Οικονομικό Πανεπιστήμιο Αθηνών
Τμήμα Πληροφορικής
ΠΜΣ στα Πληροφοριακά Συστήματα

Κρυπτογραφία και Εφαρμογές

Μαριάς Ιωάννης
marias@aueb.gr

Μαρκάκης Ευάγγελος
markakis@gmail.com

Περίληψη

- Θεωρία Αριθμών και Θεωρία Ομάδων
  - ✓ Διαιρετότητα
  - ✓ Αλγόριθμος του Ευκλείδη
  - ✓ Πρώτοι Αριθμοί
  - ✓ Αριθμητική Υπολοίπων
  - ✓ Ομάδες – Γραμμικές εξισώσεις modn
  - ✓ Δακτύλιοι - Πεδία
    - Πεδία Galois
  - ✓ Κινέζικο θεώρημα υπολοίπων
  - ✓ Υποομάδες, κυκλικές ομάδες
    - Θεωρήματα Fermat, Euler
  - ✓ Ύψωση σε δύναμη

Θεωρία Αριθμών και Θεωρία Ομάδων: Μέρος 1

Βασικές Έννοιες

Θεωρία Αριθμών

- Μια θεωρία για τους ακεραίους (Z) και ειδικά τους φυσικούς (N)
- Διαιρετότητα
  - ✓ d | a : ο d διαιρεί τον a (ο d λέγεται διαιρέτης του a και ο a πολλαπλάσιο του d)
  - ✓ Σημαίνει: a = kd για κάποιο ακέραιο k
    - Κάθε ακέραιος διαιρεί το 0.
    - Αν a > 0 και d | a, τότε |d| ≤ |a|
  - ✓ Κάθε ακέραιος a διαιρείται από τους τετριμμένους (trivial) διαιρέτες 1 και a
  - ✓ Οι μη τετριμμένοι διαιρέτες του a καλούνται παράγοντες (factors)
    - factors του 20 : 2, 4, 5, και 10

- Παρατηρήσεις:
  - ✓ $a|b \Rightarrow a|bc$ για κάθε ακέραιο c
  - ✓ $a|b \Rightarrow |a| \leq |b|$ ή $b = 0$
  - ✓ $a|b \wedge b|c \Rightarrow a|c$
  - ✓ $a|b \wedge a|c \Rightarrow a|(b + c)$ και $a|(b - c)$
  - ✓ $a|b \wedge a|c \Rightarrow a|(bx + cy)$ για κάθε ακεραίους x, y
  - ✓ $a|b \wedge b|a \Rightarrow |a| = |b|$

- Θεώρημα διαίρεσης (Division theorem)
  - ✓ **Για κάθε ζεύγος ακεραίων *a,b* με b≠0, υπάρχουν μοναδικοί ακέραιοι *q* και *r* τέτοιοι ώστε**

$$a = qb + r \ (0 \le r < |b|)$$

  - ✓ Η τιμή $q = [a/b]$ είναι το πηλίκο (***quotient***) της διαίρεσης
  - ✓ Η τιμή $r = a \bmod b$ είναι το υπόλοιπο (***remainder***) της διαίρεσης.
  - ✓ $b \mid a$ αν και μόνο αν $a \bmod b = 0$ ή $r = 0$.
- Απόδειξη:
  - ✓ Ύπαρξη: είτε induction είτε θεωρώντας το μικρότερο θετικό ακέραιο στην ακολουθία

    ….., a-3b, a-2b, a-b, a, a+b, a+2b,a+3b,…
  - ✓ Μοναδικότητα: με εις άτοπο απαγωγή

- Κοινοί διαιρέτες
  - ✓ *Αν d* είναι διαιρέτης του *a* και του *b*, τότε ο *d* είναι κοινός διαιρέτης (***common divisor)*** του *a* και *b*.
    - π.χ., οι διαιρέτες του 30 είναι 1, 2, 3, 5, 6, 10, 15, 30
    - και του 24 είναι 1, 2, 3, 4, 6, 8, 12, 24
    - Κοινοί διαιρέτες 24 και 30 είναι 1, 2, 3, και 6.
    - Ο 1 είναι κοινός διαιρέτης για κάθε δύο ακέραιους
  - ✓ Κάθε κοινός διαιρέτης είναι το πολύ min (|a|, |b|)

- Μέγιστος κοινός διαιρέτης
  - ✓ gcd(a,b): ο μεγαλύτερος από τους κοινούς διαιρέτες των ακεραίων a και b (το γράφουμε και ΜΚΔ(a, b) ή απλώς (a, b)).
    - π.χ., gcd(24, 30) = 6, gcd(5, 7) = 1, και gcd(0, 9) = 9.
  - ✓ Αν a και b δεν είναι 0, τότε ο gcd(a, b) είναι ένας ακέραιος μεταξύ 1 και min(|a|, |b|).
  - ✓ Συμβάσεις
    - gcd(0, 0) = 0
  - ✓ Ιδιότητες:
    - gcd(a,b) = gcd(b,a)
    - gcd(a,b) = gcd(-a, b)
    - gcd(a,b) = gcd(|a|, |b|)
    - gcd(a,0) = |a|
    - gcd(a, ak) = |a| για κάθε k ϵ Z

- Μέγιστος κοινός διαιρέτης
- Θεώρημα

  Αν *a* και *b* μη μηδενικοί ακέραιοι, τότε ο gcd(a, b) μπορεί να εκφραστεί ως γραμμικός συνδυασμός των a, b (Bezout's identity). Συγκεκριμένα, είναι ο μικρότερος θετικός ακέραιος του συνόλου {ax +by : x, y ϵ Z} των γραμμικών συνδυασμών των *a* και *b*
- Πορίσματα
  - Για ακέραιους *a* και *b*,

    αν $d \mid a$ και $d \mid b$ τότε $d \mid \gcd(a, b)$.
  - Για ακέραιους *a* και *b*, και μη μηδενικό *n*,

    $\gcd(an,bn) = n \gcd(a, b)$.
  - Για θετικούς ακεραίους *n*, *a*, και *b*,

    αν $n \mid ab$ και $\gcd(a, n) = 1$, τότε $n \mid b$.

- Αλγόριθμος Ευκλείδη
  - ✓ Θα επικεντρωθούμε σε μη αρνητικούς ακεραίους
  - ✓ Στηρίζεται στο:
    - Λήμμα: Για κάθε μη μηδενικό ακέραιο a και θετικό b:

    gcd(a, b) = gcd(b, a mod b)
  - ✓ Αλγόριθμος (300 B.C., Στοιχεία του Ευκλείδη, Βιβλίο 7)

    EUCLID(a, b)

    if b = 0 return a

    if a≥b return EUCLID(b, a mod b)

    else return EUCLID(a, b mod a)
    - Παράδειγμα 1
      - EUCLID(30, 21) = EUCLID(21,9) = EUCLID(9,3) = EUCLID(3,0) = 3
    - Παράδειγμα 2
      - EUCLID(18,12) = EUCLID(12, 6) = EUCLID(6, 0) = 6

- Αλγόριθμος Ευκλείδη
  - ✓ Η αναδρομή ουσιαστικά ανάγεται σε διαδοχικές διαιρέσεις
  - ✓ $a = bq_1 + r_1 \quad 0 < r_1 < b$
  - ✓ $\gcd(b, r_1)$
  - ✓ $b = r_1q_2 + r_2 \quad 0 < r_2 < r_1$
  - ✓ $\gcd(r_1, r_2)$
  - ✓ $r_1 = r_2q_3 + r_3 \quad 0 < r_3 < r_2$

    .....
  - ✓ $r_{j-2} = r_{j-1}q_j + r_j \quad 0 < r_j < r_{j-1}$
  - ✓ $\gcd(r_{j-1}, r_j)$
  - ✓ $r_{j-1} = r_jq_{j+1}$
  - ✓ return r_j

- Παραδείγμα 3
- a = 1742, b = 494
- 1742 = 3·494 + 260
- 494 = 1·260 + 234
- 260 = 1·234 + 26
- 234 = 9·26
- (1742, 494) = 26

- Παραδείγμα 4
- a = 132, b = 35
- 132 = 3·35 + 27
- 35 = 1·27 + 8
- 27 = 3·8 + 3
- 8 = 2·3 + 2
- 3 = 1·2 + 1
- 2 = 2·1
- (132, 35) = 1

✓Ποια η πολυπλοκότητα του αλγορίθμου? (Input = $O(\log_2(a) + \log_2(b))$

✓$O(\log_2(b))$ διαιρέσεις αν $a \geq b$ (Finck 1841, Lamé 1844)

✓Worst case: όταν ένας από τους a, b είναι αριθμός Fibonacci

“We might call it the granddaddy of all algorithms because it is the oldest nontrivial algorithm that has survived to the present day”, (D. Knuth)

- Εκτενής Αλγόριθμος Ευκλείδη (Extended Euclid Algorithm)
  - ✓ Ο Αλγόριθμος του Ευκλείδη μπορεί να επεκταθεί ώστε
    - να προσδιορίζει το gcd(a,b), και
    - να προσδιορίζει ένα ζεύγος ακεραίων x, y που ικανοποιούν τη σχέση gcd(a,b) = ax+by (θα μας χρειαστεί σε επόμενες ενότητες)
    - Η ιδέα είναι να κάνουμε την αντίστροφη διαδικασία του αλγορίθμου του Ευκλείδη

- Παραδείγμα 3
- a = 1742, b = 494
- 1742 = 3·494 + 260
- 494 = 1·260 + 234
- 260 = 1·234 + 26
- 234 = 9·26
- (1742, 494) = 26

- 26 = 260 - 234
  = 260 - (494 - 260)
  = 2·260 - 494
  = 2·(1742- 3·494) - 494
  = 2·1742 - 7·494

- Παραδείγμα 4
- a = 132, b = 35
- 132 = 3·35 + 27
- 35 = 1·27 + 8
- 27 = 3·8 + 3
- 8 = 2·3 + 2
- 3 = 1·2 + 1
- 2 = 2·1
- (132, 35) = 1

- 1 = 3 - 2
  = 3 - (8 - 2·3)
  = 3·3 - 8
  = 3·(27 - 3·8) - 8
  = 3·27 - 10·8
  = 3·27 - 10·(35 - 27)
  = 13·27 - 10·35
  = 13·(132 - 3·35) - 10·35
  = 13·132 - 49·35

- Πρώτοι αριθμοί
  - ✓ Ένας ακέραιος a ≥ 2 του οποίου οι μόνοι διαιρέτες είναι οι τετριμμένοι (1 και a) είναι πρώτος αριθμός (prime)
  - ✓ Οι πρώτοι αριθμοί διαδραματίζουν ειδικό ρόλο στην θεωρία αριθμών και στην κρυπτογραφία.
    - Πρώτοι 20 primes: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71
  - ✓ Ακέραιος a > 1 που δεν είναι πρώτος αναφέρεται ως σύνθετος (composite)
  - ✓ Ο 1 δεν είναι ούτε prime ούτε composite

- Πρώτοι αριθμοί
  - ✓ Κάποιοι μεγάλοι πρώτοι:
    - $(333+ 10^{793})10^{791} + 1$ (1585 ψηφία, βρέθηκε το 1987)
    - $2^{1257787} - 1$ (378632 ψηφία, βρέθηκε το 1996)
    - $2^{43112609} - 1$ (σχεδόν 13 εκατομ. ψηφία, Αύγουστος 2008)
    - Mersenne primes: πρώτοι της μορφής $2^m - 1$
      - Δεν είναι όλοι οι αριθμοί αυτής της μορφής πρώτοι
    - Fermat primes: πρώτοι της μορφής $2^{2^n} + 1$
      - Ομοίως δεν είναι όλοι οι αριθμοί αυτής της μορφής πρώτοι

Θεωρία Αριθμών

- Θεμελιώδες Θεώρημα Αριθμητικής: Κάθε ακέραιος μπορεί να γραφτεί με μοναδικό τρόπο ως γινόμενο από δυνάμεις πρώτων αριθμών

$$n = p_1^{e_1} p_2^{e_2} \ldots p_r^{e_r}$$

  - ✓ όπου p_i πρώτοι, $p_1 < p_2 < \cdots < p_r$, και e_i θετικοί ακέραιοι
  - ✓ Το 6000 γράφεται μοναδικά $2^4 \cdot 3 \cdot 5^3$
  - ✓ Απόδειξη με επαγωγή (strong induction)
  - ✓ Πόρισμα: Αν p πρώτος και p|ab, ➔ p|a ή p|b (δεν ισχύει όταν p δεν είναι πρώτος)

- Θεώρημα Ευκλείδη: Υπάρχουν άπειροι το πλήθος πρώτοι αριθμοί

- Απόδειξη: Έστω ότι είναι πεπερασμένοι το πλήθος, π.χ. $p_1, p_2, \ldots, p_n$. Θεωρήστε τον αριθμό $p_1 \cdot p_2 \cdot \ldots \cdot p_n + 1$.

- Ο gcd(a,b) θα μπορούσε να προκύψει από την παραγοντοποίηση των a, b σε πρώτους
- Έστω
  - $a = p_1^{e_1} p_2^{e_2} \ldots p_r^{e_r}$
  - $b = p_1^{f_1} p_2^{f_2} \ldots p_r^{f_r}$
- Τότε gcd (a, b) = $p_1^{\min\{e_1, f_1\}} \; p_2^{\min\{e_2, f_2\}} \; \ldots p_r^{\min\{e_r, f_r\}}$

✓ Θα ήταν αποδοτική μέθοδος αν μπορούσαμε να υπολογίσουμε τους παράγοντες p_i
  - Καμία μέθοδος μέχρι σήμερα δεν τους δίνει σε πολυωνυμικό χρόνο

✓ Ο αλγόριθμος του Ευκλείδη παραμένει ο πιο γρήγορος αλγόριθμος

- Πυκνότητα πρώτων αριθμών
- Πολύ σημαντική η γρήγορη εύρεση πρώτων στην κρυπτογραφία
- Πόσο πυκνοί είναι οι πρώτοι μέσα στο N?
- Θεώρημα: Για κάθε n≥1, υπάρχει πρώτος αριθμός μεταξύ n και 2n
- Αρχική απόδειξη: Chebyshev (1850)
- Απλούστερη απόδειξη: Erdos (1932), σε ηλικία 19 χρόνων!!

  Chebyshev said it
  and Erdos said it again
  there is always a prime
  between n and 2n

- Prime Number Theorem: Έστω Π(N) ο αριθμός των πρώτων μέχρι το N. Π(N) ~ N/logN

- Relatively prime numbers
  - ✓ Δύο ακέραιοι a, b είναι σχετικά πρώτοι μεταξύ τους (relatively prime) αν gcd(a, b) = 1.
    - Π.χ., 8 και 15 είναι relatively prime,
      - οι διαιρέτες του 8 είναι ο 1, 2, 4, και 8,
      - οι διαιρέτες του 15 είναι οι 1, 3, 5, και 15.
    - Από τον αλγόριθμο του Ευκλείδη μπορούμε να αποφασίζουμε σε πολυωνυμικό χρόνο αν 2 αριθμοί είναι σχετικά πρώτοι μεταξύ τους (θα μας χρειαστεί αργότερα)
  - ✓ <u>Παρατήρηση</u>:
    - gcd(a, p) = 1 και gcd(b, p) = 1, ➔ gcd(ab, p) = 1.

Euler's phi function

Ορισμός: Για κάθε $n \in N$ ορίζουμε τη συνάρτηση του Euler $\varphi(n)$ ως το πλήθος των αριθμών από 1 μέχρι n που είναι σχετικά πρώτοι με το n

Ιδιότητες:

- ✓ Για πρώτο αριθμό p: $\varphi(p)=p-1$
- ✓ $\varphi(p^{\alpha}) = p^{\alpha} - p^{\alpha-1} = p^{\alpha}(1-1/p)$
- ✓ $\varphi(mn) = \varphi(m)\varphi(n)$, αν $\gcd(m,n) = 1$

Πόρισμα: Για κάθε $n \in N$

$$\varphi(n) = n\prod_{p|n}\left(1-\frac{1}{p}\right)$$

(όπου το p αναφέρεται σε όλους τους πρώτους που διαιρούν το n)

Euler's phi function

- ✓ Απλοποίηση υπολογισμών
  - Π.χ., φ(45)=24, εφόσον οι πρώτοι παράγοντες του 45 είναι οι 3 και 5
    - φ(45)=45*(1-1/3)(1-1/5)=45*(2/3)(4/5)=24
  - $\varphi(1512) = \varphi(2^3*3^3*7) = \varphi(2^3)* \varphi(3^3) * \varphi(7) =$

    $(2^3-2^2) * (3^3-3^2)*(7-1)=4 * 18 * 6 = 432$
  - Υπάρχουν 432 ακέραιοι μεταξύ 1 και 1512 που είναι σχετικά πρώτοι με το 1512

- Διαίρεση, υπόλοιπα και ισοδυναμία
  - ✓ Δύο ακέραιοι είναι **ισοδύναμοι** *modulo n* αν ταυτίζονται ή αφήνουν το ίδιο υπόλοιπο όταν διαιρούνται με το n
  - ✓ Το συμβολίζουμε $a \equiv b \pmod{n}$
    - Από θεώρημα διαίρεσης: $a=q_1n+r_1$
    - Από θεώρημα διαίρεσης: $b=q_2n+r_2$
    - $a \equiv b \pmod{n}$ iff $r_1=r_2$
  - ✓ Με άλλα λόγια
    - $a \equiv b \pmod{n}$ iff $n \mid (a-b)$
  - ✓ Επομένως για κάθε θετικό *n* το σύνολο των ακεραίων κατανέμεται σε *n κλάσεις ισοδυναμίας* σε σχέση με τα υπόλοιπά τους, τις κλάσεις 0, 1, 2,..., n-1

- Διαίρεση, υπόλοιπα και ισοδυναμία
  - ✓ Κάθε κλάση αντιστοιχεί σε ένα από τα n πιθανά υπόλοιπα, r = 0,1,2,…, n-1 της διαίρεσης με το n
  - ✓ Συνήθως θα συμβολίζουμε μια κλάση ισοδυναμίας modulo n, με βάση τον αντιπρόσωπό της από το {0,1,2,…,n-1}
    - $[a]_n = \{a + kn : k \in Z\} = \{b \in Z \mid b \equiv a \pmod n\}$
      $= \{ \ldots, a-2n, a-n, a, a+n, a+2n, \ldots\}$
    - $[0]_n = \{..., -3n, -2n, -n, 0, n, 2n, 3n, \ldots\}$
    - $[1]_n = \{..., 1-3n, 1-2n, 1-n, 1, 1+n, 1+2n, 1+3n, \ldots\}$

    ……
    - $[n-1]_n = \{..., -1-2n, 1-n, -1, n-1, 2n-1, 3n-1, \ldots\}$

- Διαίρεση, υπόλοιπα και ισοδυναμία
  - ✓ Αν n=1 → όλοι οι ακέραιοι
  - ✓ Αν n=2 → $[0]_2$ είναι οι ζυγοί
    → $[1]_2$ είναι οι μονοί
  - ✓ Το σύνολο των διαφορετικών κλάσεων mod n δηλώνεται ως $Z_n = \{[a]_n: 0 \le a \le n-1\}$ ή αλλιώς $Z_n = \{0, 1, ..., n-1\}$
  - ✓ Αναφερόμαστε στο Z_n και ως το σύνολο ακεραίων mod n

Θεωρία Ομάδων

- ✓ Μια ομάδα (group) $(S, \oplus)$ είναί ένα σύνολο S μαζί με ένα τελεστή $\oplus: S \times S \rightarrow S$, έτσι ώστε να ισχύουν:
  - Κλειστότητα: Για κάθε $a, b \in S$, $(a \oplus b) \in S$
  - Προσεταιριστική ιδιότητα: Για κάθε $a, b, c \in S$, $(a \oplus b) \oplus c = a \oplus (b \oplus c)$
  - Ύπαρξη μοναδιαίου (ή ουδέτερου) στοιχείου (Identity): υπάρχει στοιχείο $e \in S$, έτσι ώστε $e \oplus a = a \oplus e = a$ για κάθε $a \in S$. Το συμβολίζουμε και με $e_{\oplus}$
  - Ύπαρξη αντιστρόφου (Inverse): για κάθε $a \in S$, υπάρχει στοιχείο $a^{-1} \in S$, που καλείται αντίστροφος του a, τέτοιο ώστε $a \oplus a^{-1} = a^{-1} \oplus a = e$
- ✓ Αν σε μια ομάδα $(S, \oplus)$ ικανοποιείται και η αντιμεταθετική ιδιότητα ($a \oplus b = b \oplus a$ για όλα τα $a, b \in S$), τότε την αποκαλούμε αβελιανή (abelian) ομάδα

- Ιδιότητες ομάδων
  - ✓ Απλοποίηση: για κάθε a, b, c ∈ S:
    - a ⊕ b = a ⊕ c → b = c (επειδή υπάρχει αντίστροφος)
  - ✓ Μοναδική λύση σε γραμμικές εξισώσεις: για κάθε a, b ∈ S:
    - η εξίσωση a ⊕ x = b έχει μοναδική λύση στο S την $x = a^{-1} \oplus b$
  - ✓ Το μοναδιαίο στοιχείο είναι μοναδικό
    - Αν υπήρχαν 2 μοναδιαία, e, e' τότε e = e ⊕ e' = e'
  - ✓ Ο αντίστροφος είναι μοναδικός
    - Έστω ότι υπήρχαν 2 αντίστροφοι y_1, y_2 για ένα στοιχείο x
    - Τότε: $y_1 = y_1 \oplus e = y_1 \oplus (x \oplus y_2) = (y_1 \oplus x) \oplus y_2 = e \oplus y_2 = y_2$
- Μια ομάδα (S, ⊕) είναι πεπερασμένη αν το σύνολο S έχει πεπερασμένο πλήθος στοιχείων
  - ✓ Τότε ο πληθικός αριθμός |S| ονομάζεται **τάξη** (order) της ομάδας

Παραδείγματα

- ✓ Το σύνολο των ακεραίων Z με τον τελεστή πρόσθεσης (δηλαδή η δομή (Z, +)) είναι αβελιανή ομάδα :
  - 0 είναι το μοναδιαίο στοιχείο
  - Ο αντίστροφος του a είναι ο –a
  - Ισχύει η προσεταιριστική ιδιότητα, και η αντιμεταθετικότητα
- ✓ Αντίθετα η δομή (Z, *) δεν είναι ομάδα
  - γιατί ο αντιστροφος του $\alpha \in Z$ δεν υπάρχει πάντα στο Z
- ✓ Τα σύνολα Z_n={0, 1, ..., n-1} αποτελούν ομάδες με πρόσθεση και πολλαπλασιασμό;

- Πράξεις και ισοτιμίες mod n

  - ✓ Αν $a \equiv a'(\mathrm{mod} n)$ και $b \equiv b'(\mathrm{mod} n)$ τότε
    - $a + b \equiv a' + b'(\mathrm{mod} n)$
    - $a * b \equiv a' * b'(\mathrm{mod} n)$
  - ✓ Επομένως ορίζουμε την πρόσθεση και τον πολλαπλασιασμό modulo n, ως $+_n$ και $*_n$, με
    - $a \bmod n +_n b \bmod n = (a+b) \bmod n$
      - $12\bmod 5+11\bmod 5=2\bmod 5+1\bmod 5=3\bmod 5 =23\bmod 5=(12+11)\bmod 5$
    - $a \bmod n *_n b \bmod n = (a*b) \bmod n$
  - ✓ Οι πράξεις εκτελούνται ως συνήθως, αλλά το αποτέλεσμα ανάγεται στην ισοδύναμη κλάση (στον αντιπρόσωπο)

- Τι είναι λοιπόν η αριθμητική υπολοίπων (Modular arithmetic);
  - ✓ Είναι αριθμητική σε ακεραίους
    - μόνο που εργαζόμαστε modulo n,
  - ✓ Έτσι στο Z_n κάθε πράξη $+_n$, $*_n$, εκτελείται κανονικά ως απλή πρόσθεση ή πολλαπλασιασμός αλλά το αποτέλεσμα αντικαθίσταται από ένα στοιχείο στο {0, 1, ..., n - 1}
    - Για παράδειγμα, στο Z_{25} ισχύουν:
    - 13+16=4, εφόσον 13+16=29=4mod25, και
    - 13·16=8 εφόσον 13·16=208=8mod25.

Πρόσθεση στο Z_6

$+_6$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

- Η δομή $(Z_n, +_n)$ είναι πεπερασμένη αβελιανή ομάδα τάξεως n
  - ✓ Η πράξη $+_n$ είναι προσεταιριστική
  - ✓ Είναι αντιμεταθετική
  - ✓ Υπάρχει μοναδιαίο στοιχείο και είναι το 0
    - $a +_n 0 = 0 +_n a = a$
  - ✓ Καθε στοιχείο $a \epsilon Z_n$ έχει αντίθετο το -a (≡ n-a modn)
    - $a +_n -a = 0$
    - Π.χ. στο Z_{13} $-4 = 9$

- Η δομή $(Z_n, *_n)$ είναι ομάδα?
  - ✓ Προσεταιριστικότητα και αντιμεταθετικότητα ισχύουν
  - ✓ Ύπαρξη μοναδιαίου: το 1
  - ✓ Ύπαρξη αντιστρόφου ως προς πολλαπλασιασμό?
  - ✓ Π.χ. Έχει αντίστροφο το 4 στο Z_6?
  - ✓ Δεδομένου ενός $a \in Z_n$ για να υπάρχει αντίστροφος, θα πρέπει να έχει λύση η εξίσωση $ax \equiv 1 (\mathrm{mod}\ n)$
  - ✓ Θεώρημα: $\gcd(a,n) = 1$ αν και μόνο αν $\exists x$ έτσι ώστε $ax \equiv 1 (\mathrm{mod}\ n)$

- Η δομή $(Z^*_n, *_n)$
  - ✓ Ας θεωρήσουμε το σύνολο

    $Z^*_n=\{a \in Z_n \mid \gcd(a, n) = 1\}$.
  - ✓ Τα στοιχεία του Z^*_n είναι τα στοιχεία του Z_n που είναι σχετικά πρώτοι με το n
  - ✓ Αν ο p είναι πρώτος, τότε $Z^*_p=\{a \mid 1 \le a \le p-1\} = Z_p \setminus \{0\}$
  - ✓ Παραδείγματα: $Z^*_{14}=\{1, 3, 5, 9, 11, 13\}$
    - $Z^*_{21}=\{1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20\}$
    - $Z^*_7=\{1, 2, 3, 4, 5, 6\}$
    - Προσέξτε ότι ο 7 είναι πρώτος, ενώ ο 21 όχι.

Θεωρία Ομάδων και Αριθμητική Υπολοίπων

- Η δομή $(Z^*_n, *_n)$ είναι πεπερασμένη αβελιανή ομάδα (συμβολίζεται και ως $U(Z_n)$)

  - ✓ Κλειστότητα: αν gcd(a,n) =1 και gcd(b, n) = 1 τότε και gcd(ab, n) = 1, το ab δεν μπορεί να έχει κοινούς διαιρέτες με το n
  - ✓ Προσεταιριστικότητα, αντιμεταθετικότητα, και ύπαρξη ουδέτερου στοιχείου (του 1), όπως και πρίν
  - ✓ Πώς κατασκευάζουμε τον πολλαπλασιαστικό αντίστροφο?
    - έστω a στοιχείο του Z^*_n (άρα gcd(a,n) = 1)
    - Τρέξε τον εκτενή αλγόριθμο Ευκλείδη ΕΑΕ(a, n).
    - Θα μας δώσει x, y τέτοια ώστε ax + ny = 1
    - Άρα $ax \equiv 1 \pmod n$,
    - Ο x είναι ο πολλαπλασιαστικός αντίστροφος του a
  - ✓ Η τάξη του Z^*_n είναι $\varphi(n)$

- Εφεξής
  - ✓ Όταν αναφερόμαστε σε κάποιο Z_n, οι πράξεις $+_n$ και $\cdot_n$ θα συμβολίζονται συνήθως με + και * (ή ·)
  - ✓ Ο multiplicative inverse του *a* δηλώνεται ως $a^{-1} \bmod n$.
  - ✓ Η διαίρεση στο $(Z^*_n, *)$ ορίζεται από την εξίσωση $a/b \equiv ab^{-1} \pmod n$
    - Παράδειγμα στο Z^*_{15}
    - Ισχύει $7^{-1} \equiv 13 \pmod{15}$, επειδή $7 \cdot 13 \equiv 91 \equiv 1 \pmod{15}$
    - οπότε $4/7 \equiv 4 \cdot 13 \equiv 7 \pmod{15}$

Γραμμικές Εξισώσεις Υπολοίπων

Έστω ότι θέλουμε να λύσουμε την εξίσωση $ax \equiv b \pmod n$, $a>0$, $n>0$

- ✓ Έχουμε ήδη αποδείξει ότι η $ax \equiv 1 \pmod n$ έχει λύση αν και μόνο αν $\gcd(a, n) = 1$.

Θεώρημα: Αν $d = \gcd(a, n)$, τότε η εξίσωση $ax \equiv b \pmod n$ έχει λύση αν και μόνο αν $d|b$. Αν x_0 μία λύση, τότε όλες οι λύσεις είναι της μορφής

$$x = x_0 + t(n/d),\ t \in Z$$

- ✓ Υπάρχουν ακριβώς d λύσεις mod n, με αντιπροσώπους

$x_0, x_1 = x_0 + (n/d), x_2 = x_0 + 2(n/d),\ldots, x_{d-1} = x_0 + (d-1)(n/d)$

- ✓ Όλες οι λύσεις είναι ισοδύναμες mod n/d

Γραμμ κές Εξ σώσε ς Υπολο πων

Πορίσματα:

- ✓ Η $ax \equiv b \pmod{n}$ είτε έχει d διακριτές λύσεις modulo n, όπου $d = \gcd(a, n)$, ή καμία

- ✓ Για κάθε $n > 1$, αν $\gcd(a, n) = 1$, τότε η εξίσωση $ax \equiv b \pmod{n}$ έχει μοναδική λύση modulo n.

Θεωρία Αριθμών και Θεωρία Ομάδων: Μέρος 2

Υπόβαθρο για το AES

Αριθμητική Υπολοίπων

Μια δομή (S, $\oplus$, $\otimes$) ονομάζεται δακτύλιος (ring) αν

- Η (S, $\oplus$) είναι αβελιανή ομάδα
- Η $\otimes$ προσεταιριστική: Για κάθε a, b, c ϵ S, (a $\otimes$ b) $\otimes$ c=a $\otimes$(b $\otimes$ c)
- Η $\otimes$ είναι επιμεριστική ως προς $\oplus$: a $\otimes$(b $\oplus$ c)=(a $\otimes$ b) $\oplus$(a $\otimes$ c) και (a $\oplus$ b) $\otimes$ c=(a $\otimes$ c) $\oplus$(b $\otimes$ c), για κάθε a, b, c ϵ S
- Αν η $\otimes$ ικανοποιεί την αντιμεταθετική ιδιότητα τότε η δομή αναφέρεται ως αντιμεταθετικός δακτύλιος
- Αν η $\otimes$ έχει μοναδιαίο στοιχείο αναφέρεται ως δακτύλιος με μοναδιαίο στοιχείο. Τα μοναδιαία στοιχεία θα τα συμβολίζουμε με $e_{\oplus}$ και $e_{\otimes}$ για τις $\oplus$ και $\otimes$ αντίστοιχα.

Παράδειγμα 1: Ο Δακτύλιος $(Z_8, +_8, *_8)$

- ✓ Είναι αντιμεταθετικός δακτύλιος

$+_8$	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

$*_8$	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

a	0	1	2	3	4	5	6	7
-a	0	7	6	5	4	3	2	1
a^{-1}	-	1	-	3	-	5	-	7

- Παράδειγμα 2: Ο Δακτύλιος πινάκων nxn (Π_{nxn}, +, *)

  - ✓ Το (Π_{nxn}, +) είναι αβελιανή ομάδα
  - ✓ Δεν ισχύει η αντιμεταθετική ιδιότητα ως προς πολλαπλασιασμό πινάκων
  - ✓ Δεν έχουν αντίστροφο όλοι οι nxn πίνακες (μόνο αυτοί που έχουν μη μηδενική ορίζουσα).

Αριθμητική Υπολοίπων

Μία δομή $(S, \oplus, \otimes)$ λέγεται σώμα ή πεδίο (field) αν

- ✓ Η $(S, \oplus)$ είναι αβελιανή ομάδα
- ✓ Η $(S- e_{\oplus}, \otimes)$ είναι αβελιανή ομάδα
- ✓ Ισχύει η επιμεριστική ιδιότητα της $\otimes$ ως προς $\oplus$
- ✓ Δηλαδή είναι ένας δακτύλιος όπου η $\otimes$ είναι αντιμεταθετική και έχει αντίστροφο και μοναδιαίο

Ιδιότητες πεδίου:

- ✓ Για κάθε a, b στο S οι εξισώσεις

  $a \oplus x = b$ και $a \otimes x = b$ $(a \neq 0)$ έχουν μοναδική λύση στο S

- ✓ Για κάθε a, b, c στο S ισχύουν οι κανόνες απλοποίησης και διαγραφής

  $a \oplus c = b \oplus c \rightarrow a = b$

  $a \otimes c = b \otimes c \rightarrow a = b$ iff $c \neq e_{\oplus}$

- ✓ Για κάθε a, b στο S ισχύει η συνεπαγωγή

  $a \otimes b = e_{\oplus} \rightarrow (a = e_{\oplus}$ ή $b = e_{\oplus})$

Παραδείγματα: Οι κάτωθι δομές είναι πεδία

- $(Q, +, *)$ των ρητών
- $(R, +, *)$ των πραγματικών
- $(C, +, *)$ των μιγαδικών
- $(\{0,1\}, +_2, *_2)$ των δυαδικών (είναι και πεπερασμένο)

+	0	1
0	0	1
1	1	0

*	0	1
0	0	0
1	0	1

Ερώτηση: Υπάρχουν άλλα πεδία με πεπερασμένο αριθμό στοιχείων?

Πεδία Galois

- Evariste Galois (1811-1832)
- Θεωρία Galois
  - ✓ Αρχικό πρόβλημα: εύρεση αναλυτικού τύπου για ρίζες πολυωνύμων 5ου ή μεγαλύτερου βαθμού

- Για κάθε πρώτο αριθμό p, η δομή $(Z_p, +_p, *_p)$ είναι πεπερασμένο πεδίο
  - ✓ $(Z_p, +_p)$ είναι αβελιανή ομάδα
  - ✓ $(Z_p^*, *_p)$ είναι αβελιανή ομάδα
  - ✓ Συμβολίζεται με GF(p) (πεδίο Galois τάξης p)
- Θεώρημα: Αν p πρώτος, το πεδίο Galois GF(p) είναι το μοναδικό πεπερασμένο πεδίο με p στοιχεία.
- Αν p δεν είναι πρώτος?

Πεδία Galois

- Πολυώνυμα στο πεδίο Galois GF(p)

- $Z_p[x]$ = Το σύνολο όλων των πολυωνύμων με συντελεστές από το GF(p). π.χ. $f(x)=a_0+a_1x+\ldots+a_kx^k$ με $a_i \in GF(p)$ (ο βαθμός συμβολίζεται ως deg(f))
- Πρόσθεση και πολλαπλασιασμός πολυωνύμων γίνεται ως συνήθως αλλά στο τέλος παίρνουμε τους συντελεστές mod p.

  Στο GF(3) $(2x^2 + x)2x = x^3 + 2x^2$
- Το $Z_p[x]$ με πρόσθεση και πολλαπλασιασμό mod p είναι δακτύλιος
- Παρατήρηση: υπάρχουν p^{k+1} πολυώνυμα βαθμού έως k στο $Z_p[x]$

Πεδία Galois

- Πολυώνυμα στο πεδίο Galois GF(p)
  - ✓ Για p=2 οι συντελεστές a_i είναι από το δυαδικό σύστημα
  - ✓ Πρόσθεση και πολλαπλασιασμός στο GF(2): XOR και AND

+	0	1
0	0	1
1	1	0

*	0	1
0	0	0
1	0	1

- Αρκετές ιδιότητες των ακεραίων του Z_p ισχύουν για τα πολυώνυμα του $Z_p[x]$
- Θα λέμε ότι $f(x) \mid g(x)$ αν υπάρχει $q(x) \in Z_p[x]$ έτσι ώστε $g(x) = q(x)f(x)$
- Για πολυώνυμα f(x), g(x), h(x) θα λέμε ότι $g(x) \equiv h(x) \pmod{f(x)}$ αν $f(x) \mid (g(x)-h(x))$

- Πολυώνυμα στο πεδίο Galois GF(p)
- Θεώρημα της διαίρεσης για πολυώνυμα: Έστω πολυώνυμα f(x), $g(x) \in Z_p[x]$ με deg(f) = n. Υπάρχουν μοναδικά πολυώνυμα q(x), $r(x) \in Z_p[x]$ έτσι ώστε:

  $g(x) = q(x)f(x) + r(x)$ και $deg(r) \leq n-1$

  ✓ r(x) είναι το υπόλοιπο της διαίρεσης, $g(x) \equiv r(x) \pmod{f(x)}$

  ✓ Παράδειγμα: έστω $g(x) = x^6 + x^4 + x^3 + x + 1$, $f(x) = x^3 + x + 1$

$$\begin{array}{l|l} x^6 + x^4 + x^3 + x + 1 & x^3 + x + 1 \\ \hline x^6 + x^4 + x^3 & x^3 = q(x) \\ \hline x + 1 & = r(x) \end{array}$$

  ✓ $g(x) = f(x) \cdot x^3 + x + 1$

- Πολυώνυμα στο πεδίο Galois GF(p)

- Η αντίστοιχη έννοια των πρώτων αριθμών στο $Z_p[x]$ είναι τα αμείωτα ή ανάγωγα (irreducible) πολυώνυμα.
- Ορισμός: Ένα πολυώνυμο f(x) με συντελεστές από ένα σώμα F ονομάζεται ανάγωγο (ή αμείωτο) στο F αν δεν είναι δυνατόν να βρεθούν δύο πολυώνυμα με συντελεστές από το F, με μικρότερο (αλλά θετικό) βαθμό, τέτοια ώστε το γινόμενό τους να είναι το f(x)
  - ✓ Το αν ένα πολυώνυμο είναι ανάγωγο εξαρτάται από το σώμα στο οποίο το θεωρούμε
  - ✓ Π.χ. $g(x) = 2x^2+x$ δεν είναι αμείωτο στο GF(3)
  - ✓ Το $g(x)=x^2+1$ αμείωτο στο GF(3)
  - ✓ Το $g(x) = x^4 + 1$ είναι ανάγωγο στο R αλλά όχι ανάγωγο στο GF(2) διότι: $g(x) = (x +1)(x^3 + x^2 + x +1)$ στο GF(2)

Πεδία Galois

- Πολυώνυμα στο πεδίο Galois GF(p)

- Δεδομένου ενός πολυωνύμου f(x) με deg(f) = n,

  $Z_p[x]/(f(x))$ = όλα τα πολυώνυμα του $Z_p[x]$ βαθμού ≤ n-1 : $p(x) = a_0+a_1x+\ldots+a_{n-1}x^{n-1}$ όπου $a_i \in GF(p)$ (= όλα τα πιθανά υπόλοιπα όταν διαιρούμε με f(x))

- Το $Z_p[x]/(f(x))$
  - ✓ περιέχει ακριβώς p^n πολυώνυμα
  - ✓ είναι δακτύλιος με πρόσθεση και πολ/μό πολυωνύμων mod f(x) (αν στον πολ/μό προκύψει πολυώνυμο βαθμού ≥ n, το ανάγουμε mod f(x))
  - ✓ Είναι πεδίο αν και μόνο αν το f(x) είναι ανάγωγο
  - ✓ Εύρεση αντιστρόφου γίνεται με εκτενή αλγόριθμο Ευκλείδη όπως και στο Z_p

Πεδία Galois

- Θεώρημα:
  - ✓ (i) Κάθε πεπερασμένο πεδίο έχει τάξη της μορφής p^n, όπου p πρώτος και n θετικός ακέραιος
  - ✓ (ii) Για κάθε πρώτο p και θετικό ακέραιο n, υπάρχει ένα μοναδικό πεπερασμένο πεδίο τάξης p^n, το οποίο συμβολίζουμε με $GF(p^n)$ και ταυτίζεται με το $Z_p[x]/(f(x))$, για κάποιο αμείωτο πολυώνυμο f(x) βαθμού n.
    - Αν υπαρχουν πολλά αμείωτα πολυώνυμα βαθμού n, δεν έχει σημασία ποιο επιλέγουμε. Τα πεδία που προκύπτουν είναι όλα ισομορφικά μεταξύ τους
- $GF(p^n)$: πολυώνυμα βαθμού αυστηρά μικρότερου του n με συντελεστές στο GF(p) και πράξεις πρόσθεση και πολ/μο mod f(x):
  - ✓ Οι συντελεστές ανάγονται mod p
  - ✓ Τα πολυώνυμα μετά τον πολ/μό ανάγονται mod f(x)

Πεδία Galois

- Πεπερασμένα πεδία μορφής GF(p^n)
  - ✓ Π.χ., για p=3 (άρα a_i =0,1,2), και n=2 έχουμε 9 πολυώνυμα:
    - 0 1 2
    - x x+1 x+2
    - 2x 2x+1 2x+2
  - ✓ Η αριθμητική επί των συντελεστών γίνεται modulo 3
- Πεπερασμένα πεδία μορφής GF(2^n)
  - ✓ Θα μας απασχολήσουν κυρίως τέτοια πεδία (π.χ. στο AES)
  - ✓ Υπάρχει πεπερασμένο πεδίο με 4 στοιχεία GF(4) = GF(2^2)
  - ✓ Υπάρχει πεπερασμένο πεδίο με 8 στοιχεία GF(8) = GF(2^3)
  - ✓ Δεν υπάρχει πεπερασμένο πεδίο με 6 στοιχεία
    - επειδή το 6 δεν είναι δύναμη κανενός πρώτου αριθμού.

- Πεπερασμένο πεδίο $GF(2^3)$ ή $GF(8)$

Integer Representation	Binary Representation	Element of GF(8)
0	000	0
1	001	1
2	010	A
3	011	A + 1
4	100	A^2
5	101	$A^2 + 1$
6	110	$A^2 + A$
7	111	$A^2 + A + 1$

τα πολυώνυμα είναι

0 1 x x+1

x^2 x^2+1 x^2+x x^2+x+1

Κάθε πολυώνυμο αντιστοιχεί σε ένα binary string με τους συντελεστές

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

Από πίνακα:

πολυώνυμο 6 + πολυώνυμο 3 =

πολυώνυμο 5

Ισοδύναμα: $(x^2+x) + (x+1) = x^2+1$

- Πεπερασμένο πεδίο $GF(2^3)$ ή $GF(8)$

Integer Representation	Binary Representation	Element of GF(8)
0	000	0
1	001	1
2	010	A
3	011	A + 1
4	100	A^2
5	101	$A^2 + 1$
6	110	$A^2 + A$
7	111	$A^2 + A + 1$

τα πολυώνυμα είναι

0	1	x	x+1
x^2	x^2+1	x^2+x	x^2+x+1

Κάθε πολυώνυμο αντιστοιχεί σε ένα binary string με τους συντελεστές

Πολλαπλασιασμός modulo αμείωτου πολυωνύμου: $f(x) = x^3+x+1$

Χρήση πινάκων για αποθήκευση όλων των πιθανών αποτελεσμάτων

Πως βρίσκουμε αμείωτο πολυώνυμο;

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

- Πεπερασμένο πεδίο GF(2^3) ή GF(8)

Integer Representation	Binary Representation	Element of GF(8)
0	000	0
1	001	1
2	010	A
3	011	A + 1
4	100	A^2
5	101	$A^2 + 1$
6	110	$A^2 + A$
7	111	$A^2 + A + 1$

Πως βρίσκουμε αμείωτο πολυώνυμο;

- ✓ Εμπειρικά
- ✓ Ένα πολυώνυμο f(x) βαθμού k ονομάζεται μονοειδές (monic) στο GF(p) αν ο συντελεστής a_k=1
- ✓ Γενικά ψάχνουμε για μονοειδή αμείωτα πολυώνυμα βαθμού n=3
- ✓ Ο σταθερός όρος πρέπει να είναι 1

- Πεπερασμένο πεδίο $GF(2^3)$ ή $GF(8)$

Integer Representation	Binary Representation	Element of GF(8)
0	000	0
1	001	1
2	010	A
3	011	A + 1
4	100	A^2
5	101	$A^2 + 1$
6	110	$A^2 + A$
7	111	$A^2 + A + 1$

αμείωτα είναι τα $p_1(x)=x^3+x+1$ και $p_2(x)=x^3+x^2+1$

Μπορούμε να επιλέξουμε π.χ. το $p_1(x)$

Πως βρίσκουμε αμείωτο πολυώνυμο;

- ✓ Εφόσον οι συντελεστές a_i μπορεί να είναι μόνο 0 και 1, υποψήφια:
  - $p_0(x) = x^3 + 1$
  - $p_1(x) = x^3 + x + 1$
  - $p_2(x) = x^3 + x^2 + 1$
  - $p_3(x) = x^3 + x^2 + x + 1$
  - Αλλά:
  - $p_0(x) = (x+1)(x^2+x+1)$
  - $p_3(x) = (x+1)(x^2+1)$

- Πεπερασμένα πεδία GF(2^m)

m	Default Primitive Polynomial	Integer Representation
1	D + 1	3
2	D^2 + D + 1	7
3	D^3 + D + 1	11
4	D^4 + D + 1	19
5	D^5 + D^2 + 1	37
6	D^6 + D + 1	67
7	D^7 + D^3 + 1	137
8	D^8 + D^4 + D^3 + D^2 + 1	285
9	D^9 + D^4 + 1	529
10	D^10 + D^3 + 1	1033
11	D^11 + D^2 + 1	2053
12	D^12 + D^6 + D^4 + D + 1	4179
13	D^13 + D^4 + D^3 + D + 1	8219
14	D^14 + D^10 + D^6 + D + 1	17475
15	D^15 + D + 1	32771
16	D^16 + D^12 + D^3 + D + 1	69643

Αμείωτα πολυώνυμα για διάφορα m

Αμείωτο πολυώνυμο

$m(x) = x^8+x^4+x^3+x+1$

Χρησιμοποιείται στα AES S-boxes

- Υπολογίζεται ο πολλαπλασιαστικός αντίστροφος για κάθε byte εισόδου A(x)
- Δηλαδή υπολογίζεται το πολυώνυμο *G*(x) τέτοιο ώστε

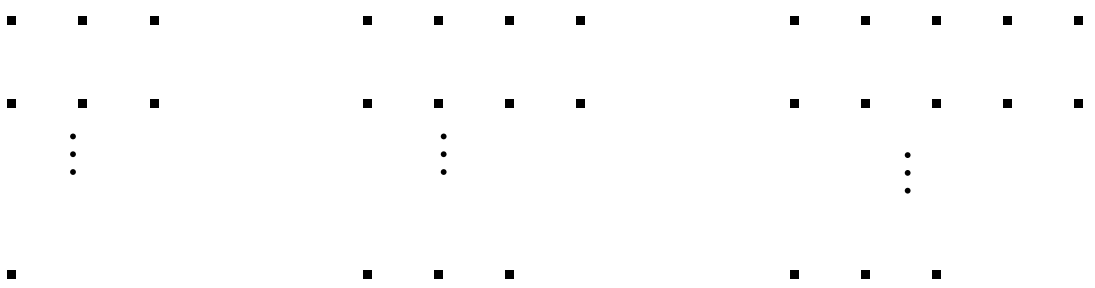
$$A(x)G(x)=1 \pmod{m(x)}$$

Θεωρία Αριθμών και Θεωρία Ομάδων: Μέρος 3

Υπόβαθρο για την Κρυπτογραφία Δημοσίου Κλειδιού

Σύστημα γραμμ κών εξ σώσεων - Chinese Remainder Theorem

- ✓ Γύρω στο 100 μ.Χ.
- ✓ Πρόβλημα: Υπάρχει ακέραιος x έτσι ώστε σε μία παρέλαση από x στρατιώτες, όταν στοιχίζονται σε
1. Τριάδες, περισσεύει 1 στην τελευταία γραμμή
2. Τετράδες, περισσεύουν 3 στο τέλος
3. Πεντάδες, περισσεύουν 3 στο τέλος



Chinese Remainder Theorem

Θεώρημα: Έστω n_1, n_2, ..., n_k θετικοί ακέραιοι σχετικά πρώτοι μεταξύ τους, δηλ. $\gcd(n_i, n_j) = 1$, $\forall\ i \neq j$. Τότε για οποιουσδήποτε ακεραίους a_1, a_2, ..., a_k, το σύστημα

$$x \equiv a_1 (\mathrm{mod}\ n_1),\ x \equiv a_2 (\mathrm{mod}\ n_2),\ \ldots,\ x \equiv a_k (\mathrm{mod}\ n_k),$$

έχει μοναδική λύση modulo n, όπου $n = n_1 n_2 \ldots n_k$.

Πόρισμα: Αν n_1, n_2, ..., n_k, θετικοί ακέραιοι σχετικά πρώτοι μεταξύ τους, τότε για όλους τους ακέραιους x και a, $x \equiv a (\mathrm{mod}\ n_i)$ για $i = 1, 2, \ldots, k$ αν και μόνο αν $x \equiv a (\mathrm{mod}\ n)$ όπου $n = n_1 n_2 \ldots n_k$.

Chinese Remainder Theorem

Απόδειξη

- Έστω $n_1, n_2, ..., n_k$ σχετικά πρώτοι μεταξύ τους
- Έστω $a_1, a_2, ..., a_k$ ακέραιοι
- $\forall i$ έστω $c_i = n/n_i$.
- $\gcd(c_i, n_i) = 1$ ➔ ο c_i έχει αντίστροφο mod n_i.
- Έστω d_i ο αντίστροφος, άρα $c_i d_i = 1 (\text{mod } n_i)$
- Ο ακέραιος $x^* = a_1c_1d_1 + a_2c_2d_2 + \ldots + a_kc_kd_k$ ικανοποιεί όλες τις εξισώσεις,

- Πολυπλοκότητα: πολυωνυμική μέσω του εκτενούς αλγορίθμου Ευκλείδη

Κινέζικο θεώρημα υπολοίπων - Παράδειγμα

- Ποιο x ικανοποιεί τις ακόλουθες εξισώσεις

  $x \equiv 2 \pmod 5$

  $x \equiv 3 \pmod{13}$
- $a_1=2, n_1=5, a_2=3, n_2=13$
- Υπολογίζουμε $n=n_1*n_2=5*13=65$, $c_1 = 65/5 = 13$, $c_2 = 5$
- Επειδή $13^{-1} \equiv 2 \pmod 5$ και $5^{-1} \equiv 8 \pmod{13}$, έχουμε $d_1=2$, $d_2=8$
  - Οι αντίστροφοι των c_1 και c_2 μπορούν να προκύψουν απο ΕΑΕ
- Τότε $x = a_1c_1d_1+a_2c_2d_2$

$$x \equiv 2 \cdot 2 \cdot 13 \cdot + 3 \cdot 5 \cdot 8 \pmod{65}$$
$$\equiv 52 + 120 = 42 \pmod{65}$$

Άρα όλες οι λύσεις είναι της μορφής $x(t)=42+65t$, $t \in Z$

Υποομάδες

- ✓ Αν $(S, \oplus)$ είναι ομάδα, $S' \subseteq S$, και $(S', \oplus)$ είναι ομάδα, τό $(S', \oplus)$ θα αναφέρεται ως υποομάδα του $(S, \oplus)$.
  - Π.χ., οι άρτιοι ακέραιοι είναι υποομάδα των ακεραίων στην πρόσθεση.
- ✓ Θεώρημα:
  - Ένα μη κενό και κλειστό υποσύνολο μιας πεπερασμένης ομάδας είναι υποομάδα
  - Π.χ., το σύνολο $(\{0, 2, 4, 6\}, +)$ είναι υποομάδα του $(Z_8, +)$ εφόσον είναι μη κενό και κλειστό ως προς + (κλειστό ως προς $+_8$).
- ✓ Θεώρημα Lagrange:
  - Αν $(S, \oplus)$ είναι πεπερασμένη ομάδα και $(S', \oplus)$ υποομάδα του $(S, \oplus)$, τότε $|S'|$ είναι διαιρέτης του $|S|$.

Υποομάδες

- Έστω υποομάδα πεπερασμένης ομάδας $(S, \oplus)$ και στοιχείο a σε αυτήν
- Έστω όλα τα στοιχεία που παράγονται από το a με τη χρήση του τελεστή της ομάδας.
  - $a^{(1)} = a$
  - $a^{(2)} = a \oplus a$
  - …
  - $a^{(k)} = a \oplus a \oplus \ldots a \oplus a$
  - ….
- Π.χ., από a=2 και ομάδα $(Z_6, +)$ παράγεται η ακολουθία 2, 4, 0, 2, 4, 0, 2, 4, 0, ...
- Από a=5 και ομάδα $(Z^*_6, *)$ παράγεται η ακολουθία 5,1,5,1,5,1, ...

- ***Υποομάδες***
  - ✓ Στην ομάδα $(Z_n, +)$ έχουμε $a^{(k)} = ka \bmod n$,
  - ✓ Στην ομάδα $(Z^*_n, *)$ έχουμε $a^{(k)} = a^k \bmod n$.
  - ✓ Για πεπερασμένες ομάδες, η ακολουθία $\{a^{(k)} : k \geq 1\}$ είναι περιοδική
  - ✓ Έστω ‹a› τα διαφορετικά στοιχεία που παράγονται στην ακολουθία $\{a^{(k)} : k \geq 1\}$
  - ✓ Θεώρημα: Η δομή (‹a›, ⊕) είναι υποομάδα (άσκηση)
  - ✓ Ο a αναφέρεται ως γεννήτορας της ‹a› και η (‹a›, ⊕) ως κυκλική ομάδα με γεννήτορα a
  - ✓ Κυκλικές υποομάδες στο $(Z_{6,}, +)$
    - ‹0› = {0} , ‹1› = {0,1,2,3,4,5} , ‹2› = {0,2,4}
  - ✓ Κυκλικές υποομάδες στο $(Z^*_7, *)$:
    - ‹1› = {1} , ‹2› = {1,2,4} , ‹3› = {1,2,3,4,5,6} = Z^*_7 (δηλαδή το Z^*_7 είναι κυκλική ομάδα)

- ***Υποομάδες***
- ***Πότε ε να κυκλ κή η ομάδα*** $(Z^*_n, *)$?

✓ <u>Θεώρημα 1:</u> Αν p πρώτος, η $(Z^*_p, *)$ είναι κυκλική ομάδα

✓ <u>Θεώρημα 2:</u> Αν $n = p^r$ όπου p περιττός πρώτος και $r \in N$, η $(Z^*_n, *)$ είναι κυκλική ομάδα

✓ <u>Θεώρημα 3:</u> Η ομάδα $(Z^*_n, *)$ είναι κυκλική αν και μόνο αν

$n = 1, 2, 4, p^r, 2p^r$, όπου p περιττός πρώτος και $r \in N$

Υποομάδες

- ✓ Τάξη ή ord(a): ο μικρότερος ακέραιος t τέτοιος ώστε $a^{(t)}=e$

- ✓ Θεώρημα
  - Τάξη στοιχείου = μέγεθος της υποομάδας που δημιουργεί (ord(a)= |‹a›|)
- ✓ Πόρισματα
  - Η ακολουθία $a^{(1)}$, $a^{(2)}$, ... είναι περιοδική με περίοδο t = ord(a)
  - $a^{(k)} = a^{(m)}$ αν και μόνο αν $k \equiv m \pmod t$
  - $a^{(k)} = a^{(k \bmod t)}$, όπου t = ord(a), για κάθε ακέραιο k

Δυνάμεις Στοιχείων σε υπόλοιπα

- Θεώρημα: Αν $(S, \oplus)$ πεπερασμένη ομάδα, τότε για κάθε $a \in S$, $a^{(|S|)} = e$, όπου e το ουδέτερο στοιχείο
- Απόδειξη με χρήση θεωρήματος Lagrange

- Πόρισμα 1: Μικρό Θεώρημα Fermat.
  - Αν p πρώτος, τότε $a^{p-1}=1 \pmod p$ για κάθε a ε $\mathbf{Z}^*_p$

- Πόρισμα 2: Θεώρημα Euler
  - Για κάθε ακέραιο n>1 $a^{\varphi(n)}=1 \pmod n$ για κάθε a ε $\mathbf{Z}^*_n$ (δηλ. για κάθε a με gcd(a, n) = 1)

Ύψωση σε δύναμη

- Έστω ότι θέλουμε να υπολογίσουμε το $a^b \bmod n$.
- Μπορεί να γίνει με b πολλαπλασιασμούς
- Εκθετική πολυπλοκότητα
- Μέθοδος επαναλαμβανόμενου τετραγωνισμού:
  - Αλγόριθμος που υπολογίζει το a^b με O(logb) πολλαπλασιασμούς
  - Στηρίζεται στη χρήση της δυαδικής αναπαράστασης του b $[b_{k-1}, ..., b_1, b_0]$ από MSB σε LSB (k ψηφία)
  - Δηλαδή $b = b_0 2^0 + b_1 2^1 + b_2 2^2 + \ldots + b_{k-2} 2^{k-2} + b_{k-1} 2^{k-1} = \sum b_i 2^i$
  - Αριθμός ψηφίων του ακεραίου b: $k = \lceil \log_2 (b+1) \rceil = O(\log b)$
- Ο αλγόριθμος υπολογίζει διαδοχικά τα $a^c \bmod n$ όπου το c παίρνει ως τιμές δυνάμεις του 2 (doublings)

Ύψωση σε δύναμη με επαναλαμβανόμενο τετραγων σμό (repeated squaring)

MODULAR-EXPONENTIATION(a, b, n)

1 $x \leftarrow a$
2 $y \leftarrow 1$
3 Let $[b_{k-1}, \ldots, b_1, b_0]$ be the binary representation of b
4 for $i \leftarrow 0$ to k-1
5 do
6 if $b_i = 1$ then $y = y \cdot x \bmod n$
7 $x = x^2 \bmod n$ //next power of 2
8 return y