Παραγωγή μεγάλων πρώτων αριθμών

Πώς υπολογίζουμε μεγάλους πρώτους αριθμούς?

- Μεγάλοι πρώτοι αριθμοί χρειάζονται στην πλειοψηφία των αλγορίθμων Δημοσίου κλειδιού
- Για να εξετάσει κανείς αν ένας αριθμός n είναι πρώτος, θα πρέπει να εξετάσει για όλους τους αριθμούς 2,3,4,…$\lfloor\sqrt{n}\rfloor$ αν διαιρούν τον n (με δεδομένο ότι ο n είναι περιττός, στην ουσία κοιτάμε μόνο τους περιττούς αριθμούς).
- Κάτι πιο αποδοτικό?

Γενική προσέγγιση

1. *Δημιουργία τυχαίου περιττού αριθμού n*
   - Τυχαία επιλογή
   - Κατασκευή με κάποιον τρόπο (υπάρχουν γνωστές κατασκευές – δεν θα μελετηθούν εδώ)
2. Εξετάζουμε αν ο*n* είναι πρώτος
   - Με ελέγχους βάση πιθανότητας (Probabilistic tests)
   - Γνήσιοι έλεγχοι (True primality tests)
3. Αν στο βήμα 2 αποφαινόμαστε ότι ο *n* είναι σύνθετος, επιστρέφουμε στο βήμα 1.

Πρώτοι αριθμοί

- Κατανομή
  - Έστω $\pi(x)$ το πλήθος των πρώτων αριθμών στο διάστημα [2,x]. Τότε,
  - $\pi(x) \sim \frac{x}{\ln x}$
  - Άρα: δεν είναι δύσκολο να βρούμε πρώτους αριθμούς (έχουν μία αρκετά ομοιόμορφη κατανομή):

Probabilistic primality tests

- Σύνολο «πειστηρίων» (witnesses) W(n), ορίζεται ως εξής:
  - Για κάποιο $a \in Z_n$, εάν ο $a \in W(n)$, τότε ο a καλείται ‘witness’ (πειστήριο ή μάρτυρας) για το ότι ο n είναι σύνθετος. Ο έλεγχος για το αν ο a είναι πειστήριο, μπορεί να γίνει σε πολυωνυμικό χρόνο.
  - Εάν ο n είναι πρώτος, τότε $W(n)=\phi$ *(κενό σύνολο)*
  - Εάν ο n είναι σύνθετος, τότε $\#W(n) \geq \frac{n}{2}$

Probabilistic primality tests

- Fermat's test
  - Γνωρίζουμε ότι αν ο *n* είναι πρώτος και $1 \le a \le n - 1$, τότε $a^{n-1} \equiv 1 \pmod{n}$
  - Τότε αν ο *n* είναι σύνθετος, υπάρχει a τέτοιο ώστε $a^{n-1} \not\equiv 1 \pmod{n}$ – τότε ο *a* είναι ένα πειστήριο για τον *n*. Εάν $a^{n-1} \equiv 1 \pmod{n}$, τότε ο *a* ονομάζεται *liar* (όχι πειστήριο) για τον *n*
  - ```
    For i = 1 to t
          choose random a, 2 ≤ a ≤ n-2
          r = a^(n-1) mod n
          if r ≠ 1, return composite
    return prime
    ```
  - Το t είναι παράμετρος, που πρέπει να είναι αρκετά μεγάλη ώστε να μειώνει τις πιθανότητες εσφαλμένης απόφασης
    ```

Probabilistic primality tests

- Fermat's test
  - Γιατί είναι Probabilistic test?
  - Αν αποφανθούμε ότι ο n δεν είναι πρώτος, τότε αυτό ισχύει εγγυημένα. Όμως, είναι πιθανό ο n να μην είναι πρώτος και μέσω του Fermat's test να αποφανθούμε ότι είναι (υπάρχει πιθανότητα λανθασμένης απόφασης)
  - Τέτοια τεστ ονομάζονται «yes-biased Monte Carlo»

Probabilistic primality tests

- Είναι καλό το Fermat's test?
- Οι αριθμοί Carmichael numbers είναι σύνθετοι ακέραιοι με την ιδιότητα $a^{n-1} \equiv 1 \pmod{n}$ για όλους τους ακέραιους a τέτοιους ώστε $\gcd(a,n) = 1$
- Παρόλο που οι αριθμοί Carmichael είναι λίγοι, αποδεικνύουν πως το Fermat's test δεν είναι μία ασφαλής επιλογή.
- Ο μικρότερος αριθμός Carmichael είναι ο $561 = 3 \times 11 \times 17$.

Probabilistic primality tests

- Miller-Rabin
  - Για *n* πρώτο αριθμό, έστω *n*-1 = $2^s r$ *(όπου ο r είναι περιττός αριθμός)*. Έστω *a* οποιοσδήποτε ακέραιος τέτοιος ώστε gcd(*a*,*n*)=1. Τότε είτε $a^r \equiv 1 \pmod{n}$ είτε $a^{2^j r} \equiv n-1 \bmod n$ για κάποιο j, $0 \leq j \leq s-1$.

Η παραπάνω παρατήρηση μας οδηγεί στον ακόλουθο ορισμό:

Probabilistic primality tests

- Έστω n σύνθετος περιττός αριθμός με n-1=2^rs, όπου ο s είναι περιττός. Έστω a ακέραιος στο διάστημα [1,n-1].
- Αν $a^r \neq 1 \pmod{n}$ και $a^{2^j r} \neq n-1 \bmod n$ για όλα τα j στο διάστημα [0,s-1], τότε ο a είναι ισχυρό πειστήριο (strong witness) για το ότι ο n είναι σύνθετος.
- Διαφορετικά, εάν ισχύει είτε $a^r \equiv 1 \pmod{n}$ είτε $a^{2^j r} \equiv n-1 \bmod n$ για κάποιο j στο διάστημα [0,s-1], τότε ο n λέγεται «ισχυρός ψευδο-πρώτος» ως προς το a. Ο α λέγεται «ισχυρό μη πειστήριο» (strong liar) για το ότι ο n είναι σύνθετος.

Πώς κατασκεύαζεται το Miller-Rabin test?

- Εάν ο n είναι σύνθετος, τότε το πολύ το ¼ των αριθμών από το διάστημα [0..n-1] είναι ισχυρά μη-πειστήρια. Για την ακρίβεια, μη-πειστήρια είναι το πολύ φ(n)/4 στοιχεία (εάν n≠9).

Παράδειγμα

- Έστω ο σύνθετος αριθμός n=91 (7 x 13). Έχουμε 91-1=90=2 x 45, δηλαδή s=1, r=45.
- Ισχύει $9^r = 9^{45} \equiv 1 \bmod 91$, οπότε ο 91 είναι ισχυρός ψευδοπρώτος ως προς τον 9. Όλα τα ισχυρά μη-πειστήρια για τον 91 (πλην του 9 που ήδη είδαμε) είναι:
- {1, 9, 10, 12, 16, 17, 22, 29, 38, 53, 62, 69, 74, 75, 79, 81, 82, 90). Το πλήθος τους είναι 18=φ(91)/4.

Probabilistic primality tests

- Miller-Rabin test
  - Find s,r st. $n-1 = 2^s r$
    For i = 1 to t
        choose random a, $2 \le a \le n-2$
        $y = a^r \bmod n$
        if $y \neq 1$ and $y \neq n-1$
            j=1
            while $j \le s-1$ and $y \neq n-1$
                $y = y^2 \bmod n$
                if y=1 return composite
                j=j++
            if $y \neq n-1$ return composite

    return prime

Ανάλυση του Miller-Rabin

- Εάν ο αλγόριθμος αποφαίνεται ότι ο n είναι σύνθετος, τότε πράγματι είναι
- Εάν ο n είναι πρώτος, ο αλγόριθμος αποφαίνεται πως ο n είναι πρώτος
- Υπάρχει περίπτωση ο n να είναι σύνθετος, αλλά το τεστ να αποφανθεί λάθος ότι είναι πρώτος. Η πιθανότητα αυτή είναι μικρότερη από $(1/4)^t$
- Για t=10, η πιθανότητα να μην κάνει λάθος ο Miller-Rabin είναι μεγαλύτερη από 0.999999

Probabilistic primality tests

- Το Miller-Rabin τεστ είναι το καλύτερο όλων (ακόμα και από το, επίσης γνωστό και διαδεδομένο, Solovay-Strassen test).
- Πάντα όμως υπάρχει μια, έστω και πάρα πολύ μικρή, πιθανότητα λάθους

True Primality Tests

- Για $s>1$, κάθε αριθμός της μορφής $n=2^s-1$ ονομάζεται αριθμός *Mersenne (εάν επιπλέον είναι πρώτος, ονομάζεται Mersenne πρώτος).*
- Για $s>2$ ένας αριθμός Mersenne είναι πρώτος αν και μόνο αν ισχύουν:
  - Ο s είναι πρώτος
  - $u_{s-2}=0$ where $u_0=4$, $u_{k+1}=(u_k^2-2) \bmod n$ for $k\geq 0$

- `Lucal-Lehmer primality test for Mersenne numbers`
  `Εξαντλητικός έλεγχος για το αν ο s είναι πρώτος`
- `Αν όχι, return composite`
- ```
  u = 4
  for k = 1 to s-2
     u=(u^2-2) mod n
  if u=0 return prime
  return composite
  ```
  ```

True Primality Tests

- Χρονοβόρα – συνήθως, πριν εφαρμοστούν σε έναν αριθμό, πρώτα αυτός εξετάζεται με κάποιο probabilistic primality test.
- Άλλα true primality tests
  - Factorization of n-1
  - Elliptic curves
  - Jacobi sum test

Για πολύ περισσότερα…

- Κεφάλαιο 4 του Handbook of Applied Cryptography