Παραγοντοποίηση

Καθηγητὴς Ν.Γ. Τζανάκης

12 Δεκεμβρίου 2007

Στὰ παρακάτω, m ὑποτίθεται ὅτι εἶναι ἕνας πολὺ μεγάλος ἀριθμὸς καὶ p ἕνας πρῶτος διαιρέτης του, τὸν ὁποῖο δὲν γνωρίζομε. Αὐτὸ ποὺ ἐπιδιώκομε εἶναι ἡ εὕρεση ἑνὸς μὴ τετριμμένου διαιρέτη τοῦ m, ὁ ὁποῖος διαιρεῖται ἀπὸ τὸν p.

Συμβολισμός: Ὅταν γιὰ κάποιο ἀκέραιο a γράφομε $[a]_m$, ἐννοοῦμε ἐκεῖνο τὸν μοναδικὸ $a_0 \in \{0, 1, \ldots, m-1\}$, τέτοιον ὥστε $a \equiv a_0 \pmod{m}$.
Ἂν G εἶναι ὁμάδα, $|G|$ συμβολίζει τὴν τάξη της.

Μία ἁπλῆ παρατήρηση εἶναι ἡ ἑξῆς: Ἂν $x \in \mathbb{Z}$, τότε $x \equiv 0 \pmod{p} \Leftrightarrow [x]_m \equiv 0 \pmod{p}$. Αὐτὸ θὰ τὸ χρησιμοποιηθεῖ ἀρκετὲς φορὲς παρακάτω, δίχως νὰ γίνει ἰδιαίτερη μνεία.

1 Γενικευμένη μέθοδος Pollard

Κατ' ἀρχάς, ἐπιλέγομε μιὰ κατηγορία ὁμάδων $\{G_q : q \text{ διατρέχει τοὺς πρώτους}\}$. Εἰδικώτερα, γιὰ τοὺς πρώτους p, ποὺ διαιροῦν τὸν m, καὶ οἱ ὁποῖοι ἀρχικῶς μᾶς εἶναι ἄγνωστοι, γνωρίζομε μὲν τὸν τῦπο τῆς ὁμάδας G_p, ἄρα καὶ κάποιες σημαντικὲς ἰδιότητές της, ἀλλὰ ὄχι τὴν ἴδια τὴν ὁμάδα. Γιὰ παράδειγμα, μπορεῖ νὰ ξέρομε ὅτι $G_p = \mathbb{F}_p^*$, δίχως ὅμως νὰ ξέρομε τὸν p. Παρ' ὅλ' αὐτά, πολλὲς ἰδιότητες τῆς $\mathbb{F}_p^*$, γιὰ γενικὸ p, μᾶς εἶναι γνωστές.
Ἂν γιὰ ἕνα τουλάχιστον πρῶτο διαιρέτη p τοῦ m ὁ ἀριθμὸς $|G_p|$ ἔχει κάποια "καλὴ ἰδιότητα" (βλ. ἀμέσως παρακάτω), τότε ὁ μέγιστος κοινὸς διαιρέτης τοῦ m καὶ ἑνὸς ἀριθμοῦ, ποὺ ὑπολογίζεται μέσῳ τῆς $|G_p|$ εἶναι μεγαλύτερος τοῦ 1. Ἂν, δὲν εἶναι ἴσος μὲ τὸν m, τότε πετύχαμε ἕνα μὴ τετριμμένο διαιρέτη τοῦ m.

Γενικὴ Ἀρχή 1.1. *Ἔστω G_p πεπερασμένη ὁμάδα, $g_0 \in G_p$ καὶ συνάρτηση $f : G_p \times \mathbb{N} \to \mathbb{N}_0$, ἔτσι ὥστε νὰ ἱκανοποιοῦνται οἱ ἑξῆς ἰδιότητες:*

1. *$f(g_0, |G_p|) \equiv 0 \pmod{p}$ γιὰ κάθε πρῶτο διαιρέτη p τοῦ m.*

2. *Ἂν γιὰ κάποιο* $a \in \mathbb{N}$ *ἱκανοποιεῖται ἡ* $f(g_0, a) \equiv 0 \pmod{p}$*, τότε, γιὰ κάθε μὴ μηδενικὸ πολλαπλάσιο* b *τοῦ* a*,* $f(g_0, b) \equiv 0 \pmod{p}$*.*

Ἔστω πεπερασμένο $S \subset \mathbb{N}$,[1] *καὶ τὸ* S *περιέχει ἕνα τουλάχιστον πολλαπλάσιο τοῦ ἀκεραίου* $|G_p|$*.* [2] *Τότε, καθὼς τὸ* s *διατρέχει τὶς τιμὲς τοῦ* S*, ὁ* $\gcd(f(g_0, s), m)$ *παίρνει, μία τουλάχιστον φορά, τιμὴ μεγαλύτερη τοῦ 1.*

Πράγματι, ἂν $k \in S$ καὶ ὁ k εἶναι πολλαπλάσιο τοῦ $|G_p|$, τότε, ἕνας προφανὴς συνδυασμὸς τῶν (1) καὶ (2) δείχνει ὅτι $f(g_0, k) \equiv 0 \pmod{p}$. Ἄρα, $p | \gcd(f(g_0, k), m)$, ποὺ σημαίνει ὅτι ὁ $\gcd(f(g_0, k), m)$ εἶναι διαιρέτης τοῦ m μεγαλύτερος τοῦ 1. Ἂν δὲν εἶναι ἴσος μὲ m, τότε εἶναι ἕνας μὴ τετριμμένος διαιρέτης τοῦ m.

1.1 Κλασικὴ μέθοδος τοῦ Pollard

Στὴ Γενικὴ Ἀρχὴ 1.1, κάνομε τὶς ἑξῆς συγκεκριμένες ἐπιλογές: $G_p = \mathbb{Z}_p^*$, $g_0 = A \bmod m$ μὲ A ὁποιονδήποτε θετικὸ ἀκέραιο πρῶτο πρὸς τὸν m. Σημειῶστε ὅτι, ἂν πάρομε στὴν τύχη ἕνα A καί, ὑπολογίζοντας τὸν $\gcd(A, m)$, τὸν βροῦμε > 1, τότε, ἄλλο ποὺ δὲν θέλαμε! Πετύχαμε ἄκοπα μὴ τετριμμένο διαιρέτη τοῦ m! Ἐπιλέγομε τώρα τὴ συνάρτηση f ὡς ἑξῆς:

$$\mathbb{Z}_p^* \times \mathbb{N} \ni ([x]_p, y) \xrightarrow{f} [x^y - 1]_m \in \mathbb{N}_0 \ .$$

Ἡ ἰδιότητα (1) τῆς Γενικῆς Ἀρχῆς 1.1 ἱκανοποιεῖται. Πράγματι, πρῶτον $|G_p| = |\mathbb{Z}_p^*| = p - 1$· δεύτερον, $\gcd(A, m) = 1$, ἄρα καὶ $\gcd(A, p) = 1$, ὁπότε $A^{p-1} - 1 \equiv 0 \pmod{p}$. Ἐπειδὴ $p | m$, ἡ τελευταία ἰσοδυναμία συνεπάγεται ὅτι $[A^{p-1} - 1]_m \equiv 0 \pmod{p}$, δηλαδή, $f([A]_p, |\mathbb{Z}_p^*|) \equiv 0 \pmod{p}$.
Ἡ ἰδιότητα (2) τῆς Γενικῆς Ἀρχῆς 1.1 ἱκανοποιεῖται, ἐπίσης. Διότι, ἂν γιὰ κάποιο φυσικὸ ἀριθμὸ a, $f([A]_p, a) \equiv 0 \pmod{p}$, τότε $[A^a - 1]_m \equiv 0 \pmod{p}$, ἄρα $A^a - 1 \equiv 0 \pmod{p}$. Συνεπῶς, ἂν b εἶναι μὴ μηδενικὸ πολλαπλάσιο τοῦ a, ἔστω $b = ac$, $c \in \mathbb{N}$, τότε $A^b - 1 = (A^a)^c - 1 =$ πολλαπλάσιο τοῦ $A^a - 1$, ἄρα $A^b - 1 \equiv 0 \pmod{p}$, καὶ αὐτὸ συνεπάγεται ὅτι $f([A]_p, b) = [A^b - 1]_m \equiv 0 \pmod{p}$.

Ἐπιλέγομε τώρα $S = \{2^n p_1^{n_1} p_2^{n_2} \cdots p_r^{n_r}\}$ μὲ $p_1, p_2, \ldots, p_r$ τοὺς r μικρότερους περιττοὺς πρώτους ἀριθμούς, δηλαδή, $p_1 = 3, p_2 = 5, p_3 = 7, \ldots$, π.χ. τοὺς πρώτους, ποὺ εἶναι μικρότεροι τοῦ 100 καὶ ἐκθέτες $n_1, \ldots, n_r$, ἂς ποῦμε, 0 ἢ 1, ἐνῶ $n = 0, 1, \ldots, 10$. Γενικά, ἂν ὅλοι οἱ πρῶτοι παράγοντες ἑνὸς

[1] Στὴν πράξη, ἐμεῖς κατασκευάζομε τὸ S καὶ πρέπει νὰ εἶναι τέτοιο ὥστε ὁ ὑπολογισμὸς τοῦ συνόλου $\{f(g_0, s) : s \in S\}$ νὰ μπορεῖ νὰ γίνει σὲ "λογικὸ χρόνο".

[2] Αὐτὴ εἶναι ἡ "καλὴ ἰδιότητα", στὴν ὁποίαν ἀναφερθήκαμε λίγο πρίν.

ἀκεραίου > 1 εἶναι μικρότεροι ἀπὸ ἕνα φρᾶγμα B καὶ οἱ ἐκθέτες τους εἶναι "πάρα πολὺ μικροί", τότε ὁ ἀκέραιος χαρακτηρίζεται B-λεῖος[3]. Μὲ αὐτὴ τὴν ὁρολογία, θὰ μπορούσαμε νὰ ποῦμε ὅτι τὸ S εἶναι τὸ σύνολο τῶν B-λείων ἀκεραίων, μὲ B, ἂς ποῦμε, 100.

Θὰ πετύχει ἡ μέθοδος Pollard νὰ ἀνακαλύψει μὴ τετριμμένο διαιρέτη τοῦ m, πολλαπλάσιο τοῦ p; "Μὲ μεγάλες πιθανότητες" ναί, ἂν ὁ p εἶναι τέτοιος ὥστε ὁ $p-1$ νὰ εἶναι B-λεῖος γιὰ τὸ συγκεκριμένο B, ποὺ ἐπιλέξαμε. Πράγματι, σ' αὐτὴ τὴν περίπτωση, καθὼς τὸ s θὰ διατρέχει τὸ σύνολο S τῶν B-λείων ἀκεραίων, θὰ πέσει σὲ κάποιο πολλαπλάσιο τοῦ $p-1$, ἔστω k. Τότε, σύμφωνα μὲ τὸ σχόλιο, ποὺ ἀκολούθησε ἀμέσως μετὰ τὴ Γενικὴ Ἀρχὴ 1.1, ὁ $\gcd(f([A]_p, k), m)$ εἶναι, μὲ μεγάλες πιθανότητες, μὴ τετριμμένος διαιρέτης τοῦ m. Παρατηρῆστε ὅτι $\gcd(f([A]_p, k), m) = \gcd([A^k - 1]_m, m) = \gcd(A^k - 1, m)$.

Μιὰ ἁπλοποίηση: Ἀντὶ τὸ s νὰ διατρέχει τὸ S ἀρκεῖ νὰ πάρει μόνο τὴν τιμὴ $2^N p_1^{N_1} \cdots p_r^{N_r}$, ὅπου οἱ $N, N_1, \ldots, N_r$ εἶναι οἱ μέγιστες τιμὲς τῶν $n, n_1, \ldots, n_r$ κατὰ τὴν κατασκευὴ τοῦ συνόλου S. Ἀντικαθιστοῦμε, δηλαδή, τὸ προηγούμενο S ἀπὸ τὸ μονοσύνολο $\{2^N p_1^{N_1} \cdots p_r^{N_r}\}$. Αὐτὸ διακαιολογεῖται ἀπὸ τὸ ὅτι, ἂν τὸ ἀρχικὸ S περιέχει ἕνα πολλαπλάσιο τοῦ $|G_p|$, τότε ὁ ἀριθμὸς $2^N p_1^{N_1} \cdots p_r^{N_r}$ εἶναι πολλαπλάσιο τοῦ $|G_p|$. Στὴν πράξη, ἐπειδὴ ἡ πιθανότητα νὰ διαιρεῖται ἕνας ἀριθμὸς ἀπὸ τὸ τετράγωνο ἑνὸς πρώτου εἶναι πολὺ μικρή (μὲ ἐξαίρεση τοὺς ἀρχικοὺς πολὺ μικροὺς πρώτους), μπορεῖ κανεὶς νὰ πάρει, γιὰ παράδειγμα, $N = 10$, $N_1 = 3$, $N_2 = \ldots = N_5 = 2$ καὶ $N_i = 1$ γιὰ $i > 5$.

1.1.1 Παράδειγμα τῆς κλασικῆς Pollard μὲ τὸ MAPLE

[3] B-smooth

```
> restart;
> with(numtheory):
```

```
Warning, the protected name order has been redefined and unprotected
```

The procedure below computes a^N modulo m

```
> dyn:=proc(a,N,m) local delta,x,E;
> delta:=1; x:=a; E:=N;
> while E > 0 do
> if E mod 2 =1 then delta:=(delta*x) mod m; E:=(E-1)/2
;
> else E:=E/2;
> fi;
> x:=x^2 mod m;
> od;
> delta;
> end:
> B:=[]:    # set of small primes
> for i from 2 to 20 do B:=[op(B),ithprime(i)] od:
B;
```

$$[3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71]$$

```
> m:=13425105781;
```

$$m := 13425105781$$

```
> g:=30; gcd(30,m);
```

$$g := 30$$

$$1$$

```
> s:=2^8:  for i from 1 to 10 do s:=s*B[i] od:  s;
```

$$25671742736640$$

```
> d:=gcd(dyn(2,s,m)-1,m);
> if d>1 then
> print(‘d is a non-trivial divisor of m; another one
is‘);
> d1:=m/d fi;
```

$$d := 104729$$

$$d\ is\ a\ non-trivial\ divisor\ of\ m;\ another\ one\ is$$

$$d1 := 128189$$

```
> ifactor(d-1);
```

$$(2)^3\ (13)\ (19)\ (53)$$

This shows that d-1 is B-smooth, which explains why Pollard's method worked in this example

```
> ifactor(d1-1);
```

$$(2)^2 \ (73) \ (439)$$

This shows that d1-1 is not B-smooth, but never mind!

1.2 Ἀναγωγὴ ἐλλειπτικῆς καμπύλης $\mathrm{mod}\, p$

Πρὶν προχωρήσομε στὴν ἑπόμενη μέθοδο, ἡ ὁποία ἀποτελεῖ μία ἄλλη ἐξειδίκευση τῆς Γενικῆς Ἀρχῆς 1.1, ἀναφέρομε κάποια πράγματα σχετικὰ μὲ τὴν ἀναγωγὴ μιᾶς ἐλλειπτικῆς καμπύλης modulo ἕνα πρῶτο $p > 3$. Πρὸς τὸ παρόν, ξεχνᾶμε τὸν m καὶ τὸ ὅτι ὁ πρῶτος p εἶναι διαιρέτης τοῦ m. Ἔστω ἡ ἐλλειπτικὴ καμπύλη μὲ ἐξίσωση $E\ :\ y^2 = x^3 + Ax + B\ \ A, B \in \mathbb{Q}$. Ἡ προβολικὴ ἐξίσωση τῆς E εἶναι $Y^2Z = X^3 + AXZ^2 + BZ^3$ καὶ κάθε σημεῖο $(x, y) \neq \mathcal{O}$ μὲ ρητὲς συντεταγμένες, ἂν τὸ δοῦμε ὡς προβολικὸ σημεῖο, μπορεῖ νὰ πάρει τὴ μορφὴ $[X, Y, Z]$, ὅπου οἱ X, Y, Z εἶναι ἀκέραιο πρῶτοι μεταξύ τους. Π.χ. ἂν ἕνα σημεῖο τῆς καμπύλης ἦταν τὸ $(\frac{5}{36}, \frac{35}{216})$, τότε αὐτό, προβολικά, ἰσοῦται μὲ

$$\left[\frac{5}{36}, \frac{35}{216}, 1\right] = [30, 35, 216]$$

καὶ $\gcd(30, 35, 216) = 1$.

Ἂν ὁ πρῶτος p εἶναι τέτοιος, ποὺ νὰ μὴ διαιρεῖ τὴ διακρίνουσα $-4A^3 - 27B^2$ τῆς E, τότε καὶ ἡ καμπύλη $\tilde{E}\ :\ Y^2Z = X^3 + \tilde{A}XZ^2 + \tilde{B}Z^3$, μὲ συντελεστὲς ἀπὸ τὸ σῶμα $\mathbb{F}_p$, ἡ λεγόμενη *ἀναγωγὴ τῆς* $E\ \mathrm{mod} p$, εἶναι ἐλλειπτικὴ καμπύλη, τῆς ὁποίας τὸ σύνολο τῶν σημείων $\tilde{E}(\mathbb{F}_p)$ γίνεται πεπερασμένη ὁμάδα, ἂν ἐφοδιασθεῖ μὲ τὴν πράξη, ποὺ ὁρίζεται ἀπὸ τοὺς ἴδιους τύπους μὲ ἐκείνους στὴν περίπτωση τῆς $E(\mathbb{Q})$, ἀλλά, στοὺς ὁποίους, οἱ ἀριθμητικὲς πράξεις γίνονται $\mathrm{mod} p$.

Ἔστω $P \in E(\mathbb{Q})$, $P \neq \mathcal{O}$, τὸ ὁποῖο γράφομε μὲ προβολικὲς συντεταγμένες $P = [a, b, c]$ καὶ $\gcd(a, b, c) = 1$. Θέτομε $\tilde{P} = [[a]_p, [b]_p, [c]_p]$. Προφανῶς, $\tilde{P} \in \tilde{E}(\mathbb{F}_p)$. Θέτομε, ἐπίσης, $\tilde{\mathcal{O}} = [[0]_p, [1]_p, [0]_p]$. Ἀποδεικνύεται ὅτι ἡ ἀπεικόνιση

$$E(\mathbb{Q}) \ni P \longrightarrow \tilde{P} \in \tilde{E}(\mathbb{F}_p)$$

εἶναι *ἐπιμορφισμὸς ὁμάδων*. Αὐτὸ παίζει πολὺ σημαντικὸ ρόλο στὴ μέθοδο παραγοντοποίησης μέσῳ ἐλλειπτικῶν καμπύλων, ποὺ θὰ δοῦμε ἀμέσως παρακάτω.

Συμβολισμός: Εἶναι εὔκολο ν' ἀποδειχθεῖ ὅτι κάθε σημεῖο $P = (x, y) \in E(\mathbb{Q})$, διάφορο τοῦ $\mathcal{O}$, ἔχει τὴ μορφὴ $P = (x, y) = (\frac{u}{v^2}, \frac{w}{v^3})$ μὲ u, v, w ἀκεραίους, $v > 0$ καὶ $\gcd(u, v) = 1 = \gcd(w, v)$. Στὰ παρακάτω θὰ λέμε τὸ v *παρονομαστὴ τοῦ* P καὶ θὰ τὸ συμβολίζομε $\mathrm{q}(P)$. Ἀφοῦ $\tilde{P} = [[uv]_p, [w]_p, [v^3]_p]$, εἶναι φανερὸ ὅτι,

$$\tilde{P} = \tilde{\mathcal{O}} \Leftrightarrow P = \mathcal{O} \ \text{ εἴτε } \ \mathrm{q}(P) \equiv 0 \pmod{p}\,. \tag{1}$$

1.3 Μέθοδος ECM τῆς Ἐλλειπτικῆς καμπύλης

Πρῶτα' ἀπ' ὅλα ἐπιλέγομε μία ἐλλειπτικὴ καμπύλη $E : y^2 = x^3 + Ax + B$, ἡ ὁποία νὰ ἔχει ἕνα σημεῖο $P \in E(\mathbb{Q})$ ἄπειρης τάξεως, τῆς ὁποίας ἡ διακρίνουσα $D = -4A^3 - 27B^2$ εἶναι πρώτη πρὸς τὸν m. Παρατηρῆστε ὅτι αὐτοὶ δὲν εἶναι δύσκολοι περιορισμοί, διότι οἱ ἀκέραιοι A, B ἐπιλέγονται αὐθαίρετα, μὲ ὅποιον τρόπο θέλομε. Λόγῳ τῆς συνθήκης $\gcd(D, m) = 1$, ἡ ἀναγωγὴ τῆς καμπύλης $\bmod p$, δηλαδή, ἡ καμπύλη $\tilde{E} : y^2 = x^3 + \tilde{A}x + \tilde{B}$, εἶναι, ἐπίσης, ἐλλειπτική.

Τώρα, στὴ Γενικὴ Ἀρχὴ 1.1 κάνομε τὶς ἑξῆς ἐπιλογές: $G_p = \tilde{E}(\mathbb{F}_p)$, $g_0 = \tilde{P}$ καὶ γιὰ $Q \in E(\mathbb{Q})$, καὶ $a \in \mathbb{N}$ ὁρίζομε

$$f(\tilde{Q}, a) = \begin{cases} 0 & \text{ἂν } \widetilde{aQ} = \tilde{\mathcal{O}} \\ [\mathrm{q}(aQ)]_m & \text{διαφορετικά} \end{cases}$$

Κατ' ἀρχάς, παρατηροῦμε ὅτι ἂν $f(\tilde{Q}, a) = 0$, τότε $\widetilde{aQ} = \tilde{\mathcal{O}}$, διότι, ἂν $[\mathrm{q}(aQ)]_m = 0$, τότε (ἀφοῦ $p|m$), $\mathrm{q}(aQ) \equiv [\mathrm{q}(aQ)]_m = 0 \pmod p$ καὶ τώρα, ἀπὸ τὴν (1) ἕπεται ὁ ἰσχυρισμός.

Ἡ ἰδιότητα (1) τῆς Γενικῆς Ἀρχῆς 1.1 ἱκανοποιεῖται. Πράγματι, Ἔστω $n = |\tilde{E}(\mathbb{F}_p)|$. Τότε, $n\tilde{P} = \tilde{O}$, ἄρα, λόγῳ ὁμομορφισμοῦ, $\widetilde{nP} = \tilde{O}$. Ἐπειδὴ τὸ P εἶναι στοιχεῖο ἄπειρης τάξεως στὴν ὁμάδα $E(\mathbb{Q})$, ἕπεται ὅτι $nP \neq \mathcal{O}$, ἄρα ἡ τελευταία ἰσότητα εἶναι δυνατὸν νὰ συμβαίνει μόνο ἂν $\mathrm{q}(nP) \equiv 0 \pmod p$. Ἐπειδὴ $p|m$, ἡ τελευταία ἰσοδυναμία συνεπάγεται τὴν $[\mathrm{q}(nP)]_m \equiv 0 \pmod p$, ἄρα $f(\tilde{P}, n) \equiv 0 \pmod p$. Ἡ ἰδιότητα (2) τῆς Γενικῆς Ἀρχῆς 1.1 ἱκανοποιεῖται ἐπίσης. Πράγματι, ἔστω ὅτι γιὰ κάποιον $a \in \mathbb{N}$ ἰσχύει $f(\tilde{P}, a) \equiv 0 \pmod p$ καὶ $b = ac$ εἶναι θετικὸ ἀκέραιο πολλαπλάσιο τοῦ a. Ἡ ὑποθεση συνεπάγεται ὅτι ὁ παρονομαστὴς τοῦ aP διαιρεῖται διὰ p, ἄρα $\widetilde{aP} = \tilde{O}$. Λόγῳ ὁμομορφισμοῦ, τότε, $a\tilde{P} = \tilde{O}$, ἄρα καὶ $ca\tilde{P} = \tilde{O}$, δηλαδή, $\tilde{O} = b\tilde{P} = \widetilde{bP}$ καί, ἐπειδὴ $bP \neq \mathcal{O}$, ἡ τελευταία ἰσότητα εἶναι δυνατὴ μόνο ἂν $\mathrm{q}(bP) \equiv 0 \pmod p$, δηλαδή, ἂν $f(\tilde{P}, b) \equiv 0 \pmod p$.

Ἡ ἐπιλογὴ τοῦ συνόλου S γίνεται ὅπως στὴν ἑνότητα 1.1. Ἡ παρατήρηση, ποὺ ἔγινε ἐκεῖ, γιὰ τὴν ἀναγωγὴ τοῦ συνόλου S σὲ μονοσύνολο, ἰσχύει καὶ ἐδῶ.

Πότε εἶναι δυνατὸν νὰ δουλέψει ἡ μέθοδος τῆς ἐλλειπτικῆς καμπύλης; Ἂν ὁ ἀκέραιος $|\tilde{E}(\mathbb{F}_p)|$ εἶναι B-λεῖος. Ποιὰ ἡ διαφορὰ καὶ τὸ πλεονέκτημα αὐτῆς ἐδῶ τῆς μεθόδου; Ὅτι, επιλέγοντας διαφορετικὰ A, B, παίρνομε μιὰ μεγάλη ποικιλία καμπύλων E, ἄρα μεγάλη ποικιλία ὁμάδων $\tilde{E}(\mathbb{F}_p)$ καί, μὲ μεγάλη πιθανότητα, κάποιας ἀπὸ αὐτὲς τὶς ὁμάδες $\tilde{E}(\mathbb{F}_p)$ ἡ τάξη θὰ εἶναι

B-λεῖος ἀριθμός. Ἀκριβέστερα, εἶναι γνωστὸ ὅτι

$$p+1-2\sqrt{p} \leq |\tilde{E}(\mathbb{F}_p)| \leq p+1+2\sqrt{p}$$

καί, καθὼς μεταβάλλεται ἡ καμπύλη E (δηλαδή, καθὼς μεταβάλλονται οἱ συντελεστὲς A, B), ἡ τάξη $|\tilde{E}(\mathbb{F}_p)|$ "καλύπτει πολὺ καλὰ" τὸ διάστημα $[p+1-2\sqrt{p}, p+1+2\sqrt{p}]$, ἄρα, σ' ἕνα τέτοιο μεγάλο διάστημα κάποια τιμὴ ἐλπίζει κανεὶς ὅτι θὰ εἶναι B-λεία. Ἂν καὶ δὲν ἔχει ἀποδειχθεῖ κάτι τέτοιο, ὅλες οἱ πειραματικὲς ἐνδείξεις συνηγοροῦν στὸ ὅτι ἔτσι ἔχουν τὰ πράγματα.

Σημαντικὸ σχόλιο. Στὸν ὁρισμὸ τῆς συνάρτησης $f(\tilde{Q}, a)$ βλέπομε ὅτι ἀπαιτεῖται ὁ ὑπολογισμὸς τοῦ ἀριθμοῦ $[\mathrm{q}(aQ)]_m$. Στὴν πράξη, εἶναι ἀνέφικτος ὁ ὑπολογισμὸς τοῦ aQ ἀκόμη καὶ γιὰ "μετρίου μεγέθους" a (π.χ. τῆς τάξεως τοῦ 10^5) καὶ γι' αὐτό, κάθε βῆμα τοῦ ἀλγορίθμου γιὰ τὸν ὑπολογισμὸ τοῦ aQ γίνεται $\bmod m$. Αὐτὸ εἶναι ἐντελῶς ἀνάλογο μὲ τὴν περίπτωση ὑπολογισμοῦ τοῦ $[x^a]_m$ γιὰ $x \in \mathbb{Z}$ καὶ a μεγάλο θετικὸ ἀκέραιο: Δὲν ὑπολογίζομε πρῶτα τὸν x^a καὶ μετὰ κάνομε τὴ διαίρεση διὰ m, ἀλλὰ σὲ κάθε βῆμα τοῦ ἀλγορίθμου ὕψωσης σὲ δύναμη οἱ πράξεις τοῦ πολλαπλασιασμοῦ γίνονται $\bmod m$. Ἐπανερχόμενοι στὴν ἐλλειπτικὴ καμπύλη, παρατηροῦμε ὅτι, γιὰ σύνθετο m, τὸ σύνολο τῶν $(x, y) \in \mathbb{Z}_m \times \mathbb{Z}_m$, ποὺ ἐπαληθεύουν τὴν $y^2 = x^3 + Ax + B$ δὲν ἀποτελεῖ ὁμάδα καὶ ἔτσι δὲν ὁρίζεται "πρόσθεση σημείων τῆς ἐλλειπτικῆς καμπύλης $\bmod m$". Παρ' ὅλ' αὐτά, μποροῦμε νὰ "ἐπεκτείνομε" τὸν ἀλγόριθμο πρόσθεσης σημείων τῆς ἐλλειπτικῆς καμπύλης σὲ ἕναν ἀλγόριθμο, ὁ ὁποῖος, ἢ θὰ ὑπολογίσει γρήγορα τὶς συντεταγμένες τοῦ $aQ \bmod m$, ἢ θὰ ἐπιστρέψει τὸ $\mathcal{O}$ (πού, ἁπλῶς, σημαίνει ὅτι $[\mathrm{q}(aQ)]_m = 0$), ἢ θὰ ἐπιστρέψει ἕνα μὴ τετριμμένο διαιρέτη τοῦ m. Περισσότερα γι' αὐτὸν τὸν ἀλγόριθμο καὶ μία ὑλοποίησή του μὲ παράδειγμα στὸ MAPLE, βλ. κεφάλαιο *Ἀλγόριθμος γιὰ τὸ ἄθροισμα* $\bmod m$ *σημείων ἐλλειπτικῆς καμπύλης*.

2 Ἡ μέθοδος ϱ τοῦ Pollard

Ἂς ὑποθέσομε ὅτι r εἶναι ἕνας μὴ τετριμμένος διαιρέτης ἑνὸς σύνθετου φυσικοῦ ἀριθμοῦ n. Ἔστω $f(x) \in \mathbb{Z}[x]$ ἕνα πολυώνυμο τουλάχιστον δευτέρου βαθμοῦ. Ἡ μέθοδος αὐτὴ στηρίζεται στὴν ὑπόθεση ὅτι, ἂν ἐπιλέξει κανεὶς τυχαῖο $x_0 \in \mathbb{Z}$ καὶ ὁρίσει ἀναδρομικὰ

$$x_{i+1} = [f(x_i)]_n \ , \tag{2}$$

ἡ προκύπτουσα συνάρτηση $\mathbb{Z}_r \to \mathbb{Z}_r$ μὲ τὴν ἰδιότητα $[x_0]_r \mapsto [x_1]_r$, $[x_1]_r \mapsto [x_2]_r$, $[x_2]_r \mapsto [x_3]_r \ldots$, ἔχει "τυχαία" συμπεριφορά, ἄρα εἶναι πολὺ πιθανὸ ὅτι ὕστερα ἀπὸ ὄχι μεγάλο ἀριθμὸ ἐπαναληπτικῶν βημάτων, θὰ ἔχουν βρεθεῖ

ὑποδεῖκτες k, j, τέτοιοι ὥστε $[x_k]_r = [x_j]_r$, ἄρα $r | \gcd(x_k - x_j, n)$, ὁπότε ἐλπίζει κανεὶς ὅτι $\gcd(x_k - x_j, n)$ εἶναι μὴ τετριμμένος διαιρέτης τοῦ n.

Ἡ τυχαία συμπεριφορὰ τῆς συνάρτησης $\mathbb{Z}_r \to \mathbb{Z}_r$, ποὺ προκύπτει μὲ τὴν παραπάνω διαδικασία, στηρίζεται, πρὸς τὸ παρόν, σὲ ἐμπειρικὰ δεδομένα. Ἡ φράση «εἶναι πολὺ πιθανὸ ὅτι ὕστερα ἀπὸ ὄχι μεγάλο ἀριθμὸ ἐπαναληπτικῶν βημάτων...» στηρίζεται στὴν ἑξῆς

Πρόταση 2.1. *Ἔστω πεπερασμένο σύνολο S μὲ πληθάριθμο r. Ἔστω θετικὸς πραγματικὸς ἀριθμὸς λ, τέτοιος ὥστε ὁ $k = 1 + \lfloor \sqrt{2\lambda r} \rfloor$ νὰ εἶναι μικρότερος ἀπὸ τὸν r. Γιὰ κάθε $x_0 \in S$ καὶ κάθε συνάρτηση $g : S \to S$ ὁρίζομε τὴν ἀναδρομικὴ ἀκολουθία $y_0, y_1, y_2, \ldots \in S$ μέσῳ τῆς $y_{i+1} = g(y_i)$, ὅπου τὸ y_0 εἶναι αὐθαίρετο. Τότε, τὸ ποσοστὸ τῶν ζευγαριῶν (g, y_0) μὲ τὴν ἰδιότητα τὰ $y_0, y_1, \ldots, y_k$ νὰ εἶναι διαφορετικὰ μεταξύ τους, εἶναι μικρότερο ἀπὸ $e^{-\lambda}$.*[4]

Γιὰ τὴν περίπτωση ποὺ ἐξετάζομε, $S = \{0, 1, \ldots, r-1\}$ καὶ οἱ συναρτήσεις μας εἶναι τῆς μορφῆς $g(y) = [f(y)]_r$, ὅπου f εἶναι πολυώνυμο μὲ ἀκέραιους συντελεστὲς καὶ r εἶναι (ἄγνωστος σ' ἐμᾶς) διαιρέτης τοῦ n. Ἂν θεωρήσομε τὰ $x_0, x_1, \ldots, x_k$ ὅπως στὴν (2) καὶ θέσομε $y_i = [x_i]_r$, $(i = 0, 1, \ldots, k)$ τότε $y_0, y_1, \ldots, y_k \in S$ καὶ $y_{i+1} = g(y_i)$, ἄρα ἐφαρμόζεται ἡ πρόταση 2.1.

Ἔτσι ὅπως περιγράφεται ἡ μέθοδος αὐτή, φαίνεται ἀναγκαῖο, γιὰ κάθε δείκτη k, νὰ ὑπολογίζεται ὁ $\gcd(x_k - x_j, n)$ γιὰ $j = 0, 1, \ldots, k-1$. Στὴν πράξη, αὐτὸ μπορεῖ νὰ ἀποφευχθεῖ ἀρκετὰ εὔκολα. Κάνομε πρῶτα τὴν ἑξῆς ἁπλῆ παρατήρηση: Ἂν $[x_k]_r = [x_j]_r$ γιὰ κάποιους διαφορετικούς, ἐν γένει, δεῖκτες k, j, τότε $[x_{k+1}]_r = [x_{j+1}]_r$. Πράγματι, λόγῳ τῆς (2) καὶ τῆς ὑποθέσεως $x_k \equiv x_j \pmod r$,

$$x_{k+1} \equiv f(x_k) \equiv f(x_j) \equiv x_{j+1} \pmod r ,$$

ἄρα $[x_{k+1}]_r = [x_{j+1}]_r$. Τώρα, προχωρώντας ἐπαγωγικά, καταλήγομε στὴ σχέση $[x_{k+i}]_r = [x_{j+i}]_r$ γιὰ $i = 1, 2, \ldots$. Διαφορετικὰ διατυπωμένη, αὐτὴ ἡ τελευταία σχέση λέει ὅτι: Ἂν $[x_k]_r = [x_j]_r$, τότε, γιὰ ὁποιοδήποτε ἄλλο ζεῦγος δεικτῶν k_1, j_1 μὲ $k_1 - j_1 = k - j$, ἰσχύει $[x_{k_1}]_r = [x_{j_1}]_r$. Ἐπειδὴ τώρα, γιὰ κάθε ζεῦγος δεικτῶν $k > j \geq 0$ ὑπάρχει (ἕνας μοναδικὸς) ἀκέραιος $t \geq 1$, τέτοιος ὥστε $2^{t-1} \leq k - j \leq 2^t - 1$,[5] ἀρκεῖ, γιὰ κάθε $j \geq 0$ νὰ ὑπολογίζομε τὸν $\gcd(x_k - x_j, n)$, μόνο γιὰ τὸ $k = 2^t - 1$, ὅπου t τὸ πλῆθος τῶν δυαδικῶν ψηφίων τοῦ j.

[4] Proposition V.2.1 στὸ [1].

[5] Δηλαδή, t εἶναι τὸ πλῆθος τῶν δυαδικῶν ψηφίων τοῦ $k - j$.

3 Παραγοντοποίηση Fermat καὶ ἡ μέθοδος τῶν συνεχῶν κλασμάτων

Ἔστω n περιττὸς ἀριθμός, ὁ ὁποῖος ἔχει πιστοποιηθεῖ ὡς σύνθετος. Ἂς ὑποθέσομε ὅτι $n = ab$, γιὰ κάποιους (περιττοὺς) ἀκεραίους $a > b > 1$. Ἰσχύει ἡ στοιχειώδης ταυτότητα

$$n = \left(\frac{a+b}{2}\right)^2 - \left(\frac{a-b}{2}\right)^2 .$$

Ἂν ὁ a εἶναι "πολὺ κοντὰ" στὸν b, ὁπότε ὁ $n_0 = ((a-b)/2)^2$ εἶναι "πολὺ μικρός", τότε ὁ $(a+b)/2$ εἶναι ἕνας ἀκέραιος τῆς μορφῆς $[\sqrt{n}] + j$, γιὰ κάποιο "πολὺ μικρὸ" φυσικὸ ἀριθμὸ j, μὲ τὴν ἰδιότητα $([\sqrt{n}] + j)^2 - n =$ *τέλειο τετράγωνο*. Μὲ αὐτὸν τὸν τρόπο βρίσκονται ταχύτατα τὰ $(a \pm b)/2$, ἄρα καὶ τὰ a, b.

Παράδειγμα: Ἔστω $n = 23360947609$. Ἐδῶ $[\sqrt{n}] = 152842$ καὶ ὑπολογίζοντας $\sqrt{(152842+j)^2 - n}$ γιὰ τὶς διάφορες φυσικὲς τιμὲς τοῦ j, διαπιστώνομε ὅτι $\sqrt{(152842+3)^2 - n} = 804$. Ἄρα, $(a-b)/2 = 804$, $(a+b)/2 = 152845$ καί, συνεπῶς, $a = 153649$, $b = 152041$.

Ἀπὸ τὰ παραπάνω συμπεραίνομε ὅτι, ἂν καταφέρομε νὰ γράψομε τὸν n ὡς διαφορὰ δύο τετραγώνων, τότε πετύχαμε καὶ τὴν παραγοντοποίησή του. Στὴν πράξη, αὐτὸ μπορεῖ νὰ ἐπιτευχθεῖ μόνο ἂν $n = ab$ καὶ ὁ a εἶναι "πολὺ κοντὰ" στὸν b. Τί θὰ γινόταν ἄν, ἀντὶ μιᾶς σχέσης $x^2 = y^2 + n$, ἀναζητούσαμε x, y τέτοια ὥστε $x^2 = y^2 + zn$ γιὰ κάποιον ἀκέραιο z; Αὐτὸ θὰ σήμαινε εὕρεση x, y τέτοιων ὥστε $x^2 \equiv y^2 \pmod{n}$. Ἂν καταφέρναμε νὰ βρίσκαμε τέτοια x, y μὲ $x \not\equiv \pm y \pmod{n}$, τότε οἱ $\gcd(x+y, n), \gcd(x-y, n)$ εἶναι δύο μὴ τεριμμένοι διαιρέτες τοῦ n. Προσπαθοῦμε, λοιπόν, νὰ βροῦμε ἕνα "σχετικῶς μικρὸ" σύνολο $\mathcal{P}$ ἀποτελούμενο ἀπὸ μικροὺς πρώτους καὶ τὸ -1, καὶ διάφορους ἀκεραίους b_i, $i = 1, 2, \ldots$ μὲ τὴν ἰδιότητα

> Τὸ ἐλάχιστο κατ' ἀπόλυτη τιμὴ ὑπόλοιπο τοῦ $b_i^2 \pmod{n}$ νὰ εἶναι $\mathcal{P}$-ἀριθμός, δηλαδή, νὰ ἐκφράζεται ὡς γινόμενο πρώτων τοῦ $\mathcal{P}$.

Ἔστω $\mathcal{P} = \{-1, p_1, p_2, \ldots, p_t\}$ καὶ ἂς ὑποθέσομε ὅτι βρήκαμε $b_1, \ldots, b_k$, τέτοια ὥστε

$$b_i^2 \equiv (-1)^{e_{0i}} p_1^{e_{1i}} p_2^{e_{2i}} \cdots p_t^{e_{ti}} \pmod{n} \quad (i = 1, 2, \ldots, k)$$

($e_{0i} = \pm 1$) καὶ

$$\sum_{i=1}^{k} e_{ji} \equiv 0 \pmod{2} \quad \text{γιὰ κάθε } j = 0, 1, \ldots t .$$

Τότε, θέτοντας $e_j = \frac{1}{2}\sum_{i=1}^{k} e_{ji}$ γιὰ $j = 1, 2, \ldots, t$, ἔχομε ὅτι

$$\left(\prod_{i=1}^{k} b_i\right)^2 \equiv \left(\prod_{j=1}^{t} p_j^{e_j}\right)^2 \pmod{n},$$

καὶ ἐλπίζομε ὅτι ἡ παραπάνω ἰσοδυναμία τῆς μορφῆς $x^2 \equiv y^2 \pmod{n}$, δὲν εἶναι τετριμμένη, δηλαδή, ἰσχύει $x \not\equiv \pm y \pmod{n}$.

3.1 Ἡ μέθοδος τῶν συνεχῶν κλασμάτων

Ἡ βασικὴ ἰδέα τῆς μεθόδου εἶναι νὰ χρησιμοποιήσει τὰ ἀναγωγήματα (convergents) τοῦ συνεχοῦς κλάσματος[6] τοῦ $\sqrt{n}$ προκειμένου νὰ βρεθοῦν μὲ πιὸ συστηματικὸ τρόπο ἀκέραιοι b_i μὲ τὶς παραπάνω ἰδιότητες. Στηρίζεται στὴν ἑξῆς

Πρόταση 3.1. *Ἔστω πραγματικὸς ἀριθμὸς $\alpha > 1$ καὶ $\frac{P_i}{Q_i}$, $i = 0, 1, 2, \ldots$ τὰ ἀναγωγήματα τοῦ συνεχοῦς κλάσματος τοῦ α. Τότε, γιὰ κάθε i, $|P_i^2 - \alpha^2 Q_i^2| < 2\alpha$.*

Ἡ ἀπόδειξη στηρίζεται στὰ ἑξῆς: (α') Γιὰ κάθε i, οἱ ἀριθμοὶ $\frac{P_i}{Q_i}$ καὶ $\frac{P_{i+1}}{Q_{i+1}}$ ἀπέχουν $\frac{1}{Q_i Q_{i+1}}$. (β') Γιὰ i ἄρτιο, $\frac{P_i}{Q_i} \le \alpha \le \frac{P_{i+1}}{Q_{i+1}}$, ἐνῶ γιὰ i περιττό, $\frac{P_{i+1}}{Q_{i+1}} \le \alpha \le \frac{P_i}{Q_i}$. Ἀπὸ αὐτὰ προκύπτει, εἰδικώτερα, ὅτι $\frac{P_i}{Q_i} < \alpha + \frac{1}{Q_i Q_{i+1}}$ καὶ $\left|\alpha - \frac{P_i}{Q_i}\right| \le \frac{1}{Q_i Q_{i+1}}$. Ὅποτε

$$\begin{aligned} |P_i^2 - \alpha^2 Q_i^2| &= Q_i^2 \left|\alpha - \frac{P_i}{Q_i}\right| \left|\alpha + \frac{P_i}{Q_i}\right| < Q_i^2 \frac{1}{Q_i Q_{i+1}} \left(\alpha + (\alpha + \frac{1}{Q_i Q_{i+1}})\right) \\ &= \frac{Q_i}{Q_{i+1}} \left(2\alpha + \frac{1}{Q_i Q_{i+1}}\right) = 2\alpha \left(\frac{Q_i}{Q_{i+1}} + \frac{1}{2\alpha Q_{i+1}^2}\right) \\ &< 2\alpha \left(\frac{Q_i}{Q_{i+1}} + \frac{1}{Q_{i+1}}\right) = 2\alpha \frac{Q_i + 1}{Q_{i+1}} \le 2\alpha \end{aligned}$$

Ἂς πάρομε τώρα $\alpha = \sqrt{n}$. Τότε, $P_i^2 \equiv P_i^2 - nQ_i^2 \pmod{n}$, ἐνῶ, ἀπὸ τὴν Πρόταση 3.1, $|P_i^2 - nQ_i^2| < 2\sqrt{n}$. Αὐτὸ συνεπάγεται ὅτι τὸ ἐλάχιστο κατ' ἀπόλυτη τιμὴ ὑπόλοιπο τοῦ $P_i^2 \bmod n$ εἶναι κατ' ἀπόλυτη τιμὴ $< 2\sqrt{n}$, ἄρα, πολὺ πιθανόν, εἶναι $\mathcal{P}$-ἀριθμός.

[6] Στὴν ἱστοσελίδα τοῦ Τμήματος θὰ βρεῖτε μεταφρασμένη τὴ «Θεωρία Ἀριθμῶν» τοῦ I.M. Vinogradov, ὅπου ἐκτίθεται πολὺ ἁπλὰ ἡ ἐντελῶς βασικὴ θεωρία τῶν συνεχῶν κλασμάτων, ἡ ὁποία μᾶς χρειάζεται ἐδῶ.

᾽Αναφορὲς

[1] N. Koblitz, *A course in Number Theory and Cryptography*, Graduate Texts in Math., vol. 114, Springer-Verlag, Berlin and New York, 1994.