Jagd nach der Monsterprimzahl

KANT Group – Prof. Dr. Michael E. Pohst

Technische Universität Berlin
Institut für Mathematik

pohst@math.tu-berlin.de

12. 06. 2004
Lange Nacht der Wissenschaften

Motivation zur Jagd nach Primzahlen

- Die Primzahlen sind Grundbausteine
- Verwendung in der Computerindustrie
- Historische Gründe

Marin Mersenne (1588 - 1648)

Historisches: Der Anfang

Mersennesche Zahlen sind Zahlen M_p der Form $2^p - 1$ mit $p \geq 2$ eine ganze Zahl.

Historisches: Der Anfang

Mersennesche Zahlen sind Zahlen M_p der Form $2^p - 1$ mit $p \geq 2$ eine ganze Zahl.

Zahlen dieser Form wurden bereits im antiken Griechenland betrachtet.

Ein Manuskript aus dem Jahr 1456 behauptet (ohne Beweis): Die Zahl

$$2^{13} - 1 = 8191$$

ist eine Primzahl. Die Behauptung ist wahr.

Ein Manuskript aus dem Jahr 1456 behauptet (ohne Beweis): Die Zahl

$$2^{13} - 1 = 8191$$

ist eine Primzahl. Die Behauptung ist wahr.

1536 Hudalricus Regius zeigt: $2^{11} - 1$ ist keine Primzahl.

Mersennesche Primzahlen

1588 Pietro Cataldi zeigte: $2^{17}-1$ und $2^{19}-1$ sind Primzahlen. Er behauptete: 2^n-1 ist für $n = 23, 29, 31, 37$ auch Primzahl.

Mersennesche Primzahlen

1588 Pietro Cataldi zeigte: $2^{17}-1$ und $2^{19}-1$ sind Primzahlen. Er behauptete: 2^n-1 ist für $n = 23, 29, 31, 37$ auch Primzahl.

1644 Marin Mersenne (1588 - 1648) behauptete: Für alle Primzahlen $n \leq 257$ ist 2^n-1 genau für $n = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257$ eine Primzahl.

Wahrheitsgehalt von Mersennes Behauptung

1772 Euler bewies nach mehreren Jahre Arbeit: $2^{31} - 1$ ist Primzahl.

Wahrheitsgehalt von Mersennes Behauptung

1772 Euler bewies nach mehreren Jahre Arbeit: $2^{31} - 1$ ist Primzahl.

225 Jahre nach Mersennes Behauptung: Es fehlt die Zahl 61.
1883 Pervushin: $2^{61} - 1$ ist eine Primzahl.

Mersennes Liste:

$$n = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257.$$

Mersennes Liste:

$$n = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257.$$

Die korrigierte Liste:

$$n = 2, 3, 5, 7, 13, 17, 19, 31, 61, \quad , 89, 107, 127, \quad .$$

Ergebnisse ohne Verwendung von Computern

Zahl	Ziffernanzahl	Jahr	Autor	Methode
$2^{17}-1$	6	1588	Cataldi	Divisionsversuche
$2^{19}-1$	6	1588	Cataldi	Divisionsversuche
$2^{31}-1$	10	1772	Euler	Divisionsversuche
$2^{127}-1$	39	1876	Lucas	Lucas-Folgen

Teil von Mersennes Liste

Der Lucas-Lehmer Test

Zu vorgegebener Primzahl p setzt man: $s_0 := 4$

und berechnet iterativ

$$s_{k+1} := {s_k}^2 - 2 \qquad (k = 0, 1, 2, \ldots, p-2).$$

(LL-Folge)

$$M_p \textbf{ Primzahl} \Leftrightarrow M_p \textbf{ teilt } s_{p-2}$$

Durchführung des Lucas-Lehmer-Tests

- Für ${s_k}' \equiv s_k \mod M_p$:
- Berechne $z = {s_k}'^2 - 2$
- Berechne ${s_{k+1}}' \equiv z \mod M_p$:

$$
\begin{aligned}
z &= r2^p + s && \left(\quad 0 \le r < 2^p - 2, \quad 0 \le s < 2^p \quad \right) \\
&= r(2^p - 1) + r + s && \left(\quad 0 \le r + s < 2(2^p - 1) \quad \right) \\
&= rM_p + r + s && \left(\quad 0 \le r + s < 2M_p \quad \right)
\end{aligned}
$$

$$
{s_{k+1}}' = \begin{cases} r + s & \text{für} \quad 0 \le r + s \le M_p \\ r + s - M_p & \text{für} \quad M_p \le r + s \end{cases}
$$

Mersennesche Primzahlen 13.-20.

Nr.	Zahl	Ziffernanzahl	Jahr	Autor
13	2^{521}	157	1952	Robinson
14	2^{607}	183	1952	Robinson
15	2^{1279}	386	1952	Robinson
16	2^{2203}	664	1952	Robinson
17	2^{2281}	687	1952	Robinson
18	2^{3217}	969	1957	Riesel
19	2^{4253}	1281	1961	Hurwitz
20	2^{4423}	1332	1961	Hurwitz

Mersennesche Primzahlen 21.-29.

21	$2^{9689}-1$	2917	1963	Gillies
22	$2^{9941}-1$	2993	1963	Gillies
23	$2^{11213}-1$	3376	1963	Gillies
24	$2^{19937}-1$	6002	1971	Tuckerman
25	$2^{21701}-1$	6533	1978	Noll & Nickel
26	$2^{23209}-1$	6987	1979	Noll
27	$2^{44497}-1$	13395	1979	Nelson, Slowinski
28	$2^{86243}-1$	25962	1982	Slowinski
29	$2^{110503}-1$	33265	1988	Colquitt, Welsh

Mersennesche Primzahlen 30.-35.

Nr.	Zahl	Ziffernanzahl	Jahr	Autor
30	$2^{132049}-1$	39751	1983	Slowinski
31	$2^{216091}-1$	65050	1985	Slowinski
32	$2^{756839}-1$	227832	1992	Slowinski, Gage
33	$2^{859433}-1$	258716	1994	Slowinski, Gage
34	$2^{1257787}-1$	378632	1996	Slowinski, Gage.
35	$2^{1398269}-1$	420921	1996	Armengaud, Woltman.

Aktueller Stand

Nr.	Zahl	Ziffernanzahl	Jahr	Autor
36	$2^{2976221}-1$	895932	1997	Spence,Woltman
37	$2^{3021377}-1$	909526	1998	Clarkson, et. al.
38	$2^{6972593}-1$	2098960	1999	Hajratwala, et. al.
39	$2^{13466917}-1$	4053946	2001	Cameron, et. al.
40	$2^{20996011}-1$	6320430	2003	Shafer, et. al.
41	$2^{24036583}-1$	7235733	2004	Findley, et. al.

Ergebnisse im Rahmen von GIMPS erzielt.

15. 05. 2004: Entdeckung der 41. Mersenneschen Primzahl.

Die Jagd nach den Mersenneschen Primzahlen geht weiter. . .

Die Jagd nach den Mersenneschen Primzahlen geht weiter. . .

Die Suche nach einer Primzahl mit 10 Millionen Ziffern startet am Institut für Mathematik

hier und jetzt**!**