Kiel trovi grandegajn primojn

Clayton Smith

La 6-an de novembro, 2003

Strategio

- Baza strategio: Elektu n. Kontrolu, ĉu n estas primo. Ripetu laŭbezone.
- Laŭ la "Teoremo de primoj", la probableco ke n estas primo estas $\sim 1/\log n$.
- Necesas $\sim \log n$ provoj por trovi primon.

Strategio

- Problemo: Kiel pruvi ke n estas primo?

  Algoritmoj por ĝenerala n povas pritrakti nur $\sim 5,000$ ciferojn.

- Fariĝas pli facile, se n estas proksima al nombro kun multaj malgrandaj faktoroj.

- $n = k \cdot a^m \pm 1$ bone funkcias.

Mersenne-aj nombroj

- $M_n = 2^n - 1$

- Se $2^n - 1$ estas primo, tiam n estas primo.

- $2^{ab} - 1 = (2^a)^b - 1^b = (2^a - 1)(\ldots)$

Mersenne-aj nombroj

- Malgrandaj ekzemploj:

$$\begin{aligned} 2^2 - 1 &= 3 \\ 2^3 - 1 &= 7 \\ 2^5 - 1 &= 31 \\ 2^7 - 1 &= 127 \\ 2^{11} - 1 &= 2047 = 23 \cdot 89 \\ &\vdots \end{aligned}$$

- Estas nur 39 konataj Mersenne-aj primoj.

Faktoroj de Mersenne-aj nombroj

Teoremo: p kaj q estu malparaj primoj, kaj q dividu $M_p = 2^p - 1$. Tiam

$$q \equiv 1 \pmod{p}$$

kaj

$$q \equiv \pm 1 \pmod{8}.$$

Eblas kombini tiujn ĉi per la "Ĉina teoremo pri restaĵoj".

Ekzemplo: $2^{31} - 1 = 2147483647$

Se q dividas $2^{31} - 1$, tiam

$$q \equiv 1 \pmod{31}$$

kaj

$$q \equiv \pm 1 \pmod{8}.$$

Laŭ la Ĉina teoremo pri restaĵoj, tio signifas ke $q \equiv 1$ aŭ $63 \pmod{248}$. Estas 374 tiaj q-oj malpli grandaj ol $\sqrt{2^{31} - 1}$, sed nur 84 el ili estas primoj.

En 1772, Euler uzis ĉi tiun metodon por pruvi ke $2^{31} - 1$ estas primo.

Primeco-testo por Mersenne-aj nombroj

Difinu la vicon $(v_k)_{k=0,1,\ldots}$ per

$$\begin{aligned} v_0 &= 4 \\ v_{k+1} &= v_k^2 - 2. \end{aligned}$$

p estu malpara primo. Tiam $M_p = 2^p - 1$ estas primo se kaj nur se $v_{p-2} \equiv 0 \pmod{M_p}$.

Lucas unue uzis ĉi tiun teston en 1876 por pruvi ke $2^{127} - 1$ estas primo. (Ĉi tiu nombro havas 39 dekumajn ciferojn.)

Ekzemplo: $2^7 - 1 = 127$

Laŭ modulo $2^7 - 1$:

$$
\begin{aligned}
v_0 &= 4 \\
v_1 &= 4^2 - 2 = 14 \\
v_2 &= 14^2 - 2 = 194 = 67 \\
v_3 &= 67^2 - 2 = 4487 = 42 \\
v_4 &= 42^2 - 2 = 1760 = 111 \\
v_5 &= 111^2 - 2 = 12319 = 0
\end{aligned}
$$

Do $2^7 - 1$ estas primo.

Rapideco

- La kvadratigo postulas plej multe da tempo; baza algoritmo postulas $O(p^2)$, sed per FFT-aj algoritmoj eblas uzi nur $O(p \log p \log \log p)$.

- Redukto laŭ modulo M_p estas facila duume, sed fakte eblas forigi ĝin entute, enplektante ĝin en la FFT-an multiplikon.

- Estas $p-2$ kvadratigoj, do la tuta rultempo estas

$$O(p^2 \log p \log \log p)$$

Rapideco

- Pri rapida ol eĉ unu probableca primeco-testo.

- Necesas ĉ. 10 tagoj por testi nombron kun 6 milionoj da ciferoj per 2.4-GHz-a procesoro.

GIMPS

- Granda Interreta Serĉo je Mersenne-aj Primoj (Great Internet Mersenne Prime Search)
- Distribuata komputado
- Fondita en 1996 de George Woltman
- http://www.mersenne.org/

GIMPS

- 40,000 komputiloj, 8.5 teraflops (bilionoj da bazaj operacioj sekunde)

- Trovis jam 5 novajn Mersenne-ajn primojn

- Trovis la 4 plej grandajn konatajn primojn

Test-procezo

- Serĉi malgrandajn faktorojn
- Serĉi pli grandajn faktorojn per la metodo “Pollard $p-1$”
- Fari Lucas-teston
- Kontroli la rezulton per dua sendependa Lucas-testo

Premioj de EFF
(Electronic Frontier Foundation)

- $50,000 por la unua primo kun miliono da ciferoj; gajnita en 1999 de GIMPS-ano Nayan Hajratwala

- $100,000 por la unua primo kun dek milionoj da ciferoj

- $150,000 por la unua primo kun cent milionoj da ciferoj

- $250,000 por la unua primo kun miliardo da ciferoj

Plej granda konata primo

- $2^{13,466,917} - 1$
- 4,053,946 ciferoj
- Trovita la 14-an de novembro, 2001 de Michael Cameron el Kanado

Nesolvitaj problemoj

- Ĉu estas senfine multaj Mersenne-aj primoj?

- Ĉu estas senfine multaj Mersenne-aj neprimoj?