Κρυπτογραφία

Έλεγχος πρώτων αριθών-Παραγοντοποίηση

Διαφάνειες: Άρης Παγουρτζής – Πέτρος Ποτίκας

Εθνικό Μετσόβιο Πολυτεχνείο
Σχολή Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών

Εισαγωγή

Υπολογιστικά δύσκολο πρόβλημα θεωρίας αριθμών: παραγοντοποίηση

Δίνεται ένας σύνθετος αριθμός N, το πρόβλημα της παραγοντοποιήσης είναι να βρούμε θετικούς ακεραίους p, q, τ.ώ. $pq = N$

Μπορεί να λυθεί *δοκιμάζοντας διαιρέσεις* , διαιρώντας με όλους τους περιττούς από 2 έως $\sqrt{N}$

Εκθετικός χρόνος ως προς το μήκος του N ($\sqrt{N}$ διαιρέσεις, χρόνου $(log(N)^c$, για κάποια σταθερά c)

Κρυπτογραφία, οι ποιο δύσκολο να παραγοντοποιηθούν αριθμοί είναι αυτοί που είναι γινόμενο μεγάλων πρώτων αριθμών

Θέλουμε να παράγουμε *αποδοτικά* δύο n-bit μεγάλους πρώτους, ώστε $N = pq$

Εισαγωγή

- Αλγόριθμος παραγωγής τυχαίου πρώτου μήκους n-bits

  Είσοδος: μήκος n; παράμετρος t
  Έξοδος : Ένας τυχαίος n-bit πρώτος

  for $i = 1$ to t **do** :
  $p' \leftarrow \{0,1\}^{n-1}$
  $p := 1||p'$
  if p is prime return p
  return fail

1. Πιθανότητα να είναι πρώτος αριθμός
2. Έλεγχος αν είναι πρώτος αριθμός

Εισαγωγή

$\pi(N)$: το πλήθος των πρώτων που είναι μικρότεροι ή ίσοι με το N

Από **θεώρημα πρώτων αριθμών**: $\pi(N) \approx N/lnN$

Αν ένας ακέραιος p επιλεγεί τυχαία από το 1 ως το N, τότε η πιθανότητα να είναι πρώτος είναι $1/lnN$

Για n 1024-bits, με $n = pq$, τα p, q είναι 512-bits, και η πιθανότητα ενός τυχαίου ακεραίου 512-bits να είναι πρώτος είναι 1/355 (ή 2/355, αν πάρω περιττό)

Έλεγχος αν ένας αριθμός είναι πρώτος

Έλεγχος αν ένας αριθμός είναι πρώτος

Το 1970 οι πρώτοι αποδοτικοί *πιθανοτικοί* αλγόριθμοι αναπτύχθηκαν

Ιδιότητα: Αν η είσοδος p είναι πρώτος, τότε η έξοδος είναι πάντα "πρώτος". Αν ο p είναι σύνθετος, τότε η έξοδος είναι "σύνθετος" με μεγάλη πιθανότητα. Ισοδύναμα, αν η έξοδος είναι "σύνθετος", τότε σίγουρα είναι σύνθετος, ενώ αν είναι "πρώτος", τότε πολύ πιθανά να είναι πρώτος (ενώ πραγματικά είναι σύνθετος).

Δύο πηγές σφάλματος: μία από την επιλογή τυχαίου υποψήφιου πρώτου και μία από τον έλεγχο αν είναι πρώτος

Fermat (primality) test

Έλεγχος Fermat

Για να δούμε αν ένας δοσμένος ακέραιος n είναι πρώτος:

Επιλέγουμε τυχαία $a \in \mathbb{Z}_n$: αν $a^{n-1} \not\equiv 1 \pmod{n}$ τότε n σύνθετος (με βεβαιότητα), αλλιώς λέμε ότι το *n περνάει το test* (ίσως είναι πρώτος). Στην δεύτερη περίπτωση επαναλαμβάνουμε.

Πρόταση.

Αν για σύνθετο n υπάρχει ένας μάρτυρας (witness) (δηλ. $a \in \mathbb{Z}_n$, $a^{n-1} \not\equiv 1 \pmod{n}$*), τότε υπάρχουν τουλάχιστον* $n/2$ *μάρτυρες.*

Απόδειξη. Χρήση Θ. Lagrange στην ομάδα των μη μαρτύρων του $U(\mathbb{Z}_n)$.

Πόρισμα: ο έλεγχος Fermat απαντάει σωστά με πολύ μεγάλη πιθανότητα για τους περισσότερους αριθμούς. Εξαιρούνται όμως οι αριθμοί Carmichael: σύνθετοι για τους οποίους δεν υπάρχει μάρτυρας Fermat. Για να καλύψουμε και αυτούς: Miller-Rabin test.

Έλεγχος πρώτων αριθμών Miller-Rabin

1. Έστω $n \in \mathbb{Z}$ θετικός περιττός αριθμός.
2. Επιλέγουμε τυχαία $b \in [2, \ldots, n-1]$. Αν $b^{n-1} \mod n \neq 1$, τότε το n δεν περνάει τον έλεγχο (είναι σίγουρα σύνθετος).

Έλεγχος πρώτων αριθμών Miller-Rabin

1. Έστω $n \in \mathbb{Z}$ θετικός περιττός αριθμός.
2. Επιλέγουμε τυχαία $b \in [2, \ldots, n-1]$. Αν $b^{n-1} \mod n \neq 1$, τότε το n δεν περνάει τον έλεγχο (είναι σίγουρα σύνθετος).
3. Αλλιώς, γράφουμε $n - 1 = 2^s t$, με t περιττό.

Έλεγχος πρώτων αριθμών Miller-Rabin

1. Έστω $n \in \mathbb{Z}$ θετικός περιττός αριθμός.
2. Επιλέγουμε τυχαία $b \in [2, \ldots, n-1]$. Αν $b^{n-1} \mod n \neq 1$, τότε το n δεν περνάει τον έλεγχο (είναι σίγουρα σύνθετος).
3. Αλλιώς, γράφουμε $n - 1 = 2^s t$, με t περιττό.
4. Αν $b^t \mod n \equiv \pm 1 \pmod n$, τότε το n περνάει τον έλεγχο (πιθανόν πρώτος).

Έλεγχος πρώτων αριθμών Miller-Rabin

1. Έστω $n \in \mathbb{Z}$ θετικός περιττός αριθμός.
2. Επιλέγουμε τυχαία $b \in [2, \ldots, n-1]$. Αν $b^{n-1} \mod n \neq 1$, τότε το n δεν περνάει τον έλεγχο (είναι σίγουρα σύνθετος).
3. Αλλιώς, γράφουμε $n - 1 = 2^s t$, με t περιττό.
4. Αν $b^t \mod n \equiv \pm 1 \pmod n$, τότε το n περνάει τον έλεγχο (πιθανόν πρώτος).
5. Αλλιώς, υψώνουμε το $b^t \mod n$ στο τετράγωνο: $b^{2t} \mod n$, έπειτα ξανά στο τετράγωνο mod$n$ κ.ο.κ. έως ότου πάρουμε ± 1 (το πολύ $s-1$ επαναλήψεις).

Έλεγχος πρώτων αριθμών Miller-Rabin

1. Έστω $n \in \mathbb{Z}$ θετικός περιττός αριθμός.
2. Επιλέγουμε τυχαία $b \in [2, \ldots, n-1]$. Αν $b^{n-1} \mod n \neq 1$, τότε το n δεν περνάει τον έλεγχο (είναι σίγουρα σύνθετος).
3. Αλλιώς, γράφουμε $n - 1 = 2^s t$, με t περιττό.
4. Αν $b^t \mod n \equiv \pm 1 \pmod n$, τότε το n περνάει τον έλεγχο (πιθανόν πρώτος).
5. Αλλιώς, υψώνουμε το $b^t \mod n$ στο τετράγωνο: $b^{2t} \mod n$, έπειτα ξανά στο τετράγωνο mod$n$ κ.ο.κ. έως ότου πάρουμε ± 1 (το πολύ $s-1$ επαναλήψεις).
6. Αν πάρουμε πρώτα -1 τότε το n περνάει τον έλεγχο (πιθανόν πρώτος), αλλιώς δεν περνάει τον έλεγχο (σίγουρα σύνθετος).

Έλεγχος πρώτων αριθμών Miller-Rabin

1. Έστω $n \in \mathbb{Z}$ θετικός περιττός αριθμός.
2. Επιλέγουμε τυχαία $b \in [2, \ldots, n-1]$. Αν $b^{n-1} \mod n \neq 1$, τότε το n δεν περνάει τον έλεγχο (είναι σίγουρα σύνθετος).
3. Αλλιώς, γράφουμε $n - 1 = 2^s t$, με t περιττό.
4. Αν $b^t \mod n \equiv \pm 1 \pmod n$, τότε το n περνάει τον έλεγχο (πιθανόν πρώτος).
5. Αλλιώς, υψώνουμε το $b^t \mod n$ στο τετράγωνο: $b^{2t} \mod n$, έπειτα ξανά στο τετράγωνο mod$n$ κ.ο.κ. έως ότου πάρουμε ± 1 (το πολύ $s-1$ επαναλήψεις).
6. Αν πάρουμε πρώτα -1 τότε το n περνάει τον έλεγχο (πιθανόν πρώτος), αλλιώς δεν περνάει τον έλεγχο (σίγουρα σύνθετος).

Ορθότητα: Θα αποδείξουμε ότι η πιθανότητα αποτυχίας είναι $< \frac{1}{2}$.

Έλεγχος πρώτων αριθμών Miller-Rabin

1. Έστω $n \in \mathbb{Z}$ θετικός περιττός αριθμός.
2. Επιλέγουμε τυχαία $b \in [2, \ldots, n-1]$. Αν $b^{n-1} \mod n \neq 1$, τότε το n δεν περνάει τον έλεγχο (είναι σίγουρα σύνθετος).
3. Αλλιώς, γράφουμε $n - 1 = 2^s t$, με t περιττό.
4. Αν $b^t \mod n \equiv \pm 1 \pmod n$, τότε το n περνάει τον έλεγχο (πιθανόν πρώτος).
5. Αλλιώς, υψώνουμε το $b^t \mod n$ στο τετράγωνο: $b^{2t} \mod n$, έπειτα ξανά στο τετράγωνο mod$n$ κ.ο.κ. έως ότου πάρουμε ± 1 (το πολύ $s-1$ επαναλήψεις).
6. Αν πάρουμε πρώτα -1 τότε το n περνάει τον έλεγχο (πιθανόν πρώτος), αλλιώς δεν περνάει τον έλεγχο (σίγουρα σύνθετος).

Ορθότητα: Θα αποδείξουμε ότι η πιθανότητα αποτυχίας είναι $< \frac{1}{2}$.

Μπορεί να γίνει *αμελητέα (negligible)* με επαναλήψεις του ελέγχου για άλλο b κάθε φορά.

Έλεγχος πρώτων αριθμών Miller-Rabin: ορθότητα

Λήμμα

Έστω G μία πεπερασμένη ομάδα και $H \subseteq G$. Αν η H περιέχει το ουδέτερο στοιχείο του G και για κάθε $a, b \in H$ ισχύει $ab \in H$, τότε η H είναι υποομάδα της G.

Λήμμα

Έστω H μία γνήσια υποομάδα μιας πεπερασμένης ομάδας G. Τότε $|H| \leq |G|/2$.

Έλεγχος πρώτων αριθμών Miller-Rabin: ορθότητα

Πρόταση

Αν n πρώτος, τότε περνάει τον έλεγχο πάντοτε (για όλα τα b). Αν n σύνθετος τότε περνάει τον έλεγχο για λιγότερα από τα μισά b.

Έλεγχος πρώτων αριθμών Miller-Rabin: ορθότητα

Πρόταση

Αν n πρώτος, τότε περνάει τον έλεγχο πάντοτε (για όλα τα b). Αν n σύνθετος τότε περνάει τον έλεγχο για λιγότερα από τα μισά b.

Απόδειξη.

Βασίζεται στην απεικόνιση $b \mapsto \langle b^t, b^{2t}, \ldots, b^{2^i t}, \ldots b^{2^s t} \rangle \pmod{n}$.

Έλεγχος πρώτων αριθμών Miller-Rabin: ορθότητα

Πρόταση

Αν n πρώτος, τότε περνάει τον έλεγχο πάντοτε (για όλα τα b). Αν n σύνθετος τότε περνάει τον έλεγχο για λιγότερα από τα μισά b.

Απόδειξη.

Βασίζεται στην απεικόνιση $b \mapsto \langle b^t, b^{2t}, \ldots, b^{2^i t}, \ldots b^{2^s t} \rangle \pmod{n}$.

Factoring sequence: $\langle \not\equiv \pm 1, \ldots, \not\equiv \pm 1, \equiv 1, \ldots \equiv 1 \rangle \pmod{n}$.

Έλεγχος πρώτων αριθμών Miller-Rabin: ορθότητα

Πρόταση

Αν n πρώτος, τότε περνάει τον έλεγχο πάντοτε (για όλα τα b). Αν n σύνθετος τότε περνάει τον έλεγχο για λιγότερα από τα μισά b.

Απόδειξη.

Βασίζεται στην απεικόνιση $b \mapsto \langle b^t, b^{2t}, \ldots, b^{2^i t}, \ldots b^{2^s t} \rangle \pmod{n}$.

Factoring sequence: $\langle \not\equiv \pm 1, \ldots, \not\equiv \pm 1, \equiv 1, \ldots \equiv 1 \rangle \pmod{n}$.

Αποδεικνύεται με χρήση του Θ. Lagrange ότι τα στοιχεία που απεικονίζονται σε non-factoring sequences είναι το πολύ τα μισά.

Λεπτομέρειες: στον πίνακα. □

Ντετερμινιστικός έλεγχος πρώτων

Αλγόριθμος AKS (2002) είναι ντετερμινιστικός, αλλά αργός (O($n^{5+\epsilon}$)) για αυτό πρακτικά χρησιμοποιούνται οι πιθανοτικοί αλγόριθμοι

Παραγοντοποίηση Pollard rho

Έστω p ο μικρότερος πρώτος διαιρέτης του n. Ψάχνουμε $x \neq x' \in \mathbb{Z}_n$, τ.ώ. $x \equiv x' (\mod p)$

Τότε $p \leq gcd(x - x', n) < n$, άρα από ΜΚΔ μπορούμε να βρούμε μη τετριμμένο διαιρέτη του n (p άγνωστο!).

Επιλέγουμε τυχαίο $X \subseteq \mathbb{Z}_n$ και υπολογίζουμε για όλα τα x, x' το $gcd(x - x', n)$

Από παράδοξο γενεθλίων, πρέπει $|X| \approx 1.17\sqrt{n}$ για να έχουμε σύγκρουση με πιθανότητα 50%.

Για να το κάνουμε αυτό θέλουμε όλα τα $gcd(x - x', n)$ (αφού p άγνωστο, άρα όχι υπολογισμός των $x \mod p$ και μετά ταξινόμηση), άρα περισσότερα από $\binom{|X|}{2} > p/2$

Χρειάζεται κάτι πιο έξυπνο

Παραγοντοποίηση Pollard rho

f : πολυώνυμο, π.χ. $f(x) = x^2 + a$ (συνήθως $a = 1$)

Έστω $x_1 \in \mathbb{Z}_n$ και $x_1, x_2, ...,$ όπου $x_j = f(x_{j-1}), j \geq 2$

Έστω $m \in \mathbb{Z}$ και $X = \{x_1, ..., x_m\}$

Για να έχω $gcd(x_j - x_i, n)$, πρέπει για κάθε νέο x_j, να πάρω όλα τα $i < j$ και να τα δοκιμάσω

Παραγοντοποίηση Pollard rho

Καλύτερο: Αν $x_i mod\, p = x_j mod\, p$, τότε $x_{i+1} mod\, p = x_{j+1} mod\, p$ (λόγω της f)

και επαναλαμβάνοντας έχουμε ότι

Αν $x_i \equiv x_j (mod\, p)$, τότε $x_{i+\delta} \equiv x_{j+\delta} (mod\, p)$, όλα τα $\delta \geq 0$

$x_1 mod\, p \rightarrow x_2 \mod p \cdots \rightarrow x_i \mod p$ (tail)

και κύκλος

$x_i mod\, p \rightarrow x_{i+1} mod\, p \cdots \rightarrow x_j \equiv x_i mod\, p$

Παραγοντοποίηση Pollard rho

Βελτίωση: δε χρειάζεται να βρούμε την πρώτη σύγκρουση, αλλά παίρνουμε $j = 2i$ (θα μπούμε πιο γρήγορα στον κύκλο)

Αν $x_i \equiv x_j (mod\, p)$, τότε $x'_i \equiv x_{2i'} (mod\, p)$, για όλα τα $i' \equiv 0 (mod\, p), i' \geq i$

Αριθμός επαναλήψεων το πολύ $\sqrt{p}$, και $p < \sqrt{n}$ η αναμενόμενη πολυπλοκότητα $O(n^{1/4})$ (όχι μαθηματική απόδειξη!)

Αποτυχία αλγορίθμου: $x_i \equiv x_j (mod\, p)$ και $x_i \equiv x_j (mod\, n)$, με μικρή πιθανότητα (p/n)

Αν αποτύχει, επανάληψη με άλλο x_1 ή άλλη συνάρτηση

Παραγοντοποίηση Pollard rho

Αλγόριθμος POLLARD RHO FACTORING (n, x_1)

external f

$x \leftarrow x_1$

$x' \leftarrow f(x) \mod n$

$p \leftarrow gcd(x - x', n)$

while $p = 1$

σχόλιο: στην i-στη επανάληψη, $x = x_i$ and $x' = x_{2i}$

$x \leftarrow f(x) \mod n$

$x' \leftarrow f(x') \mod n$

$x' \leftarrow f(x') \mod n$

$p \leftarrow gcd(x - x', n)$

if $p = n$ return ("failure") **else** return (p)

Παραγοντοποίηση Dixons

Έστω ότι μπορούμε να βρούμε $x \not\equiv \pm y (mod\ n)$, τ.ώ. $x^2 \equiv y^2 (mod\ n)$

Τότε

$$n | (x+y)(x-y)$$

αλλά κανένα από τα $x+y, x-y$ δε διαιρούνται από το n, άρα $gcd(x+y, n)$ μη τετριμμένος διαιρέτης του n

$\mathcal{B}$ *βάση παραγοντοποίησης*, έχει τους b μικρότερους πρώτους (b παράμετρος)

Βρίσκουμε ακεραίους z, τ.ω. όλοι οι πρώτοι παράγοντες του $z^2 \mod n$ είναι από το $\mathcal{B}$

Ιδέα: πάρε υποσύνολό τους ώστε κάθε πρώτος παράγοντας του $\mathcal{B}$ να χρησιμοποιείται άρτιο αριθμό φορών, ώστε να έχω $x^2 \equiv y^2 (mod\ n)$ (υποψήφιο)

Παραγοντοποίηση Dixons

Παράδειγμα

Έστω $n = 15770708441, b = 6$, τότε $\mathcal{B} = \{2, 3, 5, 7, 11, 13\}$

Έστω

$8340934156^2 = 3 \times 7 (\mod n)$
$12044942944^2 = 2 \times 7 \times 13 (\mod n)$
$2773700011^2 = 2 \times 3 \times 13 (\mod n)$

Το γινόμενό τους δίνει:

$$(8340934156 \times 12044942944 \times 2773700011)^2 = (2 \times 3 \times 7 \times 13)^2 (\mod n)$$

Ισοδύναμα: $9503435785^2 = 546^2 (\mod n)$ και από αλγόριθμο ΜΚΔ
$gcd(9503435785 - 546, 15770708441) = 115759$

Παραγοντοποίηση Dixons

Έστω $\mathcal{B} = \{p_1, p_2, \cdots, p_b\}$ η βάση παραγοντοποίησης και $c > b$ στοιχεία

$z_j^2 \equiv p_1^{a_{1j}} \times \cdots \times p_b^{a_{bj}} (mod n), i \leq j \leq c$

για κάθε ένα από αυτά παίρνουμε το $a_j = (a_{1j} mod\ 2) \cdots a_{bj} mod\ 2))$, δηλ. ένα διάνυσμα από 0,1

Αν μπορούμε να βρούμε ένα υποσύνολο διανυσμάτων, ώστε το άθροισμα mod 2 είναι 0, τότε στο γινόμενο των αντίστοιχων z_j θα χρησιμοποιήσουμε κάθε πρώτο του $\mathcal{B}$ έναν άρτιο αριθμό φορών

Εύρεση υποσυνόλου γραμμών ενός πίνακα, ώστε το άθροισμα να είναι 0, μπορεί να γίνει εύκολα (γραμμική άλγεβρα)

Παραγοντοποίηση Dixons

Πώς βρίσκουμε τα z_j:

1. Τυχαίους αριθμούς (Random Squares algorithm)
2. $j + \lceil \sqrt{kn} \rceil, j = 0, 1, 2, ..., k = 1, 2, ...$ (μικροί όταν υψωθούν στο τετράγωνο και ελαττωθούν $\mod n$)
3. $\lfloor \sqrt{kn} \rfloor$ ((όταν υψωθούν στο τετράγωνο και ελαττωθούν $\mod n$, λίγο μικρότεροι από n). Αυτό σημαίνει ότι $-z^2 mod n$ είναι μικρό και είναι πιθανό να παραγοντοποιηθεί. Άρα πρέπει να περιλάβουμε και το -1 στο $\mathcal{B}$

Παραγοντοποίηση Dixons

Πόσο μεγάλο πρέπει να είναι το $\mathcal{B}$; Πολύ μεγάλο, καλύτερη πιθανότητα να βρούμε παράγοντα, αλλά και περισσότερο χρόνο να βρούμε υποσύνολο με άθροισμα 0

αναμενόμενη χρονική πολυπλοκότητα $O(e^{(1+o(1))\sqrt{lnnlnlnn}})$ ή αν $O(m)$ η αναπαράσταση του n, $2^{(\sqrt{mlogm})}$ (υποεκθετικός)

Παραγοντοποίηση Quadratic sieve και Number field sieve

Πρακτικά χρησιμοποιούνται οι:

1. Quadratic sieve: μια ειδική διαδικασία "κόσκινου" για την επιλογή των z_j
2. Number field sieve ο πιο γρήγορος $O(e^{(1.92+o(1))(lnn)^{1/3}(lnlnn)^{2/3}})$