Υπολογιστική Θεωρία Αριθμών

Κώστας Μανές

Τμήμα Πληροφορικής
Πανεπιστήμιο Πειραιώς

Βιβλιογραφία

Σύγγραμμα μαθήματος:

V. Shoup, Μια υπολογιστική εισαγωγή στη θεωρία αριθμών και την άλγεβρα, Κλειδάριθμος, 2005.

Συμπληρωματική βιβλιογραφία:

1. Δ. Πουλάκης, Υπολογιστική θεωρία αριθμών, Κάλλιπος, 2016.
2. Α. Αντωνιάδης και Α. Κοντογεώργης, Θεωρία αριθμών και εφαρμογές, Κάλλιπος, 2015.
3. T. Apostol, Εισαγωγή στην αναλυτική θεωρία αριθμών, Gutenberg, 1986.
4. D. Bressoud and S. Wagon, A course in computational number theory, Wiley, 2008.
5. H. Cohen, Advanced topics and in computational number theory, Springer, 2000.
6. Δ. Δεριζιώτης, Μια εισαγωγή στη θεωρία αριθμών, Σοφία, 2007.
7. M. Lewinter and J. Meyer, Elementary number theory with programming, Wiley, 2016.
8. H. Niederreiter and A. Winterhof, Applied number theory, Springer, 2015.
9. W. Stein, Elementary number theory: primes, congruences, and secrets. A computational approach, Springer, 2010.
10. S. Y. Yan, Computational number theory and modern cryptography, Wiley, 2013.

Βασικές έννοιες

- Το σύνολο των πραγματικών αριθμών: $\mathbb{R}$
- Το σύνολο των ακεραίων: $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$.
- Το σύνολο των φυσικών: $\mathbb{N}^* = \mathbb{Z}_+ = \{1, 2, \ldots\}$. $\mathbb{N} = \mathbb{N}^* \cup \{0\}$. Ειδικά, συμβολίζουμε με $[n]$ το σύνολο $[n] = \{1, 2, \ldots, n\}$.
- Το σύνολο των ρητών: $\mathbb{Q} = \{m/n : n \in \mathbb{N}^*, m \in \mathbb{Z}\}$.
- **Μαθηματική επαγωγή**: Έστω $S \subseteq \mathbb{N}^*$. Αν $1 \in S$ και $n \in S \Rightarrow n + 1 \in S$, τότε $S = \mathbb{N}^*$.
- **Αρχή καλής διάταξης**: Κάθε μη κενό κάτω φραγμένο υποσύνολο των ακεραίων έχει ελάχιστο.
- **Κάτω και άνω ακέραιο μέρος (floor - ceiling)**: Για κάθε πραγματικό x ορίζονται μονοσήμαντα οι ακέραιοι $\lfloor x \rfloor$ και $\lceil x \rceil$ από τη σχέση

$$x - 1 < \lfloor x \rfloor \leq x \leq \lceil x \rceil < x + 1$$

Ο **διωνυμικός συντελεστής** ‘‘n ανά k’’ συμβολίζεται με $\binom{n}{k}$ και ορίζεται ως

$$\binom{n}{k} = \begin{cases} \dfrac{n!}{k!(n-k)!}, & 0 \le k \le n, \\ 0, & \text{αλλιώς}, \end{cases} \qquad n, k \in \mathbb{N}.$$

Από τον ορισμό προκύπτουν οι ακόλουθες ταυτότητες, για $n, k, m \in \mathbb{N}$:

$$\binom{n}{k} = \binom{n}{n-k}, \qquad \binom{n}{k} = \frac{n}{k}\binom{n-1}{k-1}, \quad k \in \mathbb{N}^*,$$
$$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}, \qquad \binom{n}{m}\binom{m}{k} = \binom{n}{k}\binom{n-k}{m-k}.$$

Η ονομασία των διωνυμικών συντελεστών προκύπτει από το *διωνυμικό θεώρημα*:

Διωνυμικό Θεώρημα

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}, \qquad n \in \mathbb{N}.$$

Βασικές ταυτότητες

$$a^n - b^n = (a-b)(a^{n-1} + a^{n-2}b + \cdots + ab^{n-2} + b^{n-1}),$$

όπου $a, b \in \mathbb{R}, n \in \mathbb{N}^*$.

Αν n περιττός, εφαρμόζοντας την παραπάνω ταυτότητα για a και $-b$, προκύπτει η ταυτότητα

$$a^n + b^n = (a+b)(a^{n-1} - a^{n-2}b + \cdots - ab^{n-2} + b^{n-1}),$$

όπου $a, b \in \mathbb{R}, n = 2k-1, k \in \mathbb{N}^*$.

Βασικά αθροίσματα

$$1 + 2 + \cdots + n = \frac{n(n+1)}{2}, \qquad n \in \mathbb{N}^*$$

$$1 + 2^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}, \qquad n \in \mathbb{N}^*$$

$$1 + 2^3 + \cdots + n^3 = \frac{n^2(n+1)^2}{4}, \qquad n \in \mathbb{N}^*$$

Σχέση διαιρετότητας

Έστω a, b ακέραιοι. Λέμε ότι ο a διαιρεί τον b και γράφουμε $a|b$ ανν ο b είναι ακέραιο πολλαπλάσιο του a, δηλαδή υπάρχει ακέραιος k ώστε $b = ka$. Αν ο a δεν διαιρεί τον b, τότε γράφουμε $a \nmid b$.

Βασικές ιδιότητες

$a, b, c, d \in \mathbb{Z}$

- $a|0$, $a|a$, $1|a$.
- Αν $0|a$, τότε $a = 0$.
- Αν $a|b$ και $b|c$, τότε $a|c$.
- Αν $c|a$ και $c|b$, τότε $c|\kappa a + \lambda b$, για κάθε $\kappa, \lambda \in \mathbb{Z}$.
- Αν $c \neq 0$, τότε $a|b \Leftrightarrow ca|cb$.
- Αν $a|b$ και $b \neq 0$, τότε $|a| \leq |b|$.
- Αν $a|b$ και $b|a$, τότε $|a| = |b|$.
- Αν $a|b$ και $c|d$, τότε $ac|bd$.

Σχέση διαιρετότητας

Θεώρημα (Διαίρεση ακεραίων με υπόλοιπο)

Για κάθε $a, b \in \mathbb{Z}$ με $b \neq 0$, υπάρχουν μοναδικοί ακέραιοι q, r τέτοιοι ώστε $a = bq + r, \qquad 0 \leq r < |b|.$

Απόδειξη.

Το σύνολο $S = \{a - bx \geq 0 : x \in \mathbb{Z}\}$ είναι κάτω φραγμένο (από το 0) και μη κενό. Πράγματι, αν $b > 0$, τότε $a - b(-|a|) \in S$, ενώ αν $b < 0$, τότε $a - b|a| \in S$. Άρα υπάρχει το $r = \min S = a - bq$. Αν $r \geq |b|$, τότε $0 \leq r - |b| = a - bq - |b| \in S$, άτοπο, διότι $r - |b| < r$. Άρα $0 \leq r < |b|$.
Τέλος, αν υπάρχουν $q', r' \in \mathbb{Z}$, ώστε $a = bq' + r'$, $0 \leq r' < |b|$, τότε $|b||q - q'| = |r' - r| < |b|$, οπότε $q = q'$ και άρα $r = r'$. □

Ο q ονομάζεται **πηλίκο** της διαίρεσης a δια b και ισούται με $q = \lfloor a/b \rfloor$. Ο r ονομάζεται **υπόλοιπο** της διαίρεσης και ισούται με $r = a - b\lfloor a/b \rfloor$.

Πρώτοι αριθμοί

Ο ακέραιος $p > 1$ είναι πρώτος ανν $n \nmid p$ για κάθε φυσικό n με $1 < n < p$. Το σύνολο των πρώτων αριθμών συμβολίζεται με $\mathbb{P}$.

Λήμμα

Κάθε φυσικός $n > 1$ έχει τουλάχιστον έναν πρώτο διαιρέτη.

Ένας φυσικός $n > 1$ με δύο ή περισσότερους πρώτους διαιρέτες ονομάζεται σύνθετος. Βάσει των παραπάνω ορισμών, ο 1 δεν είναι πρώτος ούτε σύνθετος.

Θεώρημα (Ευκλείδης)

Υπάρχουν άπειροι πρώτοι.

Πρόταση

Αν ο φυσικός n είναι σύνθετος, τότε έχει τουλάχιστον έναν πρώτο διαιρέτη p, με $p \leq \sqrt{n}$.

Αν a, b, d ακέραιοι και $d|a$ και $d|b$, τότε ο d ονομάζεται κοινός διαιρέτης των a, b. Το σύνολο S των θετικών κοινών διαιρετών των a, b είναι μη κενό ($1 \in S$) και άνω φραγμένο (π.χ. από το $|a|$), άρα έχει μέγιστο στοιχείο, το οποίο ονομάζεται μέγιστος κοινός διαιρέτης των a, b και συμβολίζεται ως μκδ(a, b) ή $\gcd(a, b)$ ή και (a, b).
Οι a, b ονομάζονται πρώτοι μεταξύ τους ανν μκδ$(a, b) = 1$.

Θεώρημα

Αν a, b ακέραιοι με $b \neq 0$ και $d = μκδ(a, b)$, τότε υπάρχουν ακέραιοι s, t τέτοιοι ώστε $d = sa + tb$. Επιπλέον, ο d είναι ο ελάχιστος θετικός ακέραιος που γράφεται στη μορφή $xa + yb$, $x, y \in \mathbb{Z}$.

Απόδειξη.

Έστω $S = \{ax + by > 0 : x, y \in \mathbb{Z}\}$. Το S είναι μη κενό ($a^2 + b^2 \in S$) και κάτω φραγμένο (από το 0) άρα έχει ελάχιστο στοιχείο, έστω το $d = sa + tb$. Θα δειχθεί ότι $d = \text{μκδ}(a, b)$.
Σύμφωνα με το Θεώρημα της διαίρεσης με υπόλοιπο, υπάρχουν $q, r \in \mathbb{Z}$ ώστε $a = dq + r$, $0 \leq r < d$. Τότε,
$r = a - dq = a - q(sa + bt) = (1 - qs)a + (-qt)b$. Αν $0 < r < d$, τότε $r \in S$, άτοπο διότι d είναι το ελάχιστο του S. Άρα $r = 0$, οπότε $a = dq$, δηλαδή $d|a$. Ομοίως προκύπτει ότι $d|b$.
Αν τώρα $c > 0$ είναι ένας άλλος κοινός διαιρέτης των a, b, τότε $c|a, c|b \Rightarrow c|sa + tb \Rightarrow c|d \Rightarrow c \leq d$. Επομένως, d είναι ο μέγιστος κοινός διαιρέτης. □

Πόρισμα

Αν $a, b, c, p, q \in \mathbb{Z}$, *τότε:*

1. *Οι* a, b *είναι πρώτοι μεταξύ τους ανν υπάρχουν* $s, t \in \mathbb{Z}$, *τέτοιοι ώστε* $sa + tb = 1$.
2. *Αν* $\mu\kappa\delta(a, b) = 1$ *και* $a|bc$, *τότε* $a|c$.
3. *Αν* p *πρώτος και* $p|ab$, *τότε* $p|a$ *ή* $p|b$.
4. $\mu\kappa\delta(a, b) = \mu\kappa\delta(a - bq, b)$ *(στην ιδιότητα αυτή βασίζεται ο αλγόριθμος του Ευκλείδη).*
5. $\mu\kappa\delta(ca, cb) = |c|\,\mu\kappa\delta(a, b)$.
6. *Αν* $d = \mu\kappa\delta(a, b)$, *τότε* $\mu\kappa\delta(a/d, b/d) = 1$.
7. *Αν* $\mu\kappa\delta(a, b) = \mu\kappa\delta(a, c) = 1$, *τότε* $\mu\kappa\delta(a, bc) = 1$.
8. *Αν* $a|c$ *και* $b|c$ *και* $\mu\kappa\delta(a, b) = 1$, *τότε* $ab|c$.

Αν a, b, c ακέραιοι και $a|c$ και $b|c$, τότε ο c ονομάζεται κοινό πολλαπλάσιο των a, b. Το σύνολο S των θετικών κοινών πολλαπλασίων των a, b είναι μη κενό ($|ab| \in S$) και κάτω φραγμένο (π.χ. από το 1), άρα έχει ελάχιστο στοιχείο, το οποίο ονομάζεται ελάχιστο κοινό πολλαπλάσιο των a, b και συμβολίζεται ως εκπ(a, b) ή $\operatorname{lcm}(a, b)$ ή και $[a, b]$.

Πρόταση

Αν a, b μη μηδενικοί ακέραιοι, τότε εκπ$(a, b) = \dfrac{|ab|}{\text{μκδ}(a, b)}$.

Απόδειξη.

Αν $a = 0$ ή $b = 0$, το αποτέλεσμα προφανώς ισχύει. Υποθέτουμε ότι $ab \neq 0$ και θέτουμε $d = \text{μκδ}(a, b)$. Αν m ένα θετικό κοινό πολλαπλάσιο των a, b, τότε ο $c = |ab|$ διαιρεί τους am και bm άρα $c|\,\text{μκδ}(am, bm) = md$, οπότε $c/d|m$. Επιπλέον, ο c/d είναι θετικό πολλαπλάσιο των a, b, άρα είναι το ελάχιστο. □

Πολυπλοκότητα αριθμητικών πράξεων

Σύμφωνα με το Θεώρημα της διαίρεσης με υπόλοιπο, κάθε θετικός ακέραιος a μπορεί να παρασταθεί μοναδικά ως άθροισμα δυνάμεων κάποιας βάσης $b > 1$ ως εξής:

$$a = r_{k-1}b^{k-1} + r_{k-2}b^{k-2} + \cdots + r_1 b + r_0 = \sum_{i=0}^{k-1} r_i b^i,$$

όπου $r_i \in \{0, 1, \ldots, b-1\}$ είναι το υπόλοιπο της διαίρεσης του $\left(a - \sum_{j=0}^{i-1} r_j b^j\right) / b^i$ δια του b. Συμβολικά γράφουμε $a = (r_{k-1}, r_{k-2}, \ldots, r_0)_b$. Ο αριθμός k ονομάζεται μήκος της b-αδικής αναπαράστασης του a και ειδικά για $b = 2$ συμβολίζεται με $\mathrm{len}(a)$, δηλαδή, γενικεύοντας για $a \in \mathbb{Z}$, είναι

$$\mathrm{len}(a) = k = \lceil \log_2(|a| + 1) \rceil = \begin{cases} 1 + \lfloor \log_2 |a| \rfloor, & a \neq 0, \\ 1, & a = 0. \end{cases}$$

Πολυπλοκότητα αριθμητικών πράξεων

Η πολυπλοκότητα των βασικών αλγορίθμων της Θεωρίας Αριθμών εκφράζεται συναρτήσει της συνάρτησης μήκους len. Συγκεκριμένα, για τις βασικές αριθμητικές πράξεις ισχύει το ακόλουθο αποτέλεσμα:

Θεώρημα

Αν a, b ακέραιοι, τότε

- *Το άθροισμα και η διαφορά $a \pm b$ υπολογίζεται σε χρόνο $O(\mathrm{len}(a) + \mathrm{len}(b))$.*
- *Το γινόμενο ab υπολογίζεται σε χρόνο $O(\mathrm{len}(a)\,\mathrm{len}(b))$.*
- *Το πηλίκο $q = \lfloor a/b \rfloor$ και το υπόλοιπο των a, b υπολογίζεται σε χρόνο $O(\mathrm{len}(a)\,\mathrm{len}(q))$.*

Ταχύτερος πολλαπλασιασμός (Karatsuba)

Αν τεθεί $n = \max\{\text{len}(a), \text{len}(b)\}$ και $a = a_0 2^m + a_1$, $b = b_0 2^m + b_1$, όπου $1 \leq m < n$ και $a_1, b_1 < 2^m$, τότε

$$\begin{aligned} ab &= a_0 b_0 2^{2m} + (a_0 b_1 + a_1 b_0) 2^m + a_1 b_1 \\ &= a_0 b_0 2^{2m} + ((a_0 + a_1)(b_0 + b_1) - a_0 b_0 - a_1 b_1) 2^m + a_1 b_1, \end{aligned}$$

οπότε, ο υπολογισμός του γινομένου ab ανάγεται στον υπολογισμό τριών γινομένων αριθμών υποδιπλάσιου μήκους, για $m = \lceil n/2 \rceil$, των $a_0 b_0$, $a_1 b_1$ και $(a_0 + a_1)(b_0 + b_1)$. Επομένως αν εφαρμοστεί η μέθοδος διαίρει και βασίλευε, προκύπτει ένας αλγόριθμος που εκτελείται σε χρόνο $O(n^{\log_2 3})$. Συγκεκριμένα, αν τεθεί $L(z, m) = (z_1, z_2, \ldots, z_m)_2$ και $R(z, m) = (z_{m+1}, z_{m+2}, \ldots, z_\ell)_2$, για κάθε ακέραιο $z = (z_1, z_2, \ldots z_\ell)_2$, τότε ο αλγόριθμος αυτός διατυπώνεται σε αναδρομική μορφή ως εξής:

Ταχύτερος πολλαπλασιασμός (Karatsuba)

Είσοδος: Οι θετικοί ακέραιοι a, b.
Έξοδος: Το γινόμενο ab.

```
K (a, b) begin
    n ← max{len(a), len(b)};
    if n = 1 then return ab;
    m ← ⌈n/2⌉;
    a_0 ← L(a, m);
    a_1 ← R(a, m);
    b_0 ← L(b, m);
    b_1 ← R(b, m);
    x ← K(a_0, b_0);
    y ← K(a_0 + a_1, b_0 + b_1);
    w ← K(a_1, b_1);
    return x2^{2m} + (y − x − w)2^m + w;
end
```

Αλγόριθμος 1: Πολλαπλασιασμός Karatsuba.

Ο αλγόριθμος του Ευκλείδη

Ο αλγόριθμος αυτός υπολογίζει τον μέγιστο κοινό διαιρέτη δύο ακεραίων a, b, βασιζόμενος στη διαίρεση με υπόλοιπο $a = bq + r$, $0 \leq r < b$ και στην ιδιότητα μκδ$(a, b) =$ μκδ$(b, a - bq)$.Αρχικά, τίθενται $r_0 = \max\{|a|, |b|\}$, $r_1 = \min\{|a|, |b|\}$ και στη συνέχεια εκτελείται για κάθε $i \geq 0$ η διαίρεση r_i δια r_{i+1}, δίνοντας το υπόλοιπο

$$r_{i+2} = r_i - r_{i+1}q_{i+1}, \text{με } 0 \leq r_{i+2} < r_{i+1}.$$

Επειδή η ακολουθία υπολοίπων είναι γνησίως φθίνουσα και παίρνει τιμές σε ένα πεπερασμένο σύνολο, έπεται ότι για κάποιο $\ell \geq 1$ θα είναι $r_{\ell+1} = 0$, οπότε ο αλγόριθμος τερματίζει μετά από ℓ διαιρέσεις και $r_\ell =$ μκδ(a, b). Στα επόμενα, θεωρούμε χωρίς βλάβη της γενικότητας ότι $a \geq b > 0$.

Ο αλγόριθμος του Ευκλείδη

Είσοδος: Οι ακέραιοι a, b, με $a \geq b > 0$.
Έξοδος: Ο μκδ(a, b).

$r \leftarrow a$;
$r' \leftarrow b$;
while $r' \neq 0$ **do**
    $r'' \leftarrow r \mod r'$;
    $r \leftarrow r'$;
    $r' \leftarrow r''$;
end while
return r;

Αλγόριθμος 2: Αλγόριθμος του Ευκλείδη για $a \geq b > 0$.

Πρόταση

Το πλήθος ℓ των βημάτων που εκτελεί ο αλγόριθμος του Ευκλείδη ικανοποιεί τη σχέση $\ell \leq 1 + \frac{\log_2 b}{\log_2 \phi}$, όπου $\phi = \frac{1+\sqrt{5}}{2}$.

Απόδειξη.

Αρκεί να δειχθεί ότι $r_{\ell-i} \geq \phi^i$, για κάθε $0 \leq i < \ell$, οπότε για $i = \ell - 1$ προκύπτει το ζητούμενο. Με επαγωγή στο i. Για $i = 0$ και $i = 1$, η σχέση ισχύει, αφού

$$r_\ell \geq 1 = \phi^0, \qquad \text{και} \qquad r_{\ell-1} > r_\ell \Rightarrow r_{\ell-1} \geq 2 > \phi.$$

Υποθέτοντας, ότι ισχύει για όλους τους φυσικούς μικρότερους του $i \geq 2$, και λαμβάνοντας υπόψη τη σχέση $\phi^2 = \phi + 1$, έχουμε $r_{\ell-i} = r_{\ell-i+2} + q_{\ell-i+1} r_{\ell-i+1} \geq r_{\ell-i+2} + r_{\ell-i+1} \geq \phi^{i-2} + \phi^{i-1} = \phi^{i-2}(\phi + 1) = \phi^i$, άρα η σχέση ισχύει για κάθε i. □

Παρατήρηση:

Άμεσα αποδεικνύεται ότι το πλήθος βημάτων ℓ μεγιστοποιείται στην περίπτωση της εύρεσης του μκδ$(F_{\ell+2}, F_{\ell+1})$, όπου F_n είναι ο n-οστός όρος της ακολουθίας Fibonacci, που ορίζεται από τον αναδρομικό τύπο:

$$F_{n+2} = F_{n+1} + F_n, \qquad F_0 = 0, F_1 = 1, \qquad n \in \mathbb{N}.$$

Πράγματι, είναι

$$\ell = 1 + \lfloor \frac{\log_2 F_{\ell+1}}{\log_2 \phi} \rfloor \Leftrightarrow \ell - 1 \leq \frac{\log_2 F_{\ell+1}}{\log_2 \phi} < \ell \Leftrightarrow \phi^{\ell-1} \leq F_{\ell+1} < \phi^{\ell}$$

και η τελευταία ανισότητα προκύπτει εύκολα με επαγωγή και με τη βοήθεια της σχέσης $\phi^2 = \phi + 1$.

Πόρισμα

Ο χρόνος εκτέλεσης του αλγορίθμου του Ευκλείδη είναι $O(\text{len}(a)\,\text{len}(b))$.

Απόδειξη.

Δεδομένου ότι εκτελούνται ℓ διαιρέσεις, η κάθε μια σε χρόνο $O(\text{len}(r_i)\,\text{len}(q_i))$, και ότι $a = r_0 \geq r_1 q_1 \geq r_2 q_2 q_1 \geq \cdots \geq r_\ell q_\ell \cdots q_1 \geq q_\ell \cdots q_1$, έχουμε ότι

$$\sum_{i=1}^{\ell} \text{len}(r_i)\,\text{len}(q_i) \leq \text{len}(b) \sum_{i=1}^{\ell} \text{len}(q_i) \leq \text{len}(b) \sum_{i=1}^{\ell} (1 + \log_2 q_i)$$

$$= \text{len}(b)\,(\ell + \log_2(q_1 q_2 \cdots q_\ell)) \leq \text{len}(b)\,(\ell + \log_2 a)$$

$$\leq \text{len}(b) \left(\frac{\log_2 b}{\log_2 \phi} + 1 + \log_2 a \right) = O(\text{len}(a)\,\text{len}(b)).$$

□

Εκτεταμένος αλγόριθμος του Ευκλείδη:

Τροποποιώντας τον αλγόριθμο του Ευκλείδη, μπορούμε επιπλέον να υπολογίσουμε τους ακεραίους s, t για τους οποίους είναι $\text{μκδ}(a, b) = sa + tb$. Συγκεκριμένα αν ορίσουμε

$$s_{i+1} = s_{i-1} - s_i q_i, \qquad t_{i+1} = t_{i-1} - t_i q_i, \quad s_0 = t_1 = 1, s_1 = t_0 = 0,$$

τότε ισχύει για κάθε $i = 0, 1, \ldots, \ell + 1$ ότι $s_i a + t_i b = r_i$, επομένως $s_\ell a + t_\ell b = \text{μκδ}(a, b)$. Το αποτέλεσμα αυτό αποδεικνύεται εύκολα με επαγωγή. Για $i \in \{0, 1\}$ είναι προφανές, αφού $r_0 = a$, και $r_1 = b$. Υποθέτοντας ότι ισχύει για $j \leq i$, έχουμε ότι

$$\begin{aligned} s_{i+1}a + t_{i+1}b &= (s_{i-1} - s_i q_i)a + (t_{i-1} - t_i q_i)b \\ &= s_{i-1}a + t_{i-1}b - (s_i a - t_i b)q_i = r_{i-1} - r_i q_i = r_{i+1}. \end{aligned}$$

Εκτεταμένος αλγόριθμος του Ευκλείδη:

Ανάλογα αποδεικνύεται ότι ο χρόνος εκτέλεσης του εκτεταμένου αλγορίθμου του Ευκλείδη είναι επίσης $O(\text{len}(a)\,\text{len}(b))$, διότι τα s_i, t_i υπολογίζονται σε χρόνο $O(\text{len}(a)\,\text{len}(b))$.

Παρατήρηση

Αν γράψουμε

$$R_{i+1} = Q_i R_i, \qquad \text{όπου } Q_i = \begin{bmatrix} 0 & 1 \\ 1 & -q_i \end{bmatrix}, \quad R_i = \begin{bmatrix} r_{i-1} \\ r_i \end{bmatrix}$$

τότε έχουμε $R_{i+1} = Q_i Q_{i-1} \cdots Q_1 R_1$, όπου $R_1 = \begin{bmatrix} a \\ b \end{bmatrix}$. Αν τεθεί $M_i = Q_i Q_{i-1} \cdots Q_1$, τότε εύκολα προκύπτει με επαγωγή ότι $M_i = \begin{bmatrix} s_i & t_i \\ s_{i+1} & t_{i+1} \end{bmatrix}$, οπότε

$$\begin{bmatrix} \text{μκδ}(a,b) \\ 0 \end{bmatrix} = \begin{bmatrix} r_\ell \\ r_{\ell+1} \end{bmatrix} = R_{\ell+1} = M_\ell R_1 = \begin{bmatrix} s_\ell & t_\ell \\ s_{\ell+1} & t_{\ell+1} \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix}$$

Διοφαντικές εξισώσεις

Διοφαντική εξίσωση (με n αγνώστους) ονομάζεται κάθε εξίσωση της μορφής

$$p(x_1, x_2, \ldots, x_n) = 0,$$

όπου το πρώτο μέλος είναι ένα πολυώνυμο με ακέραιους συντελεστές.
Κάθε n-άδα $(x_1, x_2, \ldots, x_n)$ ακεραίων που επαληθεύει την εξίσωση ονομάζεται λύση αυτής (μας ενδιαφέρουν μόνο ακέραιες λύσεις).

Γραμμική διοφαντική εξίσωση:

$a_1x_1 + a_2x_2 + \cdots + a_nx_n = c$, όπου $a_1, a_2, \ldots, a_n, c \in \mathbb{Z}$.

Πρόταση

Η γραμμική διοφαντική εξίσωση

$$ax + by = c$$

έχει λύση ανν $d|c$, *όπου* $d = \mu\kappa\delta(a, b)$.
Επιπλέον, αν (x_0, y_0) *μια λύση αυτής, τότε έχει άπειρες λύσεις, οι οποίες είναι ακριβώς τα ζεύγη* (x, y) *της μορφής*

$$x = x_0 + kb/d, \qquad y = y_0 - ka/d, \qquad k \in \mathbb{Z}.$$

Απόδειξη.

Αν (x, y) μια λύση της εξίσωσης, τότε $d|ax + by \Rightarrow d|c$. Αντίστροφα, αν $d|c$, τότε $c = zd$, $z \in \mathbb{Z}$. Επειδή $d = sa + tb$, $s, t \in \mathbb{Z}$, έπεται ότι (zs, zt) είναι μια λύση της εξίσωσης.
Αν (x_0, y_0), (x, y) δύο λύσεις της εξίσωσης, τότε $ax + by = c = ax_0 + by_0 \Rightarrow a(x - x_0) = b(y_0 - y) \Rightarrow (x - x_0)a/d = (y_0 - y)b/d$. Λαμβάνοντας υπόψη ότι μκδ$(a/d, b/d) = 1$, προκύπτει ότι $a/d|y_0 - y$, οπότε υπάρχει $k \in \mathbb{Z}$ με $y_0 - y = ka/d$, άρα και $x - x_0 = kb/d$. Αντίστροφα, αν (x_0, y_0) λύση της εξίσωσης και $(x, y) = (x_0 + kb/d, y_0 - ka/d)$, τότε $ax + by = a(x_0 + kb/d) + b(y_0 - ka/d) = ax_0 + by_0 = c$, άρα (x, y) λύση της εξίσωσης. □

Το παραπάνω αποτέλεσμα γενικεύεται επαγωγικά στην περίπτωση n αγνώστων, $n \geq 3$, όπου η εξίσωση έχει λύση ανν μκδ$(a_1, a_2, \ldots, a_n)|c$. Μάλιστα, έχει απειρία λύσεων που επίσης εκφράζεται σε παραμετρική μορφή.

Παράδειγμα

Έστω η εξίσωση $5x_1 + 6x_2 + 3x_3 + 2x_4 = 15$.
Η εξίσωση $5x_1 + 6x_2 = y$, $y \in \mathbb{Z}$, έχει λύσεις τις
$(x_1, x_2) = (-y + 6t, y - 5t)$, $t \in \mathbb{Z}$.
Η εξίσωση $y + 3x_3 = z$, $z \in \mathbb{Z}$, έχει λύσεις τις
$(y, x_3) = (4z + 3u, -z - u)$, $u \in \mathbb{Z}$.
Η εξίσωση $z + 2x_4 = 15$ έχει λύσεις τις
$(z, x_4) = (-15 + 2w, 15 - w)$, $w \in \mathbb{Z}$.
Επομένως, η γενική λύση της αρχικής εξίσωσης είναι η
(x_1, x_2, x_3, x_4), όπου

$$
\begin{aligned}
x_4 &= 15 - w \\
x_3 &= -z - u = 15 - 2w - u \\
x_2 &= y - 5t = 4z + 3u - 5t = -60 + 8w + 3u - 5t \\
x_1 &= -y + 6t = -4z - 3u + 6t = 60 - 8w - 3u + 6t
\end{aligned}
$$

και $w, u, t \in \mathbb{Z}$.

Θεώρημα (Θεμελιώδες Θεώρημα της Αριθμητικής)

Κάθε μη μηδενικός ακέραιος z εκφράζεται με μοναδικό τρόπο ως γινόμενο δυνάμεων πρώτων:

$$z = \pm p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r},$$

όπου $p_1, p_2, \ldots, p_r$ πρώτοι με $p_1 < p_2 < \cdots < p_r$, και $e_1, e_2, \ldots, e_r$ θετικοί ακέραιοι.

Πιο γενικά, μπορούμε να γράψουμε

$$z = \pm \prod_{p \in \mathbb{P}} p^{\nu_p(z)}, \quad \nu_p(z) = \begin{cases} n, & \exists n \in \mathbb{N}^*, z = p^n m, m \in \mathbb{Z}^*, p \nmid m, \\ 0, & \text{αλλιώς} \end{cases}$$

όπου το γινόμενο λαμβάνεται στο σύνολο $\mathbb{P}$ όλων των πρώτων p και η συνάρτηση $\nu_p(z)$ εκφράζει τη δύναμη του πρώτου p στην παραγοντοποίηση του z. Κατά σύμβαση, ορίζουμε $\nu_p(0) = +\infty$.

Η συνάρτηση ν_p ικανοποιεί τις ακόλουθες ιδιότητες:

1. $\nu_p(ab) = \nu_p(a) + \nu_p(b), \forall p \in \mathbb{P}$.
2. $b|a \Leftrightarrow \forall p \in \mathbb{P}, \nu_p(b) \leq \nu_p(a)$.
3. $\nu_p\left(\mu\kappa\delta(a,b)\right) = \min\{\nu_p(a), \nu_p(b)\}, \forall p \in \mathbb{P}$.
4. $\nu_p\left(\epsilon\kappa\pi(a,b)\right) = \max\{\nu_p(a), \nu_p(b)\}, \forall p \in \mathbb{P}$.

Παρατήρηση

Το προηγούμενο Θεώρημα μπορεί να γενικευθεί και στο σύνολο των ρητών, αν επιτρέψουμε στη συνάρτηση ν_p να παίρνει και αρνητικές τιμές.

Πρόταση

Αν $n \in \mathbb{N}^*$ και p πρώτος, τότε

$$\nu_p(n!) = \sum_{k \geq 1} \lfloor n/p^k \rfloor.$$

Απόδειξη.

Κάθε αριθμός i στο διάστημα $[1, n]$ συνεισφέρει στην τιμή του $\nu_p(n!)$ κατά μια μονάδα για κάθε $k \geq 1$ με $p^k | i$. Από την άλλη, για κάθε $k \in \mathbb{N}$, τα πολλαπλάσια του p^k στο διάστημα $[1, n]$ είναι $\lfloor n/p^k \rfloor$ σε πλήθος.

$$\nu_p(n!) = \sum_{i=1}^{n} \nu_p(i) \overset{*}{=} \sum_{i=1}^{n} \sum_{k \geq 1} [p^k | i] = \sum_{k \geq 1} \sum_{i=1}^{n} [p^k | i] = \sum_{k \geq 1} \lfloor n/p^k \rfloor.$$

□

*Iverson bracket: $[C] = (C)?1 : 0;$.

Οι συναρτήσεις τ και σ

Για κάθε $n \in \mathbb{N}^*$, συμβολίζουμε με $\tau(n)$ και $\sigma(n)$ το πλήθος και το άθροισμα αντίστοιχα των θετικών διαιρετών του n.

Πρόταση

Αν $n, m \in \mathbb{N}^*$, *τότε*

i) $\tau(n) = \prod_{p \in \mathbb{P}} (1 + \nu_p(n))$.

ii) $\mu\kappa\delta(n, m) = 1 \Rightarrow \tau(nm) = \tau(n)\tau(m)$.

Απόδειξη.

Άσκηση. □

Οι συναρτήσεις τ και σ

Πρόταση

Αν $n, m \in \mathbb{N}^*$, *τότε*

i) $\sigma(n) = \prod_{p \in \mathbb{P}} \frac{p^{\nu_p(n)+1} - 1}{p - 1}$.

ii) $\mu\kappa\delta(n, m) = 1 \Rightarrow \sigma(nm) = \sigma(n)\sigma(m)$.

Απόδειξη.

i) Αν $p_1, p_2, \ldots, p_k$ είναι όλοι οι πρώτοι που διαιρούν το n, τότε θεωρώντας την παράσταση

$$(1+p_1+\cdots+p_1^{\nu_{p_1}(n)})(1+p_2+\cdots+p_2^{\nu_{p_2}(n)})\cdots(1+p_k+\cdots+p_k^{\nu_{p_k}(n)})$$

και εκτελώντας τις πράξεις, προκύπτει ένα άθροισμα από όρους της μορφής $p_1^{s_1}p_2^{s_2}\cdots p_m^{s_m}$, όπου $0 \leq s_i \leq \nu_{p_i}(n)$, $i \in [m]$, και $m \in [k]$. Όμως αυτοί είναι ακριβώς οι διαιρέτες του n, άρα η παραπάνω παράσταση ισούται με $\sigma(n)$. Έτσι, λαμβάνοντας υπόψη ότι

$$1 + p + \cdots + p^{\nu_p(n)} = \frac{p^{\nu_p(n)+1} - 1}{p - 1},$$

προκύπτει το ζητούμενο αποτέλεσμα.
Το *ii*) προκύπτει άμεσα από το *i*), καθώς τα n και m δεν έχουν κοινούς πρώτους διαιρέτες. □

Κατανομή των πρώτων αριθμών

Για κάθε πραγματικό $x \geq 0$ συμβολίζουμε με $\pi(x)$ το πλήθος των πρώτων μικρότερων ή ίσων του x.

Θεώρημα (Chebyshev-1849)

$$n \geq 30 \Rightarrow c_1 \frac{n}{\ln n} \leq \pi(n) \leq c_2 \frac{n}{\ln n}, \qquad c_1 = 0.92129, c_2 = 1.056.$$

Συνεπώς, για να ελέγξουμε με διαδοχικές διαιρέσεις αν ο φυσικός n είναι πρώτος, δεδομένου ότι γνωρίζουμε όλους τους πρώτους στο $[2, \sqrt{n}]$, απαιτείται χρόνος $\Theta(\sqrt{n} \ln n)$ στη χειρότερη περίπτωση που ο n είναι όντως πρώτος. ($\Theta(\sqrt{n}/\ln \sqrt{n})$ σε πλήθος διαιρέσεις, η κάθε μια πολυπλοκότητας $O(\ln^2 n)$.)

Θεώρημα (Θεώρημα των Πρώτων Αριθμών - 1896)

$$\lim_{x\to+\infty} \frac{\pi(x)}{x/\ln x} = 1. \qquad (\textit{Ισοδύναμα}, \pi(x) \sim x/\ln x.)$$

Επομένως, η συνάρτηση $x/\ln x$ αποτελεί μια προσέγγιση της $\pi(x)$, καθώς $x \to +\infty$. Για το σφάλμα της προσέγγισης, ισχύει ο τύπος

$$\pi(x) = x/\ln x + O(x/\ln^2 x).$$

Μια καλύτερη προσέγγιση επιτυγχάνεται από τη συνάρτηση λογαριθμικού ολοκληρώματος:

$$\mathrm{li}(x) = \int_2^x \frac{dt}{\ln t}.$$

Θεώρημα (Αξίωμα του Bertrand)

Για κάθε $n \in \mathbb{N}^*$, *ισχύει ότι*

$$\pi(2n) - \pi(n) > \frac{n}{3\ln(2n)}.$$

Σύμφωνα, με το προηγούμενο Θεώρημα, υπάρχει πάντα πρώτος μεταξύ των φυσικών n και $2n$, άρα και σε κάποιο οσοδήποτε μεγάλο διάστημα. Από την άλλη, υπάρχουν οσοδήποτε μεγάλα διαστήματα που δεν περιέχουν πρώτους. Πράγματι, αν $n > 1$, τότε οι $n! + 2, n! + 3, \ldots, n! + n$ είναι όλοι σύνθετοι, γιατί διαιρούνται αντίστοιχα από τους $2, 3, \ldots, n$.

Κατανομή των πρώτων αριθμών

Τα επόμενα τρία αποτελέσματα είναι γνωστά ως Θεωρήματα του Mertens (1874).

$$\sum_{p \le x} \frac{1}{p} = \ln \ln x + O(1).$$

$$\sum_{p \le x} \frac{\ln p}{p} = \ln x + O(1).$$

$$\prod_{p \le x} (1 - 1/p) = \Theta(1/\ln x).$$

Το κόσκινο του Ερατοσθένη

Είναι ένας κλασικός αλγόριθμος για την εύρεση όλων των πρώτων στο διάστημα $[2, n]$, για κάποιο φυσικό n.

Είσοδος: $n > 2$.
Έξοδος: Η λίστα $A = (A[2], A[3], \ldots, A[n])$, με $A[i] = 1 \Leftrightarrow i \in \mathbb{P}$.

```
for k = 2 to n do  A[n] ← 1;
for k = 2 to √n do
    if A[k] = 1 then
        i ← 2k;
        while i ≤ n do
            A[i] ← 0;
            i ← i + k;
        end while
    end if
end for
```

Αλγόριθμος 3: Κόσκινο του Ερατοσθένη.

Το κόσκινο του Ερατοσθένη

Ο αλγόριθμος αυτός πραγματοποιεί $\lfloor n/p \rfloor$ διαγραφές για κάθε πρώτο p, άρα συνολικά

$$\sum_{p \leq \sqrt{n}} \lfloor n/p \rfloor$$

διαγραφές. Επομένως, από το πρώτο θεώρημα του Mertens, είναι πολυπλοκότητας $\Theta(n \ln \ln n)$.

Άσκηση.

Να τροποποιηθεί το κόσκινο του Ερατοσθένη, προκειμένου να προσδιορίζει το σύνολο των αριθμών στο διάστημα $[1, x]$ που είναι πρώτοι προς έναν δοσμένο $n \in \mathbb{N}^*$.

Αριθμοί του Mersenne: Είναι αριθμοί της μορφής $M_n = 2^n - 1$, $n \in \mathbb{N}$.

Πρόταση

Αν M_p πρώτος, τότε p πρώτος.

Απόδειξη.

Αν p σύνθετος, τότε θα υπάρχουν $r, s > 1$ με $p = rs$. Επομένως, $M_p = 2^{rs} - 1 = (2^r - 1)((2^r)^{s-1} + \cdots + 2^r + 1)$, δηλαδή ο M_p είναι γινόμενο δύο φυσικών > 1, άτοπο. □

Μέχρι σήμερα, έχουν βρεθεί μόνο 51 (Δεκ 2018 GIMPS) πρώτοι του Mersenne. Είναι ανοιχτό ερώτημα, αν το πλήθος τους είναι άπειρο.

Ένας φυσικός αριθμός n καλείται τέλειος όταν $\sigma(n) = 2n$.

Πρόταση

Ένας άρτιος n είναι τέλειος ανν $n = 2^{p-1}M_p$, για κάποιον πρώτο του Mersenne M_p.

Μέχρι σήμερα, δεν έχει βρεθεί περιττός τέλειος αριθμός. Έχει αποδειχθεί ότι αν υπάρχει τέτοιος, θα πρέπει να είναι μεγαλύτερος του 10^{1500}.

Απόδειξη.

Αν M_p πρώτος, τότε μκδ$(2^{p-1}, M_p) = 1$, οπότε

$$\begin{aligned}\sigma(n) &= \sigma(2^{p-1}M_p) = \sigma(2^{p-1})\sigma(M_p)\\ &= (1+2+\cdots+2^{p-1})(M_p+1) = (2^p-1)2^p = 2n.\end{aligned}$$

Αν n τέλειος, τότε $n = 2^k m$, όπου $k \geq 1$ και m περιττός. Επομένως,
$2^{k+1}m = 2n = \sigma(n) = \sigma(2^k m) = \sigma(2^k)\sigma(m) = (2^{k+1}-1)\sigma(m)$.
Άρα $2^{k+1}-1 | 2^{k+1}m$, οπότε $2^{k+1}-1 | m$, δηλαδή
$m = m'(2^{k+1}-1)$. Αντικαθιστώντας, στην προηγούμενη ισότητα, προκύπτει ότι $2^{k+1}m' = \sigma(m)$. Επομένως,

$$m + m' = m'(2^{k+1}-1) + m' = 2^{k+1}m' = \sigma(m),$$

οπότε οι m, m' είναι οι μόνοι θετικοί διαιρέτες του m, άρα m πρώτος, $m' = 1$, οπότε και $m = 2^{k+1}-1$. □

Αριθμοί του Fermat: Είναι αριθμοί της μορφής $F_n = 2^{2^n} + 1$, $n \in \mathbb{N}$.

Πρόταση

Αν $p = 2^m + 1$ πρώτος, τότε $m = 2^n$, για κάποιο $n \in \mathbb{N}$.

Απόδειξη.

Υπάρχει b περιττός ώστε $m = 2^n b$. Αν $b > 1$, τότε

$$p = (2^{2^n})^b + 1 = (2^{2^n} + 1)((2^{2^n})^{b-1} - \cdots + 1)$$

και οι δύο όροι του γινομένου είναι μεγαλύτεροι του 1, άτοπο διότι p πρώτος. Άρα $b = 1$. □

Οι τέσσερεις πρώτοι του Fermat είναι οι $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$. Αυτοί είναι και οι μόνοι γνωστοί, ενώ για $5 \leq n \leq 3329780$ έχει αποδειχθεί ότι ο F_n είναι σύνθετος.

Πρώτοι της Germain: Ένας πρώτος p καλείται πρώτος της Germain αν ο $2p + 1$ είναι πρώτος. Είναι άγνωστο αν το πλήθος αυτών των πρώτων είναι άπειρο.

Το κρυμμένο θεώρημα του Πλάτωνα:

Θεώρημα

Αν $3 < p < q$ δύο διαδοχικοί πρώτοι, τότε κάθε θετικός ακέραιος $n < q$ διαιρεί τον $p!$.

Με βάση αυτό το θεώρημα, μπορούμε να διατυπώσουμε έναν αλγόριθμο για την εύρεση του επόμενου πρώτου. Υπολογίζουμε το $p!$ και για κάθε $j \geq 1$ ελέγχουμε αν ο $(p + j)$ διαιρεί τον $p!$, μέχρι να βρούμε το ελάχιστο j ώστε $p + j \nmid p!$. Ο επόμενος πρώτος του p θα είναι ο $q = p + j$.

Πρώτοι που ανήκουν σε αριθμητική πρόοδο

Θεώρημα (Dirichlet - 1837)

Αν $a, b \in \mathbb{N}^*$, *με* $\mu\kappa\delta(a, b) = 1$, *τότε υπάρχουν άπειροι πρώτοι της μορφής* $an + b$, $n \in \mathbb{N}$.

Ορισμός

Αν $a, b \in \mathbb{Z}$ και $n \in \mathbb{N}^*$, λέμε ότι οι a, b είναι ισότιμοι (ή ισοδύναμοι) κατά μέτρο n (ή modulo n), και γράφουμε $a \equiv b \pmod{n}$, ανν $n|a-b$.

Λαμβάνοντας υπόψη τη διαίρεση ακεραίων με υπόλοιπο, άμεσα προκύπτει ότι οι a, b είναι ισότιμοι κατά μέτρο n ανν έχουν το ίδιο υπόλοιπο διαιρούμενοι με το n, για το λόγο αυτό ονομάζονται και ισοϋπόλοιποι.

Ιδιότητες

Αν $n, m \in \mathbb{N}^*$, $a, b, c, d \in \mathbb{Z}$, με $a \equiv b \pmod{n}$ και $c \equiv d \pmod{n}$, τότε:

- $a + c \equiv b + d \pmod{n}$,
- $ac \equiv bd \pmod{n}$,
- $a^m \equiv b^m \pmod{n}$,
- $p(a) \equiv p(b) \pmod{n}$, για οποιοδήποτε πολυώνυμο $p(x) \in \mathbb{Z}[x]$.

Η διαγραφή σε μια ισοτιμία $ac \equiv bc \pmod{n}$ του κοινού παράγοντα c δεν είναι πάντα δυνατή, ισχύει όμως (άσκηση) ότι $a \equiv b \pmod{n/d}$, όπου $d = \text{μκδ}(c, n)$, άρα η διαγραφή είναι σωστή όταν $d = 1$.

Τα σύνολα $\mathbb{Z}_n$ και $\mathbb{Z}_n^*$

Εύκολα προκύπτει ότι η σχέση ισοτιμίας είναι μια σχέση ισοδυναμίας στο $\mathbb{Z}$. Η κλάση που περιέχει το $x \in \mathbb{Z}$ συμβολίζεται με $[x]_n$, ή με $\overline{x}$, όταν είναι σαφές ποιο είναι το n. Δηλαδή, για κάθε $x \in \mathbb{Z}$, είναι

$$\begin{aligned}[x]_n &= \{y \in \mathbb{Z} : y \equiv x \pmod{n}\} = \{y \in \mathbb{Z} : n|y - x\} \\ &= \{y \in \mathbb{Z} : y - x = nk, k \in \mathbb{Z}\}\end{aligned}$$

Το σύνολο πηλίκο συμβολίζεται με $\mathbb{Z}_n$ και ονομάζεται σύνολο ακεραίων modulo n, δηλαδή

$$\mathbb{Z}_n = \{[0]_n, [1]_n, [2]_n, \ldots, [n-1]_n, \}.$$

Στο σύνολο πηλίκο $\mathbb{Z}_n$ ορίζουμε τις πράξεις $\oplus$ και $\odot$ ως εξής:

$$[x]_n \oplus [y]_n = [x + y]_n, \qquad [x]_n \odot [y]_n = [x \cdot y]_n.$$

Τα σύνολα $\mathbb{Z}_n$ και $\mathbb{Z}_n^*$

Άμεσα προκύπτει ότι η δομή $(\mathbb{Z}_n, \oplus)$ είναι αντιμεταθετική ομάδα. Αντίθετα, η δομή $(\mathbb{Z}_n \setminus \{[0]_n\}, \odot)$ δεν είναι πάντα ομάδα, διότι το στοιχείο $[x]_n$ δεν έχει πάντα συμμετρικό[1]. Αν όμως θεωρήσουμε το υποσύνολο

$$\mathbb{Z}_n^* = \{[x]_n \in \mathbb{Z}_n : \exists [y]_n \in \mathbb{Z}_n, [x]_n \odot [y]_n = [1]_n\}$$

των στοιχείων που έχουν συμμετρικό, τότε η δομή $(\mathbb{Z}_n^*, \odot)$ είναι αντιμεταθετική ομάδα, για κάθε $n \in \mathbb{N}^*$.

Παρατήρηση

Πολλοί συγγραφείς χρησιμοποιούν το σύμβολο U_n αντί του $\mathbb{Z}_n^*$, και τα σύμβολα $+, \cdot$ για τις πράξεις $\oplus, \odot$ αντίστοιχα.

[1] Για παράδειγμα, στο $\mathbb{Z}_4$, το $[2]_n$ δεν έχει συμμετρικό, αφού $[2]_n \odot [1]_n = [2]_n$, $[2]_n \odot [2]_n = [4]_n = [0]_n$, $[2]_n \odot [3]_n = [6]_n = [2]_n$.

Τα σύνολα $\mathbb{Z}_n$ και $\mathbb{Z}_n^*$

Θεώρημα

Για κάθε $n \in \mathbb{N}^*$, ισχύει ότι

$$\mathbb{Z}_n^* = \{[x]_n \in \mathbb{Z}_n : \mu\kappa\delta(x, n) = 1\}.$$

Απόδειξη.

Έστω $[x]_n \in \mathbb{Z}_n^*$. Τότε υπάρχει $[y]_n \in \mathbb{Z}$, τέτοιο ώστε $[x]_n \odot [y]_n = [1]_n$ και

$$[x]_n \odot [y]_n = [1]_n \Rightarrow [xy]_n = [1]_n \Rightarrow xy - 1 = kn, k \in Z.$$

Επομένως, αν $d = \mu\kappa\delta(x, n)$, τότε $d|xy, d|kn \Rightarrow d|1 \Rightarrow d = 1$ (διότι $d > 0$).
Αντίστροφα, αν $\mu\kappa\delta(x, n) = 1$, τότε υπάρχουν $s, t \in \mathbb{Z}$, τέτοιοι ώστε $sx + tn = 1$, οπότε
$sx = -tn + 1 \Rightarrow [sx]_n = [1]_n \Rightarrow [s]_n \odot [x]_n = [1]_n \Rightarrow [x]_n \in \mathbb{Z}_n^*$. □

Γενικά, η δομή $(\mathbb{Z}_n, \oplus, \odot)$ είναι ένας αντιμεταθετικός δακτύλιος με μοναδιαίο στοιχείο.
Από το προηγούμενο Θεώρημα προκύπτει άμεσα το επόμενο αποτέλεσμα:

Πόρισμα

Η δομή $(\mathbb{Z}_n, \oplus, \odot)$ είναι σώμα αν και μόνο αν ο n είναι πρώτος αριθμός.

Πολυπλοκότητα πράξεων στο $\mathbb{Z}_n$

Αν $x, y \in \mathbb{Z}$, τότε

- Η πρόσθεση και η αφαίρεση $x \pm y \mod n$ μπορεί να εκτελεστεί σε χρόνο $O(\text{len}(n))$.
- Ο πολλαπλασιασμός $xy \mod n$ μπορεί να εκτελεστεί σε χρόνο $O(\text{len}^2(n))$.
- Η εύρεση του πολλαπλασιαστικού αντιστρόφου $x^{-1} \mod n$ (αν υπάρχει) μπορεί να εκτελεστεί σε χρόνο $O(\text{len}^2(n))$, με τον εκτεταμένο αλγόριθμο του Ευκλείδη.
- Η δύναμη $x^k \mod n$, $k \in \mathbb{N}$, μπορεί να εκτελεστεί σε χρόνο $O(\text{len}(k)\,\text{len}^2(n))$, χρησιμοποιώντας τον αλγόριθμο επανειλημμένων τετραγωνισμών.

Είσοδος: $x, k \in \mathbb{N}^*, k = (b_{\ell-1}, \ldots, b_1, b_0)_2$.
Έξοδος: x^k.

$a \leftarrow 1$;
for $i = \ell - 1$ **down to** 0 **do**
    $a \leftarrow a^2$;
    if $b_i = 1$ **then** $a = a \cdot x$;
end for
return a;

Αλγόριθμος 4: Αλγόριθμος επανειλημμένων τετραγωνισμών.

Γραμμικές ισοτιμίες

Μια ισοτιμία της μορφής $p(x) \equiv 0 \pmod{n}$, όπου $p(x) = a_m x^m + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$, με $a_m \not\equiv 0 \pmod{n}$, ονομάζεται πολυωνυμική ισοτιμία βαθμού m. Για $m = 1$, ονομάζεται γραμμική ισοτιμία και έχει τη γενική μορφή $ax \equiv b \pmod{n}$. Επειδή η ισοτιμία αυτή έχει λύση ανν υπάρχει $y \in \mathbb{Z}$ ώστε $ax - b = ny$, από τα γνωστά των γραμμικών διοφαντικών εξισώσεων προκύπτει ότι η ισοτιμία έχει λύση ανν $d = \text{μκδ}(a, n) | b$ και το σύνολο των διαφορετικών λύσεών της mod n είναι το

$$\{x_0 + kn/d : 0 \leq k \leq d - 1\},$$

όπου x_0 μια λύση αυτής, η οποία μπορεί να υπολογισθεί κατά τα γνωστά με τον εκτεταμένο αλγόριθμο του Ευκλείδη σε χρόνο $O(\text{len}^2(n))$. Συνεπώς, το πλήθος των διαφορετικών λύσεων ισούται με d.

Το Κινέζικο Θεώρημα Υπολοίπων

Θεώρημα (Κινέζικο Θεώρημα Υπολοίπων)

Αν οι θετικοί ακέραιοι $n_1, n_2, \ldots, n_k$, $k \in \mathbb{N}^*$, *είναι ανά δύο πρώτοι προς αλλήλους, και* $a_1, a_2, \ldots, a_k$ *ακέραιοι, τότε υπάρχει μοναδικός φυσικός* x, *με* $0 \leq x < n_1 n_2 \cdots n_k$, *τέτοιος ώστε*

$$x \equiv a_i \pmod{n_i}, \qquad \text{για κάθε } i \in [k].$$

Απόδειξη.

Έστω $n = n_1 n_2 \cdots n_k$. Τότε, οι n/n_i και n_i είναι πρώτοι προς αλλήλους, οπότε υπάρχει ακέραιος b_i, τέτοιος ώστε $b_i n/n_i \equiv 1 \pmod{n_i}$ (δηλαδή ο b_i είναι ο αντίστροφος του n/n_i modulo n). Επομένως, ισχύει ότι $\frac{n}{n_i} b_i a_i \equiv a_i \pmod{n_i}$. Επιπλέον, αν $j \in [k]$, με $i \neq j$, τότε ο n/n_i είναι πολλαπλάσιο του n_j, οπότε ισχύει ότι $\frac{n}{n_i} b_i a_i \equiv 0 \pmod{n_j}$. Έτσι, αν τεθεί $x = \sum_{j=1}^{k} \frac{n}{n_j} b_j a_j$, τότε είναι $x \equiv a_i \pmod{n_i}$, για κάθε $i \in [k]$. Άρα ο x είναι μια λύση του παραπάνω συστήματος εξισώσεων.

Στη συνέχεια, θα δειχθεί ότι η λύση αυτή είναι μοναδική. Έστω ακέραιος y, με $0 \leq y < n$ και $y \equiv a_i \pmod{n_i}$, για κάθε $i \in [k]$. Τότε, είναι $x - y \equiv 0 \pmod{n_i}$, δηλαδή $n_i \mid x - y$, για κάθε $i \in [k]$. Όμως, επειδή οι $n_1, n_2, \ldots, n_k$ είναι ανά δύο πρώτοι προς αλλήλους, έπεται ότι $n \mid x - y$, δηλαδή $x \equiv y \pmod{n}$, και επειδή $0 \leq x, y < n$, τελικά είναι $x = y$. □

Εύκολα προκύπτει ότι ο x μπορεί να υπολογισθεί σε χρόνο $O(\text{len}^2(n))$.
Το παραπάνω Θεώρημα υποδεικνύει έναν τρόπο μοναδικής αναπαράστασης του αριθμού x από την έκφραση $(a_1, a_2, \ldots, a_k)$. Έτσι, αν δίδονται οι a_i, τότε ο $x < n$ προκύπτει μονοσήμαντα από τη σχέση

$$x \equiv \sum_{i=1}^{k} \frac{n}{n_i} b_i a_i \pmod{n},$$

ενώ αν δίνεται ο x, τότε οι $a_i < n_i$ προσδιορίζονται μονοσήμαντα από τις σχέσεις $a_i \equiv x \pmod{n_i}$.

Πρόταση

Αν $n = n_1 n_2 \cdots n_k$, *όπου οι* $n_1, n_2, \ldots, n_k$, $k \in \mathbb{N}^*$, *είναι θετικοί ακέραιοι, ανά δύο πρώτοι προς αλλήλους, τότε η απεικόνιση* $f : \mathbb{Z}_n \to A$, *όπου* $A = \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_k}$, *με*

$$f([x]_n) = ([x]_{n_1}, [x]_{n_2}, \ldots, [x]_{n_k})$$

είναι ένα προς ένα και επί. Επιπλέον, ο περιορισμός f^* *της* f *στο* $\mathbb{Z}_n^*$ *είναι ένα προς ένα και επί του* $A^* = \mathbb{Z}_{n_1}^* \times \mathbb{Z}_{n_2}^* \times \cdots \times \mathbb{Z}_{n_k}^*$.

Απόδειξη.

Αν $([a_1]_{n_1}, [a_2]_{n_2}, \ldots, [a_k]_{n_k}) \in A$, τότε, βάσει του Κινεζικού Θεωρήματος Υπολοίπων, υπάρχει μοναδικός $0 \leq x < n$, τέτοιος ώστε $x \equiv a_i \pmod{n_i}$, ή ισοδύναμα $[x]_{n_i} = [a_i]_{n_i}$. Επομένως, η f είναι ένα προς ένα. Επιπλέον, επειδή
$|A| = n_1 n_2 \cdots n_k = n = |Z_n|$, έπεται ότι η απεικόνιση είναι και επί.
Για την f^* έχουμε ότι

$$\begin{aligned}[x]_n \in \mathbb{Z}_n^* &\Leftrightarrow \text{μκδ}(x, n) = 1 \Leftrightarrow \text{μκδ}(x, n_i) = 1, \forall i \in [k] \\ &\Leftrightarrow [x]_{n_i} \in \mathbb{Z}_{n_i}^*, \forall i \in [k],\end{aligned}$$

οπότε $[x]_n \in \mathbb{Z}_n^* \Leftrightarrow ([x]_{n_1}, [x]_{n_2}, \ldots, [x]_{n_k}) \in A^*$, δηλαδή η f^* είναι επί του A^*. Επιπλέον θα είναι και ένα προς ένα, αφού η f είναι ένα προς ένα. □

Η συνάρτηση του Euler

Για οποιονδήποτε θετικό ακέραιο n, συμβολίζουμε με $\phi(n)$ το πλήθος των θετικών ακεραίων που είναι μικρότεροι ή ίσοι του n και πρώτοι προς αυτόν, δηλαδή

$$\phi(n) = |\{x \in [n] : \text{μκδ}(x, n) = 1\}|.$$

Η συνάρτηση $\phi(n)$ ονομάζεται συνάρτηση του Euler. Προφανώς, ισχύει ότι $\phi(n) = |\mathbb{Z}_n^*|$, για κάθε $n \in \mathbb{N}$.

Πρόταση

Αν n_1, n_2 είναι θετικοί ακέραιοι, πρώτοι προς αλλήλους, τότε

$$\phi(n_1 n_2) = \phi(n_1)\phi(n_2).$$

Απόδειξη.

Η απεικόνιση f^* της προηγούμενης Πρότασης είναι ένα προς ένα και επί, επομένως, για $k = 2$ και n_1, n_2 πρώτους προς αλλήλους, δίνει ότι

$$\phi(n) = |\mathbb{Z}_n^*| = |\mathbb{Z}_{n_1}^* \times \mathbb{Z}_{n_2}^*| = |\mathbb{Z}_{n_1}^*||\mathbb{Z}_{n_2}^*| = \phi(n_1)\phi(n_2),$$

όπου $n = n_1 n_2$. □

Η Πρόταση αυτή, προφανώς γενικεύεται για οποιοδήποτε πεπερασμένο πλήθος φυσικών, ανά δύο πρώτων προς αλλήλους.

Πρόταση

Αν p είναι πρώτος, τότε

$$\phi(p^k) = p^k\left(1 - \frac{1}{p}\right) = p^{k-1}(p-1), \quad k \in \mathbb{N}^*.$$

Απόδειξη.

Οι ακέραιοι στο διάστημα από 1 έως p που δεν είναι πρώτοι προς τον p^k είναι ακριβώς τα πολλαπλάσια του p, δηλαδή οι

$$p, 2p, 3p, \ldots, (p^{k-1}-1)p, p^k,$$

οι οποίοι είναι p^{k-1} σε πλήθος. Όμως, όλοι οι ακέραιοι στο διάστημα αυτό είναι p^k το πλήθος. Επομένως, είναι $\phi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1)$. □

Με βάση τις δύο προηγούμενες Προτάσεις, μπορούμε να υπολογίσουμε την τιμή $\phi(n)$ για οποιονδήποτε φυσικό n, αρκεί να γνωρίζουμε την ανάλυσή του σε πρώτους παράγοντες. Έτσι, για $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$, είναι

$$\begin{aligned}\phi(n) &= \phi(p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}) = \phi(p_1^{a_1})\phi(p_2^{a_2}) \cdots \phi(p_k^{a_k}) \\ &= p_1^{a_1}\left(1 - \frac{1}{p_1}\right) p_2^{a_2}\left(1 - \frac{1}{p_2}\right) \cdots p_k^{a_k}\left(1 - \frac{1}{p_k}\right) \\ &= n \prod_{i=1}^{k}\left(1 - \frac{1}{p_i}\right) = n \prod_{p \in \mathbb{P}, p|n}\left(1 - \frac{1}{p}\right).\end{aligned}$$

Πρόταση

Αν $n \in \mathbb{N}^*$, τότε

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

όπου το άθροισμα λαμβάνεται για όλους τους θετικούς διαιρέτες d του n.

Απόδειξη.

Θεωρούμε το σύνολο $A = \{k/n : k \in \mathbb{N}, 0 \leq k < n\}$ καθώς και τα σύνολα $A_d = \{a/d : a \in \mathbb{N}, 0 \leq a < d, \text{μκδ}(a, d) = 1\}$, όπου d θετικός διαιρέτης του n. Προφανώς $A_1 = \{0\}$ και τα σύνολα αυτά είναι ανά δύο ξένα (αλλιώς κάποιοι ρητοί θα είχαν δύο ανάγωγες μορφές). Αν $x = k/n \in A$, τότε $x \in A_{n/d}$, όπου $d = \text{μκδ}(k, n)$. Αντίστροφα, αν $x = a/d \in A_d$, τότε $x \in A$. Επομένως, $A = \bigcup_{d|n} A_d$ και κατά συνέπεια, $n = |A| = |\bigcup_{d|n} A_d| = \sum_{d|n} |A_d| = \sum_{d|n} \phi(d)$. □

Θεώρημα (Θεώρημα Euler-Fermat)

Αν $a, n \in \mathbb{Z}$, $n > 0$ *και* $\mu\kappa\delta(a, n) = 1$, *τότε*

$$a^{\phi(n)} \equiv 1 \pmod{n}.$$

Απόδειξη.

Αρκεί να δειχθεί στην περίπτωση που $1 < a < n$. Επειδή $\mu\kappa\delta(a, n) = 1$, έπεται ότι $[a]_n \in \mathbb{Z}_n^*$. Έστω η συνάρτηση $f : \mathbb{Z}_n^* \to \mathbb{Z}_n^*$, με $f([x]_n) = [a]_n \odot [x]_n$. Αν $[y]_n \in \mathbb{Z}_n^*$ και $[b]_n$ είναι το αντίστροφο του $[a]_n$, τότε το στοιχείο $[b]_n \odot [y]_n$ ανήκει στο $\mathbb{Z}_n^*$ και ισχύει ότι $f([b]_n \odot [y]_n) = [a]_n \odot [b]_n \odot [y]_n = [y]_n$, οπότε η f είναι επί. Επιπλέον, αν $[x_1]_n, [x_2]_n \in \mathbb{Z}_n^*$, με $[a]_n \odot [x_1]_n = [y_1]_n$ και $[a]_n \odot [x_2]_n = [y_2]_n$, τότε

$$[y_1]_n = [y_2]_n \Rightarrow [a]_n \odot [x_1]_n = [a]_n \odot [x_2]_n \Rightarrow [x_1]_n = [x_2]_n,$$

άρα η f είναι ένα προς ένα.

Απόδειξη.

Κατόπιν τούτων, αν $\mathbb{Z}_n^* = \{[x_1]_n, [x_2]_n, \ldots, [x_k]_n\}$, όπου $k = \phi(n) = |\mathbb{Z}_n^*|$, πολλαπλασιάζοντας κατά μέλη τις k εξισώσεις

$$[a]_n \odot [x_i]_n = [y_i]_n, \qquad i \in [k],$$

προκύπτει ότι

$$([a]_n)^k \odot ([x_1]_n \odot \cdots \odot [x_k]_n) = ([y_1]_n \odot \cdots \odot [y_k]_n).$$

Τέλος, λαμβάνοντας υπόψη ότι $\{[x_1]_n, [x_2]_n, \ldots, [x_k]_n\} = \{[y_1]_n, [y_2]_n, \ldots, [y_k]_n\}$, διότι η f είναι αμφιμονοσήμαντη, έπεται ότι

$$[x_1]_n \odot \cdots \odot [x_k]_n = [y_1]_n \odot \cdots \odot [y_k]_n,$$

επομένως $([a_n])^k = [1]_n$, δηλαδή $a^k \equiv 1 \pmod{n}$. □

Το μικρό Θεώρημα Fermat

Θεώρημα (Μικρό Θεώρημα Fermat)

Αν $a \in \mathbb{N}^*$ και p πρώτος, τότε

$$a^p \equiv a \pmod{p}.$$

Επιπλέον, αν $p \nmid a$, τότε

$$a^{p-1} \equiv 1 \pmod{p}.$$

Απόδειξη.

Αν $p \nmid a$, τότε μκδ$(a, p) = 1$. Επιπλέον, είναι $\phi(p) = p - 1$. Επομένως, η δεύτερη σχέση προκύπτει ως άμεση εφαρμογή του Θεωρήματος Euler-Fermat, για $n = p$. Η πρώτη σχέση προκύπτει πολλαπλασιάζοντας με a κατά μέλη, ενώ προφανώς ισχύει όταν $p|a$, αφού τότε είναι $a^p \equiv a \equiv 0 \pmod{p}$. □

Το Θεώρημα του Wilson

Θεώρημα (Θεώρημα Wilson)

Ο p είναι πρώτος αν $(p-1)! \equiv p-1 \pmod{p}$.

Απόδειξη.

Επειδή p πρώτος, έπεται ότι όλοι οι ακέραιοι στο $\{1, 2, \ldots, p-1\}$ έχουν αντίστροφο $\mod p$. Επιπλέον μόνο οι 1 και $p-1$ έχουν ως αντίστροφο τον εαυτό τους. Πράγματι,

$$([x]_p)^2 = [1]_p \Leftrightarrow [x^2-1]_p = [0]_p \Leftrightarrow [x-1]_p[x+1]_p = [0]_p$$
$$\Leftrightarrow x \in \{1, p-1\}$$

Επομένως, $2 \cdot 3 \cdots (p-2) \equiv 1 \pmod{p}$, οπότε προκύπτει το ζητούμενο.
Αντίστροφα, αν $(p-1)! \equiv p-1 \pmod{p}$ και p σύνθετος, τότε διαιρείται από τον q, $1 < q < p$, οπότε $q|(p-1)!$ και $q|p$ άρα $q|1$, άτοπο. □

Ο αλγόριθμος RSA

Ο παραλήπτης Π του κρυφού μηνύματος επιλέγει δύο πρώτους αριθμούς p, q και υπολογίζει το γινόμενο $n = pq$, καθώς και την τιμή $\phi(n) = (p-1)(q-1)$. Επιπλέον, επιλέγει έναν αριθμό e, τέτοιον ώστε $\gcd(e, \phi(n)) = 1$ και υπολογίζει τον αντίστροφο d του e modulo $\phi(n)$, δηλαδή $ed \equiv 1 \pmod{\phi(n)}$. Τέλος, στέλνει τους αριθμούς n, e σε αυτόν που πρόκειται να στείλει το μήνυμα. Ο αποστολέας Α επιλέγει το μήνυμα M που θα στείλει στον Π, τέτοιο ώστε[2] $\gcd(M, n) = 1$.

[2] Αυτή η συνθήκη προφανώς ισχύει πάντα, εκτός αν το M είναι πολλαπλάσιο του p ή του q. Επειδή ως p, q επιλέγονται μεγάλοι πρώτοι, μπορεί να υποτεθεί ότι το M είναι πάντα μικρότερο από αυτούς.

Στη συνέχεια υπολογίζει το κρυπτογραφημένο μήνυμα C από τη σχέση

$$C \equiv M^e \pmod{n},$$

το οποίο και στέλνει.
Ο Π αποκωδικοποιεί το C με τη βοήθεια του d, το οποίο γνωρίζει μόνο αυτός, βάσει της σχέσης

$$M \equiv C^d \pmod{n}.$$

Πράγματι, βάσει του Θεωρήματος Euler-Fermat δεδομένου ότι υπάρχει ακέραιος k τέτοιος ώστε $ed = k\phi(n) + 1$, είναι

$$C^d \equiv M^{ed} \equiv M^{k\phi(n)+1} \equiv M \pmod{n}.$$

Τάξη στοιχείου - Αρχικές ρίζες

Έστω G μια (πολλαπλασιαστική) ομάδα (με μοναδιαίο στοιχείο το 1). Η τάξη ενός στοιχείου $a \in G$ συμβολίζεται ως $\mathrm{ord}(a)$ και ορίζεται ως ο ελάχιστος θετικός ακέραιος m ώστε $a^m = 1$. Αν δεν υπάρχει τέτοιος m, τότε ορίζουμε $\mathrm{ord}(a) = +\infty$.
Αν $\mathrm{ord}(a) < \infty$, ισχύουν οι ακόλουθες ιδιότητες (για $k, \ell \in \mathbb{Z}$):

- $a^k = 1 \Leftrightarrow \mathrm{ord}(a) | k$
- $a^k = a^\ell \Leftrightarrow \mathrm{ord}(a) | k - \ell$
- Αν $|G| = n < +\infty$, τότε $a^n = 1$ και $\mathrm{ord}(a) | n$.

Μια (πολλαπλασιαστική) πεπερασμένη ομάδα G, τάξης $|G| = n$ ονομάζεται κυκλική (τάξης n) όταν υπάρχει $a \in G$, τέτοιο ώστε $G = \{1, a, a^2, \ldots, a^{n-1}\}$, οπότε γράφουμε $G = \langle a \rangle$. Το στοιχείο a καλείται γεννήτορας της G. Στην περίπτωση αυτή, ισχύουν τα ακόλουθα:

- Κάθε υποομάδα H της G είναι κυκλική της μορφής $H = \langle a^q \rangle$ για κάποιο θετικό διαιρέτη q του n και αντίστροφα κάθε θετικός διαιρέτης q αντιστοιχεί σε μια μοναδική υποομάδα.
- Αν $d = \text{μκδ}(n, k)$, $k > 0$, τότε $\langle a^k \rangle = \langle a^d \rangle$ και $\text{ord}(a^k) = n/d$.
- $G = \langle a^k \rangle \Leftrightarrow \text{μκδ}(n, k) = 1$, άρα η G έχει $\phi(n)$ γεννήτορες.

Ένα ερώτημα που τίθεται είναι πότε η ομάδα $\mathbb{Z}_n^*$ είναι κυκλική. Ο ακέραιος a, όπου $[a]_n \in \mathbb{Z}_n^*$, καλείται αρχική ρίζα $\mathrm{mod} n$ ανν $\mathrm{ord}_n(a) := \mathrm{ord}([a]_n) = \phi(n)$. Σε αυτή την περίπτωση, προφανώς το $[a]_n$ είναι γεννήτορας, άρα η $\mathbb{Z}_n^*$ είναι κυκλική.

Ειδικά, αν p πρώτος, τότε η $\mathbb{Z}_p^*$ είναι κυκλική και υπάρχουν $\phi(p-1)$ γεννήτορες - αρχικές ρίζες $\mathrm{mod} p$.

Αν γνωρίζουμε την παραγοντοποίηση του $p-1 = p_1^{h_1} p_2^{h_2} \cdots p_k^{h_k}$, τότε μπορούμε να βρούμε μια αρχική ρίζα $\mathrm{mod} p$ ως εξής: Το $a \in \{2, 3, \ldots, p-2\}$ είναι αρχική ρίζα αν και μόνο αν $a^{(p-1)/p_i} \not\equiv 1 \pmod{p}$, για κάθε $i \in [k]$, διότι τότε $\mathrm{ord}(a) = p-1$ αφού από το μικρό θεώρημα του Fermat είναι $a^{p-1} \equiv 1 \pmod{p}$.

Γενικότερα, ισχύει το ακόλουθο αποτέλεσμα.

Θεώρημα

Αν $n > 1$, τότε υπάρχουν αρχικές ρίζες $\bmod n$ ανν $n \in \{2, 4, p^r, 2p^r\}$, όπου $r \geq 1$ και p περιττός πρώτος. Το πλήθος των αρχικών ριζών είναι $\phi(\phi(n))$ και αν a μια από αυτές, τότε το σύνολό τους είναι το $\{a^k \bmod n : k \in [\phi(n)], \mu\kappa\delta(k, \phi(n)) = 1\}$.

Παράδειγμα

Να βρεθούν οι αρχικές ρίζες στο $\mathbb{Z}_{34}^*$. (Υπόδειξη: Να ελεγχθεί πρώτα το 3.) Στη συνέχεια να λυθούν οι εξισώσεις

$$x^3 \equiv 5 \pmod{34}, \qquad 7^x \equiv 5 \pmod{34}.$$

Τετραγωνικά υπόλοιπα

Αν $n, m, a \in \mathbb{Z}$, $n, m > 1$ και μκδ$(a, n) = 1$, ο a καλείται υπόλοιπο m-οστής δύναμης $\mathrm{mod} n$ ανν η ισοτιμία $x^m \equiv a \pmod{n}$ έχει λύση. Στην περίπτωση αυτή, ο x καλείται m-οστή ρίζα του a. Αν $m = 2$, ο a καλείται τετραγωνικό υπόλοιπο και ο x τετραγωνική ρίζα. Θα συμβολίζουμε με T_n το σύνολο[3] των τετραγωνικών υπολοίπων $\mathrm{mod} n$.

Θεώρημα

Αν a, n, m, με $n, m > 1$, $n \in \{2, 4, p^r, 2p^r\}$, όπου $r \geq 1$ και p περιττός πρώτος, μκδ$(a, n) = 1$ και $d =$ μκδ$(m, \phi(n))$, τότε το a είναι υπόλοιπο m-οστής δύναμης ανν

$$a^{\phi(n)/d} \equiv 1 \pmod{n}.$$

Το πλήθος αυτών των a είναι $\phi(n)/d$ και κάθε ένα από αυτά έχει d m-οστές ρίζες.

[3] Δηλαδή, $T_n = (\mathbb{Z}_n^*)^2 = \{\beta^2 : \beta \in \mathbb{Z}_n^*\}$.

Τετραγωνικά υπόλοιπα

Ως ειδική περίπτωση για $m = 2$, $n = p$ περιττό πρώτο, οπότε $d = \text{μκδ}(m, \phi(p)) = 2$, παίρνουμε το ακόλουθο αποτέλεσμα:

Πόρισμα

Αν p περιττός πρώτος και $1 < a < p$, τότε $|T_p| = (p-1)/2$ και

$$a \in T_p \Leftrightarrow a^{(p-1)/2} \equiv 1 \pmod{p}.$$

Επιπλέον, αν g μια αρχική ρίζα $\bmod p$, τότε $g^{(p-1)/2} \equiv -1 \pmod{p}$, δηλαδή $g \notin T_p$ και όλα τα τετραγωνικά υπόλοιπα είναι οι άρτιες δυνάμεις της g. Κάθε ένα από αυτά, έστω g^{2k} έχει δύο τετραγωνικές ρίζες, τις $\pm g^k$.

Θεώρημα

Αν a, n, m, με $m > 1$, n περιττός και $n = p_1^{h_1} p_2^{h_2} \cdots p_k^{h_k}$ η παραγοντοποίηση του n, $\mu\kappa\delta(a, n) = 1$ και $d_i = \mu\kappa\delta(m, \phi(p_i^{h_i}))$, τότε η

$$x^m \equiv a \pmod{n}$$

έχει λύση ανν η $x^m \equiv a \pmod{p_i^{h_i}}$ έχει λύση. Το πλήθος των λύσεων αυτών είναι $d_1 d_2 \cdots d_k$.

Το σύμβολο του Legendre

Έστω p περιττός πρώτος και $a \in \mathbb{Z}$.

$$(a/p) = \begin{cases} 0, & p|a, \\ 1, & a \in T_p, \\ -1, & a \notin T_p. \end{cases}$$

Ιδιότητες

- $(a/p) \equiv a^{(p-1)/2} \pmod{p}$
- $(a/p)(b/p) = (ab/p)$
- $a \equiv b \pmod{p} \Rightarrow (a/p) = (b/p)$
- $(2/p) = (-1)^{(p^2-1)/8}$
- $(p/q)(q/p) = (-1)^{(p-1)(q-1)/4}$

Ειδικότερα,

$$\left(\frac{-1}{p}\right) = \begin{cases} 1, & p \equiv 1 \pmod{4} \\ -1, & p \equiv 3 \pmod{4} \end{cases} \quad \left(\frac{2}{p}\right) = \begin{cases} 1, & p \equiv \pm 1 \pmod{8} \\ -1, & p \equiv \pm 3 \pmod{8} \end{cases}$$

Παράδειγμα

Να υπολογισθεί το $(-28/11)$.

$$(-28/11) = (-4/11)(7/11) = (-1/11)(7/11) = -(-1) = 1.$$

Παράδειγμα

Να εξετασθεί αν η ισοτιμία $x^2 + 5x + 16 \equiv 0 \mod 19$ έχει λύση. Πολλαπλασιάζοντας κατά μέλη πρώτα με το αντίστροφο του 2 modulo 19 (δηλαδή το 10) και κατόπιν με το 2, παίρνουμε την ισοδύναμη $(x + 12)^2 \equiv 14 \pmod{19}$. Έχουμε

$$(14/19) = (2/19)(7/19) = -(7/19) = -(-1)(19/7) = (5/7) = -1,$$

άρα η ισοτιμία δεν έχει λύση.

Το σύμβολο του Jacobi

Έστω $n = p_1^{h_1} p_2^{h_2} \cdots p_k^{h_k}$ περιττός και $a \in \mathbb{Z}$. Το σύμβολο του Jacobi (a/n) ορίζεται ως

$$(a/n) = (a/p_1)^{h_1}(a/p_2)^{h_2} \cdots (a/p_k)^{h_k}$$

και ικανοποιεί τη σχέση $a \in T_n \Rightarrow (a/n) = 1$.
Προσοχή! Το αντίστροφο δεν ισχύει πάντα.

Ιδιότητες

- $(ab/n) = (a/n)(b/n)$
- $(a/nm) = (a/n)(a/m)$
- $a \equiv b \pmod{n} \Rightarrow (a/n) = (b/n)$
- $(ab^2/n) = (a/n)$
- $(-1/n) = (-1)^{(n-1)/2}$
- $(2/n) = (-1)^{(n^2-1)/8}$
- $(m/n)(n/m) = (-1)^{(n-1)(m-1)/4}$

Το σύμβολο του Jacobi

Ειδικότερα,

$$(-1/n) = \begin{cases} 1, & n \equiv 1 \pmod 4 \\ -1, & n \equiv 3 \pmod 4 \end{cases} \qquad (2/n) = \begin{cases} 1, & n \equiv \pm 1 \pmod 8 \\ -1, & n \equiv \pm 3 \pmod 8 \end{cases}$$

Αν ο a αναλυθεί ως $a = 2^h a'$, όπου a' περιττός, βάσει των δύο τελευταίων ιδιοτήτων είναι

$$(a/n) = (2/n)^h (a'/n) = (-1)^{\frac{n^2-1}{8} h} (-1)^{\frac{n-1}{2}\frac{a'-1}{2}} (n/a'),$$

οπότε βάσει αυτής της σχέσης, ο επόμενος αλγόριθμος υπολογίζει σωστά το σύμβολο Jacobi.

Το σύμβολο του Jacobi

Είσοδος: Οι ακέραιοι a, n, με n περιττό.
Έξοδος: Η τιμή του (a/n).

$t \leftarrow 1$;
while $1 = 1$ **do**
  if $a = 0$ **then**
    if $n = 1$ **then return** t;
    else return 0;
  end if
  Υπολόγισε h και a' περιττό, έτσι ώστε $a = 2^h a'$;
  if $h \not\equiv 0 \pmod 2$ **and** $n \not\equiv \pm 1 \pmod 8$ **then** $t \leftarrow -t$;
  if $a' \not\equiv 1 \pmod 4$ **and** $n \not\equiv 1 \pmod 4$ **then** $t \leftarrow -t$;
  $(a, n) \leftarrow (n, a')$;
end while

Αλγόριθμος 5: Αλγόριθμος υπολογισμού του συμβόλου Jacobi.

Ο χρόνος εκτέλεσης αυτού του αλγορίθμου είναι $O(\text{len}(a)\,\text{len}(n))$.

Έλεγχος αν $a \in T_n$

- Αν $n = p$ περιττός πρώτος, τότε ελέγχουμε αν $a \in T_p$ είτε υπολογίζοντας το $a^{(p-1)/2} \mod p$, σε χρόνο $O(\text{len}(p)^3)$, είτε υπολογίζοντας το σύμβολο Legendre (a/p) με τον προηγούμενο αλγόριθμο, σε χρόνο $O(\text{len}(p)^2)$.
- Αν $n = p^e$ είναι δύναμη περιττού πρώτου, τότε $a \in T_n \Leftrightarrow a \in T_p$, οπότε η περίπτωση αυτή ανάγεται στην προηγούμενη.
- Γενικά, είναι $a \in T_n \Leftrightarrow a \in T_p$ για κάθε πρώτο p διαιρέτη του n. Αν όμως η παραγοντοποίηση του n δεν είναι γνωστή, τότε μπορούμε να υπολογίσουμε το (a/n), Αν όμως προκύψει $(a/n) = 1$, τότε δεν μπορούμε να βγάλουμε συμπέρασμα.

Υπολογισμός τετραγωνικής ρίζας

Έστω ότι p περιττός πρώτος και $0 < a < p$ με $a \in T_p$.
Ο προσδιορισμός ενός b τέτοιου ώστε $b^2 \equiv a \pmod{p}$ (οπότε όλες οι ρίζες του a είναι οι $\pm b$) είναι απλός στην περίπτωση που $p \equiv 3 \pmod{4}$: Τότε ο $(p+1)/4$ είναι ακέραιος και

$$b \equiv a^{(p+1)/4} \pmod{p}.$$

Πράγματι, επειδή $a \in T_p$, είναι $a^{(p-1)/2} \equiv 1 \pmod{p}$, επομένως

$$b^2 \equiv a^{(p+1)/2} \equiv a^{(p-1)/2} a \equiv a \pmod{p}.$$

Υπολογισμός τετραγωνικής ρίζας

Στη γενική περίπτωση που μπορεί να ισχύει $p \not\equiv 3 \pmod 4$, αναλύουμε το $p-1$ ως $p-1 = 2^h m$, όπου m περιττός και χρησιμοποιούμε επίσης ένα βοηθητικό $c \notin T_p$ (το οποίο μπορούμε να υπολογίσουμε με διαδοχικές δοκιμές, μέχρις ότου $(c/p) = -1$). Ειδικά αν $p \equiv \pm 1 \pmod 8$, τότε $(2/p) = -1$, οπότε θέτουμε $c = 2$. Θεωρούμε ότι $h > 1$, διότι αν $h = 1$, τότε $p \equiv 3 \pmod 4$, οπότε αναγόμαστε στην προηγούμενη περίπτωση. Θέτουμε $\gamma = [c^m]_p$ και $\alpha = [a^m]_p$, και έχουμε ότι

$$\begin{cases} a \in T_p \\ c \notin T_p \end{cases} \Rightarrow \begin{cases} a^{2^{h-1}m} \equiv 1 \pmod p \\ c^{2^{h-1}m} \equiv -1 \pmod p \end{cases} \Rightarrow \begin{cases} \operatorname{ord}(\alpha) | 2^{h-1} \\ \operatorname{ord}(\gamma) = 2^h \end{cases}$$

Επομένως, το γ παράγει μια ομάδα τάξης 2^h ενώ το α παράγει μια υποομάδα αυτής, άρα υπάρχει άρτιος x, με $0 \le x < 2^h$, τέτοιος ώστε $\alpha = \gamma^x$. Αν τώρα τεθεί $\kappa = \gamma^{x/2}$, τότε $\kappa^2 = \alpha = [a^{(m-1)/2}]_p \odot [a^{(m-1)/2}]_p \odot [a]_p$, οπότε αν δ το αντίστροφο του $[a^{(m-1)/2}]_p$, πολλαπλασιάζοντας κατά μέλη με δ^2, βρίσκουμε τελικά ότι $(\delta \odot \kappa)^2 = [a]_p$

Υπολογισμός τετραγωνικής ρίζας

Είσοδος: Ο περιττός πρώτος p και οι ακέραιοι $a \in T_p$, $c \notin T_p$.
Έξοδος: Ένα $\beta = [b]_p$ ώστε $b^2 \equiv a \pmod{p}$.

Υπολόγισε h και m περιττό, έτσι ώστε $p - 1 = 2^h m$;
$(\gamma, \alpha) \leftarrow ([c^m]_p, [a^m]_p)$;
Υπολόγισε x ώστε $\alpha = \gamma^x$;
$\beta \leftarrow \gamma^{x/2} \odot \alpha^{-\lfloor m/2 \rfloor}$;
return β;

Αλγόριθμος 6: Αλγόριθμος υπολογισμού τετραγωνικής ρίζας $\mathrm{mod} p$.

Υπολογισμός τετραγωνικής ρίζας

Αν $n = p^{f+1}$, όπου p πρώτος και $f > 0$, και $a \in T_n$, τότε μπορούμε να βρούμε μια ρίζα b, με $b^2 \equiv a \pmod{p^{f+1}}$, αν γνωρίζουμε μια ρίζα z, με $z^2 \equiv a \pmod{p^f}$.
Πράγματι, τότε είναι

$$b^2 \equiv a \pmod{p^{f+1}} \Rightarrow b^2 \equiv a \pmod{p^f}$$
$$\Rightarrow b^2 \equiv z^2 \pmod{p^f} \Rightarrow b \equiv \pm z \pmod{p^f}$$

Επομένως, υπάρχει u ώστε $b \equiv z + up^f \pmod{p^{f+1}}$, οπότε

$$b^2 \equiv (z + up^f)^2 \equiv z^2 + 2zup^f \pmod{p^{f+1}}$$

άρα $2zup^f \equiv (a - z^2) \pmod{p^{f+1}}$. Επειδή $p^f | a - z^2$, έπεται ότι $2zu \equiv (a - z^2) \pmod{p}$ και αν c ο πολλαπλασιαστικός αντίστροφος του $2z \bmod p$, τότε $u \equiv c(a - z^2) \pmod{p}$ και άρα το u μπορεί να υπολογισθεί.

Επομένως, στην περίπτωση που ο n είναι δύναμη πρώτου, το πρόβλημα ανάγεται επαναληπτικά στην προηγούμενη περίπτωση.

Παρατήρηση

Με παρόμοια προσέγγιση, θα μπορούσαμε να προσδιορίσουμε τέτοιο b βασιζόμενοι στην ιδιότητα
$x \equiv y \pmod{p^f} \Rightarrow x^p \equiv y^p \pmod{p^{f+1}}$ (άσκηση).

Γενικά, αν είναι γνωστή η παραγοντοποίηση του n, μπορούμε χρησιμοποιώντας τις 2 προηγούμενες περιπτώσεις και το Κινέζικο Θεώρημα Υπολοίπων, να υπολογίσουμε μια τετραγωνική ρίζα του a. Στην αντίθετη όμως περίπτωση, δεν υπάρχει γνωστός αποδοτικός αλγόριθμος. Μάλιστα, ένας τέτοιος αλγόριθμος θα μπορούσε να δώσει και έναν αποδοτικό (πιθανοτικό) αλγόριθμο παραγοντοποίησης του n.

Παρατήρηση (λύση)

Αν $x \equiv y \pmod{p^f}$, τότε $x = y + kp^f$, $k \in \mathbb{Z}$, οπότε

$$x^p = (y + kp^f)^p = y^p + py^{p-1}kp^f + \sum_{i=2}^{p} \binom{p}{i} y^{p-i}(kp^f)^i$$

$$\equiv y^p \pmod{p^{f+1}}.$$

Επιπλέον, αν $x^2 \equiv a \pmod{p^f}$ και b ο αντίστροφος του a $\bmod p^{f+1}$, έχουμε ότι

$$x^2 \equiv a \pmod{p^f} \Rightarrow x^{2p} \equiv a^p \pmod{p^{f+1}}$$

$$\Rightarrow b^{p-1}x^{2p} \equiv a \pmod{p^{f+1}} \Rightarrow (b^{(p-1)/2}x^p)^2 \equiv a \pmod{p^{f+1}}.$$

Επομένως, υπολογίζοντας μια τετραγωνική ρίζα $x \bmod p^f$ και τον αντίστροφο b του $a \bmod p^{f+1}$, βρίσκουμε την τετραγωνική ρίζα $b^{(p-1)/2}x^p$ του $a \bmod p^{f+1}$.

Πιστοποίηση πρώτου - Κριτήριο του Lucas

Στην ενότητα αυτή θεωρούμε ότι ο $n > 1$ είναι περιττός ακέραιος και εξετάζουμε μεθόδους ελέγχου - κριτήρια αν n πρώτος.
Το επόμενο αποτέλεσμα είναι γνωστό ως κριτήριο του Lucas:

Πρόταση

Ο θετικός περιττός ακέραιος n είναι πρώτος ανν υπάρχει ακέραιος $a > 1$ τέτοιος ώστε

$$a^{n-1} \equiv 1 \pmod{n} \qquad \textit{και} \qquad a^{(n-1)/p} \not\equiv 1 \pmod{n},$$

για κάθε πρώτο διαιρέτη p του $n-1$.

Απόδειξη.

Αν n πρώτος, τότε μια αρχική ρίζα a ικανοποιεί τις παραπάνω σχέσεις. Αντίστροφα, αν υπάρχει τέτοιος a, τότε προφανώς $[a]_n \in \mathbb{Z}_n^*$ (ο αντίστροφός του είναι ο $[a^{n-2}]_n$) και $r = \mathrm{ord}([a]_n) = n-1$, διότι $r|n-1$ και $r \neq (n-1)/p$, για κάθε πρώτο διαιρέτη p του $n-1$. Όμως $r|\phi(n)$ και $\phi(n) \leq n-1$, άρα $\phi(n) = n-1$, δηλαδή n πρώτος. □

Το παραπάνω κριτήριο έχει προφανώς το μειονέκτημα ότι απαιτεί τη γνώση της παραγοντοποίησης του $n-1$. Μπορεί όμως να χρησιμοποιηθεί για την κατασκευή ενός μεγάλου πρώτου. Κατασκευάζουμε τον $n-1$ ως γινόμενο γνωστών πρώτων και αν ικανοποιούνται οι συνθήκες για κάποιο $a > 1$, τότε ο n είναι πρώτος.

Πιστοποίηση πρώτου - Κριτήριο του Pocklington

Το επόμενο κριτήριο (Pocklington) απαιτεί να είναι γνωστό μόνο ένα μέρος της παραγοντοποίησης του $n-1$.

Πρόταση

Έστω θετικός περιττός ακέραιος n, με $n-1 = fr$, όπου $\mu\kappa\delta(f, r) = 1$, $f > 1$ και οι πρώτοι παράγοντες του f είναι γνωστοί. Αν υπάρχει ακέραιος $a > 1$ τέτοιος ώστε

$$a^{n-1} \equiv 1 \pmod{n} \qquad \text{και} \qquad \mu\kappa\delta(a^{(n-1)/q} - 1, n) = 1$$

για κάθε πρώτο διαιρέτη q του f, τότε ισχύει $f | p-1$, για κάθε πρώτο διαιρέτη p του n.
Επιπλέον, αν $f \geq \sqrt{n}$, τότε n πρώτος.

Απόδειξη.

Έστω p πρώτος διαιρέτης του n. Από την πρώτη σχέση είναι $(a^r)^f \equiv 1 \pmod{n}$, άρα $(a^r)^f \equiv 1 \pmod{p}$, δηλαδή $\mathrm{ord}([a^r]_p) | f$. Για τη δεύτερη σχέση, έχουμε ότι

$$\begin{aligned} \text{μκδ}(a^{(n-1)/q} - 1, n) = 1 &\Rightarrow \text{μκδ}(a^{(n-1)/q} - 1, p) = 1 \\ &\Rightarrow a^{(n-1)/q} \not\equiv 1 \pmod{p} \end{aligned}$$

Επομένως, για κάθε q πρώτο παράγοντα του f είναι $f = qk$, $rk = \frac{n-1}{f} k = \frac{n-1}{q}$ και

$$(a^r)^k \equiv a^{(n-1)/q} \not\equiv 1 \pmod{p},$$

δηλαδή $\mathrm{ord}([a^r]_p) = f$. Άρα, $f | p-1$.
Αν τώρα είναι $f \geq \sqrt{n}$ και n σύνθετος, θα υπάρχει πρώτος $p \leq \sqrt{n}$ διαιρέτης του n, οπότε $p - 1 < \sqrt{n} \leq f$, άτοπο, διότι $f | p - 1$. □

Πιστοποίηση πρώτου - Κριτήριο του Proth

Πόρισμα

Αν $n-1=2^m r$ *με* r *περιττό και* $2^m > r$, *τότε αν υπάρχει* $a>1$ *τέτοιος ώστε* $a^{(n-1)/2} \equiv -1 \pmod{n}$, *ο* n *είναι πρώτος.*

Απόδειξη.

$a^{(n-1)/2} \equiv -1 \pmod{n} \Rightarrow$ μκδ$(a^{(n-1)/2}-1, n)=$μκδ$(-2, n)=1$.
Επιπλέον, $2^m > r \Rightarrow (2^m)^2 > n-1 \Rightarrow 2^m \geq \sqrt{n}$.
Κατόπιν τούτων, το αποτέλεσμα προκύπτει εφαρμόζοντας την προηγούμενη Πρόταση για $f=2^m$. □

Παρατήρηση

Το αντίστροφο ισχύει πάντα, ακόμα και αν $2^m < r$, διότι αν n πρώτος, τότε η $a^{(n-1)/2} \equiv -1 \pmod{n}$ ικανοποιείται για a μια αρχική ρίζα $\bmod n$.

Στην παρατήρηση αυτή βασίζεται το κριτήριο των Miller-Rabin, που παρουσιάζεται παρακάτω.

Πιστοποίηση πρώτου - Κριτήριο του Fermat

Σύμφωνα με το μικρό Θεώρημα του Fermat, αν n πρώτος, τότε $a^{n-1} \equiv 1 \pmod{n}$, για κάθε $a \in \{2, 3, \ldots, n-1\}$. Επομένως, αν για κάποιο τέτοιο a έχουμε ότι $a^{n-1} \not\equiv 1 \pmod{n}$ συμπεραίνουμε ότι n σύνθετος. Είναι δυνατόν όμως για κάποιο a να ισχύει η παραπάνω ισοτιμία, παρόλο που ο n είναι σύνθετος. Τότε ο n ονομάζεται ψευδοπρώτος ως προς τη βάση a.
Αν

$$L_n = \{[a]_n \in \mathbb{Z}_n^* : a^{n-1} \equiv 1 \pmod{n}\},$$

το σύνολο των βάσεων για τις οποίες ο n είναι ψευδοπρώτος, είναι εύκολο να διαπιστώσουμε ότι L_n υποομάδα της $\mathbb{Z}_n^*$, άρα η τάξη της L_n διαιρεί την τάξη της $\mathbb{Z}_n^*$, οπότε αν $L_n \neq \mathbb{Z}_n^*$, τότε θα είναι $|L_n| \leq |\mathbb{Z}_n^*|/2$. Αυτό σημαίνει ότι αν επιλέξουμε t βάσεις $a_1, \ldots, a_t$, η πιθανότητα να ισχύει $a_1, \ldots, a_t \in L_n$ είναι το πολύ 2^{-t}.

Δυστυχώς όμως, υπάρχουν σύνθετοι αριθμοί n τέτοιοι ώστε $L_n = \mathbb{Z}_n^*$. και ονομάζονται αριθμοί Carmichael.

Ορισμός

Ένας σύνθετος ακέραιος n ονομάζεται αριθμός Carmichael ανν $a^{n-1} \equiv 1 \pmod{n}$, για κάθε $a > 1$, με μκδ$(a, n) = 1$.

Ο μικρότερος αριθμός Carmichael είναι ο $561 = 3 \cdot 11 \cdot 17$.

Πρόταση

Ένας περιττός σύνθετος ακέραιος $n > 3$ είναι αριθμός Carmichael ανν είναι της μορφής $n = p_1 p_2 \cdots p_r$, όπου $r \geq 3$, p_i, $i \in [r]$, διακεκριμένοι πρώτοι και $p_i - 1 | n - 1$, για κάθε $i \in [r]$.

Απόδειξη.

Ας είναι $n = \prod_{i=1}^{r} p_i^{e_i}$ η παραγοντοποίηση του n, όπου p_i πρώτος, $e_i \geq 1$ και $r \geq 2$, οπότε $\phi(n) = \prod_{i=1}^{r} p_i^{e_i-1}(p_i - 1)$.
Αφού για κάθε ακέραιο a με μκδ$(a, n) = 1$ είναι $a^{n-1} \equiv 1 \pmod{n}$, θα είναι και $a^{n-1} \equiv 1 \pmod{p_i^{e_i}}$, για κάθε i.
Όμως, η $\mathbb{Z}^*_{p_i^{e_i}}$ είναι κυκλική, τάξης $m_i = \phi(p_i^{e_i}) = p_i^{e_i-1}(p_i - 1)$, οπότε αν επιλεχθεί το a ώστε $\mathrm{ord}([a]_{p_i^{e_i}}) = m_i$, προκύπτει ότι $m_i | n - 1$ (αφού $m_i \leq \phi(n) \leq n - 1$). Η τελευταία σχέση ισχύει για κάθε i, άρα $p_i - 1 | n - 1$ για κάθε $i \in [r]$.
Αν τώρα $e_i > 1$, για κάποιο i, τότε $p_i | m_i | n - 1$ και $p_i | n$, δηλαδή $n \equiv 1 \pmod{p_i}$ και $n \equiv 0 \pmod{p_i}$, άτοπο.
Τέλος, αν $r = 2$, τότε $n - 1 = p_1 p_2 - 1 = (p_1 - 1)p_2 + p_2 - 1$.
Επομένως, δεδομένου ότι $p_1 - 1 | n - 1$ και $p_2 - 1 | n - 1$, έπεται ότι $p_1 - 1 | p_2 - 1$ και $p_2 - 1 | p_1 - 1$, δηλαδή $p_1 = p_2$, άτοπο.
Αντίστροφα, αν $n = p_1 p_2 \cdots p_r$, με $p_i - 1 | n - 1$, και $a \in \mathbb{Z}$, με μκδ$(a, n) = 1$, τότε $a^{p_i-1} \equiv 1 \pmod{p_i} \Rightarrow a^{n-1} \equiv 1 \pmod{p_i}$, οπότε $p_i | a^{n-1} - 1$, για κάθε i, άρα $n | a^{n-1} - 1$.

Στη συνέχεια, παρουσιάζεται ένας διαφορετικός έλεγχος, ο οποίος χρησιμοποιεί το σύνολο L'_n στη θέση του L_n και βασίζεται στην ακόλουθη Πρόταση:

Πρόταση

Έστω $n \geq 3$ περιττός ακέραιος και έστω το σύνολο

$$L'_n = \{[a]_n \in \mathbb{Z}_n^* : (a/n) \equiv a^{(n-1)/2} \pmod{n}\}.$$

Τότε ο n είναι πρώτος ανν $L'_n = \mathbb{Z}_n^*$. Επιπλέον, αν n σύνθετος, τότε $|L'_n| \leq \phi(n)/2$. δ

Παρατήρηση

Προφανώς, είναι $L'_n \subseteq L_n$, διότι $[a]_n \in \mathbb{Z}_n^* \Rightarrow (a/n) = \pm 1$, άρα $[a]_n \in L'_n \Rightarrow a^{n-1} \equiv 1 \pmod{n} \Rightarrow [a]_n \in L_n$.

Απόδειξη.

Το ευθύ προκύπτει άμεσα από τις ιδιότητες του συμβόλου Legendre. Για το αντίστροφο, υποθέτουμε ότι n σύνθετος και ότι $L'_n = \mathbb{Z}_n^*$. Επομένως, $a^{n-1} \equiv 1 \pmod{n}$, για κάθε a, δηλαδή ο n είναι αριθμός Carmichael δηλαδή της μορφής $n = p_1 p_2 \cdots p_r$, $r > 2$.

Αν επιλέξουμε θετικούς ακεραίους $a_1, a_2, \ldots, a_r$ με $\text{μκδ}(a_i, p_i) = 1$, τέτοιους ώστε

$$(a_1/p_1)(a_2/p_2)\cdots(a_r/p_r) \not\equiv a_1^{(n-1)/2} \pmod{p_1}$$

τότε από το Κινέζικο Θεώρημα Υπολοίπων υπάρχει μοναδικός $0 < a < n$, ώστε $a \equiv a_i \pmod{p_i}$, για κάθε $i \in [r]$. Προφανώς είναι $\text{μκδ}(a, n) = 1$, και από τις ιδιότητες του συμβόλου Jacobi είναι

$$(a/n) = (a/p_1)(a/p_2)\cdots(a/p_r) = (a_1/p_1)(a_2/p_2)\cdots(a_r/p_r).$$

Συνέχεια απόδειξης.

Όμως, υποθέσαμε ότι $(a/n) \equiv a^{(n-1)/2} \pmod{n}$, οπότε

$$(a/n) \equiv a^{(n-1)/2} \pmod{n} \equiv a^{(n-1)/2} \pmod{p_1} \equiv a_1^{(n-1)/2} \pmod{p_1},$$

το οποίο είναι άτοπο.
Αν τώρα ο n είναι σύνθετος, τότε βάσει των προηγούμενων, είναι $L'_n \subset \mathbb{Z}_n^*$, και δεδομένου ότι L'_n αποτελεί γνήσια υποομάδα της $\mathbb{Z}_n^*$, έπεται ότι έχει τάξη που διαιρεί την τάξη της $\mathbb{Z}_n^*$ και είναι μικρότερη από αυτήν, άρα

$$|L'_n| \leq |\mathbb{Z}_n^*|/2 = \phi(n)/2.$$

□

Πιστοποίηση πρώτου - Κριτήριο των Solovay-Strassen

Βάσει της τελευταίας Πρότασης, έχουμε τον ακόλουθο αλγόριθμο πιστοποίησης πρώτου:

Είσοδος: Ο περιττός ακέραιος $n > 3$ και ο ακέραιος $t \geq 1$.
Έξοδος: Η απάντηση ''n σύνθετος'' ή ''n πιθανώς πρώτος''.
for $i \leftarrow 1$ **to** t **do**
    Διάλεξε τυχαίο $a \in \{2, 3, \ldots, n-1\}$;
    if $\mu\kappa\delta(a, n) > 1$ **then return** ''n σύνθετος'';
    if $(a/n) \not\equiv a^{(n-1)/2} \pmod{n}$ **then return** ''n σύνθετος'';
end for
return ''n πιθανώς πρώτος'';

Αλγόριθμος 7: Αλγόριθμος Solovay-Strassen.

Ο χρόνος εκτέλεσης είναι $O(t\,\mathrm{len}(n)^3)$ (η πιο δαπανηρή πράξη είναι ο υπολογισμός δύναμης που απαιτεί χρόνο $O(\mathrm{len}(n)^3)$), επομένως είναι πολυωνυμικός για μικρές τιμές του t, π.χ. $t \leq \mathrm{len}(n)$. Επιπλέον, άμεσα προκύπτει ότι η πιθανότητα ένας σύνθετος n να περάσει τον έλεγχο ως ''πιθανώς πρώτος'' είναι το πολύ 2^{-t}.

Πρόταση

Έστω περιττός $n > 1$, με $n - 1 = 2^h m$, όπου m περιττός και $h > 0$ και έστω το σύνολο L_n'' όλων των $\alpha \in \mathbb{Z}_n^*$, με

$$\alpha^{n-1} = [1]_n \text{ και } \alpha^{2^j m} = [1]_n \Rightarrow \alpha^{2^{j-1} m} = [\pm 1]_n,$$

για κάθε $j \in [h]$. Τότε ισχύουν τα εξής:
Αν n πρώτος, τότε $L_n'' = \mathbb{Z}_n^*$.
Αν n σύνθετος, τότε $|L_n''| \leq (n-1)/4$.

Βάσει της παραπάνω Πρότασης, έχουμε τον ακόλουθο αλγόριθμο πιστοποίησης πρώτου:

Πιστοποίηση πρώτου - Κριτήριο των Miller-Rabin

Είσοδος: Ο περιττός ακέραιος $n > 3$ και ο ακέραιος $t \geq 1$.
Έξοδος: Η απάντηση ''n σύνθετος'' ή ''n πιθανώς πρώτος''.

Υπολόγισε h και m περιττό, έτσι ώστε $n - 1 = 2^h m$;
for $i \leftarrow 1$ **to** t **do**
    Διάλεξε τυχαίο $a \in \{2, 3, \ldots, n-1\}$;
    if $\mu\kappa\delta(a, n) > 1$ **then return** ''n σύνθετος'';
    $\beta = [a^m]_n$;
    if $\beta = [1]_n$ **then continue** ;
    for $j \leftarrow 0$ **to** $h - 1$ **do**
        if $\beta = [-1]_n$ **then break** ;
        if $\beta = [1]_n$ **then return** ''n σύνθετος'';
        $\beta \leftarrow \beta^2$;
    end for
    if $j = h$ **then return** ''n σύνθετος'';
end for
return ''n πιθανώς πρώτος'';

Αλγόριθμος 8: Αλγόριθμος Miller-Rabin.

Πιστοποίηση πρώτου - Κριτήριο των Miller-Rabin

Ο χρόνος εκτέλεσης είναι $O(t \operatorname{len}(n)^3)$ (η πιο δαπανηρή πράξη είναι ο υπολογισμός δύναμης που απαιτεί χρόνο $O(\operatorname{len}(n)^3)$), επομένως είναι πολυωνυμικός για μικρές τιμές του t, π.χ. $t \leq \operatorname{len}(n)$. Επιπλέον, άμεσα προκύπτει ότι η πιθανότητα ένας σύνθετος n να περάσει τον έλεγχο ως ‘‘πιθανώς πρώτος’’ είναι το πολύ 4^{-t}.

Παραγοντοποίηση ακεραίων

Στην ενότητα αυτή θεωρούμε ότι ο $n > 1$ είναι ένας περιττός ακέραιος. Οι μέθοδοι που θα παρουσιαστούν έχουν ως στόχο την εύρεση ενός μη τετριμμένου παράγοντα του n (δηλαδή διάφορου του 1 και του n), εφόσον ο n δεν είναι πρώτος.

Ειδικό ενδιαφέρον παρουσιάζει η περίπτωση όπου ο n είναι γινόμενο δύο διαφορετικών πρώτων p, q, δηλαδή $n = pq$, με $2 < p < \sqrt{n} < q < n$.

Ο πιο απλός τρόπος εύρεσης ενός πρώτου παράγοντα είναι η δοκιμαστική διαίρεση: Ελέγχουμε για κάθε πρώτο $p \leq \sqrt{n}$ αν $p|n$. Αν δεν υπάρχει τέτοιος p, τότε n πρώτος.
Όπως έχουμε ήδη δει, αν γνωρίζουμε όλους τους πρώτους στο $[2, \sqrt{n}]$, η δοκιμαστική διαίρεση απαιτεί χρόνο $\Theta(\sqrt{n} \operatorname{len} n)$ στη χειρότερη περίπτωση που ο n είναι όντως πρώτος.

Η μέθοδος του Fermat

Η μέθοδος αυτή βασίζεται στην παρατήρηση ότι αν $n = ab$, με $a \geq b > 0$, τότε θέτοντας $s = (a - b)/2$ και $t = (a + b)/2$, προκύπτει $n = t^2 - s^2 = (t + s)(t - s)$, δηλαδή υπάρχει αμφιμονοσήμαντη αντιστοιχία μεταξύ των τρόπων που ο n γράφεται ως γινόμενο δύο θετικών ακεραίων και ως διαφορά τετραγώνων δύο θετικών ακεραίων. Επομένως, αν ευρεθούν κατάλληλοι θετικοί ακέραιοι ώστε $n = t^2 - s^2$, τότε αυτόματα έχουμε μια παραγοντοποίηση του n. Αν επιπλέον $1 < t - s$, τότε η παραγοντοποίηση δεν είναι τετριμμένη.

Για την εύρεση των s, t, δοκιμάζουμε τις τιμές

$$t = \lfloor \sqrt{n} \rfloor + i, \qquad i = 1, 2, 3, \ldots$$

και ελέγχουμε αν ο $t^2 - n$ είναι τέλειο τετράγωνο, οπότε έχουμε εντοπίσει το αντίστοιχο s.

Η μέθοδος του Fermat

Αφού ο t παίρνει τιμές $\lfloor\sqrt{n}\rfloor + 1, \ldots, (a+b)/2$, έπεται ότι η μέθοδος θα κάνει $(a+b)/2 - \lfloor\sqrt{n}\rfloor$ επαναλήψεις.

Σημειώνεται ότι ο αριθμός $t+s$ που εντοπίζεται με αυτόν τον τρόπο είναι ο μικρότερος παράγοντας του n που είναι $\geq \sqrt{n}$ και αντίστοιχα ο $t-s$ είναι ο μεγαλύτερος παράγοντας $\leq \sqrt{n}$. Επομένως, αν ο n έχει παράγοντα κοντά στο $\sqrt{n}$, τότε η μέθοδος θα χρειαστεί μικρό αριθμό βημάτων.

Ειδικά, αν $n = pq$, όπου p, q πρώτοι με $2 < p < \sqrt{n} < q$, τότε το πλήθος A των βημάτων της μεθόδου είναι

$$A = (p+q)/2 - \lfloor\sqrt{n}\rfloor = \lceil(\sqrt{p} - \sqrt{q})^2/2\rceil.$$

Η μέθοδος του Fermat

Η επόμενη πρόταση γενικεύει την παρατήρηση του Fermat.

Πρόταση

Αν $n > 1$ σύνθετος περιττός ακέραιος που δεν είναι δύναμη ακεραίου, τότε υπάρχουν ακέραιοι t, s, με $t^2 \equiv s^2 \pmod{n}$ και $t \not\equiv \pm s \pmod{n}$. Επιπλέον, τότε οι μκδ$(t \pm s, n)$ είναι μη τετριμμένοι διαιρέτες του n.

Απόδειξη.

Ο n θα γράφεται ως $n = ab$, με $a, b > 1$ και μκδ$(a, b) = 1$. Αν επιλέξουμε ακέραιο s με μκδ$(s, n) = 1$, τότε από το Κινέζικο Θεώρημα Υπολοίπων, υπάρχει ακέραιος t τέτοιος ώστε $t \equiv s \pmod{a}$ και $t \equiv -s \pmod{b}$. Ισοδύναμα $a|t - s$ και $b|t + s$, οπότε $n|t^2 - s^2$, δηλαδή $t^2 \equiv s^2 \pmod{n}$.
Αν τώρα $t \equiv s \pmod{n}$, τότε $b|n|t - s$ και αφού $b|t + s$ έπεται ότι $b|2s$. Όμως μκδ$(s, n) = 1 \Rightarrow$ μκδ$(s, b) = 1$, οπότε $b|2$, άτοπο. Άρα $t \not\equiv s \pmod{n}$. Ομοίως προκύπτει ότι $t \not\equiv -s \pmod{n}$.
Τέλος, αν $t^2 \equiv s^2 \pmod{n}$ και $t \not\equiv \pm s \pmod{n}$, δηλαδή

$$n|(t - s)(t + s), \quad n \nmid t - s, \quad n \nmid t + s,$$

έπεται ότι ο n έχει έναν παράγοντα $1 < f < n$ που διαιρεί τον $t + s$. Επομένως, $1 <$ μκδ$(t + s, n) < n$. Ομοίως προκύπτει ότι $1 <$ μκδ$(t - s, n) < n$. □

Η μέθοδος του Fermat

Οι μέθοδοι που ακολουθούν προσπαθούν να βρουν ακεραίους t, s που ικανοποιούν τις ισοτιμίες της προηγούμενης πρότασης, και μέσω αυτών να πετύχουν παραγοντοποίηση του n.

Παρατήρηση

Αν θεωρήσουμε ότι $[t]_n, [s]_n \in \mathbb{Z}_n^*$, τότε η εύρεση κατάλληλων t, s ισοδυναμεί με την εύρεση μιας μη τετριμμένης τετραγωνικής ρίζας του 1 modulo n. Πράγματι, αν τεθεί $[a]_n = [t]_n \odot [s]_n^{-1}$, τότε οι ισοτιμίες της προηγούμενης πρότασης ισοδυναμούν με τις ισοτιμίες $a^2 \equiv 1 \pmod{n}$ και $a \not\equiv \pm 1 \pmod{n}$ και ο μκδ$(a-1, n)$ είναι μη τετριμμένος παράγοντας του n.

Αλγόριθμος του Dixon

Έστω y θετικός ακέραιος. Ο ακέραιος $n > 1$ ονομάζεται y-λείος, αν κάθε πρώτος διαιρέτης του είναι μικρότερος ή ίσος του y.
Ο αλγόριθμος του Dixon έχει ως εξής:

- Επιλέγουμε y και σχηματίζουμε το σύνολο $B = \{p_1, p_2, \ldots, p_k\}$, $k = \pi(y)$, των πρώτων μέχρι y. Αν κάποιος $p \in B$ διαιρεί τον n, τότε ο αλγόριθμος επιστρέφει τον p και τερματίζει.
- Βρίσκουμε $k+1$ σε πλήθος ακεραίους t_i τέτοιους ώστε οι $a_i := t_i^2 \bmod n$, $1 < a_i < n$, να είναι y-λείοι (ο έλεγχος γίνεται με δοκιμαστική διαίρεση), δηλαδή

$$a_i = p_1^{e_{i1}} p_2^{e_{i2}} \cdots p_k^{e_{ik}}, \qquad i \in [k+1]$$

  και θέτουμε $v_i := (e_{i1}, \ldots, e_{ik})$ και $\overline{v}_i := ([e_{i1}]_2, \ldots, [e_{ik}]_2)$.
- Τα διανύσματα $\overline{v}_i$ του χώρου $\mathbb{Z}_2^k$ είναι $k+1$ σε πλήθος, άρα γραμμικώς εξαρτημένα. Επομένως, μπορούμε να βρούμε (με απαλοιφή Gauss) συντελεστές $c_1, c_2, \ldots, c_{k+1} \in \{0, 1\}$, όχι όλους μηδέν, τέτοιους ώστε $\sum_{i=1}^{k+1} c_i \overline{v}_i = ([0]_2, \ldots, [0]_2)$.

Αλγόριθμος του Dixon

- Θέτουμε $(e_1, \ldots, e_k) := \sum_{i=1}^{k+1} c_i v_i$, οπότε οι e_i είναι άρτιοι. Επιπλέον, θέτουμε

  $$t \equiv t_1^{c_1} t_2^{c_2} \cdots t_k^{c_k} \pmod{n} \quad \text{και} \quad s \equiv p_1^{e_1/2} p_2^{e_2/2} \cdots p_k^{e_k/2} \pmod{n}$$

  οπότε $t^2 \equiv s^2 \pmod{n}$. Πράγματι, είναι

  $$t^2 \equiv \prod_{i=1}^{k+1} a_i^{c_i} = \prod_{i=1}^{k+1} \prod_{j=1}^{k} p_j^{c_i e_{ij}} = \prod_{j=1}^{k} \prod_{i=1}^{k+1} p_j^{c_i e_{ij}} = \prod_{j=1}^{k} p_j^{\sum_{i=1}^{k+1} c_i e_{ij}}$$
  $$= \prod_{j=1}^{k} p_j^{e_j} \equiv s^2 \pmod{n}.$$

- Αν $t \not\equiv \pm s \pmod{n}$, τότε ο αλγόριθμος επιστρέφει τον μη τετριμμένο διαιρέτη μκδ$(t - s, n)$ και τερματίζει. Αλλιώς βρίσκουμε άλλους συντελεστές c_i, αν αυτό είναι δυνατόν, ή επιλέγουμε μεγαλύτερο y.

Αλγόριθμος του Dixon

Ο χρόνος εκτέλεσης εξαρτάται από την επιλογή του y.
Αποδεικνύεται ότι η απόδοση του αλγορίθμου είναι βέλτιστη όταν επιλέγεται $y = \exp\{O((f(n))^{1/2}\}$, όπου $f(n) = \log n \log\log n$, οπότε ο χρόνος εκτέλεσης είναι $O(\exp\{c(f(n))^{1/2}\})$.
Ειδικά, αν $y = \exp\{(f(n)/2)^{1/2}\}$, τότε ο χρόνος είναι $\exp\{(2\sqrt{2} + o(1))(f(n))^{1/2}\}$.

Παρατήρηση

Αν ο n έχει $r \geq 2$ πρώτους παράγοντες, τότε η ισοτιμία $x^2 \equiv s^2 \pmod{n}$ έχει 2^r λύσεις, οπότε είναι $t \equiv \pm s \pmod{n}$ με πιθανότητα $1/2^{r-1}$.

Αλγόριθμος του δευτεροβάθμιου κόσκινου

Ο αλγόριθμος αυτός επινοήθηκε από τον Pomerance (1982) και βελτιώνει τον αλγόριθμο του Dixon, βελτιώνοντας τον τρόπο επιλογής των y-λείων τετραγώνων a_i. Για το σκοπό αυτό χρησιμοποιείται το δευτεροβάθμιο πολυώνυμο $F(x) = (x + \lfloor\sqrt{n}\rfloor)^2 - n$ και μια επιπλέον παράμετρος z. Δοκιμάζεται κάθε ακέραιος s, με $1 \leq s \leq z$ και αν ο $F(s)$ είναι y-λείος, τίθεται $a_i = (s + \lfloor\sqrt{n}\rfloor) \mathrm{mod} n$, αφού $F(s) \equiv (s + \lfloor\sqrt{n}\rfloor)^2 \pmod{n}$.
Ο έλεγχος αν ο $F(s)$ είναι y-λείος γίνεται όχι με δοκιμαστική διαίρεση, αλλά με έναν αλγόριθμο κόσκινου, ο οποίος έχει ως εξής:
Ορίζουμε ένα διάνυσμα $v = (v_1, \ldots, v_z)$, με αρχικές τιμές $v_s = F(s)$, για το οποίο τελικά θα είναι $v_s = 1$ ανν $F(s)$ y-λείος. Στη συνέχεια, υπολογίζουμε τις ρίζες $\mathrm{mod} p$ του $F(x)$, για κάθε πρώτο $p \in B$. Αυτό μπορεί να γίνει με τον αλγόριθμο για τετραγωνικές ρίζες που παρουσιάστηκε στα προηγούμενα.

Αλγόριθμος του δευτεροβάθμιου κόσκινου

Οι ρίζες θα είναι σε πλήθος 0 ή 2 για $p > 2$ και μία για $p = 2$.
Έστω R_p το σύνολο αυτών των ριζών.
Επίσης, $F(s) \equiv 0 \pmod{p} \Leftrightarrow s \equiv r \pmod{p}$, όπου $r \in R_p$.
Επιπλέον, $F(s + kp) \equiv F(s) \pmod{p}$, για κάθε $k \in \mathbb{Z}$.
Κατόπιν τούτων, αφού εκτελέσουμε την επανάληψη

```
foreach p ∈ B do
    foreach r ∈ R_p do
        s ← r;
        while s ≤ z do
            repeat v_s ← v_s/p until p ∤ v_s;
            s ← s + p;
        end while
    end foreach
end foreach
```

τελικά θα είναι $v_s = 1$ ανν $F(s)$ y-λείος.

Αλγόριθμος του δευτεροβάθμιου κόσκινου

Ο χρόνος εκτέλεσης εξαρτάται από την επιλογή των y και z. Επιλέγοντας $z = \exp\{(\log n)^{1/2+o(1)}\}$ και $y = \exp\{(1/8 \log n \log\log n)^{1/2}\}$, αποδεικνύεται ότι ο χρόνος εκτέλεσης είναι $\exp\{(1 + o(1))(\log n \log\log n)^{1/2}\}$.

Συνεχή κλάσματα

(Απλό) πεπερασμένο συνεχές κλάσμα ονομάζεται κάθε έκφραση της μορφής

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots + \cfrac{1}{a_{n-1} + \cfrac{1}{a_n}}}}}$$

όπου $a_0 \in \mathbb{N}$ και $a_1, a_2, \ldots, a_n \in \mathbb{N}^*$.
Το παραπάνω συνεχές κλάσμα συμβολίζεται με

$$[a_0; a_1, a_2, \ldots, a_n]$$

Επαγωγικά προκύπτει ότι κάθε πεπερασμένο συνεχές κλάσμα αντιστοιχεί σε κάποιον θετικό ρητό αριθμό, ο οποίος μπορεί να αναπαρασταθεί με την προηγούμενη μορφή.

Συνεχή κλάσματα

Αντίστροφα, κάθε θετικός ρητός αριθμός $\rho = a/b$, όπου $a, b \in \mathbb{N}^*$ και μκδ$(a, b) = 1$, έχει αναπαράσταση ως συνεχές κλάσμα, η οποία προκύπτει χρησιμοποιώντας τον αλγόριθμο του Ευκλείδη:

$$r_{k-1} = q_k r_k + r_{k+1}, \qquad 0 \le r_{k+1} < r_k, k \in [n], \qquad (*)$$

όπου $r_0 = a, r_1 = b, r_n = 1, r_{n+1} = 0$. Διαιρώντας κατά μέλη με r_k, προκύπτει

$$\frac{r_{k-1}}{r_k} = q_k + \frac{1}{r_k/r_{k+1}}, k \in [n-1], \quad \frac{r_{n-1}}{r_n} = q_n,$$

επομένως, $\rho = r_0/r_1 = q_1 + \dfrac{1}{r_1/r_2} = \cdots = [q_1; q_2, \ldots, q_n]$.

Σημειώνεται ότι η ίδια ακολουθία πηλίκων (q_k) προκύπτει και στην περίπτωση που μκδ$(a, b) > 1$. Ως γνωστό, η ακολουθία αυτή έχει μήκος $n \le 1 + \log b/\log\phi$ (όταν $a > b$) και υπολογίζεται σε χρόνο $O(\mathrm{len}(a)\,\mathrm{len}(b))$.

Καθώς $q_n > 1$, είναι και $\rho = [q_1; q_2, \ldots, q_n - 1, 1]$.

Εύκολα προκύπτει ότι η αναπαράσταση του ρ με $q_n > 1$ είναι μοναδική.

Οι ρητοί $\dfrac{P_k}{Q_k} = [a_0; a_1, \ldots, a_k]$, $0 \le k \le n$ ονομάζονται **συγκλίνοντες ρητοί** στο $\rho = [a_0; a_1, \ldots, a_n]$.

Λήμμα

Για τους συγκλίνοντες ρητούς P_k/Q_k στον ρητό $\rho = [a_0; a_1, \ldots, a_n]$ ισχύουν οι σχέσεις:

$$\mu\kappa\delta(P_k, Q_k) = 1, \qquad 0 \le k \le n.$$

$$P_0 = a_0, \quad P_1 = a_0 a_1 + 1, \quad Q_0 = 1, \quad Q_1 = a_1.$$

$$P_k = a_k P_{k-1} + P_{k-2}, \qquad Q_k = a_k Q_{k-1} + Q_{k-2}, \qquad 2 \le k \le n.$$

$$P_k Q_{k+1} - Q_k P_{k+1} = (-1)^{k+1}, \qquad 0 \le k < n.$$

$$P_k Q_{k+2} - Q_k P_{k+2} = (-1)^{k+1} a_{k+2}, \qquad 0 \le k < n-1.$$

Απόδειξη.

Με επαγωγή. □

Άπειρα συνεχή κλάσματα

Αν $(a_n)_{n\in\mathbb{N}}$ μια ακολουθία ακεραίων, $a_0 > 0$, $a_i \geq 0$, $i \in [n]$, τότε ορίζουμε τα συνεχή κλάσματα $P_k/Q_k = [a_0; a_1, \ldots, a_k]$, $k \in \mathbb{N}$. Προφανώς, οι P_k, Q_k είναι ακέραιοι πρώτοι μεταξύ τους και τα κλάσματα P_k/Q_k, $k \leq n$, είναι οι συγκλίνοντες ρητοί στον P_n/Q_n. Από το προηγούμενο Λήμμα προκύπτει ότι η ακολουθία $(Q_k Q_{k-1})_{k\in\mathbb{N}^*}$ είναι θετική, αύξουσα και τείνει στο $+\infty$, και ότι

$$\frac{P_k}{Q_k} - \frac{P_{k+1}}{Q_{k+1}} = \frac{(-1)^{k+1}}{Q_k Q_{k+1}},$$

οπότε

$$\frac{P_k}{Q_k} = a_0 + \sum_{i=1}^{k} \frac{(-1)^{i+1}}{Q_i Q_{i-1}},$$

Το όριο του δεύτερου μέλους, όταν $k \to \infty$, είναι μια εναλλάσσουσα σειρά, η οποία συγκλίνει, σύμφωνα με το κριτήριο Leibniz, έστω στον $x \in \mathbb{R}$. Έτσι λοιπόν, ορίζουμε το **άπειρο συνεχές κλάσμα** $x = [a_0; a_1, a_2, \ldots]$ και τα κλάσματα P_k/Q_k είναι οι συγκλίνοντες ρητοί στο x.

Παραγοντοποίηση με συνεχή κλάσματα

Η προσέγγιση αυτή, διατυπώθηκε αρχικά από τους Lehmer και Powers (1931) και τροποποιεί τον αλγόριθμο του Dixon, χρησιμοποιώντας τους αριθμητές των συνεχών κλασμάτων P_k/Q_k που προσεγγίζουν τον άρρητο $\sqrt{n}$, για τον προσδιορισμό των y-λείων τετραγώνων a_i. Συγκεκριμένα, βασίζεται στην ακόλουθη πρόταση:

Πρόταση

Αν $n \in \mathbb{N}^*$ ελεύθερος τετραγώνου, P_k/Q_k, $k \in \mathbb{N}$, οι συγκλίνοντες ρητοί στον $\sqrt{n}$ και $W_k = P_k^2 - nQ_k^2$, τότε $|W_k| < 2\sqrt{n}$.
Επιπλέον, για κάθε πρώτο διαιρέτη p του W_k είναι $(n/p) = 1$.

Κατόπιν τούτων, επιλέγουμε τους t_i μεταξύ των P_k. Θα είναι $a_i \equiv P_k^2 \equiv P_k^2 - nQ_k^2 \equiv W_k \pmod N$ και ο W_k θα είναι ο αντιπρόσωπος $\mathrm{mod} n$ του a_i, αφού $|W_k| < 2\sqrt{n}$.
Επιπλέον, θα διαιρείται μόνο από πρώτους p με $(n/p) = 1$. Ως εκ τούτου, αντί του συνόλου B, χρησιμοποιείται το $B' = \{p \in \mathbb{P} : p \leq y, (n/p) = 1\}$.

Απόδειξη.

Η ανισότητα $|W_k| < 2\sqrt{n}$ προκύπτει βάσει του Λήμματος της σελ.121.
Για το δεύτερο σκέλος, έστω p πρώτος με $p|W_k$. Αν $p|Q_k$, τότε $p|P_k$, δηλαδή μκδ$(P_k, Q_k) > 1$, άτοπο. Άρα $p \nmid Q_k$, δηλαδή ο Q_k έχει πολλαπλασιαστικό αντίστροφο, οπότε
$P_k^2 - nQ_k^2 \equiv 0 \pmod{p} \Rightarrow n \equiv (P_k Q_k^{-1})^2 \pmod{p}$, δηλαδή $(n/p) = 1$. □

Η επιτυχία της μεθόδου συνίσταται στο ότι υπάρχουν αρκετοί διαφορετικοί αριθμοί W_k, το πλήθος των οποίων ισούται με την περίοδο του συνεχούς κλάσματος του $\sqrt{n}$.
Αν η περίοδος είναι μικρή, τότε μπορεί να χρησιμοποιηθεί το συνεχές κλάσμα του $\sqrt{an}$, όπου a μικρός θετικός ακέραιος, αρκεί να έχει μεγάλη περίοδο. Τότε τίθεται $W_k = P_k^2 - anQ_k^2$ και οι ισοτιμίες είναι και πάλι $\mod n$.

Αλγόριθμος $p-1$ του Pollard

Ο αλγόριθμος αυτός είναι αποτελεσματικός όταν ο n έχει πρώτο παράγοντα p, τέτοιον ώστε ο $p-1$ να είναι γινόμενο μικρών πρώτων. Ο αλγόριθμος υποθέτει ότι για τον μικρότερο πρώτο παράγοντα p του n ο $p-1$ είναι y-λείος για κάποιο y και κατασκευάζει έναν αριθμό L που είναι επίσης y-λείος και τέτοιον ώστε $p-1|L$. Ένας τέτοιος αριθμός είναι ο

$$L = \prod_{q \in \mathbb{P}, q \leq y} q^{\lfloor \log_q n \rfloor}.$$

Πράγματι, είναι

$$\begin{aligned} n \geq p > p-1 \geq q^{\nu_q(p-1)} &\Rightarrow \log_q n > \nu_q(p-1) \\ &\Rightarrow \nu_q(L) = \lfloor \log_q n \rfloor \geq \nu_q(p-1), \end{aligned}$$

για κάθε πρώτο $q \leq y$.

Αλγόριθμος $p-1$ του Pollard

Αν τώρα $[a]_p \in \mathbb{Z}_p^*$, τότε $p-1|L \Rightarrow a^L \equiv 1 \pmod{p}$. Επομένως $d = \text{μκδ}(a^L - 1, n) > 1$. Αν επιπλέον ισχύει ότι $a^L \not\equiv 1 \pmod{q}$, για κάποιον πρώτο παράγοντα q του n, τότε $d < n$, οπότε ο d είναι μη τετριμμένος παράγοντας του n.
Αν αντίθετα είναι $a^L \equiv 1 \pmod{q}$, τότε

- Αν $q-1 \mid L$ για κάθε πρώτο $q|n$, θα πρέπει να επιλεχθεί μεγαλύτερο y.
- Αν $q-1 \nmid L$ για κάποιο πρώτο $q|n$, τότε μπορεί να επιλεχθεί διαφορετικό a.
  Αν $[a]_q$ είναι γεννήτορας του $\mathbb{Z}_q^*$, τότε θα είναι $a^L \not\equiv 1 \pmod{q}$, οπότε ο αλγόριθμος τερματίζει με επιτυχία. Η πιθανότητα επιλογής γεννήτορα είναι ως γνωστό ίση με $\phi(q-1)/(q-1)$.

Αλγόριθμος $p-1$ του Pollard

Συνοψίζοντας, ο αλγόριθμος έχει ως εξής:

1. Επιλέγουμε μικρό a (συνήθως $a = 2$) και y.
2. Υπολογίζουμε το L.
3. Υπολογίζουμε το $a^L \bmod n$.
4. Υπολογίζουμε το $d = \text{μκδ}(a^L - 1, n)$.
5. Αν $1 < d < n$, επιστρέφουμε το d, αλλιώς επιλέγουμε άλλο a ή μεγαλύτερο y.

Ο χρόνος εκτέλεσης του αλγορίθμου είναι $O(y \operatorname{len}(y)(\operatorname{len}^2(n) + y \operatorname{len}(y)))$. Πράγματι, το $L < y^y$ υπολογίζεται σε χρόνο $O(y^2 \operatorname{len}(y)^2)$, ο $a^L \bmod n$ υπολογίζεται σε χρόνο $O(y \operatorname{len}(y) \operatorname{len}^2(n))$ και ο d σε χρόνο $O(\operatorname{len}^2(n))$.

Αλγόριθμος $p-1$ του Pollard

Παρατήρηση

Υπάρχουν παραλλαγές του αλγορίθμου, στις οποίες τίθεται $L = y!$ ή $L = \text{εκπ}(2, 3, \ldots, y)$ ώστε να $p - 1 | L$ με μεγάλη πιθανότητα. Ο L υπολογίζεται επαναληπτικά και ο $d = \text{μκδ}(a^L - 1, n)$ μπορεί να υπολογιστεί μια μόνο φορά, όπως παραπάνω, ή σε κάθε επανάληψη, οπότε αν βρεθεί $1 < d < n$, ο αλγόριθμος τερματίζει.

Αλγόριθμος ρ του Pollard

Ο αλγόριθμος αυτός βρίσκει δύο ακεραίους x, y με $x \equiv y \mod p$, όπου p κάποιος (άγνωστος) πρώτος παράγοντας του n. Αν επιπλέον είναι $x \not\equiv y \mod n$, τότε $1 < d = \text{μκδ}(x - y, n) < n$, οπότε επιστρέφεται ο μη τετριμμένος παράγοντας d του n. Για το σκοπό αυτό χρησιμοποιείται ένα πολυώνυμο $f(x)$ με ακέραιους συντελεστές (συνήθως χρησιμοποιείται το $f(x) = x^2 + 1$) και μια ακολουθία ακεραίων (x_i), η οποία ορίζεται αναδρομικά ως

$$x_{i+1} = f(x_i), \qquad i \geq 0, \qquad x_0 \in \{1, 2, \ldots, n-1\}.$$

Υπολογίζονται οι όροι x_i και x_{2i} καθώς και ο

$$d = \text{μκδ}(x_i - x_{2i}, n),$$

για κάθε $i = 1, 2, \ldots$, μέχρις ότου $1 < d < n$, οπότε επιστρέφεται ο d. Αν δεν είναι δυνατό να βρεθεί τέτοιος δείκτης i, τότε δοκιμάζουμε άλλη τιμή x_0 ή άλλο πολυώνυμο f.

Αλγόριθμος ρ του Pollard

Σημειώνεται ότι ο $y_i = x_{2i}$ μπορεί να υπολογιστεί από τη σχέση

$$y_i = x_{2i} = f(x_{2i-1}) = f(f(x_{2i-2})) = f(f(y_{i-1})).$$

Είσοδος: Ο περιττός ακέραιος $n > 1$.
Έξοδος: Ο μη τετριμμένος παράγοντας d του n, ή αποτυχία.

$x \leftarrow x_0$;
$y \leftarrow x_0$;
$d \leftarrow 1$;
while $d = 1$ **do**
    $x \leftarrow f(x)$;
    $y \leftarrow f(f(y))$;
    $d \leftarrow \gcd(x - y, n)$;
end while
if $d < n$ **then return** d;
else return failure;

Αλγόριθμος 9: Αλγόριθμος ρ του Pollard.

Αλγόριθμος ρ του Pollard

Η ορθότητα του αλγορίθμου βασίζεται στην παρατήρηση ότι η ακολουθία (x_i) θα είναι από κάποιο σημείο και έπειτα περιοδική modulo p. Πράγματι, θα υπάρχουν ελάχιστοι δείκτες $i < j$ ώστε $x_i \equiv x_j \pmod{p}$, οπότε από τη γνωστή ιδιότητα

$$x \equiv y \pmod{p} \Rightarrow f(x) \equiv f(y) \pmod{p}$$

έπεται ότι $x_{i+m} \equiv x_{j+m} \pmod{p}$, για κάθε $m \geq 0$. Επομένως η περίοδός της θα είναι $T = j - i$, αφού
$x_{k+j-i} \equiv x_{k+i-i} \equiv x_k \pmod{p}$, για κάθε $k \geq i$.
Αν t είναι το ελάχιστο πολλαπλάσιο του T με $t \geq i$, τότε είναι $i \leq t < j$. Πράγματι, οι δείκτες $i, i+1, \ldots, i+T-1 = j-1$ είναι T σε πλήθος οπότε περιέχουν τουλάχιστον ένα πολλαπλάσιο του T. Επομένως, δεδομένου ότι $x_t \equiv x_{2t} \pmod{p}$, έπεται ότι ο αλγόριθμος θα κάνει το πολύ $t < j$ επαναλήψεις.

Αλγόριθμος ρ του Pollard

Αν θεωρήσουμε ότι η f είναι κατάλληλα επιλεγμένη ώστε να κατανέμει ομοιόμορφα τις τιμές της (modulo p) στο $\{0, 1, \ldots, p-1\}$, τότε η επόμενη πρόταση μπορεί να μας δώσει ένα φράγμα για το πλήθος επαναλήψεων του αλγορίθμου.

Πρόταση (Birthday bound)

Σε ένα σύνολο N αντικειμένων πρέπει να επιλεχθούν με επανατοποθέτηση τουλάχιστον $B = \frac{1+\sqrt{1+8N\ln 2}}{2}$ αντικείμενα, ώστε να έχουν επιλεχθεί τουλάχιστον δύο ίδια με πιθανότητα $\geq 1/2$.

Απόδειξη.

Το ενδεχόμενο A τα k επιλεγμένα αντικείμενα να είναι όλα διαφορετικά μεταξύ τους έχει πιθανότητα

$$P(A) = \frac{N(N-1)\cdots(N-k+1)}{N^k} = \left(1-\frac{1}{N}\right)\cdots\left(1-\frac{k-1}{N}\right)$$
$$\leq \exp\{\frac{-1}{N}\}\cdots\exp\{\frac{-(k-1)}{N}\} = \exp\{\frac{-k(k-1)}{2N}\},$$

βάσει της ανισότητας $1+x \leq e^x$, $x \in \mathbb{R}$. Επιπλέον,

$$\exp\{\frac{-k(k-1)}{2N}\} \leq 1/2 \Leftrightarrow \frac{k(k-1)}{2N} \geq \ln 2 \Leftrightarrow k^2 - k - 2N\ln 2 \geq 0$$
$$\Leftrightarrow k \geq \frac{1+\sqrt{1+8N\ln 2}}{2} = B.$$

Επομένως αν επιλεχθούν τουλάχιστον B αντικείμενα, θα έχουν επιλεχθεί δύο ίδια με πιθανότητα $1 - P(A) \geq 1/2$. □

Αλγόριθμος ρ του Pollard

Επομένως, θεωρώντας το φράγμα $B = \frac{1+\sqrt{1+8p\ln 2}}{2}$ της προηγούμενης πρότασης, η πιθανότητα να υπάρχουν δείκτες $i \leq t < 2t < j \leq B$ είναι τουλάχιστον $1/2$. Έτσι, αν $p \leq \sqrt{n}$, τότε $B = O(\sqrt{p}) = O(n^{1/4})$ και ο αλγόριθμος βρίσκει κατάλληλο δείκτη t σε χρόνο $O(n^{1/4}\,\mathrm{len}^2(n))$ με πιθανότητα τουλάχιστον $1/2$.

Διακριτός λογάριθμος

Έστω $G = \langle g \rangle$ μια κυκλική ομάδα τάξης $|G| = n \in \mathbb{N}^*$, όπου g ένας γεννήτορας αυτής. Τότε, κάθε $a \in G$ θα γράφεται στη μορφή $a = g^x$, για κάποιο $x \in \{0, 1, \ldots, n-1\}$.
Ο x καλείται διακριτός λογάριθμος του a και συμβολίζεται ως

$$x = \log_g a.$$

Στις εφαρμογές, η G είναι συνήθως μια υποομάδα της $\mathbb{Z}_p^*$, όπου p πρώτος, οπότε $n|p-1$.
Για την εύρεση του διακριτού λογαρίθμου x του a ως προς τη βάση g, δεν υπάρχουν γνωστοί αποδοτικοί (πολυωνυμικοί) αλγόριθμοι. Οι ταχύτεροι γνωστοί αλγόριθμοι είναι υποεκθετικού χρόνου.

Διακριτός λογάριθμος

Το πρωτόκολλο εδραίωσης κλειδιού Diffie-Hellman βασίζεται στη δυσκολία υπολογισμού του διακριτού λογαρίθμου και έχει ως εξής: Τα g, p και $n|p-1$ είναι γνωστά σε όλους. Οι Α και Β προκειμένου να επικοινωνήσουν επιλέγουν μυστικά ένα x και ένα y αντίστοιχα και υπολογίζουν τα $a = g^x$ και $b = g^y$, τα οποία και δημοσιοποιούν. Κατόπιν, υπολογίζουν το κοινό μυστικό κλειδί

$$k = a^y = g^{xy} = b^x$$

δηλαδή ο Α υψώνει το b στη δύναμη x και ο Β υψώνει το a στη δύναμη y. Έτσι έχουν υπολογίσει το ίδιο μυστικό κλειδί k.
Στη συνέχεια, οι Α και Β μπορούν να ανταλλάσσουν μηνύματα κρυπτογραφημένα με το μυστικό κλειδί k.
Ένας τρίτος, προκειμένου να ανακαλύψει το k, θα πρέπει να ανακαλύψει το $x = \log_g a$ ή το $y = \log_g b$, δεδομένων των a, b και g.
Σε τυπικές υλοποιήσεις, ο p έχει 1024 bits και ο n έχει 160 bits.

Αλγόριθμος βήμα βρέφους - βήμα γίγαντα

Ένας απλός αλγόριθμος (Shanks, 1969) για την εύρεση του $x = \log_g a$ έχει ως εξής:

- Αρχικά, ελέγχουμε αν $ag^{-r} = 1$ (δηλαδή αν $a = g^r$), για κάποιο $r \in \{0, 1, \ldots, m-1\}$, όπου $m = \lfloor \sqrt{n} \rfloor + 1$ (βήμα βρέφους). Ταυτόχρονα, αποθηκεύουμε τα ζεύγη (ag^{-r}, r) σε μια δομή B.
- Αν βρεθεί τέτοιο r, τότε $x = r$, αλλιώς θέτουμε $b = g^m$ και ελέγχουμε για κάθε $q \in \mathbb{N}^*$ (βήμα γίγαντα) αν $(b^q \in B)$ (δηλαδή αν $a = b^q g^r$), για κάποιο $r < m$.
- Όταν βρεθεί τέτοιο q, τότε προφανώς θα είναι $x = mq + r$ ο ελάχιστος θετικός ακέραιος με $a = g^x$.

Ο χρόνος εκτέλεσης του προηγούμενου αλγορίθμου εξαρτάται από τον χρόνο εκτέλεσης των πράξεων στην ομάδα G και αναζήτησης στη δομή B.
Αν G υποομάδα της $\mathbb{Z}_p^*$, τότε το B κατασκευάζεται σε χρόνο $O(\sqrt{n}\,\mathrm{len}^2(p))$, η αναζήτηση μπορεί να γίνει σε χρόνο $O(\mathrm{len}(p))$ και ο συνολικός χρόνος εκτέλεσης είναι $O(\sqrt{n}\,\mathrm{len}^2(p))$.

Αλγόριθμος βήμα βρέφους - βήμα γίγαντα

Είσοδος: Ο γεννήτορας g της G, η τάξη n και ένα $a \in G$.
Έξοδος: Ο $x = \log_g a$.

$m \leftarrow \lfloor \sqrt{n} \rfloor + 1$;
$B = \emptyset$;
for $r = 0$ **to** $m - 1$ **do**
  $B \leftarrow B \cup \{(ag^{-r}, r)\}$;
  if $ag^{-r} = 1$ **then return** r;
end for
$(d, q, r) \leftarrow (g^m, 1, \mathrm{inB}(d))$;
while $r = -1$ **do**
  $(b, q) \leftarrow (db, q + 1)$;
  $r \leftarrow \mathrm{inB}(b)$;
end while
return $qm + r$;

Αλγόριθμος 10: Αλγόριθμος βήμα βρέφους - βήμα γίγαντα.

Η συνάρτηση $\mathrm{inB}(d)$ επιστρέφει το r, τέτοιο ώστε $(d, r) \in B$, ή -1 αν δεν υπάρχει τέτοιο r.

Αλγόριθμος ρ του Pollard

Ο αλγόριθμος αυτός (Pollard, 1978) κατασκευάζει μια τελικά περιοδική ακολουθία (x_i). Συγκεκριμένα, η G διαμερίζεται σε τρία σύνολα S_1, S_2, S_3, με $1 \notin S_2$, και ορίζεται η συνάρτηση

$$f(x,r,s) = \begin{cases} (ax, r, (s+1) \bmod n), & x \in S_1 \\ (x^2, 2r \bmod n, 2s \bmod n), & x \in S_2 \\ (gx, (r+1) \bmod n, s), & x \in S_3 \end{cases}$$

και η ακολουθία $(x_i, r_i, s_i)_{i \in \mathbb{N}}$, με

$$(x_{i+1}, r_{i+1}, s_{i+1}) = f(x_i, r_i, s_i), \qquad (x_0, r_0, s_0) = (1, 0, 0)$$

Κάθε τριάδα (x_i, r_i, s_i) προφανώς ικανοποιεί τη σχέση $x_i = g^{r_i} a^{s_i}$. Αν $x_i = x_{2i}$ και $a = g^x$, τότε $g^{r_i} g^{x s_i} = g^{r_{2i}} g^{x s_{2i}}$, δηλαδή

$$(s_{2i} - s_i)x \equiv (r_i - r_{2i}) \pmod{n}$$

Αλγόριθμος ρ του Pollard

Είσοδος: Οι $a, g \in G$ και $n = |G|$.
Έξοδος: Ο $x = \log_g a$.
$(x, r, s) \leftarrow (1, 0, 0)$;
$(y, r', s') \leftarrow (1, 0, 0)$;
while true **do**
    $(x, r, s) \leftarrow f(x, r, s)$;
    $(y, r', s') \leftarrow f(f(y, r', s'))$;
    if $x = y$ **then**
        Λύσε την ισοτιμία $(s' - s)x \equiv (r - r') \pmod{n}$;
        return x;
    end if
end while

Αλγόριθμος 11: Αλγόριθμος ρ του Pollard.

Αλγόριθμος ρ του Pollard

Επειδή η G είναι πεπερασμένη, υπάρχουν οι ελάχιστοι ακέραιοι j, T με $x_j = x_{j+T}$, οπότε η $(x_j, x_{j+1}, \ldots)$ είναι περιοδική με περίοδο T, δηλαδή υπάρχει i, με $j < i \leq j + T$ τέτοιο ώστε $x_i = x_{2i}$, για παράδειγμα το $i = T(1 + \lfloor j/T \rfloor)$. Επομένως, ο αλγόριθμος τερματίζει.
Αν η f κατανέμει ομοιόμορφα τα x_i στο G (με κατάλληλη επιλογή των S_1, S_2, S_3), τότε ο αλγόριθμος τερματίζει μετά από $O(\sqrt{n})$ επαναλήψεις με πιθανότητα μεγαλύτερη του $1/2$.

Αναγωγή από την τάξη q^e στην τάξη q

Ας υποτεθεί ότι το στοιχείο $\gamma \in \mathbb{Z}_p^*$ παράγει μια υποομάδα G της $\mathbb{Z}_p^*$ τάξης q^e, $e > 1$. Προκειμένου να υπολογίσουμε τον $x = \log_\gamma \alpha$, $\alpha \in G$, $0 \leq x \leq q^e$, εργαζόμαστε ως εξής:

- Επιλέγουμε ακέραιο f, με $0 < f < e$, οπότε $x = q^f v + u$, για κάποια v, u, με $0 \leq u < q^f$, $0 \leq v < q^{e-f}$.
- Θέτουμε $\alpha' = a^{q^{e-f}}$ και $\gamma' = \gamma^{q^{e-f}}$. Το γ' έχει τάξη q^f, άρα είναι $\alpha' = \gamma^{xq^{e-f}} = (\gamma')^{q^f v+u} = (\gamma')^u$, επομένως $u = \log_{\gamma'} \alpha'$.
- Ομοίως, θέτοντας $\alpha'' = \alpha\gamma^{-u}$ και $\gamma'' = \gamma^{q^f}$, το γ'' έχει τάξη q^{e-f}, άρα είναι $\alpha'' = (\gamma'')^v$, επομένως $v = \log_{\gamma''} \alpha''$.
- Τελικά το πρόβλημα υπολογισμού του διακριτού λογαρίθμου ανάγεται στην περίπτωση όπου $e = 1$.

Ο χρόνος εκτέλεσης αυτής της αναγωγής εξαρτάται από την επιλογή του f. Αν επιλέγεται $f = \lfloor e/2 \rfloor$, τότε ο χρόνος εκτέλεσης, χωρίς τη βασική περίπτωση $e = 1$, είναι τάξης $O(e \operatorname{len}(e) \operatorname{len}(q) \operatorname{len}^2(p))$.

Αναγωγή από την τάξη q^e στην τάξη q

Κατόπιν τούτων, αν είναι γνωστή η παραγοντοποίηση της τάξης $|G| = n = q_1^{e_1} \cdots q_r^{e_r}$, τότε, προκειμένου να υπολογίσουμε το $x = \log_\gamma \alpha$, θέτουμε

$$\alpha_i = \alpha^{n/q_i^{e_i}}, \qquad \gamma_i = \gamma^{n/q_i^{e_i}}, \qquad i \in [r],$$

και έχουμε ότι $\alpha_i = \gamma_i^x$ και το γ_i έχει τάξη $q_i^{e_i}$.
Υπολογίζουμε με βάση τα προηγούμενα τους διακριτούς λογαρίθμους

$$x_i = \log_{\gamma_i} \alpha_i, \qquad 0 \le x_i < q_i^{e_i}, \qquad i \in [r].$$

Τέλος, το x υπολογίζεται άμεσα, βάσει του Κινέζικου Θεωρήματος, αφού είναι

$$x \equiv x_i \pmod{q_i^{e_i}}, \qquad i \in [r].$$