Πιστοποίηση πρώτου

Καθηγητὴς Ν.Γ. Τζανάκης

Τελευταία ἐνημέρωση 8/1/2008

1 Ἡ πιστοποίηση πρώτου στὴν Κρυπτογραφία

Στὴν *Κρυπτογραφία Δημοσίου Κλειδιοῦ* κάθε μία ἀπὸ τὶς ἐπικοινωνοῦσες ὀντότητες ἔχει μυστικὸ κλειδί, τὸ ὁποῖο βασίζεται στὴ γνώση πολὺ μεγάλων πρώτων ἀριθμῶν. Στὴν πράξη, μὲ τὴ βοήθεια μιᾶς *γεννήτριας τυχαίων ἀριθμῶν*, δημιουργεῖ κανεὶς ἕνα τυχαῖο ἀκέραιο ἀριθμὸ n δεδομένης τάξεως μεγέθους καὶ μετὰ ἐξετάζει ἂν αὐτὸς εἶναι πρῶτος ἢ ὄχι. Ἂν δὲν εἶναι, ἐξετάζει διαδοχικὰ τοὺς $n+1, n+2, \ldots$ μέχρις ὅτου ἀνακαλύψει πρῶτο ἀριθμό, ἢ δημιουργεῖ νέο τυχαῖο ἀριθμὸ μὲ τὴ βοήθεια τῆς γεννήτριάς του. Θὰ ἦταν θανάσιμο λάθος γιὰ ἕνα κρυπτογράφο νὰ χρησιμοποιήσει ἀριθμοὺς γνωστῆς μορφῆς, ὅπως, γιὰ παράδειγμα, εἶναι οἱ:

Ἀριθμοὶ Fermat: $F_k = 2^{2^k} + 1$
Ἀριθμοὶ τοῦ Mersenne: $M_k = 2^k - 1$

καὶ νὰ ἐπιλέξει κάποιον, ὁ ὁποῖος εἶναι πρῶτος.

Ἂν, λοιπόν, ἔχει κανεὶς ἕνα φυσικὸ ἀριθμὸ n, θέλει νὰ μπορεῖ νὰ ἀποφασίσει κατὰ πόσον αὐτὸς εἶναι πρῶτος. Ὑπάρχουν οἱ **ἀποδείξιμες** καὶ οἱ **πιθανοθεωρητικὲς** πιστοποιήσεις πρώτων.

2 Ἀποδείξιμη πιστοποίηση

Αὐτὴ γίνεται βάσει κάποιων κριτηρίων. Πρόκειται γιὰ *θεωρήματα*, τὰ ὁποῖα ἀποφαίνονται ὅτι, ἂν ὁ φυσικὸς ἀριθμὸς n πληροῖ κάποιες ὑποθέσεις, τότε εἶναι πρῶτος. Κάθε μία ἀπὸ τὶς παρακάτω προτάσεις παρέχει ἀποδείξιμη πιστοποίηση πρώτου.

Κατ' ἀρχὰς κάνομε τὴν παρατήρηση ὅτι, ἀπὸ τὸ Θεώρημα τοῦ Fermat[1], ἂν ὁ n εἶναι πρῶτος, τότε, γιὰ κάθε a πρῶτο πρὸς τὸν n, ἰσχύει $a^{n-1} \equiv 1 \pmod{n}$. Ἄρα, ἂν βρεθεῖ κάποιος a πρῶτος πρὸς τὸν n, γιὰ τὸν ὁποῖο $a^{n-1} \not\equiv 1 \pmod{n}$, τότε συμπεραίνομε μὲ βεβαιότητα ὅτι ὁ n εἶναι σύνθετος. Ἂν, ὅμως, γιὰ κάποιον b, ποὺ εἶναι πρῶτοι πρὸς τὸν n, ἰσχύει $b^{n-1} \equiv 1 \pmod{n}$, τί μποροῦμε νὰ ποῦμε γιὰ τὸν n; Ἢ, ἀκόμη περισσότερο, τί μποροῦμε νὰ ποῦμε γιὰ τὸν n ἂν *γιὰ κάθε* b πρῶτο πρὸς τὸν n ἰσχύει $b^{n-1} \equiv 1 \pmod{n}$; Δυστυχῶς, οὔτε μὲ αὐτὴ τὴν ἰσχυρότερη ὑπόθεση μποροῦμε νὰ συμπεραίνομε ὅτι ὁ n εἶναι πρῶτος· πολὺ χαρακτηριστικὸ παράδειγμα ὁ $561 = 3 \cdot 11 \cdot 17$, γιὰ τὸν ὁποῖον ἰσχύει $b^{560} \equiv 1 \pmod{561}$ γιὰ ὅλους τοὺς b μὲ $(b, 561) = 1$.

Ὁρισμός 2.1. *Ἂν ὁ n εἶναι περιττὸς σύνθετος ἀριθμὸς καὶ b ἀκέραιος πρῶτος πρὸς τὸν n, ἔτσι ὥστε νὰ ἰσχύει $b^{n-1} \equiv 1 \pmod{n}$, τότε ὁ n λέγεται ψευδοπρῶτος ὡς πρὸς τὸν b, ἢ ὡς πρὸς βάση b. Ἂν ὁ n εἶναι ψευδοπρῶτος ὡς πρὸς κάθε b ($\gcd(b, n) = 1$), τότε λέγεται ἀριθμὸς (τοῦ) Carmichael.*

Ὁ ἐλάχιστος ἀριθμὸς Carmichael εἶναι ὁ 561. Ἡ εἰκασία τοῦ R.D. Carmichael ὅτι ὑπάρχουν ἄπειροι τέτοιοι ἀριθμοί, ποὺ ἔγινε στὰ 1912, ἀποδείχθηκε 82 χρόνια μετά· βλ. [1].

Ἄσκηση 1. *Ὑπολογῖστε ὅλες τὶς βάσεις ὡς πρὸς τὶς ὁποῖες ὁ 15 εἶναι ψευδοπρῶτος. Ἀνάλογο ζήτημα καὶ γιὰ τὸν 21.*

Ἄσκηση 2. *Ἔστω ὅτι ὁ p εἶναι περιττὸς πρῶτος, τέτοιος ὥστε ὁ $q = 2p - 1$ εἶναι πρῶτος, καὶ $n = pq$. Ἀποδεῖξτε ὅτι, ὁ n ἔχει ἀκριβῶς $\phi(n)/2$ τὸ πλῆθος βάσεις ὡς πρὸς τὶς ὁποῖες εἶναι ψευδοπρῶτος.*

Ἄσκηση 3. *Ἔστω n περιττός, σύνθετος, θετικὸς ἀκέραιος καὶ b ἀκέραιος πρῶτος πρὸς τὸν n.*
(α') Ἂν ὁ p εἶναι πρῶτος διαιρέτης τοῦ n καὶ $m = n/p$ καὶ ὁ n εἶναι ψευδοπρῶτος ὡς πρὸς τὸν b, τότε $b^{m-1} \equiv 1 \pmod{p}$.
(β') Ἀποδεῖξτε ὅτι οὐδεὶς ἀριθμὸς τῆς μορφῆς $n = 3p$, μὲ $p > 3$ πρῶτο, εἶναι ψευδοπρῶτος ὡς πρὸς τὸν 2, ἢ τὸν 5, ἢ τὸν 7.
(γ') Ἀποδεῖξτε ὅτι οὐδεὶς ἀριθμὸς τῆς μορφῆς $n = 5p$, μὲ $p > 5$ πρῶτο, εἶναι ψευδοπρῶτος ὡς πρὸς τὸν 2, ἢ τὸν 3, ἢ τὸν 7.
(δ') Ἀποδεῖξτε ὅτι ὁ ἐλάχιστος θετικὸς ἀκέραιος, ὁ ὁποῖος εἶναι ψευδοπρῶτος ὡς πρὸς τὸν 3, εἶναι ὁ 91.

[1] Τὸ λεγόμενο «μικρό», σὲ ἀντιδιαστολὴ μὲ τὸ «μεγάλο» ἢ «τελευταῖο», ποὺ ἀποδείχθηκε στὰ 1995, ὕστερα ἀπὸ 350, περίπου, χρόνια.

Άσκηση 4. *Άποδεῖξτε ὅτι, ἂν ὁ n εἶναι ψευδοπρῶτος ὡς πρὸς τὸν b, τότε εἶναι ψευδοπρῶτος καὶ ὡς πρὸς τοὺς $-b$ καὶ $b^{-1} \pmod n$. Ἐπίσης, ἂν ὁ n εἶναι ψευδοπρῶτος ὡς πρὸς τοὺς b_1 καὶ b_2, τότε εἶναι ψευδοπρῶτος καὶ ὡς πρὸς τὸν $b_1 b_2$.*

Άσκηση 5. *Ἔστω ὅτι ὁ n εἶναι ψευδοπρῶτος ὡς πρὸς τὸν b καὶ $(b-1, n) = 1$. Ἀποδεῖξτε ὅτι καὶ ὁ $N = (b^n - 1)/(b - 1)$ εἶναι ψευδοπρῶτος ὡς πρὸς τὸν b.*

Άσκηση 6. *Ἔστω ὅτι ὁ k εἶναι θετικὸς ἀκέραιος, τέτοιος ὥστε καὶ οἱ τρεῖς ἀριθμοὶ $6k + 1, 12k + 1, 18k + 1$ εἶναι πρῶτοι. Ἀποδεῖξτε ὅτι τὸ γινόμενό τους εἶναι ἀριθμὸς τοῦ Carmichael.*

Άσκηση 7. *Ἀποδεῖξτε ὅτι ὅλοι οἱ ἑπόμενοι εἶναι ἀριθμοὶ τοῦ Carmichael: 1105, 1729, 2465, 2821, 6601, 29341, 172081, 278545.*

Άσκηση 8. *Ἔστω $n = pq$, ὅπου οἱ p, q εἶναι διαφορετικοὶ πρῶτοι, καὶ $d = (p - 1, q - 1)$.*
(α΄) Ἀποδεῖξτε ὅτι ὁ n εἶναι ψευδοπρῶτος ὡς πρὸς τὸν b ἄν, καὶ μόνο ἄν, $b^d \equiv 1 \pmod n$. Ὑπολογῖστε συναρτήσει τοῦ d, τὸ πλῆθος τῶν βάσεων, ὡς πρὸς τὶς ὁποῖες ὁ n εἶναι ψευδοπρῶτος.
Ὑπενθύμιση ἀπὸ τὴ Θεωρία Ἀριθμῶν: Τὸ πλῆθος τῶν διαφορετικῶν λύσεων τῆς ἰσοτιμίας $x^r \equiv 1 \pmod p$, ὅπου ὁ p εἶναι πρῶτος, εἶναι ἴσο μὲ $(r, p - 1)$.
(β΄) Ἂν $q = 2p + 1$, πόσες, συναρτήσει τοῦ p, εἶναι οἱ βάσεις ὡς πρὸς τὶς ὁποῖες ὁ n εἶναι ψευδοπρῶτος;
(α΄) Ποιὰ εἶναι ἡ πιθανότητα νὰ ἐπιλεγεῖ τυχαῖος b, πρῶτος πρὸς τὸν n καί, ὡς πρὸς αὐτόν, ὁ 341 νὰ εἶναι ψευδοπρῶτος;

Πρόταση 2.2. *Σὲ κάθε μία ἀπὸ τὶς ἑπόμενες περιπτώσεις ὁ ἀκέραιος ἀριθμὸς $n > 2$ εἶναι πρῶτος.*

1. *Ὑπάρχει κάποιος a ὡς πρὸς τὸν ὁποῖον ὁ n εἶναι ψευδοπρῶτος καὶ ἰσχύει $a^k \not\equiv 1 \pmod n$ γιὰ κάθε $k = 1, \ldots, n - 2$.*

2. *Ὑπάρχει κάποιος a ὡς πρὸς τὸν ὁποῖον ὁ n εἶναι ψευδοπρῶτος καὶ γιὰ κάθε θετικὸ διαιρέτη k τοῦ $n - 1$, ὁ ὁποῖος εἶναι γνησίως μικρότερος τοῦ $n - 1$, ἰσχύει $a^k \not\equiv 1 \pmod n$.*

3. *Ὑπάρχει κάποιος a ὡς πρὸς τὸν ὁποῖον ὁ n εἶναι ψευδοπρῶτος καὶ γιὰ κάθε πρῶτο διαιρέτη q τοῦ $n - 1$, ἰσχύει $a^{\frac{n-1}{q}} \not\equiv 1 \pmod n$.*

4. *Γιὰ κάθε πρῶτο διαιρέτη q τοῦ $n - 1$, ὑπάρχει $a_q \in \mathbb{Z}$ ὡς πρὸς τὸν ὁποῖον ὁ n εἶναι ψευδοπρῶτος καὶ $a_q^{\frac{n-1}{q}} \not\equiv 1 \pmod n$.*

5. *Ὑπάρχει $a \in \mathbb{Z}$ καὶ διαιρέτης m τοῦ $n-1$ μὲ $m^2 \geq n$, τέτοιοι ὥστε, ὁ n εἶναι ψευδοπρῶτος ὡς πρὸς τὸν a καὶ $(a^{\frac{n-1}{q}} - 1, n) = 1$ γιὰ κάθε πρῶτο διαιρέτη q τοῦ m.*

6. *Ὁ $n-1$ μπορεῖ νὰ παραγοντοποιηθεῖ ὡς $n-1 = 2^r s,\ s \leq 2^r + 1$ καὶ ὑπάρχει $a \in \mathbb{Z}$, τέτοιο ὥστε $a^{\frac{n-1}{2}} \equiv -1 \pmod{n}$.*

Ἀπόδειξη. (1) Ἐργαζόμαστε στὴν ὁμάδα $\mathbb{Z}_n^*$, τῆς ὁποίας ἡ τάξη εἶναι $\phi(n)$. Οἱ ὑποθέσεις ἰσοδυναμοῦν μὲ τὸ ὅτι τὸ $a \in \mathbb{Z}_n^*$ ἔχει τάξη $n-1$. Ἄρα, $(n-1)|\phi(n)$. Εἰδικώτερα, $n-1 \leq \phi(n)$, σχέση ἀδύνατη γιὰ σύνθετο n.
(2) Ὅπως καὶ πρίν, ἐργαζόμαστε στὴν ὁμάδα $\mathbb{Z}_n^*$. Ἀπὸ τὴν πρώτη ὑπόθεση συμπεραίνομε ὅτι ἡ τάξη τοῦ $a \in \mathbb{Z}_n^*$ εἶναι διαιρέτης τοῦ $n-1$, ἐνῶ ἀπὸ τὴ δεύτερη ὑπόθεση συμπεραίνομε ὅτι ἡ τάξη τοῦ a δὲν εἶναι γνησίως μικρότερη τοῦ $n-1$, ἄρα εἶναι ἴση μὲ $n-1$. Μετά, ἡ ἀπόδειξη ὁλοκληρώνεται ἀκριβῶς ὅπως στὴν περίπτωση 1.
(3) Ἐργαζόμαστε στὴν ὁμάδα $\mathbb{Z}_n^*$. Ἔστω r ἡ τάξη τοῦ $a \in \mathbb{Z}_n^*$. Ἀπὸ τὴν πρώτη ὑπόθεση, $r|(n-1)$ καὶ ἔστω $n-1 = rs$. Ἂν $r < s$, τότε $s > 1$ καὶ ἔστω πρῶτος διαιρέτης q τοῦ s. Λόγῳ τῆς $\frac{n-1}{q} = r\frac{s}{q}$, ὅπου $\frac{s}{q} \in \mathbb{Z}$ καὶ τῆς $a^r = 1$, συμπεραίνομε ὅτι $aa^{(n-1)/q} = 1$, ποὺ ἀντιβαίνει στὴν ὑπόθεση. Συμπεραίνομε, λοιπόν, ὅτι $r = n-1$ καὶ ὁλοκληρώνομε τὴν ἀπόδειξη ἀκριβῶς ὅπως στὴν περίπτωση 1.
(4) Ἐργαζόμαστε στὴν ὁμάδα $\mathbb{Z}_n^*$. Συμβολίζομε μὲ $q_1, \ldots, q_m$ ὅλους τοὺς διαφορετικοὺς πρώτους διαιρέτες τοῦ $n-1$. Ἐξ ὑποθέσεως ὑπάρχουν $a_1, \ldots, a_m \in \mathbb{Z}_n^*$ τέτοια ὥστε, γιὰ κάθε $i = 1, \ldots, m$ νὰ ἰσχύει $a_i^{n-1} = 1$ καὶ $a_i^{(n-1)/q_i} \neq 1$. Γιὰ κάθε i, ἔστω r_i ἡ τάξη τοῦ a_i. Ἀπὸ θεώρημα τῆς Θεωρίας Ὁμάδων συμπεραίνομε ὅτι ὑπάρχει $a \in \mathbb{Z}_n^*$, τοῦ ὁποίου ἡ τάξη ἰσοῦται μὲ $r := \text{εκπ}(r_1, \ldots, r_m)$. Ἐπειδὴ ὁ $n-1$ εἶναι πολλαπλάσιο καθενὸς r_i, ἕπεται ὅτι εἶναι πολλαπλάσιο καὶ τοῦ r. Ἀλλὰ $a^r = 1$, ἄρα καὶ $a^{n-1} = 1$. Ἂν δείξομε τώρα ὅτι $a^{(n-1)/q_i} \neq 1$, τότε, ἀπὸ τὸ 3, θὰ ἔχομε ὁλοκληρώσει τὴν ἀπόδειξη. Ἀλλά, ἂν ἦταν $a^{(n-1)/q_i} = 1$, τότε θὰ ἔπρεπε $r|\frac{n-1}{q_i}$, ἄρα καὶ $r_i|\frac{n-1}{q_i}$. Ὅμως, $a_i^{r_i} = 1$, ἄρα $a_i^{(n-1)/q_i} = 1$, ποὺ ἀντιβαίνει ποὺ ἐπιλέξαμε τὸ a_i.
(5) Ἂν εἶναι σύνθετος ὁ n, τότε ἔχει πρῶτο διαιρέτη $p \leq \sqrt{n}$. Τότε, ἂν δείξομε ὅτι $p \equiv 1 \pmod{m}$, αὐτὸ θὰ ἔχει ὡς συνέπεια ὅτι $p \geq 1+m \geq 1+\sqrt{n} > \sqrt{n}$, ἀντίφαση, ἡ ὁποία μᾶς ὁδηγεῖ στὸ συμπέρασμα ὅτι ὁ n εἶναι πρῶτος. Τώρα, γιὰ νὰ δείξομε τὴ σχέση $p \equiv 1 \pmod{m}$, πρέπει καὶ ἀρκεῖ νὰ δείξομε τὸ ἑξῆς: Γιὰ κάθε πρῶτο διαιρέτη q τοῦ m, ἂν $q^e||m$, τότε $p \equiv 1 \pmod{q^e}$. Τὸ τελευταῖο ἀποδεικνύεται ὡς ἑξῆς: Θέτομε $c = a^{(n-1)/q^e}$, ὁπότε $c^{q^e} = a^{n-1} \equiv 1 \pmod{n}$, ἄρα καὶ $c^{q^e} \equiv 1 \pmod{p}$. Ἂν ἦταν $c^{q^{e-1}} \equiv 1 \pmod{p}$, τότε $a^{(n-1)/q} \equiv 1 \pmod{p}$, ἄρα $p|(a^{(n-1)/q} - 1, n)$, ποὺ ἀντιφάσκει

μὲ τὴν ὑπόθεση. Συμπεραίνομε, λοιπόν, ὅτι ἡ τάξη τοῦ $c \bmod p$ εἶναι q^e καί, συνεπῶς, $q^e|(p-1)$, δηλαδή, $p \equiv 1 \pmod{q^e}$.
(6) Κατ' ἀρχάς παρατηροῦμε ὅτι, ἂν ὁ περιττὸς πρῶτος q εἶναι διαιρέτης ἑνὸς ἀριθμοῦ τῆς μορφῆς $x^{2^m}+1$, τότε $q \equiv 1 \pmod{2^{m+1}}$. Πράγματι, $x^{2^m} \equiv -1 \pmod{q}$, ἄρα $x^{2^{m+1}} \equiv 1 \pmod{q}$. Συνεπῶς, ἂν r εἶναι ἡ τάξη $\bmod q$ τοῦ x, τότε $r|2^{m+1}$ καὶ ἔστω $r = 2^k$, ὅπου $k \leq m+1$. Ἂν ἦταν $k \leq m$, τότε καὶ $2^m \equiv 1 \pmod{q}$, ἀντίφαση. Ἄρα, $r = 2^{m+1}$. Ὅμως, ἀφοῦ $x^{q-1} \equiv 1 \pmod{q}$, πρέπει $r|(q-1)$, δηλαδή, $q \equiv 1 \pmod{2^{m+1}}$.
Τώρα προχωροῦμε στὴν κυρίως ἀπόδειξη: Ἀπὸ τὶς ὑποθέσεις προκύπτει ἀμέσως ἡ σχέση $(a^s)^{2^{r-1}} \equiv -1 \pmod{n}$. Ἂν, λοιπόν, ὁ p εἶναι πρῶτος διαιρέτης τοῦ n, τότε ὁ p διαιρεῖ τὸν $(a^s)^{2^{r-1}}+1$, ἄρα, σύμφωνα μὲ τὴν παρατήρηση στὴν ἀρχὴ τῆς ἀπόδειξης, $p \equiv 1 \pmod{2^r}$. Εἰδικώτερα, αὐτὸ συνεπάγεται ὅτι $p \geq 1+2^r$. Ἂν ἦταν ὁ n σύνθετος, θὰ εἶχε δύο τουλάχιστον πρώτους διαιρέτες p, q (ὄχι, κατ' ἀνάγκη, διαφορετικούς), ὁπότε

$$1+2^r s = n \geq pq \geq (1+2^r)^2 = 1+2^{r+1}+2^{2r} = 1+2^r(2+2^r)\,,$$

ὁπότε $s \geq 2+2^r$, ποὺ ἀντιφάσκει πρὸς τὴν ὑπόθεση.

Ἄσκηση 9. *-Πιστοποίηση πρώτου γιὰ ἀριθμοὺς τοῦ Fermat. Ἀριθμοὶ τοῦ Fermat λέγονται οἱ ἀριθμοὶ $F_k = 2^{2^k}+1$, $k = 0,1,2,\ldots$. Παρατηρῆστε ὅτι οἱ F_0, F_1, F_2, F_3, F_4 εἶναι πρῶτοι. Ὁ Fermat διατύπωσε τὴν εἰκασία ὅτι ὁ F_k εἶναι πρῶτος γιὰ κάθε k. Ἡ εἰκασία εἶναι ἐσφαλμένη, καθὼς ὁ Euler ἀπέδειξε (δίχως νὰ διαθέτει ἰσχυρὰ ὑπολογιστικὰ ἐργαλεῖα!) ὅτι ὁ $F_5 = 641 \cdot 6700417$. Ἡ ἄσκηση αὐτὴ μᾶς δίνει ἕνα κριτήριο γιὰ τὸ πότε ὁ F_k εἶναι πρῶτος. Ἔστω $n = F_k$ ($k \geq 2$). Ἀποδεῖξτε ὅτι ὁ n εἶναι πρῶτος ἂν, καὶ μόνο ἂν, $5^{(n-1)/2} \equiv -1 \pmod{n}$. Θὰ σᾶς χρειαστεῖ νὰ ἀποδείξετε πρῶτα, ἐπαγωγικά, ὅτι $2^{2^k} \equiv 1 \pmod{5}$ γιὰ ὅλα τὰ $k \geq 2$ καί, βάσει αὐτοῦ, ὅτι $\left(\frac{5}{n}\right) = -1$*

Ἡ ἑπόμενη ἀρκετὰ παλαιά (1914) πιστοποίηση, ποὺ ὀφείλεται στὸν H. Pocklington, εἶναι χρήσιμη, ὄχι τόσο καθ' ἑαυτήν, ἀλλὰ γιατὶ ἐμπνέει τη βασικὴ ἰδέα γιὰ μία πολὺ ἐνδιαφέρουσα καὶ ἀποτελεσματικὴ πιστοποίηση, βασισμένη στὴ χρήση ἐλλειπτικῆς καμπύλης, τὴν ὁποία θὰ ἐκθέσομε ἀμέσως μετὰ τὴν πιστοποίηση τοῦ Pocklington.

Πρόταση 2.3. *Ἔστω n θετικὸς ἀκέραιος, τέτοιος ὥστε, ὁ $n-1$ ἔχει ἕνα πρῶτο διαιρέτη $q > \sqrt{n}-1$. Ἂν ὑπάρχει ἀκέραιος b, ποὺ νὰ ἱκανοποιεῖ τὶς σχέσεις $b^{n-1} \equiv 1 \pmod{n}$ καὶ $\gcd\left(b^{\frac{n-1}{q}}-1, n\right) = 1$, τότε ὁ n εἶναι πρῶτος.*

Ἀπόδειξη. Ἂν ὁ n ἦταν σύνθετος, θὰ εἶχε ἕνα πρῶτο διαιρέτη $p \leq \sqrt{n}$. Ἄρα, λόγῳ τῆς ὑποθέσεως $q > \sqrt{n}-1$, ἕπεται ὅτι $q > p-1$ καί, συνεπῶς,

$\gcd(q, p-1) = 1$. Μποροῦμε, λοιπόν, νὰ βροῦμε ἀκέραιο u, τέτοιον ὥστε, $uq \equiv 1 \pmod{p-1}$. Ἀκόμη, λόγῳ τῆς $b^{n-1} \equiv 1 \pmod{n}$, ἔχομε καὶ $b^{n-1} \equiv 1 \pmod{p}$. Βάσει αὐτῶν ἔχομε τώρα

$$b^{\frac{n-1}{q}} \equiv b^{\frac{n-1}{q}uq} \equiv (b^{n-1})^u \equiv 1 \pmod{p} ,$$

ἄρα $p | \gcd\left(b^{\frac{n-1}{q}} - 1, n\right) = 1$, ποὺ ἔρχεται σὲ ἀντίφαση μὲ τὴν ὑπόθεση.

Ἐκθέτοντας τὴν παρακάτω πιστοποίηση τῶν S. Goldwasser καὶ J. Kilian, θὰ κάνομε χρήση ἐννοιῶν καὶ ἰδεῶν ἀπὸ τὶς §§1.2, 1.3 τῶν καφαλαίων *Παραγοντοποίηση* καὶ *Ἀλγόριθμος γιὰ τὸ ἄθροισμα* $\bmod m$ *σημείων ἐλλειπτικῆς καμπύλης*.

Ὑποτίθεται ὅτι ἔχομε ἕνα μεγάλο περιττὸ ἀκέραιο n, ὁ ὁποῖος ἔχει πιστοποιηθεῖ ὡς «πρῶτος» βάσει κάποιου πιθανοθεωρητικοῦ κριτηρίου (βλ. παρακάτω παράγραφο 3). Θὰ περιγράψομε μία διαδικασία, ποὺ χρησιμοποιεῖ ἐλλειπτικὲς καμπύλες, κατὰ τὴν ὁποία, ἢ ἀνακαλύπτεται κάποιος πρῶτος διαιρέτης τοῦ n, ἢ *ἀποδεικνύεται* ὅτι ὁ n εἶναι πρῶτος.

Παίρνομε μία ἐλλειπτικὴ καμπύλη $E : y^2 = x^3 + ax + b$, ὅπου $a, b \in \mathbb{Z}$ καὶ ἕνα σημεῖο $P \in E(\mathbb{Q})$ ἄπειρης τάξης, τοῦ ὁποίου ὁ παρονομαστὴς $\mathrm{q}(P)$ [2] εἶναι πρῶτος πρὸς τὸν n. Στὴν πράξη, ἐπιλέγομε τυχαίους (μικροὺς) $x_0, y_0 \in \mathbb{Z}$ καὶ αὐθαίρετο $a \in \mathbb{Z}$, θέτομε $P = (x_0, y_0)$, καὶ $b = y_0^2 - x_0^3 - Ax_0$. Ἂν ἐπιλέξομε τὰ x_0, a ἐντελῶς αὐθαίρετα καὶ τὸ y_0 ἔτσι ὥστε νὰ εἶναι $\neq 0$ καὶ *ὄχι* διαιρέτης τοῦ $4a^3 + 27(x_0^3 + ax_0)^2$, τότε, ἀπὸ τὸ Θεώρημα τῶν Nagell-Lutz[3], εἴμαστε βέβαιοι ὅτι τὸ P εἶναι σημεῖο ἄπειρης τάξης. Μὲ κάποιο πρακτικὸ ἀλγόριθμο[4] ὑπολογίζομε τὸ πλῆθος, ἔστω m, τῶν $(x, y) \in \mathbb{Z}_n \times \mathbb{Z}_n$, τὰ ὁποῖα ἐπαληθεύουν τὴν $y^2 \equiv x^3 + ax + b \pmod{n}$. Ἐπειδὴ δὲν ξέρομε, ἀκόμη, μὲ βεβαιότητα, ὅτι ὁ n εἶναι πρῶτος, δὲν ἔχομε δικαίωμα νὰ ἰσχυρισθοῦμε ὅτι τὸ σύνολο $E_n \subseteq \mathbb{Z}_n \times \mathbb{Z}_n$ αὐτῶν τῶν σημείων ἀποτελεῖ ὁμάδα μὲ πράξη τὴν πρόσθεση σημείων πάνω στὴν ἐλλειπτικὴ καμπύλη. Παρ' ὅλα αὐτά, ἐπειδὴ ὁ n εἶναι *πιθανότατα* πρῶτος, E_n εἶναι *πιθανότατα* ὁμάδα, ἡ τάξη της εἶναι m καί, ἄρα, εἶναι σχεδὸν βέβαιο ὅτι τὸ $mP \bmod n$ "δὲν ὑπολογίζεται", ποὺ σημαίνει ὅτι ὁ παρονομαστὴς τοῦ mP *δὲν* εἶναι πρῶτος πρὸς n.

Πιστοποίηση Ἐλλειπτικῆς Καμπύλης 2.4. *(Goldwasser-Kilian)*
Ἐφαρμόζομε τὸν ἀλγόριθμο γιὰ τὸ ἄθροισμα $\bmod n$ *σημείων ἐλλειπτικῆς καμπύλης* [5] *γιὰ τὸν ὑπολογισμὸ τοῦ* $mP \bmod n$. *Ἂν ὁ ἀλγόριθμος ἐπιστρέψει*

[2] Βλ. «Παραγοντοποίηση», τέλος §1.2 .
[3] Βλ. [4], §5.
[4] Βλ.[3].
[5] Βλέπε κεφάλαιο μὲ αὐτὸν τὸν τίτλο.

ἀκέραιο ἀριθμό k, τότε ὁ n εἶναι σύνθετος καὶ ἕνας μὴ τετριμμένος διαιρέτης του εἶναι ὁ k.

Διαφορετικά, ἔστω ὅτι ὁ m ἔχει ἕνα πρῶτο διαιρέτη $q > (\sqrt[4]{n}+1)^2$ καὶ συμβαίνουν τὰ ἑξῆς: $mP \bmod n = \mathcal{O}$ καὶ $\frac{m}{q}P \bmod n$ εἶναι "κανονικὸ σημεῖο". Τότε ὁ n εἶναι πρῶτος.

᾽**Απόδειξη**. Ἀπὸ τὴν κατασκευὴ τοῦ ἀλγορίθμου εἶναι σαφὲς ὅτι, ἂν ὁ ὑπολογισμὸς τοῦ $mP \bmod n$ ἐπιστρέψει $k \in \mathbb{Z}$, αὐτὸς ὁ k εἶναι μὴ τετριμμένος διαιρέτης τοῦ n.

Ἔστω τώρα ὅτι $mP \bmod n = \mathcal{O}$ καὶ $\frac{m}{q}P \bmod n$ εἶναι "κανονικὸ σημεῖο". Ἂν ὁ n ἦταν σύνθετος, θὰ εἶχε ἕνα πρῶτο διαιρέτη $p \leq \sqrt{n}$. Ἔστω $\tilde{E}$ ἡ καμπύλη $E \bmod p$ καὶ $|\tilde{E}(\mathbb{F}_p)| = m'$. Ἔστω, ἀκόμη, $\tilde{P}$ τὸ ἀντίστοιχο τοῦ P στὴν καμπύλη $\tilde{E}$ (ἤ, σὲ διαφορετικὴ διατύπωση, ἡ ἀναγωγὴ τοῦ σημείου $P \pmod p$). Ἀπὸ τὸ Θεώρημα τοῦ Hasse[6],

$$m' \leq p + 1 + 2\sqrt{p} = (\sqrt{p}+1)^2 \leq (\sqrt[4]{n}+1)^2 < q \ ,$$

ἄρα, $(m', q) = 1$. Συνεπῶς, μποροῦμε νὰ βροῦμε ἀκέραιο u, τέτοιον ὥστε $uq \equiv 1 \pmod{m'}$, ἄρα, ὑπάρχει $k \in \mathbb{Z}$, τέτοιο ὥστε, $1 = uq + km'$. Τότε,

$$\frac{m}{q}P = \frac{m}{q}(uq + km')P = u(mP) + \frac{km}{q}(m'P) \qquad (1)$$

καὶ λόγῳ τοῦ ὁμομορφισμοῦ, ποὺ κάθε σημεῖο X τῆς ἐλλειπτικῆς καμπύλης μὲ ρητὲς συντεταγμένες τὸ στέλνει στο $\tilde{X} \in \tilde{E}(\mathbb{F}_p)$ (βλ. §1.2 τοῦ κεφαλαίου *Παραγοντοποίηση*),

$$\frac{m}{q}\tilde{P} = \frac{m}{q}(uq + km')P = u(m\tilde{P}) + \frac{km}{q}(m'\tilde{P}) \ .$$

Ἀλλὰ ἡ ὑπόθεση $mP \bmod n = \mathcal{O}$ μᾶς λέει ὅτι ὁ παρονομαστὴς τοῦ mP διαιρεῖται διὰ n, ἄρα καὶ διὰ p, ὁπότε $m\tilde{P} = \tilde{\mathcal{O}}$. Ἐπίσης, ἡ τάξη τῆς ὁμάδας $\tilde{E}(\mathbb{F}_p)$ εἶναι m', ἄρα $m'\tilde{P} = \tilde{\mathcal{O}}$. Συμπεραίνομε, λοιπόν, ὅτι τὸ δεξιὸ μέλος τῆς (1) εἶναι ἴσο μὲ $\tilde{\mathcal{O}}$. Αὐτό, ὅμως, σημαίνει ὅτι ὁ παρονομαστὴς τοῦ $\frac{m}{q}P$ διαιρεῖται διὰ p καί, συνεπῶς, ἀφοῦ $p|n$, ὁ ἀλγόριθμος γιὰ τὸν ὑπολογισμὸ τοῦ $\frac{m}{q}P \bmod n$ δὲν ἐπιστρέφει "κανονικὸ σημεῖο", γεγονὸς ποὺ ἀντιφάσκει μὲ τὴν ὑπόθεσή μας.

Φυσικά, γιὰ νὰ ἐφαρμόσομε αὐτὴ τὴν πιστοποίηση, πρέπει νὰ εἴμαστε βέβαιοι ὅτι ὁ q εἶναι πρῶτος. Γιὰ τὸν λόγο αὐτό, μποροῦμε νὰ ἐφαρμόσομε τὴν

[6]Βλ. §1.3 τοῦ κεφαλαίου *Παραγοντοποίηση*, ἢ §3.4 τοῦ κεφαλαίου *Διάφορες ὄψεις τῆς Κρυπτογραφίας δημοσίου κλειδιοῦ*, ἢ[2], Κεφάλαιο VI, σελ. 174.

παραπάνω πιστοποίηση ξανά, θέτοντας τὸν q στὴ θέση τοῦ n. Ἀλλὰ τώρα, $q < n/2$. Ἐφαρμόζοντας διαδοχικὰ τὴν παραπάνω διαδικασία, ἀνάγομε τὴν πιστοποίηση τοῦ n στὴν πιστοποίηση ἑνὸς "πολὺ μικροῦ" πρώτου q, ὁ ὁποῖος εἶναι ἤδη γνωστὸς, διαπιστωμένος, πρῶτος.

Παράδειγμα: Γιὰ προφανεῖς πρακτικοὺς λόγους, χρησιμοποιοῦμε σ' αὐτὸ τὸ παράδειγμα μικροὺς ἀριθμούς. Ἔστω ὅτι $n = 16381$. Πιθανοθεωρητικά, πιστοποιεῖται πρῶτος. Θέλομε νὰ τὸ ἀποδείξομε μὲ βεβαιότητα, ἔχοντας τοὺς ἑξῆς περιορισμούς, οἱ ὁποῖοι "μιμοῦνται" τοὺς ρεαλιστικοὺς περιορισμούς, ὅταν ὁ n εἶναι πολὺ μεγάλος. Ὑποτίθεται: (1) Ὅτι μόνον οἱ πρῶτοι < 500 εἶναι πιστοποιημένοι μὲ βεβαιότητα, καὶ (2) Γιὰ τὴν παραγοντοποίηση ἑνὸς ἀκεραίου μπορῶ νὰ δοκιμάσομε μόνο τοὺς πρώτους διαιρέτες 2,3,5,7,11.

Χρησιμοποιοῦμε τὴν καμπύλη $E : y^2 = x^3 + 31x - 61$ καὶ τὸ σημεῖο της $P = (2, 3)$, κάνοντας χρήση τῶν συμβολισμῶν τοῦ 2.4. Ὑπολογίζομε $m = 16320 = 2^6 \cdot 5 \cdot 11$. Κανένας πρῶτος διαιρέτης τοῦ m δὲν ὑπερβαίνει τὸ φρᾶγμα $(\sqrt[4]{n} + 1)^2$, ἄρα πρέπει νὰ ἀλλάξομε τὶς ἐπιλογές μας.

Διατηρώντας τὸ ἴδιο P, ἀλλὰ τροποποιώντας τὴν E, ποὺ τώρα ἂς ἐπιλέξομε νὰ εἶναι $y^2 = x^3 - 2x + 5$, ὑπολογίζομε $m = 16557$. Δοκιμάζοντας τοὺς πρώτους μέχρι τὸ 11 (βλ. περιορισμὸ (2», διαπιστώνομε ὅτι $m = 3 \cdot 5519$ καὶ τὸ 5519 δὲν διαιρεῖται μὲ κανέναν ἀπὸ αὐτοὺς τοὺς μικροὺς πρώτους. Τὸ πιθανοθεωρητικὸ κριτήριο Solovay-Strassen 3.4, ποὺ ἐφαρμόζομε μὲ παράμετρο $r = 30$, πιστοποιεῖ τὸ 5519 ὡς πρῶτο, μὲ πιθανότητα λάθους $< 2^{-30}$. Θέτοντας $q = 5519 > (\sqrt[4]{n} + 1)^2$, βλέπομε ὅτι τὸ $(m/q)P = 3P$ ὑπολογίζεται $\bmod n$, ἐνῶ τὸ $mP \bmod n$ δὲν ὑπολογίζεται. Ἄρα, ἡ πιστοποίηση 2.4 ἀποφαίνεται ὅτι:

> Ὁ 16381 εἶναι *ἀποδεδειγμένα* πρῶτος, ὑπὸ τὸν ὅρον ὅτι ὁ 5519 εἶναι *ἀποδεδειγμένα* πρῶτος. (Πρώτη διαπίστωση)

Ἐπαναλαμβάνομε τὴν ἀνάλογη διαδικασία μὲ $n = 5519$, κάνοντας χρήση τῶν ἴδιων E, P. Τώρα $m = 5613 = 3 \cdot 1871$ καί, πιθανοθεωρητικά, πιστοποιοῦμε ὅτι ὁ $q = 1871 > (\sqrt[4]{n} + 1)^2$ εἶναι πρῶτος, μὲ πιθανότητα λάθους $< 2^{-30}$. Διαπιστώνομε ὅτι τὸ $(m/q)P = 3P$ ὑπολογίζεται $\bmod n$, ἐνῶ τὸ $mP \bmod n$ δὲν ὑπολογίζεται. Ἄρα,

> Ὁ 5519 εἶναι *ἀποδεδειγμένα* πρῶτος, ὑπὸ τὸν ὅρον ὅτι ὁ 1871 εἶναι *ἀποδεδειγμένα* πρῶτος. (Δεύτερη διαπίστωση)

Μεταθέτομε, λοιπόν τὸ πρόβλημα στὴν πιστοποίηση τοῦ ἀκόμη μικρότερου $n = 1871$. Γιὰ ποικιλία, ἂς ἀλλάξομε τὴν E κρατώντας τὸ ἴδιο P, δίχως αὐτὲς οἱ ἐπιλογές μας νὰ εἶναι a priori ἀπαραίτητες. Παίρνομε τὴν $E : y^2 = x^3 +$

$4x-7$ καὶ ὑπολογίζομε $m = 1819$. Ὁ m δὲν διαιρεῖται ἀπὸ κανένα ἀπὸ τοὺς πρώτους τοὺς ≤ 11, ἀλλὰ δὲν πιστοποιεῖται πρῶτος, διότι $5^{m-1} = 5^{1818} \equiv 1131 \not\equiv \pmod{m}$. Ἡ μέθοδος ϱ τοῦ Pollard[7] ἐφαρμοζόμενη μὲ $f(x) = x^2 + 1$ καὶ $x_0 = 2$, δίνει, ὕστερα ἀπὸ μερικὰ βήματα, τὸν διαιρέτη 107, ὁ ὁποῖος εἶναι πιστοποιημένος πρῶτος. Ἔτσι, θέτομε $q = 107 > (\sqrt[4]{n}+1)^2$, καὶ διαπιστώνομε ὅτι τὸ $(m/q)P = 17P$ ὑπολογίζεται $\bmod n$, ἐνῶ τὸ $mP \bmod n$ δὲν ὑπολογίζεται. Ἀποδεδειγμένα, λοιπόν, ὁ 1871 εἶναι πρῶτος, ἄρα, λόγῳ τῆς δεύτερης καὶ τῆς πρώτης διαπίστωσης, παραπάνω, συμπεραίνομε ὅτι ὁ 16381 εἶναι *ἀποδεδειγμένα* πρῶτος.

Παράδειγμα μὲ χρήση τοῦ Maple

Βλ. ἑπόμενη σελίδα

[7] Κεφάλαιο *Παραγοντοποίηση*, §2.

Goldwasser-Kilian Primality Test with Elliptic Curves

```
>  restart;
>  AddPts:=proc(a,P1,P2,n) local S,L,b,xs,ys,d,dy1,dy2:
>  if whattype(P1)=integer then S:=P1 fi:
>  if whattype(P2)=integer then S:=P2 fi:
>  if P1=[] then S:=P2 fi:
>  if
>  P2=[] then S:=P1 fi:
>  if whattype(P1)=list and whattype(P2)=list and P1<>[]
and P2<>[] then
>  d:=gcd(P1[1]-P2[1],n):
>  if d>1 and d<n then S:=d fi:
>  if d=1 then
>  L:=modp((P2[2]-P1[2])/(P2[1]-P1[1]),n):
>  b:=modp(P1[2]-L*P1[1],n):
>  xs:=modp(L^2-P1[1]-P2[1],n):
>  ys:=modp(-(L*xs+b),n):
>  S:=[xs,ys]:
>  fi:
>  if d=n
>  then
>  if modp(P1[2]-P2[2],n)<>0 and modp(P1[2]+P2[2],n)<>0
then
>  dy1:=gcd(P1[2]+P2[2],n) :  dy2:=gcd(P1[2]-P2[2],n):
>  if dy1>1 and dy1<n then S:=dy1 fi:
>  if dy2>1 and dy2<n then S:=S,dy2 fi:
>  elif modp(P1[2]+P2[2],n)=0 then S:=[]:
>  else
>  if modp(P1[2],n)=0 then S:=gcd(P2[2],n)
>  elif
>  gcd(P1[2],n)>1 then S:=gcd(P1[2],n)
>  else
>  L:=modp((3*P1[1]^2+a)/(2*P1[2]),n):
>  b:=modp(P1[2]-L*P1[1],n):
>  xs:=modp(L^2-P1[1]-P2[1],n):
>  ys:=modp(-(L*xs+b),n):
>  S:=[xs,ys]:
>  fi:
>  fi:
>  fi:
>  fi:
>  S:
>  end:
>  DoublePt:=proc(a,P,n) local x3,y3,L,X3:
>  if whattype(P)=integer then P
>  else AddPts(a,P,P,n)
>  fi:
>  end:
```

```
> MultPt:=proc(a,P,N,n) local delta,x,E;
> if whattype(P)=integer then delta:=P:
> else
> delta:=[]; x:=P; E:=N;
> while E > 0 do
> if E mod 2 =1 then delta:=AddPts(a,delta,x,n) fi:
> x:=DoublePt(a,x,n):
> E:=floor(E/2):
> od;
> fi:
> if delta=[] then delta:=n fi:
> delta:
> end:
```

```
> n:=12049;
> m:=11846; # number of points (x,y) mod n
> a:=3;
> P:=[2,1];
> (n^0.25+1)^2;
> # a prime factor q of m should be larger than this
> ifactor(m);
```

$$n := 12049$$

$$m := 11846$$

$$a := 3$$

$$P := [2, 1]$$

$$131.7219759$$

$$(2)\ (5923)$$

```
> MultPt(a,P,m,n);
> # if this is not a "normal point"
> # but an integer equal to n then m*P = O mod n
```

$$12049$$

```
> MultPt(a,P,m/5923,n); # must return a "normal point"
```

$$[9089, 10165]$$

An other similar example

```
> n:=73999;
> m:=73736;
> a:=-2;
> P:=[2,1];
> (n^0.25+1)^2;
> ifactor(m);
```

$$n := 73999$$

$$m := 73736$$

$$a := -2$$

$$P := [2, 1]$$

$$306.0140887$$

$$(2)^3\ (13)\ (709)$$

```
> MultPt(a,P,m,n);
```

$$73999$$

```
> MultPt(a,P,m/709,n);
```

$$[65008,\ 73411]$$

3 Πιθανοθεωρητικὴ πιστοποίηση πρώτου

Μιλώντας πολὺ γενικά, πρόκειται γιὰ πιστοποίηση, ποὺ ἂν τὴν περάσει ἕνας θετικὸς περιττὸς ἀκέραιος $n > 1$, τότε, μὲ μεγάλη πιθανότητα, ὁ n εἶναι πρῶτος.

Ὑπάρχουν ποικίλες πιστοποιήσεις, ποὺ ὅλες βασίζονται στὴ χρήση ἀλγορίθμων, οἱ ὁποῖοι κάνουν χρήση τυχαίων ἀριθμῶν, εἶναι, δηλαδή, *πιθανοθεωρητικοὶ ἀλγόριθμοι*.

Ὁρισμός 3.1. *Ἔστω πραγματικὸς ἀριθμὸς $\epsilon \in [0, 1]$. Ἕνας πιθανοθεωρητικὸς ἀλγόριθμος, ὁ ὁποῖος ἀπαντᾶ σὲ ἕνα συγκεκριμένο ἐρώτημα μὲ Ν,Ο (*ΝΑΙ, ΟΧΙ*), χαρακτηρίζεται ὡς θετικὰ προκατειλημμένος Monte Carlo μὲ πιθανότητα λάθους ϵ, ἂν, ὁποτεδήποτε ἀπαντᾶ Ν, ἡ πιθανότητα νὰ ἔχει ἀπαντήσει λάθος εἶναι, τὸ πολύ, ϵ. Ἡ πιθανότητα αὐτὴ ὑπολογίζεται ἐπὶ ὅλων τῶν ἐπιλογῶν τυχαίων παραμέτρων, οἱ ὁποῖες ὑπεισέρχονται στὸν ἀλγόριθμο. Ἂν χαρακτηρισθεῖ θετικὰ προκατειλημμένος Monte Carlo, χωρὶς προσδιορισμὸ λάθους, σημαίνει ὅτι, ὁποτεδήποτε ἀπαντᾶ Ν, ἡ ἀπάντηση εἶναι, μὲ βεβαιότητα, σωστή. Ἂν ὁ ἀλγόριθμος χαρακτηρισθεῖ ἀρνητικὰ προκατειλημμένος Monte Carlo, σημαίνει ὅτι, ὁποτεδήποτε ἀπαντᾶ Ο, ἡ ἀπάντηση εἶναι, μὲ βεβαιότητα, σωστή.*

Πρὶν δώσομε ἕνα παράδειγμα ἀλγορίθμου Monte Carlo, ὑπενθυμίζομε τὸ ἑξῆς ἀπὸ τὴ Στοιχειώδη Θεωρία Ἀριθμῶν: Ἂν ὁ n εἶναι πρῶτος καὶ ὁ ἀκέραιος b εἶναι πρῶτος πρὸς τὸν n, τότε

$$b^{\frac{n-1}{2}} \equiv \left(\frac{b}{n}\right) \pmod{n}\,, \tag{2}$$

ὅπου, γενικά, γιὰ ἀκεραίους x, y πρώτους μεταξύ τους καὶ y περιττό, $\left(\frac{x}{y}\right)$ συμβολίζει τὸ σύμβολο Legendre, γνωστὸ ἀπὸ τὴ Στοιχειώδη Θεωρία Ἀριθμῶν. Τὸ ἀντίστροφο, ἐν γένει, δὲν ἀληθεύει: Ἡ σχέση (2) μπορεῖ νὰ ἰσχύει γιὰ κάποιον ἀκέραιο b, πρῶτο πρὸς τὸν n, καὶ ὁ n νὰ εἶναι σύνθετος.

Ὁρισμός 3.2. *Ἂν ὁ n εἶναι περιττὸς σύνθετος ἀριθμὸς καὶ b ἀκέραιος πρῶτος πρὸς τὸν n, ἔτσι ὥστε νὰ ἰσχύει ἡ (2), τότε ὁ n λέγεται ψευδοπρῶτος Euler ὡς πρὸς τὸν b.*

Πρόταση 3.3. *Ἂν ὁ n εἶναι ψευδοπρῶτος Euler ὡς πρὸς τὸν b, τότε εἶναι καὶ ψευδοπρῶτος ὡς πρὸς τὸν b.*

Ἡ ἀπόδειξη ἕπεται ἀμέσως ἀπὸ τὴ σχέση $\left(\frac{b}{n}\right) = \pm 1$.
Τὸ ἀντίστροφο δὲν ἰσχύει. Γιὰ παράδειγμα, ὁ 91 εἶναι ψευδοπρῶτος ὡς πρὸς

τὸν 3, ἀφοῦ $3^{90} \equiv 1 \pmod{91}$, ἀλλὰ δὲν εἶναι ψευδοπρῶτος Euler ὡς πρὸς τὸν 3, ἀφοῦ $3^{45} \equiv 27 \not\equiv \pm 1 \pmod{91}$.

Μιὰ ἁπλῆ παρατήρηση εἶναι ὅτι, ἂν $b \equiv b' \pmod{n}$ καὶ ὁ n εἶναι ψευδοπρῶτος Euler ὡς πρὸς τὸν b, τότε ὁ n εἶναι ψευδοπρῶτος Euler καὶ ὡς πρὸς τὸν b', ἄρα μποροῦμε νὰ λέμε καὶ ὅτι ὁ n εἶναι ψευδοπρῶτος ὡς πρὸς μία κλάση-στοιχεῖο τῆς ὁμάδας $\mathbb{Z}_n^*$.

Πιστοποίηση Solovay-Strassen 3.4. *Ἔστω περιττὸς ἀκέραιος $n \geq 5$ καὶ ἀκέραια παράμετρος r. Ὁ παρακάτω ἀλγόριθμος, ὁ ὁποῖος ἀπαντᾶ στὸ ἐρώτημα « εἶναι ὁ n πρῶτος ;», εἶναι (α') θετικὰ προκατειλημμένος Monte Carlo μὲ πιθανότητα λάθους 2^{-r} καὶ (β') ἀρνητικὰ προκατειλημμένος.*

1. *Διάλεξε τυχαῖο ἀκέραιο b στὸ διάστημα $[2, n-2]$.*
2. *Ἂν $\gcd(b, n) > 1$, τότε ἡ ἀπάντηση εἶναι* ΟΧΙ *καὶ ὁ ἀλγόριθμος σταματᾶ. Διαφορετικά, προχώρησε στὸ ἑπόμενο βῆμα.*
3. *Ἂν $b^{\frac{n-1}{2}} \not\equiv \left(\frac{b}{n}\right) \pmod{n}$, τότε ἡ ἀπάντηση εἶναι* ΟΧΙ *καὶ ὁ ἀλγόριθμος σταματᾶ. Διαφορετικά, προχώρησε στὸ ἑπόμενο βῆμα.*
4. *$r \leftarrow r - 1$. Ἂν $r = 0$, τότε ἡ ἀπάντηση εἶναι* ΝΑΙ *καὶ ὁ ἀλγόριθμος σταματᾶ. Διαφορετικά, πήγαινε στὸ βῆμα 1.*

Γιὰ τὴν ἀπόδειξη τοῦ ἰσχυρισμοῦ ὅτι πρόκειται γιὰ ἀλγόριθμο Monte Carlo μὲ πιθανότητα λάθους 2^{-r}, ἀρκεῖ νὰ ἡ ἀπόδειξη ὅταν $r = 1$. Αὐτή, πάλι, στηρίζεται στὴν ἑξῆς

Πρόταση 3.5. *Γιὰ κάθε φυσικὸ ἀριθμὸ $n > 2$ ὁρίζομε τὸ σύνολο*

$$E(n) = \{b \in \mathbb{Z}_n^* : \text{ καὶ } n \text{ ψευδοπρῶτος Euler γιὰ τὴν } b\} .$$

Ἂν ὁ n εἶναι σύνθετος, τότε $|E(n)| \leq \phi(n)/2$.

Ἀπόδειξη. Βασίζεται στὰ ἑξῆς:

(α') $E(n)$ εἶναι ὑποομάδα τῆς πολλαπλασιαστικῆς ὁμάδας $\mathbb{Z}_n^*$.
Ἡ ἀπόδειξη ἀφήνεται ὡς ἄσκηση.

(β') Κάθε ἀριθμὸς Carmichael εἶναι ἐλεύθερος τετραγώνου.
Πράγματι, ἔστω k ἀριθμὸς Carmichael καὶ $k = p^r m$, ὅπου ὁ p εἶναι πρῶτος, $r \geq 2$ καὶ $(m, p) = 1$. Ἔστω τώρα g γεννήτορας τοῦ $\mathbb{F}_{p^2}^*$. Μὲ τὸ κινέζικο θεώρημα βρίσκομε b, τέτοιο ὥστε $b \equiv g \pmod{p^2}$ καὶ $b \equiv 1 \pmod{m}$. Ἀπὸ αὐτὲς τὶς σχέσεις ἕπεται ὅτι ὁ b εἶναι πρῶτος πρὸς τὸν p καὶ πρὸς τὸν m, ἄρα

πρῶτος πρὸς τὸν k. Ἀφοῦ ὁ k εἶναι ἀριθμὸς Carmichael, $b^{k-1} \equiv 1 \pmod{k}$, ἄρα καὶ $b^{k-1} \equiv 1 \pmod{p^2}$. Ἀλλὰ ἡ τάξη τοῦ b στὴν ὁμάδα $\mathbb{F}_{p^2}^*$ εἶναι $\phi(p^2)$, ἄρα $\phi(p^2)|(k-1)$. Ἐπειδὴ $p|\phi(p^2)$, ἕπετι ὅτι $p|(k-1)$, προφανῶς ἄτοπο, ἀφοῦ $p|k$.

(γ') $E(n)$ εἶναι *γνήσια* ὑποομάδα τῆς πολλαπλασιαστικῆς ὁμάδας $\mathbb{Z}_n^*$.
Ἂν δὲν συνέβαινε αὐτό, θὰ ἦταν $E(n) = \mathbb{Z}_n^*$, ἄρα ὁ n θὰ ἦταν ἀριθμὸς Carmichael. Πράγματι, διότι τότε ὁ n θὰ ἦταν ψευδοπρῶτος Euler γιὰ κάθε $a \in \mathbb{Z}_n^*$, ἄρα $a^{(n-1)/2} \equiv \left(\frac{a}{n}\right) \pmod{n}$, ὁπότε $a^{n-1} \equiv 1 \pmod{n}$ γιὰ κάθε $a \in \mathbb{Z}_n^*$. Ἐπειδὴ ὁ n εἶναι σύνθετος καί, ἐπιπλέον εἶναι ἐλεύθερος τετραγώνου, λόγῳ τοῦ (β'), μποροῦμε νὰ γράψομε $n = pm$, ὅπου p πρῶτος καὶ $m > 1$ πρῶτος πρὸς τὸν p. Ἐπιλέγομε ἕνα b, τετραγωνικὸ ἀνισοϋπόλοιπο $\bmod p$ καὶ μετά, μὲ τὸ κινέζικο θεώρημα, βρίσκομε a τέτοιο ὥστε $a \equiv b \pmod{p}$ καὶ $a \equiv 1 \pmod{m}$. Ἄρα,

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p}\right)\left(\frac{a}{m}\right) = \left(\frac{b}{p}\right)\left(\frac{1}{m}\right) = (-1)(+1) = -1\,,$$

ὁπότε $a^{(n-1)/2} \equiv \left(\frac{a}{n}\right) = -1 \pmod{n}$. Ἀλλὰ τότε καὶ $a^{(n-1)/2} \equiv -1 \pmod{m}$, ἄτοπο, ἀφοῦ $a \equiv 1 \pmod{m}$.

Ἄσκηση 10. *Ἀποδεῖξτε ὅτι, ἂν ὁ n εἶναι ψευδοπρῶτος Euler ὡς πρὸς τὸν b, τότε εἶναι ψευδοπρῶτος Euler καὶ ὡς πρὸς τοὺς $-b$ καὶ $b^{-1} \pmod{n}$. Ἐπίσης, ἂν ὁ n εἶναι ψευδοπρῶτος Euler ὡς πρὸς τοὺς b_1 καὶ b_2, τότε εἶναι ψευδοπρῶτος Euler καὶ ὡς πρὸς τὸν $b_1 b_2$.*

Ἄσκηση 11. *Ἀποδεῖξτε ὅτι, ἂν ὁ n εἶναι ψευδοπρῶτος ὡς πρὸς τὸν 2, τότε ὁ $N = 2^n - 1$ εἶναι ψευδοπρῶτος Euler ὡς πρὸς τὸν 2.*

Τώρα ὁρίζομε μία ἰσχυρότερη κατηγορία ψευδοπρώτων.

Ὁρισμός 3.6. *Ἔστω ἀκέραιος $n \geq 3$, τὸν ὁποῖο γράφομε ὡς $n = 1 + 2^s t$ μὲ $s \geq 1$ καὶ t περιττό. Γιὰ b ἀκέραιο πρῶτο πρὸς τὸν n θεωροῦμε τὴ συνθήκη*

$$\begin{aligned} S(b,n) \quad : \quad & b^t \equiv 1 \pmod{n} \\ & \text{εἴτε } \exists r \in \{1,\ldots,s\} \text{ τέτοιο ὥστε } b^{2^{r-1}t} \equiv -1 \pmod{n}. \end{aligned}$$

Ἂν ὁ n εἶναι περιττὸς σύνθετος καὶ ἡ συνθήκη $S(n,b)$ εἶναι ἀληθής, ὁ n λέγεται ἰσχυρὸς ψευδοπρῶτος ὡς πρὸς τὸν b.

Ἄσκηση 12. *Ἔστω θετικὸς ἀκέραιος $n \equiv 3 \pmod 4$ καὶ ἀκέραιος b πρῶτος πρὸς τὸν n. Τότε, ὁ n εἶναι ἰσχυρὸς ψευδοπρῶτος ὡς πρὸς τὸν b ἄν, καὶ μόνο ἄν, ὁ n εἶναι ψευδοπρῶτος Euler ὡς πρὸς τὸν b.*
(Ὑπόδειξη: Παρατηρῆστε ὅτι $\left(\frac{b}{n}\right) = \left(\frac{b}{n}\right)^{(n-1)/2}$.)
Συνδυᾶστε μὲ τὴν ἄσκηση 11 γιὰ ν' ἀποδείξετε ὅτι, ἂν ὁ n εἶναι ψευδοπρῶτος ὡς πρὸς τὸν 2, τότε ὁ $N = 2^n - 1$ εἶναι ἰσχυρὸς ψευδοπρῶτος Euler ὡς πρὸς τὸν 2.

Πρόταση 3.7. *Ἂν ὁ περιττὸς ἀκέραιος n εἶναι ἰσχυρὸς ψευδοπρῶτος ὡς πρὸς τὸν ἀκέραιο b ($\gcd(b, n) = 1$), τότε εἶναι καὶ ψευδοπρῶτος Euler ὡς πρὸς τὸν b.*

Ἀπόδειξη. Ἔστω ὅτι $n = 1 + 2^s t$, ὅπου $s \geq 1$ καὶ t περιττός. Ὑποθέτομε ὅτι ὁ n εἶναι ἰσχυρὸς ψευδοπρῶτος ὡς πρὸς τὸν b, δηλαδή, ἡ συνθήκη $S(n, b)$ ἀληθεύει.

Ἂν $b^t \equiv 1 \pmod n$, τότε, προφανῶς, $b^{2^{s-1}t} \equiv 1 \pmod n$, δηλαδή, $b^{(n-1)/2} \equiv 1 \pmod n$. Μένει νὰ δείξομε ὅτι $\left(\frac{b}{n}\right) = 1$ καὶ αὐτὸ τὸ ἐπιτυγχάνομε ὡς ἑξῆς: $\left(\frac{b}{n}\right)^t = \left(\frac{b^t}{n}\right) = \left(\frac{1}{n}\right) = 1$. Ἐπειδὴ $\left(\frac{b}{n}\right) \in \{-1, 1\}$ καὶ ὁ t εἶναι περιττός, ἕπεται ὅτι $\left(\frac{b}{n}\right) = 1$.

Ἔστω τώρα ὅτι $b^{2^{r-1}t} \equiv -1 \pmod n$ γιὰ κάποιο $r \in \{1, \ldots, s\}$.

Γιὰ κάθε πρῶτο διαιρέτη p τοῦ n ἰσχύει $p \equiv 1 \pmod{2^r}$ καὶ

$$\left(\frac{b}{p}\right) = \begin{cases} -1 & \text{ἂν } p \equiv 1 + 2^r \pmod{2^{r+1}} \\ +1 & \text{ἂν } p \equiv 1 \pmod{2^{r+1}} \end{cases}.$$

Ἀπόδειξη τοῦ ἰσχυρισμοῦ. Θέτομε $p = 1 + 2^{s'}t'$, ὅπου t' περιττός. Λόγῳ τῆς $b^{2^{r-1}t} \equiv -1 \pmod n$ ἰσχύει καὶ ἡ $b^{2^{r-1}t} \equiv -1 \pmod p$, ἄρα καὶ ἡ $b^{2^{r-1}tt'} \equiv -1 \pmod p$. Ἐπίσης, ἀπὸ τὸ θεώρημα τοῦ Fermat, $b^{2^{s'}t'} \equiv 1 \pmod p$, ὁπότε, ἂν ἦταν $s' \leq r - 1$, τότε μὲ ὑψώσεις στὸ τετράγωνο θὰ ὁδηγούμαστε στὴν $b^{2^{r-1}t'} \equiv 1 \pmod p$, ἄρα καὶ στὴν $b^{2^{r-1}t't} \equiv 1 \pmod p$, ἀντίφαση. Συμπεραίνομε, λοιπόν, ὅτι $s' \geq r$, ἄρα $p \equiv 1 \pmod{2^r}$. Τώρα εἶναι ἁπλῆ ἄσκηση νὰ δείξει κανεὶς ὅτι, ἂν $s' > r$, τότε $p \equiv 1 \pmod{2^{r+1}}$, ἐνῶ ἂν $s' = r$, τότε $p \equiv 1 + 2^r \pmod{2^{r+1}}$. Συνεπῶς, ἔχομε:

$$\begin{aligned} \left(\frac{b}{p}\right)^t &\equiv b^{\frac{p-1}{2}t} \pmod p \\ &= b^{2^{s'-1}tt'} \begin{cases} b^{2^{r-1}tt'} \equiv (-1)^{t'} = -1 \pmod p & \text{ἂν } s' = r \\ (b^{2^{r-1}t})^{2^{s'-r}t'} \equiv (-1)^{2^{s'-r}t'} = +1 \pmod p & \text{ἂν } s' > r \end{cases}. \end{aligned}$$

Ἐπειδὴ ὁ t εἶναι περιττός, ἕπεται τὸ δεύτερο μέρος τοῦ ἰσχυρισμοῦ μας.

Τώρα, ἀναλύομε τὸν n σὲ πρώτους παράγοντες $n = p_1 \cdots p_k p_{k+1} \cdots p_m$ ($p_1, \ldots, p_m$ ὄχι ἀναγκαστικὰ διαφορετικοί), ὅπου $p_i \equiv 1 + 2^r \pmod{2^{r+1}}$ γιὰ $i = 1, \ldots, k$ καὶ $p_i \equiv 1 \pmod{2^{r+1}}$ γιὰ $i > k$. Τότε, σύμφωνα μὲ ὅ,τι ἀποδείξαμε παραπάνω,

$$\left(\frac{b}{n}\right) = \left(\frac{b}{p_1}\right) \cdots \left(\frac{b}{p_k}\right) \left(\frac{b}{p_{k+1}}\right) \cdot \left(\frac{b}{p_m}\right) = (-1)^k \,.$$

Ἀφ' ἑτέρου,

$$1 + 2^s t = n = p_1 \cdots p_k p_{k+1} \cdots p_m \equiv (1 + 2^r)^k \equiv 1 + 2^r k \pmod{2^{r+1}} \,,$$

ὅπου ἡ δεξιώτερη ἰσοτιμία εἶναι σαφὴς ἂν ἀναπτύξομε τὸ διώνυμο τοῦ Νεύτωνα $(1 + 2^r)^k$. Ἀπὸ τὴν τελευταία σχέση εἶναι φανερὸ ὅτι, ἂν $r < s$, τότε ὁ k εἶναι ἄρτιος, ἄρα $\left(\frac{b}{n}\right) = +1$. Ὅμως, καὶ

$$b^{(n-1)/2} = b^{2^{s-1}t} = (b^{2^{r-1}t})^{2^{s-r}} \equiv (-1)^{2^{s-r}} = 1 \pmod{n} \,,$$

ποὺ εἶναι τὸ ἀποδεικτέο. Ἂν, πάλι, $r = s$, τότε ὁ k εἶναι περιττός, ὁπότε $\left(\frac{b}{n}\right) = -1$ καθὼς καὶ

$$b^{(n-1)/2} = b^{2^{s-1}t} = b^{2^{r-1}t} \equiv -1 \pmod{n} \,.$$

Ἄσκηση 13. *Ἀπὸ τὶς προτάσεις 3.3 καὶ 3.7 περιμένει κανείς, οἱ b ὡς πρὸς τοὺς ὁποίους κάποιος δεδομένος n εἶναι ψευδοπρῶτος, νὰ εἶναι περισσότεροι ἀπὸ αὐτοὺς ὡς πρὸς τοὺς ὁποίους εἶναι ψευδοπρῶτος Euler, καὶ αὐτοί, μὲ τὴ σειρά τους, νὰ εἶναι περισσότεροι ἀπὸ τοὺς b ὡς πρὸς τοὺς ὁποίους ὁ n εἶναι ἰσχυρὸς ψευδοπρῶτος. Χαρακτηριστικὸ παράδειγμα εἶναι ὁ 561, ποὺ εἶναι ἀριθμὸς τοῦ Carmichael. Ὑπολογῖστε τὸ πλῆθος τῶν b ὡς πρὸς τοὺς ὁποίους ὁ 561 εἶναι (1) ψευδοπρῶτος, (2) ψευδοπρῶτος Euler καὶ (3) ἰσχυρὸς ψευδοπρῶτος.*

Ἄσκηση 14. *Ἀποδεῖξτε ὅτι, ἂν ὁ n εἶναι ἰσχυρὸς ψευδοπρῶτος ὡς πρὸς τὸν b, τότε εἶναι ἰσχυρὸς ψευδοπρῶτος καὶ ὡς πρὸς τοὺς $-b$ καὶ $b^{-1} \pmod{n}$. Ὅμως, ἂν ὁ n εἶναι ἰσχυρὸς ψευδοπρῶτος ὡς πρὸς τὸν b_1 καὶ τὸν b_2, τότε μπορεῖ καὶ νὰ μὴν εἶναι ψευδοπρῶτος ὡς πρὸς τὸν $b_1 b_2$, καθὼς δείχνει τὸ ἑξῆς παράδειγμα: $n = 65, b_1 = 8, b_2 = 18$. Διαπιστῶστε το κι ἐσεῖς.*

Ἄσκηση 15. *Ἔστω $n = p^r$, ὅπου ὁ p εἶναι πρῶτος καὶ $r > 1$. Ἀποδεῖξτε ὅτι, ὁ n εἶναι ἰσχυρὸς ψευδοπρῶτος ὡς πρὸς τὸν b ἂν, καὶ μόνο ἂν, ὁ n εἶναι ψευδοπρῶτος ὡς πρὸς τὸν b.*

Ἄσκηση 16. *(α΄) Ἔστω $n = pq$, ὅπου οἱ p, q εἶναι διαφορετικοὶ περιττοὶ πρῶτοι. Ἂν ὁ n εἶναι ψευδοπρῶτος ὡς πρὸς τὸν b καὶ ὁ n δὲν εἶναι ἰσχυρὸς ψευδοπρῶτος ὡς πρὸς τὸν b, τότε δεῖξτε πῶς μπορεῖ κανεὶς νὰ ὑπολογίσει εὔκολα ἕνα μὴ τετριμμένο παράγοντα τοῦ n.*

Ὑπόδειξη. Ἔστω $n - 1 = 2^s t$, ὅπου t περιττὸς καὶ k ὁ ἐλάχιστος θετικὸς ἀκέραιος, τέτοιος ὥστε $b^{2^k t} \equiv 1 \pmod{n}$. Ἂν θέσομε $c = b^{2^{k-1} t}$, τότε παρατηρῆστε ὅτι $c^2 \equiv 1 \pmod{n}$, ἐνῶ $c \not\equiv \pm 1 \pmod{n}$· συνεπῶς ἕνας μὴ τετριμμένος διαιρέτης τοῦ n εἶναι ὁ $(c + 1, n)$.

(β΄) Τί πρέπει νὰ προσέξει κανεὶς, ὅταν ἐπιλέγει τὸ δημόσιο κλειδί του $n = pq$ στὸ κρυπτοσύστημα RSA;

Ὑπόδειξη. Σύμφωνα μὲ τὴν ἄσκηση 8(α΄), ὅταν ὁ $(p - 1, q - 1)$ εἶναι μικρός, ἡ πιθανότητα νὰ πετύχει κανεὶς b, ὡς πρὸς τὸν ὁποῖον ὁ n νὰ εἶναι ψευδοπρῶτος, εἶναι ἀπειροελάχιστη.

Πιστοποίηση Miller-Rabin-Selfridge 3.8. *Ἔστω περιττὸς ἀκέραιος $n \geq 3$, τὸν ὁποῖο γράφομε ὡς $n = 1 + 2^s t$ μὲ $s \geq 1$ καὶ t περιττό, καὶ ἀκέραια παράμετρος r. Ὁ παρακάτω ἀλγόριθμος, ὁ ὁποῖος ἀπαντᾶ στὸ ἐρώτημα «εἶναι ὁ n πρῶτος;», εἶναι (α΄) θετικὰ προκατειλημμένος Monte Carlo μὲ πιθανότητα λάθους 2^{-2r} καὶ (β΄) ἀρνητικὰ προκατειλημμένος.*

1. *Διάλεξε τυχαῖο ἀκέραιο b στὸ διάστημα $[2, n - 2]$.*
2. *Ἂν $\gcd(b, n) > 1$, τότε ἡ ἀπάντηση εἶναι* ΟΧΙ *καὶ ὁ ἀλγόριθμος σταματᾶ. Διαφορετικά, προχώρησε στὸ ἑπόμενο βῆμα.*
3. *Ἂν $b^t \equiv \pm 1 \pmod{n}$, τότε πήγαινε στὸ βῆμα 5. Διαφορετικά, προχώρησε στὸ ἑπόμενο βῆμα.*
4. *Ὑπολόγισε διαδοχικὰ $b^{2t}, b^{2^2 t}, \ldots, b^{2^{s-1} t} \pmod{n}$, ὅσο οἱ τιμὲς παραμένουν $\not\equiv -1 \pmod{n}$. Ἂν ὅλες οἱ $s - 1$ παραπάνω τιμὲς εἶναι $\not\equiv -1 \pmod{n}$, ἡ ἀπάντηση εἶναι* ΟΧΙ *καὶ ὁ ἀλγόριθμος σταματᾶ. Διαφορετικά, πήγαινε στὸ ἑπόμενο βῆμα.*
5. *$r \leftarrow r - 1$. Ἂν $r = 0$, τότε ἡ ἀπάντηση εἶναι* ΝΑΙ *καὶ ὁ ἀλγόριθμος σταματᾶ. Διαφορετικά, πήγαινε στὸ βῆμα 1.*

Ἡ ἀπόδειξη στηρίζεται στὸ ὅτι, γιὰ $n > 3$ περιττὸ σύνθετο ἀκέραιο, τὸ πλῆθος τῶν ἀκεραίων b τοῦ διαστήματος $[1, n - 1]$, ὡς πρὸς τοῦς ὁποίους ὁ n εἶναι ἰσχυρὸς ψευδοπρῶτος εἶναι, τὸ πολύ, $(n - 1)/4$. Βλ. Πρόταση V.1.7 καὶ τὴν ἀπόδειξή της[8] στὸ βιβλίο [2].

[8] Στοιχειώδης, ἀλλὰ ἀρκετὰ δύσκολη.

Αναφορὲς

[1] W.R. Alford, A. Granville, C. Pomerance, There are infinitely many Carmichael numbers, *Ann. Math.* **140** (1994), 703-722.

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

[3] R. Schoof, Elliptic curves over finite fields and the computation of square roots $\mathrm{mod} p$, *Math. Comp.* **44** (1985), 483-494.

[4] J.H. Silverman, J. Tate, *Rational Points on Elliptic Curves*, Undergraduate Texts in Mathematics, Springer-Verlag, Berlin and New York, 1992.