ΚΡΥΠΤΟΓΡΑΦΙΑ ΚΑΙ ΠΟΛΥΠΛΟΚΟΤΗΤΑ

PRIMES $\in$ **P**

Από τα αριστερά προς τα δεξία **Saxena**, **Kayal** και **Agrawal**

Επιμέλεια : **Γεωργίου Κωνσταντίνος**

Ιούνιος 2003

Η ασχολία της ανθρωπότητας με τους πρώτους αριθμούς

- Παράδοση (300 π.Χ. – 2003)
- Οι άνθρωποι συλλέγουν σπάνια και όμορφα αντικείμενα
- Κανείς δεν εμίσησε τη δόξα
- Ελεγχος hardware.

  Το bug του Pentium βρέθηκε σε εφαρμογή περί δίδυμων πρώτων. Οι Pentium II και Pentium Pro ελέγχονται με εφαρμογές για πρώτους

Ιστορική αναδρομή για την πιστοποίηση πρώτων

- Το κόσκινο του Ερατοσθένη (240 π.Χ.)

- Το μικρό θεώρημα του Fermat ($17^{ος}$ αιώνας) :
  Για κάθε p πρώτο και κάθε a με $(a, p) = 1$ ισχύει ότι
  $$a^{p-1} \equiv 1 \bmod p$$

- Miller και Rabin (1976) : Πολυωνυμικός αλγόριθμος πιστοποίησης πρώτων βασισμένος στη γενικευμένη υπόθεση του Riemann.

- Miller, Solovay και Strassen (1977) : Primes in ***co-RP***

- Adleman, Pomerance και Rumely (1983) :

  Πιστοποίηση σε χρόνο $k(\log n)^{c \log\log\log n}$

  Cohen και Lenstra : θεωρητική και αλγοριθμική απλοποίηση

- Goldwasser και Killian (1986) : Αναμενόμενος πολυωνυμικός χρόνος βασισμένος σε ελλειπτικές καμπύλες. Atkin : διαφοροποιεί τον αλγόριθμο στον ECPP[1]

- Adleman και Huang (1992) : Τροποποιούν τον αλγόριθμο των Goldwasser και Killian σε μια randomized μέθοδο θέτοντας το Primes στην κλάση ***RP*** άρα και στη ***ZPP***.

- Manindra, Kayal and Nitin (2002) : Primes in ***P***

[1] Elliptic Curve Primality Proving algorithm

Η αντιμετώπιση από τον Τύπο και η αλήθεια

- *New York Times* : Τρεις Ινδοί έφεραν επανάσταση. Πλέον ο υπολογιστής μπορεί γρήγορα και οριστικά να αποφασίζει αν ένας αριθμός είναι πρώτος
  Sunday N.Y.T. : Ο νέος αλγόριθμος μπορεί να παράγει τόσο μαζικά μεγάλους πρώτους που μπορεί να εγγυηθεί απόλυτη ασφάλεια στο διαδίκτυο

- *Wall Street Journal* : Ένα υπέροχο μυαλό από την Ινδία θέτει το διαδίκτυο σε συναγερμό

- *Neue Züricher Zeitung* : Για πρώτη φορά μπορούμε να πιστοποιήσουμε πρώτους σε λογικό χρόνο

- Διαδίκτυο :
  - Επιτέλους, οι πρώτοι αριθμοί μπορούν να υπολογιστούν επακριβώς
  - Επιτέλους κανείς μπορεί να υπολογίζει πρώτους χωρίς κλάματα

- Ο μεγαλύτερος γνωστός αριθμός έχει περίπου 4.000.000 ψηφία

- Με προσεκτική υλοποίηση ο αλγόριθμος μπορεί να πιστοποιήσει 30-ψήφιους πρώτους σε 1 ημέρα

- Τα κλειδιά στην κρυπτογραφία είναι της τάξης των εκατοντάδων ψηφίων

Η καινοτομία του νέου αλγορίθμου

- Αιτιοκρατικός
- Μη πιθανοτικός
- Λογαριθμικός στην είσοδο και άρα πολυωνυμικός στο μήκος της εισόδου
- Ο αλγόριθμος είναι “embarrallel” ως προς το χρόνο αλλά όχι και το χώρο
- Δε βασίζεται σε εικασίες. Σοβαρές εικασίες και παραλλαγές που κατεβάζουν την πολυπλότητα πολύ χαμηλά

Αναφορά στην κρυπτογραφία

- Γνωστοί από παλιά γρήγοροι και αποδοτικοί αλγόριθμοι
- Ήδη γνωστές μέθοδοι για παραγωγή μεγάλων κλειδιών
- Η πιστοποίηση των πρώτων δε σχετίζεται με την παραγοντοποίηση
- Συμβολή μόνο σε θεωρητικό υπόβαθρο

Βασικοί ορισμοί και προτάσεις

- Έστω $a \in Z, r \in N$ με $(a,r)=1$. Ορίζουμε ως τάξη του $a \bmod r$, το μικρότερο φυσικό k για τον οποίο $a^k \equiv 1 \bmod r$, και θα συμβολίζεται με $o_r(a)$.

- Με $\phi(r)$ θα συμβολίζεται η συνάρτηση Euler, το πλήθος δηλαδή των φυσικών μικρότερων του r που είναι σχετικά πρώτοι μαζί του.

- Με F_p, με p πρώτος θα συμβολίζω το σώμα Galois, το πεπερασμένο δηλαδή σώμα με p στοιχεία.

- Στο δακτύλιο των πολυωνύμων $F_p[x]/h(x)$, η ισότητα $f(x)=g(x)$ θα συμβολίζεται με $f(x)\equiv g(x)\bmod(h(x),p)$.

- Για τυχαία συνάρτηση $t(n)$, με $O\sim(t(n))$ θα συμβολίζεται η κλάση $O(t(n)\,poly\log t(n))$[2]

- Έστω $a\in Z, r\in N$ με $(a,r)=1$. Τότε $o_r(a)/\phi(r)$.

[2] Για παράδειγμα, $O\sim\left(\log^k n\right)=O(\log^k(n)\,poly\log\log^k n)=O(\log^k(n)\,poly\log\log n)$, και αφού $\forall\varepsilon>0,\log^{\varepsilon} n\geq poly\log\log n$, $O\sim\left(\log^k n\right)=O\left(\log^{k+\varepsilon} n\right)$

Βασικό λήμμα

Λήμμα : Έστω a, p σχετικά πρώτοι μεταξύ τους. Τότε τα επόμενα είναι ισοδύναμα :

Ο p είναι πρώτος ***ανν*** $(x-a)^p \equiv (x^p - a) \bmod p$

- Γενίκευση του μικρού θεωρήματος του Fermat
- Επαναχρησιμοποίηση μετά την προσπάθεια των Agrawal και Biswas (1999) που απέδοσε ένα randomized αλγόριθμο.

Απόδειξη : $\Rightarrow$

Διώνυμο του Νεύτωνα

$$(x-a)^p = \sum_{i=0}^{p} (-a)^{p-i} \binom{p}{i} x^i$$

Θεωρούμε το πολυώνυμο $(x-a)^p - (x^p - a)$

- ✓ Συντελεστής μεγιστοβάθμιου όρου x^p : 0
- ✓ Σταθερός όρος : $a^p - a = a(a^{p-1} - 1)$, μηδενικό στο δακτύλιο Z_p από το θεώρημα Euler
- ✓ Υπόλοιποι συντελεστές : $(-a)^{p-i} \binom{p}{i}$, με $p / \binom{p}{i}$, αφού $0 < i < p$.

$\Leftarrow$ Έστω οτι $(x-a)^p \equiv (x^p - a) \bmod p$.

Ας υποθέσουμε (προς άτοπο) οτι ο p δεν είναι πρώτος.
Έστω $p = q_1^{k_1} q_2^{k_2} \cdots q_l^{k_l}$ η ανάλυση σε πρώτους παράγοντες.

Θεωρούμε πάλι το πολυώνυμο $(x-a)^p - (x^p - a)$
Συντελεστής του x^{q_1} : $(-a)^{p-q_1}\binom{p}{q_1}$

- Ο p δε διαιρεί το a , $((a,p)=1)$
- Ο p δε διαιρεί το$\binom{p}{q_1}$ διότι :

$$\binom{p}{q_1} = \frac{p!}{q_1!(p-q_1)!} = \frac{p!(p-q_1+1)\cdots(p-1)p}{q_1!\,p!} = \frac{(p-q_1+1)\cdots(p-1)p}{q_1!} =$$

$$\frac{(p-q_1+1)\cdots(p-1)q_1^{k_1-1}q_2^{k_2}\cdots q_l^{k_l}}{(q_1-1)!}$$

και ο p δε διαιρεί κανένα παράγοντα του γινομένου

$$(p-q_1+1)\cdots(p-1)$$

Ώστε

$$(-a)^{p-q_1}\binom{p}{q_1}\bmod p \neq 0$$

και έτσι καταλήγουμε σε αντίφαση.

□

Σχόλια για το βασικό λήμμα και η ιδέα

- Ο έλεγχος $(x-a)^p \equiv (x^p - a) \bmod p$ μπορεί να χρειαστεί εκθετικά πολλούς ελέγχους διαιρετότητας

- Μείωση των ελέγχων μέσω της μείωσης του βαθμού του πολυωνύμου

- Εύρεση κατάλληλου r με στόχο τον υπολογισμό των δύο πολυωνύμων $\bmod(x^r - 1)$

- Μπορεί να βρεθεί ένα τέτοιο r γρήγορα ;

- Είναι ο έλεγχος

$$(x-a)^p \stackrel{?}{\equiv} (x^p - a) \bmod (x^r - 1, p)$$

αποδοτικός για την πιστοποίηση πρώτων ;

- Αν πραγματικά μειώνεται το πλήθος των ελέγχων, πόσο μειώνεται η πολυπλοκότητα ;

- Υπάρχει ισοδυναμία μεταξύ των δύο κριτηρίων ;

Παρατηρήσεις

- Ο έλεγχος $(x-a)^p \stackrel{?}{\equiv} (x^p - a) \bmod (x^r - 1, p)$ δεν είναι ισοδύναμος με τον $(x-a)^p \equiv (x^p - a) \bmod p$

- Αν p πρώτος τότε $(x-a)^p \equiv (x^p - a) \bmod p$ και άρα
$$(x-a)^p \equiv (x^p - a) \bmod (x^r - 1, p)$$

- Η σχέση $(x-a)^p \equiv (x^p - a) \bmod (x^r - 1, p)$ **δεν** ικανοποιείται μόνο για πρώτους αριθμούς

- Μπορούν να βρεθούν κατάλληλα a, r έτσι ώστε
$$(x-a)^p \equiv (x^p - a) \bmod (x^r - 1, p) \textbf{ ανν } p \text{ πρώτος}$$

Ο αλγόριθμος

input : ακέραιος $n > 1$

1. if $(n = a^b,$ για κάποια $a \in N, b > 1)$ output : COMPOSITE
2. Βρες το μικρότερο r για το οποίο
$$o_r(n) > 4\log^2 n$$
3. if $1 < (a, n) < n$ για κάποιο $a \le r$, output : COMPOSITE
4. if $n \le r$, output : PRIME
5. for $a = 1$ to $\lfloor 2\sqrt{\varphi(r)}\log n \rfloor$ do
   if $(x - a)^n \neq (x^n - a) \bmod (x^r - 1, n)$ output : COMPOSITE
6. output : PRIME

Ορθότητα του αλγορίθμου

Λήμμα : Έστω $LCM(m)$ το ελάχιστο κοινό πολλαπλάσιο των m πρώτων αριθμών. Τότε για $m \geq 7$

$$LCM(m) \geq 2^m$$

Θεώρημα : Ο παραπάνω αλγόριθμος επιστρέφει PRIME **ανν** ο ακέραιος n είναι πρώτος.

Λήμμα : Αν ο n είναι πρώτος, τότε ο αλγόριθμος επιστρέφει PRIME .

Απόδειξη :

Αν ο n είναι πρώτος τότε :

- ✓ Βήμα 1^{o} : δεν υπάρχουν $a \in N, b > 1$, με $n = a^{b}$.
- ✓ Βήμα 3^{o} : για κάθε $a \le r$, $(a, n) = 1$
- ✓ Βήμα 5^{o} : από το πόρισμα του βασικού λήμματος έχουμε

$$(x-a)^{p} \equiv (x^{p}-a) \bmod (x^{r}-1, p)$$

Επομένως ο αλγόριθμος έστω και στο 7^{o} βήμα επιστρέφει PRIME

□

Πορεία προς την αντίθετη κατεύθυνση του θεωρήματος

- Ο αλγόριθμος επιστρέφει PRIME στα βήματα 4 και 6
- Αν στο $4^{ο}$ βήμα ο αλγόριθμος επιστρέψει PRIME τότε ο n είναι πρώτος (από το $3^{ο}$ βήμα και αφού $n \leq r$)
- Αν στο $6^{ο}$ βήμα ο αλγόριθμος επιστρέψει PRIME τότε είναι ο n πρώτος ;
- Η αντίθετη πορεία του θεωρήματος βασίζεται στα βήματα 2 και 5. Καταρχήν ο αριθμός r που αναζητείται στο $2^{ο}$ βήμα πράγματι υπάρχει.

Λήμμα : Υπάρχει r , $r \le \lceil 16\log^5 n \rceil$ έτσι ώστε $o_r(n) > 4\log^2 n$.

Απόδειξη : Ας είναι $r_1, r_2, \ldots, r_t$ <u>όλοι</u> οι αριθμοί με

$$o_{r_i}(n) \le 4\log^2 n$$

- ✓ Αν $o_{r_i}(n) = k_i$, τότε ο r_i διαιρεί το $n^{k_i} - 1$
- ✓ Αφού $k_i \le 4\log^2 n$, κάθε ένα από τα r_i διαιρεί το γινόμενο

$$\prod_{i=1}^{\lfloor 4\log^2 n \rfloor} \left(n^i - 1\right)$$

Εύκολα παρατηρούμε οτι :

$$\prod_{i=1}^{\lfloor 4\log^2 n \rfloor} \left(n^i - 1\right) = \left(n-1\right)\left(n^2 - 1\right)\ldots\left(n^{\lfloor 4\log^2 n \rfloor} - 1\right) \le n^{1+2+\ldots\lfloor 4\log^2 n \rfloor} \le n^{16\log^4 n} \le 2^{16\log^5 n}$$

- ✓ Το ελάχιστο κοινό πολλαπλάσιο των $\lceil 16\log^5 n \rceil$ πρώτων αριθμών είναι τουλάχιστον $2^{\lceil 16\log^5 n \rceil}$ (από προηγούμενο λήμμα)

- ✓ Όλοι οι r_i με $o_{r_i}(n) \le 4\log^2 n$, διαιρούν κάτι φραγμένο από $2^{16\log^5 n}$

Αρα εάν όλοι οι αριθμοί r μέχρι και τον $\lceil 16\log^5 n \rceil$ είχαν την ιδιότητα $o_{r_i}(n) \le 4\log^2 n$ θα έπρεπε να διαιρούν κάτι μικρότερο από το ελάχιστο κοινό τους πολλαπλάσιο

- ➢ Επομένως υπάρχει $r \le \lceil 16\log^5 n \rceil$ έτσι ώστε $o_{r_i}(n) \le 4\log^2 n$.

□

- Το προηγούμενο λήμμα εξασφαλίζει ένα r με μια χρήσιμη ιδιότητα

- Το ζητούμενο r μπορεί να βρεθεί γρήγορα

Στη συνέχεια θα θεωρούμε οτι ο αλγόριθμος έχει αποφανθεί στο 6^{o} βήμα PRIME και θα προσπαθούμε να δείξουμε την ορθότητα αυτής της θέσης

Λήμμα : Έστω p πρώτος παράγοντας του n και r όπως στο προηγούμενο λήμμα. Ισχύει οτι $p > r$ και $p, n \in Z_r^*$

Απόδειξη : Έστω p ένας πρώτος παράγοντας του n.

- ✓ Αν ο p ήταν μικρότερος από r, τότε θα είχε αποφανθεί ήδη ο αλγόριθμος στα βήματα 3 ή 4.

- ✓ Η συνθήκη του αλγορίθμου στο 3^{o} του βήμα δεν έχει ικανοποιηθεί και άρα οι n, r είναι σχετικά πρώτοι

- ✓ Αν ο r διαιρούσε τον p, τότε οι n, r δε θα ήταν σχετικά πρώτοι

Οπότε οι p, n δε μπορεί να είναι τα ουδέτερα στοιχεία στο Z_r.

□

Η ανάγκη για ένα νέο ορισμό

- Ας είναι στο εξής $l = \lfloor 2\sqrt{\phi(r)}\log n \rfloor$

- Στο 5ο βήμα η συνθήκη δεν ικανοποιείται ποτέ και άρα
$$(x-a)^n \equiv (x^n - a) \bmod (x^r - 1, n) \text{ για κάθε } a \text{ με } 1 \le a \le l$$

- Αν ο p είναι ένας πρώτος παράγοντας του n, τότε
$$(x-a)^n \equiv (x^n - a) \bmod (x^r - 1, p), \text{ για κάθε } a \text{ με } 1 \le a \le l$$

- Από το 3ο βήμα έχουμε οτι $(a, p) = 1$, και επομένως από το βασικό λήμμα
$$(x-a)^p \equiv (x^p - a) \bmod (x^r - 1, p), \text{ για κάθε } a \text{ με } 1 \le a \le l$$

- Αν ο p είναι ένας πρώτος παράγοντας του n τότε και οι δύο έχουν την ίδια συμπεριφορά για το βοηθητικό πολυώνυμο

Ορισμός : Ένα $m \in N$ θα λέγεται ενδοσκοπικό (introspective) για ένα πολυώνυμο $f(x)$ αν ισχύει οτι

$$f^m(x) \equiv f(x^m) \bmod(x^r - 1, p).$$

- Οι φυσικοί p, n είναι ενδοσκοπικοί για τα πολυώνυμα $x - a$, $\forall\ a$ με $1 \le a \le l$.

Σημαντικές ιδιότητες των ενδοσκοπικών αριθμών

- Η ιδιότητα των ενδοσκοπικών αριθμών είναι κλειστή για το πολλαπλασιασμό των αριθμών.

- Η ιδιότητα των ενδοσκοπικών αριθμών είναι κλειστή για το πολλαπλασιασμό των πολυωνύμων.

Λήμμα : Έστω οτι οι φυσικοί m, m' είναι ενδοσκοπικοί για ένα πολυώνυμο $f(x)$. Τότε και ο $m \cdot m'$ είναι ενδοσκοπικός για το πολυώνυμο $f(x)$.

Απόδειξη :

- ✓ Ο m είναι ενδοσκοπικός για το πολυώνυμο $f(x)$:

$$f^m(x) \equiv f(x^m) \bmod (x^r - 1, p)$$

$$\Rightarrow f^{m \cdot m'}(x) \equiv f^{m'}(x^m) \bmod (x^r - 1, p) \quad (1)$$

- ✓ Ομοίως για το m' έχουμε $f^{m'}(x) \equiv f(x^{m'}) \bmod (x^r - 1, p)$

- ✓ Θέτοντας $x \leftarrow x^m$ προκύπτει

$$f^{m'}(x^m) \equiv f(x^{m \cdot m'}) \bmod (x^{m \cdot r} - 1, p)$$

και επειδή $(x^r - 1)/(x^{m \cdot r} - 1)$ έχουμε οτι

$$f^{m'}(x^m) \equiv f(x^{m \cdot m'}) \bmod (x^r - 1, p) \quad (2)$$

✓ Από τις (1) και (2) προκύπτει

$$f^{m\cdot m'}(x) \equiv f(x^{m\cdot m'}) \bmod (x^r - 1, p)$$

□

Λήμμα : Έστω m ενδοσκοπικό για δύο πολυώνυμα $f(x), g(x)$.
Τότε το m είναι ενδοσκοπικό και για το πολυώνυμο $f(x)\cdot g(x)$.

Απόδειξη : Πολύ πιο απλά

$$\big(f(x)\cdot g(x)\big)^m \equiv f^m(x)\cdot g^m(x) \underset{m \text{ introspective } g(x)}{\overset{m \text{ introspective } f(x)}{\equiv}} f(x^m)\cdot g(x^m) \bmod (x^r - 1, p)$$

□

Ορισμός μιας σημαντικής ομάδας

- Ορίζουμε τα σύνολα

$$I = \left\{ n^i \cdot p^j \mid i, j \geq 0 \right\} \quad \text{και} \quad P = \left\{ \prod_{a=1}^{l} (x-a)^{e_a} \mid e_a \geq 0 \right\}$$

- Κάθε στοιχείο του πρώτου είναι ενδοσκοπικό για κάθε στοιχείο του δεύτερου

- Σύμφωνα με προηγούμενο λήμμα έχει νόημα να ορίσω ως μια υποομάδα της Z_r^* ,τα στοιχεία του I modulo r

- Στο εξής αυτή η ομάδα θα τη συμβολίζουμε με G.

Λήμμα : Η τάξη t της ομάδας G είναι μεγαλύτερη από $4\log^2 n$.

Απόδειξη :

- ✓ Από το 2^{o} βήμα έχουμε οτι για το r ισχύει $o_r(n) > 4\log^2 n$.

- ✓ Δεν υπάρχει δύναμη του n μικρότερη από $4\log^2 n$ που να μας δίνει το μοναδιαίο στοιχείο $\bmod r$.

- ✓ Η ομάδα G παράγεται από το γινόμενο των $n, p \bmod r$. Άρα θα έχει τουλάχιστον $4\log^2 n$ στοιχεία.

□