ΤΕΙ ΗΠΕΙΡΟΥ
ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ Τ.Ε
ΜΕΤΑΠΤΙΧΙΑΚΟ ΠΡΟΓΡΑΜΜΑ ΣΠΟΥΔΩΝ

Ασφάλεια

ΛΙΑΓΚΟΥ ΒΑΣΙΛΙΚΗ

ΘΕΩΡΊΑ ΑΡΙΘΜΏΝ,
ΑΛΓΕΒΡΙΚΈΣ ΔΟΜΈΣ,
ΔΎΣΚΟΛΑ ΠΡΟΒΛΉΜΑΤΑ

Syllabus

1. Διαιρετότητα
   - Μέγιστος Κοινός Διαιρέτης,
   - Αλγόριθμος Ευκλείδη, Επεκταμένος Αλγόριθμος Ευκλείδη
2. Αριθμητική Modulo n
   - Πράξεις modulo n, Κλάσσεις Ισοδυναμίας
3. Αλγεβρικές Δομές
   - Ομάδες, Δακτύλιοι, Σώματα
   - Υποομάδες, Γεννήτορας, Τάξη στοιχείου, Τάξη Ομάδας, Πρωτεύουσα Ρίζα
4. Πρώτοι Αριθμοί και Δυνάμεις Ακεραίων modulo n
   - Διακριτός Λογάριθμος, Θεωρήματα Fermat & Euler, Ολική συνάρτηση Euler
   - Τετραγωνικά Υπόλοιπα, Μη Τετραγωνικά Υπόλοιπα
   - Θεμελιώδες Θεώρημα Αριθμητικής, Κινεζικό Θεώρημα Υπολοίπων
5. Δύσκολα Προβλήματα στην Κρυπτογραφία
   - FACTORING, RSAP, DLP, DHP, SQROOT

Διαιρετότητα

Ορισμός & Ιδιότητες

Διαιρετότητα. *Ένας μη μηδενικός ακέραιος b διαιρεί τον ακέραιο a, αν $a = mb$, όπου m είναι ακέραιος. Συμβολίζουμε με $b \mid a$*

The positive divisors of 24 are 1, 2, 3, 4, 6, 8, 12, and 24.
$13 \mid 182;\ -5 \mid 30;\ 17 \mid 289;\ -3 \mid 33;\ 17 \mid 0$

Ιδιότητες:

1. *Αν $a \mid 1$ τότε $a = \pm 1$* Το 1 Διαιρεί το α
2. *Αν $a \mid b$ και $b \mid a$ τότε $a = \pm b$* Το α Διαιρεί το b και b Διαιρεί το α
3. *Κάθε $b \neq 0$ διαιρεί το 0*
4. *Αν $a \mid b$ και $b \mid c$ τότε $a \mid c$* b Διαιρεί το a και το b διαιρεί το c

$11 \mid 66$ and $66 \mid 198 \Rightarrow 11 \mid 198$

5. *Αν $b \mid g$ και $b \mid h$ τότε $b \mid (mg + nh)$, για κάθε ακέραιο m, n*

$b = 7; g = 14; h = 63; m = 3; n = 2$
$7 \mid 14$ and $7 \mid 63$.
To show $7 \mid (3 \times 14 + 2 \times 63)$,
we have $(3 \times 14 + 2 \times 63) = 7(3 \times 2 + 2 \times 9)$,
and it is obvious that $7 \mid (7(3 \times 2 + 2 \times 9))$.

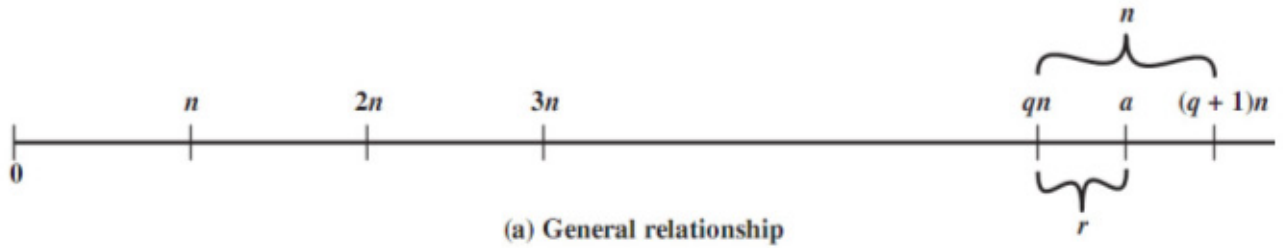
W. Stallings. Cryptography and Network Security – Principles and Practice, 5th Edition. Pearson, 2011

Διαιρετότητα

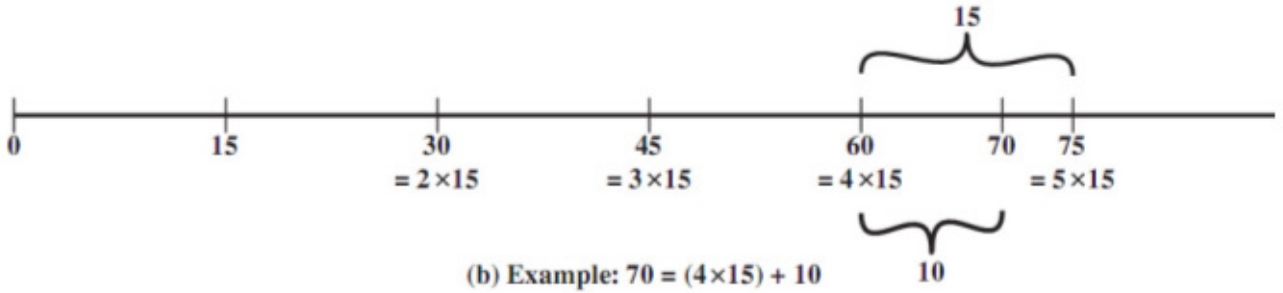
Θεώρημα της Διαίρεσης

Θεώρημα της Διαίρεσης. *Για κάθε ακέραιο a και οποιοδήποτε θετικό ακέραιο n υπάρχουν μοναδικοί ακέραιοι q και r τέτοιοι ώστε*

$$a = qn + r, \qquad 0 \le r \le n$$



(a) General relationship



(b) Example: 70 = (4×15) + 10

$a = 11;$	$n = 7;$	$11 = 1 \times 7 + 4;$	$r = 4$	$q = 1$
$a = -11;$	$n = 7;$	$-11 = (-2) \times 7 + 3;$	$r = 3$	$q = -2$

Διαιρετότητα

Μέγιστος Κοινός Διαιρέτης, Σχετικώς Πρώτοι

Μέγιστος Κοινός Διαιρέτης (ΜΚΔ): Ο ΜΚΔ, συμβολιζόμενος ως $\gcd(a, b)$ *δύο ακεραίων a, b ορίζεται ως ο μεγαλύτερος από τους κοινούς διαιρέτες των a και b:*

$$\gcd(a, b) = \max[k, \text{τέτοιο ώστε } k \mid a \text{ και } k \mid b]$$

***Εναλλακτικός ορισμός**: Ο ακέραιος d είναι ο ΜΚΔ των ακεραίων a, b αν:*

1. *Ο d είναι κοινός διαιρέτης των a και b*
2. *Αν c / a και c / b τότε d*

$$\gcd(60, 24) = \gcd(60, -24) = 12$$

Σχετικώς Πρώτοι Αριθμοί. Δύο ακέραιοι *a, b είναι σχετικώς πρώτοι αν* $\gcd(a, b) = 1$

8 and 15 are relatively prime because the positive divisors of 8 are 1, 2, 4, and 8, and the positive divisors of 15 are 1, 3, 5, and 15. So 1 is the only integer on both lists.

Διαιρετότητα

Μέγιστος Κοινός Διαιρέτης – Αλγόριθμος Ευκλείδη

Εύρεση ΜΚΔ. *Έστω ακέραιοι αριθμοί* a, b *και* $a \geq b$. *Από το θεώρημα διαιρετότητας:*

$$a = q_1 b + r_1, \qquad 0 \leq r_1 \leq b \qquad \textbf{(4.2)}$$

Αν $r_1 = 0$ *τότε* $b \mid a$ *και* $d = \gcd(a, b) = b$. *Αλλά αν* $r_1 \neq 0$ *τότε μπορούμε να θεωρήσουμε ότι* $d \mid r_1$ *(*$5^{η}$ *ιδιότητα διαιρετότητας:* $d \mid (a - q_1 b)$*). Δεδομένου λοιπόν ότι* $d \mid b$ *και* $d \mid r_1$, *έστω οποιοσδήποτε ακέραιος* c *που διαιρεί τους* b *και* r_1, *επομένως* $c \mid (q_1 b + r_1) = a$. *Αφού ο* c *διαιρεί τους* a, b, *θα πρέπει να ισχύει* $c \mid d$. *Επομένως, ισχύει ότι* $d = \gcd(b, r_1)$.

Ξαναγυρίζοντας στην (4.2), αν $r_1 \neq 0$, *και εφόσον* $b > r_1$, *από το θεώρημα διαιρετότητας:*

$$b = q_2 r_1 + r_2, \qquad 0 \leq r_2 \leq r_1$$

Όπως και πριν, Αν $r_2 = 0$ *τότε* $d = r_1$ *και αν* $r_2 \neq 0$ *τότε* $d = \gcd(r_1, r_2)$. *Η διαδικασία επαναλαμβάνεται μέχρι να εμφανιστεί κάποιο μηδενικό υπόλοιπο, π.χ. στο βήμα* $n+1$:

$$\left.\begin{array}{ll}
a = q_1 b + r_1 & 0 < r_1 < b \\
b = q_2 r_1 + r_2 & 0 < r_2 < r_1 \\
r_1 = q_3 r_2 + r_3 & 0 < r_3 < r_2 \\
\quad\vdots & \quad\vdots \\
r_{n-2} = q_n r_{n-1} + r_n & 0 < r_n < r_{n-1} \\
r_{n-1} = q_{n+1} r_n + 0 & \\
d = \gcd(a, b) = r_n &
\end{array}\right\} \qquad \textbf{(4.3)}$$

Διαιρετότητα

Μέγιστος Κοινός Διαιρέτης – Αλγόριθμος Ευκλείδη

To find $d = \gcd(a,b) = \gcd(1160718174, 316258250)$		
$a = q_1 b + r_1$	$1160718174 = 3 \times 316258250 + 211943424$	$d = \gcd(316258250, 211943424)$
$b = q_2 r_1 + r_2$	$316258250 = 1 \times 211943424 + 104314826$	$d = \gcd(211943424, 104314826)$
$r_1 = q_3 r_2 + r_3$	$211943424 = 2 \times 104314826 + 3313772$	$d = \gcd(104314826, 3313772)$
$r_2 = q_4 r_3 + r_4$	$104314826 = 31 \times 3313772 + 1587894$	$d = \gcd(3313772, 1587894)$
$r_3 = q_5 r_4 + r_5$	$3313772 = 2 \times 1587894 + 137984$	$d = \gcd(1587894, 137984)$
$r_4 = q_6 r_5 + r_6$	$1587894 = 11 \times 137984 + 70070$	$d = \gcd(137984, 70070)$
$r_5 = q_7 r_6 + r_7$	$137984 = 1 \times 70070 + 67914$	$d = \gcd(70070, 67914)$
$r_6 = q_8 r_7 + r_8$	$70070 = 1 \times 67914 + 2156$	$d = \gcd(67914, 2156)$
$r_7 = q_9 r_8 + r_9$	$67914 = 31 \times 2516 + 1078$	$d = \gcd(2156, 1078)$
$r_8 = q_{10} r_9 + r_{10}$	$2156 = 2 \times 1078 + 0$	$d = \gcd(1078, 0) = 1078$
Therefore, $d = \gcd(1160718174, 316258250) = 1078$		

W. Stallings. Cryptography and Network Security – Principles and Practice, 5th Edition. Pearson, 2011

Διαιρετότητα

Μέγιστος Κοινός Διαιρέτης – Αλγόριθμος Ευκλείδη

Table 4.1 Euclidean Algorithm Example

Dividend	Divisor	Quotient	Remainder
$a = 1160718174$	$b = 316258250$	$q_1 = 3$	$r_1 = 211943424$
$b = 316258250$	$r_1 = 211943434$	$q_2 = 1$	$r_2 = 104314826$
$r_1 = 211943424$	$r_2 = 104314826$	$q_3 = 2$	$r_3 = 3313772$
$r_2 = 104314826$	$r_3 = 3313772$	$q_4 = 31$	$r_4 = 1587894$
$r_3 = 3313772$	$r_4 = 1587894$	$q_5 = 2$	$r_5 = 137984$
$r_4 = 1587894$	$r_5 = 137984$	$q_6 = 11$	$r_6 = 70070$
$r_5 = 137984$	$r_6 = 70070$	$q_7 = 1$	$r_7 = 67914$
$r_6 = 70070$	$r_7 = 67914$	$q_8 = 1$	$r_8 = 2156$
$r_7 = 67914$	$r_8 = 2156$	$q_9 = 31$	$r_9 = 1078$
$r_8 = 2156$	$r_9 = 1078$	$q_{10} = 2$	$r_{10} = 0$

W. Stallings. Cryptography and Network Security – Principles and Practice, 5th Edition. Pearson, 2011

Αριθμητική modulo n

Modulus. *Ξαναγυρίζοντας στο Θεώρημα της Διαίρεσης,*

$$a = qn + r, \qquad 0 \le r \le n$$

Η τιμή r *είναι το υπόλοιπο της διαίρεσης όταν ο* a *διαιρείται από τον* n*:*

$$a = qn + a \bmod n$$

όπου $q = \lfloor a/n \rfloor$. *Ο αριθμός* n *ονομάζεται* ***modulus***

$$11 \bmod 7 = 4; \qquad -11 \bmod 7 = 3$$

Η πράξη $a \bmod n$ *συχνά αποκαλείται και ως* ***αναγωγή του a****, modulo n.*

Ισοδυναμία modulo n. *Δύο ακέραιοι a, b λέγονται ισοδύναμοι (congruent) modulo n αν έχουν το ίδιο υπόλοιπο όταν διαιρούνται με τον n:*

$$a \bmod n = b \bmod n, \text{ ή εναλλακτικά: } a \equiv b (\bmod n)$$

W. Stallings. Cryptography and Network Security – Principles and Practice, 5th Edition. Pearson, 2011

Αριθμητική modulo n

Ιδιότητες Ισοδυναμίας modulo n:

1. $a \equiv b (\mathrm{mod} n)$ αν $n | (a - b)$
2. $a \equiv b (\mathrm{mod} n)$ σημαίνει $b \equiv a (\mathrm{mod} n)$
3. Αν $a \equiv b (\mathrm{mod} n)$ και $b \equiv c (\mathrm{mod} n)$ τότε $a \equiv c (\mathrm{mod} n)$

$23 \equiv 8 (\mathrm{mod} 5)$	because	$23 - 8 = 15 = 5 \times 3$
$-11 \equiv 5 (\mathrm{mod} 8)$	because	$-11 - 5 = -16 = 8 \times (-2)$
$81 \equiv 0 (\mathrm{mod} 27)$	because	$81 - 0 = 81 = 27 \times 3$

Αρχή της αριθμητικής modulo n. *Έστω a, b ακέραιο και * μια από τις πράξεις* +,−,×. Τότε η αναγωγή $\mathrm{mod} n$ είναι ένας ομομορφισμός από τους ακεραίους στους ακεραίους $\mathrm{mod} n$:

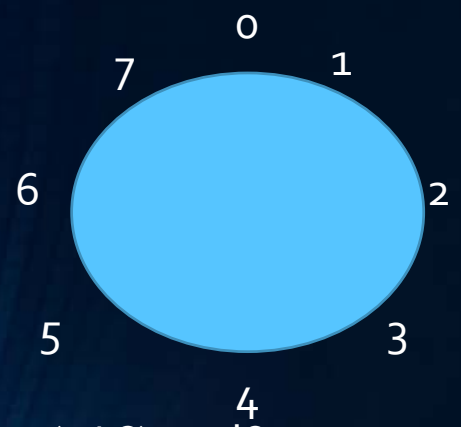
$$(a * b) \bmod n = [(a \bmod n) * (b \bmod n)] \bmod n$$

$11 \bmod 8 = 3; 15 \bmod 8 = 7$
$[(11 \bmod 8) + (15 \bmod 8)] \bmod 8 = 10 \bmod 8 = 2$
$(11 + 15) \bmod 8 = 26 \bmod 8 = 2$

$[(11 \bmod 8) - (15 \bmod 8)] \bmod 8 = -4 \bmod 8 = 4$
$(11 - 15) \bmod 8 = -4 \bmod 8 = 4$

$[(11 \bmod 8) \times (15 \bmod 8)] \bmod 8 = 21 \bmod 8 = 5$
$(11 \times 15) \bmod 8 = 165 \bmod 8 = 5$

Αριθμητική modulo n



(5*6)mod8=30 mod8=6

Όλα ο
Όλοι οι αριθμοί
Περίοδος 4
Όλοι οι αριθμοί
Περίοδος 2
Όλοι οι αριθμοί
Περίοδος 4
Όλοι οι αριθμοί

Table 4.2 Arithmetic Modulo 8

+	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7	0
2	2	3	4	5	6	7	0	1
3	3	4	5	6	7	0	1	2
4	4	5	6	7	0	1	2	3
5	5	6	7	0	1	2	3	4
6	6	7	0	1	2	3	4	5
7	7	0	1	2	3	4	5	6

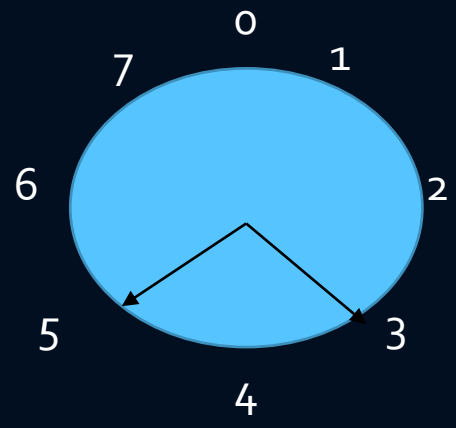
(a) Addition modulo 8

×	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	1	6	3
6	0	6	4	2	0	6	4	2
7	0	7	6	5	4	3	2	1

(b) Multiplication modulo 8

w	$-w$	w^{-1}
0	0	—
1	7	1
2	6	—
3	5	3
4	4	—
5	3	5
6	2	—
7	1	7

(c) Additive and multiplicative inverses modulo 8



(5+6)mod 8=11 mod 8=3

-w=8-w, π.χ -6→2

gcd(w,8)=1

Αριθμητική modulo n

Κλάσεις Ισοδυναμίας

Κλάση Ισοδυναμίας modulo n. Ο τελεστής mod n *αντιστοιχίζει όλους τους ακεραίους στο σύνολο των μη αρνητικών ακεραίων μικρότερων από n:*

$$Z_n = \{0,1,\ldots,(n-1)\}$$

Κάθε ένας αριθμός a στο Z_n *ορίζει μια* ***κλάση ισοδυναμίας modulo n****, που περιλαμβάνει όλους τους ακέραιους που αν διαιρεθούν με το modulus n δίνουν υπόλοιπο a:*

$$[a]_n = \{a + kn : k \in Z) = \{x \in Z : x \equiv a(\text{mod}\, n)\}\}$$

Το σύνολο όλων αυτών των κλάσεων ισοδυναμίας είναι το Z_n*:*

$$Z_n = \{[a]_n : 0 \le a \le n-1\} = \{[0],[1],\ldots,[n-1]\}$$

The residue classes (mod 4) are

$[0] = \{\ldots, -16, -12, -8, -4, 0, 4, 8, 12, 16, \ldots\}$
$[1] = \{\ldots, -15, -11, -7, -3, 1, 5, 9, 13, 17, \ldots\}$
$[2] = \{\ldots, -14, -10, -6, -2, 2, 6, 10, 14, 18, \ldots\}$
$[3] = \{\ldots, -13, -9, -5, -1, 3, 7, 11, 15, 19, \ldots\}$

Αριθμητική modulo n

Πράξεις και Ιδιότητες

Property	Expression
Commutative Laws	$(w + x) \bmod n = (x + w) \bmod n$ $(w \times x) \bmod n = (x \times w) \bmod n$
Associative Laws	$[(w + x) + y] \bmod n = [w + (x + y)] \bmod n$ $[(w \times x) \times y] \bmod n = [w \times (x \times y)] \bmod n$
Distributive Law	$[w \times (x + y)] \bmod n = [(w \times x) + (w \times y)] \bmod n$
Identities	$(0 + w) \bmod n = w \bmod n$ $(1 \times w) \bmod n = w \bmod n$
Additive Inverse $(-w)$	For each $w \in Z_n$, there exists a z such that $w + z \equiv 0 \bmod n$

Σημείωση: *Χάρη στην ύπαρξη του προσθετικού αντιστρόφου για κάθε στοιχείο, ισχύει:*

$$Αν\ (a+b) \equiv (a+c) (\bmod n)\ τότε\ b \equiv c (\bmod n) \quad \textbf{(4.4)}$$

$$(5 + 23) \equiv (5 + 7) (\bmod 8);\ 23 \equiv 7 (\bmod 8)$$

Όμως:

$$Αν\ (a \times b) \equiv (a \times c) (\bmod n)\ τότε\ b \equiv c (\bmod n)\ \textbf{αν το a είναι σχετικώς πρώτος του n} \quad \textbf{(4.5)}$$

Αριθμητική modulo n

Πράξεις και Ιδιότητες

$$6 \times 3 = 18 \equiv 2 \pmod 8$$
$$6 \times 7 = 42 \equiv 2 \pmod 8$$
Yet $3 \not\equiv 7 \pmod 8$.

With $a = 6$ and $n = 8$,

Z_8	0	1	2	3	4	5	6	7
Multiply by 6	0	6	12	18	24	30	36	42
Residues	0	6	4	2	0	6	4	2

However, if we take $a = 5$ and $n = 8$, whose only common factor is 1,

Z_8	0	1	2	3	4	5	6	7
Multiply by 5	0	5	10	15	20	25	30	35
Residues	0	5	2	7	4	1	6	3

The line of residues contains all the integers in Z_8, in a different order.

Αριθμητική modulo n

Παραλλαγή Αλγόριθμου Ευκλείδη

Παραλλαγή Αλγορίθμου Ευκλείδη. *Ο αλγόριθμος μπορεί να βασιστεί στο ακόλουθο θεώρημα: Για κάθε μη αρνητικό ακέραιο a και κάθε θετικό ακέραιο b,*

$$\gcd(a, b) = \gcd(b, a \bmod b) \quad \textbf{(4.6)}$$

$$\gcd(18, 12) = \gcd(12, 6) = \gcd(6, 0) = 6$$
$$\gcd(11, 10) = \gcd(10, 1) = \gcd(1, 0) = 1$$

Euclidean Algorithm

Calculate	Which satisfies
$r_1 = a \bmod b$	$a = q_1 b + r_1$
$r_2 = b \bmod r_1$	$b = q_2 r_1 + r_2$
$r_3 = r_1 \bmod r_2$	$r_1 = q_3 r_2 + r_3$
• • •	• • •
$r_n = r_{n-2} \bmod r_{n-1}$	$r_{n-2} = q_n r_{n-1} + r_n$
$r_{n+1} = r_{n-1} \bmod r_n = 0$	$r_{n-1} = q_{n+1} r_n + 0$ $d = \gcd(a, b) = r_n$

```
Euclid(a,b)
    if (b=0) then return a;
    else return Euclid(b, a mod b);
```

Menezes, Oorschot, Vanstone, Handbook of Applied Cryptography, CRC, 2001

Αλγόριθμος

2.104 Algorithm Euclidean algorithm for computing the greatest common divisor of two integers

INPUT: two non-negative integers a and b with $a \geq b$.
OUTPUT: the greatest common divisor of a and b.

1. While $b \neq 0$ do the following:
   1.1 Set $r \leftarrow a \bmod b$, $a \leftarrow b$, $b \leftarrow r$.
2. Return(a).

Αριθμητική modulo n

Επεκταμένος αλγόριθμος Ευκλείδη

Επεκταμένος Αλγόριθμος του Ευκλείδη. *Ο επεκταμένος αλγόριθμος υπολογίζει, εκτός από τον μέγιστο κοινό διαιρέτη d, δύο ακέραιους x, y που ικανοποιούν την ακόλουθη εξίσωση:*

$$ax + by = d = \gcd(a, b)$$

Αρχικά εκτελούμε τις διαιρέσεις του (αρχικού) αλγορίθμου (4.3) και υποθέτουμε ότι σε κάθε βήμα i βρίσκουμε ακεραίους x_i, y_i *που ικανοποιούν τη σχέση:* $r_i = ax_i + by_i$ *:*

$$\begin{array}{ll} a = q_1 b + r_1 & r_1 = ax_1 + by_1 \\ b = q_2 r_1 + r_2 & r_2 = ax_2 + by_2 \\ r_1 = q_3 r_2 + r_3 & r_3 = ax_3 + by_3 \\ \bullet & \bullet \\ \bullet & \bullet \\ \bullet & \bullet \\ r_{n-2} = q_n r_{n-1} + r_n & r_n = ax_n + by_n \\ r_{n-1} = q_{n+1} r_n + 0 & \end{array}$$

Σε κάθε βήμα i, το υπόλοιπο r_i *μπορεί να εκφραστεί ως:*

$$r_i = r_{i-2} - r_{i-1} q_i \qquad \textbf{(4.8)}$$

Επίσης, στα βήματα i-1 και i-2, βρίσκουμε τις τιμές $r_{i-2} = ax_{i-2} + by_{i-2}$ *και* $r_{i-1} = ax_{i-1} + by_{i-1}$

Αντικαθιστώντας στην (4.8), έχουμε

$$\begin{aligned} r_i &= (ax_{i-2} + by_{i-2}) - (ax_{i-1} + by_{i-1}) q_i \\ &= a(x_{i-2} - q_i x_{i-1}) + b(y_{i-2} - q_i y_{i-1}) \end{aligned}$$

Αλλά έχουμε υποθέσει ότι: $r_i = ax_i + by_i$ *. Επομένως:* $x_i = x_{i-2} - q_i x_{i-1}$ *και* $y_i = y_{i-2} - q_i y_{i-1}$

W. Stallings. Cryptography and Network Security – Principles and Practice, 5th Edition. Pearson, 2011

$$x_i = x_{i-2} - q_i x_{i-1}$$

$$y_i = y_{i-2} - q_i y_{i-1}$$

```
function extended_gcd(a, b)
    if a mod b = 0
        return {0, 1}
    else
        {x, y} := extended_gcd(b, a mod b)
        return {y, x-(y*(a div b))}
```

Αριθμητική modulo n

Επεκταμένος Αλγόριθμος Ευκλείδη

Extended Euclidean Algorithm

Calculate	Which satisfies	Calculate	Which satisfies
$r_{-1} = a$		$x_{-1} = 1; y_{-1} = 0$	$a = ax_{-1} + by_{-1}$
$r_0 = b$		$x_0 = 0; y_0 = 1$	$b = ax_0 + by_0$
$r_1 = a \bmod b$ $q_1 = \lfloor a/b \rfloor$	$a = q_1 b + r_1$	$x_1 = x_{-1} - q_1 x_0 = 1$ $y_1 = y_{-1} - q_1 y_0 = -q_1$	$r_1 = ax_1 + by_1$
$r_2 = b \bmod r_1$ $q_2 = \lfloor b/r_1 \rfloor$	$b = q_2 r_1 + r_2$	$x_2 = x_0 - q_2 x_1$ $y_2 = y_0 - q_2 y_1$	$r_2 = ax_2 + by_2$
$r_3 = r_1 \bmod r_2$ $q_3 = \lfloor r_1/r_2 \rfloor$	$r_1 = q_3 r_2 + r_3$	$x_3 = x_1 - q_3 x_2$ $y_3 = y_1 - q_3 y_2$	$r_3 = ax_3 + by_3$
•	•	•	•
•	•	•	•
•	•	•	•
$r_n = r_{n-2} \bmod r_{n-1}$ $q_n = \lfloor r_{n-2}/r_{n-3} \rfloor$	$r_{n-2} = q_n r_{n-1} + r_n$	$x_n = x_{n-2} - q_n x_{n-1}$ $y_n = y_{n-2} - q_n y_{n-1}$	$r_n = ax_n + by_n$
$r_{n+1} = r_{n-1} \bmod r_n = 0$ $q_{n+1} = \lfloor r_{n-1}/r_{n-2} \rfloor$	$r_{n-1} = q_{n+1} r_n + 0$		$d = \gcd(a, b) = r_n$ $x = x_n; y = y_n$

Table 4.4 Extended Euclidean Algorithm Example

i	r_i	q_i	x_i	y_i
–1	1759		1	0
0	550		0	1
1	109	3	1	–3
2	5	5	–5	16
3	4	21	106	–339
4	1	1	–111	355
5	0	4		

Result: $d = 1$; $x = -111$; $y = 355$

Menezes, Oorschot, Vanstone, Handbook of Applied Cryptography, CRC, 2001

Αλγόριθμος

2.107 Algorithm Extended Euclidean algorithm

INPUT: two non-negative integers a and b with $a \geq b$.
OUTPUT: $d = \gcd(a, b)$ and integers x, y satisfying $ax + by = d$.

1. If $b = 0$ then set $d \leftarrow a$, $x \leftarrow 1$, $y \leftarrow 0$, and return(d,x,y).
2. Set $x_2 \leftarrow 1$, $x_1 \leftarrow 0$, $y_2 \leftarrow 0$, $y_1 \leftarrow 1$.
3. While $b > 0$ do the following:
   3.1 $q \leftarrow \lfloor a/b \rfloor$, $r \leftarrow a - qb$, $x \leftarrow x_2 - qx_1$, $y \leftarrow y_2 - qy_1$.
   3.2 $a \leftarrow b$, $b \leftarrow r$, $x_2 \leftarrow x_1$, $x_1 \leftarrow x$, $y_2 \leftarrow y_1$, and $y_1 \leftarrow y$.
4. Set $d \leftarrow a$, $x \leftarrow x_2$, $y \leftarrow y_2$, and return(d,x,y).

Menezes, Oorschot, Vanstone, Handbook of Applied Cryptography, CRC, 2001

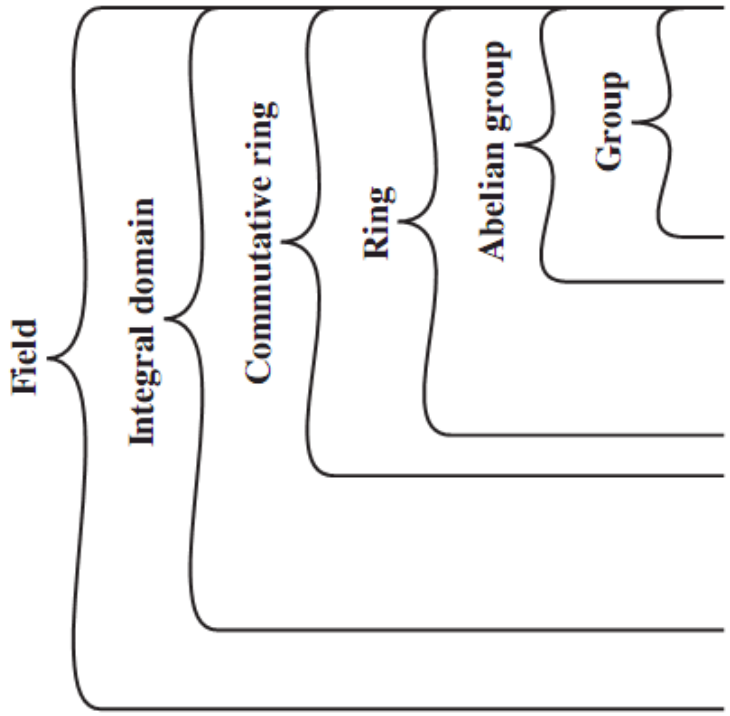
Αλγόριθμος

2.142 Algorithm Computing multiplicative inverses in $\mathbb{Z}_n$

INPUT: $a \in \mathbb{Z}_n$.
OUTPUT: $a^{-1} \bmod n$, provided that it exists.

1. Use the extended Euclidean algorithm (Algorithm 2.107) to find integers x and y such that $ax + ny = d$, where $d = \gcd(a, n)$.
2. If $d > 1$, then $a^{-1} \bmod n$ does not exist. Otherwise, return(x).

Ομάδες (Groups), Δακτύλιοι (Rings), Σώματα (Fields)



(A1) Closure under addition:	If a and b belong to S, then $a + b$ is also in S
(A2) Associativity of addition:	$a + (b + c) = (a + b) + c$ for all a, b, c in S
(A3) Additive identity:	There is an element 0 in R such that $a + 0 = 0 + a = a$ for all a in S
(A4) Additive inverse:	For each a in S there is an element $-a$ in S such that $a + (-a) = (-a) + a = 0$
(A5) Commutativity of addition:	$a + b = b + a$ for all a, b in S
(M1) Closure under multiplication:	If a and b belong to S, then ab is also in S
(M2) Associativity of multiplication:	$a(bc) = (ab)c$ for all a, b, c in S
(M3) Distributive laws:	$a(b + c) = ab + ac$ for all a, b, c in S $(a + b)c = ac + bc$ for all a, b, c in S
(M4) Commutativity of multiplication:	$ab = ba$ for all a, b in S
(M5) Multiplicative identity:	There is an element 1 in S such that $a1 = 1a = a$ for all a in S
(M6) No zero divisors:	If a, b in S and $ab = 0$, then either $a = 0$ or $b = 0$
(M7) Multiplicative inverse:	If a belongs to S and $a \neq 0$, there is an element a^{-1} in S such that $aa^{-1} = a^{-1}a = 1$

Figure 4.2 Groups, Ring, and Field

Άλλα Παραδείγματα Ομάδων:

(Z^*_{21}, x): Z^*_{21}= {1,2,4,5,8,10,11,13,16,17,19,20}

(Z^*_7, x) και $(Z^*_7, +)$ όπου Z^*_7= {1,2,3,4,5,6}

Ομάδες (Groups)

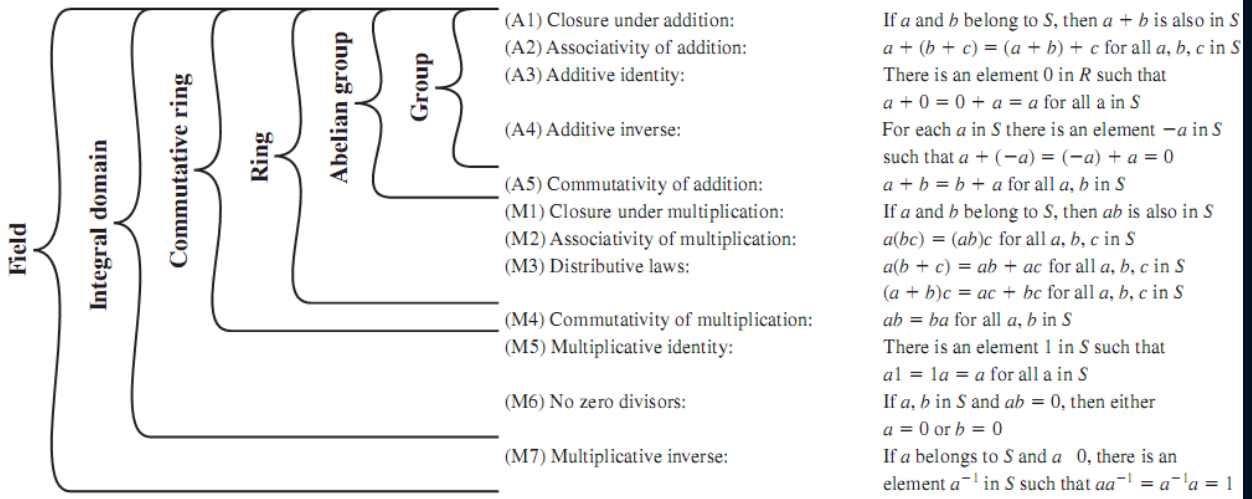


Figure 4.2 Groups, Ring, and Field

Παραδείγματα Ομάδων

- *Η δομή* $(Z,+)$ *είναι μια αντιμεταθετική (αβελιανή) προσθετική ομάδα (με ουδέτερο στοιχείο το 0). Η δομή* $(Z,\times)$ *δεν είναι πολλαπλασιαστική ομάδα (Γιατί;)*
- *Η δομή* $(Z_n,+)$ *στην πράξη της πρόσθεσης modulo n είναι επίσης παράδειγμα ομάδας*
- *Η πολλαπλασιαστική ομάδα* $(Z_n^*,\times)$ *όπου* $Z_n^* = \{a \in Z_n \mid \gcd(a,n) = 1\}$.
- *Αν n είναι πρώτος, τότε η ομάδα* $(Z_n^*,\times)$ *όπου* $Z_n^* = \{a \mid 1 \le a \le n-1\}$

Δακτύλιοι (Rings)

Παράδειγμα Δακτυλίου. *Το σύνολο* $(Z_n = \{0,1,\ldots, n\},+,\times)$ *είναι αντιμεταθετικός δακτύλιος.*

Table 4.2 Arithmetic Modulo 8

+	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7	0
2	2	3	4	5	6	7	0	1
3	3	4	5	6	7	0	1	2
4	4	5	6	7	0	1	2	3
5	5	6	7	0	1	2	3	4
6	6	7	0	1	2	3	4	5
7	7	0	1	2	3	4	5	6

(a) Addition modulo 8

×	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	1	6	3
6	0	6	4	2	0	6	4	2
7	0	7	6	5	4	3	2	1

(b) Multiplication modulo 8

w	$-w$	w^{-1}
0	0	—
1	7	1
2	6	—
3	5	3
4	4	—
5	3	5
6	2	—
7	1	7

(c) Additive and multiplicative inverses modulo 8

Άλλα Παραδείγματα Δακτυλίων

Το σύνολο των ακεραίων (Z, +, x)

Σώματα (Fields)

Παράδειγμα Σώματος. *Το σύνολο* $(R,+,\times)$ *των πραγματικών αριθμών. Το σύνολο* $(Z_p^* = \{1,\ldots, p\},+,\times)$ *όπου p είναι πρώτος, είναι ένα πεπερασμένο σώμα (finite field).*

Table 4.5 Arithmetic in GF(7)

+	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

(a) Addition modulo 7

×	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

(b) Multiplication modulo 7

w	$-w$	w^{-1}
0	0	—
1	6	1
2	5	4
3	4	5
4	3	2
5	2	3
6	1	6

(c) Additive and multiplicative inverses modulo 7

W. Stallings. Cryptography and Network Security – Principles and Practice, 5th Edition. Pearson, 2011

Β. Κάτος, Γ. Στεφανίδης. Τεχνικές Κρυπτογραφίας και Κρυπτανάλυσης. Ζυγός, 2003

Ομάδες, Υποομάδες

Πεπερασμένη Ομάδα και Τάξη Ομάδας. *Μια ομάδα* $(G,\oplus)$ *με πεπερασμένο πλήθος στοιχείων ονομάζεται πεπερασμένη. Ο πληθάριθμος* $|G|$ *καλείται* ***τάξη*** *της ομάδας.*

Υποομάδα. *Εστω* $(G,\oplus)$ *ομάδα και* H *ένα υποσύνολο του* G. *Η δομή* $(G_0,\oplus)$ *είναι υποομάδα της* $(G,\oplus)$ *αν η* $(G_0,\oplus)$ *είναι ομάδα και επίσης περιέχει το ουδέτερο στοιχείο* e *της* $(G,\oplus)$.

Θεώρημα Lagrange. *Αν* $(G,\oplus)$ *πεπερασμένη ομάδα και* $(G_0,\oplus)$ *μια υποομάδα της τότε η τάξη* $|G_0|$ *της υποομάδας είναι διαιρέτης της τάξης* $|G|$ *της ομάδας.*

Εκθετική πράξη Ομάδας. *Ορίζουμε την έκθεση σε «δύναμη» ως την επαναλαμβανόμενη εφαρμογή της πράξης της ομάδας, π.χ.* $a^3 = a \oplus a \oplus a$, *το ουδέτερο στοιχείο ως* $a^0 = e$, *καθώς επίσης* $a^{-n} = (a^{-1})^n$. *(σ.σ. στην πράξη της πρόσθεσης,* $a^k = ka$ *)*

Παράδειγμα: *Ομάδα* $(Z_6,+)$

$\langle 0 \rangle = \{0\}$

$\langle 1 \rangle = \{0, 1, 2, 3, 4, 5\}$

$\langle 2 \rangle = \{0, 2, 4\}$

Παράδειγμα: *Ομάδα* $(Z_7^*,\times)$

$\langle 1 \rangle = \{1\}$

$\langle 2 \rangle = \{1, 2, 4\}$

$\langle 3 \rangle = \{1, 2, 3, 4, 5, 6\}$

W. Stallings. Cryptography and Network Security – Principles and Practice, 5th Edition. Pearson, 2011

Β. Κάτος, Γ. Στεφανίδης. Τεχνικές Κρυπτογραφίας και Κρυπτανάλυσης. Ζυγός, 2003

Κυκλική Ομάδα - Υποομάδα

Κυκλική ομάδα. *Μια ομάδα* $(G,\oplus)$ *είναι* ***κυκλική*** *με γεννήτορα το στοιχείο* $a \in G$, *αν όλες οι δυνάμεις* a^k, *όπου* $k \geq 0$ *ακέραιος,* ***δημιουργούν*** *τη G. Το a καλείται* ***γεννήτορας*** *της G.*

Παράδειγμα. *Η δομή* $(Z,+)$ *είναι μια κυκλική ομάδα με γεννήτορα το 1.*

Αν $(G,\oplus)$ *πεπερασμένη ομάδα και* $a \in G$, *τότε το σύνολο:* $\langle a \rangle = \{a^{(k)} : k \in N^*\}$ *όλων των δυνάμεων του a ορίζει μια* ***υποομάδα*** *της* $(G,\oplus)$ *που* ***δημιουργείται από το a*** *και συμβολίζεται με* $(\langle a \rangle,\oplus\}$. *Το a καλείται και* ***γεννήτορας*** *της* $\langle a \rangle$.

Παράδειγμα: *Ομάδα* $(Z_6,+)$

$\langle 0 \rangle = \{0\}$

$\langle 1 \rangle = \{0, 1, 2, 3, 4, 5\}$

$\langle 2 \rangle = \{0, 2, 4\}$

Παράδειγμα: *Ομάδα* $(Z_7^*,\times)$

$\langle 1 \rangle = \{1\}$

$\langle 2 \rangle = \{1, 2, 4\}$

$\langle 3 \rangle = \{1, 2, 3, 4, 5, 6\}$

W. Stallings. Cryptography and Network Security – Principles and Practice, 5th Edition. Pearson, 2011

Β. Κάτος, Γ. Στεφανίδης. Τεχνικές Κρυπτογραφίας και Κρυπτανάλυσης. Ζυγός, 2003

Κυκλική Ομάδα – Υποομάδα

Τάξη στοιχείου ομάδας. *Η τάξη (order) ενός στοιχείου* $a \in G$, *συμβολικά ord(a), ορίζεται ως ο μικρότερος θετικός ακέραιος t για τον οποίο ισχύει:*

$$a^{(t)} = e \quad (\text{όπου } e \text{ το ουδέτερο στοιχείο της } (G,\oplus))$$

Θεώρημα: *Αν* $(G,\oplus)$ *είναι μια πεπερασμένη ομάδα και* $a \in G$, *τότε:*

$$ord(a) = |\langle a \rangle|$$

Πόρισμα. *Η ακολουθία των «δυνάμεων» του a:* $a^{(1)}, a^{(2)}, \ldots$, *είναι περιοδική με περίοδο* $t = ord(a)$, *δηλαδή μπορούμε να ανάγουμε τον εκθέτη του στοιχείου modulo την τάξη του:*

$$a^{(k)} = a^{(k \bmod |\langle a \rangle|)}$$

To see this last point, consider the powers of 7, modulo 19:

$$\begin{aligned}
7^1 &\equiv & &\equiv 7 \pmod{19} \\
7^2 &= 49 = 2 \times 19 + 11 & &\equiv 11 \pmod{19} \\
7^3 &= 343 = 18 \times 19 + 1 & &\equiv 1 \pmod{19} \\
7^4 &= 2401 = 126 \times 19 + 7 & &\equiv 7 \pmod{19} \\
7^5 &= 16807 = 884 \times 19 + 11 & &\equiv 11 \pmod{19}
\end{aligned}$$

W. Stallings. Cryptography and Network Security – Principles and Practice, 5th Edition. Pearson, 2011

Κυκλική Ομάδα - Υποομάδα

Subgroup	Generators	Order
$\{1\}$	1	1
$\{1, 18\}$	18	2
$\{1, 7, 11\}$	7, 11	3
$\{1, 7, 8, 11, 12, 18\}$	8, 12	6
$\{1, 4, 5, 6, 7, 9, 11, 16, 17\}$	4, 5, 6, 9, 16, 17	9
$\{1, 2, 3, \ldots, 18\}$	2, 3, 10, 13, 14, 15	18

Table 2.7: *The subgroups of* $\mathbb{Z}_{19}^*$.

Table 8.3 Powers of Integers, Modulo 19

a	a^2	a^3	a^4	a^5	a^6	a^7	a^8	a^9	a^{10}	a^{11}	a^{12}	a^{13}	a^{14}	a^{15}	a^{16}	a^{17}	a^{18}
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	4	8	16	13	7	14	9	18	17	15	11	3	6	12	5	10	1
3	9	8	5	15	7	2	6	18	16	10	11	14	4	12	17	13	1
4	16	7	9	17	11	6	5	1	4	16	7	9	17	11	6	5	1
5	6	11	17	9	7	16	4	1	5	6	11	17	9	7	16	4	1
6	17	7	4	5	11	9	16	1	6	17	7	4	5	11	9	16	1
7	11	1	7	11	1	7	11	1	7	11	1	7	11	1	7	11	1
8	7	18	11	12	1	8	7	18	11	12	1	8	7	18	11	12	1
9	5	7	6	16	11	4	17	1	9	5	7	6	16	11	4	17	1
10	5	12	6	3	11	15	17	18	9	14	7	13	16	8	4	2	1
11	7	1	11	7	1	11	7	1	11	7	1	11	7	1	11	7	1
12	11	18	7	8	1	12	11	18	7	8	1	12	11	18	7	8	1
13	17	12	4	14	11	10	16	18	6	2	7	15	5	8	9	3	1
14	6	8	17	10	7	3	4	18	5	13	11	2	9	12	16	15	1
15	16	12	9	2	11	13	5	18	4	3	7	10	17	8	6	14	1
16	9	11	5	4	7	17	6	1	16	9	11	5	4	7	17	6	1
17	4	11	16	6	7	5	9	1	17	4	11	16	6	7	5	9	1
18	1	18	1	18	1	18	1	18	1	18	1	18	1	18	1	18	1

$a \in \mathbb{Z}_{21}^*$	1	2	4	5	8	10	11	13	16	17	19	20
order of a	1	6	3	6	2	6	6	2	3	6	6	2

Β. Κάτος, Γ. Στεφανίδης. Τεχνικές Κρυπτογραφίας και Κρυπτανάλυσης. Ζυγός, 2003

Πρωτεύουσα Ρίζα Ομάδας – Διακριτός Λογάριθμος

Στην περίπτωση που για κάποιο $g \in Z_n^*$ *ισχύει* $ord(a) = |Z_n^*|$, *τότε κάθε στοιχείο του* Z_n^* *είναι μια δύναμη του g, modulo n, και το g είναι γεννήτορας του* Z_n^*. *Σε αυτήν την περίπτωση η* Z_n^* *λέγεται* ***κυκλική*** *και το g λέγεται και* ***πρωτεύουσα ρίζα*** *του* Z_n^*.

ΠΑΡΑΔΕΙΓΜΑ 2.8 – Οι δυνάμεις του 3 modulo 7 είναι

k	0	1	2	3	4	5	6	7	8	9	10	11	12	...
$3^k \bmod 7$	1	3	2	6	4	5	1	3	2	6	4	5	1	...

ενώ οι δυνάμεις του 2 modulo 7 είναι

k	0	1	2	3	4	5	6	7	8	9	10	11	12	...
$2^k \bmod 7$	1	2	4	1	2	4	1	2	4	1	2	4	1	...

Διακριτός Λογάριθμος*. Αν το* Z_n^* *έχει πρωτεύουσα ρίζα, και α οποιοδήποτε στοιχείο του, τότε υπάρχει* $z \in Z_n^*$ *τέτοιο ώστε* $g^z \equiv a(\mathrm{mod} n)$. *Το z λέγεται διακριτός λογάριθμος του a modulo n, ως προς τη βάση g.*

Παράδειγμα*. Έστω η ισοδυναμία* $2^z \equiv 3(\mathrm{mod} 13)$ *:*

$2^1 \equiv 2, 2^2 \equiv 4, 2^3 \equiv 8, 2^4 \equiv 3, 2^5 \equiv 6, 2^6 \equiv 12, 2^7 \equiv 11, 2^8 \equiv 9, 2^9 \equiv 5, 2^{10} \equiv 10,$

$2^{11} \equiv 7, 2^{12} \equiv 1 \pmod{13}$

οπότε $z = 4$.

Menezes, Oorschot, Vanstone, Handbook of Applied Cryptography, CRC, 2001

Αλγόριθμοι

4.79 Algorithm Determining the order of a group element

INPUT: a (multiplicative) finite group G of order n, an element $a \in G$, and the prime factorization $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$.
OUTPUT: the order t of a.

1. Set $t \leftarrow n$.
2. For i from 1 to k do the following:
   2.1 Set $t \leftarrow t/p_i^{e_i}$.
   2.2 Compute $a_1 \leftarrow a^t$.
   2.3 While $a_1 \neq 1$ do the following: compute $a_1 \leftarrow a_1^{p_i}$ and set $t \leftarrow t \cdot p_i$.
3. Return(t).

4.80 Algorithm Finding a generator of a cyclic group

INPUT: a cyclic group G of order n, and the prime factorization $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$.
OUTPUT: a generator α of G.

1. Choose a random element α in G.
2. For i from 1 to k do the following:
   2.1 Compute $b \leftarrow \alpha^{n/p_i}$.
   2.2 If $b = 1$ then go to step 1.
3. Return(α).

W. Stallings. Cryptography and Network Security – Principles and Practice, 5th Edition. Pearson, 2011

Πρώτοι αριθμοί

Table 8.1 Primes Under 2000

2	101	211	307	401	503	601	701	809	907	1009	1103	1201	1301	1409	1511	1601	1709	1801	1901
3	103	223	311	409	509	607	709	811	911	1013	1109	1213	1303	1423	1523	1607	1721	1811	1907
5	107	227	313	419	521	613	719	821	919	1019	1117	1217	1307	1427	1531	1609	1723	1823	1913
7	109	229	317	421	523	617	727	823	929	1021	1123	1223	1319	1429	1543	1613	1733	1831	1931
11	113	233	331	431	541	619	733	827	937	1031	1129	1229	1321	1433	1549	1619	1741	1847	1933
13	127	239	337	433	547	631	739	829	941	1033	1151	1231	1327	1439	1553	1621	1747	1861	1949
17	131	241	347	439	557	641	743	839	947	1039	1153	1237	1361	1447	1559	1627	1753	1867	1951
19	137	251	349	443	563	643	751	853	953	1049	1163	1249	1367	1451	1567	1637	1759	1871	1973
23	139	257	353	449	569	647	757	857	967	1051	1171	1259	1373	1453	1571	1657	1777	1873	1979
29	149	263	359	457	571	653	761	859	971	1061	1181	1277	1381	1459	1579	1663	1783	1877	1987
31	151	269	367	461	577	659	769	863	977	1063	1187	1279	1399	1471	1583	1667	1787	1879	1993
37	157	271	373	463	587	661	773	877	983	1069	1193	1283		1481	1597	1669	1789	1889	1997
41	163	277	379	467	593	673	787	881	991	1087		1289		1483		1693			1999
43	167	281	383	479	599	677	797	883	997	1091		1291		1487		1697			
47	173	283	389	487		683		887		1093		1297		1489		1699			
53	179	293	397	491		691				1097				1493					
59	181			499										1499					
61	191																		
67	193																		
71	197																		
73	199																		
79																			
83																			
89																			
97																			

W. Stallings. Cryptography and Network Security – Principles and Practice, 5th Edition. Pearson, 2011

Menezes, Oorschot, Vanstone, Handbook of Applied Cryptography, CRC, 2001

Πρώτοι αριθμοί – Θεώρημα Fermat

Θεώρημα Fermat. *Αν p είναι πρώτος αριθμός, τότε:*

$$a^{p-1} = 1 \pmod{p}, \quad \forall a \in Z_p^*$$

$a = 7, p = 19$
$7^2 = 49 \equiv 11 \pmod{19}$
$7^4 \equiv 121 \equiv 7 \pmod{19}$
$7^8 \equiv 49 \equiv 11 \pmod{19}$
$7^{16} \equiv 121 \equiv 7 \pmod{19}$
$a^{p-1} = 7^{18} = 7^{16} \times 7^2 \equiv 7 \times 11 \equiv 1 \pmod{19}$

Γενίκευση. *Αν p είναι πρώτος αριθμός και* $r = s \pmod{p-1}$, *τότε* $a^r = a^s \pmod{p}$ *για όλους τους ακέραιους a. Δηλαδή όταν δουλεύουμε modulo έναν πρώτο p,* ***οι εκθέτες μπορούν να αναχθούν*** *modulo* $p-1$. *Ειδικότερα, ισχύει:*

$$a^p = a \pmod{p}$$

$p = 5, a = 3 \quad a^p = 3^5 = 243 \equiv 3 \pmod{5} = a \pmod{p}$
$p = 5, a = 10 \quad a^p = 10^5 = 100000 \equiv 10 \pmod{5} \equiv 0 \pmod{5} = a \pmod{p}$

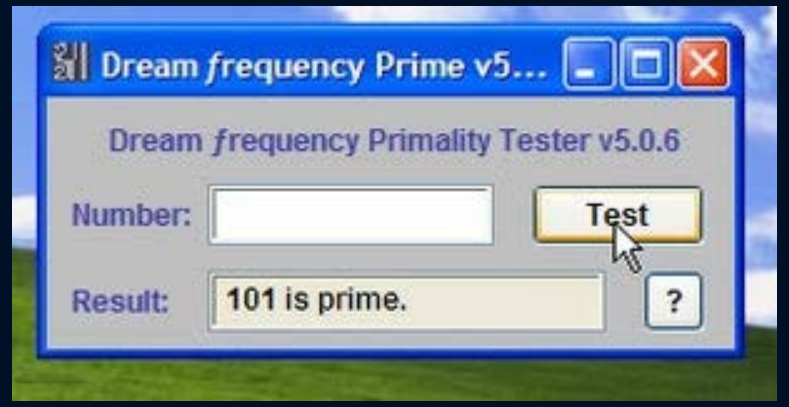
Menezes, Oorschot, Vanstone, Handbook of Applied Cryptography, CRC, 2001

Εύρεση τυχαίων Πρώτων Αριθμών

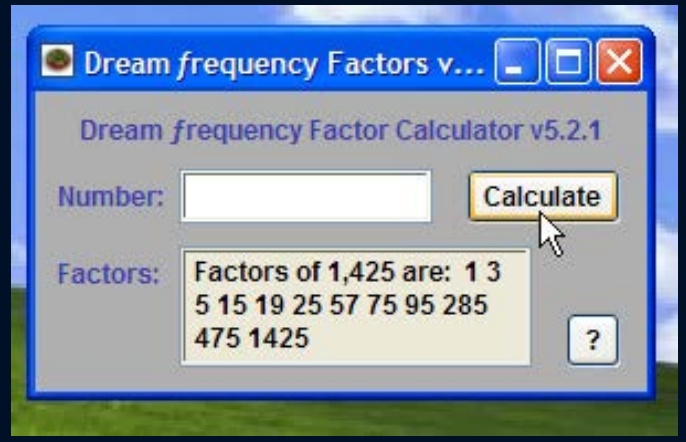
Fermat Primality Test

1. Δημιούργησε έναν τυχαίο περιττό αριθμό p
2. Επίλεξε έναν αριθμό a < p και έλεγξε εάν

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



3. Εάν ο έλεγχος είναι αληθής, τότε ο a μάλλον είναι πρώτος. Αλλιώς, πήγαινε στο βήμα 5.
4. Επανάλαβε k φορές τα βήματα 2-3, όπου k είναι μια παράμετρος ασφάλειας.
5. Προσθέτω τον αριθμό 2 στον n και επιστρέφω στο βήμα 2



Menezes, Oorschot, Vanstone, Handbook of Applied Cryptography, CRC, 2001

Αλγόριθμος

4.9 Algorithm Fermat primality test

FERMAT(n,t)
INPUT: an odd integer $n \geq 3$ and security parameter $t \geq 1$.
OUTPUT: an answer "prime" or "composite" to the question: "Is n prime?"

1. For i from 1 to t do the following:
   - 1.1 Choose a random integer a, $2 \leq a \leq n-2$.
   - 1.2 Compute $r = a^{n-1} \bmod n$ using Algorithm 2.143.
   - 1.3 If $r \neq 1$ then return("composite").
2. Return("prime").

Πρώτοι αριθμοί – Θεμελιώδες Θεώρημα

Θεμελιώδες Θεώρημα Αριθμητικής. *Κάθε θετικός ακέραιος* $a > 1$ *μπορεί να γραφεί κατά μοναδικό τρόπο ως ένα γινόμενο δυνάμεων:*

$$a = p_1^{a_1} \times p_2^{a_2} \times \ldots \times p_t^{a_t} \qquad \textbf{(4.9)}$$

όπου $p_1 < p_2 < \ldots < p_t$ *είναι πρώτοι αριθμοί και* a_i, $1 \le i \le t$ *είναι θετικοί ακέραιοι αριθμοί*

$$91 = 7 \times 13$$
$$3600 = 2^4 \times 3^2 \times 5^2$$
$$11011 = 7 \times 11^2 \times 13$$

Εναλλακτική διατύπωση. *Αν* P *είναι το σύνολο των πρώτων αριθμών, κάθε θετικός ακέραιος μπορεί να γραφεί κατά μοναδικό τρόπο:*

$$a = \prod_{p \in P} p^{a_p}, \quad a_p \ge 0$$

The integer 12 is represented by $\{a_2 = 2, a_3 = 1\}$.
The integer 18 is represented by $\{a_2 = 1, a_3 = 2\}$.
The integer 91 is represented by $\{a_7 = 1, a_{13} = 1\}$.

W. Stallings. Cryptography and Network Security – Principles and Practice, 5th Edition. Pearson, 2011

Πρώτοι αριθμοί – Θεμελιώδες Θεώρημα

Εναλλακτικός Αλγόριθμος Εύρεσης ΜΚΔ

Αλγόριθμος εύρεσης ΜΚΔ: *Αν* $a = p_1^{a_1} \times p_2^{a_2} \times \ldots \times p_t^{a_t}$ *και* $b = p_1^{f_1} \times p_2^{f_2} \times \ldots \times p_t^{f_t}$ *με* $a_i \geq 0,\ f_i \geq 0,$ *τότε:*

$$\gcd(a,b) = p_1^{\min(a_1,f_1)} \times p_2^{\min(a_2,f_2)} \times \ldots \times p_t^{\min(a_t,f_t)}$$

$$\begin{aligned} 300 &= 2^2 \times 3^1 \times 5^2 \\ 18 &= 2^1 \times 3^2 \\ \gcd(18, 300) &= 2^1 \times 3^1 \times 5^0 = 6 \end{aligned}$$

Β. Κάτος, Γ. Στεφανίδης. Τεχνικές Κρυπτο-
γραφίας και Κρυπτανάλυσης. Ζυγός, 2003

Ολική Συνάρτηση Φ(n) (Euler)

Ολική (totient) Συνάρτηση του Euler. *Η συνάρτηση του Euler,* $\Phi(n)$, *ορίζεται ως η* ***τάξη της*** $(Z_n^*, \times)$, *δηλαδή ο αριθμός των θετικών ακεραίων που είναι σχετικώς πρώτοι με τον n.*

ΠΑΡΑΔΕΙΓΜΑ 2.1 – Σύνολα ακεραίων οι οποίοι είναι σχετικά πρώτοι με τον n

n	$\{a \in \boldsymbol{Z} : 1 \le a \le n-1$ και $\gcd(a, n) = 1\}$
1	{1}
2	{1}
3	{1, 2}
4	{1, 3}
5	{1, 2, 3, 4}
6	{1, 5}
7	{1, 2, 3, 4, 5, 6}
8	{1, 3, 5, 7}
9	{1, 2, 4, 5, 7, 9}
10	{1, 3, 7, 9}

Από τον παραπάνω πίνακα προκύπτουν οι εξής τιμές της συνάρτησης $\phi(a)$ για $1 \le a \le 10$. Έτσι

a	1	2	3	4	5	6	7	8	9	10
$\phi(a)$	1	1	2	2	4	2	6	4	6	4

Θεώρημα. *Αν p, q, πρώτοι αριθμοί και* $n = pq$ *σύνθετος αριθμός, τότε:* $\Phi(n) = \Phi(p)\Phi(q)$

Ολική Συνάρτηση Φ(n) (Euler)

Ιδιότητες Συνάρτησης Euler

(1) *Αν p πρώτος αριθμός, τότε:* $\Phi(p) = p - 1$

(2) *Η Φ είναι πολλαπλασιαστική. Δηλαδή αν* $\gcd(m,n) = 1$ *τότε* $\Phi(mn) = \Phi(m)\Phi(n)$

(3) *Αν p, q, πρώτοι αριθμοί και* $n = pq$, *τότε:* $\Phi(n) = \Phi(p)\Phi(q)$

(4) *Αν* $n = p_1^{a_1} \times p_2^{a_2} \times \ldots \times p_t^{a_t}$ *τότε* $\Phi(n) = n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \cdots (1 - \frac{1}{p_t})$

Table 8.2 Some Values of Euler's Totient Function $\phi(n)$

n	$\phi(n)$	n	$\phi(n)$	n	$\phi(n)$
1	1	11	10	21	12
2	1	12	4	22	10
3	2	13	12	23	22
4	2	14	6	24	8
5	4	15	8	25	20
6	2	16	8	26	12
7	6	17	16	27	18
8	4	18	6	28	12
9	6	19	18	29	28
10	4	20	8	30	8

$\phi(21) = \phi(3) \times \phi(7) = (3 - 1) \times (7 - 1) = 2 \times 6 = 12$
where the 12 integers are $\{1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20\}$.

W. Stallings. Cryptography and Network Security – Principles and Practice, 5th Edition. Pearson, 2011

Menezes, Oorschot, Vanstone, Handbook of Applied Cryptography, CRC, 2001

Β. Κάτος, Γ. Στεφανίδης. Τεχνικές Κρυπτογραφίας και Κρυπτανάλυσης. Ζυγός, 2003

Δυνάμεις Ακεραίων modulo n - Θεώρημα Euler

Θεώρημα του Euler. *Για οποιονδήποτε ακέραιο* $n > 1$ *, ισχύει:*

$$a^{\Phi(n)} = 1 (\mathrm{mod}\, n),\ \forall a \in Z_n^*$$

$a = 3; n = 10;\ \phi(10) = 4\quad a^{\phi(n)} = 3^4 = 81 = 1 (\mathrm{mod}\ 10) = 1 (\mathrm{mod}\ n)$
$a = 2; n = 11;\ \phi(11) = 10\ a^{\phi(n)} = 2^{10} = 1024 = 1 (\mathrm{mod}\ 11) = 1 (\mathrm{mod}\ n)$

Γενίκευση. *Αν* $r = \mathrm{s}\ (\mathrm{mod}\, \Phi(n))$, *τότε* $a^r = a^{\,s} (\mathrm{mod}\, n)$ *για όλους τους αριθμούς a. Δηλαδή όταν δουλεύουμε modulo n,* ***οι εκθέτες μπορούν να αναχθούν*** *modulo* $\Phi(n)$. *Ειδικότερα:*

$$a^{\Phi(n)+1} = a (\mathrm{mod}\, n)$$

Εφαρμογή του Θεωρήματος του Euler: *Μπορούμε να χρησιμοποιήσουμε το θεώρημα του Euler στον υπολογισμό δυνάμεων στο* Z_n*:*

$7^0 \equiv 1 \pmod{10}$
$7^1 \equiv 7 \pmod{10}$
$7^2 = 49 \equiv 9 \pmod{10}$
$7^3 = 7^2 \cdot 7 \equiv 9 \cdot 7 \equiv 3 \pmod{10}$
$7^4 = 7^3 \cdot 7 \equiv 3 \cdot 7 \equiv 1 \pmod{10}$
$7^5 = 7^4 \cdot 7 \equiv 1 \cdot 7 \equiv 7 \pmod{10}$
$7^6 = 7^4 \cdot 7^2 \equiv 1 \cdot 49 \equiv 9 \pmod{10}$
⋮

Θεώρημα Euler

$2^1 \equiv 2 \pmod{10}$
$2^2 \equiv 4 \pmod{10}$
$2^3 \equiv 8 \pmod{10}$
$2^4 \equiv 6 \pmod{10}$
$2^5 \equiv 2 \pmod{10}$
$2^6 \equiv 4 \pmod{10}$
⋮

Γενίκευση

W. Stallings. Cryptography and Network Security – Principles and Practice, 5th Edition. Pearson, 2011

Δυνάμεις Ακεραίων modulo

Subgroup	Generators	Order
$\{1\}$	1	1
$\{1, 18\}$	18	2
$\{1, 7, 11\}$	7, 11	3
$\{1, 7, 8, 11, 12, 18\}$	8, 12	6
$\{1, 4, 5, 6, 7, 9, 11, 16, 17\}$	4, 5, 6, 9, 16, 17	9
$\{1, 2, 3, \ldots, 18\}$	2, 3, 10, 13, 14, 15	18

Table 2.7: *The subgroups of* $\mathbb{Z}_{19}^*$.

Table 8.3 Powers of Integers, Modulo 19

a	a^2	a^3	a^4	a^5	a^6	a^7	a^8	a^9	a^{10}	a^{11}	a^{12}	a^{13}	a^{14}	a^{15}	a^{16}	a^{17}	a^{18}
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	4	8	16	13	7	14	9	18	17	15	11	3	6	12	5	10	1
3	9	8	5	15	7	2	6	18	16	10	11	14	4	12	17	13	1
4	16	7	9	17	11	6	5	1	4	16	7	9	17	11	6	5	1
5	6	11	17	9	7	16	4	1	5	6	11	17	9	7	16	4	1
6	17	7	4	5	11	9	16	1	6	17	7	4	5	11	9	16	1
7	11	1	7	11	1	7	11	1	7	11	1	7	11	1	7	11	1
8	7	18	11	12	1	8	7	18	11	12	1	8	7	18	11	12	1
9	5	7	6	16	11	4	17	1	9	5	7	6	16	11	4	17	1
10	5	12	6	3	11	15	17	18	9	14	7	13	16	8	4	2	1
11	7	1	11	7	1	11	7	1	11	7	1	11	7	1	11	7	1
12	11	18	7	8	1	12	11	18	7	8	1	12	11	18	7	8	1
13	17	12	4	14	11	10	16	18	6	2	7	15	5	8	9	3	1
14	6	8	17	10	7	3	4	18	5	13	11	2	9	12	16	15	1
15	16	12	9	2	11	13	5	18	4	3	7	10	17	8	6	14	1
16	9	11	5	4	7	17	6	1	16	9	11	5	4	7	17	6	1
17	4	11	16	6	7	5	9	1	17	4	11	16	6	7	5	9	1
18	1	18	1	18	1	18	1	18	1	18	1	18	1	18	1	18	1

J. Katz, Y. Lindell. Introduction to Modern Cryptography. Chapman & Hall/CRC, 2008.

H. Mel, D. Baker. Cryptography Decrypted. Addison-Wesley, 2001

Δυνάμεις Ακεραίων modulo n

- Στην αριθμητική modulo n, μπορούμε να πραγματοποιήσουμε εκθετικές πράξεις με αποδοτικό τρόπο
  - Μη αποδοτικός τρόπος: $(\alpha^8 \bmod n) = (\alpha*\alpha*\alpha*\alpha*\alpha*\alpha*\alpha*\alpha) \bmod n$
  - Αποδοτικός τρόπος: $(\alpha^8 \bmod n) = ((\alpha^2 \bmod n)^2 \bmod n)^2 \bmod n$

What we're computing	As a multiplication	The result of the multiplication	Compute the modular answer
39^1	39	39	39 mod 55
39^2	39 * 39	1521	36 mod 55
39^4	$39^2 * 39^2 = 36 * 36$	1296	31 mod 55
39^8	$39^4 * 39^4 = 31 * 31$	961	26 mod 55
39^{16}	$39^8 * 39^8 = 26 * 26$	676	16 mod 55

J. Katz, Y. Lindell. Introduction to Modern Cryptography. Chapman & Hall/CRC, 2008.

H. Mel, D. Baker. Cryptography Decrypted. Addison-Wesley, 2001

Δυνάμεις Ακεραίων modulo n

- Στην αριθμητική modulo n, μπορούμε να πραγματοποιήσουμε εκθετικές πράξεις με αποδοτικό τρόπο
  - Αφελής τρόπος: $(\alpha^8 \bmod n) = (\alpha*\alpha*\alpha*\alpha*\alpha*\alpha*\alpha*\alpha) \bmod n$
  - Έξυπνος τρόπος: $(\alpha^8 \bmod n) = ((\alpha^2 \bmod n)^2 \bmod n)^2 \bmod n$

Ένα ακόμη παράδειγμα

1093028 x 190301 mod 100 =

[1093028 mod 100] x [190301 mod 100] =

28 x 1 = 28 mod 100

C. Kaufman, R. Perlman, M. Speciner. Network Security – Private Communication in a Public World. 2nd edition, Prentice Hall, 2002

Δυνάμεις Ακεραίων modulo n

$$123^2 = 123 \cdot 123 = 15129 = 213 \bmod 678$$
$$123^4 = 213 \cdot 213 = 45369 = 621 \bmod 678$$
$$123^8 = 621 \cdot 621 = 385641 = 537 \bmod 678$$
$$123^{16} = 537 \cdot 537 = 288369 = 219 \bmod 678$$
$$123^{32} = 219 \cdot 219 = 47961 = 501 \bmod 678$$

- Όταν η εκθετική πράξη είναι της μορφής $\alpha^{2\wedge x} \bmod n$ εύκολα:
  - 5 τετραγωνισμοί (πολλαπλασιασμοί & διαιρέσεις)
- Τι θα συμβεί αν δεν υψώνουμε σε δυνάμεις του 2?
  - π.χ. υπολογισμός του 123^{54}

Hints:

- Αν ξέρω το 123^x, τότε 123^{2x} εύκολο
- Επίσης, $123^{2x+1} = 123^{2x} \times 123$

Square and Multiply:

- $54_{10} = 110110_2$
- Υψώνουμε το 123 στην ακολουθία: 1_2, 11_2,

$$123^2 = 123 \cdot 123 = 15129 = 213 \bmod 678$$
$$123^3 = 123^2 \cdot 123 = 213 \cdot 123 = 26199 = 435 \bmod 678$$
$$123^6 = (123^3)^2 = 435^2 = 189225 = 63 \bmod 678$$
$$123^{12} = (123^6)^2 = 63^2 = 3969 = 579 \bmod 678$$
$$123^{13} = 123^{12} \cdot 123 = 579 \cdot 123 = 71217 = 27 \bmod 678$$
$$123^{26} = (123^{13})^2 = 27^2 = 729 = 51 \bmod 678$$
$$123^{27} = 123^{26} \cdot 123 = 51 \cdot 123 = 6273 = 171 \bmod 678$$
$$123^{54} = (123^{27})^2 = 171^2 = 29241 = 87 \bmod 678$$

Menezes, Oorschot, Vanstone, Handbook of Applied Cryptography, CRC, 2001

Αλγόριθμος

2.143 Algorithm Repeated square-and-multiply algorithm for exponentiation in $\mathbb{Z}_n$

INPUT: $a \in \mathbb{Z}_n$, and integer $0 \leq k < n$ whose binary representation is $k = \sum_{i=0}^{t} k_i 2^i$.
OUTPUT: $a^k \bmod n$.

1. Set $b \leftarrow 1$. If $k = 0$ then return(b).
2. Set $A \leftarrow a$.
3. If $k_0 = 1$ then set $b \leftarrow a$.
4. For i from 1 to t do the following:
   4.1 Set $A \leftarrow A^2 \bmod n$.
   4.2 If $k_i = 1$ then set $b \leftarrow A \cdot b \bmod n$.
5. Return(b).

Stinson, D. Cryptography: Theory and Practice. Third Edition, CRC, 2005

Κινέζικο Θεώρημα Υπολοίπων

(Chinese Remainder Theorem)

Κινέζικο Θεώρημα Υπολοίπων. *Έστω:* $m_1,..m_r$ *σχετικώς πρώτοι θετικοί ακέραιοι, και έστω* $a_1,..a_r$ *ακέραιοι. Τότε, το σύστημα των ισοδυναμιών* $x \equiv a_i (\mathrm{mod} m_i)$, $1 \le i \le r$ *έχει μοναδική λύση modulo* $M = m_1 \times ... \times m_r$ *που δίδεται από τη σχέση:*

$$x = \sum_{i=1}^{r} a_i M_i y_i \bmod M$$

όπου $M_i = M / m_i$ *και* $y_i = M_i^{-1} \bmod m_i$ *για* $1 \le i \le r$.

Παράδειγμα1*: Ποιος ο ζυγός αριθμός στο* Z_{10} *που έχει υπόλοιπο 3 όταν διαιρείται από το 5;*

Κινέζικο Θεώρημα Υπολοίπων

(Chinese Remainder Theorem)

Κινέζικο Θεώρημα Υπολοίπων - Συζήτηση. *Το θεώρημα κάνει δυο ισχυρισμούς:*

1. *Υπάρχει μια* ***αμφιμονοσήμαντη (bijection) απεικόνιση*** *μεταξύ του* Z_M *και του Καρτεσιανού γινομένου* $Z_{m_1} \times Z_{m_2} \times ... \times Z_{m_r}$, *δηλαδή για κάθε ακέραιο* x *υπάρχει μια μοναδική* r*-άδα* $(a_1,..a_r)$ *με* $0 \le a_i \le m_i$, *και για κάθε* r*-άδα* $(a_1,..a_r)$ *υπάρχει ένας μοναδικός ακέραιος* $x \in Z_M$.

$$f : Z_M \to Z_{m_1} \times Z_{m_2} \times ... \times Z_{m_r},\ x \mapsto (a_1 \bmod m_1, a_2 \bmod m_2, ..., a_r \bmod m_r)$$
$$f^{-1} : Z_{m_1} \times Z_{m_2} \times ... \times Z_{m_r} \to Z_M,\ (a_1 \bmod m_1, a_2 \bmod m_2, ..., a_r \bmod m_r) \mapsto x$$

2. *Οι πράξεις στα στοιχεία του* Z_M *μπορούν ισοδυνάμως να μεταφερθούν στο* $Z_{m_1} \times Z_{m_2} \times ... \times Z_{m_r}$, ***για αποδοτικότητα.*** *Για παράδειγμα, αν:*

$$A \leftrightarrow (a_1, a_2, ..., a_r)$$
$$B \leftrightarrow (a_1, a_2, ..., a_r)$$

τότε:

$$(A+B) \bmod M \leftrightarrow (a_1 + b_1) \bmod m_1, ..., (a_r + b_r) \bmod m_r)$$
$$(A-B) \bmod M \leftrightarrow (a_1 - b_1) \bmod m_1, ..., (a_r - b_r) \bmod m_r)$$
$$(A \times B) \bmod M \leftrightarrow (a_1 \times b_1) \bmod m_1, ..., (a_r \times b_r) \bmod m_r)$$

Stinson, D. Cryptography: Theory and Practice. Third Edition, CRC, 2005

Κινέζικο Θεώρημα Υπολοίπων

(Chinese Remainder Theorem)

Παράδειγμα 2. *Έστω* $r=3$, $m_1=7$, $m_2=11$, $m_3=13$. *Τότε,* $M=1001$. *Υπολογίζουμε* $M_1=M/m_1=143$, $M_2=M/m_2=91$, $M_3=M/m_3=77$ *και:* $y_1=M_1^{-1}\bmod m_1=5$, $y_2=M_2^{-1}\bmod m_2=4$, $y_3=M_3^{-1}\bmod m_3=12$. *Η συνάρτηση* $f^{-1}: Z_7\times Z_{11}\times Z_{13}\to Z_{1001}$ *μπορεί να οριστεί ως ακολούθως:*

$$\begin{aligned} f^{-1}(a_1,a_2,a_3) &= (145\times 5\times a_1+91\times 4\times a_2+77\times 12\times a_3)\bmod 1001 \\ &= (715a_1+364a_2+924a_3)\bmod 1001 \end{aligned}$$

Για παράδειγμα, αν $x\equiv 5(\bmod 7)$, $x\equiv 3(\bmod 11)$, $x\equiv 10(\bmod 13)$ *τότε:*

$$\begin{aligned} x &= (715\times 5+364\times 3+924\times 10)\bmod 1001 \\ &= 13907\bmod 1001 \\ &= 894 \end{aligned}$$

Κινέζικο Θεώρημα Υπολοίπων

(Chinese Remainder Theorem)

Παράδειγμα3. *Έστω η πράξη* $973+678$ *στο* Z_{1813}, *όπου* $1813=37\times49$. *Υπολογίζουμε*

$M_1=M/m_1=49$ $M_2=M/m_2=37$, $y_1=M_1^{-1}\bmod m_1=34$, $y_2=M_2^{-1}\bmod m_2=4$. *Επίσης:*

$$973\leftrightarrow(11,42)$$
$$678\leftrightarrow(12,41)$$

Η πρόσθεση «μεταφέρεται» στο $Z_{37}\times Z_{49}$ *ως εξής:*

$$(973+678)\bmod 1813\leftrightarrow((11+12)\bmod 37,(42+41)\bmod 49)$$
$$(973+678)\bmod 1813\leftrightarrow(23,34)$$

Επαλήθευση:

$$\begin{aligned}(23,34)&\leftrightarrow a_1M_1M_1^{-1}+a_2M_2M_2^{-1}\bmod M\\&=[(23)(49)(34)+(34)(37)(4)]\bmod 1813\\&=43350\bmod 1813\\&=1651\end{aligned}$$

Menezes, Oorschot, Vanstone, Handbook of Applied Cryptography, CRC, 2001

Δυνάμεις Ακεραίων modulo n

Τετραγωνική Ρίζα modulo n

Τετραγωνική Ρίζα και Τετραγωνικά Υπόλοιπα. *Αν* $x \in Z_n^*$ *ώστε* $x^2 \equiv a \pmod{n}$ *τότε ο αριθμός x καλείται* ***τετραγωνική ρίζα (square root) του a*** *modulo n, και ο a* ***τετραγωνικό υπόλοιπο*** *(quadratic residue) modulo n. Οι αριθμοί στο* Z_n^* *που δεν έχουν τετραγωνική ρίζα ονομάζονται* ***μη τετραγωνικά υπόλοιπα*** *(quadratic non-residue).*

Παράδειγμα. *Έστω:*

$a \in \mathbb{Z}_{21}^*$	1	2	4	5	8	10	11	13	16	17	19	20

Τα σύνολα Q_n *και* $\overline{Q}_n$ *των τετραγωνικών και μη τετραγωνικών υπολοίπων αντίστοιχα, είναι:*

$$Q_n = \{1,4,16\}, \qquad \overline{Q}_n = \{2,5,8,10,11,13,17,19,20\}$$

Ιδιότητες:

- *Αν p είναι πρώτος αριθμός και* $a \in Q_n$ *τότε ο a έχει ακριβώς 2 ρίζες modulo p*
- *Γενικότερα αν* $n = p_1^{e_1} \times p_2^{e_2} \times \ldots \times p_k^{e_k}$, *όπου* p_i *διακριτοί πρώτοι, και* $a \in Q_n$ *τότε ο a έχει ακριβώς* 2^k *τετραγωνικές ρίζες modulo n.*

Παράδειγμα. *Οι τετραγωνικές ρίζες του 12 modulo 37 είναι οι αριθμοί 7, 30. Οι ρίζες του 121 modulo 315 είναι: 11, 74, 101, 151, 164, 214, 241, 304.*

Menezes, Oorschot, Vanstone, Handbook of Applied Cryptography, CRC, 2001

Αλγόριθμος

3.36 Algorithm Finding square roots modulo a prime p where $p \equiv 3 \pmod 4$

INPUT: an odd prime p where $p \equiv 3 \pmod 4$, and a square $a \in Q_p$.
OUTPUT: the two square roots of a modulo p.

1. Compute $r = a^{(p+1)/4} \bmod p$ (Algorithm 2.143).
2. Return$(r, -r)$.

Menezes, Oorschot, Vanstone, Handbook of Applied Cryptography, CRC, 2001

«Δύσκολα» προβλήματα

Υπολογιστική Ασφάλεια (Computational Security)

Πρόβλημα	***Περιγραφή***
FACTORING	*Δεδομένου ενός αριθμού n, βρες την παραγοντοποίηση του, δηλαδή γράψε το n στη μορφή:* $n = p_1^{e_1} \times p_2^{e_2} \times \ldots \times p_k^{e_k}$ *όπου* p_i *διακριτοί πρώτοι και* $e_i \geq 1$.
RSAP	*Δεδομένων: (α) ενός θετικού ακεραίου n που είναι το γινόμενο δύο διακριτών πρώτων αριθμών p και q, (β) ενός θετικού ακεραίου e τέτοιου ώστε* $\gcd(e,(p-1)(q-1)) = 1$, *και (γ) ενός ακεραίου c, βρες έναν ακέραιο m τέτοιον ώστε* $m^e \equiv c (\mathrm{mod}\, n)$.
SQROOT	*Δεδομένων ενός σύνθετου ακεραίου n και ενός τετραγωνικού υπολοίπου* $a \in Q_n$ *modulo n, βρες μια τετραγωνική ρίζα του a modulo n.*
DLP	*Δεδομένου ενός πρώτου αριθμού p, ενός γεννήτορα g του* Z_p^* *και ενός ακεραίου* $\beta \in Z_p^*$, *βρες ακέραιο x,* $0 \leq x \leq p-2$ *ώστε* $g^x \equiv \beta (\mathrm{mod}\, p)$.
DHP	*Δεδομένου ενός πρώτου αριθμού p, ενός γεννήτορα g του* Z_p^* *και στοιχείων* $g^a \bmod p$, $g^b \bmod p$, *βρες το* $g^{ab} \bmod p$.

Menezes, Oorschot, Vanstone, Handbook of Applied Cryptography, CRC, 2001

Αλγόριθμος

3.44 Algorithm Finding square roots modulo n given its prime factors p and q

INPUT: an integer n, its prime factors p and q, and $a \in Q_n$.
OUTPUT: the four square roots of a modulo n.

1. Use Algorithm 3.39 (or Algorithm 3.36 or 3.37, if applicable) to find the two square roots r and $-r$ of a modulo p.
2. Use Algorithm 3.39 (or Algorithm 3.36 or 3.37, if applicable) to find the two square roots s and $-s$ of a modulo q.
3. Use the extended Euclidean algorithm (Algorithm 2.107) to find integers c and d such that $cp + dq = 1$.
4. Set $x \leftarrow (rdq + scp) \bmod n$ and $y \leftarrow (rdq - scp) \bmod n$.
5. Return$(\pm x \bmod n, \pm y \bmod n)$.