$2^{37.156.667} - 1$ ist eine Primzahl!

Hans-Michael Elvenich
(Lanxess Leverkusen)

michael@elvenich.de

Am 6. September 2008 um 21.54 Uhr MESZ entdeckte mein Computer eine der größten bisher bekannten Mersenne[1]-Primzahlen. Diese Zahl hat 11.185.272 Ziffern und damit mehr als die von der US-Stiftung Electronic Frontier Foundation[2], kurz EFF, geforderten 10 Millionen Stellen. Diese Stiftung hatte darauf ein Preisgeld von 100.000 Dollar ausgesetzt. Allerdings hatte die Universität von Kalifornien in Los Angeles zwei Wochen vorher eine noch größere Zahl entdeckt und somit den fast zehnjährigen Wettlauf quasi mit einem „Fotofinish" für sich entschieden.

Mersenne-Zahlen sind Zahlen der Form $M_p = 2^p - 1$, wobei der Exponent p selbst eine Primzahl sein muss, ansonsten handelt es sich um eine zusammengesetzte Zahl. Ist diese Zahl M_p prim, so spricht man von einer *Mersenne-Primzahl*.

Nachdem bisher 42 Kandidaten von meinem Rechner nach längeren Prüfungen als nicht prim identifiziert worden waren, wurde mir am 2. Februar 2008 der 43. Prüfling von GIMPS[3] (Great Internet Mersenne Prime Search) zugeteilt. Eigentlich hätte mein neuester Rechner, ein PC mit einer Intel ® Core^{TM} 2 Duo CPU E8300 @ 2,83 GHz diese Zahl im 24/7-Betrieb (24 Stunden am Tag und 7 Tage in der Woche) in nur 42 Tagen überprüfen können, allerdings hatte ich mich ab Januar 2008 dazu entschlossen, meinen Rechner nicht mehr wie die bisherigen vier Jahre dauernd laufen zu lassen, sondern nur noch vier bis fünf Stunden pro Tag. Die immer weiter steigenden Energiekosten hatten mich dazu veranlasst. Mein Rechner hatte einen jährlichen Verbrauch von fast 3.000 kWh. Durch diese Sparmaßnahme wurde aus dem eigentlichem Endberechnungsdatum (15. März 2008) der 6. September 2008.

Man braucht kein Mathematiker zu sein, um sich bei dieser Suche zu beteiligen. Man lädt eine Software[4] aus dem Internet, welche die Leerlaufzeiten des PCs ausnutzt, um zugeteilte Primzahlkandidaten zu testen. 1996 gründete der Programmierer George Woltman[5] das GIMPS-Projekt. Hier werden PCs durch das Internet zusammen geschaltet, um eine größere gemeinsame Rechenkraft zu erhalten. Bis heute haben sich fast 26.000 Nutzer mit ca. 140.000 PCs registriert. Die aktiven PCs (16 %) haben heute eine durchschnittliche gemeinsame Rechenleistung von 40 TFLOP (Trillions of calculations) pro Sekunde, also 40 Billionen Gleitkommaoperationen pro Sekunde, entsprechend 40 TeraFLOPS. Zum Vergleich: Im März 2006 wurde der damals neueste „schnellste" Computer Deutschlands in Jülich in Betrieb genommen, der JUBL (Jülicher Blue Gene/L). Mit 45,6 TeraFLOPS bot er zu diesem Zeitpunkt als sechstschnellster Computer der Welt die Rechenleistung von 15.000 „normalen" zeitgemäßen PCs[6]. Als Nachfolger wurde in Jülich der JUGENE (Jülicher BlueGene/P) aufgebaut. Dieser hat seit einem Upgrade letztes Jahr 825,5 TeraFLOPS und belegt nun Platz 3.[7]

Diese auf Ihrem heimischen Rechner installierte Software testet zugewiesene Testkandidaten der Form $M_p = 2^p - 1$. Diese Form hat den Vorteil, dass man sie relativ einfach durch den Lucas-Lehmer-Test auf die Primeigenschaft testen kann. Die GIMPS-Software prüft zunächst, ob für den Mersenne-Primzahlenkandidaten ein kleiner Faktor (z. B. bis 275) gefunden werden kann. Anschließend folgt die P-1-Factoring-Stufe. Mit diesen beiden Vortests möchte man relativ kleine Primfaktoren ausschließen, bevor man den doch etwas länger dauernden Lucas-Lehmer-Test startet. Dieser Test verwendet nur Grundrechenarten. Für die Multiplikationen verwendet die Software die schnelle „Irrational Base Discrete Weighted Transform" (IBDWT), entwickelt von Richard Crandall.[8] Der Lucas-Lehmer-Test liefert als Ergebnis nur eine Ja/Nein-Aussage, aber keine Faktoren. Im Zahlenbereich um $2^{37.156.667} - 1$ lag die Chance, dass der Kandidat eine Primzahl ist, bei ca. $1 : 320.000$. Innerhalb von 13 Jahren wurden durch das GIMPS-Projekt 13 neue Mersenne-Primzahlen entdeckt:

[1] Marin Mersenne, französischer Mathematiker uvm., 1588-1648 (`http://de.wikipedia.org/wiki/Marin_Mersenne`)
[2] EFF Cooperative Computing Awards (`http://www.eff.org/awards/coop`)
[3] Great Internet Mersenne Prime Search (`http://www.mersenne.org/`)
[4] GIMPS Software (`http://www.mersenne.org/freesoft/`)
[5] George Woltman (`http://en.wikipedia.org/wiki/George_Woltman`)
[6] FLOPS (`http://de.wikipedia.org/wiki/FLOPS`)
[7] Liste der 500 schnellsten Computersysteme, Wikipedia (`http://de.wikipedia.org/wiki/TOP500`)
[8] Richard Crandall, US-Informatiker (`http://de.wikipedia.org/wiki/Richard_Crandall`)

Jahr	Zahl	Ziffern	Entdecker
1996	$2^{1.398.269} - 1$	420.921	Armengaud, GIMPS
1997	$2^{2.976.221} - 1$	895.932	Spence, GIMPS
1998	$2^{3.021.377} - 1$	909.526	Clarkson, GIMPS
1999	$2^{6.972.593} - 1$	2.098.960	Hajratwala, GIMPS
2001	$2^{13.466.917} - 1$	4.053.946	Cameron, GIMPS
2003	$2^{20.996.011} - 1$	6.320.430	Shafer, GIMPS
2004	$2^{24.036.583} - 1$	7.235.733	Findley, GIMPS
2005	$2^{25.964.951} - 1$	7.816.230	Nowak, GIMPS
2005	$2^{30.402.457} - 1$	9.152.052	Cooper, Boone, GIMPS
2006	$2^{32.582.657} - 1$	9.808.358	Cooper, Boone, GIMPS
2008	$2^{37.156.667} - 1$	11.185.272	Elvenich, GIMPS
2009	$2^{42.643.801} - 1$	12.837.064	Strindmo, GIMPS
2008	$2^{43.112.609} - 1$	12.978.189	Smith, GIMPS

Ausblick: Für die erste bekannte Primzahl mit mehr als 100 Millionen Stellen hat die EFF einen weiteren Preis in Höhe von 150.000 Dollar ausgesetzt. Meiner Meinung nach wird bei gleicher Erhöhung der Rechnerleistungen wie in den vergangenen Jahren dies erst 2018 mit Hilfe von Standard-PCs möglich sein. Ziel meiner weiteren Aktivitäten ist es, ein Verfahren zur Generierung von Primzahlen zu finden bzw. im Umkehrschluss einen schnellen Test für spezielle Primzahlen. Primzahl-Enthusiasten können ihre interessanten Projektarbeiten unter meiner Webseite `www.primzahlen.de` veröffentlichen.

Komplexe Multiplikation: von numerisch bis symbolisch

Andreas Enge
(INRIA Bordeaux–Sud-Ouest)

andreas.enge@math.u-bordeaux.fr

Die Theorie der komplexen Multiplikation vereint in bemerkenswerter Weise Analysis (Funktionentheorie, Riemannsche Flächen) und Algebra (Zahlentheorie, Klassenkörpertheorie). In der Praxis führt das dazu, dass sich algebraische, diskrete Objekte mit analytischen, numerischen Methoden berechnen lassen.

Anwendungen

Die Hauptanwendung der komplexen Multiplikation besteht darin, elliptische Kurven über einem endlichen Körper mit vorab bekannter Punktezahl zu konstruieren. Sei $D < 0$ eine quadratische Diskriminante und q eine Primzahlpotenz, so dass die Gleichung

$$4q = t^2 - v^2 D \tag{1}$$

eine Lösung in ganzen Zahlen t, v mit $\mathrm{ggT}(t, v) = 1$ besitzt. Dann gibt es eine elliptische Kurve über $\mathbb{F}_q$ mit $N = q + 1 - t$ Punkten; wir werden im folgenden sehen, wie sich eine solche Kurve in Zeit

$$O\tilde{}\left(|D|\right) := O\left(|D| \, \log^{O(1)} |D|\right)$$

bestimmen lässt.

Dies kann ausgenutzt werden, um für die Kryptographie geeignete Kurven zu berechnen. Mit den Fortschritten beim Zählen der Punkte auf zufälligen Kurven[1] wurde diese Anwendung zunächst obsolet, um dann im Zuge paarungsbasierter Kryptographie[2] eine Renaissance

[1] F. Vercauteren: *Counting points on curves over finite fields*, Computeralgebra-Rundbrief 43, 2008, S. 16–19
[2] F. Heß: *Kryptographie mit elliptischen Kurven*, Computeralgebra-Rundbrief 39, 2006, S. 14–18