Βασικὴ Ὑπολογιστικὴ Ἀριθμοθεωρία ἀπαραίτητη στὴν Κρυπτολογία

Καθηγητὴς Ν.Γ. Τζανάκης

Τελευταία ἐνημέρωση 9/10/2007

1 Κόστος ὑπολογισμῶν

1.1 Οἱ βασικὲς πράξεις

Δουλεύομε, ὅπως ὁ ὑπολογιστής, μὲ δυαδικοὺς ἀριθμούς. Στοιχειώδεις πράξεις, δηλαδή, πράξεις μὲ μοναδιαῖο κόστος ὑπολογιστικοῦ χρόνου, μεταξὺ δύο bits εἶναι οἱ παρακάτω, ὅπου ὁ τόνος δίπλα σὲ ἕνα ψηφίο σημαίνει ὅτι δημιουργεῖται καὶ κρατούμενο:

Πρόσθεση δίχως κρατούμενο ἀπὸ μεταφορά					Πρόσθεση μὲ κρατούμενο ἀπὸ μεταφορά				
		0	1	0	1		0	1	0	1
	$+$	0	0	1	1	$+$	0	0	1	1
		0	1	1	$0'$		1	$0'$	$0'$	$1'$

Ἀφαίρεση δίχως κρατούμενο ἀπὸ μεταφορά					Ἀφαίρεση μὲ κρατούμενο ἀπὸ μεταφορά				
		0	1	0	1		0	1	0	1
	$-$	0	0	1	1	$-$	0	0	1	1
		0	1	$1'$	0		$1'$	0	$0'$	$1'$

Πολ/σιασμὸς δίχως κρατούμενο ἀπὸ μεταφορά					Πολ/σιασμὸς μὲ κρατούμενο ἀπὸ μεταφορά (δὲν χρειάζεται στὴν πράξη)				
		0	1	0	1		0	1	0	1
	$\times$	0	0	1	1	$\times$	0	0	1	1
		0	0	0	1		1	1	1	$0'$

- Σύγκριση δύο bits .

Στὶς παρακάτω προτάσεις, οἱ λογάριθμοι μπορεῖ νὰ εἶναι ὡς πρὸς ὁποιαδήποτε βάση, ἐπειδὴ περιέχονται μέσα σὲ σύμβολο $O(\cdot)$. Πράγματι, λόγῳ τῆς σχέσεως $\log_a x = \log_a b \log_b x$, οἱ $\log_a x$ καὶ $\log_b x$ διαφέρουν κατὰ σταθερά, ἡ ὁποία δὲν ἐπηρρεάζει τὸ σύμβολο O.

Πρόταση 1.1.1. *Ὑποθέτομε ὅτι ὁ a εἶναι N-bit ἀκέραιος καὶ ὁ b εἶναι n-bit ἀκέραιος. Τὸ κόστος γιὰ τὸν ὑπολογισμὸ τοῦ $a \pm b$ εἶναι $O(\max(N,n))$, ἐνῶ τὸ κόστος ὑπολογισμοῦ τοῦ ab εἶναι $O(Nn)$. Τὸ κόστος γιὰ τὴ σύγκριση τῶν a, b εἶναι $O(\min(N,n))$. Ἄρα, συναρτήσει τῶν a, b, τὸ κόστος γιὰ τὸν ὑπολογισμὸ τοῦ $a \pm b$ εἶναι $O(\max(\log a, \log b))$, τὸ κόστος ὑπολογισμοῦ τοῦ ab εἶναι $O(\log a \log b)$ καὶ τὸ κόστος συγκρίσεως τῶν a, b εἶναι $O(\min(\log a, \log b))$.*

Ἄσκηση 1. *Ἔστω ὅτι οἱ $a_1, \ldots, a_m$ εἶναι n-bit ἀκέραιοι. Γιὰ κάθε $k = 2, \ldots, m$ θέτομε $S_k = a_1 + \cdots + a_k$. Ἀποδεῖξτε ὅτι, ἂν $2^i \leq m$ τότε $S_{2^i} < 2^{n+i}$. Μετά, ἀποδεῖξτε ὅτι, γιὰ κάθε i τέτοιο ὥστε $2^i \leq m$ καὶ γιὰ ὅλα τὰ k τέτοια ὥστε $2^{i-1} < k \leq 2^i$, ὁ S_k εἶναι $(n+i)$-bit ἀκέραιος. Μὲ τὴ βοήθεια αὐτῶν ἀποδεῖξτε ὅτι τὸ κόστος ὑπολογισμοῦ τοῦ $a_1 + \cdots + a_m$ εἶναι $(O(mn)$.*

Ἄσκηση 2. *Ἔστω ὅτι A, B εἶναι δύο $m \times m$ πίνακες μὲ n-bit ἀριθμούς. Ἀποδεῖξτε ὅτι γιὰ τὸν πολλαπλασιασμὸ AB ἀπαιτοῦνται $O(m^3 n^2)$ βήματα.*

Γιὰ τὴν εὐκλείδεια διαίρεση (Θεώρημα 2.1.1) δύο ἀκεραίων a καὶ b, εἶναι πολλὲς φορὲς χρήσιμο νὰ φανταζόμαστε ὅτι τὴν ἐκτελοῦμε, ὅπως στὸ σχολεῖο, "μὲ τὴ γωνία", συμπληρώνοντας τὸ ἕνα μετὰ τὸ ἄλλο τὰ ψηφία τοῦ διαιρέτη. Παρατηρῆστε ὅτι τὰ βήματα ποὺ γίνονται, εἶναι, προφανῶς, τόσα ὅσα καὶ τὰ ψηφία τοῦ πηλίκου τῆς διαίρεσης, ἄρα, ἀφοῦ τὸ πηλίκο εἶναι $[a/b]$, τὸ πλῆθος τῶν βημάτων εἶναι $O(\log_2(a/b)) = O(\log(a/b))$. Στὴν περίπτωσή μας, ποὺ οἱ ἀριθμοὶ εἶναι γραμμένοι στὸ δυαδικὸ σύστημα, τὰ πράγματα εἶναι πολὺ ἁπλά, διότι, ἕνας ἀριθμὸς μὲ n δυαδικὰ ψηφία, "χωράει" σ' ἕναν ἄλλο δυαδικὸ ἀριθμὸ n ψηφίων μία ἢ καμμία φορά[1], ὅπως φαίνεται ἀπὸ τὴν ἑπόμενη ἄσκηση.

Ἄσκηση 3. *Θὰ λέμε ὅτι ἕνας n-bit ἀκέραιος εἶναι γνήσιος n-bit ἀκέραιος ἂν τὸ ἀριστερώτερο ψηφίο του εἶναι 1. Ἔστω τώρα b ἕνας γνήσιος n-bit ἀκέραιος καὶ x ἕνας n-bit ἀκέραιος.*
(i) Ἰσχύει $x < 2b$, ἄρα ὁ b χωράει στὸν x μία ἢ καμμία φορά.
(ii) Ἔστω $x < b$ καὶ $x = \overline{s_{n-1} \ldots s_1 s_0}$ ($s_i \in \{0,1\}$ γιὰ κάθε i) καὶ $t \in \{0,1\}$. Τότε $\overline{s_{n-1} \ldots s_1 s_0 t} < 2b$, ἄρα ὁ γνήσιος n-bit ἀκέραιος b χωράει στὸν $(n+1)$-bit ἀκέραιο $\overline{s_{n-1} \ldots s_1 s_0 t}$ μία ἢ καμμία φορά.
Μὲ βάση τὰ παραπάνω δεῖξτε ὅτι ἡ ἐκτέλεση τῆς "διαίρεσης μὲ γωνία" ἑνὸς ἀκεραίου a μὲ ἕνα γνήσιο n-bit ἀκέραιο b ὑπολογίζει ἁπλούστατα τὰ ψηφία (bits) τοῦ πηλίκου ὡς ἑξῆς (ὑποθέτομε $a \geq b$): Ξεκινοῦμε μὲ τὸ ἀριστερώτερο n-bit τμῆμα τοῦ a ἂν αὐτὸ εἶναι $\geq b$ ἢ μὲ τὸ ἀριστερώτερο $(n+1)$-bit τμῆμα τοῦ a, στὴν ἀντίθετη περίπτωση. Γράφομε τὸ ψηφίο 1 στὸ πηλίκο, καὶ στὶς δύο περιπτώσεις. Γιὰ καθένα ἀπὸ τὰ ἑπόμενα

[1] Δηλαδή, τὸ πηλίκο τῆς εὐκλείδειας διαίρεσής τους εἶναι 0 ἢ 1.

βήματα: Ἔστω ὅτι σὲ κάποιο βῆμα ἔχομε τὸ μερικὸ ὑπόλοιπο v. Αὐτὸς εἶναι ἕνας (ὄχι κατ' ἀνάγκη γνήσιος) n-bit ἀκέραιος. "Κατεβάζομε ἕνα ψηφίο t τοῦ διαιρετέου καὶ τὸ "κολλᾶμε" στὰ δεξιὰ τοῦ v, ὁπότε δημιουργεῖται ἕνας (ὄχι κατ' ἀνάγκη γνήσιος) $(n+1)$-bit ἀκέραιος v'. Ἂν $v' < b$ τότε "κολλᾶμε" στὰ δεξιὰ τοῦ πηλίκου τὸ (νέο) ψηφίο 0, διαφορετικά, τὸ 1.

Βασισμένοι στὴν παραπάνω ἄσκηση μποροῦμε ν' ἀποδείξομε τὴν ἑξῆς

Πρόταση 1.1.2. *Ἂν ὁ a εἶναι N-bit ἀκέραιος καὶ ὁ b εἶναι n-bit ἀκέραιος καὶ $a \geq b$, τότε τὸ κόστος ὑπολογισμοῦ τοῦ πηλίκου καὶ τοῦ ὑπολοίπου τῆς εὐκλείδειας διαίρεσης τοῦ a διὰ b εἶναι $O(\log b \log(a/b)) = O(n(N-n))$.*

Ἡ ἀπόδειξή της εἶναι πολὺ ἁπλή, ἂν φαντασθεῖ κανεὶς ὅτι οἱ a, b εἶναι δυαδικοί, τῶν ὁποίων ἡ διαίρεση γίνεται "μὲ τὴ γωνία". Τὰ ἐπαναληπτικὰ βήματα εἶναι, προφανῶς, τόσα ὅσα καὶ τὰ bits τοῦ q, δηλαδή, $[a/b]$, ἄρα $O(\log(a/b))$. Ἀλλὰ σὲ κάθε ἐπαναληπτικὸ βῆμα ἐκτελεῖται μία σύγκριση καὶ μία, τὸ πολύ, ἀφαίρεση δύο ἀριθμῶν μήκους ἴσου μὲ αὐτὸ τοῦ b, ὁπότε τὸ κόστος σὲ κάθε ἐπαναληπτικὸ βῆμα εἶναι $O(\log b)$.

Ἡ παρακάτω πρόταση εἶναι πόρισμα τῆς προηγούμενης.

Πρόταση 1.1.3. *Ἔστω ὅτι $a \geq b > 0$ καὶ q, r, ἀντιστοίχως, τὸ πηλίκο καὶ τὸ ὑπόλοιπο τῆς εὐκλείδειας διαίρεσης τοῦ a διὰ b (βλ. Θεώρημα 2.1.1). Τὸ κόστος ὑπολογισμοῦ τῶν q, r εἶναι $O(\log b \log a)$.*

Ἄσκηση 4. *Πᾶρτε ἕνα τυχαῖο 10-bit ἀκέραιο a καὶ ἕνα 4-bit ἀκέραιο b καὶ ἐκτελέστε τὴ διαίρεση a διὰ b μὲ τὸν «ἀλγόριθμο τῆς γωνίας».*

2 Βασικοὶ Ἀλγόριθμοι

2.1 Εὐκλείδειος Ἀλγόριθμος

Θεώρημα 2.1.1. *Γιὰ κάθε ζεῦγος ἀκεραίων $a \geq b > 0$ ὑπάρχει ἕνα ἀκριβῶς ζεῦγος ἀκεραίων (q, r), ποὺ ἱκανοποιεῖ τὴ συνθήκη*

$$a = bq + r \quad \text{καὶ} \quad 0 \leq r \leq b \ .$$

Πιὸ συγκεκριμένα, $q = \left\lfloor \dfrac{a}{b} \right\rfloor$. Ὁ q εἶναι τὸ πηλίκο καὶ ὁ r τὸ ὑπόλοιπο τῆς εὐκλείδειας διαίρεσης τοῦ a διὰ b.

Γιὰ κάθε $x \in \mathbb{R}$, τὸ σύμβολο $\lfloor x \rfloor$ συμβολίζει τὸν μέγιστο ἀκέραιο, ὁ ὁποῖος δὲν ὑπερβαίνει τὸν x. Γιὰ παράδειγμα, $\lfloor 3{,}12 \rfloor = 3$ καὶ γιὰ κάθε ἀκέραιο n, $\lfloor n \rfloor = n$.

Πρόταση 2.1.2. *Μὲ τὶς ὑποθέσεις καὶ τὸν συμβολισμὸ τοῦ θεωρήματος 2.1.1,* $\gcd(a, b) = \gcd(b, r)$.

Συμβολισμός: Στὰ παρακάτω, γιὰ κάθε ζευγάρι (a, b) ὅπως στὸ Θεώρημα 2.1.1 θέτομε $E(a, b) = (q, r)$.

Ἀλγόριθμος 2.1.3. *Ἔστω ἕνα ζευγάρι ἀκεραίων $a \geq b > 0$. Ὁρίζομε $r_0 = a$, $r_1 = b$ καί, ἐπαναληπτικά, γιὰ $i = 1, 2, \ldots$ θέτομε $E(r_{i-1}, r_i) = (q_{i+1}, r_{i+1})$. Τότε, σὲ κάποιο βῆμα, ἔστω $i = n \geq 2$, εἶναι $r_{n+1} = 0$, ἐνῶ $0 < r_n < r_{n-1} < \ldots < r_2 < r_1 = b$. Τότε, $\gcd(a, b) = r_n$. Ἀκόμη, $n < 2 \log_2 b + 1$.*

Ἡ ἀνισότητα γιὰ τὸ n δείχνει ὅτι ὁ ἀλγόριθμος εἶναι πολὺ γρήγορος. Ἡ ἀνισότητα αὐτὴ ἀποδεικνύεται εὔκολα, ἂν ἀποδείξετε πρῶτα ὅτι γιὰ κάθε $i = 1, \ldots, n-1$ ἰσχύει $r_{i+1} < r_{i-1}/2$. Αὐτή ἡ τελευταία ἀνισότητα, μὲ τὴ σειρά της, ἀποδεικνύεται ἂν ξεχωρίσετε τὶς περιπτώσεις $r_i \leq r_{i-1}/2$ καὶ $r_i > r_{i-1}/2$ καί, στὴ δεύτερη περίπτωση, νὰ κάνετε χρήση τῆς σχέσης $r_{i+1} = r_{i-1} - r_i q_{i+1}$. %

Ἄσκηση 5. *Μὲ τὸν συμβολισμὸ καὶ τὶς ὑποθέσεις τοῦ Ἀλγορίθμου 2.1.3, ἀποδεῖξτε ὅτι $q_2 q_3 \cdots q_n q_{n+1} \leq a$. Μὲ τὴ βοήθεια αὐτῆς τῆς σχέσης καὶ τῆς Πρότασης 1.1.3, ἀποδεῖξτε μετά, ὅτι τὸ κόστος τῆς ὅλης διαδικασίας τοῦ Εὐκλειδείου Ἀλγορίθμου εἶναι $O(\log a \log b)$.*

Ἀλγόριθμος 2.1.4. *(Μὲ τὸν συμβολισμὸ τοῦ θεωρήματος 2.1.1.)*
Ὁ ἑξῆς ἀλγόριθμος ὑπολογίζει ἀκεραίους x, y, τέτοιους ὥστε $ax + by = \gcd(a, b)$: Ὁρίζομε $s_{-1} = 1$, $s_0 = 1$ καὶ ἀναδρομικά, γιὰ $i = 1, \ldots, n$,

$$s_i = s_{i-2} - s_{i-1} q_{n-i+2} \ .$$

Τότε, $s_{n-1} a + s_n b = \gcd(a, b)$.

Ἀπόδειξη: Δεῖξτε ἐπαγωγικὰ ὅτι, γιὰ $i = 0, \ldots, n$ ἰσχύει $r_n = s_i r_{n-i+1} + s_{i-1} r_{n-i}$.

Ἄσκηση 6. *Μὲ τὸν συμβολισμὸ καὶ τὶς ὑποθέσεις τῶν 2.1.3 καὶ 2.1.4, ἀποδεῖξτε πρῶτα ὅτι, γιὰ $i = 0, \ldots, n$ τὸ πρόσημο τοῦ s_i εἶναι ἐναλλὰξ $(-1)^i$ καὶ $|s_{i-1}| \leq |s_i|$ γιὰ $i = 1, \ldots n$. Μετά, ἀποδεῖξτε ὅτι $|s_i| = |s_{i-2}| + |s_i| q_{n-i+2}$ γιὰ ὅλα τὰ $i = 2, \ldots, n$. Τέλος, ἀποδεῖξτε ὅτι τὸ κόστος ὑπολογισμοῦ τῶν s_{n-1}, s_n εἶναι $\log a \log b$.*

2.2 Ὕψωση σὲ δύναμη, εὕρεση ἀντιστρόφου, ταυτόχρονες ἰσοδυναμίες

Ἀλγόριθμος 2.2.1. *Ἔστω $(A, \cdot)$ ἀντιμεταθετικὴ ἡμιομάδα μὲ οὐδέτερο στοιχεῖο, συμβολιζόμενο 1 (δηλαδή, ἰσχύουν τὰ ἀξιώματα τῆς ἀβελιανῆς ὁμάδας ἐκτός, ἴσως, ἀπὸ τὴν ὕπαρξη ἀντιστρόφου). Τότε, γιὰ δοθὲν $a \in A$ καὶ ἐκθέτη $n > 1$, ὁ παρακάτω ἀλγόριθμος ὑπολογίζει τὸ a^n κάνοντας πράξεις, ποὺ τὸ πλῆθος τους εἶναι τῆς τάξεως $\log_2 n$:*
Χρησιμοποιεῖς τὶς βοηθητικὲς μεταβλητὲς δ, x καὶ ϵ.
Ἀρχικὸ βῆμα: $\delta \leftarrow 1$, $x \leftarrow a$, $\epsilon \leftarrow n$.

Ἐνόσῳ τὸ $\epsilon > 1$ ΚΑΝΕ*:*
ΑΝ ϵ *περιττός,* $\delta \leftarrow \delta \cdot x$ ΤΕΛΟΣ ΑΝ
$x \leftarrow x^2, \quad \epsilon \leftarrow \lfloor \epsilon/2 \rfloor$.
ΤΕΛΟΣ ΚΑΝΕ
$\delta \leftarrow \delta x$
Τύπωσε δ
ΤΕΛΟΣ

Ἄσκηση 7. *Φτιᾶξτε μία διαδικασία, ἡ ὁποία, κατὰ τὴν ἐκτέλεση τοῦ ἀλγορίθμου 2.2.1, συμπληρώνει βαθμιαῖα ἕνα πίνακα μὲ τὶς τιμὲς τῶν* δ, x, ϵ *καὶ κατασκευᾶστε τὸν πίνακα* a^n *ὅταν ὁ ἐκθέτης* n *εἶναι κάποιος συγκεκριμένος 3ψήφιος ἢ 4ψήφιος ἀκέραιος (σὲ δεκαδικὸ σύστημα).*

Ἄσκηση 8. *Ἀποδεῖξτε ὅτι τὸ πλῆθος τῶν βημάτων τοῦ Ἀλγορίθμου 2.2.1 εἶναι* $O(\log n)$. *(β΄) Ἔστω ὅτι οἱ* m, a, n *εἶναι φυσικοὶ ἀριθμοὶ καὶ* $0 < a < m$. *Ἀποδεῖξτε ὅτι τὸ κόστος ὑπολογισμοῦ τοῦ* $a^n \bmod m$ *εἶναι* $O(\log n \cdot \max(\log^2 m, \log n))$.

Εὕρεση ἀντιστρόφου $\bmod m$. Ἂν ὁ ἀκέραιος a εἶναι πρῶτος πρὸς τὸν m, τότε, ἀπὸ τὸ *Θεώρημα τοῦ Euler* $a^{\phi(m)} \equiv 1 \pmod m$, ἄρα, στὴν ὁμάδα $\mathbb{Z}_m^*$, $a^{\phi(m)-1} = a^{-1}$. Ἡ ὕψωση σὲ δύναμη γίνεται ταχύτατα μὲ τὸν Ἀλγόριθμο 2.2.1. Ὅμως, στὴν περίπτωση ποὺ ὁ m εἶναι πολὺ μεγάλος καὶ ἔχει κάποιους πολὺ μεγάλους πρώτους διαιρέτες, εἶναι ἀδύνατον, ἀπὸ πρακτικὴ ἄποψη, νὰ ὑπολογίσομε τὸν $\phi(m)$, διότι ὁ μόνος μέχρι σήμερα[2] γνωστὸς τρόπος γιὰ τὸν ὑπολογισμὸ τοῦ $\phi(m)$ βασίζεται στὴ γνώση τῶν πρώτων διαιρετῶν p τοῦ m:

$$\phi(m) = m \prod_{p|m} \left(1 - \frac{1}{p}\right) .$$

Ἀντίθετα, ὁ Ἀλγόριθμος 2.1.4 δὲν ἀπαιτεῖ αὐτὴ τὴ γνώση, εἶναι ταχύτατος, ἐπίσης, καὶ μᾶς δίνει ἀκεραίους x, y, τέτοιους ὥστε, $ax + my = 1$, ἄρα $ax \equiv 1 \pmod m$, δηλαδή, στὴν ὁμάδα $\mathbb{Z}_m^*$, $x = a^{-1}$.

Ἄσκηση 9. *Ἀποδεῖξτε ὅτι, γιὰ* $0 < a < m$ *καὶ* $\gcd(a, m) = 1$, *τὸ κόστος ὑπολογισμοῦ τοῦ* $a^{-1} \bmod m$ *εἶναι* $O(\log^2 m)$.

Ἐρχόμαστε τώρα στὶς ταυτόχρονες ἰσοδυναμίες. Τὸ πρόβλημα εἶναι τὸ ἑξῆς: Δίνονται ἀριθμοὶ $m_1, m_2, \ldots, m_r$ *ἀνὰ δύο πρῶτοι μεταξύ τους*, τυχόντες ἀκέραιοι $a_1, a_2, \ldots, a_r$ καὶ ζητεῖται ἀκέραιος x, τέτοιος ὥστε, συγχρόνως νὰ ἰσχύουν οἱ σχέσεις

$$x \equiv a_1 \pmod{m_1} \; x \equiv a_2 \pmod{m_2} \; \ldots x \equiv a_r \pmod{m_r} . \qquad (1)$$

Λόγου χάρη (κλασικὸ πρόβλημα), οἱ ἄνδρες ἑνὸς τάγματος τοποθετοῦνται σὲ 5άδες καὶ περισσεύουν δύο, τοποθετοῦνται σὲ 6άδες καὶ περισσεύει ἕνας, τοποθετοῦνται

[2] 10 Νοεμβρίου 2007

σὲ 7άδες καὶ περισσεύουν τρεῖς. Ἂν τὸ πλῆθος τῶν ἀνδρῶν εἶναι μεταξὺ 300 καὶ 400, ποιὸ ἀκριβῶς εἶναι τὸ πλῆθος τους;

Σχετικὰ μὲ τὴν ἐπίλυση τοῦ συστήματος 1 ἰσχύει τὸ ἑξῆς

Θεώρημα 2.2.2. *(Κινέζικο Θεώρημα Ὑπολοίπων) Μὲ τὶς παραπάνω ὑποθέσεις γιὰ τὰ* $m_1, \ldots, m_r$ *καὶ* $a_1, \ldots, a_r$*, θέτομε*

$$m = m_1 m_2 \cdots m_r \ , \ M_i = \frac{m}{m_i} \ , \ M_i' \equiv M_i^{-1} \pmod{m_i} \quad (i = 1, 2, \ldots, r) \ .$$

Τότε ὁ

$$x = a_1 M_1 M_1' + a_2 M_2 M_2' + \cdots + a_r M_r M_r'$$

εἶναι λύση τῆς (1). Ἂν y *εἶναι, ἐπίσης, λύση τῆς (1), τότε* $x \equiv y \pmod{m}$.

Ἡ ὑπόθεση γιὰ τοὺς $m_1, m_2, \ldots, m_r$, νὰ εἶναι ἀνὰ δύο πρῶτοι μεταξύ τους, εἶναι πολὺ οὐσιαστική! Εἶναι πολὺ ἰσχυρότερη ἀπὸ τὴν ὑπόθεση ὅτι οἱ ἀριθμοὶ αὐτοὶ εἶναι πρῶτοι μεταξύ τους. Γιὰ παράδειγμα, οἱ 10,15,49 εἶναι πρῶτοι μεταξύ τους (ὁ μόνος κοινὸς καὶ στοὺς τρεῖς διαιρέτης εἶναι ὁ 1), ἐνῶ, *ἀνὰ δύο*, δὲν εἶναι πρῶτοι μεταξύ τους, ἀφοῦ $(10, 15) = 5$.

Παρατηρῆστε ὅτι κάθε M_i ἔχει παράγοντες ὅλα τὰ m_j πλὴν τοῦ m_i, Εἰδικώτερα, μὲ βάση καὶ τὴν ὑπόθεσή μας, αὐτὸ σημαίνει ὅτι $(M_i, m_i) = 1$, ἄρα ἐξασφαλίζεται ἡ ὕπαρξη τοῦ M_i' καὶ ὁ ὑπολογισμός του γίνεται πολὺ γρήγορα, ὅπως σχολιάσαμε παραπάνω, χάρη στὸν Ἀλγόριθμο 2.1.4.

Συνιστώμενη σχετικὴ βιβλιογραφία.

- N. Koblitz, *Algebraic aspects of Cryptography*, Springer 1999, κεφάλαιο 2.
- R.A. Mollin, *An introduction to Cryptography*, Chapman & Hall/CRC 2007 (δεύτερη ἔκδοση), Παράρτημα Β.
- Ν.Γ. Τζανάκης *Σημειώσεις Θεωρίας Ἀριθμῶν* (στὴν προσωπικὴ ἱστοσελίδα), κεφάλαιο 1.