ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ

ΚΡΥΠΤΟΓΡΑΦΙΑ

4η Διάλεξη

Κωνσταντίνου Ελισάβετ

Τμήμα Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων

Άδειες Χρήσης

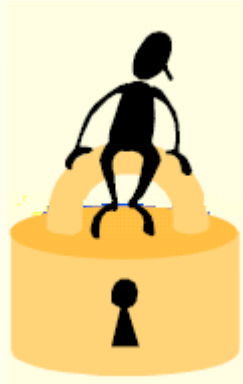
- Το παρόν εκπαιδευτικό υλικό υπόκειται σε άδειες χρήσης Creative Commons.
- Για εκπαιδευτικό υλικό, όπως εικόνες, που υπόκειται σε άλλου τύπου άδειας χρήσης, η άδεια χρήσης αναφέρεται ρητώς.

Χρηματοδότηση

- Το παρόν εκπαιδευτικό υλικό έχει αναπτυχθεί στα πλαίσια του εκπαιδευτικού έργου του διδάσκοντα.
- Το έργο «**Ανοικτά Ακαδημαϊκά Μαθήματα στο Πανεπιστήμιο Αιγαίου**» έχει χρηματοδοτήσει μόνο τη αναδιαμόρφωση του εκπαιδευτικού υλικού.
- Το έργο υλοποιείται στο πλαίσιο του Επιχειρησιακού Προγράμματος «Εκπαίδευση και Δια Βίου Μάθηση» και συγχρηματοδοτείται από την Ευρωπαϊκή Ένωση (Ευρωπαϊκό Κοινωνικό Ταμείο) και από εθνικούς πόρους.

Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

Κρυπτογραφία



Κωνσταντίνου Ελισάβετ
ekonstantinou@aegean.gr

http://www.icsd.aegean.gr/ekonstantinou

Η συνάρτηση φ(.) του Euler

Για κάθε ακέραιο n > 0, έστω φ(n) το πλήθος των ακεραίων στο διάστημα [1, n] που είναι **σχετικά πρώτοι με το n**. Η συνάρτηση φ(.) καλείται Euler phi function.

Ιδιότητες:

1) Αν **p είναι πρώτος**, τότε $\varphi(p) = p-1$.
2) Αν **gcd(n, m) = 1**, τότε $\varphi(nm) = \varphi(n)\varphi(m)$.
3) Αν $n = p_1^{e1}p_2^{e2}\ldots p_k^{ek}$ τότε $\varphi(n) = n(1-1/p_1)(1-1/p_2)\ldots(1-1/p_k)$.

Παράδειγμα:

$\varphi(20) = 20(1-1/2)(1-1/5) = 8$.

Πράγματι, οι αριθμοί στο [1,20] που είναι σχετικά πρώτοι με το 20 είναι οι 1,3,7,9,11,13,17 και 19.

Euler, 1707-1783

Ισοδυναμίες και Ισοτιμίες

Ορισμός: Έστω n ένας θετικός ακέραιος. Ο ακέραιος a καλείται ισότιμος (congruent) με τον ακέραιο b modulo n, συμβολικά

$$a \equiv b \bmod n$$

αν n | a-b (δηλαδή αν η ποσότητα a-b διαιρείται με το n) ή διαφορετικά αν a = kn + b για κάποιον ακέραιο k. Αν το n δεν διαιρεί το a-b, τότε ο a καλείται ανισότιμος με τον b modulo n, συμβολικά

$$a \not\equiv b \bmod n$$

Παραδείγματα:

$24 \equiv 9 \bmod 5$ $24 \equiv 39 \bmod 5$

$24 \equiv 4 \bmod 5$ $-11 \equiv 3 \bmod 7$ $-4 \equiv -13 \bmod 9$

Ισοδυναμίες και Ισοτιμίες

Η σχέση ισοτιμίας $\equiv$ είναι μία σχέση ισοδυναμίας στο $\mathbb{Z}$ (σύνολο ακεραίων). Δηλαδή ισχύουν τα εξής:

1) $a \equiv a \bmod n$ για κάθε a στο $\mathbb{Z}$
2) $a \equiv b \bmod n \implies b \equiv a \bmod n$
3) αν $a \equiv b \bmod n$ και $b \equiv c \bmod n \implies a \equiv c \bmod n$
4) αν $a \equiv a_1 \bmod n$ και $b \equiv b_1 \bmod n \implies a + b \equiv a_1 + b_1 \bmod n$ και $ab \equiv a_1 b_1 \bmod n$

Για κάθε a που ανήκει στο $\mathbb{Z}$, η κλάση ισοδυναμίας του a είναι η $[a] = \{x \in \mathbb{Z} \mid x \equiv a \bmod n\}$ και καλείται κλάση ισοτιμίας ή κλάση υπολοίπων του $a \bmod n$.

Ισοδυναμίες και Ισοτιμίες

Ορισμός: Οι ακέραιοι modulo n, συμβολίζονται με $\mathbb{Z}_n$ και είναι το σύνολο των κλάσεων ισοδυναμίας των {0, 1, 2, ..., n-1}. Όλες οι πράξεις στο $\mathbb{Z}_n$ γίνονται modulo n.

Το σύνολο $\mathbb{Z}_n$ αποτελεί αντιμεταθετικό δακτύλιο.

Αν το n είναι πρώτος, τότε το σύνολο $\mathbb{Z}_n$ είναι σώμα (συνήθως συμβολίζεται με $\mathbb{F}_p$ και καλείται πρώτο πεπερασμένο σώμα).

γιατί??

Ισοδυναμίες και Ισοτιμίες

Παραδείγματα:

1) Έστω ο δακτύλιος $\mathbb{Z}_{25}$. Αυτός αποτελείται από τα στοιχεία {0, 1, 2, ..., 24}. Αν a = 8 και b = 13 είναι δύο στοιχεία του $\mathbb{Z}_{25}$, υπολογίστε τα αποτελέσματα των πράξεων a+b, a-b, και ab.

Λύση:

a+b = 8+13 = 21 ≡ 21 mod 25

a-b = 8-13 = -5 ≡ 20 mod 25

ab = 8*13 = 104 ≡ 4 mod 25

2) Ποια από τα παρακάτω είναι σωστά?

31 ≡ 53 mod 22, 31 = 53 mod 22

7 ≡ 21 mod 14, 7 = 21 mod 14

21 ≡ 7 mod 14, 21 = 7 mod 14

Ισοδυναμίες και Ισοτιμίες

Πώς ορίζεται η διαίρεση στο $\mathbb{Z}_n$?

Ένα στοιχείο a του $\mathbb{Z}_n$ λέμε ότι είναι αντιστρέψιμο αν υπάρχει ένας αριθμός x στο $\mathbb{Z}_n$ για τον οποίο ισχύει ότι

$$ax \equiv 1 \bmod n$$

Δεν έχουν όλοι οι αριθμοί στο $\mathbb{Z}_n$ αντίστροφο. Συγκεκριμένα, ένας αριθμός a στο $\mathbb{Z}_n$ αντιστρέφεται αν και μόνο αν $\gcd(a, n) = 1$.

Άρα, για να μπορεί να οριστεί η πράξη a/b στο $\mathbb{Z}_n$ θα πρέπει το b να αντιστρέφεται.

Ισοδυναμίες και Ισοτιμίες

Παράδειγμα:

Έστω τα στοιχεία a = 7 και b = 9 του δακτυλίου $\mathbb{Z}_{14}$. Υπολογίστε τα a/b και b/a.

Λύση:

Αρχικά πρέπει να δούμε αν τα a και b αντιστρέφονται. Ισχύει ότι gcd(a, 14) = 7 και gcd(b, 14) = 1. Άρα ορίζεται μόνο η πράξη a/b. Το $b^{-1} = 9^{-1} \equiv 11 \bmod 14$ (γιατί $9*11 \equiv 1 \bmod 14$).

Άρα, $a/b = 7*11 = 77 \equiv 7 \bmod 14$.

Ερώτημα: Γιατί το $\mathbb{Z}_n$ αποτελεί σώμα αν το n είναι πρώτος?

Ισοδυναμίες και Ισοτιμίες

Ορισμός: Αν n > 1 είναι ένας φυσικός αριθμός και a ένας ακέραιος τέτοιος ώστε gcd(a, n) = 1, τότε ο μικρότερος θετικός ακέραιος r με την ιδιότητα

$$a^r \equiv 1 \bmod n$$

καλείται τάξη (order) του a mod n.

(η τάξη ορίζεται μόνο για τα αντιστρέψιμα στοιχεία του $\mathbb{Z}_n$)

Ορισμός: Η πολλαπλασιαστική ομάδα του $\mathbb{Z}_n$ είναι η $\mathbb{Z}_n^* = \{a \in \mathbb{Z}_n \mid \gcd(a, n) = 1\}$. Δηλαδή η πολλαπλασιαστική ομάδα αποτελείται από τα αντιστρέψιμα στοιχεία του $\mathbb{Z}_n$. Η τάξη $|\mathbb{Z}_n^*|$ του $\mathbb{Z}_n^*$ είναι ίση με φ(n). Αν n είναι πρώτος αριθμός, τότε $\mathbb{Z}_n^* = \{1, 2, \ldots, n-1\}$.

Δύο Βασικά Θεωρήματα

Θεώρημα του Euler:
Αν $a \in \mathbb{Z}_n^*$ τότε $a^{\varphi(n)} \equiv 1 \bmod n$.

Η τάξη οποιουδήποτε στοιχείου του $\mathbb{Z}_n^*$ είναι είτε ίση με φ(n) ή διαιρεί ακριβώς το φ(n).

Μικρό Θεώρημα του Fermat:
Έστω p ένας πρώτος αριθμός. Αν gcd(a, p) = 1 για κάποιον ακέραιο αριθμό a, τότε $a^{p-1} \equiv 1 \bmod p$.

Fermat, 1601-1665

Γεννήτορες Ομάδων

Αν για κάποιο στοιχείο α του $\mathbb{Z}_n^*$ η τάξη του είναι ίση με φ(n), τότε το στοιχείο αυτό καλείται γεννήτορας του $\mathbb{Z}_n^*$.

Δηλαδή ισχύει ότι $\mathbb{Z}_n^* = \{a^i \bmod n \mid 0 \le i \le \varphi(n) - 1\}$.

Κάθε ομάδα που έχει έναν τουλάχιστον γεννήτορα καλείται κυκλική.

Πώς δημιουργείται ένας γεννήτορας για μια κυκλική ομάδα?

→ αν μια κυκλική ομάδα έχει τάξη t, τότε κάθε γεννήτορας θα έχει τάξη t

→ η τάξη οποιουδήποτε άλλου στοιχείου της ομάδας θα πρέπει να διαιρεί ακριβώς το t

Αλγόριθμος Δημιουργίας Γεννήτορα

ΑΛΓΟΡΙΘΜΟΣ 1.2.1 ***Μέθοδος υπολογισμού ενός γεννήτορα*** a ***μιας κυκλικής ομάδας*** G ***με τάξη*** t.
Είσοδος: *Η ομάδα* G *και η τάξη της* $t = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$.
Έξοδος: *Ένας γεννήτορας* a *της ομάδας* G.

1. Επέλεξε ένα τυχαίο $a \in G$
2. **Για** $i = 1$ μέχρι k **υπολόγισε**
{
   $s = a^{\frac{t}{p_i}}$
   αν $s = 1$ **τότε** πήγαινε στο βήμα 1
}
3. Επέστρεψε στην έξοδο το a.

Παρατηρήσεις πάνω στον Αλγόριθμο

1) Αν η ομάδα G είναι ίση με $\mathbb{Z}_p^*$ όπου p είναι ένας πρώτος αριθμός, τότε η τάξη t = p-1 και όλες οι πράξεις a^{t/p_i} γίνονται modulo p.
2) Αν η ομάδα G είναι ίση με $\mathbb{Z}_n^*$ όπου n είναι ένας σύνθετος αριθμός, τότε η τάξη t = φ(n) και όλες οι πράξεις a^{t/p_i} γίνονται modulo n.
3) Τέλος, για να βρεθούν οι πρώτοι παράγοντες της τάξης της ομάδας θα πρέπει να εφαρμοστεί ένας αλγόριθμος παραγοντοποίησης. Εναλλακτικά, αν ζητείται να δημιουργηθεί γεννήτορας για μια ομάδα $\mathbb{Z}_p^*$ όπου p είναι ένας πρώτος αριθμός, τότε αρκεί να βρεθεί ένα p_1 τέτοιο ώστε η τάξη $t = p-1 = 2p_1$.

Τετραγωνικά Υπόλοιπα

Ορισμός: Έστω η ισοτιμία

$$x^2 \equiv a \bmod n$$

όπου n φυσικός αριθμός και a ακέραιος αριθμός σχετικά πρώτος προς τον n (δηλαδή a ανήκει στο Z_n^*). Τότε ο a θα καλείται τετραγωνικό υπόλοιπο (quadratic residue) modulo n. Αν δεν υπάρχει x που να ικανοποιεί την παραπάνω ισοτιμία, τότε ο a καλείται μη-τετραγωνικό υπόλοιπο (quadratic non-residue) modulo n.

Το σύνολο των τετραγωνικών υπολοίπων modulo n θα το συμβολίζουμε με Q_n και το σύνολο των μη-τετραγωνικών υπολοίπων με $\overline{Q_n}$.

Τετραγωνικά Υπόλοιπα

Για κάθε περιττό πρώτο αριθμό p υπάρχουν ακριβώς (p-1)/2 τετραγωνικά υπόλοιπα και (p-1)/2 μη-τετραγωνικά υπόλοιπα modulo p. Δηλαδή τα μισά στοιχεία του Z_p^* είναι τετραγωνικά υπόλοιπα και τα άλλα μισά όχι.

Αν ο αριθμός α είναι τετραγωνικό υπόλοιπο modulo p, τότε ισχύει ότι

$$a^{(p-1)/2} \equiv 1 \bmod p$$

και αν δεν είναι τότε

$$a^{(p-1)/2} \equiv -1 \bmod p.$$

Οι ισοτιμίες αυτές χρησιμοποιούνται για να ελεγχθεί εάν ένας αριθμός είναι τετραγωνικό υπόλοιπο ή όχι.

Το Σύμβολο του Legendre

Το σύμβολο του Legendre $\left(\frac{a}{p}\right)$, όπου p είναι ένας πρώτος αριθμός και a ένας ακέραιος αριθμός σχετικά πρώτος ως προς τον p, ορίζεται ως

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \bmod p$$

Δηλαδή το σύμβολο του Legendre επιστρέφει την τιμή 1 αν ο a είναι τετραγωνικό υπόλοιπο modulo p και την τιμή -1 αν δεν είναι.

Τα σύμβολα των Jacobi και Kronecker γενικεύουν το σύμβολο του Legendre σε οποιοδήποτε ακέραιο b.

Κινέζικο Θεώρημα Υπολοίπου

Κινέζικο Θεώρημα Υπολοίπου (Chinese Remainder Theorem - CRT):

Αν οι ακέραιοι n_1, n_2, …, n_k είναι ανά δύο πρώτοι μεταξύ τους, τότε το σύστημα των ισοτιμιών

$$x \equiv a_1 \bmod n_1$$
$$x \equiv a_2 \bmod n_2$$
$$.$$
$$.$$
$$x \equiv a_k \bmod n_k$$

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

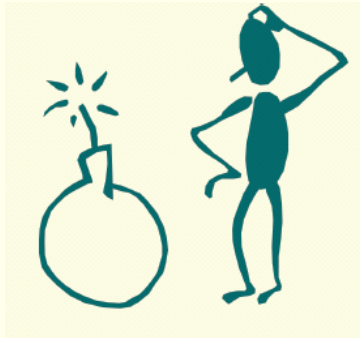
Η λύση των παραπάνω ισοτιμιών υπολογίζεται από τον αλγόριθμο του Gauss.

$$x \equiv \sum_{i=1}^{k} a_i N_i M_i \pmod{n} \qquad N_i = n/n_i \qquad M_i = N_i^{-1} \pmod{n_i}.$$

Παράδειγμα

Ένας Κινέζος στρατηγός κάθε πρωί μετράει τους στρατιώτες του και με την παρακάτω μέθοδο βρίσκει πόσοι λείπουν από τους 1000 συνολικά που έχει, στην πρωινή αναφορά τους: τους ζητά να παραταχτούν σε σειρές των 11, 13 και 17, και μετρά πόσοι περισσεύουν κάθε φορά.

Αν ένα πρωί δει ότι περισσεύουν 3 από τις σειρές των 11, 4 από τις σειρές των 13 και 9 από τις σειρές των 17, πόσοι συνολικά είναι οι στρατιώτες που έχουν παρουσιαστεί?



Πως βρίσκω τον αντίστροφο?

Αλγόριθμος του Ευκλείδη:

If a > b, then gcd(a, b) = gcd(b, a mod b).

Επεκταμένος αλγόριθμος του Ευκλείδη:

Input: a, b
Output: d = gcd(a, b) and x,y s.t. ax + by = d.

- Πως μπορώ να χρησιμοποιήσω τον επεκταμένο αλγόριθμο του Ευκλείδη για να βρω το a^{-1} mod n?

Πως δημιουργείται ένας πρώτος?

Διαδικασία:

1. Δημιουργείται ένας τυχαίος περιττός αριθμός κατάλληλου μεγέθους.
2. Ελέγχεται αν είναι πρώτος
3. Αν είναι σύνθετος, επιστρέφουμε στο 1ο βήμα.

Στο 2ο βήμα ο αλγόριθμος ελέγχου μπορεί να αποδεικνύει ότι ο αριθμός είναι πρώτος (provable prime) ή να καταδεικνύει ότι με μεγάλη πιθανότητα ο αριθμός είναι πρώτος (probable prime).

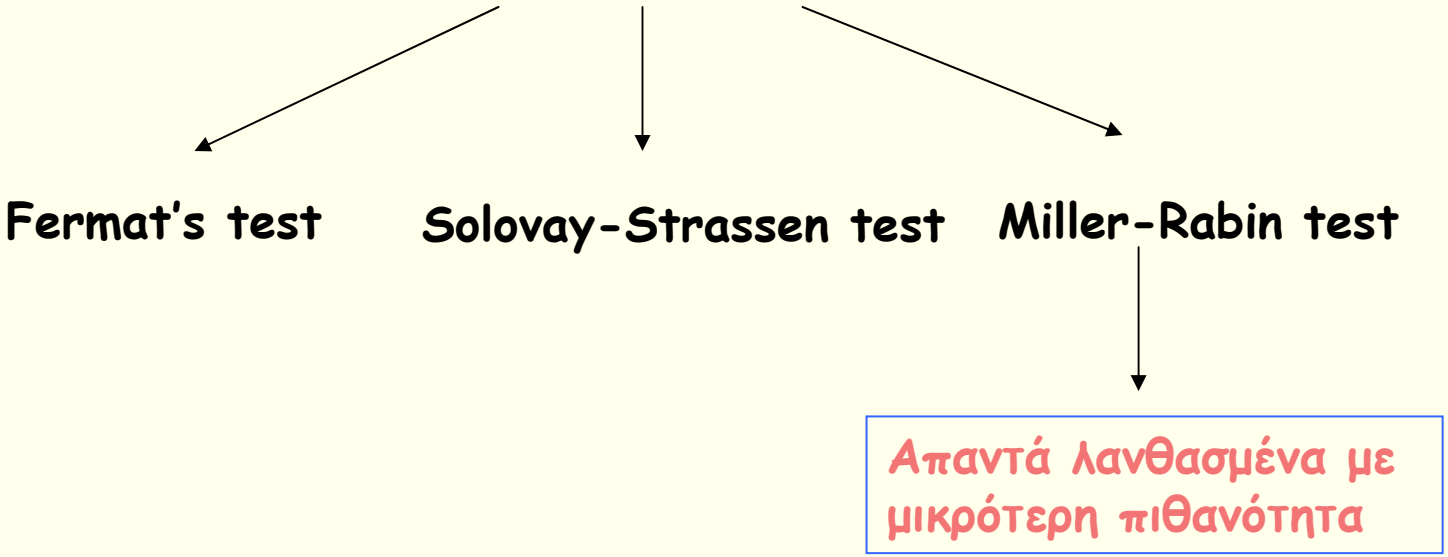
Προφανώς η δεύτερη κατηγορία αλγορίθμων είναι πολύ πιο αποδοτική από την πρώτη.

Έλεγχοι Πρώτου Αριθμού

A) True Primality Tests

→ **Αποδεικνύουν με βεβαιότητα ότι ένας αριθμός είναι πρώτος**

B) Probabilistic Primality Tests



Μια σημαντική ανακάλυψη...

Μέχρι τις αρχές του 21ου αιώνα δεν υπήρχε ντετερμινιστικός αλγόριθμος πολυωνυμικού χρόνου που να αποφασίζει εάν ένας περιττός αριθμός είναι πρώτος ή όχι (true primality test). Μάλιστα, υπήρχε η εικασία ότι για το συγκεκριμένο πρόβλημα δεν θα μπορούσε να υπάρξει πολυωνυμικός αλγόριθμος.

Primes is in P!

Agrawal, Kayal, Saxena, 2002

Πιθανοτικός Έλεγχος Miller-Rabin

Βασίζεται στην παρακάτω πρόταση:

Έστω ότι n είναι ένας πρώτος αριθμός και $n-1 = 2^r s$, όπου s περιττός. Για κάθε a ο οποίος είναι σχετικά πρώτος με τον n (gcd(a, n) = 1) ισχύει είτε $a^s \equiv 1 \bmod n$ ή $a^{2^j s} \equiv -1 \bmod n$ για κάποιο j, $0 \le j \le r-1$.

Αν ο n <u>ΔΕΝ</u> είναι πρώτος, αλλά παρόλα αυτά ισχύει είτε ότι $a^s \equiv 1 \bmod n$ ή $a^{2^j s} \equiv -1 \bmod n$ για κάποιο j, τότε ο a καλείται strong liar για τον n (συμπεριφέρεται σαν πρώτος).

Διαφορετικά, καλείται strong witness.

Πιθανοτικός Έλεγχος Miller-Rabin

ΑΛΓΟΡΙΘΜΟΣ 5.3.1 ***Πιθανοτικός έλεγχος των Miller-Rabin.***
Είσοδος: *Ένας ακέραιος $n \geq 3$ και μια παράμετρος t.*
Έξοδος: *Το 0 αν ο n δεν είναι πρώτος και 1 αν είναι.*

Βρες θετικό ακέραιο r και περιττό s τέτοιους ώστε $n-1 = 2^r s$.

Για $i = 1$ μέχρι t **υπολόγισε**
{
  τυχαίο ακέραιο a, με $2 \leq a \leq n-2$.
  $x = a^s \pmod{n}$
  αν $x \neq 1$ και $x \neq n-1$ **τότε**:
  {
    θέσε $j = 1$
    όσο $j \leq r-1$ και $x \neq n-1$ **υπολόγισε**:
    {
      $x = x^2 \pmod{n}$
      αν $x = 1$ επέστρεψε στην έξοδο το 0 (ο n δεν είναι πρώτος)
      $j = j + 1$
    }
    αν $x \neq n-1$ επέστρεψε στην έξοδο το 0 (ο n δεν είναι πρώτος)
  }
}

Επέστρεψε στην έξοδο το 1 (ο n είναι πρώτος).

Πιθανοτικός Έλεγχος Miller-Rabin

Μια εύλογη τιμή για την παράμετρο t είναι η 10 ή 20.

Για κάθε ακέραιο n που δεν είναι πρώτος, η πιθανότητα ο αλγόριθμος των Miller-Rabin να επιστρέψει λάθος αποτέλεσμα είναι $(1/4)^t$.

Διάβασμα…

Σημειώσεις μαθήματος, Κεφάλαια 2.4, 2.5, 4.1 και 4.2 του Handbook of Applied Cryptography, βιβλιογραφικές αναφορές που υπάρχουν στις σημειώσεις