Μια μικρή υπενθύμιση από τη θεωρία Galois

- Οι n-οστές ρίζες της μονάδας αποτελούν μια κυκλική ομάδα τάξεως n.

- Ένα στοιχείο z θα ονομάζεται αρχική ρίζα της μονάδας αν είναι μια n-οστή ρίζα της μονάδας και παράγει την παραπάνω ομάδα

- Το τυχαίο στοιχείο z^k της ομάδας θα παράγει και αυτό την ομάδα μόνο αν το k είναι σχετικά πρώτο με την τάξη της ομάδας.

- Υπάρχουν ακριβώς $\phi(n)$ αρχικές ρίζες της μονάδας

- Αν $z_1, z_2, \cdots, z_{\phi(n)}$ είναι όλες οι διακεκριμένες αρχικές ρίζες της μονάδας, τότε το πολυώνυμο

$$Q_n(x) = (x - z_1)(x - z_2)\cdots(x - z_{\phi(n)})$$

θα ονομάζεται n-οστό κυκλοτομικό πολυώνυμο.

Ορισμός 2ης σημαντικής ομάδας

- Το πολυώνυμο $Q_r(x)$ διαιρεί το πολυώνυμο $x^r - 1$,
- Επί του σώματος F_p το πολυώνυμο $x^r - 1$ αναλύεται από το $Q_r(x)$ σε πρώτους παράγοντες τάξης $o_r(p)$
- Ας είναι $h(x)$ ένας τέτοιος παράγοντας.
- Θα συμβολίζω με G την ομάδα

$$P = \left\{ \prod_{a=1}^{l} (x-a)^{e_a} \mid e_a \geq 0 \right\} \text{ modulo } \left(h(x), p\right)$$

- Στο σώμα $F = F_p[x]/h(x)$, η ομάδα G παράγεται από τα πολυώνυμα $x+1, x+2, \ldots, x+l$ και είναι υποομάδα της πολλαπλασιαστικής ομάδας F

Λήμμα : Το πλήθος των θετικών ακέραιων ριζών της εξίσωσης $x_1 + x_2 + \ldots + x_v = k$ είναι $\binom{v+k-1}{k}$.

Φράγματα για την τάξη της ομάδας G

Λήμμα : Η τάξη της G είναι τουλάχιστον $\binom{t+l-2}{t-1}$.

Απόδειξη :

- ✓ Ας είναι $f(x), g(x)$, δύο διαφορετικά πολυώνυμα $f(x), g(x)$ του $P = \left\{ \prod_{a=1}^{l} (x-a)^{e_a} \mid e_a \geq 0 \right\}$ με βαθμό μικρότερο από την τάξη t της ομάδας G.

- ✓ Αν δεν ήταν διαφορετικά και στη G θα έπρεπε για το τυχαίο $m \in I$ να ισχύει $f^m(x) \equiv g^m(x)$

- ✓ Από τη σχέση των I, G θα είχαμε στο F, $f(x^m) \equiv g(x^m)$ και το πολυώνυμο $R(x^m) = f(x^m) - g(x^m)$ θα είχε ρίζα για κάθε $m \in I$

- ✓ Οι m, r είναι σχετικά πρώτοι και άρα το x^m μας δίνει μια r -οστή αρχική ρίζα της μονάδας.

- ✓ Στο σώμα F και από την επιλογή των f, g , το πολυώνυμο R δε μπορεί να έχει t διακριτές ρίζες (την τάξη δηλαδή του G).

- ✓ Τελικά τα πολυώνυμα f, g με βαθμό μικρότερο από την τάξη της ομάδας G, είναι διαφορετικά και στην ομάδα G

- ✓ Επειδή $p > r$ και $l = \lfloor 2\sqrt{\phi(r)} \log n \rfloor < 2\sqrt{r} \log n \leq r$, δύο διακριτά στοιχεία $i, j \leq l = \lfloor 2\sqrt{\phi(r)} \log n \rfloor$, διατηρούν τη σχέση τους στο σώμα F_p

- ✓ Τα $x+1, x+2, \ldots, x+l$ είναι διακριτά πολυώνυμα.

- ✓ Αν $h(x) = x - a$ τότε κάποιο από τα $x+1, x+2, \ldots, x+l$ είναι μηδενικό

- ✓ Τουλάχιστον τα $l-1$ από τα $x+1, x+2, \ldots, x+l$ που παραγουν την G δεν είναι τα μηδενικά πολυώνυμα στο F.

✓ Οι συνδυασμοί δυνάμεων $d_1, d_2, \ldots, d_{l-1}$ των $x+1, x+2, \ldots, x+l$ που μπορούμε να πάρουμε ώστε η δύναμη να είναι το πολύ $t-1$ είναι όσες και ακέραιες ρίζες της ανίσωσης $d_1 + d_2 + \ldots + d_{l-1} < t-1$

✓ Το πλήθος ριζών της εξίσωσης $d_1 + d_2 + \ldots + d_{l-1} + d_l = t-1$ είναι

$$\binom{l+t-1-1}{t-1} = \binom{t+l-2}{t-1}$$

□

• Εκτός από το κάτω φράγμα για την τάξη της ομάδας G, κάτω από ορσιμένες συνθήκες μπορούμε να πετύχουμε και άνω φράγμα

Λήμμα : Αν το n δεν είναι δύναμη του p τότε η G έχει λιγότερα από $\frac{n^{2\sqrt{t}}}{2}$ στοιχεία.

Απόδειξη :

- ✓ Θεωρούμε το υποσύνολο του $I = \{n^i \cdot p^j \mid i, j \geq 0\}$, $I' = \{ n^i \cdot p^j \mid 0 \leq i, j \leq \lfloor \sqrt{t} \rfloor \}$.

- ✓ Αφού το n δεν είναι δύναμη του p, συμπεραίνουμε οτι $|I'| = \left(\lfloor \sqrt{t} \rfloor + 1 \right)^2$.

- ✓ Η τάξη του G είναι t, και άρα υπάρχουν τουλάχιστον δύο στοιχεία m_1, m_2, του I' που θα είναι ισότιμα $\bmod r$

- ✓ Ας είναι $m_1 > m_2$ και τότε ισχύει οτι $x^{m_1} \equiv x^{m_2} \bmod\left(x^r - 1\right)$

- ✓ Αν $f(x) \in P = \left\{ \prod_{a=1}^{l} (x-a)^{e_a} \mid e_a \geq 0 \right\}$ και αφού το m_1 είναι ενδοσκοπικό για το $f(x)$ έχουμε οτι

$$f^{m_1}(x) = f\left(x^{m_1}\right) \bmod\left(x^r - 1, p\right) \overset{(1)}{\Rightarrow}$$
$$f^{m_1}(x) = f\left(x^{m_2}\right) \bmod\left(x^r - 1, p\right)$$

- ✓ Επίσης το m_2 είναι ενδοσκοπικό για το $f(x)$, και έτσι η τελευταία σχέση γίνεται : $f^{m_1}(x) = f^{m_2}(x) \bmod\left(x^r - 1, p\right).$

- ✓ Τα $f^{m_1}(x), f^{m_2}(x)$ είναι ισότιμα στο σώμα F και το $f(x)$ ως στοιχείο του G πρέπει να διαιρεί το πολυώνυμο $R(x) = x^{m_1} - x^{m_2}$

- ✓ Το πολυώνυμο $R(x) = x^{m_1} - x^{m_2}$ έχει τουλάχιστον $|\mathcal{G}|$ διακριτές ρίζες στο σώμα F

- ✓ Το πολυώνυμο $R(x) = x^{m_1} - x^{m_2}$ έχει βαθμό

$$m_1 \overset{m_1 \in I}{\leq} (np)^{\lfloor \sqrt{t} \rfloor} < \frac{n^{2\sqrt{t}}}{2}$$

(αφού κάθε διαιρέτης του n είναι το πολύ $n/2$)

- ✓ Η επιλογή του $f(x)$ ήταν αυθαίρετη και επομένως

$$|\mathcal{G}| < \frac{n^{2\sqrt{t}}}{2} .$$

□

Η ολοκλήρωση της απόδειξης

Λήμμα : Αν ο αλγόριθμος επιστρέψει PRIME τότε ο αριθμός n της εισόδου είναι πρώτος.

Απόδειξη :

- ✓ Υποθέτουμε οτι ο αλγόριθμος επιστρέφει PRIME στο 6^{o} βήμα και ας είναι p ένας παράγοντας του n.

- ✓ Από προηγούμενο λήμμα έχουμε οτι αν $|G| = t$ και $l = \lfloor 2\sqrt{\phi(r)}\log n \rfloor$, τότε $|G| \geq \binom{t+l-2}{t-1}$.

✓ Ισχύουν τα παρακάτω

(1) - $t > 2\sqrt{t}\log n$

(2) - $l = \lfloor 2\sqrt{\phi(r)}\log n \rfloor \geq \lfloor 2\sqrt{t}\log n \rfloor$ (G υποομάδα της Z_r^*).

(3) - $2\sqrt{t}\log n \geq 3$ (4) - για $x > 3$ ισχύει $\binom{2x-1}{x} > 2^x$

✓ $|G| \overset{1}{\geq} \binom{l-1+\lfloor 2\sqrt{t}\log n \rfloor}{\lfloor 2\sqrt{t}\log n \rfloor} \overset{2}{\geq} \binom{2\lfloor 2\sqrt{t}\log n \rfloor - 1}{\lfloor 2\sqrt{t}\log n \rfloor} \overset{3}{\geq} 2^{\lfloor 2\sqrt{t}\log n \rfloor} \geq \frac{n^{2\sqrt{t}}}{2}$.

- ✓ Από προηγούμενο λήμμα και αν ο n δεν είναι δύναμη του p ισχύει οτι $|G| < \frac{n^{2\sqrt{t}}}{2}$

- ✓ Το n είναι δύναμη του p δηλαδή υπάρχει k με $p^k = n$.

- ✓ Τότε $k = 1$ γιατί αλλιώς το $1^{\text{ο}}$ βήμα του, ο αλγόριθμου θα επέστρεφε COMPOSITE.

- ✓ Ώστε $p = n$ δηλαδή ο n είναι πρώτος.

□

Ανάλυση πολυπλοκότητας

- Πράξεις μεταξύ αριθμών με m ψηφία μπορούν να υλοποιηθούν σε χρόνο $O \sim (m)$.

- Επίσης πράξεις μεταξύ πολυωνύμων βαθμού d και συντελεστών m ψηφίων, μπορούν να υπλοποιηθούν σε χρόνο $O \sim (d \cdot m)$.

Θεώρημα : Η χρονική ασυμπτωτική πολυπλοκότητα του αλγορίθμου είναι

$$O \sim (\log^{10,5} n)$$

Απόδειξη

- ✓ Στο $1^{ο}$ βήμα ο αλγόριθμος απαιτεί $O \sim (\log^3 n)$ βήματα
- ✓ Στο $2^{ο}$ βήμα βρίσκουμε ένα r, πάνω φραγμένο από $O(\log^5 n)$.
- ✓ Για κάθε ένα από τα υποψήφια r θα πρέπει να ελέγξουμε αν $n^k \overset{?}{\equiv} 1 \bmod r$. Εξασφαλίζουμε ένα r ελέγχοντας αν $n^k \neq 1 \bmod r$ για κάθε $k \leq 4\log^2 n$, κάτι που απαιτεί $O \sim (\log^2 n \log r)$ βήματα.
- ✓ Στο $2^{ο}$ βήμα απαιτούνται $O \sim (\log^7 n)$ βήματα.

- ✓ Στο 3ο βήμα απαιτείται ο υπολογισμός του μέγιστου κοινού διαιρέτη για r ζευγάρια αριθμών. Κάθε ένας από αυτούς απαιτεί χρόνο $O(\log n)$

- ✓ Για το 4ο βήμα η πολυπλοκότητα είναι $O(\log n)$

- ✓ Στο 5ο βήμα έχουμε να κάνουμε $\lfloor 2\sqrt{\phi(r)}\log n \rfloor$ ελέγχους με πολυώνυμα βαθμού r και συντελεστές $O(\log n)$ ψηφίων

- ✓ Κάθε έλεγχος απαιτεί $O(\log n)$ πολλαπλασιασμούς και έτσι απαιτούνται στο 5ο βήμα
  $O\sim(r\sqrt{\phi(r)}\log^3 n) = O\sim(r^{3/2}\log^3 n) = O\sim(\log^{10,5} n)$ πράξεις

□

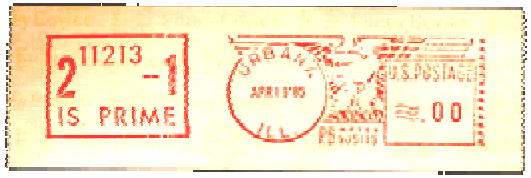
Πρώτοι αριθμοί με ιστορία – αριθμοί Mersenne

- Ο μοναχός Marin Mersenne (1588-1648) στον πρόλογο του έργου του '*Cogitata Physica-Mathematica'* εικάζει οτι όλοι οι αριθμοί της μορφής $2^n - 1$ που είναι πρώτοι με $n \leq 257$ είναι αυτοί για $n = 2,3,5,7,13,17,19,31,67,127$ και 257

- Αν και η εικασία αποδεικνύεται λανθασμένη, δωρίζει το όνομά του σε αυτούς τους αριθμούς.

- Οι Fermat(1640), Euler(1750), Lucas(1876), Pervouchine (1883), Powers(αρχές 1900) τροποποιούν τη λίστα στη σωστή $n = 2,3,5,7,13,17,19,31,61,89,107$ και 127.

Γνωστοί αριθμοί Mersenne



#	Εκθέτης p	Πλήθος ψηφίων στο δεκαδικό	έτος	ερευνητής
1	2	1	----	----
2	3	1	----	----
3	5	2	----	----
4	7	3	----	----
5	13	4	1456	Ανώνυμος
6	17	6	1588	Cataldi
7	19	6	1588	Cataldi

8	31	10	1772	Euler
9	61	19	1883	Pervushin
10	89	27	1911	Powers
11	107	33	1914	Powers
12	127	39	1876	Lucas
13	521	157	1952	Robinson
14	607	183	1952	Robinson
15	1279	386	1952	Robinson
16	2203	664	1952	Robinson
17	2281	687	1952	Robinson
18	3217	969	1957	Riesel
19	4253	1281	1961	Hurwitz
20	4423	1332	1961	Hurwitz
21	9689	2917	1963	Gillies
22	9941	2993	1963	Gillies
23	11213	3376	1963	Gillies
24	19937	6002	1971	Tuckerman

25	21701	6533	1978	Noll & Nickel
26	23209	6987	1979	Noll
27	44497	13395	1979	Nelson & Slowinski
28	86243	25962	1982	Slowinski
29	110503	33265	1988	Colquitt & Welsh
30	132049	39751	1983	Slowinski
31	216091	65050	1985	Slowinski
32	756839	227832	1992	Slowinski & Gage
33	859433	258716	1994	Slowinski & Gage
34	1257787	378632	1996	Slowinski & Gage
35	1398269	420921	1996	Armengaud, Woltman, et. al. (GIMPS)
36	2976221	895932	1997	Spence, Woltman, et. al. (GIMPS)
37	3021377	909526	1998	Clarkson, Woltman, et. al. (GIMPS, PrimeNet)
38	6972593	2098960	1999	Hajratwala, Woltman,

??	13466917	4053946	2001	et. al. (GIMPS, PrimeNet) Cameron, Woltman, et. al. (GIMPS, PrimeNet)

- Δεν είναι γνωστό αν πράγματι ο τελευταίος αριθμός είναι ο $39^{ος}$ αριθμός Mersenne

- Τα τελευταία αποτελέσματα βασίζονται στη διαδικτυακή εφαρμογή Great Internet Mersenne Prime Search του George Woltman

Ενδιαφέροντα θεωρήματα

- Ένας άρτιος αριθμός είναι τέλειος ανν είναι της μορφής $2^{n-1}(2^n-1)$ με 2^n-1 να είναι πρώτος

- Αν 2^n-1 είναι πρώτος, τότε και ο n είναι πρώτος

- Ας είναι p,q δύο πρώτοι. Αν ο q διαιρεί τον $M_p=2^p-1$, τότε $q=\pm 1 \bmod 8$ και $q=2kp+1$ για κάποιο ακέραιο k.

- Εστω p πρώτος με $p=3 \bmod 4$. Τότε $2p+1$ είναι επίσης πρώτος ανν ο $2p+1$ διαιρεί τον $M_p=2^p-1$.

Πρώτοι αριθμοί με ιστορία – Sophie Germain

Ορισμός : Ένας πρώτος p λέγεται Sophie Germain πρώτος αν και ο $2p+1$ είναι πρώτος.

- Γύρω στα 1825 η Sophie Germain αποδεικνύει την εικασία του Fermat για τους αριθμούς που αργότερα πήραν το όνομά της

- Οι Sophie Germain πρώτοι της μορφής $p = k2^n - 1$ αντιστοιχούν στις δυνάμεις των αριθμών Mersenne που δεν είναι πρώτοι

Μεγάλοι γνωστοί Sophie Germain πρώτοι

#	πρώτος	πλήθος ψηφίων	έτος	ερευνητής
1	$\mathbf{2540041185 \cdot 2^{114729}-1}$	34547	2003	TwinGen, PRP,
2	$\mathbf{18912879 \cdot 2^{98395}-1}$	29628	2002	Angel, Augustin,
3	$\mathbf{1213822389 \cdot 2^{81131}-1}$	24432	2002	Angel, Augustin,
4	$\mathbf{109433307 \cdot 2^{66452}-1}$	20013	2001	Underbakke,
5	$\mathbf{984798015 \cdot 2^{66444}-1}$	20011	2001	Underbakke,
6	$\mathbf{3714089895285 \cdot 2^{60000}-1}$	18075	2000	Indlekofer, Jarai,
7	$\mathbf{37561665 \cdot 2^{34090}-1}$	10270	2003	Claude Abraham
8	$\mathbf{831264873 \cdot 2^{33539}-1}$	10106	2003	Schoenberger,

9	**$168851511 \cdot 2^{33250}-1$**	10018	2003	Kremelberg,
10	**$918522549 \cdot 2^{33216}-1$**	10008	2003	Rouse, Proth.exe
11	**$305686839 \cdot 2^{33216}-1$**	10008	2002	Rouse, Proth.exe
12	**$26702697 \cdot 2^{33216}-1$**	10007	2002	Rouse, Proth.exe
13	**$18131 \cdot 22817\#-1$**	9853	2000	Lifchitz, Larvala
14	**$18458709 \cdot 2^{32611}-1$**	9825	1999	Charles F. Kerchner
15	**$415365 \cdot 2^{30052}-1$**	9053	1999	Scott, Proth.exe
16	**$60940331 \cdot 2^{29439}+1$**	8870	2002	saridis, Proth.exe
17	**$23345 \cdot 2^{28601}+1$**	8615	2003	Axelsson, Proth.exe
18	**$18482685 \cdot 2^{27182}-1$**	8190	2001	Rouse, Proth.exe
19	**$22717075 \cdot 2^{26000}+1$**	7835	2001	NewPGen, Jobling
20	**$161193945 \cdot 2^{25253}-1$**	7611	2001	Narayanan, Proth.exe

Η εικασία Sophie Germain και ο αλγόριθμος AKS

- Όπως εκτιμήθηκε από τον Wrench η σταθερά των δίδυμων πρώτων είναι $c_2 = \prod_{p \geq 3} \frac{p(p-2)}{(p-1)^2} = 0.6601618158\ldots$

- Η εικασία των Hardy-Littlewood ορίζει οτι το πλήθος των αριθμών Sophie Germain στο διάστημα $[N, N+l]$ να είναι περίπου

$$2c_2\left(\frac{N+l}{\log^2(N+l)} - \frac{N}{\log^2 N}\right)$$

- Εικάζεται οτι το πλήθος των Sophie Germain πρώτων μικρότερων από N τείνει ασυμπτωτικά στο

$$2c_2 \int_2^N \frac{dx}{\log x \log(2x+1)}.$$

Εικασία για την πυκνότητα των Sophie-Germain πρώτων :

- ❖ Το πλήθος των Sophie Germain πρώτων $p < x$ τείνει ασυμπτωτικά στο $2c_2 \frac{x}{\log^2 x}$

- Η εκτίμηση για τη σταθερά των δίδυμων πρώτων δείχνει να δίνει αναπάντεχα καλά αποτελέσματα

Πλήθος Sophie Germain πρώτων μικρότερων από N		
N	**πραγματικό**	**Εκτίμηση**
1,000	37	39
100,000	1171	1166
10,000,000	56032	56128
100,000,000	423140	423295
1,000,000,000	3308859	3307888
10,000,000,000	26569515	26568824

Πρόταση : Αν ισχύει η εικασία για την πυκνότητα των Sophie Germain πρώτων, η πολυπλοκότητα του αλγορίθμου κατεβαίνει στο $O \sim (\log^6 n)$

Απόδειξη :

- ✓ Λόγω της εικασίας και για κατάλληλη σταθερά θα υπάρχουν τουλάχιστον $\log^2 n$ Sophie Germain πρώτοι στο διάστημα $\left[8\log^2 n, c\log^2(\log(\log n))\right]$

- ✓ Κάθε ένα από τους πρώτους αυτούς q θα είναι εκτός του διαστήματος $\left[2, \frac{q-1}{2}\right]$

- ✓ Αν για έναν τέτοιο q ισχύει οτι $o_q(n) \leq 2$, τότε ένα άνω φράγμα για τον q είναι τάξης $O(\log n)$

- ✓ Υπάρχει πρώτος $r = O \sim (\log^2 n)$ με $o_r(n) \geq 4\log^2 n$

- ✓ Στο 2^o και 5^o βήμα μειώνεται το πλήθος των πράξεων

- ✓ Η πολυπλοκότητα του αλγορίθμου είναι πλέον
$$O \sim (\log^6 n)$$

□

Αναμενόμενη πολυπλοκότητα για τον AKS

- Έχουν γίνει σημαντικές προσπάθειες για να αποδειχθεί η εικασία Sophie Germain

- Ο Goldfeld (1969) έδειξε οτι αν συμβολίσουμε με $P(n)$ το μέγιστο πρώτο διαιρέτη του n, τότε πρώτοι αριθμοί με την ιδιότητα $P(q-1) > q^{\frac{1}{2}+c}$ με $c \approx \frac{1}{12}$ έχουν πυκνότητα στους πρώτους μη μηδενική.

- Βελτίωση της πρότασης από τον Fouvry

Λήμμα : Υπάρχουν σταθερές $c > 0$ και $n_o \in N$ τέτοια που για κάθε $x > n_o$ και για $t \le 0{,}6683$ να ισχύει οτι το πλήθος των στοιχείων του συνόλου

$$\{q \mid q \text{ πρώτος με } q \le x \text{ και } P(q-1) > q^t\}$$

είναι μεγαλύτερο ή ίσο από $c\dfrac{x}{\ln x}$.

- Το σύνολο $\{q \mid q \text{ πρώτος με } q \le x \text{ και } P(q-1) > q^t\}$ παρουσιάζει θετική πυκνότητα στους πρώτους

Θεώρημα : Η αναμενόμενη πολυπλοκότητα του αλγορίθμου είναι

$$O \sim (\log^{7,5} n)$$

Απόδειξη :

- ✓ Λόγω της πυκνότητα των πρώτων με $P(q-1) > q^{\frac{2}{3}}$ με μεγάλη πιθανότητα, στο 2^{o} βήμα του ο αλγόριθμος θα εντοπίζει ένα $r = O(\log^{3} n)$.

- ✓ Η πολυπλοκότητα του AKS πέφτει στο $O \sim (\log^{7,5} n)$.

□

Η εικασία του Artin και ο αλγόριθμος AKS

Η εικασία πυκνότητας του Emil Artin :

- Αν $n \neq 1$ και επιπλέον το n δεν είναι τέλειο τεράγωνο, τότε το σύνολο όλων των πρώτων για τους οποίους ο n είναι αρχική ρίζα είναι άπειρο

- Αν ο n δεν είναι δύναμη κάποιου αριθμού μεγαλύτερου από τη μονάδα και επιπλέον αν για το αποτετραγωνισμένο μέρος του n' ισχύει οτι $n' \neq 1 \bmod 4$ τότε η πυκνότητα του παραπάνω συνόλου είναι

$$C_{\text{Artin}} = \prod_{k=1}^{\infty} \left[1 - \frac{1}{p_k (p_k - 1)} \right] = 0{,}3739558136\ldots$$

- Δεδομένου $n \in N$ που δεν είναι τέλειο τεράγωνο, το πλήθος των πρώτων $p \le m$ για τους οποίους $o_p(n) = p - 1$ τείνει ασυμπτωτικά στο $C_{\text{Artin}}(n)\dfrac{m}{\ln m}$, όπου $C_{\text{Artin}}(n) > 0{,}35$

- Με υπόθεση τη γενικευμένη εικασία του Riemann, η εικασία του Artin αποδείχθηκε από τον Hooley το 1967

- Κανείς δεν έχει αποδείξει αυτό το κομμάτι της εικασίας ακόμα και για σταθεροποιημένο n.

Πρόταση : Αν ισχύει η εικασία του Artin για πρώτους που είναι της τάξης του $O(\log^2 n)$, τότε $r = O(\log^2 n)$. Η πολυπλοκότητα του αλγορίθμου γίνεται $O \sim (\log^6 n)$

Η εικασία των Kayal και Saxena

Εικασία :

- Αν ένας πρώτος r δε διαιρεί το n και αν $(x-1)^n = (x^n - 1) \bmod (x^r - 1, n)$ *, τότε n πρώτος είτε $n^2 = 1 \bmod r$

- Η εικασία έχει ελεγχθεί από τους Neeraj Kayal και Nitin Saxena για $r \leq 100$ και $n \leq 10^{10}$

Πρόταση : Αν ισχύει η εικασία των Kayal και Saxena τότε η πολυπλοκότητα του αλγορίθμου μπορεί να γίνει $O \sim (\log^3 n)$

Απόδειξη :

- ✓ Επιλέγουμε ένα r που δε θα διαιρεί το $n^2 - 1$,
- ✓ Το γινόμενο των πρώτων που είναι μικρότεροι από x είναι τουλάχιστον e^x και άρα το r βρίσκεται στο $[2,4 \log n]$
- ✓ Η σχέση * είναι ελέγξημη σε χρόνο $O \sim (r \log^2 n)$
- ✓ Η πολυπλοκότητα του αλγορίθμου γίνεται $O \sim (\log^3 n)$

□

Η εξέλιξη του AKS

- Άυγουστος 2002 : Δημοσίευση από τους Agrawl, Kayal και Saxena

- Πριν το τέλος του 2002 και ανεξάρτητα οι Pomerance και Lenstra δημοσιεύουν ανεξάρτητα δικές τους σκέψεις στο "The cyclotomic ring test of AKS" και "Primality testing with cyclotomic rings"

- Νοέμβριος 2002 : Ο Berrizbeitia δημοσιεύει εργασία με τίτλο "Sharpening 'Primes in P' for a large family of numbers"

- Μετά τους 2 πρώτους μήνες του 2003 και με παρέμβαση του Lenstra διορθώνονται μικρά λάθη και απλοποιείται ο αλγόριθμος σε αυτόν που ήδη παρουσιάστηκε

- Αρχές του 2003 : Ο Cheng Qi προτείνει πιστοποίηση πρώτων στο ECPP με χρήση μιας επαναληπτικής διαδικασίας από το AKS. Νέα πολυπλοκότητα $O \sim (\log^4 n)$

- Μάρτιος 2003 : Οι Lenstra και Pomerence δημοσιεύουν εργασία με τίτλο “Primality testing with Gaussian periods”. Νέα πολυπλοκότητα για το AKS $O \sim (\log^6 n)$

- Μάρτιος 2003 : Ο Daniel Bernstein, τροποποιεί τον AKS σε ένα randomized αλγόριθμο τάξης $O \sim (\log^4 n)$

Υλοποίηση του AKS

- Πολλές προσπάθειες υλοποίησης έχουν δημοσιευτεί κυρίως σε Mapple, Mathematica και C++

- Μαρτιος 2003 : Οι Crandall και Παπαδόπουλος με τη βοήθεια των Lenstra και Pomerence δημοσιεύουν εργασία με τίτλο “On the implementation of AKS-class primality tests”

- Η πειραματική πολυπλοκότητα του AKS μετά την παρέμβαση του Lenstra σε υπολογιστή Apple G4 (1 GHz) είναι

$$T \approx C \log^6 n \ \text{με} \ C \approx 1000 \,\text{clocks}$$

Γνωστά και αναμενόμενα αποτελέσματα

- Βελτιωμένος (Lenstra) AKS : Για την πιστοποίηση 30-ψήφιου αριθμού απαιτείται σχεδόν μία μέρα

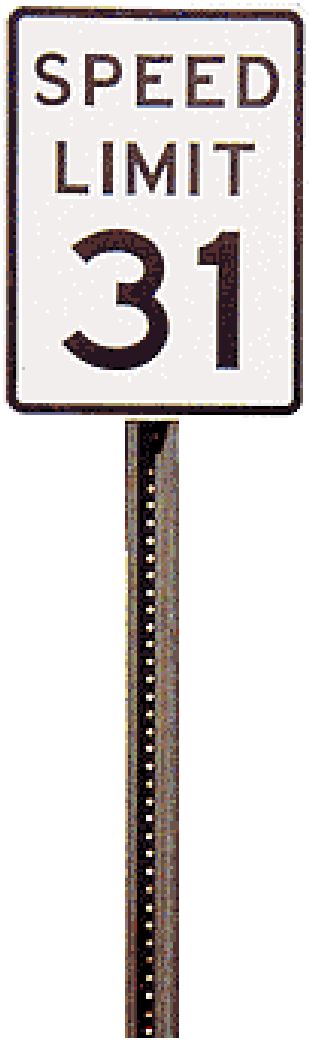
- Αλγόριθμος Bernstein : Πιστοποίηση 300-ψήφιου αριθμού στον ίδιο χρόνο. Εκτιμάται οτι με βελτίωση και πάλι σε μια μέρα ένας 700-ψήφιος αριθμός είναι μέσα στις δυνατότητες

- Οι 10^{24} περίπου CPU υπολογισμοί που έχουν γίνει μέχρι σήμερα στην ανθρωπότητα θα έδιναν απάντηση για ένα 100.000 ψήφιο αριθμό

Ανοιχτά προβλήματα για τους φιλόδοξους

- Υπάρχουν περιττοί τέλειοι αριθμοί;
- Υπάρχουν άπειροι το πλήθος αριθμοί Mersenne;
- Η εικασία του Goldbach. Κάθε άρτιος μεγαλύτερος του 2 γράφεται σαν άθροισμα δύο πρώτων.
- Το πρόβλημα των περιττών του Goldbach: Κάθε περιττός μεγαλύτερος του 5 γράφεται ως άθροισμα τριών πρώτων.
- Κάθε άρτιος γράφεται ως διαφορά δυο πρώτων.
- Υπάρχουν άπειροι δίδυμοι πρώτοι;
- Υπάρχουν άπειροι πρώτοι της μορφής $n^2 + 1$;
- Υπάρχει πάντα πρώτος μεταξύ των n^2 και $(n+1)^2$;
- Υπάρχουν άπειροι Fermat-πρώτοι[1] αριθμοί;

[1] Πρώτοι αριθμοί της μορφής $2^{2^n} + 1$


SPEED
LIMIT
31