το θεώρημα ισομορφισμών δακτυλίων εξασφαλίζει ότι

$$\mathbb{Q}[x]/p_n(x)\mathbb{Q}[x] \cong \mathrm{Im}(\phi) = \mathbb{Q}(\zeta).$$

Συγκεκριμένα τώρα στο sage δίνουμε:

```
sage:L.<zeta>=CyclotomicField(7);L
Cyclotomic Field of order 7 and degree 6
sage:zeta^7
1
sage:1/zeta
-zeta^5 - zeta^4 - zeta^3 - zeta^2 - zeta - 1
sage:(zeta^4+5*zeta+1).complex_embedding()
3.21648014139125 + 3.47527367322259*I
```

Παρατηρούμε ότι οι πράξεις με το κυκλοτομικό σώμα αριθμών γίνονται ακριβώς στο πρόγραμμα sage. Μπορούμε να υπολογίσουμε σε κάθε βήμα δεκαδικές προσεγγίσεις των στοιχείων του κυκλοτομικού σώματος, αλλά αυτό δεν έχει κανένα πλεονέκτημα. Στην πραγματικότητα οι πράξεις κινητής υποδιαστολής μειονεκτούν, αφού σε αυτές εμφανίζονται σφάλματα προσέγγισης.

3.3.1 Πρόταση:
Για κάθε $a \in \mathbb{Z}$ *ισχύει ότι*

$$\sum_{\nu=0}^{p-1} \zeta_p^{a\cdot\nu} = \begin{cases} p & \text{αν } a \equiv 0 mod p \\ 0 & \text{διαφορετικά} \end{cases}.$$

Επιπλέον αν x, y *είναι τυχαίοι ακέραιοι*

$$\sum_{\nu=0}^{p-1} \zeta_p^{(x-y)\nu} = \begin{cases} p & \text{αν } x \equiv y mod p \\ 0 & \text{διαφορετικά} \end{cases}.$$

Απόδειξη Αν $p \mid a$ τότε $\zeta_p^a = 1$ και στο άθροισμα μετέχουν p το πλήθος προσθεταίοι ίσοι με 1. Σε διαφορετική περίπτωση χρησιμοποιούμε τον τύπο άθροισης γεωμετρικής προόδου.

Η δεύτερη ισότητα είναι άμεση συνέπεια της πρώτης.

3.3.2 Ορισμός:
Σταθεροποιούμε έναν πρώτο $p \neq 2$. *Το άθροισμα Gauss που αντιστοιχεί στον* $a \in \mathbb{Z}$ *ορίζεται ως*

$$G_a = \sum_{n=1}^{p-1} \left(\frac{n}{p}\right) \zeta^{a\cdot n}.$$

3.3.3 Πρόταση:
Ισχύει ότι

$$G_0 = \sum_{n=0}^{p-1} \left(\frac{n}{p}\right) = 0.$$

Απόδειξη Έχουμε αποδείξει ότι η συνάρτηση $\phi(n) = \left(\frac{n}{p}\right)$ είναι μη-τετριμμένος ομομορφισμός ομάδων $\mathbb{Z}_p^* \to \{\pm 1\}$. Συνεπώς ο πυρήνας είναι μια υποομάδα δείκτη 2 στην $\mathbb{Z}_p^*$ που έχει $p-1$ το πλήθος στοιχεία. Με άλλα λόγια τα μισά στοιχεία είναι τετραγωνικά υπόλοιπα και τα άλλα μισά δεν είναι. Το ζητούμενο αποτέλεσμα είναι σαφές.

3.3.4 Πρόταση:
Ισχύει ότι

$$G_a = \left(\frac{a}{p}\right) G_1.$$

Απόδειξη Στην περίπτωση $a = 0$ το αποτέλεσμα είναι σαφές αφού και τα δύο μέλη της προς απόδειξη εξίσωσης είναι μηδενικά.

Αν $a \neq 0$ τότε έχουμε

$$\left(\frac{a}{p}\right) G_a = \left(\frac{a}{p}\right) \sum_{n=0}^{p-1} \left(\frac{n}{p}\right) \zeta_p^{a\cdot n}$$
$$= \sum_{n=0}^{p-1} \left(\frac{an}{p}\right) \zeta_p^{a\cdot n} = G_1$$

Το τελικό αποτέλεσμα προκύπτει πολλαπλασιάζοντας την παραπάνω εξίσωση με $\left(\frac{a}{p}\right)$.

3.3.5 Θεώρημα:
Για κάθε a ακέραιο, $(a,p) = 1$ ισχύει

$$G_a^2 = (-1)^{(p-1)/2} p.$$

□

Απόδειξη Υπολογίζουμε ότι

$$G_a G_{-a} = \left(\frac{a}{p}\right) G_1 \left(\frac{-a}{p}\right) G_1$$
$$= \left(\frac{-1}{p}\right) \left(\frac{a}{p}\right)^2 G_1^2$$
$$= (-1)^{(p-1)/2} G_1^2.$$

Υπολογίζουμε τώρα ότι

$$\sum_{a=0}^{p-1} G_a G_{-a} = (p-1)(-1)^{(p-1)/2} G_1^2.$$

Από την άλλη υπολογίζουμε

$$G_a G_{-a} = \sum_{n=0}^{p-1} \zeta^{an} \left(\frac{n}{p}\right) \sum_{m=0}^{p-1} \left(\frac{m}{p}\right) \zeta^{-am}.$$

$$= \sum_{n=0}^{p-1} \sum_{m=0}^{p-1} \left(\frac{n}{p}\right) \left(\frac{m}{p}\right) \zeta^{a(n-m)}.$$

Υπολογίζουμε και πάλι το άθροισμα

$$\sum_{a=0}^{p-1} G_a G_{-a} = \sum_{n=0}^{p-1} \sum_{m=0}^{p-1} \sum_{a=0}^{p-1} \zeta^{a(n-m)}.$$

Το τελευταίο άθροισμα (ως προς a) μηδενίζεται, όταν n, m είναι ανισοϋπόλοιπα mod p ενώ όταν $n \equiv m \bmod p$ δίνει τιμή p.

Άρα καταλήγουμε στο

$$\sum_{a=0}^{p-1} G_a G_{-a} = \sum_{n=0}^{p-1} \left(\frac{n}{p}\right)^2 p = p(p-1).$$

Τελικά εξισώνοντας τους δύο διαφορετικούς τρόπους υπολογισμού του $\sum_{a=0}^{p-1} G_a G_{-a}$ καταλήγουμε στο

$$G_1^2 = (-1)^{(p-1)/2} p$$

και τέλος

$$G_a^2 = \left(\frac{n}{p}\right)^2 G_1^2 = G_1^2 = (-1)^{(p-1)/2} p.$$

□

Ας ελέγξουμε την αλήθεια των παραπάνω με τη βοήθεια του sage

```
sage:
p=7
L.<zeta>=CyclotomicField(p)
g5=sum(legendre_symbol(n,p)*zeta^(5*n) for n in range(1,p))
gn5=sum(legendre_symbol(n,p)*zeta^(-5*n) for n in range(1,p))
g1=sum(legendre_symbol(n,p)*zeta^(1*n) for n in range(1,p))
g5*gn5==(-1)^((p-1)/2)*g1^2
True
```

Interactive

3.4. Απόδειξη του νόμου τετραγωνικής αντιστροφής

Έστω q ένας περιττός πρώτος και $p \neq q$. Θέτουμε $p^* = (-1)^{(p-1)/2} p$ και έχουμε ότι $G_1^2 = p^*$. Έχουμε αποδείξει ότι

$$(p^*)^{(q-1)/2} \equiv \left(\frac{p^*}{q}\right) \bmod q.$$

Από την άλλη

$$G_1^{q-1} = (G_1^2)^{(q-1)/2} = (p^*)^{(q-1)/2}$$

και πολλαπασιάζοντας με G_1 καταλήγουμε στην εξίσωση

$$G_1^q \equiv G_1 \left(\frac{p^*}{q}\right) \mathrm{mod} q\mathbb{Z}[\zeta]$$

Ο δακτύλιος $\mathbb{Z}[\zeta]/q\mathbb{Z}[\zeta]$ είναι χαρακτηριστικής q, και συνεπώς ισχύει ότι

$$(x+y)^q \equiv x^q + y^q \mathrm{mod} q.$$

Υπολογίζουμε τώρα την

$$G_1^q = \left(\sum_{n=0}^{p-1} \left(\frac{n}{p}\right) \zeta^n\right)^q$$

$$= \sum_{n=0}^{p-1} \left(\frac{n}{p}\right)^q \zeta^{nq} = G_q \mathrm{mod} q.$$

Καταλήγουμε συνεπώς στην

$$G_q = \left(\frac{q}{p}\right) G_1 \equiv \left(\frac{p^*}{q}\right) G_1 \mathrm{mod} p.$$

Πολλαπλασιάζοντας με G_1 και αφού $G_1^2 = p^*$ και $p \neq q$ καταλήγουμε στο

$$\left(\frac{p^*}{q}\right) \equiv \left(\frac{p^*}{q}\right) \mathrm{mod} q.$$

Όμως και τα δύο μέλη της παραπάνω ισότητας είναι ± 1 και αφού $q \neq 2$ καταλήγουμε στην

$$\left(\frac{q}{p}\right) = \left(\frac{p^*}{q}\right)$$

Τέλος, το Θεώρημα του Euler δίνει ότι

$$\left(\frac{p^*}{q}\right) = \left(\frac{-1}{q}\right)^{(p-1)/2} \left(\frac{p}{q}\right) = (-1)^{\frac{(p-1)(q-1)}{2}} \left(\frac{p}{q}\right)$$

και ο νόμος της τετραγωνικής αντιστροφής έχει αποδειχτεί.

3.4.1. Υπολογισμός του συμβόλου Legendre για το $p = 2$. Για τη μελέτη της περίπτωσης αυτής θα χρησιμοποιήσουμε μια γεωμετρική μέθοδο. Θα θεωρήσουμε το σύνολο των λύσεων της εξίσωσης

$$x^2 + y^2 \equiv 1 \mathrm{mod} p$$

Δηλαδή τα σημεία $(x, y) \in \mathbb{F}_p$ τα οποία ικανοποιούν την παραπάνω εξίσωση.

Μία προφανής λύση είναι το σημείο με συντεταγμένες $(-1, 0) \in \mathbb{F}_p$. Το σύνολο των ευθειών που περνούν από αυτό το σημείο είναι το

$$y = t(x+1)$$

όπου το t διατρέχει τα σημεία του $\mathbb{F}_p$. Καθεμία από τις ευθείες αυτές έχει δύο κοινά σημεία με τον παραπάνω κύκλο $\mathrm{mod} p$. Το ένα είναι το $(-1, 0)$ το άλλο το υπολογίζουμε λύνοντας το σύστημα:

$$C(\mathbb{F}_p) : t^2(x+1)^2 = x^2 = 1 \Rightarrow (x+1)(t^2(x+1) + x - 1) = 0$$

από όπου λογαριάζουμε

$$x = \frac{1-t^2}{1+t^2}, y = \frac{2t}{1+t^2}.$$

Παρατηρούμε ότι κάθε λύση της παραπάνω εξίσωσης οδηγεί σε ένα t και κάθε t σε μία λύση. Όμως δεν μπορούμε να επιτρέψουμε στο $1 + t^2$ να γίνει 0.

Ξεχωρίζουμε λοιπόν δύο περιπτώσεις: Η εξίσωση $1+t^2$ έχει λύση $\mathrm{mod} p$. Αυτό μπορεί να συμβεί μόνο στην περίπτωση που το -1 είναι τετραγωνικό υπόλοιπο $\bmod p$. Όμως έχουμε υπολογίσει ότι

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}.$$

Για να είναι το -1 τετραγωνικό υπόλοιπο πρέπει και αρκεί το $p-1 \equiv 0 \mathrm{mod} p$ ή ισοδύναμα $p \equiv 1 \mathrm{mod} 4$. Σε αυτή την περίπτωση κάθε σημείο $t \in \mathbb{F}_p$ που δεν είναι τετραγωνική ρίζα του -1 δίνει δύο σημεία της $C(\mathbb{F}_p)$. Συνολικά λοιπόν έχουμε $p-2$ σημεία τομής ευθείων. Αυτά μαζί με το αρχικό σημείο $(-1,0)$ δίνουν ένα σύνολο από $p-1$ σημεία.

Η δεύτερη περίπτωση είναι το -1 να μην είναι τετραγωνικό υπόλοιπο $\mathrm{mod} p$. Όμοια με την προηγούμενη περίπτωση βλέπουμε ότι αυτό μπορεί να συμβεί ακριβώς στην περίπτωση $p \equiv 3 \mathrm{mod} 4$. Τώρα και οι p τιμές του t δίνουν σημεία πάνω στην καμπύλη. Σε αυτά προσθέτουμε και το αρχικό σημείο για να πάρουμε ότι το $C(\mathbb{F}_p)$ έχει $p+1$ σημεία.

Θεωρούμε το σύνολο S των ζευγαριών $(a,b) \in (\mathbb{Z}/p\mathbb{Z})^* \times (\mathbb{Z}/p\mathbb{Z})^*$ τα οποία ικανοποιούν την $a+b=1$ και $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right) = 1$.

Το σύνολο S σχετίζεται με το $C(\mathbb{F}_p)$. Πράγματι, αν θέσουμε $a = x^2$ και $b = y^2$ βλέπουμε ότι κάθε σημείο $(x,y) \in C(\mathbb{F}_p)$ διαφορετικό από τα $(\pm 1, 0)$ και $(0, \pm 1)$ απεικονίζεται σε ένα σημείο του S και μάλιστα η συνάρτηση αυτή είναι 4 προς 1. Δηλαδή

$$\#S = (C(\mathbb{F}_p) - 4)/4,$$

συνεπώς

$$\#S = \begin{cases} (p+1-4)/4 & \text{αν } p \equiv 3 \mathrm{mod} 4 \\ (p-1-4)/4 & \text{αν } p \equiv 1 \mathrm{mod} 4 \end{cases}$$

Από τα παραπάνω προκύπτει ότι $\#S$ είναι περιττός αν $p \equiv \pm 1 \mathrm{mod} 8$.

Η συνάρτηση $\sigma(a,b) = (b,a)$ είναι μια ενέλιξη του συνόλου S, δηλαδή μια συνάρτηση 1-1 επί $\sigma : S \to S$ με την επιπλέον ιδιότητα ότι $\sigma^2 = 1$. Η σ έχει ακριβώς ένα σταθερό σημείο αν και μόνο αν υπάρχει $a \in \mathbb{Z}/p\mathbb{Z}$ ώστε $2a = 1$ και $\left(\frac{a}{p}\right) = 1$. Επιπλέον η $2a = 1$ έχει λύση στο $\mathbb{Z}/p\mathbb{Z}$ με $\left(\frac{a}{p}\right) = 1$ αν και μόνο αν $\left(\frac{2}{p}\right) = 1$. Μία ενέλιξη όμως έχει ένα σταθερό σημείο αν και μόνο αν $\#S$ είναι περιττός. Συνεπώς έχουμε καταλήξει στον τύπο:

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{2}}.$$

Παρατήρηση Ο τετραγωνικός νόμος αντιστροφής μάς επιτρέπει να υπολογίζουμε το σύμβολο του Legendre με τον παρακάτω τρόπο. Καταρχήν ο υπολογισμός του σύμβολου $\left(\frac{a}{p}\right)$ ανάγεται στον υπολογισμό του συμβόλου $\left(\frac{\nu}{p}\right)$, όπου ν είναι το υπόλοιπο της διαίρεσης του a με p. Συνεπώς μπορούμε να υποθέσουμε ότι το $a < p$. Στη συνέχεια παραγοντοποιούμε το a σε γινόμενο πρώτων παραγόντων

$$a = p_1 \cdots p_s$$

και κάθε σύμβολο της μορφής $\left(\frac{p_i}{p}\right)$ το αντιστρέφουμε σύμφωνα με τον κανόνα

$$\left(\frac{p_i}{p}\right) = (-1)^{\frac{(p-1)(p_i-1)}{8}} \left(\frac{p}{p_i}\right).$$

Στη συνέχεια, αντί του συμβόλου $\left(\frac{p}{p_i}\right)$, μπορούμε να υπολογίσουμε το $\left(\frac{u_i}{p_i}\right)$, όπου u_i είναι το υπόλοιπο της διαίρεσης του p με το p_i και να συνεχίσουμε τη διαδικασία μέχρι τέλους. Τα σύμβολα της μορφής $\left(\frac{2}{p_i}\right)$ αν εμφανιστούν τέτοια τα υπολογίζουμε εύκολα αφού είναι ίσα με $(-1)^{\frac{p_i^2-1}{8}}$.

Μπορούμε να κάνουμε την παραπάνω διαδικασία αποτελεσματικότερη εισαγάγοντας το σύμβολο του Jacobi, το οποίο γενικεύει το σύμβολο του Legendre και κάνει τη διαδικασία συντομότερη αφού αποφεύγουμε το στάδιο της παραγοντοποίησης. Η τεχνική αυτή αν και δεν είναι ιδιαίτερα δύσκολη να περιγραφεί δεν θα μας απασχολήσει εδώ.

Παράδειγμα Να εξετασθεί αν η ισοτιμία

$$x^2 \equiv -154 \mathrm{mod} 163$$

έχει λύση.

Ο 163 είναι πρώτος αριθμός ενώ το -154 αναλύεται σε γινόμενο πρώτων παραγόντων $-154 = (-1)\cdot 2\cdot 7\cdot 11$. Επομένως

$$\left(\frac{-154}{163}\right) = \left(\frac{-1}{163}\right)\left(\frac{2}{163}\right)\left(\frac{7}{163}\right)\left(\frac{11}{163}\right)$$

Τώρα

$$\left(\frac{-1}{163}\right) = (-1)^{\frac{163-1}{2}} = (-1)^{81} = -1.$$

Επειδή $163 \equiv 3 \mathrm{mod} 8$ έχουμε $\left(\frac{2}{163}\right) = -1$. Επίσης αφού $7 \equiv 1 \mathrm{mod} 4$

$$\left(\frac{7}{163}\right) = -\left(\frac{163}{7}\right) = -\left(\frac{2}{7}\right) = (-1)(+1) = -1.$$

Αφού $11 \equiv 3 \mathrm{mod} 4$

$$\left(\frac{11}{163}\right) = -\left(\frac{163}{11}\right) = -\left(\frac{9}{11}\right) = -\left(\frac{3}{11}\right)^2 = -1.$$

Τελικά έχουμε

$$\left(\frac{-154}{163}\right) = (-1)(-1)(-1)(-1) = +1$$

και συνεπώς η ισοτιμία έχει λύση.

Στο πρόγραμμα sage ο παραπάνω υπολογισμός γίνεται ως εξής: (το σύμβολο Kronecker είναι η γενίκευση του συμβόλου του Legendre που δίνει τιμή 0 όταν ο αριθμητής είναι διαιρετός με p.)

```
1 sage:kronecker(-154,163)
2 1
```

Παράδειγμα Για ποιούς περιττούς πρώτους αριθμούς p η ισοτιμία

$$x^2 \equiv 5 \mathrm{mod} p$$

έχει λύση;

Η ισοτιμία έχει λύση ακριβώς τότε όταν $\left(\frac{5}{p}\right) = 1$. Τώρα $\left(\frac{5}{p}\right) = 1$ αν και μόνο αν $\left(\frac{p}{5}\right) = 1$. Αν $p \equiv 1, 4 \mathrm{mod} 5$, τότε $\left(\frac{p}{5}\right) = 1$. Αν $p \equiv 2, 3 \mathrm{mod} 5$, τότε $\left(\frac{p}{5}\right) = -1$. Συνεπώς έχει λύση ακριβώς τότε όταν

$$p \equiv \pm 1 \mathrm{mod} 5.$$

Μπορούμε να βρούμε με το sage όλα τα τετραγωνικά υπόλοιπα και όλα τα τετραγωνικά μη υπόλοιπα ως εξής:

```
sage:R=[x for x in range(63) if kronecker(x,63)==1];R
[1, 2, 4, 8, 11, 16, 22, 23, 25, 29, 32, 37, 43, 44, 46,
 50, 53, 58]
sage:NR=[x for x in range(63) if kronecker(x,63)==-1];NR
[5, 10, 13, 17, 19, 20, 26, 31, 34, 38, 40, 41, 47, 52, 55,
59, 61, 62]
```

Interactive

Βιβλιογραφία

Lemmermeyer, F. 2000. *Reciprocity Laws: From Euler to Eisenstein*. Monographs in Mathematics. Springer. https://books.google.gr/books?id=EwjpPeK6GpEC.

Αντωνιάδης, Ι., και Α. Κοντογεώργης. 2015. *Θεωρία Αριθμών Και Εφαρμογές*. Εκδόσεις Κάλλιπος.

Λάκκης, Κ. 1990. *Θεωρία Αριθμών*. Εκδόσεις Ζήτη.

4 Πεπερασμένα Σώματα

4.1. Επεκτάσεις σωμάτων

Θα ξεκινήσουμε εισάγοντας τον αναγνώστη σε μια σειρά από απαραίτητες αλγεβρικές έννοιες. Περισσότερες πληροφορίες μπορεί να αντληθούν από γενικά βιβλία Άλγεβρας (Βάρσος et al. 2012), (Fraleigh 2011) αλλά και από βιβλία Θεωρίας Galois (Stewart 2003).

4.1.1 Ορισμός:
Ας υποθέσουμε ότι $K \subset L$ *είναι ένας εγκλεισμός σωμάτων. Το* L *θα λέγεται επέκταση του σώματος* K.

Παρατήρηση Αν το L είναι επέκταση του K από τις ιδιότητες των πράξεων του σώματος μπορούμε να αποδείξουμε ότι το L είναι ένας διανυσματικός χώρος υπέρ του σώματος K με τις πράξεις

$$L \times L \to L$$

$$(x, y) \mapsto x + y$$

και

$$K \times L \to L$$

$$(\lambda, x) \mapsto \lambda x.$$

Θα ονομάζουμε βαθμό (και θα το συμβολίζουμε με $[L : K]$) της επέκτασης L/K τη διάσταση $\dim_K L$.

Παράδειγμα Το σώμα των μιγαδικών αριθμών $\mathbb{C}$ είναι διδιάστατος $\mathbb{R}$-διανυσματικός χώρος και συνεπώς $[\mathbb{C} : \mathbb{R}] = 2$.

Ας θεωρήσουμε μία επέκταση L/K, ένα στοιχείο $a \in L$ και τον ομομορφισμό εκτίμησης

$$\phi_a : K[x] \to L$$

$$f \mapsto \phi_a(f) := f(a).$$

Αν ο πυρήνας της ϕ_a είναι διαφορετικός του μηδενικού ιδεώδους, τότε το a λέγεται *αλγεβρικό*. Στην περίπτωση αυτή αφού ο δακτύλιος $K[x]$ είναι περιοχή κυρίων ιδεωδών ο πυρήνας θα είναι ένα ιδεώδες της μορφής

$$\ker(\phi_a) = g(x)K[x],$$

για κάποιο κατάλληλο πολυώνυμο $g \neq 0$, το οποίο θα το ονομάζουμε το *ελάχιστο πολυώνυμο* του a.

Διαφορετικά, αν δηλαδή ο πυρήνας της ϕ_a είναι το μηδενικό ιδεώδες, το στοιχείο a θα ονομάζεται *υπερβατικό*.

Παρατήρηση Το ότι το ιδεώδες των πολυωνύμων που μηδενίζονται στο a είναι κύριο και παράγεται από το ελάχιστο πολυώνυμο g, έχει τη συνέπεια ότι κάθε πολυώνυμο που μηδενίζεται στο a να είναι διαιρετό με g. Η συμπεριφορά αυτή είναι παρόμοια με τη γνώριμη ιδιότητα του ελαχίστου πολυωνύμου μιας γραμμικής απεικόνισης από τη γραμμική άλγεβρα.

Παραδείγματα Σε μία επέκταση σωμάτων για παράδειγμα $\mathbb{C}/\mathbb{Q}$ μπορεί να υπάρχουν και αλγεβρικά και υπερβατικά στοιχεία. Για παράδειγμα το $\sqrt{2}$ είναι αλγεβρικό αφού ο πυρήνας της συνάρτησης $\phi_{\sqrt{2}}$ είναι το ιδεώδες του δακτυλίου $\mathbb{Q}[x]$ που περιέχει κάθε πολυώνυμο που είναι διαιρετό με το $x^2 - 2$. Τα στοιχεία π, e είναι γνωστό ότι είναι υπερβατικά, αν και μία απόδειξη υπερβαίνει τους στόχους του βιβλίου αυτού.

4.1.2 Ορισμός:
Θα λέμε μία επέκταση L/K *αλγεβρική αν κάθε στοιχείο* $a \in L$ *είναι αλγεβρικό υπέρ του* K. *Θα λέμε μια επέκταση* L/K *πεπερασμένη αν* $[L : K] < \infty$.

Είναι σαφές ότι κάθε πεπερασμένη επέκταση είναι αλγεβρική. Πράγματι αν $x \in L$ θεωρούμε το σύνολο των δυνάμεων $\{1, x, x^2, \ldots, x^n\}$ όπου $n = [L : K]$. Αυτά είναι $n + 1$ στοιχεία σε έναν χώρο διάστασης n, άρα είναι γραμμικά εξαρτημένα. Άρα υπάρχουν στοιχεία $a_i \in K$ ώστε

$$a_0 + a_1 x + \cdots a_n x^n = 0,$$

δηλαδή το x μηδενίζει ένα πολυώνυμο με συντελεστές από το K και είναι αλγεβρικό.

Από την άλλη υπάρχουν αλγεβρικές επεκτάσεις που δεν είναι πεπερασμένες όπως θα δούμε στη συνέχεια.

4.1.3 Πρόταση:
Αν M/L *και* L/K *δύο πεπερασμένες επεκτάσεις, τότε και η* M/K *είναι πεπερασμένη και μάλιστα ισχύει:*

$$[M : K] = [M : L] \cdot [L : K].$$

Απόδειξη Πρόκειται για ένα γνωστό θεώρημα της γραμμικής άλγεβρας της συμπεριφοράς της διάστασης σε επέκταση των βαθμωτών. Η απόδειξη βασίζεται στην επιλογή μιας βάσης $\{v_1, \ldots, v_{[M:L]}\}$ του M πάνω από το L και στην επιλογή μιας βάσης $\{w_1, \ldots, w_{[L:K]}\}$ του L πάνω από το K.Τα $[M : L] \cdot [L : K]$ το πλήθος στοιχεία $v_i w_j$ αποτελούν μία βάση του M πάνω από το K.

4.1.4 Ορισμός:
Για ένα σώμα K *η αλγεβρική κλειστότητα* $\overline{K}$ *του* K *ορίζεται να είναι μια αλγεβρική επέκταση του* K *ώστε κάθε πολυώνυμο* $f \in K[x]$ *να έχει όλες τις ρίζες του στο* K.

Παρατηρήσεις Η ύπαρξη της αλγεβρικής κλειστότητας ενός τυχαίου σώματος απαιτεί το λήμμα του Zorn και παραλείπεται. Επίσης μπορεί κανείς να αποδείξει ότι η αλγεβρική κλειστότητα του K είναι μοναδική μέχρι ισομορφισμού που σταθεροποιεί κάθε στοιχείο του K.

Στην περίπτωση του σώματος $\mathbb{Q}$ μπορούμε να θεωρήσουμε το σώμα

$$\overline{\mathbb{Q}} := \cap_{L \in I} L$$

όπου η τομή λαμβάνεται πάνω στο σύνολο των επεκτάσεων L/K που είναι αλγεβρικά κλειστές και περιέχουν το $\mathbb{Q}$. Το σύνολο I είναι μη κενό αφού περιλαμβάνει το αλγεβρικά κλειστό σώμα $\mathbb{C}$.

Η επέκταση $\overline{\mathbb{Q}}/\mathbb{Q}$ είναι ένα από τα δυσκολότερα και περισσότερο ενδιαφέροντα θέματα στη μελέτη της Θεωρίας Αριθμών αλλά και των Μαθηματικών γενικότερα.

Στη συνέχεια του μαθήματος θα μελετήσουμε συστηματικά την επέκταση $\overline{\mathbb{F}}_p/\mathbb{F}_p$.

4.1.5 Πρόταση:
Θεωρούμε ένα ανάγωγο πολυώνυμο $f(x) \in \mathbb{F}[x]$. *Το σώμα* $K := \mathbb{F}[x]/f\mathbb{F}[x]$ *είναι ένας διανυσματικός χώρος υπέρ του σώματος* $\mathbb{F}$ *και*

$$[K : \mathbb{F}] := dim_{\mathbb{F}} K = deg f.$$

Απόδειξη Παρατηρούμε ότι χώρος πηλίκο είναι σε ένα προς ένα αντιστοιχία με τα δυνατά υπόλοιπα της διαίρεσης με $f(x)$ τα οποία είναι όλα τα πολυώνυμα βαθμού γνήσια μικρότερου του d.

Ο τελευταίος χώρος έχει ως βάση τα στοιχεία $\{1, x, \ldots, x^{d-1}\}$ και συνεπώς $\dim_{\mathbb{F}} K = \deg f$.

4.1.6 Θεώρημα:
Θεωρούμε ένα πολυώνυμο $f(x) \in \mathbb{F}[x]$. *Τότε υπάρχει μια επέκταση* K *του* $\mathbb{F}$, *ώστε το* f *να έχει όλες τις ρίζες του στο* K.

Απόδειξη Με επαγωγή στον βαθμό. Αν $\deg(f) = 1$ τότε $K = \mathbb{F}$. Υποθέτουμε ότι για πολυώνυμα βαθμού $< n$ και για όλα τα σώματα η πρόταση είναι αληθής. Θεωρούμε ένα πολυώνυμο βαθμού n και επιλέγουμε έναν ανάγωγο παράγοντα h του f. Υπάρχει σώμα $K_1 = \mathbb{F}[x]/\langle h \rangle$ στο οποίο το h και άρα και το f έχει μια ρίζα. Δηλαδή

$$f(x) = (x - \rho)g(x).$$

Το αποτέλεσμα προκύπτει από την επαγωγική υπόθεση για το g.

4.2. Στοιχεία θεωρίας Galois

Ας υποθέσουμε ότι έχουμε μία επέκταση L/K σωμάτων. Θεωρούμε το σύνολο των αυτομορφισμών

$$Gal(L/K) = \{\sigma : L \to L, \sigma|_K = Id_k\},$$

δηλαδή των ισομομορφισμών σωμάτων $L \to L$ οι οποίοι όταν περιοριστούν στο σώμα K το κρατούν σταθερό. Το σύνολο $Gal(L/K)$ απότελεί ομάδα με πράξη τη σύνθεση.

Παράδειγμα Η ομάδα Galois της επέκτασης $\mathbb{C}/\mathbb{R}$ είναι ισόμορφη με την $\mathbb{Z}/2\mathbb{Z}$ και περιέχει δύο στοιχεία -τον ταυτοτικό ισομορφισμό και τη μιγαδική συζυγία-. Πράγματι, προκειμένου να περιγράψουμε έναν ισομορφισμό $\sigma : \mathbb{C} \to \mathbb{C}$ που αφήνει το σώμα $\mathbb{R}$ σταθερό, αρκεί να περιγράψουμε πόσο κάνει το $\sigma(i)$ αφού

$$\sigma(x + iy) = x + \sigma(i)y,$$

για $x, y \in \mathbb{R}$. Όμως, $i^2 = -1$ συνεπώς εφαρμόζοντας τον σ έχουμε ότι $\sigma(i)^2 = -1$, δηλαδή το $\sigma(i)$ δεν μπορεί να είναι τίποτε άλλο από μια τετραγωνική ρίζα του -1. Άρα $\sigma(i) = \pm i$, στη μία περίπτωση ο σ είναι η ταυτότητα, ενώ στην άλλη ο σ είναι η μιγαδική συζυγία.

4.2.1 Πρόταση:
Αν ο $a \in L$ *είναι ένα αλγεβρικό στοιχείο και ικανοποιεί μια αλγεβρική σχέση* $f(a) = 0$, *όπου το* $f(x) \in K[x]$, *τότε κάθε στοιχείο της Gal*(L/K) *στέλνει το* a *σε μία άλλη ρίζα του* $f(x)$.

ΑπόδειξηΤο θεώρημα αυτό είναι σαφές αφού αν

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n$$

τότε η σχέση

$$\sigma(f(a)) = \sigma(0) = 0$$

δίνει ότι

$$a_0 + a_1\sigma(a) + \cdots + a_n\sigma(a)^n = 0$$

δηλαδή το $\sigma(a)$ είναι επίσης ρίζα του $f(x)$.

Παρατήρηση Το παραπάνω είναι γενίκευση του γνωστού θεωρήματος: οι ρίζες πολυωνύμων με πραγματικούς συντελεστές εμφανίζονται σε ζευγάρια συζυγών μιγαδικών αριθμών.

Ερώτημα Ας υποθέσουμε ότι έχουμε ένα ανάγωγο πολυώνυμο f στο $K[x]$, και έστω $a_1, \ldots, a_n$ οι ρίζες του f. Είναι σωστό ότι κάθε μετάθεση των $a_1, \ldots, a_n$ επεκτείνεται σε ένα ισομορφισμό σωμάτων μιας κατάληλης επέκτασης του L;

Πριν απαντήσουμε ας δούμε μία περίπτωση που αυτό δεν ισχύει. Για p πρώτο, το πολυώνυμο

$$1 + x + \cdots + x^{p-1}$$

είναι ένα ανάγωγο πολυώνυμο του $\mathbb{Q}[x]$. Οι ρίζες του είναι όλες οι p-ρίζες της μονάδας και όλες είναι δύναμη μίας τέτοιας, δηλαδή υπάρχει μία ζ_p ώστε κάθε άλλη p-ρίζα του 1 να είναι της μορφής ζ_p^i για κάποιο $1 \leqslant i \leqslant p-1$.

Σε αυτή την περίπτωση, αν $\sigma(\zeta) = \zeta^{i_0}$ (δεν θα μπορούσε να είναι τίποτε άλλο παρά μία άλλη p-ρίζα του 1) τότε αφού ο σ είναι ένας ισομορφισμός σωμάτων θα πρέπει να έχουμε ότι

$$\sigma(\zeta_p^k) = \zeta_p^{ki_0}.$$

Αυτό σημαίνει ότι αν "προσδιορίσουμε" την εικόνα μίας p-ρίζας του 1 έχουμε προσδιορίσει τις εικόνες όλων των άλλων ριζών. Συνεπώς δεν εμφανίζονται όλες οι δυνατές μεταθέσεις μεταξύ των ριζών.

Με άλλα λόγια τα στοιχεία της ομάδας Galois είναι συγκεκριμένες μεταθέσεις που πρέπει να σέβονται κάθε αλγεβρική σχέση μεταξύ των ριζών. Η ιδέα για τη σχέση αυτή μεταξύ μεταθέσεων και αλγεβρικών σχέσεων μεταξύ των ριζών ήταν το εφαλτήριο του E. Galois για την ανάπτυξη της ομώνυμης θεωρίας. Στην περίπτωση που οι ρίζες είναι αρκετά ανεξάρτητες εμφανίζεται ολόκληρη η S_n ως ομάδα Galois.

Πρόβλημα Δίνεται μία πεπερασμένη ομάδα G. Υπάρχει μια επέκταση $L/\mathbb{Q}$ η οποία να έχει ως ομάδα Galois την ομάδα G;

Αυτό είναι ένα διάσημο βαθύ άλυτο πρόβλημα γνωστό και ως αντίστροφο πρόβλημα της Θεωρίας του Galois.

Για την επίλυσή του έχουν χρησιμοποιηθεί πλήθος εργαλεία από σχεδόν κάθε περιοχή των μαθηματικών. Ο J.P. Serre φέρεται να έχει πει ότι το αντιστρόφο πρόβλημα της θεωρίας του Galois μας δίνει τη δικαιολογία να μελετήσουμε πολλά και διαφορετικά μαθηματικά.

Σχήμα 4.1. Evariste Galois 1811-1832, Το παρόν έργο αποτελεί κοινό κτήμα (public domain). Πηγή: Wikimedia Commons

Ας υποθέσουμε ότι έχουμε έναν αλγεβρικό αριθμό $\alpha \in L$ σε μία επέκταση του $L/\mathbb{Q}$. Μπορούμε να θεωρήσουμε τον αριθμό α modulo p? Δεν έχει νόημα! Μπορούμε όμως να υπολογίζουμε ένα πολυώνυμο με συντελεστές στο $\mathbb{Z}$ που να έχει το α ως ρίζα και να θεωρήσουμε το πολυώνυμο αυτό modulo p. Πώς θα το υπολογίσουμε αυτό το πολύωνυμο;

Ας δούμε μερικά παραδείγματα:

1. Να βρεθεί ένα πολυώνυμο με ρητούς συντελεστές που να έχει το $a+ib$ ως ρίζα, όπου $a, b \in \mathbb{Q}$. Ένα τέτοιο πολυώνυμο είναι το
$$(x-(a+ib))(x-(a-ib)) = x^2 - 2ax + (a+ib)(a-ib)$$
$$= x^2 - 2ax + (a^2+b^2).$$
Προφανώς αυτό το πολυώνυμο είναι το ελάχιστο πολυώνυμο του $\mathbb{Q}[x]$ που έχει το $a+ib$ ως ρίζα, αφού αν έχει το $a+ib$ θα πρέπει να έχει και τη συζυγή ρίζα. Επιπλέον αν το $b \neq 0$ το παραπάνω πολυώνυμο είναι ανάγωγο. Παρατηρήστε ότι οι συντελεστές του πολυωνύμου δίνονται ως συμμετρικές εκφράσεις των ριζών:
$$(x-\rho_1)(x-\rho_2) = x^2 - (\rho_1+\rho_2)x + \rho_1\rho_2.$$
Επιπλέον μπορούμε να δούμε ότι στην περίπτωση που $\rho_1 = \rho$, $\rho_2 = \overline{\rho}$, το άθροισμα $\rho + \overline{\rho}$ και το γινόμενο των ριζων $\rho\overline{\rho}$ είναι αναλλοίωτα στοιχεία κάτω από τη μιγαδική συζυγία.
2. Να βρεθεί ένα πολυώνυμο στο $\mathbb{Q}[x]$ το οποίο να έχει ρίζα το $a+b\sqrt{2}$. Θα δουλέψουμε με τον ίδιο τρόπο με το πολυώνυμο
$$(x-(a+b\sqrt{2}))(x-(a-b\sqrt{2})) = x^2 - 2ax + (a^2-2b^2).$$

Και πάλι αν το $a+b\sqrt{2}$ είναι ρίζα και το $a-b\sqrt{2}$ θα πρέπει να είναι ρίζα. Το παραπάνω πολυώνυμο είναι ανάγωγο, αρκεί το $b \neq 0$.

Σχήμα 4.2. J.P. Serre, Δημιουργός: R. Schmid, Το παρόν έργο αποτελεί κοινό κτήμα (public domain). Πηγή: Wikimedia Commons

3. Ας δούμε τώρα κάτι δυσκολότερο: Μπορούμε να βρούμε ένα πολυώνυμο που να έχει ρίζα το $\sqrt{2}+\sqrt{3}$; Υπολογίζουμε ότι

$$(x-\sqrt{2}-\sqrt{3})(x+\sqrt{2}-\sqrt{3})(x-\sqrt{2}+\sqrt{3})(x+\sqrt{2}+\sqrt{3}) =$$
$$= x^4 - 10x + 1$$

Ο παραπάνω υπολογισμός γίνεται στο sage ως εξής:

```
sage:R.<x,y> = PolynomialRing(QQ,2);R
Multivariate Polynomial Ring in x, y over Rational Field
sage:S.<sq2,sq3> = QuotientRing(R,R.ideal(x^2-2,y^2-3));S
Quotient of Multivariate Polynomial Ring in x, y over
Rational Field by the ideal (x^2 - 2, y^2 - 3)
sage:RR.<X> = PolynomialRing(S);RR
(X-sq2-sq3)*(X-sq2+sq3)*(X+sq2-sq3)*(X+sq2+sq3)
X^4 - 10*X^2 + 1
```

Interactive

Ορίζουμε τον δακτύλιο R ως έναν δακτύλιο δύο μεταβλητών με συντελεστές από τους ρητούς. Στη συνέχεια ορίζουμε έναν νέο δακτύλιο S, στις μεταβλητές sq2,sq3 στον οποίο επιβάλλουμε (μέσω της κατασκευής ενός δακτυλίου πηλίκου) να είναι οι τετραγωνικές ρίζες του $2, 3$ αντίστοιχα. Κατασκευάζουμε τέλος τον δακτύλιο πολυωνύμων $S[X]$ μέσα στον οποίο εκτελούμε τη ζητούμενη πράξη!

4.3. Πεπερασμένα Σώματα

Η βιβλιογραφία για τα πεπερασμένα σώματα είναι εκτενής. Πέρα από βιβλία γενικής άλγεβρας μπορούμε να προτείνουμε τα (Lidl and Niederreiter 1997) και (Mullen and Panario 2013).

4.3.1 Θεώρημα:
Κάθε πεπερασμένο $\mathbb{F}$ σώμα έχει p^h το πλήθος στοιχεία όπου h είναι η διάσταση του $\mathbb{F}$ ως διανυσματικού χώρου υπέρ του $\mathbb{F}_p$.

Απόδειξη Θεωρούμε το $\mathbb{F}$ ώς διανυσματικό χώρο υπέρ του σώματος $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$. Αναγκαστικά η διάσταση είναι πεπερασμένη. Θεωρούμε μία βάση $\{e_1, \ldots, e_h\}$ του $\mathbb{F}$. Κάθε στοιχείο του $\mathbb{F}$ γράφεται στη μορφή:

$$\lambda_1 e_1 + \cdots \lambda_h e_h,$$

όπου τα λ_i διατρέχουν το $\mathbb{Z}/p\mathbb{Z}$. Προφανώς το $\mathbb{F}$ έχει p^h στοιχεία, όσες και οι επιλογές των $\lambda_i \in \mathbb{F}_p$.

Αντιστρόφως, αν δοθεί μια δύναμη πρώτου p^h υπάρχει σώμα με p^h το πλήθος στοιχεία; Αν το $h = 1$ είναι σαφές ότι υπάρχει ένα τέτοιο σώμα το $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Μάλιστα κάθε άλλο σώμα με p το πλήθος στοιχεία είναι ισόμορφο με το $\mathbb{F}_p$, αφού θα πρέπει να περιέχει ένα σώμα ισόμορφο με το $\mathbb{F}_p$ και αφού έχουν το ίδιο πλήθος στοιχείων είναι ισόμορφα.

Θα χρειαστούμε την παρακάτω

4.3.2 Πρόταση:
Σε κάθε δακτύλιο R χαρακτηριστικής p για κάθε $x, y \in R$ ισχύει:

$$(x+y)^{p^h} = x^{p^h} + y^{p^h}.$$

Απόδειξη Θα το αποδείξουμε πρώτα για $h = 1$. Ισχύει ότι

$$(x+y)^p = \sum_{\nu=0}^{p} \binom{p}{\nu} x^\nu y^{p-\nu}.$$

Ισχύει $\binom{p}{0} = \binom{p}{p} = 1$.

Οι συντελεστές $\binom{p}{\nu}$ $1 \leqslant \nu \leqslant p-1$ είναι όλοι διαιρετοί με p. Πράγματι,

$$\binom{p}{\nu} = p\frac{(p-1)!}{i!(p-i)!} \in \mathbb{Z}$$

Κανείς παράγοντας του παρονομαστή (που είναι όλοι γνήσια μικρότεροι του p) δεν διαιρεί το p. Άρα διαιρουν το $(p-1)!$ Συνεπώς $\frac{(p-1)!}{i!(p-i)!} \in \mathbb{Z}$ και

$$\binom{p}{\nu} \equiv 0 \mathrm{mod} p \quad 1 \leqslant \nu \leqslant p-1.$$

Αυτό αποδεικνύει ότι

$$(x+y)^p = x^p + y^p.$$

Η γενική περίπτωση προκύπτει με επαγωγή: Αν ισχύει

$$(x+y)^{p^{h-1}} = x^{p^{h-1}} + y^{p^{h-1}},$$

τότε υψώνουμε στην p και χρησιμοποιούμε την περίπτωση $h = 1$ για να δείξουμε ότι

$$(x+y)^{p^h} = x^{p^h} + y^{p^h}.$$

Χρειαζόμαστε ένα κριτήριο που θα εξασφαλίζει ότι ένα πολυώνυμο έχει απλές ρίζες. Πρώτα θα χρειαστεί να αναπτύξουμε μια έννοια παραγώγου σε έναν οποιονδήποτε δακτύλιο. Ο ορισμός μας δεν θα περιλαμβάνει καθόλου την έννοια του ορίου.

4.3.3 Ορισμός:
Για κάθε σώμα $\mathbb{F}$ υπάρχει μια συνάρτηση $D : \mathbb{F}[x] \to \mathbb{F}[x]$, η οποία ικανοποιεί

1. $D(f+g) = D(f) + D(g)$ *για κάθε* $f, g \in \mathbb{F}[x]$.
2. $D(fg) = fD(g) + D(f)g$
3. $D(x) = 1, D(c) = 0$ *για κάθε* $c \in \mathbb{F}$.

Απόδειξη Παρατηρούμε ότι η 3η ιδιότητα σε συνδυασμό με τη δεύτερη επιβάλλει $D(cf) = cD(f)$ για κάθε $c \in \mathbb{F}$, δηλαδή η D είναι γραμμική.

Λόγω γραμμικότητας αρκεί να ορίσουμε τη συνάρτησή μας πάνω στα στοιχεία x^ν, $\nu \in \mathbb{N}$. Επιπλέον, αφού $D(x) = 1$ έχουμε ότι

$$D(x^n) = D(x)x^{n-1} + xD(x^{n-1}).$$

Η παραπάνω σχέση επιβάλει να ορίσουμε $D(x^n) = nx^{n-1}$, όπως μπορούμε να δείξουμε με επαγωγή.

4.3.4 Πρόταση:
Αν $p(x) \in \mathbb{F}[x]$ πολυώνυμο βαθμού m με συντελεστές από ένα σώμα $\mathbb{F}$ τότε η εξίσωση $p(x) = 0$ έχει το πολύ m διακεκριμένες ρίζες στο $\mathbb{F}$.

Απόδειξη Θα εφαρμόσουμε τη μέθοδο της επαγωγής ως προς τον βαθμό του πολυωνύμου $p(x)$. Αν $m = 1$ τότε το $p(x) = ax + b$, $a \neq 0$ και η $p(x)$ έχει ακριβώς μία λύση στο $\mathbb{F}$ την $x = -b/a$.

Αν $m \geqslant 2$ και η $p(x) = 0$ δεν έχει καμία λύση τελειώσαμε. Αν η εξίσωση $p(x) = 0$ έχει μία λύση a τότε

$$p(x) = (x-a)g(x)$$

όπου $g(x) \in \mathbb{F}[x]$. Αν έχουμε μια άλλη ρίζα b η οποία είναι διαφορετική από την a τότε επειδή

$$p(b) = (b-a)g(b) = 0$$

και $b - a \neq 0$ έχουμε ότι $g(b) = 0$, δηλαδή το b είναι ρίζα του $g(x)$ το οποίο όμως έχει βαθμό $m-1$, οπότε για αυτό μπορούμε να χρησιμοποιήσουμε την επαγωγική υπόθεση.

Εφαρμογή Ισχύει ότι

$$(p-1)! \equiv -1 \mathrm{mod} p$$

για κάθε πρώτο αριθμό p. Η παραπάνω ισότητα είναι γνωστή στη βιβλιογραφία ως θεώρημα του Wilson. Αν το $p = 2$, τότε η παραπάνω ισότητα ισχύει. Αν p περιττός πρώτος παρατηρούμε ότι η εξίσωση $x^p - x$ έχει ως ρίζα κάθε στοιχείο του $\mathbb{F}_p$, οπότε το ζητούμενο προκύπτει με σύγκριση του σταθερού όρου των πολυωνύμων

$$x(x-1)(x-2)\cdots(x-(p-1)) = x^p - x.$$

Παράδειγμα Στον δακτύλιο $R[x]$, όταν το R δεν είναι σώμα, μπορεί ένα πολυώνυμο να έχει περισσότερες λύσεις από τον βαθμό του. Για παράδειγμα η εξίσωση δευτέρου βαθμού

$$x^2 - 1 = 0$$

στον $\mathbb{Z}/8\mathbb{Z}$ έχει 4-λύσεις, τις $x = 1, 3, 5, 7$. Αυτό δεν έρχεται σε αντίθεση με την παραπάνω πρόταση αφού το $\mathbb{Z}/8\mathbb{Z}$ δεν είναι σώμα.

4.3.5 Θεώρημα:
Το πολυώνυμο $f \in \mathbb{F}[x]$ έχει πολλαπλή ρίζα στο $\rho \in \mathbb{F}$, δηλαδή είναι διαιρετό με $(x-\rho)^i$ για $i \geqslant 2$ αν και μόνο αν $f(\rho) = D(f)(\rho) = 0$.

Απόδειξη Ας υποθέσουμε ότι $f(x) = (x-\rho)^i g(x)$ και $(x-\rho)$ δεν διαιρεί το $g(x)$. Παραγωγίζουμε και έχουμε:

$$Df(x) = (x-\rho)^i D(g(x)) + i(x-\rho)^{i-1} g(x).$$

Το συμπέρασμα είναι άμεσο.

Το παραπάνω αποτέλεσμα μας εξασφαλίζει ότι το πολυώνυμο $x^p - x$ έχει απλές ρίζες, αφού $D(x^p - x) = -1$. Επιπλέον το $x^p - x$ έχει ως ρίζα κάθε στοιχείο του $\mathbb{F}_p$, όπως μπορούμε να δείξουμε με επαγωγή. Πράγματι $1^p = 1$, υποθέτουμε ότι $n^p = n$ και υπολογίζουμε ότι $(n+1)^p = n^p + 1^p = n+1$.

Ας θεωρήσουμε το πολυώνυμο $g_{p,h} := x^{p^h} - x$. Με βάση το κριτήριο της παραγώγου όλες οι ρίζες του είναι διαφορετικές. Επιπλέον μπορούμε να αποδείξουμε ότι οι ρίζες έχουν τη δομή σώματος. Πράγματι, έστω ένα αρκετά μεγάλο σώμα το οποίο να περιέχει όλες τις ρίζες του $g_{p,h}$. Η ιδιότητα

$$(a+b)^{p^h} = a^{p^h} + b^{p^h}$$

επιβάλλει ότι το άθροισμα και η διαφορά ριζών του $g_{p,h}$ είναι ρίζα του $g_{p,h}$. Επίσης το γινόμενο ριζών είναι ρίζα και οι ρίζες του $g_{p,h}$ αποτελούν ένα σώμα.

Θα δείξουμε τώρα ότι κάθε πεπερασμένο σώμα με p^h στοιχεία ταυτίζεται με το σώμα ριζών του $g_{p,h}$. Πράγματι, έστω ένα σώμα με p^h στοιχεία. Αναγράφουμε τα στοιχεία του σώματος

$$\{a_1, \ldots, a_{p^h}\}$$

με $a_1 = 0$, $a_2 = 1$. Έστω ένα μη μηδενικό στοιχείο a. Πολλαπλασιάζουμε όλα τα στοιχεία του σώματος με a και έχουμε τα

$$\{aa_1, \ldots, aa_{p^h}\}.$$

Ο πολλαπλασιασμός με a διατηρεί τα μη μηδενικά στοιχεία και συνεπώς

$$\prod_{i=2}^{p^h} a_i = \prod_{i=2}^{p^h} aa_i,$$

άρα το τυχαίο μη μηδενικό στοιχείο ικανοποιεί την εξίσωση

$$a^{p^h-1} = 1$$

με άλλα λόγια είναι ρίζα του πολυωνύμου $g_{p,h}$. Προφανώς και το 0 είναι ρίζα του $g_{p,h}$.

Στο πρόγραμμα sage μπορούμε να κατασκευάσουμε πεπερασμένα σώματα ως εξής:

```
sage:k = GF(9, 'a');k
Finite Field in a of size 3^2
sage:for i,x in enumerate(k):  print i,x
0 0
1 a
2 a + 1
3 2*a + 1
4 2
5 2*a
6 2*a + 2
7 a + 2
8 1
```

Interactive

4.3.6 Θεώρημα:
Η πολλαπλασιαστική ομάδα ενός πεπερασμένου σώματος είναι μια κυκλική ομάδα.

Απόδειξη 1η Γνωρίζουμε ότι η πολλαπλασιαστική ομάδα G του σώματος είναι αβελιανή με τάξη p^n-1. Από το θεώρημα ταξινόμησης των πεπερασμένων αβελιανών ομάδων αυτή θα είναι της μορφής:

$$G = \mathbb{Z}/n_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/n_r\mathbb{Z},$$

για φυσικούς αριθμούς $n_1, \ldots, n_r$ των οποίων το γινόμενο είναι $p^n - 1$. Θεωρούμε το ελάχιστο κοινό πολλαπλάσιο τους m. Είναι σαφές ότι $m \leqslant n_1 \cdots n_r$. Ένα τυχαίο στοιχείο $x \in G$ θα είναι της μορφής $x = (x_1, \ldots, x_n)$ όπου $x_\nu \in \mathbb{Z}/n_\nu\mathbb{Z}$. Άρα $x^m = 1$. Όμως η εξίσωση $x^m - 1$ σε ένα σώμα έχει το πολύ m ρίζες άρα $m = p^n - 1 = |G|$. Αυτό σημαίνει ότι $(n_i, n_j) = 1$ και συνεπώς η ομάδα G είναι κυκλική.

4.3.7 Ορισμός:
Κάθε γεννήτορας της κυκλικής ομάδας $(\mathbb{F}_{p^h})^*$ θα λέγεται πρωταρχικό στοιχείο.

Παράδειγμα Στο σώμα με 7 στοιχεία έχουμε $\mathbb{F}_7^* = \{1, 2, 3, 4, 5, 6\}$. Παρατηρούμε ότι οι δυνάμεις του 2 είναι οι $\{2, 2^2 = 4, 2^3 = 8 = 1\}$, άρα το 2 έχει τάξη 3 και δεν μπορεί να παράγει ολόκληρη την

πολλαπλασιαστική ομάδα. Θεωρούμε τώρα τις δυνάμεις του 3. $3^2 = 9 = 2$, άρα το 3 έχει τάξη 6 και παράγει όλη την ομάδα.

Θα χρειαστούμε μερικά στοιχεία από τη θεωρία των κυκλικών ομάδων.

4.3.8 Πρόταση:
Σε μία κυκλική ομάδα με γεννήτορα T *και τάξη* m, *το στοιχείο* T^i *έχει τάξη* $m/(m,i)$.

Απόδειξη Πράγματι αν s είναι η τάξη του T^i, τότε $T^{is} = 1$ και έτσι $m \mid is$. Συνεπώς $m/(i,m) \mid s$. Από την άλλη $(T^i)^{m/(i,m)} = (T^m)^{i/(i/m)} = 1$. Άρα $s \mid m/(i,m)$, συνεπώς $s = m/(i,m)$.

4.3.9 Πρόταση:
Θεωρούμε μια κυκλική ομάδα $G = \langle T \rangle$ *με τάξη* m. *Για κάθε διαιρέτη* $\delta \mid m$ *το πλήθος των στοιχείων με τάξη* δ *είναι* $\phi(\delta)$.

Απόδειξη Σύμφωνα με την παραπάνω πρόταση τα στοιχεία T^i με $(a,i) = 1$ είναι ακριβώς τα στοιχεία με τάξη m. Αυτά είναι ακριβώς $\phi(m)$ το πλήθος.

Ένα στοιχείο με τάξη $\delta \mid m$ είναι (πάλι σύμφωνα με την παραπάνω πρόταση) το στοιχείο $T^{m/\delta}$. Αυτό γεννά μια κυκλική ομάδα $\langle T^{m/\delta} \rangle$ η οποία έχει για γεννήτορες τα στοιχεία $T^{(m/\delta)j}$ με $(j,\delta) = 1$. Τα στοιχεία αυτά είναι $\phi(\delta)$ το πλήθος.

4.3.10 Πρόταση:
Για κάθε φυσικό αριθμό m *ισχύει*

$$m = \sum_{\delta \mid m} \phi(\delta).$$

Απόδειξη Εδώ θα δώσουμε μια απόδειξη βασισμένη στη θεωρία των κυκλικών ομάδων. Θεωρούμε την κυκλική ομάδα με τάξη m και διαμερίζουμε τα στοιχεία της ανάλογα με την τάξη τους. Από το θεώρημα του Lagrange οι δυνατές τάξεις στοιχείων της ομάδας είναι οι διαιρέτες $\delta \mid m$. Από την παραπάνω πρόταση ο τύπος είναι σαφής.

Κάνοντας χρήση του τύπου

$$\phi(m) = \sum_{\delta \mid m} \phi(\delta)$$

μπορούμε να δώσουμε ακόμα μία απόδειξη ότι η πολλαπλασιαστκή ομάδα ενός πεπερασμένου σώματος είναι κυκλική. Θα χρειαστούμε το παρακάτω:

4.3.11 Πρόταση:
Μια πεπερασμένη ομάδα G *με τάξη* m *είναι κυκλική αν και μόνο αν για κάθε διαιρέτη* $\delta \mid m$ *υπάρχει το πολύ μία κυκλική υποομάδα της* G *με τάξη* δ.

Απόδειξη Αν η G είναι κυκλική, τότε είναι σαφές ότι έχουμε ακριβώς μια υποομάδα με τάξη δ για κάθε $\delta \mid m$.

Αντιστρόφως, τα στοιχεία με τάξη δ στην ομάδα G είναι ή 0 ή $\phi(\delta)$. Πράγματι αν δεν υπάρχει στοιχείο με τάξη δ το πλήθος τους είναι 0 ενώ αν υπάρχει στοιχείο με τάξη δ τότε αυτό θα παράγει μια κυκλική ομάδα με τάξη δ η οποία θα είναι μοναδική. Αυτό θα έχει ως συνέπεια το πλήθος των στοιχείων με τάξη δ αν δεν είναι 0 να είναι $\phi(\delta)$. Διαμερίζουμε και πάλι τα στοιχεία της ομάδας με τάξη δ. Από τον τύπο του αθροίσματος έχουμε ότι

$$\sum_{\delta \mid m} \phi(\delta) = m = \sum_{\delta' \mid m} \phi(\delta')$$

όπου το αριστερό άθροισμα διατρέχει τους διαιρέτες $\delta \mid m$ ενώ το δεξί τους διαιρέτες δ' για τους οποίους υπάρχει στοιχείο τάξης δ' στην ομάδα G. Είναι σαφές (αφού και τα δύο αθροίσματα δίνουν αποτέλεσμα m) ότι για κάθε διαιρέτη υπάρχει στοιχείο τάξης δ και θεωρώντας $\delta = m$, έχουμε ότι η ομάδα είναι κυκλική.

Μπορούμε τώρα να δείξουμε ότι η πολλαπλασιαστική ομάδα ενός πεπερασμένου σώματος είναι κυκλική: Πράγματι, για κάθε $\delta \mid p^h - 1 = |\mathbb{F}_{p^h}|$ τα στοιχεία με τάξη δ είναι ακριβώς οι δ-ρίζες της μονάδας οι οποίες είναι οι λύσεις της εξίσωσης

$$x^\delta - 1 = 0$$

η οποία έχει το πολύ δ το πλήθος ρίζες.

4.3.12 Πρόταση:
Κάθε υπόσωμα του σώματος $\mathbb{F}_{p^n}$ έχει p^d στοιχεία με $d \mid n$. Επιπλέον, για $d \mid n$ υπάρχει μοναδικό υπόσωμα του $\mathbb{F}$ με p^d το πλήθος στοιχεία.

Απόδειξη Έστω K υπόσωμα του $\mathbb{F}_{p^n}$. Η χαρακτηριστική του είναι p άρα έχουμε την παρακάτω αλυσίδα σωμάτων:

$$\mathbb{F}_p \subset K \subset \mathbb{F}_{p^n}.$$

Ο βαθμός της επέκτασης $[K : \mathbb{F}_p] = d$, ενώ ο βαθμός της επέκτασης $[\mathbb{F}_{p^n} : \mathbb{F}_p] = n$. Άρα

$$n = d \cdot [\mathbb{F}_{p^n} : K].$$

Αντιστρόφως αν $d \mid n$, τότε $(p^d - 1) \mid (p^n - 1)$, αφού:

$$(p^n - 1) = (p^d)^{n/d} - 1 = (p^d - 1)(1 + p^d + p^{2d} + \cdots + p^{d(n/d-1)}).$$

Άρα $x^{p^d-1} - 1 \mid x^{p^n-1} - 1$ και συνεπώς $x^{p^d} - x \mid x^{p^n} - x$. Το σώμα ριζών του $x^{p^d} - x$ έχει p^d στοιχεία και δεν υπάρχει άλλο τέτοιο σώμα (αφού κάθε μη μηδενικό θα ήταν ρίζα του $x^d - x$.)

Παρατήρηση Αφού η ομάδα $\mathbb{F}_{p^h}$ είναι κυκλική τάξης $p^h - 1$, υπάρχουν ακριβώς $\phi(p^h - 1)$ γεννήτορές της (πρωταρχικά στοιχεία).

4.3.13 Πρόταση:
Για κάθε πεπερασμένο σώμα $\mathbb{F}_{p^k}$ και κάθε n υπάρχει ένα ανάγωγο πολυώνυμο βαθμού n.

Απόδειξη Θεωρούμε ένα σώμα E με p^{nk} το πλήθος στοιχεία. Θεωρούμε ένα πρωταρχικό στοιχείο ζ του E. Ισχύει ότι $E = \mathbb{F}_{p^k}(\zeta)$. Ο βαθμός της επέκτασης $\mathbb{F}_{p^k}(\zeta)/\mathbb{F}_{p^k}$ είναι n και ταυτίζεται με τον βαθμό του ανάγωγου πολυώνυμου του ζ. Το ελάχιστο πολυώνυμο του ζ είναι συνεπώς ίσο με n.

4.3.14 Θεώρημα:
Έστω $\mathbb{F}_{p^n}$ ένα πεπερασμένο σώμα με p^n το πλήθος στοιχεία. Θεωρούμε ένα ανάγωγο πολυώνυμο $\sigma(x) \in \mathbb{F}_{p^n}[x]$. Αν ζ είναι μια ρίζα του πολυωνύμου $\sigma(x)$, τότε το σώμα ριζών του $\sigma(x)$ είναι το $\mathbb{F}_{p^n}(\zeta)$. Με άλλα λόγια, αν επισυνάψουμε μία ρίζα του αναγώγου πολυωνύμου τότε τις επισυνάπτουμε όλες.

Απόδειξη Το σώμα $\mathbb{F}_{p^n}(\zeta)$, όπου ζ ρίζα του $\sigma(x)$ είναι ένα σώμα με p^{nd} στοιχεία, όπου $d = \deg(\sigma(x))$. Άρα το $\mathbb{F}_{p^n}(\zeta)$ είναι το σώμα ριζών του $x^{p^{nd}} - x$. Το $\sigma(x)$ διαιρεί το $x^{p^{nd}} - x$. Συνεπώς όλες οι ρίζες του $\sigma(x)$ είναι και ρίζες του $x^{p^{nd}} - x$.

Παρατήρηση Σε σώματα χαρακτηριστικής 0 το παραπάνω θεώρημα δεν είναι σωστό. Πράγματι το πολυώνυμο $x^3 - 2 \in \mathbb{Q}[x]$ έχει μια πραγματική ρίζα την $\sqrt[3]{2} \in \mathbb{R}$. Το σώμα $\mathbb{Q}(\sqrt[3]{2})$ δεν περιέχει τις άλλες δύο μιγαδικές ρίζες $\sqrt[3]{2}\omega$, $\sqrt[3]{2}\omega^2$ του $x^3 - 2$, όπου $\omega, \omega^2 = \overline{\omega}$ είναι οι μιγαδικές τρίτες ρίζες της μονάδας.

4.3.15 Πρόταση:
Έστω $\mathbb{F}_{p^h}$ σώμα με $q = p^h$ το πλήθος στοιχεία και $\sigma(x)$ ανάγωγο πολυώνυμο υπέρ του σώματος $\mathbb{F}_{p^h}$ και το οποίο έχει βαθμό d. Το $\sigma(x) \mid (x^{q^n} - x)$ αν και μόνο αν $d \mid n$.

Απόδειξη Έστω ζ μια ρίζα του $\sigma(x)$. Το σώμα $\mathbb{F}_q(\zeta)$ είναι ένα σώμα με q^d το πλήθος στοιχεία. Αν $\sigma(x) | x^{q^n} - x$ τότε το ζ είναι ρίζα του $x^{q^n} - x$ και συνεπώς το $\mathbb{F}_q(\zeta)$ με q^d το πλήθος στοιχεία είναι υπόσωμα του $\mathbb{F}_{q^n}$. Το σώμα ριζών του $x^{q^n} - x$ με q^n το πλήθος στοιχεία έχει ένα υπόσωμα με q^d στοιχεία αν και μόνο αν $d \mid n$.

4.4. Ο τελεστής του Frobenious

Θεωρούμε το πεπερασμένο σώμα $\mathbb{F}_q$ με $q = p^h$ το πλήθος στοιχεία. Θα δείξουμε ότι για κάθε φυσικό αριθμό d, υπάρχει μοναδικό μέχρι ισομορφισμού σώμα F ώστε $[F : \mathbb{F}_q] = d$. Το σώμα αυτό είναι το σώμα $\mathbb{F}_{q^d}$.

Ο τελεστής του Frobenious είναι μία συνάρτηση:

$$F_q : \mathbb{F}_{q^d} \to \mathbb{F}_{q^d}$$

$$x \mapsto x^q.$$

Παρατηρούμε ότι

$$F_q(x + y) = F_q(x) + F_q(y)$$

και ότι

$$F_q(xy) = F_q(x) \cdot F_q(y).$$

Επιπλέον ισχύει ότι $x \in \mathbb{F}_{q^d}$ είναι στοιχείο του $\mathbb{F}_q$ αν και μόνο αν $F_q(x) = x$.

Πράγματι έχουμε αποδείξει ότι τα στοιχεία του σώματος $\mathbb{F}_q$ είναι ακριβώς οι ρίζες του πολυωνύμου $x^q - x$. Αυτό σημαίνει ότι η συνάρτηση του Frobenious είναι γραμμική απεικόνιση του $\mathbb{F}_{q^d}$ αν

θεωρήσουμε το $\mathbb{F}_{q^d}$ ως διανυσματικό χώρο υπέρ του σώματος $\mathbb{F}_q$, δηλαδή

$$F_q(\lambda x + \mu y) = \lambda F_q(x) + \mu F_q(y),$$

για κάθε $x, y \in \mathbb{F}_{q^d}$ και $\lambda, \mu \in \mathbb{F}_q$.

Ας θεωρήσουμε την αλγεβρική κλειστότητα $\overline{\mathbb{F}}_q$ του σώματος $\mathbb{F}_q$. Κάθε στοιχείο x του σώματος $\overline{\mathbb{F}}_q$ είναι αλγεβρικό υπέρ του σώματος $\mathbb{F}_q$, άρα ικανοποιεί ένα ελάχιστο πολυώνυμο βαθμού d για κάποιο d και συνεπώς είναι στοιχείο του σώματος $\mathbb{F}_{q^d}$ για κάποιο d. Μπορούμε σε κάθε περίπτωση να ορίσουμε τον τελεστή του Frobenious ως συνάρτηση

$$F_q : \overline{\mathbb{F}}_q \to \overline{\mathbb{F}}_q,$$

$$x \mapsto x^q.$$

Έχουμε αποδείξει ότι

4.4.1 Θεώρημα:
Για κάθε $x \in \overline{\mathbb{F}}_q$

$$x \in \mathbb{F}_q \text{ } \textit{αν και μόνο αν} \text{ } F_q(x) = x.$$

Επίσης το παραπάνω μπορεί να γενικευτεί ως εξής:
Για κάθε $x \in \overline{\mathbb{F}}_q$

$$x \in \mathbb{F}_{q^\ell} \text{ } \textit{αν και μόνο αν} \text{ } (F_q)^\ell(x) = F_{q^\ell}(x) = x.$$

Παρατήρηση Ο τελεστής του Frobenious παίζει τον ρόλο της μιγαδικής συζυγίας η οποία είναι μία συνάρτηση $\mathbb{C} \to \mathbb{C}$. Είναι γνωστό ότι οι πραγματικοί αριθμοί είναι τα σταθερά στοιχεία της συζυγίας, δηλαδή ένα $x \in \mathbb{C}$ ανήκει στο $\mathbb{R}$ αν και μόνο αν $\overline{x} = x$.

Παρατήρηση Το σώμα $\mathbb{F}_{p^h}$ είναι το υπόσωμα του $\overline{\mathbb{F}}_p$ που σταθεροποιείται από τον τελεστή F_q, $q = p^h$. Τα υποσώματα του $\mathbb{F}_q$ είναι της μορφής $\mathbb{F}_{p^\ell}$ που σταθεροποιούνται από τον F_{p^ℓ}. Αφού $\mathbb{F}_{p^\ell} \subset \mathbb{F}_q$ ο τελεστής F_q ανήκει στην ομάδα που παράγει ο F_{p^ℓ}, άρα $F_q = F_{p^\ell}^s$ για κάποια δύναμη s. Δηλαδή $p^{\ell s} = p^h$. Δηλαδή δείξαμε και με έναν διαφορετικό τρόπο ότι τα υποσώματα του σώματος $\mathbb{F}_{p^h}$ αντιστοιχούν στους διαιρέτες του h.

Παρατήρηση Μία γνωστή πρόταση σχετικά με τα πραγματικά πολυώνυμα αναφέρει ότι αν ένα πολυώνυμο $f(x) \in \mathbb{R}[x]$ έχει μία ρίζα τότε θα έχει και τη συζυγή της. Η ανάλογη πρόταση στην περίπτωση των πεπερασμένων σωμάτων είναι η εξής:

4.4.2 Πρόταση:
Αν a *ρίζα του πολυωνύμου* $f \in \mathbb{F}_q[x]$ *τότε και όλες οι δυνάμεις* $F_q^i(a)$ *θα είναι ρίζες του* f.

Απόδειξη Έστω $f(x) = \sum_{\nu=0}^{n} a_\nu x^\nu$. Εφαρμόζουμε τον τελεστή F_q^i στην εξίσωση

$$f(a) = 0 \Leftrightarrow \sum_{\nu=0}^{n} a_\nu a^\nu = 0$$

και χρησιμοποιούμε το γεγονός ότι ο F_q^i είναι ομομορφισμός δακτυλίων καθώς και το ότι σταθεροποιεί τα στοιχεία του σώματος $\mathbb{F}_q$ για να καταλήξουμε στην εξίσωση:

$$\sum_{\nu=0}^{n} a_\nu F_q^i(a)^\nu = 0 \Leftrightarrow f(F_q^i(a)) = 0$$

Στην πραγματικότητα η ομάδα Galois της επέκτασης $\mathbb{F}_{q^d}/\mathbb{F}_q$ παράγεται από τον τελεστή του Frobenious. Καταρχήν ο τελεστής του Frobenious είναι ένας αυτομορφισμός $\mathbb{F}_{q^d} \to \mathbb{F}_{q^d}$ ο οποίος κρατά σταθερό το σώμα $\mathbb{F}_q$.

Ας είναι $\mathbb{F}_{q^d} = \mathbb{F}_q[x]/\langle f(x)\rangle$ μία γραφή του σώματος $\mathbb{F}_{q^d}$ ως πηλίκο ενός πολυωνυμικού δακτυλίου modulo το κύριο ιδεώδες που παράγεται από ένα ανάγωγο πολυώνυμο f.

Σταθεροποιούμε μία ρίζα $a \in \mathbb{F}_{q^d}$ του f. Αποδείξαμε ότι οι

$$a, a^q, a^{q^2}, a^{q^3} \dots$$

είναι επίσης ρίζες του $f(x)$. Αυτές λέγονται συζυγείς του a. Η ακολουθία έχει πεπερασμένο πλήθος διακεκριμένων μεταξύ τους στοιχείων. Υποθέτουμε $a \neq 0$. Έστω δ ο ελάχιστος θετικός ακέραιος για τον οποίο υπάρχει j με $0 \leqslant j < \delta$ ώστε $a^{q^\delta} = a^{q^j}$. Τότε

$$1 = a^{q^\delta - q^j} = a^{q^j(q^{\delta-j}-1)}.$$

Η τελευταία σχέση μας λέει ότι η τάξη $\mathrm{ord}(a)$ του a ως στοιχείο της πολλαπλασιαστικής ομάδας $\mathbb{F}_{q^d}^*$ ικανοποιεί

$$\mathrm{ord}(a) \mid q^j(q^{\delta-j}-1).$$

Από την άλλη μεριά $\#\mathbb{F}_{q^d}^* = q^d - 1$, οπότε $\mathrm{ord}(a) \mid q^d - 1$ και συνεπώς $(\mathrm{ord}(a), q^j) = 1$, άρα έχουμε $\mathrm{ord}(a) \mid (q^{\delta-j}-1)$ ή

$$a^{q^{\delta-j}} = a.$$

Το δ όμως είναι ο εκθέτης της πρώτης επανάληψης. Συνεπώς θα πρέπει $j = 0$ οπότε

$$a^{q^\delta} = a.$$

Όμως $a \in \mathbb{F}_{q^d}$ και $\#\mathbb{F}_{q^d} = q^d$ το οποίο σύμφωνα με το θεώρημα του Lagrange δίνει $a^{q^d} = a$.

Θα αποδείξουμε την παρακάτω:

4.4.3 Πρόταση:

$$(x^m - 1, x^n - 1) = x^{(m,n)} - 1.$$

Πράγματι μπορούμε να υποθέσουμε ότι $m > n$. Σε αυτή την περίπτωση

$$x^m - 1 - x^{m-n}(x^n - 1) = x^{m-n} - 1.$$

Συνεπώς ένα πολυώνυμο που διαιρεί και το $x^m - 1$ και το $x^n - 1$ θα διαιρεί και το $x^{m-n} - 1$. Από την επαγωγική υπόθεση

$$(x^{m-n} - 1, x^n - 1) = x^{(m-n,n)} - 1$$

όμως

$$(m, n) = (m - n, n)$$

συνεπώς

$$(x^m - 1, x^n - 1) = (x^{m-n} - 1, x^n - 1) = x^{(m-n,n)} - 1 = x^{(m,n)} - 1.$$

□

Από την παραπάνω πρόταση παίρνουμε ότι $a^{q^{(d,\delta)}} = a$. Αυτό όμως είναι σε κάθε περίπτωση άτοπο, διότι υποθέσαμε ότι δ είναι η πρώτη επανάληψη της ακολουθίας

$$a, a^q, a^{q^2}, a^{q^3} \dots$$

Εκτός αν $(\delta, d) = \delta$. Δηλαδή πρέπει το $\delta \mid d$.

Συμπέρασμα: Το πλήθος των διακεκριμένων συζυγών δ του a είναι ένας διαιρέτης του d. Το δ αυτό θα λέγεται βαθμός του a. Μάλιστα είναι ο ελάχιστος θετικός ακέραιος ώστε

$$q^\delta \equiv 1 \mathrm{mod} t,$$

όπου $t = \mathrm{ord}(a)$. Δηλαδή αποδείξαμε το

4.4.4 Θεώρημα:
Το πλήθος των (διακεκριμένων) συζυγών του a, *έστω* δ, *είναι ένας διαιρέτης του* d. *Ο* δ *είναι ο ελάχιστος θετικός ακέραιος που ικανοποιεί την*

$$t = ord(a) \mid q^\delta – 1.$$

Ακόμα, αν $\lambda = \mu\delta + r$ *όπου* $0 \leqslant r \leqslant \delta – 1$ *τότε*

$$a^{q^\lambda} = a^{q^r}.$$

Απόδειξη Θα αποδείξουμε ότι αν $\lambda = \mu\delta + r$ όπου $0 \leqslant r \leqslant d – 1$ τότε

$$a^{q^\lambda} = a^{q^r}.$$

Παρατηρούμε ότι

$$a^{q^\lambda} = a^{q^{\mu\delta+r}} = \left(a^{q^\delta}\right)^{q^r} = a^{q^r}.$$

□

Το ελάχιστο πολυώνυμο του a θα πρέπει να έχει τουλάχιστον δ ρίζες. Συγκεκριμένα αποδείξαμε ότι μαζί με το a και οι δυνάμεις

$$a, a^q, a^{q^2}, a^{q^3} \dots a^{q^{\delta-1}}$$

είναι επίσης ρίζες. Έστω

$$f_a(x) := (x–a)(x–a^q)\cdots(x – a^{\delta-1})$$

και $f(x)$ το ελάχιστο πολυώνυμο του f.

Τότε το $f_a(x)$ διαιρεί το $f(x)$. Θα αποδείξουμε ότι $f_a(x) = f(x)$. Γράφουμε

$$f_a(x) := (x–a)(x–a^q)\cdots(x – a^{\delta-1}) = \sum_{\nu=0}^{\delta} A_\nu x^\nu,$$

όπου $A_i \in \mathbb{F}_{q^d}$. Υψώνουμε στην q-δύναμη (δηλαδή εφαρμόζουμε τον τελεστή του Frobenious) για να πάρουμε

$$f_a(x)^q := (x–a)^q(x–a^q)^q\cdots(x – a^{\delta-1})^q = \sum_{\nu=0}^{\delta} A_\nu^q x^{q\nu}.$$

Επιπλέον έχουμε ότι $(x – b)^q = x^q – (-1)^q b^q = x^q – b^q$. Αυτό μας δίνει ότι το

$$f_a(x)^q = f_a(x^q) = \sum_{\nu=0}^{\delta} A_\nu x^{\nu q}$$

και έτσι καταλήγουμε στην

$$\sum_{\nu=0}^{\delta} A_\nu x^{\nu q} = \sum_{\nu=0}^{\delta} A_\nu^q x^{\nu q}$$

άρα

$$A_i^q = A_i$$

για κάθε $i = 1, \ldots, \delta - 1$, συνεπώς $A_i \in \mathbb{F}_q$. Αποδείξαμε λοιπόν το ακόλουθο:

4.4.5 Θεώρημα:
Αν $\mathbb{F}_{q^d}$ πεπερασμένο σώμα με q^d στοιχεία και K υπόσωμα με με q στοιχεία και $\alpha \in \mathbb{F}_{q^d}$, τότε το ελάχιστο πολυώνυμο του α ως προς το σώμα K είναι το

$$f_\alpha(x) := (x - \alpha)(x - \alpha^q) \cdots (x - \alpha^{\delta - 1}),$$

όπου δ είναι ο ελάχιστος φυσικός τέτοιος ώστε

$$q^\delta \equiv 1 \mathit{modord}(\alpha).$$

Παράδειγμα Για $q = 2$ και $d = 4$ θεωρούμε την επέκταση

$$\mathbb{F}/K \text{ όπου } \mathbb{F} = \mathbb{F}_{16}, K = \mathbb{F}_2 = \{0, 1\}$$

Παρατηρούμε ότι το $x^4 + x + 1 \in \mathbb{F}_2[X]$ είναι ανάγωγο. Θα κατασκευάσουμε το σώμα με $16 = 2^4$ στοιχεία μέσω αυτού του πολυωνύμου, δηλαδή θα κατασκευάσουμε το

$$\mathbb{F}_{16} = \mathbb{F}_2[x]/\langle x^4 + x + 1 \rangle.$$

Ο $\mathbb{F}_{16}$ είναι $\mathbb{F}_2$-διανυσματικός χώρος διάστασης 4.

Αν με α συμβολίσουμε το x (modulo $x^4 + x + 1$) τότε, ως διάνυσμα, το α είναι το $(0, 0, 1, 0)$. Τα στοιχεία του $\mathbb{F}_{16}$ θα αντιστοιχούν σε διατεταγμένες τετράδες (a, b, c, d) όπου τα a, b, c, d είναι οι συντελεστές του υπολοίπου της διαίρεσης με x^4+x+1, το υπόλοιπο δηλαδή θα είναι ax^3+bx^2+cx+d.

Υπολογίζουμε τις δυνάμεις του α:
$\alpha^2 \to x^2$ επομένως $\alpha^2 = (0, 1, 0, 0)$
$\alpha^3 \to x^3$ επομένως $\alpha^3 = (1, 0, 0, 0)$
$\alpha^4 \to x^4$ (modulo $x^4 + x + 1 = \alpha + 1$ επομένως $\alpha^4 = (0, 0, 1, 1)$
$\alpha^5 = \alpha^2 + \alpha$ επομένως $\alpha^5 = (0, 1, 1, 0)$
$\alpha^6 = \alpha^3 + \alpha^2$ επομένως $\alpha^6 = (1, 1, 0, 0)$
$\alpha^7 = \alpha^4 + \alpha^3 = \alpha^3 + \alpha + 1$ επομένως $\alpha^7 = (1, 0, 1, 1)$
$\alpha^8 = \alpha^4 + \alpha^2 + \alpha = \alpha^2 + 2\alpha + 1 = \alpha^2 + 1$ επομένως $\alpha^8 = (0, 1, 0, 1)$
$\alpha^9 = \alpha^4 + \alpha$ επομένως $\alpha^9 = (1, 0, 1, 0)$
$\alpha^{10} = \alpha^4 + \alpha^2 = \alpha^2 + \alpha + 1$ επομένως $\alpha^{10} = (0, 1, 1, 1)$
$\alpha^{11} = \alpha^3 + \alpha^2 + \alpha$ επομένως $\alpha_{11} = (1, 1, 1, 0)$
$\alpha^{12} = \alpha^4 + \alpha^3 + \alpha^2 = \alpha^3 + \alpha^2 + \alpha + 1$ επομένως $\alpha^{12} = (1, 1, 1, 1)$
$\alpha^{13} = \alpha^4 + \alpha^3 + \alpha^2 + \alpha = \alpha^3 + \alpha^2 + 2\alpha + 1 = \alpha^3 + \alpha^2 + 1$ επομένως $\alpha^{13} = (1, 1, 0, 1)$
$\alpha^{14} = \alpha^4 + \alpha^3 + \alpha = \alpha^3 + 2\alpha + 1 = \alpha^3 + 1$ επομένως $\alpha^{14} = (1, 0, 0, 1)$
$\alpha^{15} = \alpha^4 + \alpha = 2\alpha + 1 = 1$ επομένως $\alpha^{15} = (0, 1, 0, 1)$
Κατασκευάζουμε τον παρακάτω πίνακα:

Πίνακας 4.1: Δυνάμεις του α, τάξεις και ελάχιστα πολυώνυμα

i	α^i	ord(α^i)	deg(α)	ελάχιστο πολυώνυμο
0	(0001)	1	1	$x+1$
1	(0010)	15	4	$(x–\alpha)(x–\alpha^2)(x–\alpha^4)(x–\alpha^8)$
2	(0100)	15	4	$(x–\alpha)(x–\alpha^2)(x–\alpha^4)(x–\alpha^8)$
3	(1000)	5	4	$(x–\alpha^3)(x–\alpha^6)(x–\alpha^9)(x–\alpha^{12})$
4	(0011)	15	4	$(x–\alpha)(x–\alpha^2)(x–\alpha^4)(x–\alpha^8)$
5	(0110)	3	2	$(x–\alpha^5)(x–\alpha^{10})$
6	(1100)	5	4	$(x–\alpha^3)(x–\alpha^6)(x–\alpha^9)(x–\alpha^{12})$
7	(1011)	15	4	
8	(0101)	15	4	$(x–\alpha)(x–\alpha^2)(x–\alpha^4)(x–\alpha^8)$
9	(1010)	5	4	$(x–\alpha^3)(x–\alpha^6)(x–\alpha^9)(x–\alpha^{12})$
10	(0111)	3	2	$(x–\alpha^5)(x–\alpha^{10})$
11	(1110)	15	4	
12	(1111)	5	4	$(x–\alpha^3)(x–\alpha^6)(x–\alpha^9)(x–\alpha^{12})$
13	(1101)	15	4	
14	(1001)	15	4	
15	(0001)			

Θυμόμαστε ότι ο βαθμός του α^i είναι ο ελάχιστος φυσικός $d > 0$ τέτοιος ώστε

$$q^d \equiv 1(\text{mod} \text{ord}(\alpha^i)).$$

Εδώ για το α έχουμε $t = 15$ και $q = 2$, οπότε θέλουμε

$$2^d \equiv 1(\text{mod} 15).$$

Δηλαδή $d = 4$. Έχουμε ότι:

$$(x–\alpha)(x–\alpha^2)(x–\alpha^4)(x–\alpha^8) = (x^2–\alpha x–\alpha^2 x + \alpha^3)(x–\alpha^4)(x–\alpha^8) =$$
$$= (x^3–\alpha x^2–\alpha^2 x^2 + \alpha^3 x–\alpha^4 x^2 + \alpha^5 x + \alpha^6 x–\alpha^7)(x–\alpha^8) =$$
$$= (x^3–(\alpha + \alpha^2 + \alpha^4)x^2 + (\alpha^3 + \alpha^5 + \alpha^6)x–\alpha^7)(x–\alpha^8) =$$
$$= x^4–(\alpha+\alpha^2+\alpha^4)x^3+(\alpha^3+\alpha^5+\alpha^6)x^2–\alpha^7 x–\alpha^8 x^3+\alpha^8(\alpha+\alpha^2+\alpha^4)x^2–\alpha^8(\alpha^3+\alpha^5 x^2+\alpha^6)x+\alpha^{15} =$$
$$= x^4 + (\alpha^8 + \alpha^4 + \alpha^2 + \alpha)x^3 + (\alpha^{12} + \alpha^{10} + \alpha^9 + \alpha^6 + \alpha^5 + \alpha^3)x^2 + (\alpha^{14} + \alpha^{13} + \alpha^{11} + \alpha^7)x + \alpha^{15} =$$
$$= x^4 + 0x^3 + 0x62 + 1x + 1 =$$
$$= x^4 + x + 1$$

Αυτό δεν είναι τυχαίο. Είναι το πολυώνυμο απ' το οποίο ξεκινήσαμε. Θα υπολογίσουμε τώρα το ελάχιστο πολυώνυμο του $b = \alpha^3$. Τα α^2, α^4, α^8 είναι τα συζυγή του α, άρα το ελάχιστο πολυώνυμο και για αυτά είναι το ίδιο με του α. Αν πάρουμε το $(x–\alpha^3)(x–\alpha^6)(x–\alpha^9)(x–\alpha^{12})$ θα βρούμε το $x^4 + x^3 + x^2 + x + 1$. Θα μπορούσαμε να κάνουμε τον υπολογισμό στο sage, αλλά ας δούμε ένα διαφορετικό επιχείρημα: Ονομάζουμε $b = \alpha^3$ τότε έχουμε:

$$1 = (0001)$$
$$b = (1000)$$
$$b^2 = (1100)$$
$$b^3 = (1010)$$

$$b^4 = (1111)$$

Παρατηρούμε από το δεξί μέρος των παραπάνω εξισώσεων ότι

$$b^4 + b^3 + b^2 + b + 1 = 0.$$

Αλλά $b = a^3 \neq 1$ οπότε $b^5 = (a^3)^5 = a^{15} = 1$ Το b είναι μια 5–ρίζα της μονάδας, δηλαδή ρίζα του πολυωνύμου

$$x^5–1 = (x–1)(x^4 + x^3 + x^2 + x + 1).$$

4.5. Ν-στές ρίζες της μονάδας

Σε ένα σώμα $\mathbb{F}$ το x θα λέγεται n-οστή ρίζα της μονάδας αν και μόνο αν είναι ρίζα της εξίσωσης $x^n = 1$.

Αν το n είναι δύναμη της χαρακτηριστικής, τότε υπάρχει μόνο μια n-στή ρίζα της μονάδας, το 1. Πράγματι

$$x^{p^h} - 1 = 0 \text{ είναι ισοδύναμο με } (x-1)^{p^h} = 0$$

δηλαδή $x = 1$.

Ομοίως αν $n = p^h \cdot m$, $(m, p) = 1$ τότε οι n-στές ρίζες της μονάδας είναι ίδιες με τις m-ρίζες της μονάδας αφού

$$x^n - 1 = 0 \text{ είναι ισοδύναμο με } (x^m - 1)^{p^h} = 0.$$

4.5.1 Ορισμός:
Έστω $(n, p) = 1$ *με* E_n *θα συμβολίζουμε το σύνολο των* n*-οστών ριζών της μονάδας στο σώμα* $\overline{\mathbb{F}}_p$.

Το πλήθος των στοιχείων του E_n είναι n αφού το πολυώνυμο ορισμού έχει απλές ρίζες (η παράγωγός του $D(x^n - 1) = nx^{n-1}$ έχει μοναδική ρίζα το 0 άρα δεν μηδενίζεται σε ρίζα της μονάδας).

Το σύνολο E_n είναι ομάδα τάξης n η οποία είναι κυκλική, αφού είναι υποομάδα της πολλαπλασιαστικής ομάδας του σώματος που περιέχει όλες τις ρίζες.

4.5.2 Θεώρημα:
Έστω E *το σώμα ριζών του πολυωνύμου* $x^n - 1$ *υπέρ του πεπερασμένου σώματος* $\mathbb{F}_q$. *Ο βαθμός* $[E : \mathbb{F}_q] = s$ *είναι ο ελάχιστος φυσικός ώστε*

$$q^s \equiv 1 mod n.$$

Απόδειξη Αφού το πλήθος των στοιχείων του E θα είναι q^s η ομάδα E^* θα έχει τάξη $q^s - 1$ και συνεπώς $n \mid q^s - 1$, συνεπώς $q^s \equiv 1 \bmod n$.

Αντιστρόφως, έστω ότι $n \mid q^r - 1$ τότε $(x^n - 1) \mid (x^{q^r} - x)$. Άρα κάθε ρίζα του $x^n - 1$ είναι ρίζα του $(x^{q^r} - x)$ και συνεπώς περιέχεται στο $\mathbb{F}_{q^r}$. Έχουμε αποδείξει ότι το σώμα ριζών E του $x^n - 1$ περιέχεται στο σώμα με q^r στοιχεία αρκεί να ισχύει ότι $n \mid q^r - 1$. Το ελάχιστο σώμα E είναι αυτό που εμφανίζεται στον ελάχιστο s για τον οποίο ισχύει $n \mid q^s - 1$.

4.5.3 Ορισμός:
Ένας γεννήτορας ω της κυκλικής ομάδας E_n θα λέγεται πρωταρχική n-ρίζα της μονάδας.

Από τη μία έχουμε τα πρωταρχικά στοιχεία στο σώμα ριζών E του πολυωνύμου $x^n - 1$ τα οποία γεννούν μια κυκλική ομάδα E^* με τάξη $q^s - 1$ και από την άλλη έχουμε την κυκλική υποομάδα $E_n < E^*$. Ας υποθέσουμε ότι ω είναι ένας γεννήτορας της E_n. Είναι σαφές ότι

$$\omega = \zeta^\ell,$$

όπου ζ είναι ένα πρωταρχικό στοιχείο (γεννήτορας της E^*) και ℓ κατάλληλη δύναμη ώστε το ω να έχει τάξη n.

Είναι γνωστό ότι το στοιχείο ζ^ℓ έχει τάξη

$$\frac{q^s - 1}{(\ell, q^s - 1)}.$$

Στον παραπάνω τύπο αντικαθιστούμε το $q^s - 1 = nr$ και έχουμε

$$\frac{q^s - 1}{(\ell, q^s - 1)} = \frac{nr}{(\ell, nr)}.$$

Απαιτούμε το τελευταίο κλάσμα να είναι ίσο με n το οποίο είναι ισοδύναμο με $r = (\ell, nr)$, δηλαδή $\ell = rm = \frac{q^s-1}{n} m$ με $(m, n) = 1$. Καταλήγουμε λοιπόν στον παρακάτω χαρακτηρισμό:

4.5.4 Θεώρημα:
Αν ζ είναι ένα πρωταρχικό στοιχείο του σώματος ριζών E του $x^n - 1$ στο $\mathbb{F}[x]$, τότε το σύνολο των πρωταρχικών ριζών του είναι το

$$\left\{ \zeta^{\frac{q^s-1}{n} \cdot m}, 1 \leqslant m < n, (m, n) = 1 \right\}.$$

Πώς θα υπολογίσουμε πρωταρχικά στοιχεία; Ας θεωρήσουμε ένα σώμα με q το πλήθος στοιχεία, όπου το q είναι μια δύναμη πρώτου. Αν το πεπερασμένο σώμα είναι μεγάλο τότε τα πράγματα είναι δύσκολα. Υπάρχει ένας αλγόριθμος, γνωστός ως αλγόριθμος του Gauss που ως έξοδό του δίνει δίνει στοιχεία του πεπερασμένου σώματος $a_1, \ldots, a_k$ ώστε

$$\operatorname{ord}(a_1) < \operatorname{ord}(a_2) < \cdots < \operatorname{ord}(a_k) = q - 1.$$

Επιπλέον ισχύει ότι $\operatorname{ord}(a_i) \mid \operatorname{ord}(a_{i+1})$.

Ο αλγόριθμος αυτός δίνεται από τα παρακάτω βήματα:

1. Έστω $i = 1$ και $a_1 \in \mathbb{F}^*$ με $\operatorname{ord}(a_1) = t_1$.
2. Αν $t_i = q - 1$ τελειώσαμε. Το a_i είναι ένα πρωταρχικό στοιχείο.
3. Αν $\operatorname{ord}(a_i) < q - 1$ επιλέγουμε μη-μηδενικό στοιχείο του $\mathbb{F}$ (έστω b), ώστε το b να μην είναι δύναμη του a_i που υπολογίσαμε στο προηγούμενο βήμα. Έστω ότι $\operatorname{ord}(b) = s$. Αν $s = q - 1$ θέτουμε $a_{i+1} = b$ και τελειώσαμε.
4. Διαφορετικά βρίσκουμε $d \mid t_i$ και $e \mid s$ τέτοια ώστε $(d, e) = 1$ και $d \cdot e = [t_i, s]$. Οπότε θέτουμε
$$a_{i+1} = a_i^{t_i/d} b^{s/e},$$
$t_i = [t_i, s]$, $i \to i + 1$ και πηγαίνουμε στο δεύτερο βήμα.

Παράδειγμα Ας θεωρήσουμε το σώμα $\mathbb{F}_{25}$ με 25 το πλήθος στοιχεία. Θεωρούμε το πολυώνυμο $x^2-2 \in \mathbb{F}_5[x]$. Το πολυώνυμο αυτό είναι ανάγωγο ως προς το σώμα $\mathbb{F}_5$ αφού είναι βαθμού 2 και κανένα στοιχείο του $\mathbb{F}_5$ δεν είναι ρίζα του. Συνεπώς το σώμα $\mathbb{F}_{25}$ είναι ισόμορφο με το σώμα $\mathbb{F}_5[x]/\langle x^2-2\rangle$.

Ξεκινάμε τον αλγόριθμο του Gauss: Θέτουμε $a_1 = x$ και υπολογίζουμε τις δυνάμεις του a_1.

$$a_1^0 = 1, a_1^1 = x^1 = x, a_1^2 = x^2 = 2, x^3 = 2x, x^4 = 4, x^5 = 4x, x^6 = 3, x^7 = 3x, x^8 = 1.$$

Η τάξη της κυκλικής ομάδας του $\mathbb{F}_{25}$ είναι 24.

Εφαρμόζουμε το βήμα 2. Διαλέγουμε ένα στοιχείο b το οποίο δεν είναι δύναμη του a_1 για παράδειγμα το $1+x$. Υπολογίζουμε τις δυνάμεις του b.

$$b, b^2 = 2x+3, b^3 = 2, b^4 = 2x+2$$

$$b^5 = 4x+1, b^6 = 4, b^7 = 4x+4, b^8 = 3x+2$$

$$b^9 = 3, b^{10} = 3x+3, b^{11} = x+4, b^{12} = 1$$

Το στοιχείο b έχει τάξη 12 και πάλι δεν έχουμε τετραγωνική ρίζα.

Εφαρμόζουμε τώρα το βήμα 4. Ψάχνουμε d, e με $d \mid t_1 = 8$ και $e \mid s = 12$ ώστε $(d, e) = 1$ και $d \cdot e = [t_1, s] = (8, 12) = 24$. Υπολογίζουμε ότι $d = 8$ και ότι $e = 3$. Σύμφωνα με το βήμα 4 παίρνουμε

$$a_2 = a_1^{t_1/d} b^{s/e}.$$

Δηλαδή

$$a_2 = a_1^{8/8} b^{12/3} = a_1 b^4 = 2x+4.$$

Σε μία ομάδα με δύο στοιχεία A, B για τα οποία ισχύει $AB = BA$ και τα οποία έχουν τάξεις m, n με $(m, n) = 1$ έχουμε ότι η τάξη του γινομένου είναι nm.

Συνεπώς το $2x+4$ έχει τάξη 24 και είναι μία πρωταρχική ρίζα στο $\mathbb{F}_{25}$.

```
sage:F=FiniteField(5);F
Finite Field of size 5
sage:R.<x>=PolynomialRing(F);R
Univariate Polynomial Ring in x over Finite Field of size
sage:I = R.ideal([x^2-2]);I
Principal ideal (x^2 + 3) of Univariate Polynomial
 Ring in x over Finite Field of size 5
sage:S=R.quotient_ring(I);S
Univariate Quotient Polynomial Ring in xbar
over Finite Field of size 5 with
modulus x^2 + 3
sage:is_field(S)
true
```

Interactive

Ας υπολογίσουμε τις δυνάμεις του x με το sage:

```
for i in range(1,9):
    i,x^i
(1, x)
(2, 2)
(3, 2*x)
(4, 4)
(5, 4*x)
(6, 3)
(7, 3*x)
(8, 1)
```

Και ας κάνουμε το ίδιο για τις δυνάμεις του $1 + x$

```
for i in range(1,13):
    i,(1+x)^i
(1, x + 1)
(2, 2*x + 3)
(3, 2)
(4, 2*x + 2)
(5, 4*x + 1)
(6, 4)
(7, 4*x + 4)
(8, 3*x + 2)
(9, 3)
(10, 3*x + 3)
(11, x + 4)
(12, 1)
```

Ας κάνουμε τον ίδιο υπολογισμό για τον γεννήτορα $2x + 4$ που υπολογίσαμε:

```
for i in range(1,25):
    i,(4+2*x)^i
(1, 2*x + 4)
(2, x + 4)
(3, 2*x)
(4, 3*x + 3)
(5, 3*x + 4)
(6, 3)
(7, x + 2)
(8, 3*x + 2)
(9, x)
(10, 4*x + 4)
(11, 4*x + 2)
(12, 4)
(13, 3*x + 1)
```

```
(14, 4*x + 1)
(15, 3*x)
(16, 2*x + 2)
(17, 2*x + 1)
(18, 2)
(19, 4*x + 3)
(20, 2*x + 3)
(21, 4*x)
(22, x + 1)
(23, x + 3)
(24, 1)
```

Ας υπολογίσουμε τώρα το ελάχιστο πολυώνυμο του στοιχείου $2x+4$. Για αυτό θα επιστρατεύσουμε την ομάδα Galois η οποία είναι τάξης 2 και αποτελείται από δύο στοιχεία: την ταυτότητα Id και τη συνάρτηση σ η οποία στέλνει το x στο $-x$. Το ελάχιστο πολυώνυμο θα πρέπει να έχει ρίζα τουλάχιστον το $2x+4$, $\sigma(2x+4) = -2x+4$. Υπολογίζουμε ότι

$$(X-(2x+4))(X-(-2x+4)) = X^2 - 8X + 8 = X^2 + 2X + 5.$$

Το παραπάνω είναι το ελάχιστο πολυώνυμο του $2x+4$. Η κατασκευή του σώματος με 25 στοιχεία ως πηλίκο

$$\mathbb{F}_{25} = \mathbb{F}_5[a]/\langle a^2 + 2x + 5\rangle,$$

υπερτερεί από την προηγούμενη στην παράσταση των στοιχείων του σώματος.

4.6. Ανάγωγα πολυώνυμα σε πεπερασμένα σώματα

Έστω ένα πεπερασμένο σώμα. Τα πρωταρχικά στοιχεία είναι οι γεννήτορες της κυκλικής ομάδας K^*. Το ελάχιστο πολυώνυμο ενός πρωταρχικού στοιχείου λέγεται ένα πρωταρχικό πολυώνυμο.

4.6.1 Θεώρημα:
Έστω $\mathbb{F}_q$ ένα πεπερασμένο σώμα. Το πολυώνυμο $f(x) \in \mathbb{F}_q[x]$ είναι πρωταρχικό για κάποια επέκταση του $\mathbb{F}_q$ βαθμού d αν και μόνο αν ισχύει ότι $f(x) \mid x^{q^d-1}-1$ και $f(x)$ δεν διαιρεί το x^k-1 για $k < q^d-1$.

Απόδειξη Έχουμε ήδη αποδείξει ότι ένα ανάγωγο πολυώνυμο βαθμού d θα πρέπει να διαιρεί το $x^{q^d-1}-1$. Αν $f(x)$ δεν διαιρεί το x^k-1 και $k < q^{d-1}$ καμία ρίζα του f δεν έχει τάξη μικρότερη του q^d-1, άρα έχει την σωστή τάξη q^d-1.

Αντιστρόφως, αν το πολυώνυμο $f(x)$ είναι πρωταρχικό, τότε θα δείξουμε ότι $f(x)$ δεν διαιρεί το x^k-1 για $k < q^d-1$. Ας θεωρήσουμε τη ρίζα ζ του $f(x)$. Οι άλλες ρίζες του πολυωνύμου θα είναι οι

$$\zeta, F_q(\zeta) = \zeta^q, F_{q^2}(\zeta) = \zeta^{q^2}, \ldots, F_{q^{d-1}}(\zeta) = \zeta^{q^d-1}$$

αυτές είναι ανά δύο διαφορετικές και δεν μπορεί να είναι ρίζες του πολυωνύμου x^k-1 βαθμού $k < q^d-1$.

Αν και είναι δύσκολο να υπολογίσουμε τα ανάγωγα πολυώνυμα του $\mathbb{F}_q$ μπορούμε να υπολογίζουμε το πλήθος τους. Είναι γνωστό ότι

$$x^{q^n} - x = \prod_{d|n} V_d,$$

όπου V_d είναι το γινόμενο όλων των μονικών αναγώγων πολυωνύμων του $\mathbb{F}_q[x]$ βαθμού d. Αν λοιπόν I_d είναι το πλήθος των διακεκριμένων μονικών πολυωνύμων βαθμού d, τότε συγκρίνοντας βαθμούς έχουμε

$$q^n = \sum_{d|n} d \cdot I_d.$$

Από τον νόμο αντιστροφής του Moebious που έχουμε αποδείξει προκύπτει ότι

$$I_n = \frac{1}{n} \sum_{d|n} \mu(d) q^{n/d}.$$

4.6.1. Κυκλοτομικά Πολυώνυμα. Θα ορίσουμε πρώτα τα κυκλοτομικά πολυώνυμα στον δακτύλιο $\mathbb{Z}[x]$.

4.6.2 Ορισμός:
Το n-οστό κυκλοτομικό πολυώνυμο $\Phi_n(x)$ είναι το μοναδικό ανάγωγο πολυώνυμο στο $\mathbb{Z}[x]$ το οποίο διαιρεί το $x^n - 1$ αλλά όχι το $x^k - 1$ για κάθε $k < n$.

4.6.3 Πρόταση:
Αν ζ είναι μία ρίζα του Φ_n τότε και ζ^d είναι ρίζα του Φ_n για κάθε d, $(d, n) = 1$.

Απόδειξη Θα δώσουμε μια απόδειξη βασισμένη σε αυτή του Schur. Για ένα πλήθος άλλων αποδείξεων εμπλουτισμένες με ιστορικά στοιχεία παραπέμπουμε στο άρθρο του S. Weintraub.

Θεωρούμε το πολυώνυμο $x^n - 1$ και θέτουμε Δ τη "διακρίνουσά", του δηλαδή την ποσότητα

$$\Delta = \prod_{i<j} (\zeta_n^i - \zeta_n^j)^2 =$$

$$= \pm \prod_{i \neq j} (\zeta_n^i - \zeta_n^j) =$$

$$= \pm \prod_{i \neq j} \zeta_n^i (1 - \zeta_n^{j-i}) =$$

$$= \pm \prod_{i} \zeta_n^i \prod_{k \neq 0} (1 - \zeta_n^k).$$

Το γινόμενο

$$\prod_{k \neq 0} (1 - \zeta_n^k) = n.$$

Πράγματι είναι ίσο με την τιμή $x = 1$ στο πολυώνυμο

$$h(x) = \prod_{k \neq 0} (x - \zeta_n^k) = \frac{x^n - 1}{x - 1} =$$

$$= 1 + x + x^2 + \cdots + x^{n-1}.$$

Άρα ο υπολογισμός της διακρίνουσας ολοκληρώνεται στον

$$\Delta = \pm n^n.$$

Για να δείξουμε ότι ζ_n^d είναι ρίζα του $\Phi_n(x)$, αρκεί να δείξουμε ότι αν ζ ριζα του $\Phi_n(x)$ τότε και ζ^p είναι ρίζα για κάθε πρώτο p που δεν διαιρεί το n. Ας υποθέσουμε πως όχι. Το $\Phi_n(x)$ είναι ένας ανάγωγος παράγοντας (όταν ολοκληρωθεί η απόδειξη θα έχουμε δείξει ότι είναι και μοναδικός) του πολυωνύμου $x^n - 1$. Συνεπώς θα έχουμε ότι

$$\Phi_n(x) = (x - \zeta_1) \cdots (x - \zeta_k),$$

για κάποιες n-στές ρίζες του 1, $\zeta_1 = \zeta$ και που δεν συμπεριλαμβάνουν το ζ^p. Αυτό σημαίνει ότι το $\Phi_n(\zeta^p)$ αποτελείται από διαφορές n-οστών ριζών της μονάδας και διαιρεί το n^n. Από την άλλη, είναι ένα μη μηδενικό στοιχείο του $\mathbb{Q}(\zeta) = \mathbb{Z}[x]/\langle \Phi_n(x) \rangle$ και έχει μια μορφή

$$\Phi_n(\zeta^p) = a_0 + a_1\zeta + \cdots + a_{n-1}\zeta^{n-1}.$$

Αν την παραπάνω έκφραση τη θεωρήσουμε modulo p, καταλήγουμε σε ένα δακτύλιο χαρακτηριστικής p και έκει έχουμε

$$\Phi_n(\zeta^p) \equiv \Phi_n(\zeta)^p = 0 \mathrm{mod} p$$

Άρα όλοι οι συντελεστές a_i είναι διαιρετοί με p και συνεπώς $p \mid n^n$, άτοπο.

Παρατηρούμε ότι αν $d \mid n$, τότε $x^d - 1$ διαιρεί το $x^n - 1$. Επιπλέον λόγω μοναδικής παραγοντοποίησης στον δακτύλιο $K[x]$ το ελάχιστο κοινό πολλαπλάσιο πολυωνύμων που διαιρούν το $x^n - 1$ επίσης διαιρεί το $x^n - 1$.

Το πολυώνυμο $x - a$ διαιρεί το $f(x)$ αν και μόνο αν $f(a) = 0$. Συνεπώς $a^t = 1$ αν και μόνο αν $x - a$ διαιρεί το $x^t - 1$. Επίσης ο παραπάνω ορισμός δίνει ότι $\Phi_n(a) = 0$, άρα $a^n = 1$ και επίσης ότι το a δεν είναι ρίζα μικρότερης τάξης γιατί αν $a^t = 1$, τότε το $x - a$ διαιρεί το $x^t - 1$. Αυτό όμως είναι άτοπο αφού το $\Phi_n(x)$ είναι ανάγωγο, συνεπώς αν έχει μία κοινή ρίζα με το $x^t - 1$ τότε θα πρέπει το $\Phi_(x) \mid x^t - 1$ το οποίο δεν γίνεται από τον ορισμό του $\Phi_n(x)$. Μάλιστα το πολυώνυμο $x^n - 1$ έχει απλές ρίζες και το πολυώνυμο $\Phi_n(x)$ έχει ρίζες ακριβώς τάξης n.

Ο παραπάνω υπολογισμός μας επιτρέπει να υπολογίσουμε την ομάδα Galois της επέκτασης $\mathbb{Q}(\zeta_n)/\mathbb{Q}$.

4.6.4 Πρόταση:
Η ομάδα Galois της $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ δίνεται:

$$\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) = \left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^*.$$

Όπου για κάθε d με $(d, n) = 1$ και $1 \leqslant d \leqslant n - 1$

$$\sigma_d(\zeta) \mapsto \zeta_n^d.$$

Απόδειξη Πράγματι μόλις δείξαμε ότι το πολυώνυμο Φ_d έχει ως ρίζες τις πρωταρχικές ρίζες της μονάδας ζ_n^d. Αυτές είναι και οι δυνατότητες διαφορετικών αυτομορφισμών του σώματος $\mathbb{Q}(\zeta_n) \cong \mathbb{Q}[x]/\langle \Phi_n(x) \rangle$.

Οι ρίζες του $\Phi(n)$ είναι οι πρωταρχικές d ρίζες της μονάδας, δηλαδή οι γεννήτορες της ομάδας των n-οστών ριζών του 1. Μάλιστα αν ζ_n είναι μια πρωταρχική ρίζα της μονάδας, οποιαδήποτε άλλη πρωταρχική ρίζα της μονάδας θα είναι ρίζα του $\Phi_n(x)$, δηλαδή

$$\Phi_n(x) = \prod_{1 \leqslant k < n, (k,n)=1} (x - \zeta_n^k),$$

όπου $\zeta_n = e^{2\pi i/n}$.

4.6.5 Πρόταση:
Ο μέγιστος κοινός διαιρέτης των $\Phi_n(x)$ *και* $\Phi_m(x)$ *για* $n \neq m$ *δίνεται:*

$$(\Phi_m, \Phi_n) = 1.$$

Απόδειξη Έχουμε αποδείξει ότι

$$(x^m - 1, x^n - 1) = x^{(m,n)} - 1.$$

Από την άλλη, ας θεωρήσουμε έναν d κοινό διαιρέτη των n, m και ας υποθέσουμε ότι $m > n$. Είναι σαφές ότι ο $d \leqslant n < m$, συνεπώς ο d είναι γνήσιος διαιρέτης του m.

Από τον ορισμό του κυκλοτομικού πολυωνύμου προκείπτει ο τύπος:

$$\Phi_m(x) = \frac{x^m - 1}{\text{ΕΚΠ των } x^d - 1, 0 < d < m, d \mid m}$$

έχουμε ότι το $\Phi_m(x)$ διαιρεί το $\frac{x^m-1}{x^d-1}$, αφού ο παρονομαστής που ορίζει το $\Phi_m(x)$ έχει ίσως και άλλους διαιρέτες.

Επιπλέον αφού το $x^m - 1$ έχει απλές ρίζες, το $\Phi_n(x)$ δεν έχει κανέναν κοινό διαιρέτη με το $\Phi_m(x)$. Αυτό σημαίνει ότι $(\Phi_m, \Phi_n) = 1$.

4.6.6 Πρόταση:
Ισχύει

$$x^n - 1 = \prod_{d|n} \Phi_d(x).$$

Απόδειξη Αυτό είναι σαφές ως εξής: Όλες οι n-στές ρίζες της μονάδας μπορούν να χωριστούν ανάλογα με την τάξη τους σε ρίζες με τάξη ακριβώς d όπου το $d \mid n$.

Παρατήρηση Μία ενδιαφέρουσα συνέπεια του παραπάνω τύπου είναι ο αναδρομικός τύπος υπολογισμού πολυωνύμων Φ_n:

$$\Phi_n(x) = \frac{x^n - 1}{\prod_{d|n, d<n} \Phi_d(x)}$$

Παραδείγματα:

- Για p πρώτο το $\Phi(p)$ μπορεί να υπολογιστεί και με τη βοήθεια του παραπάνω τύπου

$$\Phi_p(x) = \frac{x^p - 1}{x - 1} = 1 + x + x^2 + \cdots + x^{p-1}$$

- Για $n = 2p$ έχουμε

$$\Phi_{2p}(x) = \frac{x^{2p} - 1}{\Phi_1(x)\Phi_2(x)\Phi_p(x)} = \frac{x^{2p} - 1}{\Phi_2(x)(x^p - 1)} = \frac{x^p + 1}{x + 1} =$$
$$= x^{p-1} - x^{p-2} + x^{p-3} - \cdots + x^2 - x + 1.$$

- Για $n = p^2$ όπου p πρώτος έχουμε

$$\Phi_{p^2}(x) = \frac{x^{p^2} - 1}{\Phi_1(x)\Phi_p(x)} = \frac{x^{p^2} - 1}{x^p - 1} =$$

$$= x^{p(p-1)} + x^{p(p-2)} + \cdots + x^p + 1.$$

- Γενικά μπορούμε με επαγωγή να δείξουμε ότι

$$\Phi_{p^e}(x) = \Phi_p(x^{p^{e-1}}) =$$
$$= x^{(p-1)p^{e-1}} + x^{(p-2)p^{e-1}} + \cdots + x^{2p^{e-1}} + x^{p^{e-1}} + 1.$$

Κάνοντας χρήση του sage μπορούμε να υπολογίσουμε κυκλοτομικά πολυώνυμα με τον αναδρομικό τύπο αλλά και με την ενσωματωμένη συνάρτηση:

```
sage:cyclotomic_polynomial(5,'x')
x^4 + x^3 + x^2 + x + 1
sage:prod(cyclotomic_polynomial(d,'x') for d in divisors(24))
x^24 - 1
cyclotomic_polynomial(3^10,'x')
x^39366 + x^19683 + 1
```

Μπορούμε να καταγράψουμε όλα τα κυκλοτομικά πολυώνυμα

```
sage:for i in range(1,10):
        cyclotomic_polynomial(i,'x')
x - 1
x + 1
x^2 + x + 1
x^2 + 1
x^4 + x^3 + x^2 + x + 1
x^2 - x + 1
x^6 + x^5 + x^4 + x^3 + x^2 + x + 1
x^4 + 1
x^6 + x^3 + 1
```

Interactive

Μπορεί εύκολα να πιστέψει κανείς ότι οι συντελεστές των κυκλοτομικών πολυωνύμων είναι ± 1. Αυτό δεν είναι όμως σωστό αφού το x^{41} έχει συντελεστή 2 στο $\Phi_{105}(x)$:

```
sage:cyclotomic_polynomial(105,'x')
x^48 + x^47 + x^46 - x^43 - x^42 -
2*x^41 - x^40 - x^39 + x^36 + x^35 +
x^34 + x^33 + x^32 + x^31 - x^28 -
x^26 - x^24 - x^22 - x^20 + x^17 +
x^16 + x^15 + x^14 + x^13 + x^12 -
x^9 - x^8 - 2*x^7 - x^6 - x^5 + x^2 +
x + 1
```

Interactive

Ο τύπος της αντιστροφής του Möbius μας επιτρέπει επίσης να γράψουμε

4.6.7 Θεώρημα:

$$\Phi_n(x) = \prod_{d|n}(x^d - 1)^{\mu(\frac{n}{d})}$$

Απόδειξη Έχουμε αποδείξει τον προσθετικό τύπο αντιστροφής

$$f(n) = \sum_{d|n} g(d) \Rightarrow g(n) = \sum_{d|n} \mu(d) f\left(\frac{n}{d}\right).$$

Με τον ίδιο ακριβώς τρόπο μπορούμε να αποδείξουμε μια πολλαπλασιαστική έκδοση

$$f(n) = \prod_{d|n} g(d) \Rightarrow g(n) = \prod_{d|n} f\left(\frac{n}{d}\right)^{\mu(d)}.$$

Θα μπορούσαμε να πάμε από την πολλαπλασιαστική στην εκθετική περίπτωση με χρήση εκθετικών-λογαρίθμων αλλά μπορούμε να δώσουμε και μία απευθείας απόδειξη:

$$\prod_{d|n} f(n/d)^{\mu(d)} = \prod_{d|n}\left(\prod_{t|\frac{n}{d}} g(t)\right)^{\mu(d)} = \prod_{t|n} g(t)^{\sum_{d|n,t}\frac{n}{d}\mu(d)} =$$

$$\prod_{t|n} g(t)^{\sum_{d|\frac{n}{t}}\mu(d)} = g(n)$$

Παρατήρηση Το $\Phi_n(x)$ είναι πηλίκο δύο μονικών πολυωνύμων με ακέραιους συντελεστές. Στον αριθμητή είναι οι παράγοντες με $\mu(n/d) = +1$ και στον παρονομαστή είναι οι παράγοντες με $\mu(n/d) = -1$.

Για παράδειγμα

$$\Phi_{18}(x) = \prod_{d|18}(x^d - 1)^{\mu(18/d)} = \frac{(x^{13} - 1)(x^{18-1})}{(x^6 - 1)(x^9 - 1)},$$

δηλαδή είναι πηλίκο δύο μονικών πολυωνύμων με ακέραιους συντελεστές βαθμών 21 ο αριθμητής και 15 ο παρονομαστής.

Για να διαπιστώσουμε ότι $\Phi_{18}(x) \in \mathbb{Z}[x]$ μπορούμε να κάνουμε τη διαίρεση ή να επιχειρηματολογήσουμε κατά Berlekamp:

Το $\Phi_{18}(x)$ είναι πολυώνυμο βαθμού $\phi(18) = \phi(2)\phi(3^2) = 6$. Αν πάρουμε ένα πολυώνυμο modulo x^7, επειδή το $\deg\Phi_{18}(x) = 6 < 7$ δεν χάνουμε τίποτα. Υπολογίζουμε λοιπόν:

$$\Phi_{18}(x) = \frac{(x^3 - 1)(-1)}{(x^6 - 1)(-1)} = \frac{1 - x^3}{1 - x^6} \text{ modulo } x^7$$

Στη συνέχεια υπολογίζουμε

$$\frac{1-x^3}{1-x^6} = \frac{(1-x^3)(1+x^6)}{(1-x^6)(1+x^6)} = \frac{(1-x^3)(1+x^6)}{1-x^{12}}.$$

Όμως $1-x^{12} \equiv 1 \mathrm{mod} x^7$. Επομένως

$$\phi_{18}(x) = (1-x^3)(1+x^6) = 1-x^3+x^6 \bmod x^7$$

και τελικά

$$\Phi_{18}(x) = x^6 - x^3 + 1.$$

Ως μία εφαρμογή ας αποδείξουμε μια ειδική περίπτωση του θεωρήματος του Dirichlet σχεικά με την απειρία των πρώτων αριθμών που εμφανίζονται σε αριθμητικές προόδους:

4.6.8 Θεώρημα:
Υπάρχουν άπειροι πρώτοι της μορφής $p \equiv 1 mod n$.

Απόδειξη Το κυκλοτομικό πολυώνυμο $\Phi_n(x)$ είναι ένα μη σταθερό μονικό πολυώνυμο στον δακτύλιο $\mathbb{Z}[x]$ και έχει σταθερό συντελεστή ± 1.

Ας υποθέσουμε ότι υπήρχαν πεπερασμένοι το πλήθος πρώτοι $p_1, \ldots, p_t$ ισοδύναμοι με $1 \mathrm{mod} n$. Τότε, για αρκετά μεγάλο ακέραιο ℓ θα είχαμε

$$N = \Phi_n(\ell n p_1 \cdots p_t) \geqslant 1$$

και προφανώς ο N είναι ακέραιος. Συνεπώς για κάθε p_i θα είχαμε

$$N \equiv \pm 1 \mathrm{mod} p_i,$$

αφού μόνο ο σταθερός όρος επιβιώνει $\mathrm{mod} p_i$. Άρα για όλα τα p_i, p_i δεν διαιρεί το N. Ο αριθμός N όμως έχει πρώτους παράγοντες και έστω p ένας από αυτούς. Αφού δε $N = \pm 1 \mathrm{mod} n$ έχουμε $(N, p) = 1$. Έχουμε ότι

$$\Phi_n(\ell n p_1 \cdots p_t) = N \equiv 0 \mathrm{mod}\, p$$

συνεπώς το $\ell n p_1 \cdots p_t$ έχει τάξη n στην ομάδα $U(\mathbb{F}_p)$ η οποία έχει τάξη $p-1$, άρα $n \mid p-1$, άτοπο.

4.6.2. Κυκλοτομικά σώματα αριθμών. Αυτά είναι σώματα της μορφής $\mathbb{Q}(\zeta_n) = \mathbb{Q}[x]/\Phi_n(x)$ και είναι ιδιαίτερα σημαντικά στην αλγεβρική θεωρία των αριθμών.

Ας δούμε δύο κλασικές εφαρμογές των παραπάνω σωμάτων που μπορεί να γίνουν εύκολα κατανοητές

4.6.2.1. *Τα κανονικά πολύγωνα.* Ο Gauss απέδειξε ότι ένα κανονικό πολύγωνο με 17 πλευρές είναι δυνατόν να κατασκευαστεί με κανόνα και διαβήτη. Γενικότερα ισχύει ότι ένα κανονικό p-γωνο μπορεί να κατασκευαστεί με κανόνα και διαβήτη αν το $\phi(p) = p-1$ είναι δύναμη του 2 ή με άλλα λόγια αν ο p είναι ένας πρώτος αριθμός του Fermat. Προφανώς ο 17 είναι ένας πρώτος αριθμός του Fermat, αφού $\phi(17) = 16 = 2^4$.

Είναι σαφές ότι με κανόνα και διαβήτη μπορούμε να υπολογίσουμε σημεία τα οποία βρίσκονται στην τομή δύο τετραγωνικών καμπυλών άρα οι συντεταγμένες τους είναι σε τετραγωνικές επεκτάσεις σωμάτων που έχουν ήδη συντεταγμένες σε τετραγωνικές επεκτάσεις του σώματος των ρητών αριθμών.

Το ερώτημα λοιπόν ανάγεται στο εξής: Μπορεί το n-κυκλοτομικό σώμα να κατασκευαστεί ως μια ακολουθία τετραγωνικών επεκτάσεων; Με άλλα λόγια θα πρέπει να χαρακτηρήσουμε τους πρώτους αριθμούς για τους οποίους $\phi(p) = p-1$ είναι δύναμη του 2.

Γενικότερα μπορεί να αποδειχτεί ότι το $\phi(n)$ είναι δύναμη του 2 αν και μόνο αν είναι της μορφής $2^k p_1 p_2 \cdots p_r$ όπου $k \geqslant 0$ και τα p_j είναι διαφορετικοί πρώτοι του Fermat δηλαδή πρώτοι της μορφής $2^s + 1$.

4.6.2.2. *Το τελευταίο θεώρημα του Fermat.* Δεν χρειάζεται να πούμε πολλά για αυτό το πασίγνωστο πρόβλημα. Είναι σαφές ότι τα γινόμενα συμπεριφέρονται καλύτερα από τα αθροίσματα αφού έχουμε μοναδικότητα στην ανάλυση σε πρώτους αλλά δεν υπάρχει ανάλογο αποτέλεσμα για τα αθροίσματα.

Στην προσπάθειά μας να μελετήσουμε τις ακέραιες λύσεις της εξίσωσης

$$x^n + y^n = z^n$$

μια φυσιολογική ιδέα είναι να διασπάσουμε το αρχικό άθροισμα δυνάμεων ως

$$x^n + y^n = (x + y)(x + \zeta y) \cdots (x + \zeta^{n-1} y).$$

Η παραπάνω διάσπαση δεν μπορεί να γίνει στον δακτύλιο των ακέραιων, μπορεί όμως να γίνει στον δακτύλιο των $\mathbb{Z}[\zeta]$, ο οποίος είναι ένας υποδακτύλιος του κυκλοτομικού σώματος $\mathbb{Q}(\zeta)$, ο οποίος παίζει για το σώμα $\mathbb{Q}(\zeta)$ τον ρόλο που παίζει για το σώμα $\mathbb{Q}$ ο δακτύλιος $\mathbb{Z}$.

Πολλές αποδείξεις του τελευταίου θεωρήματος του Fermat δόθηκαν, ήταν όμως εσφαλμένες, διότι ο δακτύλιος $\mathbb{Z}$ δεν υπάρχει μονοσήμαντη ανάλυση σε αδιάσπαστα στοιχεία. Αυτή ήταν η αρχή της αλγεβρικής Θεωρίας αριθμών η οποία κατάφερε να μετρήσει τη μη μονοσήμαντη ανάλυση μέσω της ομάδας κλάσεων Cl_n. Έτσι μπορεί πράγματι να δώσει κανείς μια απόδειξη του τελευταίου θεωρήματος του Fermat για όλους τους πρώτους ώστε p δεν διαιρεί το $|Cl_n|$.

Η πλήρης απόδειξη χρειαζόταν μία νέα ιδέα -αυτή των ελλειπτικών καμπυλών- και θα πούμε περισσότερα σε επόμενο κεφάλαιο.

4.6.3. Κυκλοτομικά πολυώνυμα. Τα κυκλοτομικά πολυώνυμα είναι ανάγωγα πολυώνυμα στο $\mathbb{Z}[x]$. Αυτό δεν είναι σωστό πάνω από πεπερασμένα σώματα. Για παράδειγμα:

$$\Phi_4(x) = x^2 + 1 = \begin{cases} (x+1)^2 & \text{στο } \mathbb{F}_2 \\ \text{αναγωγο} & \text{στο } \mathbb{F}_3 \\ (x+1)^2 & \text{στο } \mathbb{F}_4 \\ (x-2)(x-3) & \text{στο } \mathbb{F}_5 \end{cases}$$

Ισχύει το

4.6.9 Θεώρημα:
Αν p πρώτος p δεν διαιρεί το n τότε για $k \geqslant 1$ ισχύουν

1. $\Phi_{np^k}(x) = \Phi_{np}(x^{p^{k-1}})$ *για σώματα κάθε χαρακτηριστικής*
2. $\Phi_{np^k} = \frac{\Phi_n(x^{p^k})}{\Phi_n(x^{p^{k-1}})}$ *για σώματα κάθε χαρακτηριστικής*
3. $\Phi_{np^k}(x) = \Phi_n(x)^{p^k - p^{k-1}}$ *μόνο σε σώματα χαρακτηριστικής* p, $(n, p) = 1$.

Απόδειξη Χωρίς απόδειξη.
Παραδείγματα

$$\Phi_{72}(x) = \Phi_{8\cdot 3^2}(x) = \Phi_{8\cdot 3}(x^3) = \Phi_{3\cdot 2}\left((x^3)^{2^{3-1}}\right) = \Phi_6(x^{12}) =$$

$$(x^{12})^2 - x^{12} + 1 = x^{24} - x^{12} + 1.$$

Επίσης

$$\Phi_{72}(x) = \frac{\Phi_8(x^9)}{\Phi_8(x^3)} = \frac{x^{36+1}}{x^{12}+1} = x^{24} - x^{12} + 1.$$

Σε σώμα χαρακτηριστικής 3 ισχύει

$$\Phi_{72}(x) = \Phi_8(x)^{3^2-3} = \big(\Phi_8(x)\big)^6 =$$

$$(x^4+1)^6 = \big((x^4+1)^3\big)^2 = x^{24} - x^{12} + 1.$$

Έστω λοιπόν $\mathbb{F}_q$ πεπερασμένο σώμα τάξης $q = p^l$ με $(p, n) = 1$. Υπάρχει φυσικός αριθμός λ με την ιδιότητα

$$q^\lambda \equiv 1 \bmod p$$

Ας είναι m ο ελάχιστος αριθμός με αυτή την ιδιότητα, δηλαδή η τάξη του q στην $\mathbb{F}_p^*$. Ας θεωρήσουμε το σώμα $\mathbb{F}_{q^m}$ με q^m στοιχεία.

Επειδή $n \mid q^m - 1$ από προηγούμενο θεώρημα έχουμε ότι υπάρχει $a \in \mathbb{F}_{q^m}$, ώστε $\mathrm{ord}(a) = n$. Έχουμε

$$\Phi_d(x) = \prod_{0 \leqslant j < h-1 \mathrm{ord}(a^j) = d} = \prod_{\mathrm{ord}(b)} (x - b),$$

και

$$\Phi_n(x) = \prod_{d \mid n} (x^d - 1)^{\mu(n/d)}$$

Αυτό σημαίνει ότι το $\Phi_d(x)$ αναλύεται στο «μεγάλο» σώμα $\mathbb{F}_{q^m}$ σε γινόμενο γραμμικών παραγόντων.

Τι γίνεται στο μικρό σώμα $\mathbb{F}_q$; Το ελάχιστο πολυώνυμο του a έχει ρίζες

$$a, a^q, \ldots, a^{q^{d-1}}.$$

Δηλαδή υπάρχουν ακριβώς d-συζυγή του a στο σώμα $\mathbb{F}_q$, όπου d ο ελάχιστος φυσικός τέτοιος ώστε $q^d \equiv 1 \bmod n$. Αλλά αυτό εμείς το ορίσαμε και το είπαμε m. Επομένως το $\Phi_n(x)$ έχει έναν ανάγωγο παράγοντα βαθμού m.

Ποια είναι τα ανάγωγα πολυώνυμα των άλλων ριζών του $\Phi_n(x)$;

Εξ ορισμού όλα έχουν βαθμό $d = m$. Με το ίδιο επιχείρημα όπως και προηγουμένως έπεται ότι υπάρχουν ακριβώς $d = m$ συζυγή.

4.6.10 Θεώρημα:
Αν p πρώτος, p δεν διαιρεί το n και $q = p^l$ τότε το $\Phi_n(x)$ στο $\mathbb{F}_q = K$ αναλύεται σε γινόμενο ανάγωγων πολυωνύμων, βαθμού m, όπου m ο ελάχιστος φυσικός με την ιδιότητα

$$q^m \equiv 1 mod n.$$

Παράδειγμα Το $\Phi_7(x)$ υπέρ του $\mathbb{F}_2 = K$. Έχουμε ότι $\phi(7) = 6$. Θα πρέπει να βρούμε το m για $q = 2$ και $n = 7$. Δηλαδή τον ελάχιστο φυσικό τέτοιο ώστε $2^m \equiv 1 \bmod 7$. Οπότε $m = 3$. Επομένως το $\Phi_7(x)$ αναλύεται στο $\mathbb{F}_2$ σε γινόμενο $6/3 = 2$ ανάγωγων (κυκλικών) πολυωνύμων βαθμού 3 το καθένα.

Ας κάνουμε τον υπολογισμό στο sage:

```
sage:Phi=cyclotomic_polynomial(7,'x');Phi
x^6 + x^5 + x^4 + x^3 + x^2 + x + 1
```

```
sage:Phi.is_irreducible()
True
sage:R.<t> = PolynomialRing(FiniteField(2));R
Univariate Polynomial Ring in t over Finite Field of
size 2 (using NTL)
sage:ff = ZZ[x].hom([t]); ff
Ring morphism:
  From: Univariate Polynomial Ring in x over Integer Ring
  To:   Univariate Polynomial Ring in t over Finite Field
  of size 2 (using NTL)
  Defn: x |--> t
sage:factor(ff(Phi))
(t^3 + t + 1) * (t^3 + t^2 + 1)
```

Interactive

Πρώτα κατασκευάσαμε το $\Phi_7(x)$ και ελέγξαμε ότι είναι ανάγωγο. Στη συνέχεια κατασκευάσαμε τον δακτύλιο των πολυωνύμων $R = \mathbb{F}_2[t]$ και τον ομομρφισμό $\mathbb{Z}[x] \to \mathbb{F}_2[t]$ ο οποίος λαμβάνει τους συντελεστές modulo 2. Τέλος παραγοντοποιήσαμε την εικόνα του $\Phi_7(x)$ modulo 2.

Συνεχίζουμε τη θεωρητική προσέγγιση στο ίδιο παράδειγμα. Αν α οποιοδήποτε στοιχείο τάξης 7 στο $F = \mathbb{F}_{2^3}$, οι ανάγωγοι παράγωντες του $\Phi_7(x)$ στο $= \mathbb{F}_2$ θα είναι

$$f_1(x) = (x-\alpha)(x-\alpha^2)(x-\alpha^4)$$

$$f_3(x) = (x-\alpha^3)(x-\alpha^6)(x-\alpha^5)$$

Το $\mathbb{F}_{2^3} \cong \mathbb{F}_2[x]/\langle f(x)\rangle$, όπου $f(x)$ ανάγωγο μονικό πολυώνυμο του $\mathbb{F}_2[x]$. Ένα τέτοιο πολυώνυμο είναι το x^3+x+1, επομένως αν για α πάρουμε μια ρίζα του x^3+x+1 θα έχουμε $\alpha^3+\alpha+1=0$. Οπότε $\alpha^3 = -(\alpha+1)$ ή $\alpha^3 = \alpha+1$. Με αυτόν τον τρόπο καταλήγουμε ότι

$$f_1(x) = x^3+x+1 \text{ και } f_3(x) = x^3+x^2+1.$$

Παράδειγμα Να παραγοντοποιήσουμε το $\Phi_{180}(x)$ στο $\mathbb{F}_3$. Έχουμε ότι $180 = 2^2\cdot 3^2\cdot 5$. Επομένως

$$\Phi_{180}(x) = \Phi_{20}(x)^{9-3} = \Phi_{20}(x)^6.$$

Συνεπώς θα πρέπει να παραγοντοποιήσουμε το κυκλοτομικό πολυώνυμο $\Phi_{20}(x)$ στο $\mathbb{F}_3$. Επειδή $3^4 \equiv 1 \bmod 20$ έχουμε ότι $m = 4$ και $n = 20$ με $\phi(n) = \phi(20) = 8$. Άρα το $\phi_{20}(x)$ είναι ίσο με το γινόμενο $8/4 = 2$ αναγώγων πολυωνύμων βαθμού 4 το καθένα. Οπότε, αν α στοιχείο τάξης 20 στο $\mathbb{F}_{3^4}$ τότε οι δυο παράγοντες του $\Phi 20(x)$ είναι:

$$f_1(x) = (x-\alpha)(x-\alpha^3)(x-\alpha^9)(x-\alpha^7)$$

$$f_2(x) = (x-\alpha^{11})(x-\alpha^{13})(x-\alpha^{19})(x-\alpha^{17})$$

Αν πάλι έχουμε στο $\mathbb{F}_{3^4}$ ότι και α ρίζα του $q(X)$ μπορούμε να υπολογίσουμε επακριβώς τα $f_1(x)$ και $f_2(x)$.

Ας πάμε με ωμή βία να κάνουμε τον ίδιο υπολογισμό στο sage:

```
sage:Phi=cyclotomic_polynomial(180,'x');Phi
x^48 + x^42 - x^30 - x^24 - x^18 + x^6 + 1
sage:Phi.is_irreducible()
True
sage:R.<t> = PolynomialRing(FiniteField(3));R
Univariate Polynomial Ring in t over Finite Field of size 3
sage:ff = ZZ[x].hom([t]); ff
Ring morphism:
  From: Univariate Polynomial Ring in x over Integer Ring
  To:   Univariate Polynomial Ring in t over Finite Field
                                                of size 3
  Defn: x |--> t
sage:factor(ff(Phi))
(t^4 + t^3 + 2*t + 1)^6 * (t^4 + 2*t^3 + t + 1)^6
```

Interactive

Θα προσπαθήσουμε να ανακαλύψουμε τεχνικές που μας επιτρέπουν να βρούμε τους ανάγωγους παράγοντες του κυκλοτομικού πολυωνύμου $\Phi_n(x)$ στο $\mathbb{F}_q$ επακριβώς. Ως πρώτο βήμα θα προσπαθήσουμε να βρούμε κριτήρια για το πότε το $\Phi_n(x)$ είναι ανάγωγο.

Έχουμε αποδείξει ότι

$\Phi_n(x)$ ανάγωγο στο $\mathbb{F}_q$ αν και μόνο αν $\left\{ \begin{array}{c} q^{\phi(n)} \equiv 1 \mathrm{mod} n \\ q^k \neq 1 \mathrm{mod} n \text{ για κάθε } k < \phi(n) \end{array} \right\}$

Η παραπάνω εξίσωση μας λέει ότι η ομάδα των πρώτων κλάσεων υπολοίπων mod n, η οποία έχει τάξη $\phi(n)$, είναι κυκλική και έχει το q ως γεννήτορα. Δηλαδή ότι το q είναι πρωταρχική ρίζα modulo n.

Από τη Θεωρία Αριθμών όμως γνωρίζουμε ότι οι μοναδικές τιμές του n για τις οποίες υπάρχει πρωταρχική ρίζα mod n είναι $n = 1, 2, 4, p^s, 2p^s$, $s \in \mathbb{N}$ και p πρώτος, $p \neq 2$.

Επομένως, αν το n δεν είναι της παραπάνω μορφής, τότε $\Phi_n(x)$ όχι ανάγωγο στο $\mathbb{F}_q$. Απ' την άλλη μεριά, αν το n είναι τέτοιας μορφής, τότε

$$\Phi_n(x) \text{ ανάγωγο στο } \mathbb{F}_q \Leftrightarrow \text{ το } q \text{ είναι πρωταρχική ρίζα mod } n.$$

Παράδειγμα Έστω $n = 7$. Τότε $(7) = 6$. Παίρνουμε τους πρώτους ως προς 7 modulo 7: $1, 2, 3, 4, 5, 6 (\mathrm{mod} 7)$ $2^3 \equiv 1 \mathrm{mod} 7$ συνεπώς $\mathrm{ord}_7(2) = 3$. Επομένως, το 2 δεν είναι πρωταρχική ρίζα mod 7.

$3^1 \equiv 3 \mathrm{mod} 7$, $3^2 \equiv 2 \mathrm{mod} 7$), $3^3 \equiv 6 \mathrm{mod} 7$ συναπώς $\mathrm{ord}_7(3) = 6$. Το 3 είναι πρωταρχική ρίζα mod 7. Οι άλλες πρωταρχικές ρίζες προκύπτουν από τις δυνάμεις του 3^d με $1 \leqslant d < 6$ $(d, 6) = 1$, δηλαδή η μοναδική άλλη πρωταρχική ρίζα είναι το $3^5 \equiv 5 \mathrm{mod} 7$

Άρα, $\Phi_7(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$ είναι ανάγωγο στο σώμα $\mathbb{F}_q$ αν και μόνο αν

$$q \equiv 3 \mathrm{mod} 7 \text{ ή } q \equiv 5 \mathrm{mod} 7.$$

Για παράδειγμα για $q = 3, 5, 17, 19, \ldots$ το $\Phi_7(x)$ είναι ανάγωγο στο $\mathbb{F}_q$.

Ας πάρουμε τώρα $n = 8$ (αναμένουμε να μην έχει πρωταρχικές ρίζες). Έχουμε ότι $\phi(8) = 4$. Οι πρώτες κλάσεις mod 8 είναι: $1, 3, -3 = 5, 7$. $7^2 \equiv (-3)^2 \equiv 3^2 \equiv 1 \mathrm{mod} 8$ και ομοίως $(\pm 1)^2 \equiv 1 \mathrm{mod} 8$, δηλαδή όλα τα στοιχεία έχουν τάξη 2.

Αυτό σημαίνει ότι το πολυώνυμο $\Phi_8(x) = x^4 + 1$ δεν είναι ποτέ ανάγωγο στο $\mathbb{F}_p$ για κάθε πρώτο p. Αντιθέτως το $\Phi_8(x)$ είναι ανάγωγο στο $\mathbb{Z}$.

Πιο γενικά: Αν $f(x)$ οποιοδήποτε πολυώνυμο του $\mathbb{F}_q[x]$ θα περιγράψουμε αλγόριθμο (του Berlekamp) παραγοντοποίησης του $f(x)$ σε γινόμενο ανάγωγων παραγόντων.

4.6.11 Θεώρημα:
Αν $f(x)$ μονικό πολυώνυμο με $deg f(x) = n$ όπου $f(x) \in \mathbb{F}_q$ και αν $h(x) \in \mathbb{F}_q[x]$, τέτοιο ώστε

$$h(x)^q \equiv h(X) mod f(X)$$

τότε

$$f(x) = \prod_{s \in \mathbb{F}_q} (f(x), h(x) - s).$$

(χωρίς απόδειξη)

Παρατήρηση Αν υπάρχει $s_0 \in \mathbb{F}_q$ τέτοιο ώστε

$$h(X) \equiv s_0 \mathrm{mod} f(x),$$

τότε η παραγοντοποίηση του προηγούμενου θεωρήματος είναι τετριμμένη. Δηλαδή ένας παράγοντας είναι το $f(x)$ και οι άλλοι είναι 1.

Το επόμενο θεώρημα θα μας δώσει ότι αν $f(x)$ διαιρείται από δυο ή περισσότερα διακεκριμένα ανάγωγα πολυώνυμα τότε υπάρχει πολυώνυμο $h(x)$ τέτοιο ώστε η παραγοντοποίηση του προηγούμενου θεωρήματος να μην είναι τετριμμένη.

Θεωρούμε τον δακτύλιο

$$V(f) := \mathbb{F}_q[x]/\langle f(x) \rangle$$

σαν n-διάστατο $\mathbb{F}_q$-διανυσματικό χώρο, όπου $n = \deg f$, με βάση τα $\{1, x, x^2, \ldots, x^n - 1\}$. Έστω

$$R(f) = \{h(x) \in \mathbb{F}_q[x] \text{ ώστε } h(x)^q \equiv h(x) \mathrm{mod} f(x)\}.$$

Το $R(f)$ είναι διανυσματικός υπόχωρος του $V(f)$ διότι

$$\left(s_1 h_1(x) + s_2 h_2(x)\right)^q = s_1^q + h_1(x)^q + s_2^q h_2(x)^q$$

$$= s_1 h_1(x) + s_2(x) h_2(x) \text{ mod } f(x).$$

4.6.12 Θεώρημα:
Αν

$$f(x) = \prod_{i=1}^{m} P_i(x)^{\ell_i},$$

όπου $P_i(x)$ διακεκριμένα ανά δύο ανάγωγα μονικά πολυώνυμα, τότε $dim_{\mathbb{F}_q} R(f) = m$.

(χωρίς απόδειξη)

Παρατήρηση: Αν καταφέρουμε να υπολογίσουμε τη διάσταση του χώρου m, τότε γνωρίζουμε το πλήθος των ανάγωγων παραγόντων του $f(x)$ (Θα είναι m).

Παράδειγμα Έστω

$$f(x) = x^4 + x + 1$$

και $q = 2$ τότε $\mathbb{F}_2$. Αν

$$h(x) = h_0 + h_1 x + h_2 x^2 + h_3 x^3$$

τότε η συνθήκη

$$h(x)^q \equiv h(x) \bmod f(x)$$

γράφεται

$$h_0 + h_1 x^2 + h_2 x^4 + h_3 x^6 \equiv h_0 + h_1 x + h_2 x^2 + h_3 x^3 \bmod (x^4 + x + 1).$$

Ισχύει ότι

$$x^4 \equiv x + 1 \bmod (x^4 + x + 1)$$

οπότε και

$$x^6 \equiv x^3 + x^2 \bmod (x^4 + x + 1)$$

και έχουμε ότι

$$h(X)^2 = h_0 + h_1 x^2 + h_2(x + 1) + h_3(x^3 + x^2) \bmod (x^4 + x + 1).$$

Οπότε αν παραστήσουμε το πολυώνυμο

$$h(x) = h_0 + h_1 x + h_2 x^2 + h_3 x^3$$

με το διάνυσμα στήλη $(h_0, h_1, h_2, h_3)^t$, τότε

$$h(X) \in R(f) \Leftrightarrow h(X)^2 \equiv h(X) \bmod f(X)$$

ή ισοδύναμα

$$h_0 \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} + h_1 \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} + h_2 \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \end{pmatrix} + h_3 \begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \end{pmatrix} = h_0 \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} + h_1 \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} + h_2 \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} + h_3 \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

Δηλαδή το $h(X) \in R(f)$ ισοδυναμεί με το ότι το διάνυσμα $(h_0, h_1, h_2, h_3)^t$ ανήκει στον χώρο μηδενισμού του πίνακα B, όπου

$$B = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix} - Id = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

Κάνοντας στοιχειώδεις μετασχηματισμούς στον πίνακα B, συγκεκριμένα προσθέτοντας στη γραμμή 2 τη γραμμή 1 και στη γραμμή 3 τη γραμμή 2 φέρνουμε τον B στη μορφή:

$$B = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

Παρατηρούμε ότι $(h_0, h_1, h_2, h_3) \in R(f) \Leftrightarrow h_1 = h_2 = h_3 = 0$. Συνεπώς η διάσταση του παραπάνω χώρου $\dim(R(f)) = 1$ και το $f(x)$ είναι δύναμη αναγώγου. Όμως $f'(x) = 4x^3 + 1 = 1$. Άρα έχει απλές ρίζες και το f είναι ανάγωγο.

Παράδειγμα Έστω ότι θέλουμε να παραγοντοποιήσουμε το

$$f(x) = x^5 + x + 1$$

στο $\mathbb{F}_2$ Αν

$$h(x) = h_0 + h_1 x + h_2 x^2 + h_3 x^3 + h_4 x^4$$

τότε θέλουμε να έχουμε

$$h(x)^2 \equiv h(x) \mathrm{mod}(x^5 + x + 1).$$

Θα χρησιμοποιήσουμε τις ισοτιμίες: $x^5 \equiv x + 1 \mathrm{mod}\ (x^5 + x + 1)$, $x^6 \equiv x^2 + x \mathrm{mod}\ (x^5 + x + 1)$ και $x^8 \equiv x^4 + x^3 \mathrm{mod}\ (x^5 + x + 1)$. Η ισοδυναμία

$$h(x)^2 \equiv h(X) \mathrm{mod}\ f(x)$$

γράφεται ισοδύναμα στο σύστημα

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 \end{pmatrix} \begin{pmatrix} h_0 \\ h_1 \\ h_2 \\ h_3 \\ h_4 \end{pmatrix} = \mathrm{Id} \begin{pmatrix} h_0 \\ h_1 \\ h_2 \\ h_3 \\ h_4 \end{pmatrix},$$

δηλαδή στον ιδιοχώρο της ιδιοτιμής 1. Υπολογίζουμε ότι η διάσταση του ιδιοχώρου αυτού είναι 2 και μία βάση του $R(f)$ είναι τα $1, x + x^3 + x^4$.

Επομένως το $f(x)$ είναι γινόμενο δύο αναγώγων πολυωνύμων πιθανόν σε κάποια δύναμη το καθένα.

Υπολογίζουμε κατά τα γνωστά τους μέγιστους κοινούς διαιρέτες

$$(x^5 + x + 1, x^4 + x^3 + x) = x^3 + x^2 + 1$$

$$(x^5 + x + 1, x^4 + x^3 + x + 1) = x^2 + x + 1$$

Επομένως,

$$x^5 + x + 1 = (x^3 + x^2 + 1)(x^2 + x + 1).$$

Γνωρίζουμε ότι $x^3 + x^2 + x$ και $x^2 + x + 1$ ανάγωγα στο $\mathbb{F}_2$. Άρα η ανάλυση του $f(x)$ σε γινόμενο ανάγωγων πολυωνύμων είναι

$$f(x) = x^5 + x + 1 = (x^3 + x^2 + 1)(x^2 + x + 1).$$

Ο αλγόριθμος του Berlekamp μπορεί να απλοποιηθεί σημαντικά αν το πολυώνυμο που θέλουμε να παραγοντοποιήσουμε είναι της μορφής x^n–1 όπου $(n, q) = 1$.

4.6.13 Θεώρημα:
Το πολυώνυμο

$$h(x) = \sum_{i=0}^{n-1} h_i x^i$$

επαληθεύει την ισοδυναμία

$$h(x)^q \equiv h(x) mod\ (x^n - 1)$$

αν και μόνο αν

$$h_{iq} = h_i \text{ για κάθε } i = 0, 1, 2, \ldots, n-1$$

(όπου οι δείκτες θεωρούνται modulo n*).*

(χωρίς απόδειξη)

Παρατήρηση: Επειδή $(n, q) = 1$, η απεικόνιση $i \mapsto qi \bmod n$ είναι μια μετάθεση του συνόλου $\{0, 1, 2, \ldots, n-1\}$.

Παράδειγμα: Για $q = 2$ και $n = 5$ έχουμε ότι

$$\{0, 1, 2, 3, 4\} \mapsto \{0, 2, 4, 6, 8\} \equiv \{0, 2, 4, 1, 3\} \bmod 5.$$

Δηλαδή έχουμε τη μετάθεση:

$$\begin{pmatrix} 0 & 1 & 2 & 3 & 4 \\ 0 & 2 & 4 & 1 & 3 \end{pmatrix}$$

Παράδειγμα: Για $q = 3$ και $n = 20$ η μετάθεση που θα προκύψει σε γινόμενο κύκλων γράφεται:

$$(0)(1397)(261814)(412168)(515)(10)(11131917).$$

Συνεπώς κάθε πολυώνυμο $h(x)$ που επαληθεύει την ισοδυναμία

$$h(x)^3 \equiv h(x) \bmod x^{20} - 1$$

θα πρέπει να είναι $\mathbb{F}_3$-γραμμικός συνδυασμός των ακολούθων 7 πολυωνύμων:

$$h_0 = 1$$
$$h1(x) = x + x^3 + x^9 + x^7$$
$$h2(x) = x^2 + x^6 + x^{18} + x^{14}$$
$$h_4(x) = x^4 + x^12 + x^16 + x^8$$
$$h_5(x) = x^5 + x^{15}$$
$$h_10(x) = x^{10}$$
$$h_{11}(x) = x^{11} + x^{13} + x^{19} + x^{17}$$

Οι κύκλοι των μεταθέσεων $i \to qi \bmod n$ λέγονται κυκλοτομικά cosets.

Μελετάμε το πολυώνυμο $f(x) = x^{20}–1$ στο σώμα $\mathbb{F}_3$. Η τάξη του 3 modulo 20 είναι 4 αφού $3^4 \equiv 1 \bmod 20$. Επομένως, αν περάσουμε στο σώμα $\mathbb{F}_{3^4}$ τότε αυτό θα έχει ένα στοιχείο τάξης 20, δηλαδή

$$x^{20}–1 = \prod_{j=0}^{19} (x - a^j),$$

όπου a ένα στοιχείο τάξης 20 του $\mathbb{F}_{3^4}$.

Έχουμε ήδη δει ότι η παραγοντοποίηση του $x^{20}–1$ στο $\mathbb{F}_3$ καθορίζεται από την παραγοντοποίηση του $x^{20}–1$ στο $\mathbb{F}_{3^4}$. Έστω για παράδειγμα ότι το ελάχιστο πολυώνυμο του a στο σώμα $\mathbb{F}_3$ είναι το

$$f_1(x) = (x–a)(x–a^3)(x–a^9)(x–a^7)$$

Επειδή για κάθε $i = 1, 3, 7, 9$ έχουμε ότι $(i, 20) = 1$, έπεται ότι τα στοιχεία a^i για κάθε $i = 1, 3, 7, 9$ είναι επίσης τάξης 20. Επομένως το $f_1(x)$ είναι ανάγωγος παράγοντας, όχι μόνο του $x^{20}–1$ αλλά και του $\Phi_{20}(x)$. Ομοίως αν $f_i(x)$ είναι το ελάχιστο πολυώνυμο του a_i, τότε το $f_i(x)$ είναι και ανάγωγο πολυώνυμο του $\Phi_{n/(n,i)}(x)$. Αν τώρα συμβολίσουμε το κυκλοτομικό coset που περιέχει το i με Ci φτιάχνουμε τον ακόλουθο πίνακα:

Πίνακας 4.2: Πίνακας Κυκλοτομικών cosets

i	C_i	$\lvert C_i\rvert = \deg f_i(x)$	$\frac{20}{(20,i)}$
0	0	1	1
1	(1, 3, 9, 7)	4	20
2	(2, 6, 18, 14)	4	10
4	(4, 12, 16, 8)	4	5
5	(5, 15)	2	4
10	(10)	1	2
11	(11, 13, 19, 17)	4	20

Με τη βοήθεια του παραπάνω πίνακα μπορούμε να φτιάξουμε τον πίνακα των παραγόντων του x^{20}–1 οι οποίοι δίνονται μέσω τον κυκλοτομικών πολυωνύμων $\Phi_d(x)$, όπου $d \mid 20$.

Πίνακας 4.3: Παράγοντες του $x^{20} - 1$.

d	$\Phi_d(x)$	παράγοντες
1	x–1	$f_1(x)$ ανάγωγο
2	$x + 1$	$f_{10}(x) = x$–a^{10} ανάγωγο
4	$x^2 + 1$	$f_5(x)$ ανάγωγο
5	$x^4 + x^3 + x^2 + x + 1$	$f_4(x)$ ανάγωγο
10	x^4–$x^3 + x^2$–$x + 1$	$f_2(x)$ ανάγωγο
20	x^8–$x^6 + x^4$–$x^2 + 1$	$f_1(x)f_{11}(x)$

Μόνο το $\Phi_{20}(x)$ δεν παραγοντοποιείται πλήρως σε γινόμενο αναγώγων για αυτό εφαρμόζουμε και πάλι τον αλγόριθμο του Berlekamp. Για κάθε $h_i(x)$ ισχύει:

$$x^{20}\text{–}1 = (x^{20}\text{–}1, h_i(x))(x^{20}\text{–}1, h_i(x) + 1)(x^{20}\text{–}1, h_i(x) + 2)$$

Επειδή $\Phi_{20}(x) | x^{20}\text{–}1$ έπεται ότι

$$h^3(x) \equiv h(x) \mathrm{mod} \Phi_{20}(x).$$

Οπότε,

$$\Phi_{20}(x) = (\Phi_{20}(x), h_i(x))(\Phi_{20}(x), h_i(x) + 1)(\Phi_{20}(x), h_i(x) + 2) =$$
$$| = (x^4 + x^3 + 2X + 1)(x^4 + 2x^3 + x + 1).$$

Έτσι παραγοντοποιήσαμε πλήρως το x^{20}–1 σε γινόμενο αναγώγων πολυωνύμων. Στο sage η παραπάνω κατασκευή θα μπορούσε να γίνει ως:

```
sage:Phi20=cyclotomic_polynomial(20,'x');Phi20
sage:R.<t> = PolynomialRing(FiniteField(3))
sage:ff = ZZ[x].hom([t]);
sage:factor(ff(Phi20))
(t^4 + t^3 + 2*t + 1) * (t^4 + 2*t^3 + t + 1)
sage:factor(ff(x^20-1))
(t + 1) * (t + 2) * (t^2 + 1) * (t^4 + t^3 + 2*t + 1) *
```

```
8 (t^4 + t^3 + t^2+ t + 1) * (t^4 + 2*t^3 + t + 1) *
9 (t^4 + 2*t^3 + t^2 + 2*t + 1)
```

4.7. Ο κυκλοτομικός νόμος αντιστροφής.

Παρατηρούμε ότι ο τετραγωνικός νόμος αντιστροφής δεν είναι τίποτε άλλο παρά μια μέθοδος να προσδιορίζουμε πότε το ανάγωγο πολυώνυμο $x^2 - a$ διασπάται σε γινόμενο πρωτοβάθμιων παραγόντων. Συγκεκριμένα, για να αποφασίσουμε αν το a είναι ή όχι τετραγωνικό υπόλοιπο θα πρέπει να υπολογίζουμε το σύμβολο του Legendre $\left(\frac{a}{p}\right)$.

Θα μπορούσαμε να ρωτήσουμε όμως το εξής θέμα: Ορίζουμε το σύνολο

$$\mathrm{Spl}(x^2 - a) := \left\{p \text{ πρώτοι ώστε το } (x^2 - a)\text{να διασπάται σε γινόμενο 1-βαθμίων πολ/μων}\right\}.$$

Ας υποθέσουμε για απλότητα ότι το a είναι και αυτό πρώτος. Ο προσδιορισμός του συνόλου $\mathrm{Spl}(x^2 - a)$ περιλαμβάνει τον υπολογισμό απείρων συμβόλων του Legendre. Και όμως με τον τετραγωνικό νόμο αντιστροφής αυτό μπορεί να αλλάξει!

Για παράδειγμα αν το $q = 17$ τότε

$$\left(\frac{17}{p}\right) = \left(\frac{p}{17}\right)$$

και τώρα οι πρώτοι χωρίζονται ανάλογα με τη συμπεριφορά τους σε κλάσεις modulo 17. Δηλαδή το 17 είναι τετραγωνικό υπόλοιπο για τους πρώτους οι όποιοι είναι ισοδύναμοι με

$$p \equiv 1, 2, 4, 8, 9, 13, 15, 16 \mathrm{mod}\ 17$$

Εντελώς όμοια αποδεικνύεται ότι οι κατασκευή του παραπάνω παραδείγματος ισχύει γενικά και ο τετραγωνικός νόμος αντιστροφής εκφράζεται ως εξής:

4.7.1 Θεώρημα:
Έστω q περιττός πρώτος. Τότε το σύνολο $Spl(x^2 - q)$ ορίζεται μέσω ισοδυναμιών modulo q αν $q \equiv 1 mod 4$ και μέσω ισοδυναμιών modulo $4q$ αν $q \equiv 3 mod 4$.

Ο νόμος ανάλυσης των κυκλοτομικών πολυωνύμων αποδείξαμε ότι δίνεται ως εξής:

$$\mathrm{Spl}(\Phi_n(x)) = \{p \text{ πρώτος ώστε } p \equiv 1 \bmod n\}$$

τον οποίο και θα ονομάζουμε *κυκλοτομικό νόμο αντιστροφής*. Παρατηρούμε και πάλι ότι και αυτός εκφράζεται μέσω ισοδυναμιών.

Το 9ο πρόβλημα του Hilbert (πρόκειται για μια σειρά προβλημάτων που έθεσε ο Hilbert, σαν τα βασικά προβλήματα των μαθηματικών που μπαίνουν άλυτα στο κατώφλι του 20ού αιώνα. Η διάλεξη δόθηκε στο Παγκόσμιο Συνέδριο Μαθηματικών στα 1900, στο Παρίσι.) ασχολείται με την εύρεση του περισσότερο γενικού νόμου αντιστροφής σε κάθε αλγεβρικό σώμα αριθμών. Η λύση του προβλήματος θα ερχόταν μέσω της θεωρίας κλάσεων σωμάτων, όπως υποστήριζε. Το πρόβλημα λύθηκε για όλες τις αβελιανές επεκτάσεις από τον Artin, ενώ σημαντική συνεισφορά είχαν οι Teiji Takagi, Phillip Furtwängler, Helmut Hasse, Claude Chevalley και άλλοι.

Τελειώνοντας, θέλουμε να σημειώσουμε ότι υπάρχουν πολλές γενικεύσεις του νόμου αυτού. Μέσω του θεωρήματος των Kronecker-Weber έγινε σαφές ότι αν θέλουμε να κατανοήσουμε την αριθμητική

των αβελιανών επεκτάσεων του σώματος των ρητών αριθμών αρκεί να κατανοήσουμε την αριθμητική των κυκλοτομικών σωμάτων.

4.8. Προσθετικά Πολυώνυμα

Στην παράγραφο αυτή θα μελετηθεί η θεωρία των προσθετικών πολυωνύμων, περισσότερα στοιχεία μπορούν να αναζητηθούν στο (Goss 1997). Θεωρούμε ένα σώμα k πεπερασμένης χαρακτηριστικής και έστω $\overline{k}$ η αλγεβρική κλειστότητά του.

4.8.1 Ορισμός:
Θα λέμε ότι ένα πολυώνυμο $P(x) \in k[x]$ *είναι προσθετικό στο σώμα* k *αν και μόνο αν ισχύει:*

$$P(a+b) = P(a) + P(b),$$

για οποιαδήποτε στοιχεία $a, b \in k$. *Θα λέμε ότι το πολυώνυμο είναι απολύτως προσθετικό αν και μόνο αν είναι προσθετικό στο σώμα* $\overline{k}$.

Παρατήρηση: Στη χαρακτηριστική p το πολυώνυμο $\tau_p(x) = x^p$ είναι προσθετικό και απολύτως προσθετικό πολυώνυμο. Επίσης είναι σαφές ότι αν P, G είναι προσθετικά πολυώνυμα και $a \in \overline{k}$, τότε $P + G$, aP, $P \circ G$ είναι επίσης προσθετικά πολυώνυμα.

4.8.2 Ορισμός:
Θα συμβολίζουμε με $k\{\tau_p\}$ *τον υποχώρο του* $k[x]$ *που παράγεται από τους γραμμικούς συνδυασμούς των πολυωνύμων* $\tau_p^i(x) = x^{p^i}$.

Παρατήρηση: Το σύνολο $k\{\tau_p\}$ εφοδιασμένο με τις πράξεις της πρόσθεσης και της σύνθεσης αποτελεί έναν δακτύλιο. Αν $k \neq \mathbb{F}_p$, τότε ο δακτύλιος αυτός είναι μη αντιμεταθετικός, αφού

$$\tau_p(a) = a^p \tau_p,$$

για $a \in k$.

Αν το k είναι ένα σώμα με άπειρο πλήθος στοιχεία, τότε το πολυώνυμο $P(x) \in k[x]$ είναι προσθετικό αν και μόνο αν $P(x) \in k\{\tau_p\}$. Ιδιαίτερα, το σύνολο των απολύτως προσθετικών πολυωνύμων είναι το σύνολο $k\{\tau_p\}$.

Απόδειξη: Είναι σαφές ότι όλα τα πολυώνυμα στο $\{\tau_p\}$ είναι προσθετικά.

Αντιστρόφως, έστω ένα προσθετικό πολυώνυμο. Θεωρούμε την τυπική παράγωγό του $P'(x)$. Δηλαδή αν

$$P(x) = \sum_{\nu=0}^{n} a_\nu x^\nu,$$

τότε

$$P'(x) = \sum_{\nu=1}^{n} a_\nu \nu x^{\nu-1}.$$

Παρατηρούμε ότι αν το P είναι προσθετικό τότε για κάθε $a \in k$ έχουμε

$$P(x+a) - P(x) - P(a)$$

είναι μηδέν για κάθε τιμή $x \in k$ και αφού το k είναι άπειρο αυτό σημαίνει ότι το $P(x)$ θα πρέπει να είναι μηδενικό. Πράγματι, αν δεν ήταν θα είχε κάποιο πεπερασμένο βαθμό και συνεπώς θα είχε το πολύ τόσες ρίζες όσες ο βαθμός του.

Συνεπώς

$$P'(a) = \frac{d}{dx}P(x+a)\Big|_{x=0} = \frac{d}{dx}(P(x)+P(a))\Big|_{x=0} = P'(0).$$

Άρα και πάλι επειδή το σώμα k έχει άπειρα στοιχεία έχουμε ότι η παράγωγος είναι ένα σταθερό πολυώνυμο:

$$P'(x) = P'(0) = c.$$

Δηλαδή,

$$P(x) = cx + \sum_{j=2}^{n} a_j x^{n_j},$$

όπου όλοι οι εκθέτες n_j είναι διαιρετοί με p. Θα απομονώσουμε τους εκθέτες που είναι διαιρετοί μόνο με p και θα τους μαζέψουμε σε ένα πολυώνυμο $P_0(x)$ και θα μαζέψουμε τους εκθέτες που εκτός από p είναι διαιρετοί και με άλλους πρώτους. Δηλαδή

$$P(x) = P_0(x) + P_1(x).$$

Θα δείξουμε ότι το $P_1(x)$ είναι το μηδενικό πολυώνυμο. Είναι σαφές ότι είναι και αυτό προσθετικό.

Στην αλγεβρική κλειστότητα $\overline{k}$ του σώματος k η συνάρτηση $x \to x^p$ είναι αυτομορφισμός. Για κάθε στοιχείο $y \in \overline{k}$ υπάρχει μοναδικό x ώστε $x^p = y$. Παρατηρήστε ότι εν γένει σε σώματα χαρακτηριστικής 0 κάθε στοιχείο έχει n το πλήθος n-στές ρίζες, αρκεί να βρούμε μία και να την πολλαπλασιάσουμε με τις n-στές ρίζες της μονάδας. Στη χαρακτηριστική p όμως υπάρχει μόναδικη p-ρίζα της μονάδας.

Μπορούμε λοιπόν να θεωρήσουμε τη συνάρτηση $x \mapsto x^{1/p^e}$, η οποία είναι προσθετική αν και μη πολυωνυμική. Έστω p^e η μεγαλύτερη δύναμη του p η οποία διαιρεί όλους τους εκθέτες του $P_1(x)$. Θεωρούμε το πολυώνυμο:

$$P_2(x) = P_1(x)^{1/p^e} \in \overline{k}[x].$$

Το πολυώνυμο $P_2(x)$ είναι προσθετικό, και το προηγούμενο επιχείρημα δείχνει ότι θα πρέπει να είναι μηδενικό.

4.8.3 Ορισμός:
Θα λέμε ότι το προσθετικό πολυώνυμο $P(x) \in k[x]$ είναι $\mathbb{F}_{p^h}$-γραμμικό αν και μόνο αν

$$P(\lambda x) = \lambda P(x)$$

για κάθε $\lambda \in \mathbb{F}_{p^h}$.

Παρατηρούμε ότι τα $\mathbb{F}_{p^h}$-γραμμικά πολυώνυμα είναι αυτά που είναι k γραμμικοί συνδυασμοί των στοιχείων x^{p^h}.

4.8.4 Θεώρημα:
Θεωρούμε ένα διαχωρίσιμο πολυώνυμο $P(x) \in k[x]$ και έστω $S := \{\rho_1, \ldots, \rho_m\}$ το σύνολο των ριζών του. Το πολυώνυμο $P(x)$ είναι προσθετικό αν και μόνο αν το σύνολο S είναι προσθετική ομάδα. Επιπλέον το $P(x)$ είναι $\mathbb{F}_{p^h}$-γραμμικό αν και μόνο αν το σύνολο $\mathbb{F}_{p^h}$-διανυσματικός χώρος.

Απόδειξη: Θα πρέπει να δείξουμε ότι το πολυώνυμο

$$P(x) = \prod_{i=1}^{m}(x - \rho_i)$$

είναι προσθετικό. Παρατηρούμε ότι αν $\rho \in S$ τότε

$$P(x + \rho) = P(x),$$

διότι σε μία προσθετική ομάδα S, αν το ρ_i διατρέχει το S, τότε και το $\rho + \rho_i$ επίσης διατρέχει το S. Στη συνέχεια θεωρούμε το πολυώνυμο

$$G(x) = P(x + y) - P(x) - P(y) \in k[x],$$

για μια τιμή $y \in k$. Αυτό είναι ένα πολυώνυμο βαθμού $\deg G < \deg P$ συνεπώς αν έχει $\deg P$ ρίζες είναι ταυτοτικά μηδενικό. Πράγματι παρατηρούμε ότι κάθε $\rho \in S$ είναι ρίζα του πολυωνύμου G.

Για τη γραμμικότητα, υποθέτουμε ότι το S είναι ένας $\mathbb{F}_{p^h}$-διανυσματικός χώρος. Σε αυτή την περίπτωση έχουμε ότι $|S| = (p^{hj}$ και ο βαθμός του P είναι ο ίδιος. Θεωρούμε το πολυώνυμο, για $\lambda \in \mathbb{F}_{p^h}$

$$G(x) = P(\lambda x) - \lambda P(x).$$

Παρατηρούμε ότι $\deg G < \deg P$. Πράγματι, ο μεγιστοβάθμιος όρος του $G(x)$ είναι

$$(\lambda^{p^{hj}} - \lambda)x^{p^{hj}},$$

και αφού $\lambda \in \mathbb{F}_{p^h}$ ο όρος αυτός δεν εμφανίζεται.

Από την άλλη $G(\rho) = 0$ για κάθε $\rho \in W$ συνεπώς έχουμε περισσότερες ρίζες από τον βαθμό του πολυωνύμου, άρα το πολυώνυμο είναι ταυτοτικά ίσο με το μηδέν.

4.8.1. Η ορίζουσα Moore. Είναι γνωστό (ορίζουσα Vandermonde) ότι

$$\det \begin{pmatrix} 1 & \dots & 1 \\ x_1 & \dots & x_n \\ \vdots & & \vdots \\ x_1^{n-1} & \dots & x_n^{n-1} \end{pmatrix} = \prod_{i<j}(x_i - x_j).$$

Εδώ θα δώσουμε μια διαφορετική q-έκδοση του παραπάνω τύπου. Έχουμε ένα σώμα $\mathbb{F}_q$ με $q = p^h$ το πλήθος στοιχεία, και έστω $W \subset k$ ένας $\mathbb{F}_q$-διανυσματικός χώρος.

Ορίζουμε την ορίζουσα Moore να είναι το παρακάτω:

$$\Delta(w_1, \dots, w_n) = \det \begin{pmatrix} w_1 & \dots & w_n \\ w_1^q & \dots & w_n^q \\ & \vdots & \\ w_1^{q^{n-1}} & \dots & w_n^{q^{n-1}} \end{pmatrix}.$$

Το σύνολο $\{w_1, \dots, w_n\}$ είναι $\mathbb{F}_q$-γραμμικά ανεξάρτητο αν και μόνο αν $\Delta(w_1, \dots, w_n) \neq 0$.

Απόδειξη Ας υποθέσουμε πρώτα ότι $\Delta(w_1, \dots, w_n) \neq 0$. Θα δείξουμε ότι σε αυτή την περίπτωση τα $\{w_1, \dots, w_n\}$ είναι $\mathbb{F}_q$ γραμμικά ανεξάρτητα.

Πράγματι αν $\lambda_i \in \mathbb{F}_p$ συντελεστές ώστε

$$\sum_{\nu=1}^{n} \lambda_\nu w_\nu = 0,$$

τότε

$$\sum_{\nu=1}^{n} \lambda_\nu^{q^i} w_\nu^{q^i} = \sum_{\mu=1}^{n} \lambda_\nu w_\nu^{q^i},$$

για κάθε $i = 0, \dots, n-1$, αφού $\lambda_i \in \mathbb{F}_p$ και συνεπώς $\lambda_i^q = \lambda_i$.

Συνεπώς καταλήγουμε σε μία σχέση της μορφής

$$\sum_{\nu=1}^{n} \lambda_\nu \begin{pmatrix} w_\nu \\ w_\nu^q \\ \vdots \\ w_\nu^{q^{n-1}} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Αφού δε $\Delta(w_1, \dots, w_n) \neq 0$ η παραπάνω εξίσωση έχει ως λύση μόνο την $(\lambda_1, \dots, \lambda_n) = 0$.

Αντιστρόφως ας υποθέσουμε ότι το σύνολο $\{w_1, \dots, w_n\}$ είναι γραμμικά ανεξάρτητο. Θα δείξουμε ότι $\Delta(w_1, \dots, w_n) \neq 0$. Θα δουλέψουμε επαγωγικά. Η περίπτωση $n = 1$ είναι προφανής. Ας υποθέσουμε ότι για $n-1$ οποιαδήποτε γραμμικά ανεξάρτητα στοιχεία $\{w_1, \dots, w_{n-1}\}$ η ορίζουσα $\Delta(w_1, \dots, w_{n-1}) \neq 0$. Ας υποθέσουμε ότι $\Delta(w_1, \dots, w_{n-1}) = 0$ και $\{w_1, \dots, w_n\}$ γραμμικά ανεξάρτητα, συνεπώς υπάρχουν στοιχεία $\lambda_1, \dots, \lambda_n \in k$ για τα οποία να ισχύει:

$$\lambda_1 w_1 + \cdots + \lambda_n w_n = 0$$

$$\lambda_1 w_1^q + \cdots + \lambda_n w_n^q = 0$$

$$\dots$$

$$\lambda_1 w_1^{q^{n-1}} + \cdots + \lambda_n w_n^{q^{n-1}} = 0$$

Μπορούμε χωρίς περιορισμό της γενικότητας να υποθέσουμε ότι το $\lambda_1 = 1$ (πράγματι κάποιος συντελεστής και υποθέτουμε ο πρώτος είναι μη μηδενικός, στη συνέχεια διαιρούμε όλες τις εξισώσεις με αυτόν για να υποθέσουμε ότι είναι ίσος με ένα).

Στη συνέχεια υψώνουμε την i-στή εξίσωση στην q-δύναμη και την αφαιρούμε από την $i+1$-στη για όλες τις εξισώσεις για να καταλήξουμε στο σύστημα:

$$(\lambda_2 - \lambda_2^q) w_2^q + \cdots + (\lambda_n - \lambda_n^q) w_n^q = 0$$

$$\dots$$

$$(\lambda_2 - \lambda_2^q) w_2^{q^{n-1}} + \cdots + (\lambda_n - \lambda_n^q) w_n^{q^{n-1}} = 0$$

Παρατηρούμε ότι το σύνολο $\{w_2^q, \dots, w_n^q\}$ είναι ένα γραμμικά ανεξάρτητο σύνολο υπέρ του $\mathbb{F}_q$ συνεπώς $\Delta(w_2^q, \dots, w_n^q) \neq 0$. Συνεπώς η αρχική εξίσωση έχει συντελεστές στο $\mathbb{F}_q$ και το σύνολο $\{w_1, \dots, w_n\}$ είναι $\mathbb{F}_q$-γραμμικά εξαρτημένο, άτοπο.

Στη συνέχεια θα δώσουμε έναν κλειστό τύπο προκειμένου να εκφράσουμε το προσθετικό πολυώνυμο που αντιστοιχεί σε έναν $\mathbb{F}_q$-διανυσματικό χώρο W. Ας θεωρήσουμε $\{w_1, \dots, w_n\}$ μια βάση του W και ας είναι

$$W_i = \langle w_1, \dots, w_i \rangle.$$

Θεωρούμε τα πολυώνυμα

$$P_W := \prod_{a \in W} (x - a).$$

4.8.5 Θεώρημα:
Το πολυώνυμο P_W *υπολογίζεται ως*

$$P_W(x) = \frac{\Delta(w_1, \ldots, w_n, x)}{\Delta(w_1, \ldots, w_n)}.$$

Απόδειξη Παρατηρούμε ότι ένα στοιχείο x είναι ρίζα του πολυωνύμου

$$\Delta(w_1, \ldots, w_n, x)$$

αν και μόνο αν $x \in \langle w_1, \ldots, w_n \rangle$. Με άλλα λόγια το πολυώνυμο $\Delta(w_1, \ldots, w_n, x)$ έχει ακριβώς ως ρίζες τα στοιχεία του διανυσματικού χώρου W.

Επίσης αν αναπτύξουμε την ορίζουσα $\Delta(w_1, \ldots, w_n, x)$ ως προς την τελευταία γραμμή βλέπουμε ότι ο συντελεστής του μεγιστοβάθμιου όρου είναι η ορίζουσα $\Delta(w_1, \ldots, w_n)$ και για να καταλήξουμε στο μονικό πολυώνυμο P_W, θα πρέπει να διαιρέσουμε με αυτόν.

4.9. Το σώμα με ένα στοιχείο

Ας ξεκαθαρίσουμε ότι όλα τα σώματα είναι αντιμεταθετικοί δακτύλιοι με μονάδα και συνεπώς περιέχουν δύο τουλάχιστον στοιχεία το 0 και το 1. Θα θέλαμε παρόλα αυτά να έχουμε έναν γενικευμένο ορισμό που θα επιτρέψει να δώσουμε κάποιο νόημα στην οριακή κατάσταση $\lim_{q \to 1} \mathbb{F}_q = \mathbb{F}_1$.

Το σώμα αυτό το οραματίστηκε πρώτος το 1956 ο Jacques Tits, στη μελέτη του σχετικά με τα buildings. Όπως θα δούμε στο κεφάλαιο των ελλειπτικών καμπυλών ο τελεστής του Frobenious παίζει πολύ σημαντικό ρόλο στη μέτρηση των σημείων μιας αλγεβρικής καμπύλης ή πολλάπλότητας στον πύργο σωμάτων $\mathbb{F}_{p^\ell}$. Στην πραγματικότητα αυτό ήταν το βασικό εργαλείο στο να αποδείξει κανείς την εικασία του Riemann για ζήτα συναρτήσεις ορισμένες σε σώματα συναρτήσεων.

Στην πραγματικότητα πολλοί μαθηματικοί έχουν προτείνει το πώς η απόδειξη για σώματα συναρτήσεων θα μπορούσε να μεταφερθεί στη μελέτη της κλασικής εικασίας του Riemann μέσω ενός κατάλληλα ορισμένου σώματος με ένα στοιχείο.

Τα παραπάνω είναι δύσκολα να τα αναπτύξουμε στα πλαίσια ενός προπτυχιακού βιβλίου. Μπορούμε όμως μεταφράζοντας τον A. Connes να κάνουμε πλάκα με το F_{un} ακολουθώντας τις ιδέες των Kapranov-Smirnov σχετικά με το $\mathbb{F}_1$ και τις επεκτάσεις του $\mathbb{F}_{1^n}$.

Δεν μπορούμε να πούμε τι είναι το $\mathbb{F}_1$. Παρόλα αυτά μπορούμε να επιχειρηματολογήσουμε ότι ένας διανυσματικός V χώρος πάνω από το $\mathbb{F}_1$ είναι απλά ένα σύνολο. Η διάσταση του V ως διανυσματικού χώρου πάνω από το $\mathbb{F}_1$ είναι απλά ο πληθικός αριθμός του V.

Προχωρώντας την ιδέα αυτή η $GL_n(\mathbb{F}_1) = S_n$. Η συνάρτηση ορίζουσας είναι απλά η συνάρτηση προσήμου $\operatorname{sgn} : S_n \to \{\pm 1\}$, δηλαδή

$$\lim_{q \to 1} GL_n(\mathbb{F}_q) = S_n.$$

Έτσι η $SL_n(\mathbb{F}_1)$ δεν είναι άλλη από την A_n. Δηλαδή, η γραμμική άλγεβρα υπέρ του $\mathbb{F}_1$ είναι η συνδυαστική θεωρία των πεπερασμένων συνόλων.

Για να το κάνουμε περισσότερο ενδιαφέρον ας αναφέρουμε ότι το σύνολο των διανυσματικών υποχώρων διάστασης k μέσα σε έναν διανυσματικό χώρο διάστασης n είναι ένα γεωμετρικό αντικείμενο γνωστό ως η πολλαπλότητα Grassmann. Μπορούμε να μετρήσουμε ακριβώς το πλήθος των σημείων

μιας τέτοιας πολλαπλότητας πάνω από ένα πεπερασμένο σώμα και να δούμε ότι

$$\lim_{q \to 1} \#G(n, r)(\mathbb{F}_q) = \binom{n}{r},$$

το οποίο είναι συμβατό με την παραπάνω θεώρηση.

Δεν γνωρίζουμε τι είναι το $\mathbb{F}_1[t]$. Παρόλα αυτά μπορούμε να επιχειρηματολογήσουμε ότι $GL_d(\mathbb{F}_1[t])$ θα πρέπει να είναι η πλήρης ομάδα κοτσίδων σε d-κλωστές.

Θα τελειώσουμε αυτή την αναλογία αναφέροντας ότι η επέκταση $\mathbb{F}_{1^n}$ του $\mathbb{F}_1$ δεν είναι τίποτε άλλο από το $\{0\} \cup \mu_n$, όπου μ_n είναι το σύνολο των n-στών ριζών της μονάδας.

Ελπίζουμε ότι όλα τα παραπάνω θα οδηγήσουν τον αναγνώστη να ανατρέξει για περισσότερες πληροφορίες στη βιβλιογραφία.

Βιβλιογραφία

Fraleigh, J.B. 2011. *Εισαγωγή Στην Άλγεβρα*. Πανεπιστημιακές Εκδόσεις Κρήτης.

Goss, D. 1997. *Basic Structures of Function Field Arithmetic*. Ergebnisse Der Mathematik Und Ihrer Grenzgebiete ; 3. Folge, Bd. 35. Springer Berlin Heidelberg. https://books.google.gr/books?id=cIV3AaOcPDcC.

Lidl, R., και H. Niederreiter. 1997. *Finite Fields*. EBL-Schweitzer, τ. 20,μ. 1. Cambridge University Press. https://books.google.gr/books?id=xqMqxQTFUkMC.

Mullen, G.L., και D. Panario. 2013. *Handbook of Finite Fields*. Discrete Mathematics και Its Applications. CRC Press. https://books.google.gr/books?id=YADSBQAAQBAJ.

Stewart, I. 2003. *Galois Theory, Third Edition*. Chapman Hall/CRC Mathematics Series. Taylor & Francis. https://books.google.gr/books?id=C9/_Vivwgf5cC.

Βάρσος, Δ., Δ. Δεριζιώτης, Ι. Εμμανουήλ, Μ. Μαλιάκας, και Ο. Ταλέλλη. 2012. *Μια Εισαγωγή Στην Άλγεβρα*. Σοφία Α. Ε.

5

Απλά Κρυπτοσυστήματα

5.1. Κρυπτολογία-Κρυπτογραφία

5.1.1 Ορισμός:
Κρυπτολογία-Κρυπτογραφία είναι η επιστήμη που μελετάει τις μεθόδους με τις οποίες η επικοινωνία ανθρώπων να είναι μυστική ώστε κάποιος ανεπιθύμητος να μην μπορεί να αντιληφθεί το περιεχόμενο της επικοινωνίας.

Η κρυπτογραφία δεν πρέπει να συγχέεται με την κωδικοποίηση που ασχολείται με το πώς μπορούν να γίνουν αντιληπτά και να διορθωθούν λάθη μετάδοσης.

Η Κρυπτοανάλυση είναι η αντίστροφη προσπάθεια που ασχολείται με το πώς ο ενδιάμεσος μπορεί να υποκλέψει το περιεχόμενο του μηνύματος.

Οι εφαρμογές είναι πολλές:

- Ηλεκτρονική επικοινωνία-e-mail,
- Μεταφορά χρημάτων-e-banking,
- Βιομηχανική - Στρατιωτική - Διπλωματική ασφάλεια.

5.1.2 Ορισμός:
Ένα κρυπτοσύστημα είναι μια διατεταγμένη πεντάδα (P, C, K, E, D)*, όπου*

- P *είναι πεπερασμένο σύνολο των μηνυμάτων που θέλουμε να στείλουμε,*
- C *είναι πεπερασμένο σύνολο των κρυπτογραφημένων μηνυμάτων (cipher text),*
- K *είναι πεπερασμένο σύνολο των κλειδιών κωδικοποίησης (Keyspace),*
- *Για κάθε* $k \in K$ *υπάρχει κανόνας κρυπτογράφησης* $e_k \in E$ *και ένας κανόνας αποκρυπτογράφησης* $d_k \in D$ *ώστε* $d_k(e_k) = x$.

5.1.1. Το κρυπτοσύστημα της μεταφοράς. Τα γράμματα μπορούν να μετατραπούν σε αριθμούς:

Πίνακας 5.1: Πίνακας αντιστοιχίας γραμμάτων

A	B	C	D	E	F	G
1	2	3	4	5	6	7

H	I	J	K	L	M	N
8	9	10	11	12	13	14

O	P	Q	R	S	T	U
15	16	17	18	19	20	21

V	W	X	Y	Z
22	23	24	25	26

Έχουμε τα σύνολα
P $= \mathbb{Z}/26$ (ακέραιοι modulo 26)
C $= \mathbb{Z}/26$
K $= \mathbb{Z}/26$
Το μήνυμα NUMBER THEORY μεταφράζεται ως

Πίνακας 5.5: Μετάφραση μηνύματος

N	U	M	B	E	R	T	H	E	O	R	Y
14	21	13	2	5	18	20	8	5	15	18	25

5.1.2. Το κρυπτοσύστημα της αντικατάστασης. Στο σύστημα αυτό P $= \mathbb{Z}/26$, K $= S_{26}$, το σύνολο των μεταθέσεων σε 26 γράμματα.

Η συνάρτηση κρυπτογράφησης είναι μια μετάθεση:

Πίνακας 5.6: Πίνακας Συνάρτησης κρυπτογράφησης

A	B	C	D	E	F	G
d	e	r	y	v	o	h

H	I	J	K	L	M	N
e	z	x	w	p	t	b

O	P	Q	R	S	T	U
g	f	j	q	n	m	u

O	P	Q	R	S	T	U

V	W	X	Y	Z
s	k	a	c	i

Το μήνυμα NUMBER THEORY μεταφράζεται ως

Πίνακας 5.10: Μετάφραση μηνύματος

N	U	M	B	E	R	T	H	E	O	R	Y
b	u	t	e	v	q	m	e	v	g	q	c

Παρατήρηση Ο αριθμός κλειδιών είναι μεγάλος 26!, παρόλα αυτά το σύστημα μπορεί να αποκρυπτογραφηθεί εύκολα με βάση τη στατιστική εμφάνιση των γραμμάτων της αλφαβήτου.

5.1.3. Το αφινικό Κρυπτοσύστημα. $\mathsf{P} = \mathsf{C} = \mathbb{Z}/26$

$$\mathsf{K} = \{(a, b)\ (\mathbb{Z}/26 \times \mathbb{Z}/26)\}.$$

Για ένα σταθερό (a, b) έχουμε

$$e_k(x) = ax + b$$

Έστω

$$ax + b = y \bmod 26 \Rightarrow ax = y - b \bmod 26$$

Την παραπάνω εξίσωση θα πρέπει να έχει μοναδική λύση ως προς x. Αυτό συμβαίνει αν και μόνο αν ΜΚΔ (a,26) =1. Αν θεωρήσουμε την ισοδυναμία

$$a \cdot x = 1 \bmod 26$$

και συμβολίσουμε τη λύση της με $x = a^{-1}$, τότε

$$d_k(y) = a^{-1}(y - b) \bmod 26.$$

Παράδειγμα Έστω το κλειδί $= (7, 3)$ και ο $(7, 26) = 1$ ισχύει

$$e_k(x) = 7x + 3 \bmod 26.$$

Για τη συνάρτηση αποκωδικοποίησης πρέπει $7^{-1} = 15$ αφού $7x = 1 \bmod 26$. Επομένως

$$d_k(y) = 15(y - 3) = 15y - 19 \bmod 26$$

Έστω ότι θέλουμε να στείλουμε το μήνυμα "hot"
Κωδικοποίηση

$$\begin{array}{lll} h \to 8 & e_k(7) = 7 \cdot 8 + 3 = 59 \equiv 7 & \bmod 26 \\ o \to 15 & e_k(14) = 7 \cdot 15 + 3 = 108 \equiv 4 & \bmod 26 \\ t \to 20 & e_k(19) = 7 \cdot 20 + 3 = 143 \equiv 13 & \bmod 26 \end{array}$$

Άρα Cipher Text = GDM
Αποκωδικοποίηση

$$d_k(7) = 15 \cdot 7 - 19 = 86 = 8 \text{mod} 26 \qquad 8 \to h$$
$$d_k(4) = 15 \cdot 4 - 19 = 41 \equiv 15 \text{mod} 26 \quad 15 \to o$$
$$d_k(19) = 7 \cdot 13 - 19 \equiv 20 \text{mod} 26 \qquad 20 \to t$$

Σημείωση: Για να λύσουμε την $7x = 1 \text{mod} 26$: Γνωρίζουμε ότι αν $(a, b) = d$, τότε υπάρχουν $x_0, y_0 \in \mathbb{Z}$ ώστε $d = ax_0 + y_0$ και πρέπει να βρούμε τα x_0, y_0, d. Για παράδειγμα $26 = 7 \cdot 3 + 5$ και $7 = 5 \cdot 1 + 2$ και $5 = 2 \cdot 2 + 1$. Προχωράμε αντίστροφα:

$$1 = 5 - 2 \cdot 2 = 5 - 2(7 - 5) = -2 \cdot 7 + 3 \cdot 5 =$$

$$-2 \cdot 7 + 3(26 - 3 \cdot 7) = 3 \cdot 26 - 11 \cdot 7$$

Άρα $26 \cdot 3 + 7(-11)$ όπου $x_0 = 3$ και $y_0 = 7$. Είναι $7(-11) \equiv 1 \text{mod} 26$ και $-11 = 15$ στο $\mathbb{Z}_{26}$ Δηλαδή $a^{-1} = 15$.

5.2. Το Κρυπτοσύστημα Vigenere

$P = C = (\mathbb{Z}_{26})^m = K$ όπου $m \in \mathbb{N}$ με $m \neq 0$. Έστω $k \in K$ δηλαδή $k = (k_1, k_2, \ldots, k_m)$ με $k_i \in \mathbb{Z}_{26}$. Θεωρούμε τις συναρτήσεις

$$e_k(x_1, x_2, \ldots, x_m) = (x_1 + k_1, x_2 + k_2, \ldots, x_m + k_m)$$

και

$$d_k(y_1, y_2, \ldots, y_m) = (y_1 - k_1, y_2 - k_2, \ldots, y_m - k_m)$$

Παρατηρήσεις

1. Το σύστημα είναι πολυαλφαβητικό, άρα η κρυπτοανάλυση είναι πιο δύσκολη από ότι στα προηγούμενα μονοαλφαβητικά συστήματα.
2. Το πλήθος των κλειδιών είναι 26^m. Επειδή το m είναι αυθαίρετο μπορούμε να φτιάξουμε κρυπτοσύστημα με όσο αριθμό κλειδιών επιθυμούμε.
3. Δεν χρειάζεται το κείμενο να έχει πλήθος γραμμάτων πολλαπλάσιο του m, αν κατά την ομαδοποίηση προκύψει ομάδα με μικρότερο πλήθος γραμμάτων - έστω $u < m$ από αυτή του κλειδιού κρατάμε το κομμάτι του κλειδιού που χρειαζόμαστε δηλαδή τα πρώτα u γράμματα.

Έστω $m = 6$ και κλειδί η λέξη CIPHER , δηλαδή $k = (2, 8, 15, 7, 4, 17)$.

Παράδειγμα Κωδικοποίησης

Έστω ότι θέλουμε να στείλουμε το μήνυμα "Number Theory". Μετατρέπουμε το μήνυμα σε αριθμούς, ομαδοποιούμε ανά 6 και προσθέτουμε το κλειδί στο $\mathbb{Z}_{26}$.

Μήνυμα $14, 21, 13, 2, 5, 18, 20, 8, 5, 15, 18, 25$.

Ομαδοποίηση $(14, 21, 13, 2, 5, 18), (20, 8, 5, 15, 18, 25)$

Προσθέτουμε το κλειδί

$$(14, 21, 13, 2, 5, 18) + (2, 8, 15, 7, 4, 17) = (16, 3, 2, 9, 9, 9),$$

$$(20, 8, 5, 15, 18, 25) + (2, 8, 15, 7, 4, 17) = (22, 16, 20, 22, 16)$$

Το μήνυμα γίνεται λοιπόν: PCBIIIVPTVP

5.3. Το Κρυπτοσύστημα του Hill

$P = C = (\mathbb{Z}_{26})^m$, με $m \in \mathbb{N}, m \neq 0$. Το σύνολο K αποτελείται από τους $m \times m$ πίνακες με στοιχεία από το $\mathbb{Z}_{26}$. Αν $x = (x_1, x_2, \ldots, x_m) \in P$ και $k = (k_{i,j})$, $1 \leqslant i, j \leqslant m$ τότε

$$y = (y_1, y_2, \ldots, y_m) = e_k(x) = k \cdot x.$$

Για να ορίζεται η αντίστροφη συνάρηση θα πρέπει να υπάρχει ο αντίστροφος πίνακας k^{-1} και αυτό γίνεται αν και μόνο αν η ορίζουσα $\det(k)$ είναι αντιστρέψιμο στοιχείο στο $\mathbb{Z}_{26}$ ισοδύναμα αν και μόνο αν $(\det(k), 26) = 1$. Η συνάρτηση αποκωδικοποίησης είναι η

$$d_k(y) = k^{-1} \cdot y.$$

Παράδειγμα Κλειδί

$$k = \begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix}$$

και $\det(k) = 53 \equiv 1 \mathrm{mod} 26$

Παράδειγμα Ας υποθέσουμε ότι θέλουμε να στείλουμε την λέξη MATH $\to (13, 1, 20, 8)$.

Για την κωδικοποίηση έχουμε:

$$\begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix} \begin{pmatrix} 13 \\ 1 \end{pmatrix} = \begin{pmatrix} 21 \\ 20 \end{pmatrix}, \begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix} \begin{pmatrix} 20 \\ 8 \end{pmatrix} = \begin{pmatrix} 24 \\ 12 \end{pmatrix}.$$

Δηλαδή το κρυπτογραφημένο μήνυμα είναι UTXL.

Η αποκρυπτογράφηση γίνεται με πολλαπλασιασμό με τον αντίστροφο πίνακα

$$k^{-1} = \begin{pmatrix} 7 & -8 \\ -3 & 11 \end{pmatrix}$$

Έτσι

$$\begin{pmatrix} 7 & -8 \\ -3 & 11 \end{pmatrix} \cdot \begin{pmatrix} 21 \\ 20 \end{pmatrix} = \begin{pmatrix} 13 \\ 1 \end{pmatrix}, \begin{pmatrix} 7 & -8 \\ -3 & 11 \end{pmatrix} \cdot \begin{pmatrix} 24 \\ 12 \end{pmatrix} = \begin{pmatrix} 20 \\ 8 \end{pmatrix}$$

Παρατηρήσεις Αν $\det k \neq 1$ τότε $\det(k)^{-1}$ συμβολίζει τον αντίστροφο της $\det(k)$ στον δακτύλιο $\mathbb{Z}_{26}$ Δηλαδή θα πρέπει να λύσουμε την ισοδυναμία

$$\det(k) \cdot x \equiv 1 \mathrm{mod} 26).$$

5.4. Το κρυπτοσύστημα μεταθέσεων

Το κρυπτοσύστημα αυτό αποτελεί ειδική περίπτωση του κρυπτοσυστήματος του Hill. Θεωρούμε μια μετάθεση $\sigma \in S_m$ δηλαδή μια μετάθεση του συνόλου $\{1, 2, \ldots, m\}$. Στη μετάθεση αυτή αντιστοιχεί ένας πίνακας μεταθέσεων k_σ ο οποίος ορίζεται ως

$$k_{ij} = \begin{cases} 1 & \text{αν } j = \sigma(i) \\ 0 & \text{διαφορετικά} \end{cases}$$

Ο πίνακας αυτός έχει την ιδιότητα να μεταθέτει τα στοιχεία των στηλών που πολλαπλασιάζονται με αυτόν, και κάνει αναγραμματισμούς.

Έχουμε $P = C = \mathbb{Z}_{26}^m$,

$$e_\sigma(x_1, x_2, \ldots, x_n) = (x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(m)})$$

και

$$d_\sigma(x_1, x_2, \ldots, x_n) = e_{\sigma^{-1}}(x_1, x_2, \ldots, x_n).$$

Έτσι αν το κλειδί είναι η μετάθεση $(m = 6)$

Πίνακας 5.11: Πίνακες μετάθεσης

1	2	3	4	5	6
3	5	1	6	4	2

το μήνυμα Nice party in Sparti γράφεται

N	i	c	e	p	a
c	a	n	p	i	e

r	t	y	i	n	S
y	s	r	n	t	i

p	a	r	t	i	q
r	q	p	i	a	t

Το μήνυμά μας έγινε: canpieysrntirqpiat.

5.5. Κρυπτοσυστήματα Ροής

Ιδέα: Χρησιμοποιούμε κλειδί ροής $z = z_1, z_2, \ldots$ και κρυπτογραφούμε το μήνυμα

$$x = x_1, x2, \ldots$$

$$y = y_1, y_2, \ldots = e_{z_1}(x1), e_{z_2}(x_2), \ldots,$$

Η συνάρτηση f_i (εξαρτάται από το κλειδί k και από τους $i-1$ χαρακτήρες του μηνύματος) χρησιμοποιείται για να μας δώσει το z_i (i- οστό στοιχείο του κλειδιού ροής). Δηλαδή:

$$z_i = f_i(k, x_1, x_2, \ldots, x_{i-1}).$$

Το z_i χρησιμοποιείται και δίνει το $y_i = e_{z_i}(x_i)$. Επομένως κρυπτογραφούμε το μήνυμα $x_1, x_2, \ldots, x_{i-1}$ υπολογίζοντας διαδοχικά τα $z_1, y_1, z_2, y_2, \ldots$

Ορισμός: Διατεταγμένη 7-αδα (P, C, K, L, F, E, D) όπου

P: πεπερασμένο σύνολο όλων των δυνατών plaintext C: πεπερασμένο σύνολο όλων των δυνατών cipher text K: πεπερασμένο σύνολο όλων των δυνατών κλειδιών L: πεπερασμένο σύνολο που λέγεται αλφάβητο κλειδιών ροής $F = (f_1, f_2, \ldots)$ σύνολο-γεννήτορας κλειδιών ροής. Για κάθε $i \geqslant 1$ είναι $f_i : K \times P^{i-1} \to L$.

Για κάθε $z \in L$ υπάρχει $e_z \in E$ και $d_z(e_z(x)) = x,\ x \in P$. Δηλαδή

$$e_z : P \to C \text{ και } d_z : C \to P.$$

Το κρυπτοσύστημα ροής θα λέγεται συγχρονισμένο όταν το κλειδί ροής εξαρτάται μόνο από το κλειδί k. Θα λέγεται περιοδικό με περίοδο d,όταν $z_{i+d} = z_i$ για κάθε $i \geqslant 1$.

Παρατήρησεις: 1. Όλα τα προηγούμενα κρυπτοσυστήματα μπορούν να θεωρηθούν ως ειδική περίπτωση του κρυπτοσυστήματος ροής όταν $z_i = k$, για κάθε $k \geqslant 1$.

2. Το Vigenere με κλειδί μήκους m μπορεί να θεωρηθεί περιοδικό κρυπτοσύστημα ροής, με περίοδο m. Το Vigenere μοιάζει με το μεταφοράς $e_z(x) = x + z$ και $d_z(y) = y - z$. Συνήθως $P = C = L = \mathbb{Z}_2$ και $e_z(x) = x + z \bmod 2$ και $d_z(y) = y - z \bmod 2$

3. Άλλη μέθοδος (συγχρονισμένου) κλειδιού ροής:

Αν ξεκινήσουμε από $(k_1, k_2, \ldots, k_m)$ και ας θέσουμε $z_i = k_I$ για $1 \leqslant i \leqslant m$. Συνεχίζουμε να παράγουμε το κλειδί ροής χρησιμοποιώντας την αναδρομική σχέση βαθμού m

$$z_{i+m} = \sum_{j=0}^{m-1} c_j z_{i+j} \bmod 2,$$

όπου $c_i \in \mathbb{Z}_2$ δοσμένα και $c_0 = 1$. Εδώ το k αποτελείται από 2^m τιμές τις $k_1, \ldots, k_m$ και $c_0, c_1, \ldots, c_{m-1}$.

5.6. Κρυπτοανάλυση

Υποθέτοντας ότι το σύστημα επικοινωνίας είναι γνωστό θα δούμε πώς με τη βοήθεια της στατιστικής ανάλυσης εμφάνισης γραμμάτων μπορούμε να υποκλέψουμε το μήνυμα.

Συχνότητα εμφανίσης γραμμάτων:

Πίνακας 5.15: Συχνότητες εμφάνισης γραμμάτων

Γράμμα	Συχνότητα
E	0,120
T,A,O,I,N,S,H,R	0,06 έως 0.09 (σε φθίνουσα σειρά)
D,L	0,04
C,U,M,W,F,G,Y,P,B	0,015 έως 0,028
V,K, J, X,Q, Z	<0,01

Συχνότητα εμφανίσεως διγραμμάτων, σε φθίνουσα σειρά της συχνότητας εμφανίσεως:

TH, HE, IN, ER, AN, RE, ED, ON, ES, ST, EN, AT, TO, NT, HA, ND, OU, EA, NG, AS, OR, TI, IS, ET, IT, AR, TE, SE, HI, OE

Συχνότητα εμφανίσεως τριγραμμάτων,σε φθίνουσα σειρά της συχνότητας εμφανίσης: THE, ING, AND, HER, ERG, ENT, THA, NTH, WAS, ETH, FOR, DTH

Ας υποθέσουμε ότι γνωρίζουμε ότι το παρακάτω μήνυμα
FMXVEDKAPHFERBNDKRXRSREFMORUDSDKDVSHVUFEDKAPRKDLYEVLR HHRH έχει κρυπτογραφηθεί με το αφινικό σύστημα:

Στο παραπάνω ciphertext μελετούμε τη συχνότητα εμφάνισης γραμμάτων και φτιάχνουμε τον πίνακα:

Πίνακας 5.16: Συχνότητες εμφάνισης γραμμάτων στο ciphertext

Γράμμα	Συχνότητα	Γράμμα	Συχνότητα	Γράμμα	Συχνότητα
A	2	J	0	S	3
B	1	K	5	T	0
C	0	L	2	U	2
D	7	M	2	V	4
E	5	N	1	W	0
F	4	O	1	X	2

Γράμμα	Συχνότητα	Γράμμα	Συχνότητα	Γράμμα	Συχνότητα
G	0	P	2	Y	1
H	5	Q	0	Z	0
I	0	R	8		

Τα γράμματα με τη μεγαλύτερη συχνότητα εμφάνισης στο κρυπτομήνυμα είναι:

Πίνακας 5.17: Γράμματα με τη μεγαλύτερη συχνότητα εμφάνισης στο ciphertext

Γράμμα	Συχνότητα
R	8
D	7
E, H, K	5
F, S,V	4

Βάσει των συχνοτήτων εμφάνισης κάνουμε τις εξής αντιστοιχίσεις:

1. $\mathsf{R} \to \mathsf{E}, e_k(5) = 18$ άρα $5a + b \equiv 18 \mathrm{mod} 26$
2. $\mathsf{D} \to \mathsf{T}, e_k(20) = 4$ άρα$20a + b \equiv 4 \mathrm{mod} 26$

Λύνουμε το παραπάνω σύστημα οπότε πιθανές λύσεις είναι: $a = 6$ και $b = 14$. Επειδή όμως $(6, 26) = 2 \neq 1$ υπάρχει λάθος στην αρχική αντιστοίχιση.

Δοκιμάζουμε εκ νέου

1. $\mathsf{R} \to \mathsf{E}, e_k(5) = 18$ άρα $5a + b \equiv 18 \mathrm{mod} 26$
2. $\mathsf{E} \to \mathsf{T}, e_k(20) = 5$ άρα $20a + b \equiv 20 \mathrm{mod} 26$

το οποίο δίνει $a = 14$ και πάλι άτοπο.

Δοκιμάζουμε εκ νέου

1. $\mathsf{R} \to \mathsf{E}, e_k(5) = 18$ άρα $5a + b \equiv 18 \mathrm{mod} 26$
2. $\to \mathsf{T}, e_k(20) = 8$ άρα $20a + b \equiv 8 \mathrm{mod} 26$

η οποία δίνει λύση $a = 22$ και πάλι άτοπο.

Δοκιμάζουμε εκ νέου

1. $\mathsf{R} \to \mathsf{E}, e_k(5) = 18$ άρα $5a + b \equiv 18 \mathrm{mod} 26$
2. $\to \mathsf{T}, e_k(20) = 11$ άρα $20a + b \equiv 11 \mathrm{mod} 26$

η οποία έχει ως λύση $a = 3$ και $b = 3$, δηλαδή πιθανό κλειδί είναι το $a = 3$, $b = 3$. Υπολογίζουμε ότι $a^{-1} \equiv 9 \mathrm{mod} 26$ και

$$d_k(y) = 9(y - 3) = 9y - 3,$$

και παρατηρούμε ότι πράγματι η συνάρτηση αυτή αποκρυπτογραφεί το ζητούμενο μήνυμα, αφού η αποκρυπτογράφηση δίνει:

algorithms are quite general definitions of arithmetic processes

που αποτελεί το μήνυμα (plaintext)

5.6.1. Κρυπτανάλυση συστήματος αντικατάστασης. Στα παρακάτω ακολουθούμε το παράδειγμα του βιβλίου του D. R. Stinson Cryptography: Theory and Practice (Stinson 2005).

Επιθυμούμε να αποκρυπτογραφήσουμε το κρυπτογραφημένο μήνυμα:

```
YIFQFMZRWQFYVECFMDZPCVMRZWNMDZVEJBTXCDDUMJ
NDIFEFMDZCDMQZKCEYFCJMYRNCWJCSZREXCHZUNMXZ
NZUCDRJXYYSMRTMEYIFZWDYVZVYFZUMRZCRWNZDZJJ
XZWGCHSMRNMDHNCMFQCHZJMXJZWIEJYUCFWDJNZDIR
```

Υπολογίζουμε τον πίνακα συχνοτήτων εμφάνισης των γραμμάτων:

Πίνακας 5.18: Συχνότητες εμφάνισης γραμμάτων στο μήνυμα

Γρ.	Συχ.	Γρ.	Συχ.	Γρ.	Συχ.	Γρ.	Συχ.
A	0	H	4	O	0	V	5
B	1	I	5	P	1	X	8
C	15	J	11	Q	4	Y	10
D	13	K	1	R	10	Z	20
E	7	L	0	S	3	F	11
M	16	T	2	G	1	N	9
U	5						

1. Επειδή το Z έχει τη μεγαλύτερη συχνότητα εμφάνισης λογικό είναι να υποθέσουμε ότι $\rightarrow e$ δηλαδή ότι $\mathrm{d_k(Z)} = e$
2. Τα C,D,F,J,M,R,Y έχουν τουλάχιστον 10 εμφανίσεις. Λογικό είναι να υποθέσουμε ότι ανήκουν στο σύνολο {t,a,o,i,n,s,h,r}. Επειδή οι συχνότητες αυτές διαφέρουν πολύ λίγο τίθεται η εξής ερώτηση: Πού αντιστοιχεί το καθένα;

Καταρχήν κοιτάζουμε τα διγράμματα: *Z και Z* αφού γνωρίζουμε ότι $\rightarrow e$. Υπολογίζουμε τον παρακάτω πίνακα εμφάνισης διγραμμάτων:

Πίνακας 5.19: Συχνότητες εμφάνισης διγραμμάτων

Δίγραμμα	Εμφανίσεις	Δίγραμμα	Εμφανίσεις
DZ	4	FZ	2
ZW	4	ZR	2
NZ	3	ZV	2
ZU	3	ZC	2
RZ	2	ZD	2
HZ	2	ZJ	2
XZ	2		

1. Επειδή το ZW εμφανίζεται 4 φορές και το WZ δεν εμφανίζεται καθόλου, ενώ το W εμφανίζεται λίγες φορές (8 φορές) είναι λογικό να υποθέσουμε ότι $\mathrm{d_k(W)} = \mathrm{d}$.
2. Επειδή το DZ εμφανίζεται 4 φορές και το ZD εμφανίζεται 2 φορές είναι λογικό να υποθέσουμε ότι $\mathrm{d_k(D)} \in \{\mathrm{r}, \mathrm{s}, \mathrm{t}\}$. Τίθεται ξανά ερώτηση: Πού αντιστοιχεί το καθένα;

Με την υπόθεση $d_k(Z) = e$ και $d_k(W) = d$ επιστρέφουμε ξανά στο κρυπτογράφημα και παρατηρούμε:

Τα τριγράμματα ZRW και RZW εμφανίζονται στην αρχή, ενώ το RW πολύ αργότερα. Επίσης το R εμφανίζεται συχνά στο κείμενο (10 φορές) και το nd είναι ένα συχνά εμφανιζόμενο δίγραμμα. Έτσι μπορούμε να υποθέσουμε ότι $d_k(R) = n$ Μέχρι τώρα η αποκρυπτογράφηση δίνει:

_ _ _ _ _ _ end _ _ _ _ _ _ _ _ _ _ e _ _ _ _ ned _ _ _ e _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ e _ _ _ _ e _ _ _ _ _ _ _ _ _ _ n _ _ d _ _ _ en _ _ _ _ e _ _ _ _ e _ e _ _ _ n _ _ _ _ n _ _ _ _ _ _ _ ed _ _ _ e _ _ _ e _ _ ne _ nd _ e_ e _ _ _ ed _ _ _ _ _ n _ _ _ _ _ _ _ _ _ _ e _ _ _ _ ed _ _ _ _ _ _ _ d _ _ _ e _ _ n

Υποθέτουμε ότι $d_k(N) = h$, διότι το NZ (he) είναι κοινό δίγραμμα (εμφανίζεται 3 φορές), ενώ το ZN (eh) όχι. Αν αυτό είναι σωστό, τότε μέσα στο κείμενο έχει σχηματιστεί: ne_ndhe. Το μόνο συχνά επαναλαμβανόμενο τρίγραμμα που τελειώνει σε nd είναι το and.

Λογικό λοιπόν είναι να υποθέσουμε ότι $d_k(C) = a$.

Στη συνέχεια θεωρούμε το δεύτερο πιο συχνά εμφανιζόμενο γράμμα, που είναι το M (16 φορές). Πιστεύουμε ότι αποτελεί κρυπτογράφημα του nh _ Δεν υπάρχει τρίγραμμα συχνά εμφανιζόμενο με nh, άρα το h_ πιθανά θα αποτελεί αρχή κάποιας λέξης. Τα διγράμματα όμως με h _ είναι τα he, ha, hi. Επειδή στα a, e έχουμε αντιστοιχίσει ήδη άλλα γράμματα τώρα αναμένουμε ότι $d_k(M) = i$ ή $d_k(M) = o$

Επειδή το ai είναι πολύ πιο συχνό από το ao το δίγραμμα CM του κρυπτογραφήματος μας υποβάλλει την ιδέα να δοκιμάσουμε πρώτα το $d_k(M) = i$

Σ' αυτό το στάδιο το κείμενο γίνεται :

_ _ _ _ _ iend _ _ _ _ _ a _ i _ _ e _ a _ inedhi _ e _ _ _ _ _ a _ _ _ i _ h _ _ _ _ i *ea* i _ e _ a _ _ _ a _ i _ nhad _ a _ en _ _ a _ e _ hi _ ehe _ a _ n _ _ _ _ in _ i _ _ ed _ _ _ e _ _ _ e _ ineandhe _ e_ _ _ ed _ a _ _ inhi _ _ hai _ _ a _ e _ i _ *ed* _ _ _ *a* d __ he _ _n

Επόμενο βήμα: Ποιο γράμμα αποτελεί κρυπτογράφηση του o; Επειδή το o έχει μεγάλη πιθανότητα συχνότητας εμφάνισης ψάχνουμε γράμματα που εμφανίζονται συχνά στο κείμενο. Υποψήφια γράμματα είναι τα : D, F ,J ,Y Πιο πιθανό από αυτά είναι το Y. Αν π.χ. παίρναμε το F θα είχαμε τριάδα φωνηέντων aoi για το CFM ή για το CJM κάτι το οποίο είναι μη αποδεκτό. Υποθέτουμε λοιπόν ότι $d_k(Y) = o$.

Μετά το Z και το M τα τρία πιο συχνά εμφανιζόμενα γράμματα είναι τα D,F,J με 13, 11, 11 φορές εμφάνισης αντίστοιχα. Εικάζουμε λοιπόν ότι {D,F,J }= {r,s,t} Δύο εμφανίσεις του τριγράμματος NMD μας υποβάλλουν την ιδέα να υποθέσουμε ότι $d_k(D) = s$ κάτι που μας δίνει τη λέξη his. (Αυτό είναι συμβιβαστό με την προηγούμενη υπόθεση ότι $d_k(D) \in \{r, s, t\}$)

Το τμήμα HNCMF θα μπορούσε να είναι κρυπτογράφημα της λέξης chair. Αυτό σημαίνει ότι $d_k(F) = r$, $d_k(H) = e$ και $d_k(J) = t$. Συνεπώς $d_k(R) = n$ $d_k(C) = a$ $d_k(M) = i$ ή $d_k(M) = o$ $d_k() = i$ $d_k() =$ $d_k(D) = s$ $d_k(F) = r$ $d_k(H) = c$ $d_k(J) = t$

Το κείμενο γίνεται

o_r _ riend _ ro _ _ arise _ a_ inedhise _ _ t _ _ _ ass _ ithis *r* riseasi _ e _ a *orationhadta* en _ _ ace _ hi _ ehe *asnt* oo _ in _ i _ o _ redso _ e _ ore *ineandhesett* ed _ ack _ inhischair _ aceti _ ted _ _ to *ardsthes* n

Τώρα είναι πολύ εύκολη η αποκρυπτογράφηση:

our friend from paris examined his empty glass with surprise as if evaporation had taken place while he wasn't looking. I poured some more wine and he settled back in his chair face tilted up towards the sun.

Βιβλιογραφία

Stinson, D. R. 2005. *Cryptography: Theory and Practice, Third Edition*. Discrete Mathematics and Its Applications. Taylor & Francis. https://books.google.gr/books?id=FAPLBQAAQBAJ.

6

Κρυπτοσυστήματα Ανοιχτού κλειδιού

6.1. Συστήματα βασισμένα στη Θεωρία Αριθμών

6.1.1. RSA. Το σύστημα αυτό βασίζεται στην ιδέα ότι ενώ ο πολλαπλασιασμός ακέραιων είναι μια διαδικασία που γίνεται εύκολα και γρήγορα δεν ισχύει το ίδιο για την αντίστροφη διαδικασία -την παραγοντοποίηση-. Έτσι, ένας πρώτος αριθμός με μεγάλο αριθμό διαιρετών, προσεχτικά διαλεγμένος είναι πολύ δύσκολο και χρονοβόρο να παραγοντοποιήθει. Περισσότερες πληροφορίες στο (Menezes, Oorschot, και Vanstone 1996) και στο (Αντωνιάδης and Κοντογεώργης 2015).

Η ιδέα του συστήματος RSA ανήκει στους R. Rivest, Adi Shamir, Leonard Adleman ενώ η ονομασία του προκύπτει από τα αρχικά των ονομάτων τους.

Σχήμα 6.1. Ron Rivest, Adi Shamir και Leonard Adleman. Τα παρόντα έργα αποτελούν κοινό κτήμα (public domain). Πηγή: Wikimedia Commons 2 3

Για την κατασκευή του συστήματος ακολουθούμε τα παρακάτω βήματα:

1. Επιλέγουμε δύο μεγάλους πρώτους p, q και υπολογίζουμε το γινόμενό τους $n = p \cdot q$.
2. Υπολογίζουμε το $\phi(n) = (p-1)(q-1)$.
3. Επιλέγουμε ένα στοιχείο a πρώτο προς το $\phi(n)$ και επιπλέον υπολογίζουμε και τον αντίστροφό του b ώστε $ab \equiv 1 \mod \phi(n)$.

4. Δημοσιοποιούμε τα n, b, ενώ τα a, p, q τα κρατάμε μυστικά.

Η συνάρτηση κρυπτογράφησης για κάποιον που θέλει να μας στείλει κάποιο μήνυμα είναι η

$$e_k(x) \equiv x^b \mathrm{mod} n.$$

Για να αποκρυπτογραφήσουμε το μήνυμα που μας έστειλαν χρησιμοποιούμε την συνάρτηση

$$d_k(y) \equiv y^a \mathrm{mod} n.$$

Θα πρέπει να αποδείξουμε ότι

$$d_k(e_k(x)) = x \qquad \text{για κάθε } x \in \mathbb{Z}_n.$$

Πράγματι, αν $(x, n) = 1$, τότε το Θεώρημα του Euler δίνει

$$x^{\phi(n)} \equiv 1 \mathrm{mod} n.$$

Επομένως

$$d_k(e_k(x)) \equiv d_k(x^b) = x^{ab} \mathrm{mod} n.$$

Γράφουμε $ab = 1 + \phi(n)t$ με $t \in \mathbb{Z}$, οπότε

$$d_k(e_k(x)) \equiv x^{1+\phi(n)t} \equiv x(x^{\phi(n)})^t \equiv x \mathrm{mod} n.$$

Ακόμα και όταν $(x, n) > 1$ ισχύει το ίδιο. Επειδή $n = pq$ αν $(x, n) > 1$, τότε $x = c \cdot p$ ή $x = c \cdot q$ με $(c, pq) = 1$ ($x < pq = n$).

Επειδή $(c, n) = 1$ έχουμε ότι $c^{ab} = c$. Θα εξετάσουμε τον παράγοντα που δεν είναι πρώτος προς τον n. Μπορούμε να υποθέσουμε ότι $x = p$. Θα αποδείξουμε

$$p^{ab} = p \mathrm{mod} pq.$$

Η τελευταία ισοδυναμία ισχύει ακριβώς τότε όταν

$$p^{ab-1} \equiv 1 \mathrm{mod} q,$$

δηλαδή ακριβώς τότε όταν

$$p^{\phi(n)t} \equiv 1 \mathrm{mod} q.$$

Η τελευταία όμως ισχύει, διότι

$$p^{q-1} \equiv 1 \mathrm{mod} q,$$

οπότε και

$$\left(p^{q-1}\right)^{(p-1)t} \equiv 1 \mathrm{mod} q.$$

Παρατήρηση Αν ο n δεν είναι γινόμενο δύο διαφορετικών μεταξύ τους πρώτων αριθμών, δεν ισχύει η παραπάνω σχέση.

Παρατήρηση Το κείμενο θα πρέπει να κωδικοποιηθεί και να σταλεί ως ένας αριθμός. Αν υλοποιήσουμε τον αλγόριθμο με τέτοιο τρόπο ώστε να στέλνουμε έναν-έναν χαρακτήρα, τότε το μήνυμα μπορεί να αποκρυπτογραφηθεί με μεθόδους στατιστικής ανάλυσης.

Παράδειγμα Ας πάρουμε $p = 47$ και $q = 59$.

$$n = p \cdot q = 47 \cdot 59 = 2773, \quad \phi(n) = 2668.$$

Επιλέγουμε $b = 17$, $(17, 2668) = 1$. Λύνουμε την ισοδυναμία

$$17x \equiv 1 \mathrm{mod} 2668$$

και βρίσκουμε $a = 157$. Υποθέτουμε ότι θέλουμε να κρυπτογραφήσουμε το μήνυμα “Its all go”. Το χωρίζουμε σε ζευγάρια.

Πίνακας 6.1: Παράδειγμα RSA

IT	S	AL	L	GO
0920	1900	0112	1200	0715

Κωδικοποίηση

$$0920^{17} \equiv 0948 \text{mod} 2713$$

Αποκρυπτογράφηση

$$948^{157} \equiv 920 \text{mod} 2273$$

και το 920 αντιστοιχεί στο "IT". Ομοίως και τα υπόλοιπα.

Παράδειγμα Ο παρακάτω κώδικας στο Sage δημιουργεί ένα κλειδί με b το πλήθος bits.

Κατασκευάζουμε το κλειδί με την παρακάτω συνάρτηση που έχει ως όρισμα τον αριθμό των bits και σαν έξοδο δίνει τα a, b, n.

```
def rsa(bits):
    proof = (bits <= 1024)
    p = next_prime(ZZ.random_element(2**(bits//2+1)),
            proof=proof)
    q = next_prime(ZZ.random_element(2**(bits//2+1)),
            proof=proof)
    n = p*q
    phi_n = (p-1)*(q-1)
    while True:
        a = ZZ.random_element(1,phi_n)
        if gcd(a,phi_n) == 1: break
    b = lift(Mod(a,phi_n)^(-1))
    return a, b, n
```

Οπότε δίνοντας την εντολή

```
a,b,n=rsa(1024)
a,b,n
(850800699260606227843543737300910793286812004655778 2\
6662094506114341835718976174637438302714149440115354 7\
7170711981887196167636192114112584863779279170736562 5\
4151644524474585781404137314336540911073317538412265 5\
6127965830971482786281784267594229701747323150326820 1\
0019407048403523254370167214196792976540 5,
6627429510652216285446576522632246749827406801354944 1\
8308363552683927059130010260051855714895295142159825 8\
2469570973862819631967198379553992223417142706673663 9\
3576071701552052185844904742688500473749510256290413 6\
0587814208898758392826542264350587107301802379830401 9\
```

```
228775726320792656679111243034913581893 3,
160909042362832763257889313851320177172790362180687 23\
568373356047650922977346344599237817878612244419177 89\
468364810973018146602286153750580251683257758022991 27\
660095891358163272132226501112074188110691820809051 45\
367295439559695334501493540916002651318147192645519 34\
398412523360424546555324911343278890922 99)
```

Καταλήγουμε στα επιθυμητά a, b, n. Το κλειδί που σχηματίστηκε παραπάνω δεν μπορεί να παραγοντοποιηθεί (σε εύλογο χρονικό διάστημα), με την εντολή

```
factor(n)
```

Παραθέτουμε τις επόμενες δύο συναρτήσεις οι οποίες μετατρέπουν ακολουθίες γραμματοσυμβόλων σε ASCII σε κρυπτογραφημένο μήνυμα. Τα σύμβολα ASCII χρειάζονται 256 ψηφία, οπότε στην πραγματικότητα δουλεύουμε σε ένα αριθμητικό σύστημα με βάση το 256.

```
def encode(s):
    s = str(s)
    return sum(ord(s[i])*256^i for i in range(len(s)))

def decode(n):
    n = Integer(n)
    v = []
    while n != 0:
        v.append(chr(n % 256))
        n //= 256     # this replaces n by floor(n/256)
    return ''.join(v)
```

Έτσι για να στείλουμε το μήνυμα “How from here morning morning?” δίνουμε

```
m=encode('How from here morning morning?'); m
437598522078581712110088947734419441411953466611 0312\
30743291695793139528
```

Ενώ η αποκρυπτογράφηση γίνεται:

```
decode(437598522078581712110088947734419441411953466 61\
10312307432916957931395 28)
'How from here morning morning?'
```

Interactive

6.1.2. Ψηφιακή υπογραφή με χρήση RSA. Αν θέλουμε να υπογράψουμε ένα μήνυμα, ώστε ο παραλήπτης να μπορεί να επιβεβαιώσει ότι είμαστε πράγματι εμείς και όχι κάποιος κακόβουλος ενδιάμεσος ο οποίος παρουσιάζεται σαν να είμαστε εμείς, μπορούμε να το κάνουμε με τον εξής τρόπο, χρησιμοποιώντας το ιδιωτικό μας κλειδί (n, a) αποστέλοντας το

$$s = m^a \mathrm{mod} n$$

Ο παραλήπτης του μηνύματος και της υπογραφής μας υπολογίζει την τιμή s^b χρησιμοποιώντας το δημόσιο κλειδί και το συγκρίνει με το m. Αυτή η μέθοδος υπογραφής έχει μια παγίδα όπως θα δούμε στη συνέχεια.

6.1.3. Ασφάλεια. Ο αλγόριθμος θεωρείται από τους πλέον ασφαλείς. Κανείς δεν ξέρει αν υπάρχει αλγόριθμος (μη δημοσιευμένος) που να παραγοντοποιεί σε πολυωνυμικό χρόνο μεγάλους αριθμούς. Το μεγαλύτερο πρόβλημα είναι η κακή χρήση του αλγορίθμου.

Ας υποθέσουμε ότι υποκλέπτουμε το κρυπτογραφημένο μήνυμα

$$m^b$$

και προφανώς γνωρίζουμε και το δημόσιο κλειδί (n, b) με το οποίο κρυπτογραφήθηκε, αλλά όχι το κρυπτογραφημένο μήνυμα. Κρυπτογραφούμε το κρυπτογραφημένο μήνυμα ξανά με το δημόσιο κλειδί. Επαναλαμβάνουμε τη διαδικασία κρυπτογράφησης πολλές φορές, δηλαδή υπολογίζουμε το

$$m^{b^j} \mathrm{mod} n$$

Κάποια στιγμή (όταν $b^{j+1} \equiv 1 \mathrm{mod} \phi(n)$) θα πάρουμε το m^b, οπότε το μήνυμα θα είναι το b^{j-1}.

Ας χρησιμοποιήσουμε την εντολή rsa που ορίσαμε παραπάνω για να φτιάξουμε ένα μικρό κλειδί.

```
a,b,n =rsa(10); a,b,n
(2947, 1123, 3599)
```

Ας υποθέσουμε ότι το μήνημά μας είναι ο αριθμός 1234. Το κρυπτογραφούμε

```
m=1234
Mod(m^b,n)
746
```

Και τώρα επαναλαμβάνουμε τη διαδικασία της κρυπτογράφησης, γνωρίζουμε το "κρυπτογραφημένο μήνυμα" 746 και το δημόσιο κλειδί $(n, b) = (3559, 1123)$.

```
m1=746
for i in range(28):
    m1=Mod(m1^b,n)
    i,m1

(1, 3491)
(2, 3064)
(3, 1112)
(4, 624)
(5, 2332)
(6, 136)
```

```
(7, 2698)
(8, 2515)
(9, 319)
(10, 868)
(11, 502)
(12, 2576)
(13, 2820)
(14, 14)
(15, 3369)
(16, 929)
(17, 1783)
(18, 2393)
(19, 807)
(20, 2088)
(21, 1722)
(22, 3430)
(23, 563)
(24, 1173)
(25, 3247)
(26, 1295)
(27, 1234)
(28, 746)
```

Στην 28η επανάληψη εμφανίστηκε το αρχικό κρυπτογραφημένο μήνυμα, άρα το ακρυπτογράφητο είναι το προηγούμενο -το 1234! Φυσικά η μέθοδος αυτή χρειάζεται αρκετό χρόνο αν το b έχει μεγάλη τάξη mod $\phi(n)$, κάτι που πρέπει να πάρουμε υπόψιν σε έναν καλό σχεδιασμό του RSA.

Κακή Χρήση

Έχουμε στην κατοχή μας δυο κλειδιά της μορφής (n, b_1), (n, b_2) και δύο κρυπτογραφήσεις του ίδιου μηνύματος m με τα κλειδιά αυτά, δηλαδή γνωρίζουμε (κρυφακούγοντας σε ένα δίκτυο)

$$m_1 = m^{b_1} \mod n$$

και

$$m_2 = m^{b_2} \mod n$$

Αν επιπλέον $(b_1, b_2) = 1$ τότε υπολογίζουμε $x, y \in \mathbb{Z}$ ώστε

$$xb_1 + yb_2 = 1$$

και συνεπώς μπορούμε υπολογίζοντας το

$$m_1^x \cdot m_2^y = m^{b_1 x + b_2 y} = m \mod n$$

να υπολογίσουμε το m χωρίς να παραγονοποιήσουμε το n.

Μικρό b

Αν το b είναι σχετικά μικρό (έστω $b = 3$), τότε για μικρές τιμές του m (αρκεί $m < n^{1/b}$), τότε το $c = m^b < n$, δηλαδή είναι σαν να έχουμε κάνει πράξεις στους ακέραιους. Συνεπώς μπορούμε να υπολογίσουμε την b-ρίζα του c και να υπολογίσουμε το m.

Ένας τρόπος να οδηγηθούμε στην κατάσταση αυτή είναι να έχουμε το ίδιο μήνυμα κρυπτογραφημένο και σταλμένο σε πολλούς (έστω r το πλήθος τους) παραλλήπτες οι οποίοι έχουν τον ίδιο εκθέτη b αλλά διαφορετικά $n_1, \ldots, n_r$. Τότε με τη βοήθεια του Θεωρήματος του Κινέζου μπορούμε να υπολογίσουμε το

$$m^b \mathrm{mod}[n_1, \ldots, n_r]$$

και τώρα έχουμε σημαντικές ελπίδες το

$$c = m^b < [n_1, \ldots n_r]$$

ώστε να χρησιμοποιήσουμε την μέθοδο της b-ρίζας.

Ίδιο κλειδί για υπογραφή

Ας υποθέσουμε ότι ο Παναγιώτης ο οποίος έχει ιδιωτικό κλειδί (n, a) και δημόσιο κλειδί (n, b) βάζει εύκολα την υπογραφή του σε ό,τι μήνυμα του δώσουμε. Αν κρυφακούσουμε ένα κρυπτογραφημένο μήνυμα x με παραλήπτη τον Παναγιώτη, τότε μπορούμε να ζητήσουμε από τον Παναγιώτη να μας υπογράψει το $r^b \cdot c$, όπου $(r, n) = 1$. Τότε ο Παναγιώτης μας επιστρέφει το

$$(r^b \cdot c)^a = r \cdot m \mathrm{mod} n$$

όπου m είναι το αρχικό μήνυμα (άγνωστο σε εμάς) ώστε $m^b = c$. Πολλαπλασιάσαμε με τον r αντί να στείλουμε το c σκέτο στον Παναγιώτη για υπογραφή, γιατί το μήνυμα $r \cdot m$ δεν είναι άμεσα κατανοητό ώστε να καταλάβει ο Παναγιώτης ότι τον εξαπατούμε για να μας αποκρυπτογραφήσει ο ίδιος το μήνυμα που προορίζεται για αυτόν!

Προφανώς αφού το r είναι αντιστρέψιμο μπορούμε εύκολα να βρούμε το m.

Με λίγα λόγια δεν πρέπει να χρησιμοποιούμε το ίδιο κλειδί για υπογραφή και αποκρυπτογράφηση και γενικότερα να προσέχουμε πού βάζουμε την υπογραφή μας!

6.1.4. Ύψωση σε δύναμη. Η κρυπτογράφηση RSA απαιτεί τον υπολογισμό της ύψωσης σε δύναμη modulo n. Στην περίπτωση που γνωρίζουμε την παραγοντοποίηση του n, θα μπορούσαμε να χρησιμοποιήσουμε τεχνικές όπως το θεώρημα του Euler

$$x^{\phi(n)} \equiv 1 \mathrm{mod} n$$

προκειμένου να απλοποιήσουμε τις πράξεις μας. Η παραγοντοποίηση του n και συνεπώς και η τιμή του $\phi(n)$ δεν είναι γνωστή στον αποστολέα.

Σε κάθε περίπτωση ένας τρόπος για να περιορίσουμε δραστικά το πλήθος των πράξεων που απαιτούνται όπως και τη μνήμη είναι να γράψουμε τον εκθέτη σε δυαδική μορφή:

$$e = \sum_{i=0}^{r-1} a_i 2^i$$

και στη συνέχεια να υπολογίζουμε το

$$b^e \equiv b^{(\sum_{i=0}^{r-1} a_i 2^i)} = \prod_{i=0}^{r-1} \left(b^{2^i}\right)^{a_i}$$

Για παράδειγμα ας υπολογίσουμε το

$$7^{345678912} \mathrm{mod} 18165151$$

Ο υπολογισμός της δυαδικής μορφής γίνεται ως εξής: Αν e περιττός $a_0 = 1$, αλλιώς $a_0 = 0$. Αντικαθιστούμε το e με το $\left[\frac{e}{2}\right]$ και συνεχίζουμε όμοια μέχρι να φτάσουμε στο 0. Στο παράδειγμά μας,

$$541043 = (10001110100000100001)_2.$$

Στη συνέχεια υψώνουμε διαδοχικά στο τετράγωνο

$$\begin{array}{rcrl}
7 & = & 7 & \mod 18165151 \\
7^2 & = & 49 & \mod 18165151 \\
7^{2^3} & = & 2401 & \mod 18165151 \\
7^{2^4} & = & 5764801 & \mod 18165151 \\
7^{2^5} & = & 4796913 & \mod 18165151 \\
7^{2^6} & = & 14438188 & \mod 18165151 \\
7^{2^7} & = & 16179105 & \mod 18165151 \\
7^{2^8} & = & 15991127 & \mod 18165151 \\
7^{2^9} & = & 7879037 & \mod 18165151 \\
7^{2^{10}} & = & 2156379 & \mod 18165151 \\
7^{2^{11}} & = & 543208 & \mod 18165151 \\
7^{2^{12}} & = & 218420 & \mod 18165151 \\
7^{2^{13}} & = & 5609874 & \mod 18165151 \\
7^{2^{14}} & = & 16317151 & \mod 18165151 \\
7^{2^{15}} & = & 1116547 & \mod 18165151 \\
7^{2^{16}} & = & 2890079 & \mod 18165151 \\
7^{2^{17}} & = & 2214629 & \mod 18165151 \\
7^{2^{18}} & = & 9002792 & \mod 18165151 \\
7^{2^{19}} & = & 12145310 & \mod 18165151 \\
7^{2^{20}} & = & 8503586 & \mod 18165151
\end{array}$$

Το ζητούμενο αποτέλεσμα προκύπτει πολλαπλασιάζοντας τις δυνάμεις που εμφανίζονται με 1 στο δυαδικό ανάπτυγμα:

$$7 \cdot 7^{2^5} \cdot 7^{2^{11}} \cdot 7^{2^{13}} \cdot 7^{2^{14}} \cdot 7^{2^{15}} \cdot 7^{2^{18}} \cdot 7^{2^{19}} = 11256737.$$

6.1.5. El Gammal. Το σύστημα αυτό αναπύχθηκε από τον T. El Gamal (ElGamal 1984) Στη γενική περίπτωση του συστήματος έχουμε μια κυκλική ομάδα G τάξης q η οποία παράγεται από το στοιχείο g. Για την ασφάλεια του κρυπτοσυστήματος θα πρέπει να απαιτήσουμε η ομάδα να πληρεί μια σειρά από προϋποθέσεις ώστε το κρυπτοσύστημα να είναι ανθεκτικό στις γνωστές επιθέσεις. Περισσότερα θα πούμε στη συνέχεια.

Έχουμε δύο πρόσωπα λοιπόν -τον Παναγιώτη και τη Σουζάνα- που θέλουν να ανταλλάξουν ένα μήνυμα.

1. Η Σουζάνα διαλέγει ένα x στο σύνολο $\{1, \ldots, q-1\}$.
2. Στην συνέχεια υπολογίζει το $h = g^x$.
3. Δημοσιεύει ο h μαζί με μία περιγραφή της ομάδας G, q, g ως το δημόσιο κλειδί της. Το x το κρατάει μυστικό και είναι το ιδιωτικό κλειδί της.

Αν ο Παναγιώτης θέλει να στείλει ένα μήνυμα $m \in G$ στην Σουζάνα τότε

1. διαλέγει ένα y και υπολογίζει το $c_1 = g^y$.
2. Υπολογίζει το $s = h^y$.
3. Υπολογίζει το $c_2 = m \cdot s$.

4. Ο Παναγιώτης στέλνει το κρυπτογραφημένο κείμενο

$$(c_1, c_2) = (g^y, m \cdot h^y) = (g^y, m \cdot (g^x)^y)$$

στη Σουζάνα.

Αποκρυπτογράφηση

1. Η Σουζάνα υπολογίζει το $s = c_1^x$
2. Στην συνέχεια υπολογίζει

$$c_2 \cdot s^{-1} = m(g^x)^y ((g^y)^x)^{-1} = m$$

το οποίο είναι το αρχικό μήνυμα.

Σχήμα 6.2. T. El Gamal,Δημιουργός A. Klink, Το παρόν έργο αποτελεί κοινό κτήμα (public domain). Πηγή: Wikimedia Commons

Υλοποίηση Η ομάδα G είναι συνήθως

1. η πολλαπλασιαστική ομάδα ενός σώματος $G = \mathbb{F}^*_{p^f}$ με απλούστερη δυνατή περίπτωση την $f = 1$.
2. η ομάδα των σημείων μιας ελλειπτικής καμπύλης (τις ελλειπτικές καμπύλες θα τις ορίσουμε σε επόμενο κεφάλαιο)

6.1.6. Το πρόβλημα του διακριτού λογαρίθμου. Για να ανακαλύψει κάποιος το ιδιωτικό κλείδι x θα πρέπει από το g^x να μπορέσει να υπολογίσει το x. Θα πρέπει να επιλέξει την ομάδα G με τέτοιο τρόπο ώστε το πρόβλημα αυτό να είναι δύσκολο να επιλυθεί.

6.1.1 Ορισμός:
Το πρόβλημα του διακριτού λογαρίθμου σε μία κυκλική ομάδα G *με γεννήτορα* g *είναι για δεδομένο* $x \in G$ *να υπολογιστεί ο εκθέτης* $k \in \mathbb{N}$, *ώστε* $g^k = x$.

Παρατήρηση: Για τον υπολογισμό του "συνεχούς λογαρίθμου" μπορούμε να χρησιμοποιήσουμε το γεγονός ότι η εκθετική συνάρτηση $e^x : \mathbb{R} \to \mathbb{R}^*$ είναι γνήσια αύξουσα, και να ακολουθήσουμε μια ακολουθία δοκιμών: Έστω ότι $y \in \mathbb{R}$ και θέλουμε να υπολογίσουμε το $x \in \mathbb{R}$ ώστε $e^x = y$. Διαλέγουμε ένα πραγματικό $x_1 \in \mathbb{R}$ και υπολογίζουμε το e^{x_1}. Αν αυτό είναι μικρότερο του y δοκιμάζουμε με $x_1 < x_2$ μέχρι να βρούμε $y < x_2$ (ανάλογη διαδικασία ακολουθούμε και στην περίπτωση που $e^{x_1} > y$). Στη συνέχεια δοκιμάζουμε με το ενδιάμεσο σημείο $x_3 = \frac{x_2+x_1}{2}$ και αν $e^{x_3} > y$ θεωρούμε το $x_4 = x_1 + x_3 2$, ενώ αν $e^{x_3} < y >$ θεωρούμε το $x_4 = \frac{x_3+x_4}{2}$, και συνεχίζοντας με αυτόν τον τρόπο κατασκευάζουμε μια ακολουθία ρητών που να συγκλίνει στο x.

Αυτή η διαδικασία δεν μπορεί να ακολουθηθεί, για παράδειγμα στην περίπτωση $G = \mathbb{F}_p$, αφού δεν υπάρχει κάποια ανισότητα να μας καθοδηγήσει.

Η πιο απλή μέθοδος θα ήταν (αφού έχουμε ένα πεπερασμένο πρόβλημα σε μία πεπερασμένη ομάδα) να αρχίσουμε να υπολογίζουμε δυνάμεις του γεννήτορα g μέχρι να υπολογιστεί το $g^k = y$.

Για παράδειγμα ας δουλέψουμε modulo 73 (που παρεμπιπτόντως είναι ο Τσακ Νόρις των πρώτων!).

Υπολογίζουμε πρώτα μια πρωταρχική ρίζα modulo 73 για παράδειγμα το 5

```
a=primitive_root(73);a
5
```

Στη συνέχεια δοκιμάζουμε να βρούμε k, ώστε $5^k \equiv 37 \mathrm{mod} 73$.

```
for i in range(1,72):
    i,Mod(5^i,73)

(1, 5)
(2, 25)
(3, 52)
(4, 41)
(5, 59)
(6, 3)
(7, 15)
(8, 2)
(9, 10)
(10, 50)
(11, 31)
(12, 9)
(13, 45)
(14, 6)
(15, 30)
(16, 4)
```

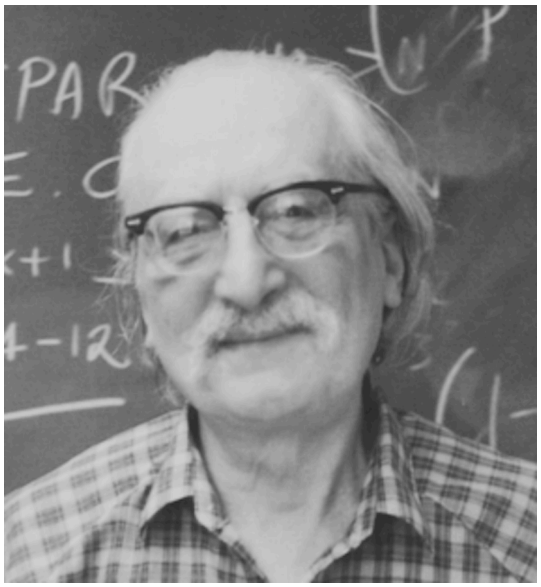
```
(17, 20)
(18, 27)
(19, 62)
(20, 18)
(21, 17)
(22, 12)
(23, 60)
(24, 8)
(25, 40)
(26, 54)
(27, 51)
(28, 36)
(29, 34)
(30, 24)
(31, 47)
(32, 16)
(33, 7)
(34, 35)
(35, 29)
(36, 72)
(37, 68)
(38, 48)
(39, 21)
(40, 32)
(41, 14)
(42, 70)
(43, 58)
(44, 71)
(45, 63)
(46, 23)
(47, 42)
(48, 64)
(49, 28)
(50, 67)
(51, 43)
(52, 69)
(53, 53)
(54, 46)
(55, 11)
(56, 55)
(57, 56)
(58, 61)
(59, 13)
(60, 65)
```

```
(61, 33)
(62, 19)
(63, 22)
(64, 37)
(65, 39)
(66, 49)
(67, 26)
(68, 57)
(69, 66)
(70, 38)
(71, 44)
```

Η ζητούμενη τιμή εμφανίστηκε στο $k = 64$, σχετικά προς το τέλος. Δεν υπάρχει κανένας έλεγχος που θα εμφανιστεί ο ζητούμενος αριθμός.

6.2. Baby step giant step

Η μέθοδος αυτή προτάθηκε από τον Daniel Shanks (Shanks and Daniel 1971) και αφορά την επίλυση του προβλήματος του διακριτού λογαρίθμου.



Σχήμα 6.3. Daniel Shanks, Πηγή: Wikimedia Commons

Θεωρούμε μια κυκλική ομάδα G η οποία έχει τάξη n και γεννήτορα g. Για ένα τυχαίο στοιχείο $h \in G$ προσπαθούμε να βρούμε x ώστε

$$g^x = h.$$

Ο αλγόριθμος Baby step giant step βασίζεται στο να γράψουμε το x ως $x = im + j$ με $m = \lceil \sqrt{n} \rceil$ και $0 \leqslant i < m$ και $0 \leqslant j < m$, οπότε η παραπάνω σχέση γράφεται στη μορφή:

$$h(g^{-m})^i = g^j.$$

Ο αλγόριθμος υπολογίζει ένα κατάλογο των τιμών g^j για διάφορες τιμές του j. Στη συνέχεια σταθεροποιεί ένα m και δοκιμάζει τιμές του i στο αριστερό μέρος της τελευταίας εξίσωσης, κάνοντας χρήση των προϋπολογισμένων τιμών του g^j.

Περισσότερο αναλυτικά τα βήματα του αλγορίθμου είναι:

1. Θέτουμε $m = \lceil n \rceil$
2. Για όλα τα j με $0 \leqslant j < m$ υπολόγισε όλα τα ζευγάρια (j, g^j) και αποθήκευσέ τα σε έναν πίνακα.
3. Υπολόγισε το g^{-m}
4. Θέτουμε $c \to h$.
5. Για i να τρέχει από 0 μέχρι $m - 1$
   1. Έλεγχος αν το c είναι η δεύτερη συντεταγμένη ενός ζευγαριού που ήδη υπολογίσαμε
   2. Αν ναι επιστρέφουμε $x = im + j$
   3. Αν όχι θέτουμε $c \to cg^{-m}$ και ξαναεκτελούμε από το βήμα 5.

Παράδειγμα Θέλουμε να λύσουμε με τη μέθοδο baby step giant step στην ομάδα $\mathbb{Z}/73\mathbb{Z}$ το πρόβλημα $5^x = 37 \mathrm{mod} 73$.

Θέτουμε $m = \lceil \sqrt{73} \rceil = 9$. Υπολογίζουμε όλες τις δυνάμεις 5^j για $j = 0, \ldots, 9$

Πίνακας 6.2: Πίνακας δυνάμεων του 5

j	0	1	2	3	4	5	6	7	8	9
5^j	1	5	25	52	41	59	3	15	2	10

Στη συνέχεια υπολογίζουμε τις τιμές $37(5^{-9i})$ για $i = 0, \ldots, 9$

Πίνακας 6.3: Πίνακας των τιμών $37(5^{-9i})$ για $i = 0, \ldots, 9$

i	0	1	2	3	4	5	6	7	8	9
$37(5^{-9i})$	37	11	23	68	36	62	50	5	37	11

και παρατηρούμε ότι $5 = 5^1 = 37 * (5^{-9*7})$ συνεπώς $x = im + j = 7 \cdot 9 + 1 = 64$, όπως είχαμε υπολογίσει και με τη μέθοδο της "ωμής βίας".

Προκειμένου να μπορέσουμε να μετρήσουμε τη βελτίωση του αλγορίθμου σε σχέση με αυτόν της "ωμής βίας" εισαγάγουμε τις δύο παρακάτω συναρτήσεις στο Sage:

```
def baby_giant(h,g,p):
    baby = [1]
    giant = [h]
    n = 1+ floor(sqrt(p -1))

    for i in range(1,n):
        baby.append(Mod(baby[i -1]*g,p))
```

```
    g = Mod(g, p)^-n
    for j in range(1,n):
    giant.append(Mod(giant[j-1]*g,p))

    for inters in set(baby).intersection(set(giant)):
        print  baby.index(inters)+n*giant.index(inters)

def br_fr (h,g,p):
    for x in range (p -1):
        if Mod (g , p )^ x == Mod (h , p ):
            print x
            break
```

Παρατηρήστε ότι η baby Giant είναι 161 φορές γρηγορότερη από τη μέθοδο της ωμής βίας.

```
time baby_giant (7 ,3 ,2^19 -1)
time br_fr (7,3,2^19-1)
243983
Time: CPU 0.01 s, Wall: 0.01 s
243983
Time: CPU 1.61 s, Wall: 1.61 s
```

Interactive

Βιβλιογραφία

ElGamal, Taher. 1984. “A Public Key Cryptosystem και a Signature Scheme Based on Discrete Logarithms.” In *Advances in Cryptology*, 10–18. Lecture Notes in Computer Science. Springer Berlin Heidelberg. doi:10.1007/3-540-39568-7_2.

Menezes, A.J., P.C. van Oorschot, και S.A. Vanstone. 1996. *Handbook of Applied Cryptography*. Discrete Mathematics και Its Applications. CRC Press. https://books.google.gr/books?id=nSzoG72E93MC.

Shanks, Daniel, και Shanks Daniel. 1971. “Class Number, a Theory of Factorization, και Genera.” *Proceedings of Symposia in Pure Mathematics*. doi:10.1090/pspum/020/0316385.

Αντωνιάδης, Ι., και Α. Κοντογεώργης. 2015. *Θεωρία Αριθμών Και Εφαρμογές*. Εκδόσεις Κάλλιπος.

7 Ελλειπτικές Καμπύλες

7.1. Ιστορικά στοιχεία

Οι ελλειπτικές καμπύλες είναι καμπύλες οι οποίες οφείλουν το όνομά τους στο πρόβλημα της εύρεσης μήκους τόξου πάνω σε ελλείψεις. Το πρόβλημα αυτό ανάγεται σε υπολογισμό ολοκληρωμάτων της μορφής:

$$\int \frac{1}{\sqrt{x^2 + ax + b}} dx.$$

Ο υπολογισμός των παραπάνω ολοκληρωμάτων ήταν ένα από τα κύρια προβλήματα της ανάλυσης τον προπερασμένο αιώνα και πρώτης τάξεως Μαθηματικοί όπως οι Euler, Weierstrass, Abel, Jacobi ασχολήθηκαν μαζί τους.

Στην πραγματικότητα το παραπάνω ολοκλήρωμα οδηγεί στη μελέτη δύο (μιγαδικών) συναρτήσεων x, y οι οποίες ικανοποιούν μια εξίσωση της μορφής

$$y^2 = x^3 + ax + b$$

ή ισοδύναμα τη μελέτη των μιγαδικών αριθμών $(x, y) \in \mathbb{C}^2$ που ικανοποιούν την παραπάνω εξίσωση. Η σύγχρονη μελέτη του παραπάνω προβλήματος εντάσσεται στα πλαίσια των επιφανειών Riemann.

Οι τεχνικές που αναπτύχθηκαν στα πλαίσια του παραπάνω προβλήματος μπορεί να χρησιμοποιηθούν για κυβικές καμπύλες που ορίζονται πάνω από οποιοδήποτε σώμα και για Διοφαντικά προβλήματα. Σκοπός αυτού του κεφαλαίου είναι να δώσουμε μια όσο το δυνατόν στοιχειώδη μελέτη ελλειπτικών καμπυλών πάνω από πεπερασμένα σώματα $\mathbb{F}_q$. Ο αναγνώστης μπορεί να συμβουλευτεί για περισσότερες πληροφορίες τα βιβλία (Αντωνιάδης 1999), (Milne 2006), (Blake, Seroussi, and Smart 1999) και στο (Silverman and Tate 1992).

7.2. Ορισμοί

7.2.1 Ορισμός:
Θεωρούμε ένα σώμα K *και στο σύνολο των διατεταγμένων τριάδων* $K^3 - (0,0,0)$ *ορίζουμε τη σχέση ισοδυναμίας* $(x_1, y_1, z_1) \sim (x_2, y_2, z_3)$ *αν και μόνο αν υπάρχει* $\lambda \in K^*$ *με* $(x_1, y_1, z_1) = \lambda(x_2, y_2, z_3)$.

Το σύνολο πηλίκο θα το ονομάζουμε προβολικό επίπεδο και θα το συμβολίζουμε με

$$\mathbb{P}^2(K) = \frac{K^3 - (0,0,0)}{\sim}.$$

Το προβολικό επίπεδο μπορούμε να το ταυτίσουμε με το σύνολο των μη-τετριμμένων ευθειών στον χώρο K^3. Θα συμβολίζουμε την κλάση ισοδυναμίας του $(x, y, z) \neq (0, 0, 0)$ με $[x : y : z]$. Παρατηρούμε ότι τα σημεία $[x, y, 1]$ είναι σε ένα προς ένα αντιστοιχία με το επίπεδο K^2, ενώ τα σημεία $[x, y, 0]$ αποτελούν μια ευθεία που την ονομάζουμε την ευθεία στο άπειρο.

Για κάθε πολυώνυμο $f(x, y) \in K[x, y]$,

$$f = \sum_{i,j} a_{ij} x^i y^j$$

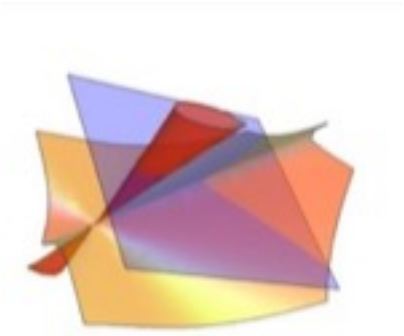
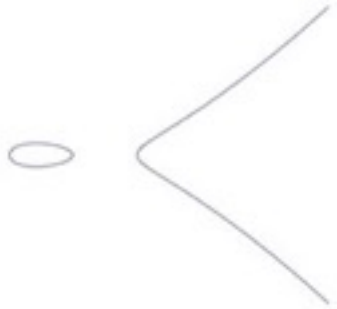
βαθμού n θα συμβολίζουμε με F το αντίστοιχο ομογενές πολυώνυμο

$$F = \sum_{i,j} a_{ij} x^i y^j z^{n-i-j}.$$

Τη διαδικασία αυτή θα την ονομάζουμε *ομογενοποίηση*. Γεωμετρικά όταν δουλεύουμε πάνω από το σώμα των πραγματικών αριθμών το ομογενοποιημένο σύνολο αντιστοιχεί στον κώνο που γράφουν οι ευθείες που περνούν από το σημείο $(0, 0, 0)$ και από ένα σημείο της καμπύλης $f(x, y), z = 1$.

Στο παρακάτω σχήμα έχει σχεδιαστεί ο κώνος μιας προβολικής καμπύλης (πορτοκαλί χρώμα) μαζί με το επίπεδο $z = 1$ (μπλε χρώμα) αλλά και η επίπεδη καμπύλη στο επίπεδο $z = 1$.

Πίνακας 7.1: Σύγκριση προβολικής και επίπεδης απεικόνισης ελλειπτικής καμπύλης.

$y^2z = x(x - z)(x - 2z)$	$y^2 = x(x - 1)(x - 2)$
	

Άσκηση: Πυθαγόρειες Τριάδες. Να βρεθούν οι ακέραιες λύσεις της εξίσωσης

$$x^2 + y^2 = z^2.$$

Λύση Παρατηρούμε ότι έχουμε ένα ομογενές πολυώνυμο βαθμού 2. Κάθε λύση $(x, y, z) \in \mathbb{Z}^3$ αντιστοιχεί σε μία λύση $X = x/z, Y = y/z \in \mathbb{Q}^2$. Οι ρητές λύσεις πάνω στον κύκλο μπορούν να υπολογιστούν ως εξής:

Θεωρούμε το σημείο $(-1, 0)$ το οποίο ικανοποιεί την εξίσωση του κύκλου $X^2 + Y^2 = 1$. Από το σημείο αυτό φέρνουμε την ευθεία $Y = \lambda(X + 1)$ η οποία τέμνει τον κύκλο στο σημείο $(-1, 0)$ αλλά και σε ένα ακόμα σημείο το οποίο μπορούμε να το υπολογίσουμε αντικαθιστώντας την τιμή του Y στην εξίσωση του κύκλου:

$$\lambda^2(X + 1)^2 + X^2 = 1 \Rightarrow (X + 1)(\lambda^2(X + 1) + X - 1) = 0$$

από όπου λογαριάζουμε ότι

$$X = \frac{1 - \lambda^2}{\lambda^2 + 1}, \qquad Y = \frac{2\lambda}{\lambda^2 + 1}.$$

Όσο το $\lambda = n/m$ διατρέχει τους ρητούς αριθμούς το ζευγάρι (X, Y) διατρέχει τις ρητές ρίζες της εξίσωσης του κύκλου και κατά συνέπεια (με απαλοιφή των παρονομαστών) καταλήγουμε στις ακέραιες ρίζες

$$(x, y, z) = (m^2 - n^2, 2nm, m^2 + n^2).$$

Στην πραγματικότητα κάθε φορά που έχουμε μια πυθαγόρεια τριάδα (x_0, y_0, z_0), παρατηρούμε ότι και κάθε ακέραιο πολλαπλάσιό της $(\kappa x_0, \kappa y_0, \kappa z_0)$ θα είναι πυθαγόρεια τριάδα.

Σχήμα 7.1. Βαβυλωνιακή επιγραφή με Πυθαγόρειες Τριάδες γνωστή ως Plimpton 322, Το παρόν έργο αποτελεί κοινό κτήμα (public domain). Πηγή: Wikimedia Commons

Η παραπάνω μέθοδος δούλεψε γιατί από το θεμελιώδες Θεώρημα της Άλγεβρας μία ευθεία και μια τετραγωνική εξίσωση τέμνονται σε δύο σημεία. Η κατάσταση αλλάζει στην περίπτωση που έχουμε τομές ευθειών με κυβικές καμπύλες.

7.2.2 Ορισμός:
Θεωρούμε ένα κυβικό πολυώνυμο της μορφής $x^3 + ax + b$ *με απλές ρίζες. Μια ελλειπτική καμπύλη υπέρ του σώματος* K *θα είναι το σύνολο των* $x, y \in K$ *που ικανοποιούν μια εξίσωση της μορφής:*

$$E : y^2 = x^3 + ax + b,$$

μαζί με ένα σημείο στο άπειρο $\mathcal{O}$*, ώστε το κυβικό πολυώνυμο* $x^3 + ax + b$ *να έχει απλές ρίζες. Η συνθήκη για τις απλές ρίζες μπορεί να εκφραστεί με το ότι* $16(4a^3 + 27b^2) \neq 0$.

Ισοδύναμα μπορούμε να αναζητήσουμε σημεία στο προβολικό επίπεδο $[x : y : z]$ τα οποία να ικανοποιούν την ομογενοποιημένη εξίσωση

$$E : y^2z = x^3 + axz^2 + bz^3.$$

Έστω τα σημεία $P = (x_1, y_1)$ και $Q = (x_2, y_2)$ επί της ελλειπτικής καμπύλης. Σχηματίζουμε την ευθεία L που ενώνει τα δύο αυτά σημεία. Η ευθεία τέμνει την ελλειπτική καμπύλη σε ένα τρίτο σημείο PQ. Από το σημείο PQ φέρνουμε την κάθετη ευθεία στον άξονα των x η οποία τέμνει την ελλειπτική καμπύλη στο σημείο $P + Q$. Το σημείο αυτό το ορίζουμε να είναι άθροισμα των σημείων P, Q.

Στην περίπτωση που θέλουμε να υπολογίσουμε το σημείο $P + P$, αντί να θεωρήσουμε τη χορδή όπως στην προηγούμενη περίπτωση, θεωρούμε την εφαπτομένη.

Στην περίπτωση που ένας προσθετέος είναι το σημείο στο άπειρο, θέτουμε $P + \mathcal{O} = P$, δηλαδή το σημείο στο άπειρο είναι το ουδέτερο της πράξης.

Ας υποθέσουμε ότι $P_1 = (x_1, y_1)$ και $P_2 = (x_2, y_2)$. Οι παραπάνω κανόνες πρόσθεσης μπορούν να εκφραστούν με τον εξής απλό τρόπο:

Ας υποθέσουμε ότι $P_1, P_2 \neq \mathcal{O}$.

- Αν $x_1 = x_2$ και $y_1 = -y_2$ θέτουμε $P_1 + P_2 = \mathcal{O}$. Δηλαδή συμμετρικά σημεία ως προς τον άξονα των x έχουν άθροισμα $\mathcal{O}$.
- Διαφορετικά θέτουμε

$$\lambda = (3x_1 + a)/(2y_1) \text{ αν } \quad P_1 = P_2$$

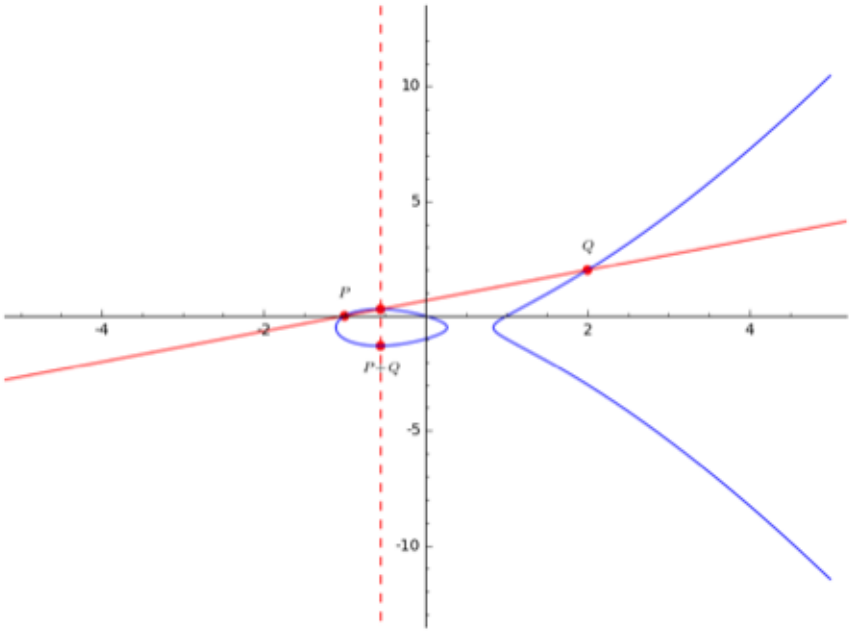
$$\lambda = (y_1 - y_2)/(x_1 - x_2) \text{ αν } \quad P_1 \neq P_2$$

Το σημείο $P_1 + P_2$ έχει συντεταγμένες (x_3, y_3) που δίνονται από τους τύπους:

$$(x_3, y_3) = (\lambda^2 - x_1 - x_2, -\lambda x_3 - y_1 + \lambda x_1)$$

Interactive

7.2.3 Θεώρημα:
Τα σημεία της ελλειπτικής καμπύλης με πράξη την πρόσθεση σημείων όπως ορίστηκε παραπάνω αποτελούν αβελιανή ομάδα.



Σχήμα 7.2. Πρόσθεση δύο σημείων της ελλειπτικής καμπύλης $y^2 + y = x^3 - x$

Απόδειξη Θα πρέπει να αποδείξουμε ότι η πράξη είναι αντιμεταθετική (προφανές), ότι το $\mathcal{O}$ είναι το ουδέτερο στοιχείο (εξ ορισμού) ότι κάθε στοιχείο έχει αντίστροφο (είναι το συμμετρικό ως προς τον άξονα των x) και ότι η πράξη είναι προσεταιριστική, δηλαδή

$$P + (Q + R) = (P + Q) + R.$$

Το τελευταίο είναι αρκετά δύσκολο να δειχτεί με τα στοιχειώδη εργαλεία που θέλουμε να χρησιμοποιήσουμε. Μπορούμε όμως να δώσουμε μία απόδειξη με "ωμή βία" χρησιμοποιώντας το πρόγραμμα sage.

7.3. Χρήση του Πακέτου Sage

Η ελλειπτική καμπύλη $y^2 = x^3 - 10x + 9$ στο sage ορίζεται ως:

```
E=EllipticCurve([3,4])
```

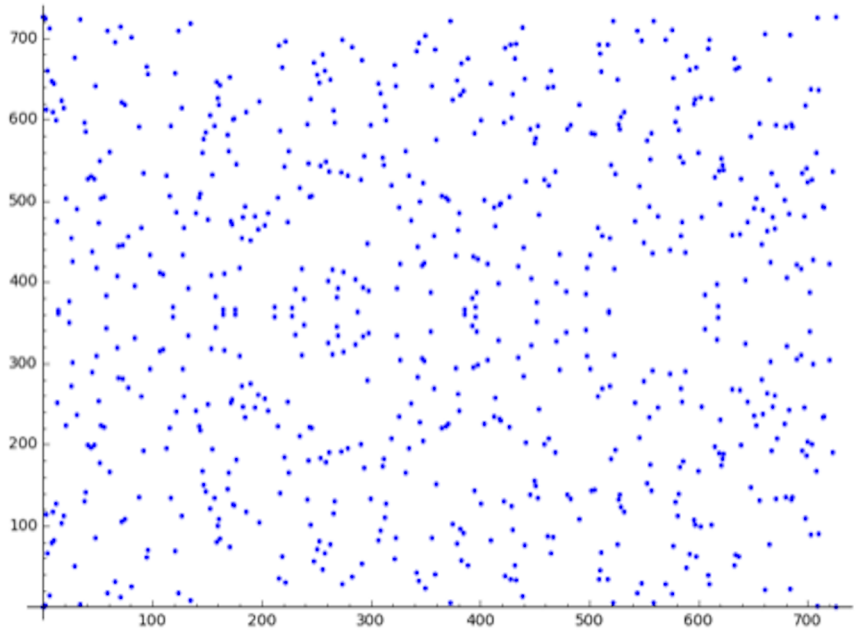
Ενώ για να δώσουμε σημεία επί αυτής αρκεί να δώσουμε τις συντεταγμένες τους.

```
P=E([0,3])
Q=E([1,0])
```

Το άθροισμα υπολογίζεται με τις εντολές

```
P+Q

3P+6Q
```



Σχήμα 7.3. Σχηματική απεικόνιση της ελλειπτικής καμπύλης $y^2 + y = x^3 - x$ στο σώμα $\mathbb{F}_{389}$

Interactive

7.4. Τάξεις Σημείων Ελλειπτικής Καμπύλης

Θεωρούμε μια ελλειπτική καμπύλη $E : y^2 = x^3 + ax + b$ ορισμένη στο σώμα K. Τα σημεία $(0, x)$ ανήκουν στην ελλειπτική καμπύλη αν και μόνο αν το x είναι ρίζα του πολυωνύμου $x^3 + ax + b$. Υπάρχουν τρία τέτοια σημεία, μετά από μια επέκταση του σώματος K. Μαζί με το ουδέτερο σημείο στο άπειρο σχηματίζουν μια ομάδα ισόμορφη με την $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Γενικά, αν επιλέξουμε ένα στοιχείο P στην E, μπορούμε να θεωρήσουμε όλες τις δυνάμεις nP για κάθε φυσικό αριθμό n. Ή θα έχουμε $nP = \mathcal{O}$ για κάποιο φυσικό αριθμό n οπότε το σημείο P θα έχει πεπερασμένη τάξη, ή διαφορετικά το σημείο θα έχει άπειρη τάξη και θα παράγει μια υποομάδα της ελλειπτικής καμπύλης ισόμορφη με την άπειρη κυκλική ομάδα $\mathbb{Z}$.

7.5. Το Θεώρημα Του Mordell

7.5.1 Θεώρημα:
Η ομάδα των σημείων $E(\mathbb{Q})$ *είναι μια πεπερασμένα παραγόμενη αβελιανή ομάδα. Δηλαδή*

$$E(\mathbb{Q})) = \mathbb{Z}^r \times \prod_{i=1}^{s} \frac{\mathbb{Z}}{n_i\mathbb{Z}}.$$

Στην πραγματικότητα μπορούμε να είμαστε περισσότερο ακριβείς για το κομμάτι της πεπερασμένης τάξης του $E(\mathbb{Q})$, αφού ισχύει το Θεώρημα του B. Mazur:

7.5.2 Θεώρημα:
Η ομάδα των σημείων πεπερασμένης τάξης σε μια ελλειπτική καμπύλη είναι ισόμοφη με μία από τις παρακάτω 15 ομάδες:

$$\frac{\mathbb{Z}}{N\mathbb{Z}}, \quad 1 \leqslant N \leqslant 10 \text{ ή } N = 12$$

$$\frac{\mathbb{Z}}{2\mathbb{Z}} \times \mathbb{Z}2N\mathbb{Z} \quad 1 \leqslant N \leqslant 4.$$

Επιπλέον κάθε μία από τις παραπάνω ομάδες μπορεί να εμφανιστεί ως ομάδα πεπερασμένης τάξης μιας ελλειπτικής καμπύλης ορισμένης πάνω από το $\mathbb{Q}$.

B. Mazur, CC-AS 3.0 G.M. Bergman	L. Mordel, CC-AS 2.0 K.Jacobs
	

Τα παραπάνω έργα αποτελούν κοινό κτήμα (public domain). Πηγή: Wikimedia Commons, Wikimedia Commons.

7.6. Ελλειπτικές Καμπύλες στη Μορφή του Legendre

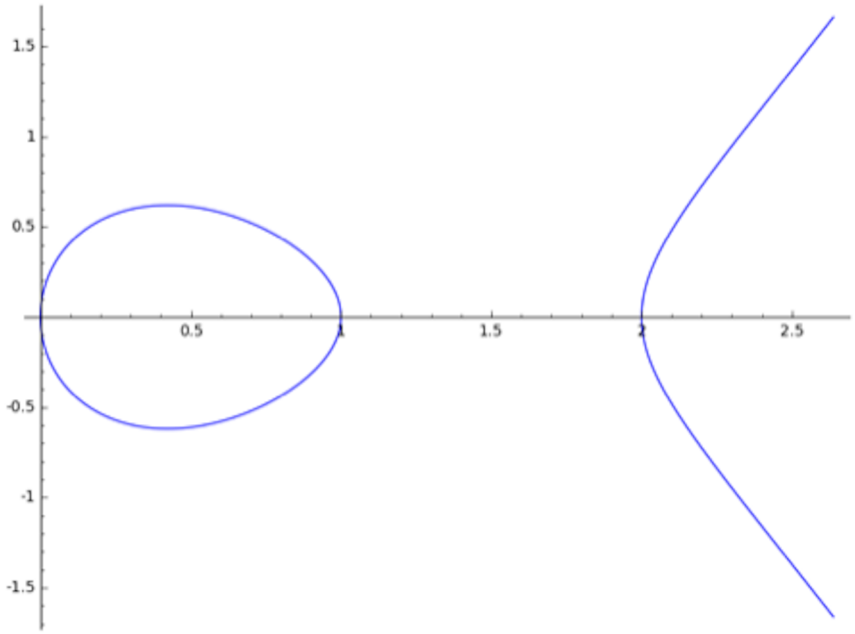
Πρόκειται για ελλειπτικές καμπύλες που δίνονται στη μορφή

$$y^2 = x(x-1)(x-\lambda)$$

Interactive

Πρόβλημα Το πρόβλημα των ισοδύναμων αριθμών. Θα λέμε ότι ο φυσικός αριθμός $n \geqslant 1$ είναι ισοδύναμος αν υπάρχει ένα ορθογώνιο τρίγωνο με πλευρές ρητούς αριθμούς και εμβαδόν ίσο με n. Να υπολογιστούν οι ισοδύναμοι αριθμοί.

Παρατηρούμε ότι οι Πυθαγόρειες τριάδες δίνουν ως αποτέλεσμα ισοδύναμους αριθμούς, για παράδειγμα το τρίγωνο με πλευρές $(3, 4, 5)$ έχει εμβαδόν 6 αλλά δεν είναι



Σχήμα 7.4. Για $\lambda = 2$ έχουμε τη γραφική παράσταση:

οι μοναδικές δυνατότητες αφού το ορθογώνιο τρίγωνο με πλευρές $(3/2, 20/3, 41, 6)$ έχει εμβαδόν ίσο με 5. Δεν επιτρέπουμε όμως τρίγωνα με άρρητους αριθμούς, έτσι το τρίγωνο με πλευρές $(1, 2, \sqrt{5})$ έχει εμβαδόν 1 αλλά δεν είναι επιτρεπτό. Θα δείξουμε ότι το 1 δεν είναι ισοδύναμος αριθμός.

Ο αριθμός $n \geqslant 1$ είναι ισοδύναμος αν και μόνο αν η ελλειπτική καμπύλη $y^2 = x^3 - n^2x$ έχει ένα σημείο $(x, y) \in \mathbb{Q}^2$ ώστε $y^2 \neq 0$. Ακριβέστερα υπάρχει μια ένα προς ένα απεικόνιση ανάμεσα στα σύνολα:

$$I_n = \left\{(a, b, c) : a^2 + b^2 = c^2, \frac{ab}{2} = n\right\}$$

και

$$E_n = \left\{(x, y) : y^3 = x^3 - n^2x, y \neq 0\right\}.$$

Οι συναρτήσεις αντιστοιχίας δίνονται από τους τύπους

$$f : I_n \to E_n$$
$$(a, b, c) \mapsto \left(\frac{nb}{c-a}, \frac{2n^2}{c-a}\right)$$

και

$$g : E_n \to I_n$$
$$(x, y) \mapsto \left(\frac{x^2 - n^2}{y}, \frac{2nx}{y}, \frac{x^2 + n^2}{y}\right)$$

Το πρόβλημα των ισοδύναμων αριθμών είναι ανοιχτό, ενώ υπάρχει και μία λύση του από τον Tunnel η οποία όμως προϋποθέτει την αλήθεια της εικασίας των Birch-Swinnerton-Dyer.

7.6.1 Θεώρημα:
[Tunnel,1983] Αν n *είναι ένας περιττός ελεύθερος τετραγώνου θετικός ακέραιος και* n *είναι ένας ισοδύναμος αριθμός, τότε τα παρακάτω σύνολα έχουν ίσους πληθικούς αριθμούς:*

$$\#\{(x,y,z)\in\mathbb{Z}^3 : n = 2x^2+y^2+32z^2\} =$$
$$= \frac{1}{2}(\#\{(x,y,z)\in\mathbb{Z}^3 : n = 2x^2+y^2+8z^2\})$$

Ενώ αν ο n *είναι άρτιος ισοδύναμος αριθμός, τότε τα παρακάτω σύνολα έχουν ίσους πληθικούς αριθμούς:*

$$\{(x,yz)\in\mathbb{Z}^3 : \frac{n}{2} = 4x^2+y^2+32z^2\} =$$
$$= \frac{1}{2}\left(\#\left\{(x,y,z)\in\mathbb{Z}^3 : \frac{n}{2} = 4x^2+y^2+8z^2\right\}\right).$$

Στην περίπτωση που η εικασία Birch-Swinerton-Dyer είναι σωστή, οι παραπάνω εξισώσεις δίνουν μια ικανή συνθήκη ώστε ο n *να είναι ισοδύναμος αριθμός.*

Για παράδειγμα για $n = 2$ έχουμε ότι $\frac{n}{2} = 1 = 4x^2+y^2+32z^2$ αν και μόνο αν $x = z = 0$ και $y = \pm 1$, άρα το αριστερό μέρος της ισότητας είναι ίσο με 2. Το δεξί όμως είναι ίσο με 1 και η ανισότητα δεν ισχύει, συνεπώς το 2 δεν είναι ισοδύναμος αριθμός.

Το τελευταίο Θεώρημα του Fermat

Έστω $n \geqslant 3$. Υπάρχουν λύσεις της εξίσωσης $x^n + y^n = z^n$ για $(x,y,z)\in\mathbb{Z}^3$ με $xyz \neq 0$;

Αυτό είναι ένα από τα διασημότερα προβλήματα της Θεωρίας Αριθμών το οποίο τέθηκε για πρώτη φορά από τον Pierre de Fermat, ο οποίος στο εξώφυλλο της έκδοσης του βιβλίου Αριθμητικά του Διόφαντου έγραψε ότι βρήκε μια θαυμάσια απόδειξη του θεωρήματος αυτού, αλλά το περιθώριο (στο οποίο συνήθιζε να κρατά σημειώσεις) είναι πολύ μικρό να τη χωρέσει.

Είναι σχετικά εύκολο να δείξει κανείς ότι αρκεί να αποδειχτεί η εικασία για n περιττό πρώτο αριθμό και για $n = 4$. Ο ίδιος ο Fermat μελέτησε τις περιπτώσεις $n = 3, 4$ και έδειξε ότι δεν έχουν λύσεις. Για την περίπτωση $p \geqslant 3$ ο Gerhard Frey έδωσε την ιδέα ότι αν η εξίσωση

$$a^p + b^p = c^p$$

έχει μη τετριμμένη λύση τότε οι ελλειπτικές καμπύλες

$$E : y^2 = x(x-a^p)(y-b^p)$$

έχουν τόσο περίεργες ιδιότητες που θα πρέπει να μην ικανοποιούν την τότε υπόθεση των Taniyama-Shimura-Weil .

Ο Ken Ribet μετέτρεψε τη διαίσθηση του Frey σε αυστηρή απόδειξη και ο Andrew Wiles το 1995 (Wiles 1995) απέδειξε μια περίπτωση της εικασίας των Taniyama-Shimura-Weil αρκετή για να μπορέσει να απόδειξει την εικασία του Fermat.

Δείτε: Fermat Last Theorem BBC Horizon

Διαβάστε:

Σχήμα 7.5. Pierre de Fermat, Το παρόν έργο αποτελεί κοινό κτήμα (public domain). Πηγή: Wikimedia Commons

1. Simon Singh **Το τελευταίο Θεώρημα του Fermat** Εκδόσεις Τραυλός (Singh 1997).
2. Αριστείδης Κοντογεώργης **Ημιευσταθείς Ελλειπικές Καμπύλες και το Τελευταίο Θεώρημα του Fermat**, μεταπτυχιακή εργασία Πανεπιστήμιο Κρήτης 1995 (Κοντογεώργης 1994).

7.7. Πολυώνυμα διαίρεσης

Θεωρούμε την ελλειπτική καμπύλη ορισμένη σε ένα σώμα K της μορφής:

$$y^2 = x^3 + Ax + B.$$

Με μια προσεκτική ματιά στις αλγεβρικές εκφράσεις που αφορούν τον νόμο ομάδας, είναι φανερό ότι οι συντεταγμένες του αθροίσματος δύο σημείων $P_1 + P_2$ της καμπύλης είναι ρητές συναρτήσεις των συντεταγμένων των P_1, P_2. Με επαναληπτική διαδικασία η απεικόνιση

$$(x, y) \to [m](x, y)$$

Σχήμα 7.6. Andrew Wiles, Δημιουργός K. Barner, Το παρόν έργο αποτελεί κοινό κτήμα (public domain). Πηγή: Wikimedia Commons

μπορεί να εκφρασθεί με όρους ρητών συναρτήσεων των x, y. Πιό συγκεκριμένα έχουμε:

Έστω E μια ελλειπτική καμπύλη όπως παραπάνω και έστω m ένας θετικός ακέραιος. Τότε υπάρχουν πολυώνυμα $\psi_m, \theta_m, \omega_m$ τέτοια ώστε για $P = (x, y) \in E(K)$ με $[m]P \neq 0$ έχουμε,

$$[mP] = \left(\frac{\theta_m(x,y)}{\psi_m^2(x,y)}, \frac{\omega_m(x,y)}{\psi_m^3(x,y)} \right)$$

7.7.1 Ορισμός:
Το πολυώνυμο $\psi_m(x, y)$ *ονομάζεται το* m*-οστό πολυώνυμο διαίρεσης της καμπύλης* E *και μπορεί να θεωρηθεί ως ένα πολυώνυμο στον δακτύλιο* $\mathbb{Z}[x, y, A, B]$.

Τα πολυώνυμα διαίρεσης ορίζονται αναδρομικά από τους τύπους:

$$\psi_0 = 0$$

$$\psi_1 = 1$$

$$\psi_2 = 2y$$

$$\psi_3 = 3x^4 + 6Ax^2 + 12Bx - A^2$$

$$\psi_4 = 4y(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - 8B^2 - A^3)$$

$$\dots$$

$$\psi_{2m+1} = \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3 \text{ για } m \geqslant 2$$

$$\psi_{2m} = \left(\frac{\psi_m}{2y}\right) \cdot (\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2) \text{ για } m \geqslant 3$$

Τα πολυώνυμα $\phi_n(x)$ και $\omega_n(x)$ δίνονται από τους τύπους:

$$\phi_n(x) = x\psi_n^2(x) - \psi_{n+1}(x)\psi_{n-1}(x),$$

$$\omega_n(x) = \frac{\psi_{n+2}(x)\psi_{n-1}^2(x) - \psi_{n-2}(x)\psi_{n+1}^2(x)}{4y}.$$

7.7.2 Ορισμός:
Η ομάδα των m σημείων στρέψης (m-torsion points) ορίζεται να είναι η

$$E[m] = \{P\ E(K) | [m]P = O\}$$

Το m-οστό πολύωνυμο διαίρεσης ψ_m χαρακτηρίζει τα m − torsion σημεία της E, σύμφωνα με το παρακάτω:

7.7.3 Θεώρημα:
Έστω P σημείο στο $E(K)\backslash O$ κι έστω $m \geqslant 1$. Τότε $P \in E[m]$ εάν και μόνον εάν $\psi_m(P) = 0$.

Παρατηρούμε ότι για τον υπολογισμό των m − torsion σημείων μπορούμε να χρη- σιμοποιήσουμε πολυώνυμα μιας μεταβλητής, αντί των πολυωνύμων ψ_m τα οποία έχουν δύο μεταβλητές x, y.

7.7.4 Ορισμός:

$$\bar{f}_m = \psi_m \text{ αν } m = 2k+1, k \in \mathbb{N},$$
$$\bar{f}_m = \frac{\psi_m}{\psi_2} \text{ αν } m = 2k, k \in \mathbb{N}.$$

Παρατηρώντας ότι το y χρησιμοποιείται στον αναδρομικό ορισμό του ψ_m μόνο μέσω του πολυωνύμου ψ_2 και ότι το ψ_2^2 δεν εξαρτάται από το y, προκύπτει ότι το $\bar{f}_m$ είναι ένα πολυώνυμο το οποίο εξαρτάται μόνο από το x. Ο βαθμός του $\bar{f}_m$ είναι το πολύ $(m^2-1)/2$, εάν ο m είναι περιττός και το πολύ $(m^2-4)/2$, εάν ο m είναι άρτιος (οι βαθμοί είναι ακριβώς ίδιοι εάν η χαρακτηριστική του σώματος δεν διαιρεί τον m, για m περιττό, ή τον $m/2$, για m άρτιο).

Ο χαρακτηρισμός των m-torsion points μπορεί να αναδιατυπωθεί με τη βοήθεια των πολυωνύμων $\bar{f}_m$ ως εξής:

7.7.5 Θεώρημα:
Έστω $P = (x, y)$ *σημείο στο* $E(K)$ O *τέτοιο ώστε* $[2]P \neq O$ *κι έστω* $m \geqslant 2$.*Τότε* $P \in E[m]$ *εάν και μόνον εάν* $\bar{f}_m(x) = 0$.

Παρατήρηση Το παραπάνω θεώρημα δεν συμπεριλαμβάνει τα 2 − torsion σημεία. Αυτά τα σημεία ικανοποιούν την $\psi_2(P) = 0$, με το οποίο διαιρούμε το ψ_m για να πάρουμε το $\bar{f}_m$, όταν το m είναι άρτιος.

7.8. Ελλειπτικές Καμπύλες Ορισμένες Πάνω Από Πεπερασμένα Σώματα

Θεωρούμε μια ελλειπτική καμπύλη ορισμένη πάνω από ένα πεπερασμένο σώμα $\mathbb{F}_{p^h}$ με p^h το πλήθος στοιχεία. Είναι σαφές ότι μια τέτοια καμπύλη θα είναι μια πεπερασμένη αβελιανή ομάδα και ένα προφανές φράγμα της τάξης της είναι το

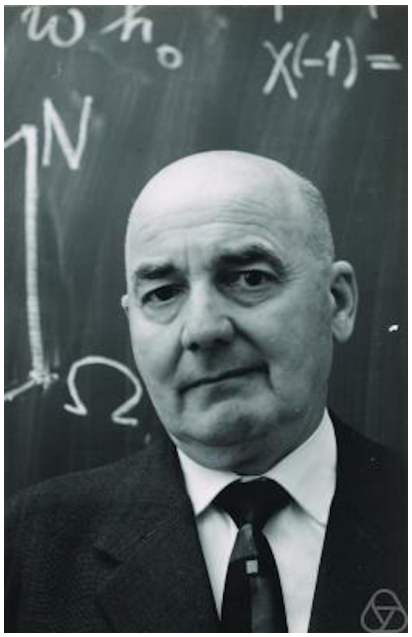
$$|E| \leqslant p^{2h} + 1.$$

Ένα από τα βασικά προβλήματα είναι να υπολογιστεί η τάξη της και στη συνέχεια η δομή της (που θα είναι ευθύ άθροισμα από κυκλικές ομάδες σύμφωνα με το θεώρημα δομής αβελιανών ομάδων.

Ο H. Hasse απέδειξε ότι το καλύτερο φράγμα ισχύει

$$|E| = p^h + 1 \pm s,$$

όπου το $|s| \leqslant 2\sqrt{p^h}$. Ο αριθμός s στη βιβλιογραφία είναι γνωστός ως το ίχνος του Frobenious. Θα αναφέρουμε περισσότερα για αυτό και θα δώσουμε μια απόδειξη του φράγματος του Hasse στη συνέχεια.



Σχήμα 7.7. H. Hasse, Το παρόν έργο αποτελεί κοινό κτήμα (public domain). Πηγή: Wikimedia Commons

7.9. Θεωρία των Ελλειπτικών καμπυλών πάνω από τους μιγαδικούς αριθμούς.

Ορισμός: Ένα lattice L στο σώμα των μιγαδικών αριθμών είναι το σύνολο που παράγεται από όλους τους $\mathbb{Z}$-συνδυασμούς από δύο γραμμικά ανεξάρτητα διανύσματα e_1, e_2 του $\mathbb{C}$.

Σχήμα 7.8. Weierstrass, Το παρόν έργο αποτελεί κοινό κτήμα (public domain). Πηγή: Wikimedia Commons

Ο Weierstrass κατασκεύασε μια συνάρτηση (που εξαρτάται από ένα lattice L)

$$\mathbb{C} \to \mathbb{C}$$

η οποία ορίζεται από τον τύπο:

$$\wp(z, L) = \frac{1}{z^2} + \sum_{\lambda \in L - \{0\}} \left(\frac{1}{(z+\lambda)^2} - \frac{1}{\lambda^2} \right).$$

Η συνάρτηση του Weierstrass ικανοποιεί τη διαφορική εξίσωση

$$\wp'(z)^2 = 4\wp(z)^3 - g_2(L)\wp(z) - g_3(L).$$

Δηλαδή το ζευγάρι $(x, y) = (\wp(z), \wp'(z))$ παραμετρίζει την ελλειπτική καμπύλη

$$y^2 = 4x^3 - g_2(L)x - g_3(L).$$

Παρατήρηση: Οι υπερβατικές συναρτήσεις $(x, y) = (\sin(x), \cos(x)) = (\sin(x), \sin'(x))$ ικανοποιούν την εξίσωση $x^2 + y^2 = 1$ και συνεπώς παραμετρίζουν τον κύκλο.

Η συνάρτηση του Weierstrass είναι περιοδική με περίοδο το laticce L. Δηλαδή

$$(\wp(z+\lambda), \wp'(z+\lambda)) = (\wp(z), \wp'(z)).$$

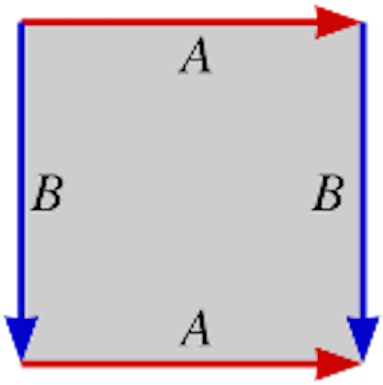
Σε επίπεδο θεωρίας ομάδων αυτό σημαίνει ότι

$$\frac{\mathbb{C}}{L} \cong E(\mathbb{C}).$$

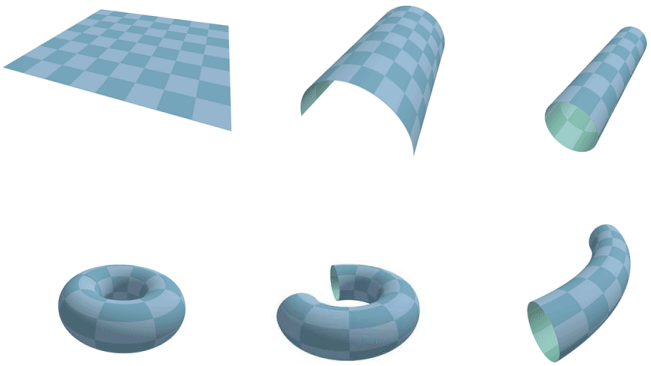
Από τοπολογικής πλευράς αυτό σημαίνει ότι το εσωτερικό του lattice, δηλαδή το παραλληλόγραμμο που αποτελείται από τα σημεία

$$z = ae_1 + be_2 : \text{ με } 0 \leqslant a, b < 1$$

καλύπτει την ελλειπτική καμπύλη ενώ οι απέναντι πλευρές του παραλληλογράμμου ταυτίζονται δίνοντας στο πηλίκο τη δομή του "λουκουμά".



Σχήμα 7.9. Οι Πλευρές A και B ταυτίζονται στο πηλίκο



Σχήμα 7.10. Λουκουμάς-κολλώντας τις πλευρές παρ/μου, Το παρόν έργο αποτελεί κοινό κτήμα (public domain). Πηγή: Wikimedia Commons

Οι συναρτήσεις $g_2(L), g_3(L)$ εξαρτώνται από το lattice L, και δίνονται από τον τύπο:

$$g_2(L) = 60 \sum_{\lambda \in L - \{0\}} \frac{1}{\lambda^4} \qquad g_3(L) = 140 \sum_{\lambda \in L - \{0\}} \frac{1}{\lambda^6},$$

αποτελούν δε παραδείγματα από σειρές Eisenstein.

7.10. Αλγεβρική Θεωρία Ελλειπτικών καμπυλών.

Στην παράγραφο αυτή θα μελετήσουμε διάφορες αναλλοίωτες της ελλειπτικής καμπύλης που ορίζεται από την εξίσωση:

$$y^2 = x^3 + ax + b.$$

Για κάθε πολυώνυμο μιας μεταβλητής $f(x)$ ορίζεται η διακρίνουσά του. Αυτός είναι ένας αριθμός που γενικεύει τη γνωστή διακρίνουσα δευτεροβάθμιου πολυωνύμου και είναι ίσο με το 0, αν και μόνο αν το αρχικό πολυώνυμο έχει διπλή ρίζα. Στην περίπτωση του κυβικού πολυωνύμου $x^3 + ax + b$ η διακρίνουσα δίνεται από τον τύπο: $-16(4a^3 + 27b^2)$. Παρατηρούμε ότι οι ελλειπτικές καμπύλες έχουν πάντα διακρίνουσα διαφορετική του μηδενός.

Η j-invariant της ελλειπτικής καμπύλης ορίζεται από την εξίσωση:

$$j(E) = \frac{(4a)^3}{4a^3 + 27b^2} = -\frac{4a^3}{\Delta(E)}.$$

Δύο ελλειπτικές καμπύλες ορισμένες πάνω από ένα αλγεβρικά κλειστό σώμα είναι ισόμορφες αν και μόνο αν έχουν την ίδια j-invariant.

Η πρόταση αυτή δεν είναι σωστή όταν οι ελλειπτικές καμπύλες δεν είναι ορισμένες πάνω από αλγεβρικά κλειστό σώμα. Γίνονται ισόμορφες πάνω από μια τετραγωνική επέκταση του σώματος ορισμού.

Για κάθε αριθμό $j_0 \in K$ υπάρχει ελλειπτική καμπύλη E ορισμένη υπέρ το K που να έχει j-invariant ίση με j_0.

Απόδειξη:

Αν το j είναι διαφορετικό από το $0, 1728$, τότε η ελλειπτική καμπύλη με τύπο

$$E : y^2 + xy = x^3 - \frac{36}{j_0 - 1728}x - \frac{1}{j_0 - 1728}$$

έχει διακρίνουσα

$$\Delta(E) = \frac{j_0^3}{(j_0 - 1728)^3} \text{ και } j(E) = j_0.$$

Όταν το $j_0 = 0$ θεωρούμε την ελλειπτική καμπύλη:

$$E : y^2 + y = x^3, \text{ με } \Delta(E) = -27 \text{ και } j = 0$$

ενώ για j_0 θεωρούμε την ελλειπτική καμπύλη:

$$E : y^2 = x^3 + x, \text{ με } \Delta(E) = -64 \text{ και } j = 1728.$$

Ο αριθμός 1728 αν του προσθέσουμε 1 είναι ο δεύτερος Taxicab number δηλαδή είναι ο μικρότερος αριθμός που μπορεί να γραφεί ως άθροισμα δυο θετικών κύβων με δύο διαφορετικούς τρόπους: $1729 = 1 + 12^3 = 9^3 + 10^3$. Η ονομασία αυτή δόθηκε από τον αριθμό του ταξί που μετέφερε τον Hardy στο νοσοκομείο που νοσηλεύονταν ο Ramanujan. Όπως αναφέρει ο Hardy: “I remember once going to see him when he was lying ill at Putney. I had ridden in taxi-cab No. 1729, and remarked that the number seemed to be rather a dull one, and that I hoped it was not an unfavourable omen.”No“, he replied,”it is a very interesting number; it is the smallest number expressible as the sum of two [positive] cubes in two different ways.”

Κάθε στοιχείο του $\mathbb{F}_p$ είναι j-invariant μιας ελλειπτικής καμπύλης πάνω από το $\mathbb{F}_p$. Όταν το $j \neq 0, 1728$ αυτή η ελλειπτική καμπύλη δίνεται από

$$y^2 = x^3 + 3kc^2x + 2kc^3,$$

όπου $k = j/(1728 - j)$ και το c είναι οποιοδήποτε στοιχείο του $\mathbb{F}_p$. Υπάρχουν δύο μη ισόμορφες ελλειπτικές καμπύλες E, E' υπέρ του $\mathbb{F}_p$ που αντιστοιχούν σε διαφορετικές επιλογές του c. Αυτές έχουν τάξεις

$$|E| = p + 1 - t$$

και

$$|E| = p + 1 + t.$$

Παρατήρηση Από τον ορισμό της j-invariant προκύπτει ότι οι καμπύλες E, E' μοιράζονται την ίδια j-invariant. Για τις περισσότερες j-invariants $j \in \mathbb{F}_p$, υπάρχουν όσον αφορά τον ισομορφισμό, ακριβώς δύο ελλειπτικές καμπύλες επί του $\mathbb{F}_p$ με $j(E) = j$, Η καμπύλη E και η διαστροφή της. Υπάρχουν όμως δύο πολύ γνωστές εξαιρέσεις:

$$j = 0, p = 1(\mathrm{mod} 3)$$

$$j = 1728, p = (1\mathrm{mod} 4)$$

όπου στην πρώτη περίπτωση υπάρχουν 6 καμπύλες ενώ στη δεύτερη 4.

7.10.1. Δακτύλιος Ενδομορφισμών. Μια συνάρτηση $f : E \to E$ θα λέμε ότι είναι ενδομορφισμός της ελλειπτικής καμπύλης αν εκφράζεται μέσω ρητών συναρτήσεων και αν στέλνει το ουδέτερο στοιχείο στο ουδέτερο στοιχείο. Οι ενδομορφισμοί αποτελούν δακτύλιο όπου η πρόσθεση είναι η πρόσθεση συναρτήσεων και ο πολλαπλασιασμός η σύνθεση. Τον δακτύλιο αυτόν θα τον συμβολίζουμε με $\mathrm{End}(E)$.

Ας σταθεροποιήσουμε έναν ακέραιο $n \in \mathbb{Z}$. Μπορούμε να ορίσουμε τον ενδομορφισμό που στέλνει κάθε $P \in E$ στο nP. Με αυτόν τον τρόπο το $\mathbb{Z}$ είναι υποδακτύλιος του $\mathrm{End}(E)$.

Σε ελλειπτικές καμπύλες ορισμένες πάνω από σώματα χαρακτηριστικής 0 στις περισσότερες περιπτώσεις δεν υπάρχουν άλλοι ενδομορφισμοί.

Εάν το $d \in \mathbb{Z}_{<0}$ δηλώνει τη διακρίνουσα μιας τετραγωνικής τάξης έχουμε,

$$\mathrm{End}(E) \cong \mathbb{Z}[\delta] = \mathbb{Z} + \delta\mathbb{Z}$$

όπου,

$$\delta = \frac{\sqrt{d}}{2}, d = 2k, k \in \mathbb{Z}_{<0}$$

$$\delta = \frac{1 + \sqrt{d}}{2}, d = 2k + 1, k \in \mathbb{Z}_{<0}$$

Παρατήρηση Οι ελλειπτικές καμπύλες E, E' έχουν ισόμορφο ενδομορφισμό δακτυλίων.

Εάν $p = 1(\mathrm{mod} 3)$, οι 6 καμπύλες με $j = 0$ όλες έχουν τον ενδομορφισμό δακτυλίου τους ισόμορφο με τον $\mathbb{Z}[(1 + \sqrt{-3})/2]$ ενώ οι 4 καμπύλες με $j = 1728$, όλες έχουν $\mathrm{End}(E) = \mathbb{Z}[i]$.

Σε ελλειπτικές καμπύλες ορισμένες πάνω από ένα πεπερασμένο σώμα $\mathbb{F}_q$ υπάρχει πάντα και ένας επιπλέον ενδομορφισμός, ο *ενδομορφισμός του Frobenious*, ο οποίος ορίζεται ως εξής: Το σημείο P με συντεταγμένες (x, y) απεικονίζεται στο σημείο $\phi(P)$ με συντεταγμένες (x^q, y^q). Ο ενδομορφισμός αυτός έχει ενδιαφέρον γιατί είναι γνωστό ότι ένα στοιχείο $x \in \overline{\mathbb{F}}_q$ ανήκει στο $\mathbb{F}_q$ αν και μόνο αν $x^q = x$. Με άλλα λόγια τα σημεία που παραμένουν σταθερά από τη δράση του Frobenious είναι ακριβώς τα σημεία της ελλειπτικής καμπύλης πάνω από το πεπερασμένο σώμα $\mathbb{F}_q$.

Αυτή η παρατήρηση μας επιτρέπει να μετρήσουμε το *ίχνος* του Frobenious όπως αυτό εμφανίζεται στον τύπο του Hasse.

Ο ενδομορφισμός του Frobenious ικανοποιεί τη σχέση:

$$\phi^2 - t\phi + q = 0.$$

Γενικά είναι γνωστό ότι οποιοσδήποτε επιπλέον ενδομορφισμός σε ελλειπτική καμπύλη E ικανοποιεί μια παρόμοια σχέση.

Αν υπάρχουν επιπλέον ενδομορφισμοί ϕ τότε αυτοί ικανοποιούν μια τετραγωνική εξίσωση της μορφής:

$$\phi^2 + a\phi + b = 0,$$

της οποίας η διακρίνουσα είναι αρνητική (εδώ οφείλεται και το όνομα *μιγαδικός πολλαπλασιασμός*).

Παρατήρηση: Το φράγμα του Hasse είναι ισοδύναμο με το ότι η τετραγωνική εξίσωση που ικανοποιεί ο Frobenius έχει αρνητική διακρίνουσα.

7.11. Ελλειπτικά Κρυπτοσυστήματα

Το σύστημα ElGamal το οποίο χρησιμοποιήσαμε για την κυκλική ομάδα $G = \mathbb{F}_p^*$ μπορεί να χρησιμοποιηθεί με πολύ καλά αποτελέσματα και στην περίπτωση των ελλειπτικών καμπυλών.

Η βασική ιδέα του ElGamal έχει ήδη περιγραφεί, οπότε θα παρουσιάσουμε μια υλοποίησή του περιγράφοντας το σύστημα Digital Rights Management που χρησιμοποιούσε η Microsoft στις αρχές του 2000 καθώς και τον τρόπο με τον οποίο εσπασε από τον hacker Beale Streamer ακολουθώντας την περιγραφή του W. Stein.

Θα δουλέψουμε πάνω από μια ελλειπτική καμπύλη E ορισμένη στο σώμα $\mathbb{F}_p$, όπου

$$p = 78596310237942882237669478944689739620749856895 1$$

η οποία δίνεται από την εξίσωση:

$$y^2 = x^3 + 3176890812513255034763174764138276932727469559 27x$$

$$+7905289660787875871812057202571853543210065193 4.$$

Η παραπάνω ελλειπτική καμπύλη είναι ισόμορφη με μια κυκλική ομάδα τάξης

$$7859631023794288223766930248817149576126861574 29,$$

ενώ ένας γεννήτορας δίνεται από το σημείο

$$B = (7715072162626498261706482685655798899077692541 76,$$

$$3901575102465566285252794592665149955625331966 55).$$

Το σύστημα της Microsoft, όταν ο χρήστης εγκαθιστούσε το DRM λογισμικό στο μηχάνημά του παρήγαγε ένα ιδιωτικό κλειδί:

$$n = 67080503113991051351752720769306045630021705447 3$$

το οποίο γραφόταν σε διάφορα αρχεία του υπολογιστή. Προκειμένου ο χρήστης να μπορέσει να ακούσει ένα μουσικό κομμάτι θα έπρεπε, (αφού έστελνε τον αριθμό της πιστωτικής κάρτας του) να κατεβάσει ένα αρχείο άδειας (licence file), το οποίο θα του επέτρεπε να ακούσει το μουσικό κομμάτι.

Στην πραγματικότητα ο χρήστης δημοσιεύε ως δημόσιο κλειδί το (p, E, B, nB). Το μήνυμα προς τον χρήστη από τη Microsoft αποθηκεύεται ως ένα στοιχείο P της ελλειπτικής καμπύλης. Επιλέγοντας έναν τυχαίο πρώτο η Microsoft έστελνε στον χρήστη τα σημεία

$$(rB, P + rnB) = (A, B).$$

Για να παραλάβει το σημείο P ο χρήστης που θα του επιτρέψει να ξεκλειδώσει το μουσικό αρχείο θα πρέπει να υπολογίσει το

$$P = B - nA = P + rnB - n(rB).$$

Το αρχείο της άδειας είναι ένα μήνυμα που ο χρήστης στέλνει στον εαυτό του. Περιέχει το ζευγάρι των σημείων $(rB, P + r(nB))$, όπου

$$rB = (17967100321831574638502665573308604498219442466 0,$$

$$69783438535968636824930128267514183093517631471 8)$$

και

$$P + r(nB) = (137851038548264467372645158093004000343639118915,$$

$$110848589228676224057229230223580815024224875699).$$

Όταν ο υπολογιστής του χρήστη θέλει να παίξει ένα συγκεκριμένο αρχείο, τότε διαβάζει το μυστικό κλειδί

$$n = 67080503113991051351752720769306045630021705447 3$$

και υπολογίζει το

$$n(rB) = (328901393518732637577115650601768681044040715701,$$

$$586947838087815993601350565488788846203887988162).$$

Αφαιρώντας το από το $P + r(nB)$ παίρνει το

$$P = (14489646124220757767,$$

$$669337780373284096274895136618194604469696830074).$$

Η x-συντεταγμένη 14489646124220757767 είναι το κλειδί που ξεκλειδώνει το μουσικό αρχείο. Αν ο χρήστης γνώριζε το ιδιωτικό κλειδί n που ο υπολογιστής του παρήγαγε θα μπορούσε να παράγει το P, να ξεκλειδώσει το μουσικό αρχείο και να το μοιραστεί με οποιονδήποτε.

Αν και η παραπάνω μέθοδος είναι πολύ δύσκολο να αντιμετωπιστεί λύνοντας το πρόβλημα του διακριτού λογαρίθμου, το παραπάνω σύστημα "έσπασε" από τον Beale Screamer γιατί η implementation του αλγορίθμου ήταν φτωχή. Σε κάθε περίπτωση το ιδιωτικό κλειδί ήταν αποθηκευμένο στον υπολογιστή του χρήστη. Πώς μπορεί το software να το χρησιμοποιεί χωρίς να το γνωρίζει ο χρήστης;

```
p = 78596310237942882237669478944689739620749856895 1
 E = EllipticCurve(GF(p), \
[31768908125132550347631747641382769327274695592 7,
79052896607878758718120572025718535432100651934])
E.cardinality()
78596310237942882237669302488171495761268615742 9
E.cardinality().is_prime()
True
B = E([
77150721626264982617064826856557988990776925417 6,
39015751024655662852527945926651499556253319665 5])
n=67080503113991051351752720769306045630021705447 3
r=70674630913457179596452846564371866229568459543
P = E([14489646124220757767,
66933778037328409627489513661819460446969683007 4])
encrypt = (r*B, P + r*(n*B))
encrypt[1] - n*encrypt[0] == P # decrypting works
True
```

7.11.1. Το πρόβλημα του διακριτού λογαρίθμου για Ελλειπτικές Καμπύλες. Δίνεται μία ελλειπτική καμπύλη E ορισμένη πάνω από ένα πεπερασμένο σώμα $\mathbb{F}_q$. Το πρόβλημα του διακριτού λογαρίθμου είναι το εξής: Αν

$$Q = nP,$$

ζητείται να βρεθεί το n. Το πρόβλημα αυτό μπορεί να ορίστει σε κάθε αβελιανή ομάδα G, και είδαμε διάφορους τρόπους να το αντιμετωπίσουμε όταν $G = \mathbb{F}_p^*$. Η πρακτική ένδειξη είναι το πρόβλημα του διακριτού λογαρίθμου σε ελλειπτικές καμπύλες, όπως και τα κρυπτοσυστήματα που προκύπτουν όπως το ElGamal είναι δυσκολότερο να επιλυθούν από τα αντίστοιχα συστήματα στην πολλαπλασιαστική υποομάδα ενός πεπερασμένου σώματος.

Βιβλιογραφία

Blake, I.F., G. Seroussi, and N. Smart. 1999. *Elliptic Curves in Cryptography*. Lecture Note Series. Cambridge University Press. https://books.google.gr/books?id=0/_vegzgyqGMC.

Milne, J. S. 2006. *Elliptic Curves*. BookSurge Publishers.

Silverman, J.H., and J. Tate. 1992. *Rational Points on Elliptic Curves*. Springer Undergraduate Texts in Mathematics and Technology. Springer. https://books.google.gr/books?id=mAJei2-JcE4C.

Singh, Simon. 1997. *Το Τελευταίο Θεώρημα Του Φερμά*. Εκδόσεις Τραυλός.

Wiles, Andrew. 1995. "Modular Elliptic Curves and Fermat's Last Theorem." *Ann. Math.*, Second Series, 141 (3). Annals of Mathematics: 443–551. doi:10.2307/2118559.

Αντωνιάδης, Ι. 1999. *Ελλειπτικές Καμπύλες (Το Θεώρημα Του Mordell)*. ΕΠΕΑΕΚ Προμηθέας.

Κοντογεώργης, Αριστείδης. 1994. *Ημιευσταθείς Ελλειπτικές Καμπύλες Και Το Τελευταίο Θεώρημα Του Fermat*. Μεταπτυχιακή Εργασία Πανεπιστήμιο Κρήτης, Ηράκλειο.

8

Μέθοδοι Παραγοντοποίησης

8.1. Κριτήρια ελέγχου πρώτων αριθμών

Προκειμένου να κατασκευάσουμε αποτελεσματικά κρυπτοσυστήματα βασισμένα στη θεωρία αριθμών χρειαζόμαστε να κατασκευάσουμε πρώτους, και περισσότερο συγκεκριμένα, χρειαζόμαστε τεχνικές για να ελέγξουμε άν ένας δεδομένος φυσικός αριθμός είναι πρώτος ή όχι. Η γνώση και οι τεχνικές από τη θεωρία αριθμών είναι απαραίτητες και για περισσότερες λεπτομέρειες παραπέμπουμε στο (Αντωνιάδης and Κοντογεώργης 2015).

Μία αφελής μέθοδος ελέγχου πρώτων αριθμών θα ήταν να δοκιμάζουμε πιθανούς διαιρέτες. Καταρχήν μπορούμε να ελέγξουμε το μέγεθος των πρώτων διαιρετών ενός φυσικού:

8.1.1 Πρόταση:
Αν ο φυσικός αριθμός n *είναι σύνθετος, τότε έχει έναν πρώτο παράγοντα* p, $p \leqslant \sqrt{n}$.

Απόδειξη Αφού ο n είναι σύνθετος, έχει τουλάχιστον μία ανάλυση της μορφής:

$$n = a \cdot b \text{ με } 1 < a \leqslant b < n.$$

Ένα τουλάχιστον από τα a, b είναι μικρότερο ή ίσο της $\sqrt{n}$, διότι αν $a > \sqrt{n}$ και $b > \sqrt{n}$ θα είχαμε $n = a \cdot b > \sqrt{n} \cdot \sqrt{n} = n$, άτοπο. Επειδή το $a > 1$ έχει, έναν τουλάχιστον πρώτο διαιρέτη p.

Ο πρώτος αυτός είναι διαιρέτης του n και $p \leqslant a \leqslant \sqrt{n}$.

Παρατήρηση Η παραπάνω πρόταση μας δίνει ένα κριτήριο ελέγχου πρώτων αριθμών. Έτσι για παράδειγμα ο φυσικός αριθμός $n = 179$ είναι πρώτος. Αν ήταν σύνθετος θα είχε έναν πρώτο διαιρέτη $p \leqslant \sqrt{179} < 14$. Οι πρώτοι οι μικρότεροι του 14 είναι οι 2, 3, 5, 7, 11 και 13. Κανένας τους δεν διαιρεί το 179. Συνεπώς ο 179 δεν είναι σύνθετος, άρα είναι πρώτος. Φυσικά το κριτήριο δεν είναι εφαρμόσιμο για μεγάλους φυσικούς αριθμούς.

Παρατήρηση Αν γνωρίζαμε ότι ένας σύνθετος αριθμός n περιέχει ℓ-το πλήθος διαιρέτες τότε ένας τουλάχιστον από αυτούς θα είναι μικρότερος από την $\sqrt[\ell]{n}$. Σε διαφορετική περίπτωση, αν δηλαδή και οι ℓ διαιρέτες ήταν γνήσια μεγαλύτεροι του $\sqrt[\ell]{n}$ τότε το γινόμενο θα ήταν γνήσια μεγαλύτερο του n.

Η κρυπτογραφία βασίζεται στη δυσκολία να παραγοντοποιήσουμε έναν σύνθετο αριθμό σε γινόμενο πρώτων. Από την παραπάνω παρατήρηση προκύπτει ότι δυσκολεύουμε περισσότερο την παραγοντοποίηση του αριθμού n, αν αυτός είναι γινόμενο δύο πρώτων που είναι περιπού ίδιου μεγέθους κοντά

στην $\sqrt{n}$. Από την άλλη το να είναι το n γινόμενο δύο πρώτων παραγόντων είναι η "κερκόπορτα" του αλγορίθμου Fermat, που θα αναπτύξουμε παρακάτω.

8.1.1. Το κόσκινο του Ερατοσθένη. Σύμφωνα με τη μέθοδο αυτή, αν θέλουμε να βρούμε όλους τους πρώτους μέχρι τον φυσικό αριθμό n, γράφουμε όλους τους ακέραιους από το 2 μέχρι τον φυσικό αριθμό n και διαγράφουμε διαδοχικά όλα τα πολλαπλάσια του 2 του 3, του 5 κλπ. Οι αριθμοί που απομένουν είναι πρώτοι.

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	60
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Σχήμα 8.1. Το κόσκινο του Ερατοσθένη

8.1.2. Ψευδοπρώτοι. Ένα κριτήριο ελέγχου πρώτων είναι το θεώρημα του Fermat το οποίο αναφέρει ότι για πρώτους αριθμούς p και $(a, p) = 1$ ισχύει

$$a^p \equiv a \mathrm{mod}.p$$

Αν έχουμε λοιπόν έναν φυσικό αριθμό και θέλουμε να δούμε αν είναι πρώτος ή όχι μπορούμε να δοκιμάσουμε να υπολογίσουμε αν ισχύει για κάποιο a

$$a^n \equiv a \mathrm{mod} n$$

Αν στην παραπάνω εξίσωση δεν έχουμε ισότητα, τότε είμαστε σίγουροι ότι ο αριθμός n δεν είναι πρώτος. Έτσι ο αριθμός 10 δεν είναι πρώτος αφού

$$2^{10} \equiv 4 \mathrm{mod} 10.$$

Τι γίνεται όμως αν βρούμε ισότητα για παράδειγμα $(2, 341) = 1$, ο $341 = 11 \cdot 31$ δεν είναι πρώτος και όμως έχουμε

$$2^{341} \equiv 2 \mathrm{mod} 341$$

8.1.2 Ορισμός:
Ο αριθμός n θα λέγεται ψευδοπρώτος ως προς τη βάση a αν ισχύει

$$a^n \equiv a mod n$$

Είναι σαφές ότι στο παραπάνω κριτήριο δοκιμάζουμε μόνο μία βάση ενώ ένας πρώτος θα πρέπει να είναι ψευδοπρώτος για κάθε βάση $(a, n) = 1$. Αυτό οδηγεί στον επόμενο

8.1.3 Ορισμός:
Ο σύνθετος ακέραιος $n > 1$ *θα λέγεται αριθμός Carmichael όταν*

$$a^n \equiv a mod n$$

για κάθε ακέραιο a, $(a, n) = 1$.

Είναι σαφές ότι υπάρχουν σύνθετοι αριθμοί Carmichael όπως ο $561 = 3 \cdot 11 \cdot 17$, όπως μπορούμε να τσεκάρουμε στο sage:

```
def IsCarmichael(a):
    R = Zmod(a)
    L = R.list_of_elements_of_multiplicative_group();
    Carmichael=True;
    for j in L:
        if Mod(j^a-j,a) <> Mod(0,a):
            Carmichael=False;
    return Carmichael

IsCarmichael(561)
True
```

Μπορούμε να προχωρήσουμε ψάχνοντας όλους τους αριθμούς Carmichael σε ένα συγκεκριμένο διάστημα:

```
[n for n in range(1,2000) if IsCarmichael(n)]
[1, 561, 1105, 1729]
```

Μπορείτε να συνεχίσετε το ψάξιμο όρων της ακολουθίας ή να την αναζητήσετε στη λίστα του Sloane

Interactive

Ενδιαφέρον είναι ότι το 1729 είναι ένας Hardy-Ramanujan αριθμός "Ταξί".
Διαβάστε
Άρθρο του S. Singh στο BBC news

8.1.3. Το κριτήριο Miller-Rabin. Παρατηρούμε ότι αν το p είναι πρώτος αριθμός τότε η εξίσωση

$$x^2 \equiv 1 mod p$$

έχει μοναδικές λύσεις $x \equiv \pm 1 \mathrm{mod} p$, αφού αυτές είναι πάντα λύσεις και σε ένα σώμα μια εξίσωση έχει το πολύ τόσες ρίζες όσες ο βαθμός του πολυωνύμου. Στην περίπτωση που η εξίσωση

$$x^2 \equiv 1 \mathrm{mod} n,$$

έχει και άλλες λύσεις, τότε το n είναι σύνθετος.

8.1.4 Ορισμός:
Ένας αλγόριθμος Monte-Carlo είναι ένας πιθανοθεωρητικός αλγόριθμος του οποίου η απάντηση "Ναι" σε κάποιο πρόβλημα είναι πάντα σωστή, αλλά η απάντηση "όχι" μπορεί να είναι και λάθος.
Θα λέμε ότι ο αλγόριθμος Monte-Carlo έχει πιθανότητα λάθους ε, όταν σε περιπτώσεις που η απάντηση θα έπρεπε να είναι είναι "ναι", ο αλγόριθμος δίνει τη λάθος απάντηση με πιθανότητα το πολύ ε.

Ο αλγόριθμός Miller-Rabin είναι ένας Monte-Carlo αλγόριθμος στον οποίο η απάντηση "ναι" σημαίνει ότι ο n είναι σύνθετος.

Θεωρούμε έναν περιττό φυσικό n, $n > 1$ τον οποίο γράφουμε στη μορφή:

$$n - 1 = 2^k \cdot m,$$

με $(m, 2) = 1$ περιττός και $k \geqslant 1$. Το κριτήριο Miller-Rabin δίνεται με τον αλγόριθμο, που περιγράφεται στα παρακάτω βήματα:

1. Επιλέγουμε τυχαία έναν ακέραιο $a \in \mathbb{Z}$, $1 \leqslant a \leqslant n - 1$.
2. Υπολογίζουμε το $b := a^m \mathrm{mod} n$. Αν $b \equiv 1 \mathrm{mod} n$, τότε η απάντηση είναι: "ο n είναι πρώτος" και σταματάμε.
3. Σε διαφορετική περίπτωση υπολογίζουμε διαδοχικά τις δυνάμεις

   $$b, b^2 = a^{2m}, b^4 = a^{2^2 m}, \ldots, b^{2^{k-1} m} \mathrm{mod} n$$

   Αν σε κάποιο βήμα βρούμε ότι $a^{2^i m} \equiv -1 \mathrm{mod} n$, τότε και πάλι απαντούμε ότι "ο n είναι πρώτος". Αν δεν βρούμε ποτέ $a^{2^i m} \equiv -1 \mathrm{mod} n$ απαντούμε ότι "ο n είναι σύνθετος".

Θα αποδείξουμε ότι η απάντηση για τον n ότι είναι σύνθετος είναι σίγουρη, ενώ η απάντηση ότι είναι πρώτος είναι επισφαλής. Υπάρχουν, σύνθετοι ακέραιοι που μασκαρεύονται σε πρώτους.

Έστω ότι ο αλγόριθμός δίνει απάντηση "Ναι, ο n είναι σύνθετος", για κάποιο πρώτο αριθμό n, και θα καταλήξουμε σε άτοπο.

Από την απάντηση που πήραμε συμπεραίνουμε ότι

$$a^m \neq 1 \mathrm{mod} n.$$

Επίσης ο αλγόριθμος ελέγχει τις τιμές

$$a^m, a^{2m}, \ldots, a^{2^{k-1} m} \mathrm{mod} n.$$

Και πάλι, αφού η απάντηση είναι ότι "ο n είναι σύνθετος" έχουμε

$$a^{2^i m} \neq -1 \mathrm{mod} n,$$

για κάθε $i = 0, 1, 2, \ldots, k - 1$. Αν όμως, όπως έχουμε υποθέσει, ο n είναι πρώτος, το θεώρημα του Fermat δίνει

$$a^{n-1} \equiv 1 \mathrm{mod} n,$$

δηλαδή

$$a^{2^k m} \equiv 1 \mathrm{mod} n$$

Αν $x := a^{2^{k-1}m}$ η ισοδυναμία γράφεται

$$x^2 \equiv 1 \mod n.$$

Λόγω της υπόθεσης, ότι ο n είναι πρώτος έπεται ότι η ισοδυναμία έχει μοναδικές λύσεις $x = \pm 1 \mod n$. Εμείς όμως έχουμε

$$x = a^{2^{k-1}m} \neq -1 \mod n.$$

Επομένως, αναγκαστικά θα ισχύει:

$$x = a^{2^{k-1}m} \equiv 1 \mod n.$$

Αν τώρα $y := a^{2^{k-2}m}$, έχουμε

$$y^2 \equiv 1 \mod n,$$

οπότε, όπως και παραπάνω, καταλήγουμε στο συμπέρασμα ότι

$$y = a^{2^{k-2}m} \equiv 1 \mod n.$$

Συνεχίζουμε επαγωγικά και καταλήγουμε στο συμπέρασμα ότι και

$$a^m \equiv 1 \mod n,$$

άτοπο. Άρα ο n είναι σύνθετος.

8.1.5 Ορισμός:
Αν ένας σύνθετος πρώτος δεν αναγνωριστεί ως τέτοιος από το κριτήριο των Miller-Rabin, ως προς τη βάση b, *θα λέγεται ισχυρός ψευδο-πρώτος ως προς τη βάση* b.

Θα αναφέρουμε το παρακάτω κριτήριο ελέγχου πρώτων:

8.1.6 Πρόταση:
Αν n *σύνθετος θετικός ακέραιος τότε ο* n *περνάει το Miller-Rabin test το πολύ για* $\frac{n-1}{4}$*-βάσεις* b, $1 \leqslant b \leqslant n-1$.

Επομένως, αν ένας φυσικός περάσει το test για περισσότερες από $\frac{n-1}{4}$ βάσεις, τότε είναι πρώτος.
Ο αναγνώστης καλείται να πειραματιστεί με τον υπολογισμό των ισχυρών ψευδοπρώτων στο Sage:

Interactive

Ο κώδικας υπολογισμού προέρχεται από τη σελίδα του F. Chamizo.

Για το κριτήριο των Miller-Rabin ο αναγνώστης καλείται να πειραματιστεί με το Sage στον παρακάτω σύνδεσμο:

Interactive

Αποτυπώνουμε την έξοδο του προγράμματος παρακάτω: Με την παράμετρο secur=1 βλέπουμε μια λίστα των περιττών αριθμών $3 < n < 50000$ που περνάνε το test, ενώ είναι σύνθετοι. Αλλάζοντας την παράμετρο σε secur =2 ο αλγόριθμος γίνεται ντετερμινιστικός.

```
secur = 1
for n in range(3,50000,2):
    if (is_prime(n)==False)and\
        (miller_rabin(n,secur)=='likely prime'):
        print n, 'passes the test but is not prime', factor(n)

2047 passes the test but is not prime 23 * 89
3277 passes the test but is not prime 29 * 113
4033 passes the test but is not prime 37 * 109
4681 passes the test but is not prime 31 * 151
8321 passes the test but is not prime 53 * 157
15841 passes the test but is not prime 7 * 31 * 73
29341 passes the test but is not prime 13 * 37 * 61
42799 passes the test but is not prime 127 * 337
49141 passes the test but is not prime 157 * 313
```

8.2. Παραγοντοποίηση

Η δυσκολία του συστήματος RSA βασίζεται στη δυσκολία παραγοντοποίησης. Για την κρυπτανάλυση τέτοιων συστημάτων χρειαζόμαστε αποτελεσματικούς αλγόριθμους παραγοντοποίησης.

8.2.1. Απλή δοκιμή. Πρόκειται για τον απλούστερο δυνατό αλγόριθμο για να παραγοντοποιήσουμε τον φυσικό n, και στον οποίο δοκιμάζουμε όλους τους πρώτους μικρότερους του $\sqrt{n}$

```
def FactorTrial(n):
    primes=prime_range(sqrt(n))
    factors = []
    for p in primes:
        e = 0
        while n % p == 0:
            e = e + 1
            n = n // p
        if e > 0:
            factors.append((p, e))
            if n == 1:
                break
    return (Factorization(factors), n)

FactorTrial(382736482736)
(2^4 * 317, 75460663)
```

Interactive

8.2.2. Αλγόριθμος παραγοντοποίσης του Fermat. Η μέθοδος στηρίζεται στην ακόλουθη

8.2.1 Πρόταση:
Για κάθε περιττό φυσικό αριθμό n, $n > 1$ *υπάρχει μία αμφιμονοσήμαντη αντιστοιχία μεταξύ των παραγοντοποιήσεων του* n, *σε γινόμενο δύο θετικών ακέραιων* $n = ab$, $a \geqslant b > 0$ *και παραστάσεων του* n, *ως διαφορά τετραγώνων* $n = t^2 - s^2$, *όπου* s *και* t *φυσικοί αριθμοί.*
Η αντιστοιχία δίνεται από τις ισότητες

$$t = \frac{a+b}{2},\ s = \frac{a-b}{2}\quad a = t+s,\ b = t-s.$$

Απόδειξη Αν $n = a\cdot b = \left(\frac{a+b}{2}\right)^2 - \left(\frac{a-b}{2}\right)^2 = t^2 - s^2$. Αν πάλι $n = t^2 - s^2 = (t-s)(t+s) = a\cdot b$, όπου $a = t - s$ και $b = t + s$, δηλαδή $t = \frac{a+b}{2}$ και $s = \frac{a-b}{2}$

Η ιδέα του Fermat ήταν, αν $n = a \cdot b$ και $a,\ b$ δύο περιττοί ακέραιοι, περίπου του ίδιου μεγέθους, τότε ο $s = \frac{a-b}{2}$ είναι σχετικά μικρός και ο t λίγο μεγαλύτερος της $\sqrt{n}$. Επομένως, θα μπορούσαμε να υπολογίσουμε τους a και b δοκιμάζοντας διάφορες τιμές του t στις $[\sqrt{n}] + 1$, $[\sqrt{n}] + 2, \ldots$, μέχρι να βρούμε κάποιο t για το οποίο το $t^2 - n = s^2$, είναι τέλειο τετράγωνο.

Παράδειγμα Να παραγοντοποιηθεί ο φυσικός αριθμός $n = 200819$.

Ο $[\sqrt{n}] + 1 = [\sqrt{200819}] + 1 = 449$. Για $t = 449$ υπολογίζουμε $449^2 - 200819 = 782$, το οποίο δεν είναι τέλειο τετράγωνο.

Παίρνουμε $t = 450$, $450^2 - 200819 = 1681 = 41^2$. Επομένως $200819 = 450^2 - 41^2 = (450 + 41)(450 - 41) = 491 \cdot 409$.

Αν οι ακέραιοι a και b δεν είναι του ίδιου μεγέθους για κάθε παραγοντοποίηση του $n = ab$, τότε είναι πιθανόν η μέθοδος Fermat να ανακαλύψει τους παράγοντες $a,\ b$ μετά από αρκετές δοκιμές. Στην περίπτωση είναι πιο βολικό να χρησιμοποιούμε την ακόλουθη γενίκευση.

Επιλέγουμε ένα μικρό φυσικό αριθμό k και θέτουμε $t = k[\sqrt{n}] + 1$, $k[\sqrt{n}] + 2, \ldots$ μέχρι να επιτύχουμε παράσταση της μορφής $t^2 - k \cdot n$ η οποία είναι τέλειο τετράγωνο,

$$t^2 - k \cdot n = s^2$$

Όταν τα επιτύχουμε αυτό έχουμε $(t + s)(t - s) = kn$. Αυτό σημαίνει ότι οι $t + s$ και n έχουν κάποιο, μη-τετριμμένο, κοινό παράγοντα ο οποίος ευρίσκεται από τον υπολογισμό του $(t + s,\ n)$.

Παράδειγμα Να παραγοντοποιηθεί ο 14167.

Αν προσπαθήσουμε με την κλασική παραγοντοποίηση Fermat, θα πρέπει να θέσουμε $t = 377,\ 378,\ \ldots$ και να ...κουραστούμε θέτοντας διάφορες τιμές του t. Αν όμως θέσουμε $t = [\sqrt{3n}+1] = 652,\ 653,\ 654,\ 655$, βρίσκουμε

$$655^2 - 3 \cdot 141467 = 68^2$$

και υπολογίζουμε τον $(655 + 68,\ 141467) = 241$.

Τελικά μια παραγοντοποίηση του αριθμού 14167 είναι $241 \cdot 587$.

Η απάντηση στο ερώτημα γιατί δούλεψε η μέθοδος για $k = 3$ είναι ότι στην παραγοντοποίηση του $n = a \cdot b = 241 \cdot 587$ το $b = 587$ είναι κοντά στο $3a = 3 \cdot 241 = 723$.

Από τα παραπάνω φαίνεται ότι χρειαστήκαμε 4 μόνο τιμές του t, ενώ αν εφαρμόζαμε τη μέθοδο για $k = 1$ θα χρειαζόμασταν 38 τιμές του t.

Στο sage ορίζουμε τη συνάρτηση παραγοντοποίησης:

```
def Ferfac(m):
       if m <= 0: return [m]
       if is_even(m): return [2,m/2]
       a = ceil(sqrt(m))
       while not is_square(a^2-m):
         a = a + 1
       b = sqrt(a^2-m)
       return [a - b,a + b]
```

Την παραπάνω συνάρτηση χρησιμοποιούμε ως εξής:

```
p=next_prime(10^20)
q=next_prime(p+10^3)
p,q,p*q,Ferfac(p*q)
(100000000000000000039,
100000000000000001071,
10000000000000000111000000000000000041769,
[100000000000000000039, 100000000000000001071])
```

Interactive

8.2.3. Αλγόριθμος παραγοντοποίησης του Dixon.

8.2.2 Πρόταση:
Αν x, y *ακέραιοι και* $x^2 \equiv y^2 mod n$ *και* $x \neq \pm y$, *τότε ο φυσικός* $d = (x - y, n)$ *είναι μη-τετριμμένος παράγοντας του* n.

Απόδειξη Έχουμε $n \mid x^2 - y^2 = (x-y)(x+y)$, ενώ n δεν διαιρεί το $(x-y)$ και n δεν διαιρεί το $(x+y)$. Είναι φανερό ότι $d \mid n$. Θα αποδείξουμε ότι $1 < d < n$.

Αν $d = n$, θα είχαμε $n \mid (x-y)$, άτοπο. Αν $d = 1$ τότε αφού $n = (x+y)(x-y)$ και $(x-y, n) = 1$ έπεται ότι $n \mid (x+y)$, πάλι άτοπο. □

Παράδειγμα Υπολογίζουμε ότι $10^2 \equiv 32^2 \text{mod} 77$, $10 \neq 32 \text{mod} 77$, $10 \neq -32 \text{mod} 77$. Επομένως ο 77 και ένας γνήσιος παράγοντας αυτού είναι ο $(10 - 32, 77) = 11$.

Υπάρχουν αρκετές παραλαγές του αλγορίθμου αυτού στο πώς θα υπολογίζουμε τους ακέραιους x, y ώστε $x^2 \equiv y^2 \text{mod} n$. Ας εξετάσουμε μία:

Διαλέγουμε ένα φράγμα B και θεωρούμε τους πρώτους $p_1, \ldots, p_n$ που είναι μικρότεροι ή ίσοι του B. Στη συνέχεια ψάχνουμε θετικούς ακέραιους z ώστε $z^2 \text{mod} N$ να έχει παράγοντες στο σύνολο των

$P = \{p_1, \ldots, p_n\}$. Μπορούμε λοιπόν να γράψουμε

$$z^2 \equiv \prod_{p_i \in P} p_i^{a_i} \text{mod.}$$

Όταν έχουμε αρκετές από τις παραπάνω σχέσεις (αρκεί να έχουμε περισσότερες από το πλήθος του P), τότε μπορούμε να χρησιμοποιήσουμε τη μέθοδο της απαλοιφής του Gauss προκειμένου να πολλαπλασιάσουμε τις σχέσεις αυτές ώστε το πλήθος των παραγόντων στο αριστερό μέλος της εξίσωσης να είναι άρτιος, δηλαδή:

$$z_1^2 z_2^2 \cdots z_k^2 \equiv \prod_{p_i \in P} p_i^{a_{i,1}+a_{i,2}+\cdots+a_{i,k}} \text{ modN}$$

όπου

$$a_{i,1} + a_{i,2} + \cdots + a_{i,k} \equiv 0 \text{mod} 2.$$

Πράγματι $\#P + 1$ σχέσεις της μορφής

$$z_j^2 \equiv \prod_{p_i \in P} p_i^{a_{i,j}} \text{mod},$$

μπορούν να αποτυπωθούν ως ένας πίνακας στο σώμα $\mathbb{F}_2$ με $\#P + 1$ γράμμες και $\#P$ στήλες, από όπου μπορούμε να βρούμε μια σχέση γραμμικής $\mathbb{F}_2$-εξάρτησης.

Ας κάνουμε ένα παράδειγμα: έστω $n = 3439$. Θεωρούμε ως $P = \{2, 3, 5, 7\}$ και έχουμε τις παρακάτω σχέσεις:

x	$x^2 - n$
59	$42 = 2 \cdot 3 \cdot 7$
62	$405 = 3^3 \times 5$
67	$1050 = 2 \times 3 \times 5^2 \times 7$
73	$1890 = 2 \times 3^3 \times 5 \times 7$
143	$17010 = 2 \times 3^5 \times 5 \times 7$

Οι εκθέτες απομονώνονται ως:

αριθμός	εκθέτης
42	(1,1,0,1)
405	(0,4,1,0)
1050	(1,1,2,1)
1890	(1,3,1,1)
17010	(1,5,1,1)

οι οποίοι modulo 2 δίνουν τον πίνακα:

αριθμός	εκθέτης
42	(1,1,0,1)
405	(0,0,1,0)
1050	(1,1,0,1)
1890	(1,1,1,1)
17010	(1,1,1,1)

Για να βρούμε έναν κατάλληλο πολλαπλασιασμό θεωρούμε τον 5×4 πίνακα με στοιχεία από τον $\mathbb{F}_2$

$$= \begin{pmatrix} 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix}$$

και κάθε στοιχείο του πυρήνα θα μας δώσει τη σχέση που θέλουμε. Για παράδειγμα, το $(1,0,1,0,0) \in \ker A$ μας δίνει τον πολλαπλασιασμό:

$$3953^2 = (59 \times 67) \equiv (2 \times 3 \times 5 \times 7)^2 \mathrm{mod} n.$$

Αφού δε $3953 \pm 210 \neq 0 \mathrm{mod} n$ καταλήγουμε στο $(3953 - 210, n) = 19, 3953 + 210, n) = 181$.

Με αυτόν τον τρόπο έχουμε καταλήξει σε μία σχέση τετραγώνων της μορφής $x^2 \equiv y^2 \mathrm{mod} N$ όπως θέλαμε.

Η υλοποίηση στο sage είναι αρκετά πολύπλοκη, αφού χρειαζόμαστε σειρά από αλγορίθμους να χειριστούν κάθε κομμάτι της διαδικασίας. Ακολουθούμε τον κώδικα από το Blog του F. Kraiem και ο αναγνώστης καλείται να πειραματιστεί στους παρακάτω συνδέσμους:

Interactive

Στην παραπάνω υλοποίηση κατασκευάζεται μία υπορουτίνα παραγοντοποίησης ενός ακέραιου ως προς ένα σύνολο πρώτων P η trial(n,primes), μία υπορουτίνα αναγνώρισης αριθμών που διαιρούνται μόνο από πρώτους στο P, η smooth(n,fbase). Αν η είσοδος διαιρείται μόνο από πρώτους στο σύνολο P επιστρέφει τη λίστα των εκθετών, σε διαφορετική περίπτωση δεν επιστρέφει τίποτα. Επιπλέον υλοποιείται μια υπορουτίνα η dixonfact(n,primes) που βρίσκει έναν μη-τετριμμένο παράγοντα.

8.2.4. Ο p-1-αλγόριθμος παραγοντοποίησης του Pollard. Υποθέτουμε ότι μας δίνεται ο φυσικός αριθμός n για τον οποίο υποψιαζόμαστε ότι είναι σύνθετος και θέλουμε να τον παραγοντοποιήσουμε. Επιλέγουμε έναν ακέραιο B, ως φράγμα εργασίας.

1. Θέτουμε $a = 2$
2. Υπολογίζουμε τις δυνάμεις $\alpha = a^j \mathrm{mod} n$ για $j = 2, 3, \ldots, B$
3. Υπολογίζουμε το $d = (\alpha - 1, n)$
4. Αν $1 < d < n$, τότε ο d είναι ένας γνήσιος παράγοντας του n (επιτυχία), αλλιώς δεν βρήκαμε γνήσιο παράγοντα του n (αποτυχία).

Αν τώρα p πρώτος διαιρέτης του n και υποθέτουμε ότι κάθε δύναμη πρώτου διαιρέτη του $p - 1$, έστω q, είναι μικρότερη ή ίση του B θα έχουμε $(p - 1) \mid B!$

Για το τελικό α που θα βρούμε στο δεύτερο βήμα του αλγορίθμου ισχύει

$$\alpha \equiv 2^{B!} \mathrm{mod} n$$

και κατ' επέκταση

$$\alpha \equiv 2^{B!} \mathrm{mod} p,$$

για όλους τους διαιρέτες του n. Επειδή $(p - 1) \mid B!$ έπεται ότι $B! = (p - 1)t$ με $t \in \mathbb{Z}$ και συνεπώς

$$2^{B!} \equiv (2^{p-1})^t \mathrm{mod} p$$

Επειδή $2^{p-1} \equiv 1 \mathrm{mod} p$, τελικά προκύπτει ότι $\alpha \equiv 2^{B!} \equiv 1 \mathrm{mod} p$.

Επειδή $p \mid (\alpha - 1)$ και $p \mid n$, έπεται ότι $p \mid (\alpha - 1, n) =: d$ και συνεπώς $1 < p \leqslant d$. Αν $d = n$, θα είχαμε $n \mid (\alpha - 1)$. Όμως το $\alpha - 1 < n$ οπότε θα έπρεπε $\alpha = 1$. Επομένως, βρίσκουμε έναν μη-τετριμμένο παράγοντα d του n και συνεχίζουμε την προσπάθεια παραγοντοποίησης των d και n/d.

Παράδειγμα: Θεωρούμε τον φυσικό $n = 540143$. Επιλέγουμε $B = 8$. Επομένως $k := [1, 2, \ldots, 8] = 840$. Θέτουμε $a = 2$ και υπολογίζουμε

$$2^{840} \equiv 53047 \bmod n$$

Επίσης $(53047, n) = 421$ συνεπώς $540143 = 421 \cdot 1283$.

Παρατήρηση: Αν το B που επιλέξαμε δεν αρκεί για το σκοπό του επιλέγουμε κάποιον άλλο μεγαλύτερο του αρχικού και επαναλαμβάνουμε τη διαδικασία.

Μερικές φορές ο αλγόριθμος δεν λειτουργεί για $a = 2$, οπότε μπορούμε να δοκιμάσουμε για $a = 3$ και αν πάλι δεν λειτουργεί να δοκιμάσουμε με μεγαλύτερες τιμές του a.

Παράδειγμα Επιθυμούμε να παραγοντοποιήσουμε τον $n = 187$. Επιλέγουμε $B = 15$. Επομένως $k = [1, 2, \ldots, 15] = 360360$. Για $a = 2$ ο $(2^{360360} - 1, 187) = 187$ και δεν καταφέρνουμε να τον παραγοντοποιήσουμε.

Για $a = 3$ έχουμε $3^{360360} - 1 \equiv 66 \bmod 187$ και επομένως $(3^{360360} - 1, 187) = (66, 187) = 11$. Συνεπώς $187 = 11 \cdot 17$.

Παράδειγμα Ο παρακάτω κώδικας sage υλοποιεί τον αλγόριθμο του Pollard:

```
def EKP(B):
     return prod([p^int(math.log(B)/math.log(p))
     for p in prime_range(B+1)])
N=3*13*37
print "N=",N
B=10
print "B=",B
m=EKP(B)
print "EKP=",m
a=2
print gcd(a^m-1,N)
a=3
print gcd(a^m-1,N)
```

Θεωρούμε τον αριθμό $N = 1443$. Το ελάχιστο κοινό πολλαπλάσιο των αριθμών από 1 μέχρι 10 υπολογίζεται να είναι $m = 2520$. Ο μέγιστος κοινός διαιρέτης $(2^m - 1, N) = 1443$ και η μέθοδος του Pollard αποτυγχάνει στην περίπτωση αυτή. Όμως $(3^m - 1, N) = 481$ που είναι ένας μη τετριμμένος διαιρέτης του N. Μπορείτε να δοκιμάστε παραδείγματα στο sage στον σύνδεσμο:

Interactive

8.2.5. Ο αλγόριθμος παραγοντοποίησης ρ του Pollard. Η ιδέα του αλγορίθμου είναι η εξής:

Έστω n σύνθετος ακέραιος και p ο ελάχιστος πρώτος παράγοντας του n. Αν μπορούμε να βρούμε ακέραιους

$$x_0, x_1, x_2, \ldots, x_\ell$$

τέτοιους ώστε για κάποιους δείκτες $i, j \in \{0, 1, 2, \ldots, \ell\}$ να ισχύουν

$$x_i \equiv x_j \mathrm{mod} p \text{ και } x_i \neq x_j \mathrm{mod} n,$$

τότε ο $(x_i - x_j, n)$ είναι ένας γνήσιος διαιρέτης του n αφού $p \mid (x_i - x_j, n) \mid n$ και $(x_i - x_j, n) \neq n$.

Τα ερωτήματα που προκύπτουν είναι πώς θα επιλέξουμε τα x_i και στη συνέχεια με ποιον σύντομο τρόπο θα διαπιστώσουμε την ύπαρξη ενός κατάλληλου ζευγαριού με τις παραπάνω ιδιότητες. Είναι φανερό ότι ο υπολογισμός του $(x_i - x_j, n)$ για όλους τους δείκτες $0 \leqslant i, j \leqslant \ell$ είναι μια αρκετά χρονοβόρα διαδικασία.

Η ακολουθία $x_0, x_1, \ldots, x_\ell$ θα πρέπει να είναι κατά το δυνατόν τυχαία (random) ακολουθία. Επιλέγουμε τυχαία το $x_0 = 2$ και μια πολυωνυμική συνάρτηση $f(x)$ με ακέραιους συντελεστές και υπολογίζουμε αναδρομικά τους υπόλοιπους όρους της ακολουθίας

$$x_{i+1} \equiv f(x_i) \mathrm{mod} n, 0 \leqslant x_{i+1} < n.$$

Για να επαναλαμβάνονται οι όροι της ακολουθίας (mod$p$) μετά από λογικό αριθμό βημάτων θα πρέπει να επιλέξουμε κατάλληλη πολυωνυμική συνάρτηση $f(x)$. Δεν θέλουμε να υπάρχει κάποιος ακέραιος $a \mathrm{mod} p$ τέτοιος ώστε η ακολουθία

$$x_1 = f(a), x_2 = f(x_1) = f(f(a)) = f^{(2)}(a), \ldots, x_\ell = f^{(\ell)}(a)$$

να δίνει για μεγάλο ℓ διαφορετικές τιμές mod$p$.

Ας ονομάσουμε ((ρ-αριθμό)) μιας τέτοιας ακολουθίας x_i ως προς τον πρώτο αριθμό p τον μεγαλύτερο ακέραιο m για τον οποίο υπάρχει ένα $a \mathrm{mod} p$ τέτοιο ώστε όλοι οι όροι της ακολουθίας

$$f(a), \ldots, f^{(m)}(a)$$

να είναι ανά δύο διαφορετικοί mod$p$. Εμείς θέλουμε ακολουθίες με μικρό ρ-αριθμό. Επομένως δεν μπορούμε να επιλέξουμε πρωτοβάθμια πολυωνωμική συνάρτηση

$$f(x) = aX + b.$$

Αυτό διότι, όταν $a \neq 1 \mathrm{mod} p$, τότε ο ((ρ-αριθμός)) είναι η τάξη του $a \mathrm{mod} p$ και αυτός είναι συνήθως ένας μεγάλος διαιρέτης του $p - 1$.

Αν $a \equiv 1 \mathrm{mod} p$ και $b \neq 0 \mathrm{mod} p$, τότε $f(X) = X + b$ και ο ρ-αριθμός είναι ακριβώς p, αφού $f(x_1) \equiv f(x_2) \mathrm{mod} p$ αν και μόνο αν $x_1 \equiv x_2 \mathrm{mod} p$.

Θα πρέπει επομένως να επιλέξουμε μία πολυωνυμική συνάρτηση δευτέρου βαθμού φαίνεται ότι μια καλή επιλογή είναι η πολυωνυμική συνάρτηση $f(X) = X^2 + 1$.

Τώρα είναι φανερό ότι αν $x_i \equiv x_j \mathrm{mod} p$, τότε και $x_{i+1} \equiv f(x_i) \equiv f(x_j) \equiv x_{j+1} \mathrm{mod} p$. Αυτό σημαίνει ότι η ακολουθία γίνεται από ένα σημείο και πέρα, περιοδική (mod$p$) με περίοδο $(i-j)$. Συνεπώς, αν $r \geqslant i, t \geqslant i$, kai $r \equiv t \mathrm{mod}(i - j)$ τότε

$$x_r \equiv x_t \mathrm{mod} p.$$

Αν λοιπόν s είναι το ελάχιστο πολλαπλάσιο του $(i - j)$ το οποίο είναι $\geqslant i$, έχουμε

$$x_{2s} \equiv x_s \mathrm{mod} p.$$

Υπολογίζουμε επομένως πολύ λιγότερους μέγιστους κοινούς διαιρέτες από τους συνδυασμούς ανά δύο. Συγκεκριμένα υπολογίζουμε τους

$$(x_{2s} - x_s, n) \text{ με } s = 1, 2, 3, \ldots$$

μέχρι να βρούμε κάποιον διάφορο του 1 και του n.

Παράδειγμα Έστω $n = 2047$. Για $x_0 = 2$ και $f(x) = x^2 + 1$ υπολογίζουμε τους όρους της ακολουθίας

$$x_{i+1} = f(x_i) \bmod n$$

$$\begin{array}{cccc} x_0 = 2 & x_1 = 5 & x_2 = 26 & x_3 = 677 \\ x_4 = 1849 & x_5 = 312 & x_6 = 1136 & x_7 = 887 \\ x_8 = 722 & x_9 = 1347 & x_{10} = 768 & x_{11} = 289 \quad x_{12} = 1642 \end{array}$$

Στη συνέχεια υπολογίζουμε τους

$$(x_{2s} - x_s, n), \text{ για } s = 1, 2, 3, 4, 5, 6$$

$$(26 - 5, 2047) = 1$$

$$(1849 - 26, 2047) = 1$$

$$(1136 - 677, 2047) = 1$$

$$(722 - 1842, 2047) = 1$$

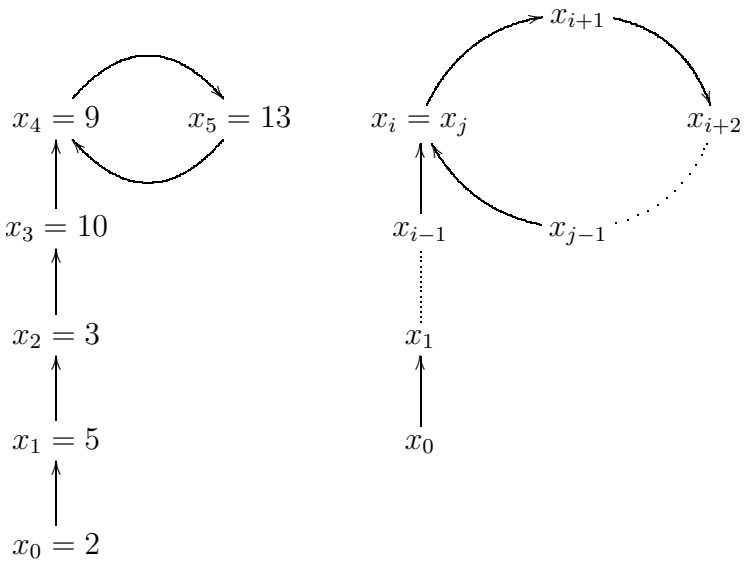
$$(768 - 312, 2047) = 1$$

$$(1642 - 1136, 2047) = 23$$

Επομένως $2047 = 23 \cdot 89$.

Στο παράδειγμά μας έχουμε

$$\begin{array}{ccc} x_1 \equiv 5 \bmod 23 & x_2 \equiv 3 \bmod 23 & x_3 \equiv 10 \bmod 23 \\ x_4 \equiv 9 \bmod 23 & x_5 \equiv 13 \bmod 23 & x_6 \equiv 9 \bmod 23 \\ x_7 \equiv 13 \bmod 23 & x_8 \equiv 9 \bmod 23 & x_9 \equiv 13 \bmod 23 \\ x_{10} \equiv 9 \bmod 23 & x_{11} \equiv 13 \bmod 23 & x_{12} \equiv 9 \bmod 23 \end{array}$$



Σχήμα 8.2. Σχήμα ρ

Παρατήρηση Όταν γνωρίζουμε το x_i προκειμένου να υπολογίσουμε το x_{2i} δεν χρειάζεται να υπολογίσουμε όλους τους ενδιάμεσους όρους

$$x_{i+1}, x_{i+2}, \ldots, x_{2i-1}, x_{2i}.$$

Αν $y_i = x_{2i}$ παρατηρούμε ότι

$$y_1 = x_2 = f(x_1) = f(f(x_0)) = f(f(y_0)),$$
$$y_2 = x_4 = f(x_3)f(f(x_2)) = f(f(y_1))$$

και γενικότερα

$$y_i = x_{2i} = f(f(y_{i-1})).$$

Επομένως σε κάθε βήμα υπολογίζουμε

$$x_i = f(x_{i-1}) \mathrm{mod} n$$
$$y_i = f(f(y_{i-1})) \mathrm{mod} n$$

8.2.6. Παραγοντοποίηση με ελλειπτικές καμπύλες. Όπως είδαμε σε προηγούμενο κεφάλαιο, η μέθοδος RSA βασίζεται στη δυσκολία να παραγοντοποιήσουμε μεγάλους ακέραιους αριθμούς. Στο κεφάλαιο αυτό θα περιγράψουμε τη μέθοδο του Lenstra (Lenstra 1987), η οποία χρησιμοποιεί ελλειπτικές καμπύλες για την παραγοντοποίηση.

Σχήμα 8.3. "Hendrik Lenstra MFO" Δημιουργός: George M. Bergman, Το παρόν έργο αποτελεί κοινό κτήμα (public domain). Πηγή: Wikimedia Commons

8.2.7. Από τη μέθοδο του Pollard στη μέθοδο του Lenstra. Σταθεροποιούμε ένα B όπως και στη μέθοδο του Pollard. Αν $N = pq$ με p, q πρώτοι ώστε οι $p-1$ και $q-1$ να μην είναι B-ομαλοί, τότε η μέθοδος του Pollard θα αποτύχει.

Η μέθοδος του Pollard δουλεύει στην ουσία στην κυκλική ομάδα $\mathbb{F}_p^*$ η οποία έχει σταθερή τάξη $p-1$. Οι ελλειπτικές καμπύλες δίνουν μια οικογένεια ομάδων που σχετίζονται με το p, αλλά η τάξη τους μπορεί να πάρει τις τιμές

$$\#E(\mathbb{F}_p) = p + 1 \pm s,$$

όπου το s μπορεί να πάρει τιμές στο διάστημα $0 \leqslant s \leqslant 2\sqrt{p}$ σύμφωνα με το θεώρημα του Hasse. Υπάρχει λοιπόν πολύ μεγαλύτερη επιλογή στις τάξεις της ομάδας. Ο αριθμός $p-1$ μπορεί να μην είναι B-ομαλός αλλά να είναι B-ομαλός ο $p-2$.

Περιγραφή της Μεθόδου

1. Διαλέγουμε το B.
2. Υπολογίζουμε το ελάχιστο κοινό πολλαπλάσιο των αριθμών $1, \ldots, B$.
3. Διαλέγουμε μια τυχαία ελλειπτική καμπύλη στον δακτύλιο $\mathbb{Z}/N\mathbb{Z}$ και ένα σημείο επί αυτής. Για παράδειγμα αν διαλέξουμε ένα τυχαίο $a \in \mathbb{Z}/N\mathbb{Z}$ ώστε $4a^3 + 27$ δεν είναι διαιρετό με N τότε το σημείο $P = (0, 1)$ είναι σημείο πάνω στην ελλειπτική καμπύλη $y^2 = x^3 + ax + 1$.
4. Επιχειρούμε να υπολογίζουμε τις δυνάμεις mP. Αν κάπου αποτύχουμε να υπολογίσουμε μια δύναμη αυτό θα οφείλεται στο ότι κάποιος παρονομαστής Π στους τύπους πρόσθεσης σημείων είναι διαιρετός με N. Αν ο μέγιστος κοινός διαιρέτης $(\Pi, N) < N$, τότε το (Π, N) είναι ένας μη-τετριμμένος διαιρέτης του N και η μέθοδος έχει ολοκληρωθεί. Διαφορετικά δοκιμάζουμε με διαφορετική ελλειπτική καμπύλη.

Ο παρακάτω κώδικας είναι από το βιβλίο (Stein 2008) **Elementary Number Theory**

```
def ecm(N, B=10^3, trials=10):
    m = prod([p^int(math.log(B)/math.log(p))
              for p in prime_range(B+1)])
    R = Integers(N)
    R.is_field = lambda : True
    for _ in range(trials):
            while True:
                a = R.random_element()
                if gcd(4*a.lift()^3 + 27, N) == 1: break
            try:
                m * EllipticCurve([a, 1])([0,1])
            except ZeroDivisionError, msg:
                # msg: "Inverse of <int> does not exist"
                return gcd(Integer(str(msg).split()[2]), N)
    return 1

N=5959
ecm(N, B=20)
```

Interactive 1 Interactive 2

Lenstra Jr., H. W. (1987). "Factoring integers with elliptic curves". Annals of Mathematics 126 (3): 649–673. JSTOR 1971363. MR 89g:11125

8.2.8. Η πρόκληση παραγοντοποίησης της RSA. Τα εργαστήρια της RSA, μιας εταιρίας που ιδρύθηκε από τους εφευρέτες του ομώνυμου αλγορίθμου έχουν δημοσιεύσει μια λίστα από σύνθετους αριθμούς, για τους οποίους μέχρι το 2007 έδιναν και χρηματικά έπαθλα για την παραγοντοποίησή τους. Κάποιοι από αυτούς παραγοντοποιήθηκαν άμεσα, ενώ ο μεγαλύτερος από αυτούς (για τον οποίο υπήρχε και ένα έπαθλο 200.000 δολλαρίων) θα αργήσει πολύ να παραγοντοποιηθεί.

```
RSA-2048 =  25195908475657893494027183240048398571
            42928212620403202777713783604366202070
            75955562640185258807844069182906412495
            15082189298559149176184502808489120072
            84499268739280728777673597141834727026
            18963750149718246911650776133798590957
            00097330459748808428401797429100642458
            69181719511874612151517265463228221686
            99875491824224336372590851418654620435
            76798423387184774447920739934236584823
            82428119816381501067481045166037730605
            62016196762561338441436038339044149526
            34432190114657544454178424020924616515
            72335077870774981712577246796292638635
            63732899121548314381678998850404453640
            23527381951378636564391212010397122822
            120720357
```

Βιβλιογραφία

Lenstra, H W, Jr. 1987. “Factoring Integers with Elliptic Curves.” *Ann. Math.*, Second Series, 126 (3). Annals of Mathematics: 649–73. doi:10.2307/1971363.

Stein, W. 2008. *Elementary Number Theory: Primes, Congruences, and Secrets: A Computational Approach*. Undergraduate Texts in Mathematics. Springer New York. https://books.google.gr/books?id=5hYd0yX4mrMC.

Αντωνιάδης, Ι., and Α. Κοντογεώργης. 2015. *Θεωρία Αριθμών Και Εφαρμογές*. Εκδόσεις Κάλλιπος.

9

Κατασκευή Ελλειπτικών καμπυλών με δεδομένη τάξη

Σε αυτό το κεφάλαιο αντιμετωπίζουμε τα παρακάτω προβλήματα:

1. Δοσμένης μιας ελλειπτικής καμπύλης E ορισμένης πάνω από ένα πεπερασμένο σώμα $\mathbb{F}_q$ πώς μπορούμε να μετρήσουμε την τάξη της ομάδας $\#E(\mathbb{F}_p)$;
2. Αν δοθεί ένας αριθμός μπορούμε να κατασκευάσουμε μια ελλειπτική καμπύλη που να έχει τάξη ίση με N;

Τα παραπάνω προβλήματα σχετίζονται άμεσα με την ασφάλεια των αλγορίθμων που παράγονται από μια δεδομένη ελλειπτική καμπύλη. Προκειμένου ένα ελλειπτικό κρυπτοσύστημα να είναι ασφαλές στις γνωστές επιθέσεις θα πρέπει η τάξη της ελλειπτικής καμπύλης να πληροί μια σειρά από ιδιότητες. Για περισσότερες πληροφορίες σχετικά με τις μεθόδους που χρησιμοποιούμε παραπέμπουμε στο (Blake, Seroussi, and Smart 1999). Για μια περισσότερο θεωρητική προσέγγιση της θεωρίας των ελλειπτικών καμπυλών παραπέμπουμε στο (Αντωνιάδης 1999), (Milne 2006) και (Silverman 1986).

9.1. Αλγόριθμοι μέτρησης σημείων

9.1.1. Ο Αλγόριθμός του Shanks. Ο αλγόριθμος αυτός ξεκινάει με ένα τυχαίο σημείο $P \in E(\mathbb{F}_p)$ και υπολογίζει έναν ακέραιο m στο διάστημα $(p+1-2\sqrt{p}, p+1+2\sqrt{p})$, τέτοιον ώστε $[m]P = 0$. Εάν ο m είναι ο μόνος ακέραιος με αυτή την ιδιότητα, τότε σύμφωνα με το φράγμα του Hasse προκύπτει ότι

$$m = \#E(\mathbb{F}_p).$$

Για να βρει το σημείο εκκίνησης $P = (x, y) \in E(\mathbb{F}_p)$, ο αλγόριθμος διαλέγει τυχαίες τιμές του x ώσπου το

$$x^3 + ax + b$$

να είναι τετράγωνο στο $\mathbb{F}_p$. Τότε υπολογίζει μία τετραγωνική ρίζα y του $x^3 + ax + b$.

Ο αριθμός m υπολογίζεται σύμφωνα με τη στρατηγική baby step giant step που μελετήσαμε στο πρόβλημα του διακριτού λογαρίθμου. Ο αλγόριθμος δίνεται από τα παρακάτω βήματα:

1. Επιλέγουμε τυχαίο σημείο $P \in E(\mathbb{F}_p)$ και θέτουμε $k = \lceil 2\sqrt[4]{p} \rceil$.
2. Υπολογίζουμε τα $i \cdot P$ για τις τιμές $i = 0, \ldots, k-1$. Αν για κάποιο i υπολογίσουμε $i \cdot P = 0$ τότε επιστρέφουμε στο βήμα 1 και επιλέγουμε ένα νέο σημείο P.
3. Θέτουμε $Q = k \cdot P$.

4. Υπολογίζουμε το
$$R_j = \lfloor p + 1 - 2\sqrt{p} \rfloor \cdot P + j \cdot Q.$$
για τις τιμές $j = 1, \ldots, k$ και ελέγχουμε αν $R_j = i \cdot P$ για κάποιο i. Αν βρούμε μόνο ένα ζευγάρι (i, j) με $R_j = i \cdot P$ τότε η τάξη της ομάδας είναι
$$\#E(\mathbb{F}_p) = \lfloor p + 1 - 2\sqrt{p} \rfloor + k \cdot j - i$$
και ο αλγόριθμος τερματίζεται. Σε διαφορετική περίπτωση αν βρούμε δύο τέτοια ζευγάρια (i, j) και (i', j') μπορούμε να υπολογίσουμε την τάξη του σημείου P από τη σχέση
$$|P| = |k(j - j') - (i - i')|.$$
Στην περίπτωση που $|P| < \sqrt{p} - 1$, επιστρέφουμε στο βήμα 1. και διαλέγουμε ένα άλλο σημείο.

5. Υπολογίζουμε ένα δεύτερο τυχαίο σημείο $P' \in E(\mathbb{F}_p)$. Με τα βήματα 2-4 υπολογίζουμε την τάξη του. Υπολογίζουμε την τάξη του P' στην ομάδα πηλίκο $E(\mathbb{F}_p)/\langle P \rangle$, δηλαδή τον ελάχιστο διαιρέτη του d' του $|P'|$ ώστε $d' \cdot P' \in \langle P \rangle$. Αυτό πάλι μπορεί να γίνει με τη βοήθεια μιας baby-step giant step μεθόδου. Αν $d = |P| \cdot d' < 4\sqrt{p}$, τότε επιστρέφουμε στο βήμα 5.

6. Προσδιορίζουμε το ελάχιστο πολλαπλάσιο x του d στο διάστημα $[p+1-2\sqrt{p}, p+1+2\sqrt{p}]$. Τότε το $\#E(F_p) = x$ και ο αλγόριθμος τερματίζεται.

Θα περιγράψουμε τώρα γιατί ο παραπάνω αλγόριθμος δίνει αποτελέσματα. Η συνθήκη τερματισμού στο βήμα 4 είναι σωστή γιατί η τάξη της ομάδας βρίσκεται στο διάστημα του Hasse. Από την άλλη, η τάξη είναι πολλαπλάσιο της τάξης του P και υπάρχει μόνο ένα πολλαπλάσιο του P στο διάστημα Hasse αφού εξασφαλίσαμε ότι $|P| \geqslant 4\sqrt{p}$ και αυτό πρέπει να είναι η τάξη της ομάδας.

Επιπλέον γνωρίζουμε ότι πάνω από το $\mathbb{F}_p$ η δομή της ομάδας $E(\mathbb{F}_p)$ είναι η
$$E(\mathbb{F}_p) \cong \frac{\mathbb{Z}}{m\mathbb{Z}} \times \frac{\mathbb{Z}}{n\mathbb{Z}},$$
όπου χωρίς περιορισμό της γενικότητας μπορούμε να υποθέσουμε ότι $m \geqslant n \geqslant 1$. Αν $m \geqslant 4\sqrt{p}$ τότε μπορεί να αποδειχτεί ότι ένα σχετικά μεγάλο μέρος των σημείων της E έχει τάξη $\geqslant 4\sqrt{p}$. Αν βρεθεί ένα τέτοιο σημείο τότε ο αλγόριθμος τερματίζεται στο βήμα 4.

Σε κάθε περίπτωση $\#E(\mathbb{F}_p) \geqslant (\sqrt{p} - 1)^2$ και συνεπώς $m\sqrt{p} - 1$. Συνεπώς, είναι πολύ πιθανό το βήμα 1. να επιλέξει ένα τέτοιο σημείο μετά από επαναλήψεις των βημάτων 1-4. Για να ολοκληρωθεί ο υπολογισμός θα πρέπει να βρεθεί ένα σημείο P' με τάξη $\geqslant 5$ στην ομάδα $E(\mathbb{F}_p/\langle P \rangle)$. Όμως αν $m < 4\sqrt{p}$, τότε ένα τέτοιο σημείο θα βρεθεί σχετικά γρήγορα.

Για μία τυχαία καμπύλη ο αλγόριθμος θα τερματιστεί σύντομα στο βήμα 4. Όμως υπάρχουν για παράδειγμα καμπύλες με $p = k^2 + 1$ και
$$E(\mathbb{F}_p) \cong \frac{\mathbb{Z}}{p\mathbb{Z}} \times \frac{\mathbb{Z}}{p\mathbb{Z}}.$$
Για τις καμπύλες αυτές απαιτούνται τα επιπλέον βήματα.

9.1.2. Ο Αλγόριθμός του J. F. Mestre. Ο αλγόριθμός δίνει μια εναλλακτική αντιμετώπιση στην περίπτωση που ο αλγόριθμος του Shanks δεν τερματίζεται στα βήματα 1-4.

Χρησιμοποιεί την έννοια της "τετραγωνικής διαστροφής" (quadratic twist!) μιας ελλειπτικής καμπύλης. Συνοπτικά αν η ελλειπτική καμπύλη E εκφράζεται από την εξίσωση
$$y^2 = x^3 + ax + b,$$

τότε η διεστραμμένη καμπύλη E' δίνεται από τον τύπο

$$gy^2 = x^3 + ax + b$$

για κάποιο μη τετραγωνικό υπόλοιπο $g \in \mathbb{F}_p^*$. Η κλάση ισομορφισμού αυτής της καμπύλης δεν εξαρτάται από την επιλογή του g. Η εξίσωση του Weierstrass για την καμπύλη E' είναι,

$$y^2 = x^3 + ag^2x + bg^3.$$

Οι δύο καμπύλες έχουν τάξεις που ικανοποιούν τη σχέση

$$\#E(\mathbb{F}_p) + \#E'(\mathbb{F}_p) = 2(p+1),$$

οπότε για τον υπολογισμό του $\#E(\mathbb{F}_p)$ μπορούμε να υπολογίσουμε το $\#E'(\mathbb{F}_p)$. Επιπλέον θα δούμε ότι αν ο εκθέτης της μιας καμπύλης είναι μικρός τότε ο εκθέτης της άλλης δεν είναι.

Μπορούμε να χρησιμοποιήσουμε αυτή την παρατήρηση ως εξής: εάν για την ελλειπτική καμπύλη E ο αλγόριθμος του Shanks απέτυχε για κάποιον αριθμό σημείων P, επειδή κάθε φορά περισσότερες από μία τιμές του m βρέθηκαν ώστε $[m]P = O$, τότε αντικαθιστούμε την E με την E' και προσπαθούμε ξανά.

Η ομάδα $E(\mathbb{F}_p)$ είναι ακριβώς ο πυρήνας του ενδομορφισμού $F-Id$ ο οποίος αφήνεται να δρασει στην ομάδα $E(\overline{\mathbb{F}}_p)$. Συνεπώς, ο εκθέτης της $E(\mathbb{F}_p)$ είναι $(p+1-t)/n$ όπου n είναι ο μέγιστος ακέραιος τέτοιος ώστε η $E(\mathbb{F}_p)$ να περιέχει μια υποομάδα ισομορφική με το $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. Ισοδύναμα ο n είναι ο μέγιστος ακέραιος για τον οποίο $F \equiv 1 (\mathrm{mod} n)$ στον $\mathrm{End}(E)$.

9.1.1 Θεώρημα:
Έστω $p > 457$ πρώτος κι έστω E μία ελλειπτική καμπύλη επί του $\mathbb{F}_p$. Τότε είτε η E είτε η διαστροφή της E', περιέχει ένα $\mathbb{F}_p$-ρητό σημείο τάξης το λιγότερο $\sqrt[4]{p}$.

Απόδειξη Οι δακτύλιοι ενδομορφισμών των E, είναι ισόμορφοι με την ίδια τετραγωνική τάξη $\mathcal{O}$ διακρίνουσας d. Έστω F ο ενδομορφισμός του Frobenious της E. Έστω ακόμη n ο μέγιστος ακέραιος τέτοιος ώστε $F \equiv 1 (\mathrm{mod} n)$ στο $\mathrm{End}(E)$ και $N = (p+1-t)/n$ να είναι ο εκθέτης της $E(\mathbb{F}_p)$. Έχουμε τότε ότι,

$$\mathbb{Z}[F] \subset \mathbb{Z}\left[\frac{F-1}{n}\right] \subset \mathcal{O}$$

από όπου προκύπτει ότι το n διαιρεί τον δείκτη $[\mathcal{O} : \mathbb{Z}[F]]$. Αφού $[\mathcal{O} : \mathbb{Z}[F]]^2$ είναι ίσο με το πηλίκο των διακρινουσών των τάξεων $\mathcal{O}$ και $\mathbb{Z}$ έχουμε ότι ο n^2 διαιρεί τον $(t^2-4p)/d$, όπου t^2-4p είναι η διακρίνουσα τάξης του $\mathbb{Z}[F]$.

Ομοίως, έστω m ο μέγιστος ακέραιος τέτοιος ώστε $-F \equiv 1 (\mathrm{mod} m)$ στον $\mathrm{End}(E)$ κι έστω $M = (p+1-t)/m$ ο εκθέτης της $'$. Τότε,

$$\mathbb{Z}[F] \subset \mathbb{Z}\left[\frac{F-1}{m}\right] \subset \mathcal{O}$$

Οπότε ο m^2 επίσης διαιρεί τον $(t^2-4p)/d$.

Αφού ο n διαιρεί τον $F-1$ και ο m διαιρεί τον $F+1$ παρατηρούμε ότι ο (n, m) διαιρεί τον $(F-1, F+1)$ ο οποίος διαιρεί το 2. Οπότε έχουμε,

$$n^2m^2 | 4\frac{t^2-4p}{d}.$$

Επειδή $|d| \geqslant 3$ αυτό σημαίνει ότι

$$(nm)^2 \, 4\frac{4p-t^2}{d}.$$

Εάν $N, M < 4\sqrt{2}$, έχουμε ότι,

$$((p+1)^2-t^2)^2 = (nNmM)^2 < (4\sqrt{p})^4 \cdot 4\frac{4p-t^2}{3}$$

οπότε,

$$p^4 + 4p^3 < (p+1)^4\frac{4^6}{3}p^3 - t^4 - \left(\frac{4^5}{3} - 2(p+1)^2\right)t^2 \leqslant \frac{4^6}{3}p^3$$

το οποίο σημαίνει ότι $p < 1362$. Εάν εξετάσουμε όλες τις περιπτώσεις για $p \leqslant 457$ θα δούμε πως το θεώρημα ισχύει.

Για να είναι σίγουρος κανείς ότι ο αλγόριθμος του Shanks θα δουλέψει για μία ελλειπτική καμπύλη E, δεν χρειάζεται να βρει ένα ρητό σημείο αυτής, τάξης το λιγότερο $4\sqrt{p}$. Αυτό που χρειάζεται είναι ένα σημείο P της καμπύλης με την ιδιότητα όπως περιγράφεται στο επόμενο

9.1.2 Θεώρημα:
Έστω $p > 229$ πρώτος κι έστω E μία ελλειπτική καμπύλη επί του $\mathbb{F}_p$. Τότε είτε η E είτε η διαστροφή της E' περιέχει ένα $\mathbb{F}_p$-ρητό σημείο P, με την ιδιότητα ότι ο μόνος ακέραιος $m \in (p+1-2\sqrt{p}, p+1+2\sqrt{p})$ για τον οποίο ισχύει $[m]P = O$, είναι η τάξη της ομάδας των σημείων της ελλειπτικής καμπύλης.

Απόδειξη Από την απόδειξη του αποτελέσματος του J. F. Mestre το θεώρημα ισχύει για $p > 457$. Ένας υπολογισμός για κάθε περίπτωση ξεχωριστά μας δείχνει ότι ισχύει για κάθε $p > 229$.

9.1.3. Ο Αλγόριθμός του Schoof. Το θεώρημα του Hasse εξασφαλίζει ότι

$$\#E(\mathbb{F}_q) = q + 1 - t, |t| \leqslant 2\sqrt{q}.$$

Η κύρια ιδέα του αλγόριθμου είναι ο καθορισμός του t modulo ενός συνόλου πρώτων αριθμών l, με $l \leqslant l_{max}$, όπου l_{max} είναι ο ελάχιστος πρώτος τέτοιος ώστε,

$$\prod_{2 \leqslant l \leqslant l_{max}} l > 4\sqrt{q}.$$

Τότε εύκολα υπολογίζεται από το Κινέζικο Θεώρημα Υπολοίπων η τιμή του t, οπότε καθορίζεται και η τάξη της ομάδας.

Αρχικά παρατηρούμε ότι εύκολα βρίσκουμε την τιμή του t όταν $l = 2$ για κάθε μία περίπτωση σώματος επί του οποίου βρισκόμαστε.

Για την περίπτωση της περιττής χαρακτηριστικής έχουμε ότι $t = \#E(\mathbb{F}_q)$ modulo 2, οπότε εύκολα προκύπτει ότι

$$\#E(\mathbb{F}_q) \equiv 1 (\mathrm{mod} 2)$$

αν και μόνο αν το $x^3 + ax + b$ ανάγωγο επί του $\mathbb{F}_q$. Η τελευταία σχέση είναι ισοδύναμη με την

$$(x^3 + ax + b, x^q - x) = 1.$$

Για σώματα χαρακτηριστικής 2, επειδή η καμπύλη είναι non-supersingular έχουμε ότι $t \equiv 1$ modulo 2.

Για l περιττό τώρα. Ο ενδομορφισμός του Frobenious ικανοποιεί την εξίσωση,

$$F^2 - [t]F + [q] = 0.$$

Αυτό θα το χρησιμοποιήσουμε για τα σημεία στο $E[l]^* = E[l]\backslash\{O\}$. Έστω,

$$q_l = q(\mathrm{mod} l)$$

και

$$t_l = t(\mathrm{mod} l)$$

όπου οι ελάχιστοι μη αρνητικοί αντιπρόσωποι της κλάσης υπολοίπων είναι ο q_l και ο t_l. Εάν κάποια τιμή του $\tau \in \{0, 1, \ldots, l-1\}$ βρεθεί ώστε για κάποιο σημείο $P = (x, y) \in E[l]^*$ να έχουμε,

$$(x^{q^2}, y^{q^2}) + [q_l](x, y) = [\tau](x^q, y^q),$$

τότε προκύπτει ότι $\tau = t_l$, δηλαδή βρίσκουμε το t modulo l. Το τ το οποίο ικανοποιεί την εξίσωση είναι μοναδικό αφού το l είναι πρώτος και $P \neq O$.

Για τον καθορισμό της τιμής του τ, ισχυριζόμαστε προς το παρόν ότι όλες οι τιμές του $\tau \in \{0, 1, \ldots, l-1\}$ δοκιμάζονται. Πρώτα υπολογίζονται οι x-συντεταγμένες και στα δύο μέλη της παραπάνω εξίσωσης, για τον δοσμένο πρώτο l και την τιμή του τ το οποίο εξετάζουμε, τα οποία είναι ρητές συναρτήσεις των x, y, οι οποίες περιέχουν τα πολυώνυμα διαίρεσης. Στη συνέχεια με την πράξη της πρόσθεσης ελλειπτικών καμπυλών υπολογίζεται το

$$(x^{q^2}, y^{q^2}) + [q_l](x, y)$$

Με απαλοιφή παρανομαστών κι εάν είναι απαραίτητο μειώνοντας όσες δυνάμεις του y είναι μεγαλύτερες της μονάδας modulo στην εξίσωση της καμπύλης προκύπτει μία εξίσωση της μορφής

$$a(x) + yb(x) = 0 \to y = \frac{a(x)}{b(y)}.$$

Η εξίσωση της καμπύλης με βάση κάποια από τις παραπάνω δύο εξισώσεις, έχει ως μεταβλητή πλέον μόνο το x, οπότε γράφεται ως,

$$h_X(x) = 0.$$

Για να ελέγξουμε εάν η $h_X(x) = 0$ έχει λύση για την x-συντεταγμένη του σημείου που ανήκει στο $E[l]^*$ υπολογίζουμε τον μέγιστο κοινό διαιρέτη (h_X, f_l). Εάν, $(h_X, f_l) = 1$, τότε δεν υπάρχει λύση στο $E[l]^*$ η οποία να ικανοποιεί τη ζητούμενη εξίσωση, οπότε δοκιμάζουμε την επόμενη τιμή του τ. Εάν, $(h_X, f_l) \neq 1$, τότε υπάρχει σημείο στο $E[l]^*$ τέτοιο ώστε,

$$(x^{q^2}, y^{q^2}) + [q_l](x, y) = [\tau](x^q, y^q) = \pm[\tau](x^q, y^q).$$

Το πρόσημο του σημείου του δεξιού μέλους της παραπάνω εξίσωσης δεν είναι προκαθορισμένο, διότι το πρόσημο της x-συντεταγμένης είναι το ίδιο για κάθε πρόσημο. Για να το καθορίσουμε, ισχυριζόμαστε αρχικά ότι είναι $+$. Υπολογίζουμε την y-συντεταγμένη και στα δύο μέλη της εξίσωσης, όπου όπως με την x-συντεταγμένη, μετά απο την απαλοιφή παρανομαστών και την αντικατάσταση της y μεταβλητής, προκύπτει μια εξίσωση της μορφής,

$$h_Y(x) = 0$$

όπου το h_Y έχει αναχθεί στον βαθμό $O(l^2)$

Όμοια, εάν $(h_Y, f_l) \neq 1$ τότε υπάρχει ένα σημείο που ικανοποιεί την εξίσωση και το πρόσημο είναι $+$. Εάν, $(h_X, f_l) = 1$ τότε το πρόσημο είναι $-$.

Παρατηρούμε ότι για δοσμένο τ η διαδικασία στην πραγματικότητα ελέγχει τα $\pm\tau$, οπότε είναι επαρκές το τ να ανήκει στο $0 \leqslant \tau \leqslant \frac{l-2}{2}$.

9.2. Κατασκευή ελλειπτικών καμπυλών

9.2.1. Μιγαδική Προσέγγιση ξανά. Σε αυτή την παράγραφο θεωρούμε τα lattices παράγονται από τα $1, \tau$, όπου το $\tau = a + ib$ είναι ένας μιγαδικός αριθμός με $b > 0$. Το σύνολο των αριθμών που είναι επιτρεπτές για το τ ονομάζεται υπερβολικό επίπεδο και συμβολίζεται με $\mathbb{H}$. Έτσι, σε αυτή τη θεώρηση οι σειρές Eisenstein που ορίστηκαν παραπάνω είναι συναρτήσεις του τ. Ομοίως η διακρίνουσα και η j-invariant επίσης μπορούν να γραφούν ως συναρτήσεις του τ.

Οι συναρτήσεις g_2, g_3, Δ, j ως συναρτήσεις του $\tau \in \mathbb{H}$ παραμένουν αναλλοίωτες κάτω από μετασχηματισμούς της μορφής:

$$\tau \mapsto \frac{a\tau + b}{c\tau + d}, \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2, \mathbb{Z}).$$

Ειδικότερα, οι παραπάνω συναρτήσεις (που στη βιβλιογραφία ονομάζονται modular) είναι περιοδικές. Αυτό επιτρέπει να θεωρήσουμε το ανάπτυγμα Fourier τους, μέσα στο οποίο "κρύβεται" αριθμητική πληροφορία.

Για παράδειγμα το ανάπτυγμα Fourier της j-invariant δίνεται από τον τύπο:

$$j(\tau) = \frac{1}{q} + 744 + 196884q + 21493760q^2 + 864299970q^3 + \cdots,$$

όπου $q = e^{2\pi i \tau}$.

9.2.2. Παιχνίδια με την j-invariant. Ας υπολογίσουμε την τιμή της j-invariant στο $\frac{1+\sqrt{-163}}{2}$. Αυτό μπορεί να γίνει με το ανάπτυγμα Fourier. Παρατηρούμε ότι για μικρές τιμές του q η συνεισφορά στο ανάπτυγμα Fourier δίνεται από το $1/q$. Έτσι με ακρίβεια 100 δεκαδικών ψηφίων υπολογίζουμε ότι

```
t=(1+sqrt(-163))/2
    = 1/2 +6.3835726674...936*I

     1/exp(2*Pi*I*t)= -262537412640768743.9999999999992500/
     725971981856888793538563373369908627075374103782106 47/
     9101186073129-3.434108189257855572773640382466514643 8/
     194103928029212310100823535285156436004061713842392 78/
     930629331 E-88*I
```

Αυτό σημαίνει ότι το $j\left(\frac{1+\sqrt{-163}}{2}\right) = 1/q + 744 + \cdots$ είναι ίσο με 262537412640768000 όπως υπολογίζει κανείς και με

```
    ellj(t)= -262537412640768000.00000000000000
```

Παρατήρηση: Ο αριθμός $1/q$ που χρησιμοποιήσαμε για να υπολογίσουμε μια προσέγγιση του $j(\tau)$ είναι υπερβατικός αφού

$$1/q = e^{\pi\sqrt{163}},$$

και το θεώρημα Gelfond-Schneider εξασφαλίζει ότι ο $e^{\pi a}$ είναι υπερβατικός, αν ο a είναι αλγεβρικός. Το $j(\tau)$ γίνεται ακέραιος, χάρη στη συνεισφορά των υπόλοιπων άπειρων προσθετέων του αναπτύγματος Fourier.

Παρατήρηση: Γενικά, οι υπολογισμοί κινητής υποδιαστολής σχετικά με την j-invariant είναι πολύ απαιτητικοί και χρησιμοποιούνται σειρά από "έξυπνα κόλπα" για να γίνουν όσο το δυνατόν αποτελεσματικότεροι. Μια αποτελεσματική αντιμετώπιση βρίσκεται στις βιβλιοθήκες του gp-pari το οποίο και χρησιμοποιήσαμε στους παραπάνω υπολογισμούς.

Οι συντελεστές του αναπτύγματος Fourier σχετίζονται με τη θεωρία αναπαραστάσεων μιας ομάδας που ονομάζεται στη βιβλιογραφία το τέρας και είναι μια τεράστια απλή ομάδα με τάξη:

$$2^{46} \cdot 3^{20} \cdot 5^9 \cdot 7^6 \cdot 11^2 \cdot 13^3 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71.$$

Η παραπάνω αναπάντεχη συσχέτιση παρατηρήθηκε από τον John Conway και Simon Norton το 1979. Αποδείχτηκε το 1992 από τον R. Borcherds το 1992. Τόσο η απόδειξη όσο και μετέπειτα εργασίες δίνουν επιπλέον αναπάντεχες συνδέσεις με τη conformal field theory αλλά και με τη θεωρία χορδών από τη Φυσική.

Διαβάστε:

1. What is the Monster
2. The mathematical Work of 1998 Fields Medalist
3. Ματίνα Μάντζαρη:Monstrous Moonshine, το τέρας και οι περίεργες φιλίες του Πτυχιακή εργασία Παν. Αιγαίου 2010

9.3. Ελλειπτικές Καμπύλες με μιγαδικό Πολλ/σμό

Υπενθυμίζουμε ότι αν μια ελλειπτική καμπύλη έχει ως δακτύλιο ενδομορφισμών έναν δακτύλιο που είναι μεγαλύτερος από τον δακτύλιο $\mathbb{Z}$, δηλαδή περιέχει ενδομορφισμούς $\phi \notin \mathbb{Z}$, τότε αυτοί ικανοποιούν μια σχέση

$$\phi^2 + a\phi + b = 0,$$

της οποίας η διακρίνουσα είναι αρνητική (εδώ οφείλεται και το όνομα *μιγαδικός πολλαπλασιασμός*).

Έστω τώρα ένα $\tau \in \mathbb{H}$, για παράδειγμα αυτό που ικανοποιεί τη σχέση $\tau^2 - t\tau + q = 0$ για μια αρνητική διακρίνουσα D. Το θεώρημα του *μιγαδικού πολλαπλασίασμου* εξασφαλίζει ότι το $j(\tau)$ είναι ικανοποιεί μια αλγεβρική εξίσωση με συντελεστές στο $\mathbb{Z}$ και ότι η ελλειπτική καμπύλη με E_τ, έχει j-invariant $j(\tau)$ και δακτύλιο $\mathrm{End}(E_\tau) = \mathbb{Z}[\tau]$. Επιπλέον αν θεωρήσουμε την εξίσωση που ικανοποιεί το $j(\tau)$ modulo p, τότε καταλήγουμε σε μια j-invariant που δίνει ελλειπτική καμπύλη πάνω από το σώμα $\mathbb{F}_p$ με ενδομορφισμό Frobenious να ικανοποιεί το ίδιο πολυώνυμο $\phi^2 - t\phi + q = 0$.

9.4. Τετραγωνικές μορφές διακρίνουσας D

Ο K.F. Gauss στο έργο του Disquisitiones Arithmeticae μελέτησε τις τετραγωνικές μορφές διακρίνουσας D

$$ax^2 + bxy + cy^2; b^2 - 4ac = -D, a, b, c \in \mathbb{Z} \ \ (a, b, c) = 1,$$

μέχρι μια σχέση ισοδυναμίας. Σε σύγχρονη γλώσσα η σχέση ισοδυναμίας αυτή εκφράζεται ως: Θα λέμε ότι δυο τετραγωνικές μορφές είναι ισοδύναμες αν υπάρχει μετασχηματισμός της $\mathrm{SL}(2, \mathbb{Z})$ που να στέλνει τη μία στην άλλη.

Ένα πλήρες σύστημα αντιπροσώπων $\mathrm{CL}(D)$ των κλάσεων είναι τα (a, b, c) ώστε

$$|b| \leqslant a \leqslant \sqrt{\frac{D}{3}}, a \leqslant c, (a, b, c) = 1, b^2 - 4ac = -D$$

αν $|b| = a$ ή $a = c$ τότε $b \geqslant 0$.

Σχήμα 9.1. K.F. Gauss, Το παρόν έργο αποτελεί κοινό κτήμα (public domain). Πηγή: Wikimedia Commons

9.4.1 Θεώρημα:
Θεωρούμε το $\tau \in \mathbb{H}$ *το οποίο ικανοποιεί ένα μονικό τετραγωνικό πολυώνυμο στο* $\mathbb{Z}[x]$. *Θεωρούμε την ελλειπτική καμπύλη* $E_\tau = \mathbb{C}/(\mathbb{Z} + \tau\mathbb{Z})$ *η οποία έχει* j*-invariant* $j(\tau)$. *Ο αριθμός* $j(\tau)$ *ικανοποιεί μια αλγεβρική εξίσωση που δίνεται από:*

$$H_D(x) = \prod_{[a,b,c]\in CL(D)} \left(x - j\left(\frac{-b+\sqrt{-D}}{2a}\right)\right) \in \mathbb{Z}[x].$$

Επιπλέον μια ρίζα της αναγωγής του πολυωνύμου $H_D(x)$ *modulo* p *οδηγεί στην κατασκευή μίας ελλειπτικής με Frobenious που έχει το ίδιο χαρακτηριστικό πολυώνυμο με το* τ.

Παράδειγμα: Για $D = 491$ έχουμε ότι

$$CL(D) = [1,1,123], [3,\pm 1,41], [9,\pm 7,15], [5,\pm 3,25], [11,\pm 9,3].$$

Για κάθε μία από τις παραπάνω τριάδες $[a,b,c]$ υπολογίζουμε τη ρίζα

$$\rho = \frac{-b+i\sqrt{491}}{2s},$$

που έχει θετικό φανταστικό μέρος.

Έτσι καταλήγουμε στον πίνακα:

$[a,b,c]$	ρίζα	j-invariant

$[a,b,c]$	ρίζα	j-invariant
$[1,1,123]$	$\rho_1=(-1+i\sqrt{491})/2$	-1.7082855 E30
$[3,1,41]$	$\rho_2=(-1+i\sqrt{491})/6$	5.977095 E9 + 1.0352632 E10I
$[3,-1,41]$	$\rho_3=(1+i\sqrt{491})/6$	5.9770957 E9 - 1.0352632 E10I
$[9,7,15]$	$\rho_4=(-7+i\sqrt{491})/18$	-1072.7816 + 1418.3793I
$[9,-7,15]$	$\rho_5=(7+i\sqrt{491})/18$	-1072.7816 - 1418.3793I
$[5,3,25]$	$\rho_6=(-3+i\sqrt{491})/10)$	-343205.38 + 1058567.0I
$[5,-3,25]$	$\rho_7=(3+i\sqrt{491})/10$	-343205.38 - 1058567.0I
$[11,9,13]$	$\rho_8=(-9+i\sqrt{491})/22$	6.0525190 + 170.50800I
$[11,-9,13]$	$\rho_9=(9+i\sqrt{491})/22$	6.0525190 - 170.50800I

Υπολογίζουμε το πολυώνυμο

$$f(x)=\prod_{i=1}^{9}(x-j(\rho_i))$$

με ακρίβεια 100 δεκαδικών ψηφίων και καταλήγουμε στο

```
x^9 + (17082855199382935607111650508 80.00000+ 0.E-105*I)*x^8 +
(-20419995943814746224552691418802908299264.
0000000000000000000000000000000000000000000000000000000000 +
5.527147875260444561 E-76*I)*x^7 +
(24410449766543274815871531378358313021155670228992 0.
0000000000000000000000000000000000000000000000000 -
3.203247249195215313 E-66*I)*x^6 +
(16806109970717648926762170533796935238933528040486364774 4.
0000000000000000000000000000000000000000000000000 -
8.477642883414348322 E-61*I)*x^5
+ (30266340622871033999335677742593898488443328160369893457 4743552.
0000000000000000000000000000000000000000000000000 +
1.1797555025677485282 E-53*I)*x^4 +
(64548590008561678492635478603558110892092369718837594939 3249280.
0000000000000000000000000000000000000000000000000 +
5.552991534850878913 E-50*I)*x^3 +
(95704113804639787096552080857655294919888566573818364375 0394920697856.
0000000000000000000000000000000000000000000000000 -
1.5307563300801091721 E-47*I)*x^2 +
(73228628710337844192365961292732508455291085022217625567 07445472002048.
0000000000000000000000000000000000000000000000000 +
4.458155165749330 23 E-45*I)*x +
(27831365943253888043128977216106999444228139865055751457 2676582234307592192.
0000000000000000000000000000000000000000000000000
- 3.587324068671531702 E-43*I)
```

.. το οποίο με μαγικό τρόπο είναι ένα πολυώνυμο με ακέραιους συντελεστές. Στο παραπάνω υποθέτουμε ότι οι μιγαδικοί συντελεστές οι οποίοι πολλαπλασιάζονται με έναν αριθμό 10^{-40} ή μικρότερο, είναι μηδενικοί.

9.5. Γενική μέθοδος κατασκευής ελλειπτικών καμπυλών

Θέλουμε να κατασκευάσουμε μια ελλειπτική καμπύλη πάνω από το πεπερασμένο σώμα $\mathbb{F}_p$ που να έχει $p+1-m$ το πλήθος στοιχεία.

1. Αρκεί να κατασκευάσουμε το $j \in \mathbb{F}_p$.
2. Το φράγμα του Hasse μας εξασφαλίζει ότι $Z := 4p-(p+1-m)^2 \geqslant 0$. Γράφουμε το $Z = Dv^2$ ως ένα τετράγωνο v^2 επί έναν αριθμό D που δεν είναι διαιρετός με τετράγωνο.
3. Η εξίσωση $4p = u^2 + Dv^2$ για κάποιο u ικανοποιεί την $m = p+1 \pm u$. Ο αρνητικός αριθμός $-D$ λέγεται CM διακρίνουσα για τον πρώτο p.
4. $x^2 - \mathrm{tr}(F)x + p \mapsto \Delta = \mathrm{tr}(F)^2 - 4p = -Dv^2$.

Αλγόριθμος:

1. Διαλέγουμε έναν πρώτο p. Διαλέγουμε τη μικρότερη D μαζί με $u, v \in \mathbb{Z}$ ώστε να έχει λύση η $4p = u^2 + Dv^2$.
2. Αν μία από τις τιμές $p+1-u$, $p+1+u$ έχει τάξη πρώτο αριθμό τότε προχωράμε στην κατασκευή της ελλειπτικής καμπύλης. Αν όχι δοκιμάζουμε άλλο p.
3. Υπολογίζουμε το πολυώνυμο Hilbert $H_D(x) \in \mathbb{Z}[x]$ με χρήση των τιμών της j-invariant.
4. Στη συνέχεια υπολογίζουμε το πολυώνυμο $H_D(x) \mathrm{mod} p$. Μία λύση του είναι η j-invariant που ψάχνουμε. Η ελλειπτική καμπύλη με αυτή την j-invariant $j \neq 0, 1728$ είναι η

$$y^2 = x^3 + 3kc^2x + 2kc^3, k = j/(1728-j), c \in \mathbb{F}_p.$$

Για διαφορετικές τιμές του c αντιστοιχούν οι δύο διαφορετικές ελλειπτικές καμπύλες E, E' οι οποίες έχουν τάξεις $p+1 \pm t$. Η μία είναι η

$$y^2 = x^3 + ax + b$$

και η άλλη η

$$y^2 = x^3 + ac^2x + bc^3,$$

όπου το c είναι ένα μη-τετραγωνικό υπόλοιπο στο $\mathbb{F}_p$.

Για να επιλέξουμε αυτή με τη σωστή τάξη, διαλέγουμε ένα σημείο P και υπολογίζουμε την τάξη του n ώστε $nP = \mathcal{O}$. Το n θα διαιρεί το $p+1-t$ ή το $p+1+t$.

Βιβλιογραφία

Blake, I.F., G. Seroussi, and N. Smart. 1999. *Elliptic Curves in Cryptography*. Lecture Note Series. Cambridge University Press. https://books.google.gr/books?id=0/_vegzgyqGMC.

Milne, J. S. 2006. *Elliptic Curves*. BookSurge Publishers.

Silverman, J.H. 1986. *The Arithmetic of Elliptic Curves*. Applications of Mathematics. https://books.google.fr/books?id=6y/_SmPc9fh4C.

Αντωνιάδης, Ι. 1999. *Ελλειπτικές Καμπύλες (Το Θεώρημα Του Mordell)*. ΕΠΕΑΕΚ Προμηθέας.

Παράρτημα

9.6. Το πρόγραμμα Sage

Το πρόγραμμα Sage είναι ένα ελεύθερο ανοιχτού κώδικα σύστημα λογισμικού, το οποίο βασίστηκε στον συνδυασμό πολλών υπαρχόντων συστημάτων για υπολογιστικά μαθηματικά και ο σκοπός του είναι να αποτελέσει μια ανοιχτού λογισμικού εναλλακτική λύση για πακέτα όπως το Magma, Maple, Mathematica και Matlab.

Ας δούμε μερικά παραδείγματα:

```
sage: 2 + 2
4
factor(-2015)
-1 * 5 * 13 * 31
```

Μπορούμε να πάρουμε πρώτους αριθμούς

```
prime_range(100)
[2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53,
59, 61, 67, 71, 73, 79, 83, 89, 97]
```

ή να μετρήσουμε το πλήθος των πρώτων που είναι μικρότεροι του 10^6.

```
prime_pi(10^6)
78498
```

Το πρόγραμμα μπορεί επίσης να χειριστεί έννοιες από τον απειροστικό λογισμό, όπως αόριστα και ορισμένα ολοκληρώματα:

```
integrate(1 + x + x^2, x)
1/3*x^3 + 1/2*x^2 + x
numerical_integral(1 + x + x^2, 0, 3)[0]
16.500000000000004
```

Και να κάνει γραφικές παραστάσεις συναρτήσεων και όχι μόνο.

Το πρόγραμμα sage αποτελεί μια πλήρη γλώσσα προγραμματισμού με δομή όπως η python. Μπορούμε να εκτελέσουμε βρόγχους (loops) πάνω στα αντικείμενά του. Έτσι μπορούμε να υπολογίσουμε τα τετράγωνα όλων των πρώτων που είναι μικρότεροι του 1000 με τον παρακάτω κώδικα:

```
sum=0
for i in prime_range(1000):
    sum=sum+i^2
    print sum
49345379
```

9.6.1. Χειρισμός πολυωνύμων. Ας ορίσουμε πρώτα τον πολυωνυμικό δακτύλιο $\mathbb{Q}[t]$

```
sage: R = PolynomialRing(QQ, 't')
sage: R
Univariate Polynomial Ring in t over Rational Field
```

Οι παραπάνω εντολές δηλώνουν στο sage ότι η αλφαριθμητική μεταβλητή (string) 't' συμβολίζει τη μεταβλητή του δακτυλίου στην εμφάνιση στην οθόνη. Αυτό **δεν** ορίζει το σύμβολο t για χρήση στο Sage, δηλαδή δεν μπορούμε να το χρησιμοποιήσουμε για να εισαγάγουμε ένα πολυώνυμο όπως το $t^2 + 2t + 1$.

Θα μπορούσαμε εναλλακτικά να δώσουμε

```
sage: S = QQ['t']
sage: S == R
True
```

Στον παραπάνω ορισμό ορίσαμε τον δακτύλιο S και ρωτήσαμε (η έκφραση με τα δύο == έχει την έννοια της ερώτησης) αν οι δακτύλιοι S, R ταυτίζονται, και πήραμε θετική (true) απάντηση. Και αυτός ο τρόπος ορισμού έχει το ίδιο πρόβλημα στη χρήση της μεταβλητής t.

Ένας πολύ βολικότερος τρόπος είναι να δώσουμε

```
sage: R.<t> = PolynomialRing(QQ)
```

ή

```
sage: R.<t> = QQ['t']
<div>
```

ή

```
sage: R.<t> = QQ[]
```

Οι παραπάνω ορισμοί ορίζουν τη μεταβλητή να είναι η μεταβλητή του πολυωνυμικού δακτυλίου, οπότε μπορούμε εύκολα να ορίσουμε στοιχεία του δακτυλίου:

```
sage: poly = (t+1) * (t+2); poly
t^2 + 3*t + 2
sage: poly in R
True
```

Στο παραπάνω ο τελεστής 'in' έδωσε θετική απάντηση (true), αφού πράγματι το πολυώνυμο είναι στοιχείο του δακτυλίου R.

Σε κάθε περίπτωση θα μπορούσαμε να βρούμε τον γεννήτορα του πολυωνυμικού δακτυλίου ως εξής:

```
sage: R = PolynomialRing(QQ, 't')
sage: t = R.0
sage: t in R
True
```

Οι πραγματικοί και οι μιγαδικοί αριθμοί είναι δομές κινητής υποδιαστολής και οι πράξεις δεν γίνονται με ακριβή τρόπο. Ιδιαίτερα οι μιγαδικοί αριθμοί θεωρούνται ότι παράγονται πάνω από τους πραγματικούς με το σύμβολο i

```
sage: CC
Complex Field with 53 bits of precision
sage: CC.0  # 0th generator of CC
1.00000000000000*I
```

Ας κάνουμε μερικά παραδείγματα στον δακτύλιο $\mathbb{Q}[t]$

```
sage: R, t = QQ['t'].objgen()
sage: f = 2*t^7 + 3*t^2 - 15/19
sage: f^2
4*t^14 + 12*t^9 - 60/19*t^7 + 9*t^4 - 90/19*t^2 + 225/361
sage: cyclo = R.cyclotomic_polynomial(7); cyclo
t^6 + t^5 + t^4 + t^3 + t^2 + t + 1
sage: g = 7 * cyclo * t^5 * (t^5 + 10*t + 2)
sage: g
7*t^16 + 7*t^15 + 7*t^14 + 7*t^13 + 77*t^12 + 91*t^11 +
91*t^10 + 84*t^9+ 84*t^8 + 84*t^7 + 84*t^6 + 14*t^5
sage: F = factor(g); F
(7) * t^5 * (t^5 + 10*t + 2) *
(t^6 + t^5 + t^4 + t^3 + t^2 + t + 1)
sage: F.unit()
7
sage: list(F)
[(t, 5), (t^5 + 10*t + 2, 1), (t^6 + t^5 + t^4 + t^3 + t^2
 + t + 1, 1)]
```

Παρατηρούμε ότι η παραγοντοποίηση καταγράφει και τη μονάδα του δακτυλίου.

Η διαίρεση δύο πολυωνύμων δίνει αποτέλεσμα στον δακτύλιο πηλίκων, τον οποίο το sage ορίζει αυτόματα:

```
sage: x = QQ['x'].0
sage: f = x^3 + 1; g = x^2 - 17
sage: h = f/g;  h
(x^3 + 1)/(x^2 - 17)
sage: h.parent()
Fraction Field of Univariate Polynomial Ring in x over
Rational Field
```

Αν ορίσουμε τη μεταβλητή με διαφορετικό όνομα έχουμε έναν διαφορετικό πολυωνυμικό δακτύλιο για το sage

```
sage: R.<x> = PolynomialRing(QQ)
sage: S.<y> = PolynomialRing(QQ)
sage: x == y
False
sage: R == S
False
sage: R(y)
x
sage: R(y^2 - 17)
x^2 - 17
```

Ο δακτύλιος προσδιορίζεται από τη μεταβλητή. Ορίζοντας έναν δακτύλιο με άλλο όνομα αλλά την ίδια μεταβλητή δεν καταλήγουμε σε διαφορετικούς δακτυλίους.

```
sage: R = PolynomialRing(QQ, "x")
sage: T = PolynomialRing(QQ, "x")
sage: R == T
True
sage: R is T
True
sage: R.0 == T.0
True
```

Μπορούμε να ορίσουμε πολυωνυμικούς δακτυλίους πάνω από οποιονδήποτε δακτύλιο βάσης.

```
sage: R.<T> =PolynomialRing(GF(7)); R
Univariate Polynomial Ring in T over Finite Field of size 7
```

Ας δούμε ένα παράδειγμα ενός αθροίσματος όπου κάθε όρος έχει και διαφορετικό όνομα:

```
sage: f = sum(1/var('n%s'%i)^i for i in range(10))
1/n1 + 1/n2^2 + 1/n3^3 + 1/n4^4 + 1/n5^5 + 1/n6^6 +
1/n7^7 + 1/n8^8 + 1/n9^9 + 1
```

Σε αυτό το βιβλίο θα χρησιμοποιήσουμε τη δυνατότητα του να τρέξει σε cloud server, ώστε ο χρήστης να έχει πρόσβαση σε αυτό μέσα από μια σελίδα του φυλλομετρητή του χωρίς να χρειαστεί να το εγκαταστήσει στον υπολογιστή του.

Γλωσσάριο

Αγγλικά	Ελληνικά
keyspace	σύνολο κλειδιών κωδικοποίησης
ciphertext	κρυπτογραφημένο μήνυμα
quadratic twist	τετραγωνική διαστροφή
loop	βρόγχος
string	αλφαριθμητική μεταβλητή