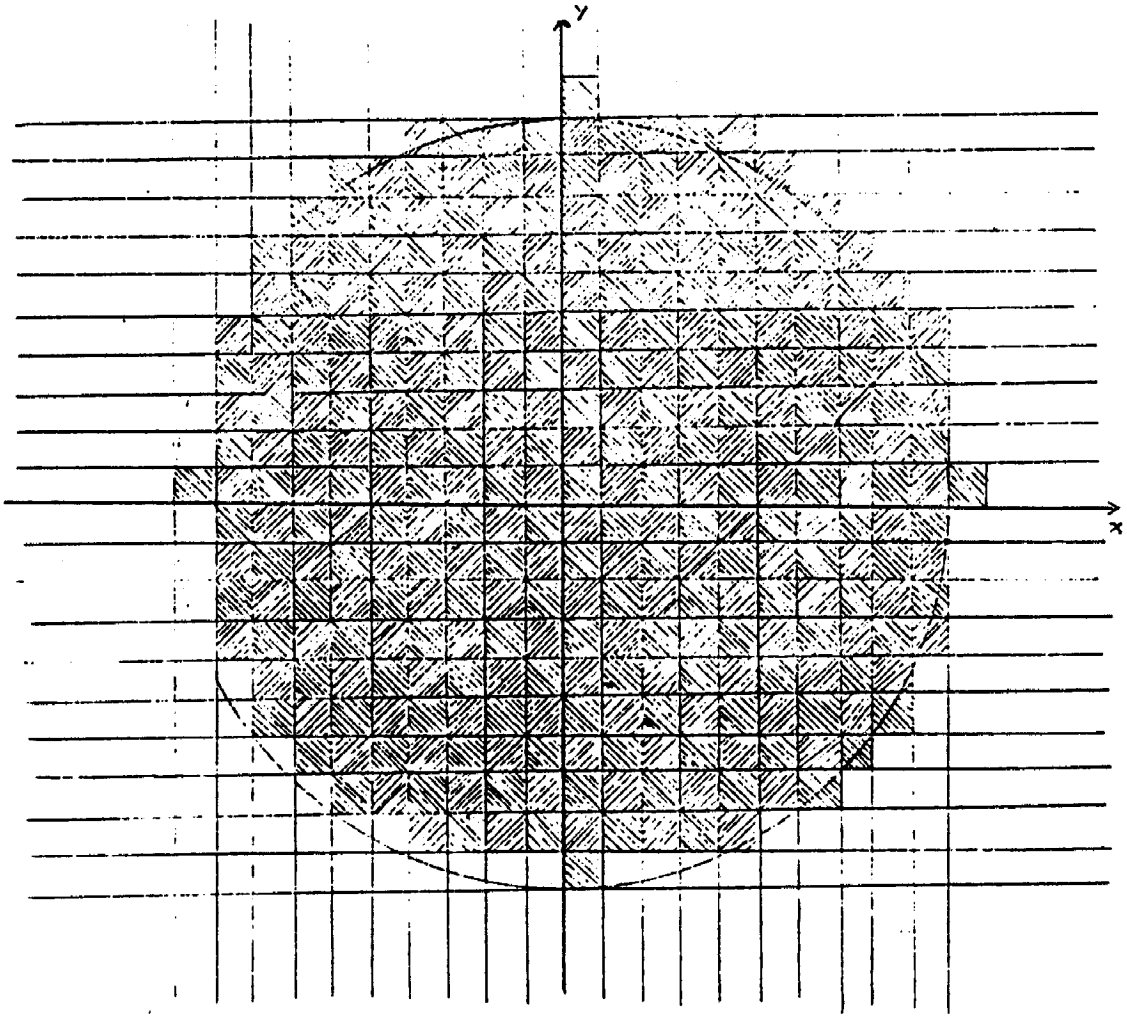
Neuere Entwicklungen in der Zahlentheorie

Johannes Schoissengeier, Wien

Das Kreisproblem

Gegeben sei ein Kreis mit Mittelpunkt $(0,0)$ und Radius $\sqrt{R}$. Das *Kreisproblem* besteht darin, die Anzahl $A(R)$ der Punkte mit ganzzahligen Koordinaten, die innerhalb des Kreises oder auf ihm liegen, für große R möglichst genau anzugeben. Ordnen wir jedem solchen Punkt das Quadrat mit Seitenlänge 1 zu, dessen linke untere Ecke er ist, so werden wir vermuten, daß diese Anzahl in erster Näherung $R\pi$, der Flächeninhalt des Kreises ist.



Anzahl der Punkte im Kreis $x^2 + y^2 = 100$.

Will man genaueres wissen, so ist also $|A(R) - R\pi|$ nach oben abzuschätzen. Dazu führen wir folgende Bezeichnung ein: wir schreiben $f(x) = O(x^\alpha)$, wenn es ein $c > 0$ gibt, sodaß für alle $x > 1$ $|f(x)| \leq cx^\alpha$, d.h. wenn $f(x)$ nicht schneller gegen unendlich wächst als x^α. Wir suchen nun das kleinste α, sodaß $A(R) - R\pi = O(R^\alpha)$ ist; genauer, da wir gar nicht wissen, ob es ein solches gibt (es könnte ja für jedes solche α noch ein kleineres mit dieser Eigenschaft geben),

$$\theta := \inf\{\alpha | A(R) - R\pi = O(R^\alpha)\}.$$

Hardy [HA] und Landau [LA1] waren die ersten, die $\theta \geq \frac{1}{4}$ gezeigt haben, eine Abschätzung, die bis heute nicht verbessert worden ist.

Welch große Anstrengungen unternommen wurden, um θ zu bestimmen, von dem heute allgemein angenommen wird, daß es gleich $\frac{1}{4}$ ist, beweist die folgende eindrucksvolle Liste:

$\theta \leq 1/2$	C.F. Gauß
$\theta \leq 1/3$	W. Sierpiński [SI]
$\theta < 1/3$	J. G. van der Corput [CO]
$\theta \leq 37/112 = 0.3303...$	E. Landau [LA2], J. E. Littlewood-A. Walfisz [LW]
$\theta \leq 163/493 = 0.3299...$	A. Walfisz [WA]
$\theta \leq 27/82 = 0.3292...$	L.W. Nieland [NI]
$\theta \leq 15/46 = 0.3260...$	E.C. Titchmarsh [TI]
$\theta \leq 13/40 = 0.325$	L.-K. Hua [HU]
$\theta \leq 12/37 = 0.3243...$	J. Chen [CH]
$\theta \leq 35/108 = 0.32407...$	W.-G. Nowak [NO]
$\theta \leq 139/429 = 0.32400...$	G. Kolesnik [KOL]
$\theta \leq 7/22 = 0.\overline{318}$	H. Iwaniec, C.J. Mozzochi [IM]
$\theta \leq 23/73 = 0.3150...$	M.N. Huxley [HUX]

Die Riemannsche Vermutung

Es sei für $\Re(s) > 0$ $\zeta(s) = (1 - 2^{1-s})^{-1} \sum_{n=1}^{\infty} \frac{(-1)^{n+1}}{n^s}$. Die Reihe konvergiert für diese s. Das bedeutendste ungelöste Problem der Zahlentheorie besteht darin zu zeigen (oder zu widerlegen), daß alle Nullstellen dieser Funktion Realteil $\frac{1}{2}$ haben. Es ist dies für die ersten 1 500 000 001 Nullstellen mit positivem (oder auch negativem) Imaginärteil bewiesen, wenn man sie der Größe nach ordnet [LRW].

Die Bedeutung dieser von Riemann stammenden Vermutung ergibt sich aus folgendem: bezeichnet $\pi(x)$ die Anzahl der Primzahlen $p \leq x$ und $\mathrm{li}(x) = \int_2^x \frac{du}{\log u}$, so besagt der Primzahlsatz, daß $\pi(x) \sim \mathrm{li}(x)$ ist. Das Problem besteht nun darin, die kleinste Zahl α zu finden, für die $\pi(x) - \mathrm{li}(x) = O(x^\alpha)$ noch richtig ist, oder, da wir nicht wissen, ob es ein solches überhaupt gibt, $\alpha_0 = \inf\{\alpha | \pi(x) - \mathrm{li}(x) = O(x^\alpha)\}$ zu bestimmen. Dieses α_0 ist nun gleich dem größten Realteil einer Nullstelle von ζ, oder genauer, da wir nicht wissen, ob er existiert, gleich $\sup\{\Re(s) | \zeta(s) = 0\}$. Da wir $\alpha_0 = \frac{1}{2}$ nicht beweisen können, müssen sich die Mathematiker mit dem viel schwächeren Ergebnis (für ein gewisses $c > 0$)

$$\pi(x) - \mathrm{li}(x) = O(xe^{-c(\log x)^{3/5}(\log\log x)^{-2/5}})$$

zufriedengeben, das im wesentlichen von Vinogradov stammt und schon seit 1958 bekannt ist [VI].

In engem Zusammenhang mit der Riemannschen Vermutung steht die sogenannte *Mertensche Vermutung*. Bezeichnen μ die Möbiussche μ-Funktion (es ist $\mu(n) = (-1)^k$, wenn n das Produkt von k verschiedenen Primzahlen ist, und $= 0$ sonst), so hat Mertens vermutet, daß für alle $n \in \mathbb{N}$ $|\sum_{t=1}^{n} \mu(t)| < \sqrt{n}$. Diese Vermutung würde die Riemannsche implizieren, ist aber, wie in [OR] gezeigt wurde, falsch. Sie bewiesen daß es unendlich viele $n \in \mathbb{N}$ gibt, mit $|\sum_{t=1}^{n} \mu(t)| \geq 1{,}06\sqrt{n}$. Allerdings konnten sie kein solches n angeben; das kleinste ist wahrscheinlich $> 10^{30}$.

Kryptographie

Bis zum Jahr 1976 sind geheime Botschaften dadurch ausgetauscht worden, daß Sender und Empfänger denselben Schlüssel hatten. Daher war es notwendig, sich diesen Schlüssel gegenseitig mitzuteilen, was einem Dritten das Abhören theoretisch ermöglicht hat. Dieser Schlüssel ist nichts anderes als eine Bijektion σ, die jeder Nachricht $(a_1, ..., a_n)$ die verschlüsselte Nachricht $(\sigma(a_1), ..., \sigma(a_n))$ zugeordnet hat. Es war also zumindest notwendig, daß der Sender σ und der Empfänger σ^{-1} kennt.

1976 wurde von Diffie und Hellman [DH] etwas ganz Neues vorgeschlagen. σ wird öffentlich bekannt gegeben. Das hat den Vorteil, daß jeder dem Empfänger eine Nachricht zukommen kann. Die Berechnung von σ^{-1} ist aber ohne zusätzliche Information nur durch unrealistisch lange Rechenzeiten möglich. Diese Zusatzinformation hat nur der Empfänger. Es ist also in diesem System gar nicht notwendig, daß sich Sender und Empfänger kennen.

Solche Bijektionen σ stellt nun die Zahlentheorie zur Verfügung. Das allerwichtigste und meist gebrauchte Verfahren ist das sogenannte RSA-Verfahren, das nach Rivest, Shamir und Adleman [RSA] benannt ist. Es funktioniert folgendermaßen:

Der Empfänger wählt eine natürliche Zahl n, deren Primfaktorzerlegung nur er kennt, und gibt n öffentlich bekannt. Ferner wählt er eine zu $\varphi(n)$ teilerfremde Zahl $e > 1$, die er ebenfalls bekannt gibt. Die Wahl von e läßt sich leicht bewerkstelligen, weil er die Primteiler von n, also auch $\varphi(n) = n \prod_{p|n}(1 - \frac{1}{p})$ kennt. Schließlich wählt er noch eine ganze Zahl f, die $ef \equiv 1 \pmod{\varphi(n)}$ erfüllt. Diese Zahl behält der Empfänger für sich.

Es ist nun jedem Menschen, der n und e kennt, möglich, dem Empfänger öffentlich eine Botschaft auf folgendem Weg zukommen zu lassen. Die Botschaft, die meist aus Buchstaben besteht, wird zunächst in eine Zahl übersetzt, etwa, indem A 01, B 02, ..., Z 26 und dem Leerzeichen zwischen zwei Wörtern 00 zugeordnet wird. Ist die entstehende Zahl k größer als n, so muß sie in Blöcke zerlegt werden. Der Sender schickt nun dem Empfänger $k^e \pmod n$, also k^e, mod n reduziert. Der Empfänger bildet nun $(k^e)^f \pmod n$. Diese Zahl ist aber gleich k, die ursprüngliche Botschaft. Das liegt daran, daß es eine ganze Zahl

l gibt, die $ef = 1 + l\varphi(n)$ erfüllt. Es ist also $k^{ef} = k(k^{\varphi(n)})^l \equiv k \cdot 1^l = k \pmod n$ nach dem Kleinen Fermatschen Satz.

BEISPIEL: Im Jahr 1977 wurde im Scientific American das folgende Problem gestellt: Gegeben sind

$n :=$ 1 1438 1625 7578 8886 7669 2357 7997 6146 6120 1021 8296 7212 4236 2562 5618 4293 5706 9352 4573 3897 8305 9712 3563 9587 0505 8989 0751 4759 9290 0268 7954 3541,

$k^e :=$ 9686 9613 7546 2206 1477 1409 2225 4355 8829 0575 9991 1245 7431 9874 6951 2093 0816 2982 2514 5708 3569 3147 6622 8839 8962 8013 3919 9055 1829 9451 5781 5154

und $e := 9007$.

Man entschlüssle die Botschaft k.

Mögliche Einwände: (1) Wenn obiges k zu n nicht teilerfremd ist, läßt sich der Kleine Fermatsche Satz nicht anwenden. Das kann durch verschiedene Vorsichtsmaßnahmen verhindert werden. In der Praxis ist n das Produkt von zwei verschiedenen Primzahlen mit je etwa 65 Stellen. Die Wahrscheinlichkeit, daß zufällig eine dieser Primzahlen die Botschaft k teilt, ist ganz außerordentlich gering, jedenfalls weniger, als die Chance, drei mal hintereinander im Lotto zu gewinnen. Es läßt sich diese Unannehmlichkeit, daß k und n einen Teiler haben könnten, auch noch auf andere Weise umgehen, indem man statt φ eine zu ihr verwandte Funktion verwendet, was auch noch andere Vorteile hat.

(2) Bedenken wir, daß k vielleicht hundert Stellen hat und e möglicherweise ebenfalls, so kommt der Einwand, daß sich k^e auch mit den allergrößten Maschinen nicht mehr ausrechnen läßt. Das ist aber auch gar nicht notwendig, wenn wir bedenken, daß k^e nur mod n benötigt wird. In der Praxis geht man so vor: wir stellen $e = 2^{e_1} + 2^{e_2} + \cdots + 2^{e_t}$ $(e_1 > \ldots > e_t)$ zur Basis 2 dar (was sehr rasch geht) und berechnen k^e mit der Formel $k^e = k^{2^{e_1}} k^{2^{e_2}} k^{2^{e_t}}$. Zur Berechnung von $k^{2^{e_i}} \pmod n$ ist nur mehr fortgesetztes Quadrieren mod n notwendig. Die Berechnung von k^e mod n geht so in $O(\log^3 n)$ Schritten vor sich. Auf dieselbe Weise entschlüsselt der Empfänger bei der Berechnung von $(k^e)^f$. Dieses Verfahren wird neuerdings nach D. Knuth benannt, war aber ganz gewiß schon Euler bekannt.

Wir fassen zusammen: sind n und e gegeben, so wird in der primen Restklassengruppe $(\mathbb{Z}/n\mathbb{Z})^*$ die Bijektion $k \mapsto k^e$ betrachtet, deren Inverse $k \mapsto k^f$ ist und die sich ohne Zusatzinformation (nämlich der Primfaktorzerlegung von n) nicht in vernünftiger Zeit berechnen läßt.

Große Primzahlen

Zum Verschlüsseln benötigen wir große Primzahlen. Da die Primzahlen der Form $2^m - 1$, wie Sie vieleicht wissen, tabelliert sind, empfiehlt es sich, diese nicht zu nehmen. Überhaupt ist es ratsam, Zahlen der Form $a^b \pm c$ mit kleinen a und c nicht zu nehmen, da es für diese ein recht rasches Faktorisierungsprogramm gibt [LLMP].

Es sei also eine natürliche Zahl n gegeben, die getestet werden soll, ob sie prim ist. Wir schreiben $n - 1$ in der Form $2^s t$, wobei t ungerade sein soll und wählen eine zufällige natürliche Zahl $k < n$. Es gilt dann:

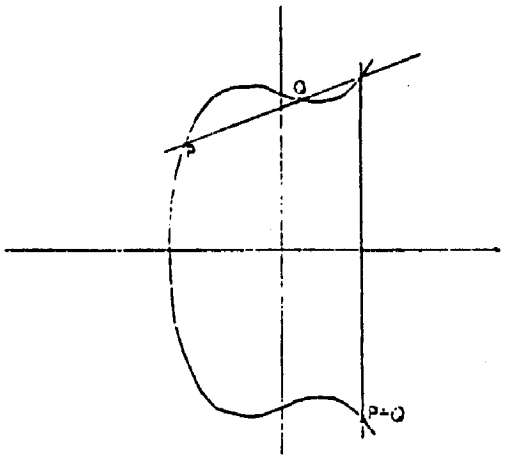
Ist n prim, so ist entweder $k^t \equiv 1 \pmod{n}$
oder es gibt ein j, $0 \leq j < s$, mit $k^{2^j t} \equiv -1 \pmod{n}$.

Wenn diese Bedingung verletzt ist, ist n nicht prim. Es genügt, das für sehr wenige k zu testen. So gibt es z.B. nur ein ungerades n <25 000 000 000, das nicht prim ist und diesen Test für $k = 2, 3, 5$ und 7 besteht [PSW]. Ist die Riemannsche Vermutung richtig und $n > 1$ nicht prim, so gibt es immer ein $k < 2\log^2 n$, das den Test nicht besteht [MI], [BA]. Unter der Annahme der Richtigkeit der Riemannschen Vermutung gelingt es also sehr rasch zu entscheiden, ob eine Zahl prim ist.

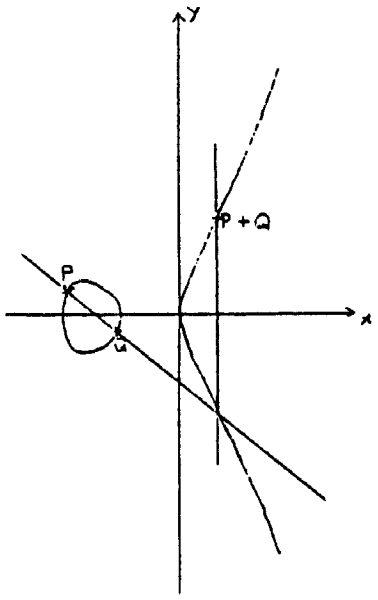
ACHTUNG: Diese Methode ermöglicht es nicht, einen Faktor von n zu finden, wenn n zusammengesetzt ist. Diese Aufgabe ist viel schwieriger und würde, wenn sie gelänge, das RSA-Verfahren wertlos machen.

Faktorisierung von Zahlen

Ich möchte hier einen recht modernen Algorithmus vorstellen, nämlich den, der elliptische Kurven benützt. Es sei K ein Körper und es sei $p(X) \in K[X]$ ein Polynom vom Grad 3 mit Koeffizienten in K. Wir betrachten die Menge $E_p(K) := \{(x, y) \in K \times K | y^2 = p(x)\} \cup \{\infty\}$. Auf dieser Kurve gibt es eine Verknüpfung $+$, die aus ihr eine abelsche Gruppe macht. Sind zwei Punkte $P = (x_1, y_1)$, $Q = (x_2, y_2)$ gegeben, so verbinden wir sie mit einer Geraden $P + t(Q - P)$ $(t \in K)$ und schneiden sie mit der Kurve. Zwei dieser Schnittpunkte kennen wir bereits (nämlich P und Q). Da eine Gleichung dritten Grades, von der zwei Nullstellen in K sind, auch die dritte Lösung in K hat, ergibt sich so ein weiterer Punkt (x_3, y_3). Setzen wir $P + Q = (x_3, -y_3)$, so erhalten wir auf $E_p(K)$ die gesuchte Addition. Eine gewisse Ausnahme von dieser Regel liegt dann vor, wenn $Q = (x_1, -y_1)$ ist. Dann setzen wir $P + Q = \infty$. ∞ spielt dann die Rolle des Nullelementes in der Gruppe. Führen wir die Rechnung analytisch durch, so erhalten wir, daß im wesentlichen $(x_3, y_3) = (f(x_1, y_1, x_2, y_2), g(x_1, y_1, x_2, y_2))$ ist, wobei f und g rationale Funktionen über K sind. Insbesondere gibt es (wieder im wesentlichen) für $m \in \mathbb{Z}$ rationale Funktionen f_m, g_m, sodaß für jeden Punkt $P = (x, y)$ auf der Kurve $mP = (f_m(x, y), g_m(x, y))$ gilt. Wir nennen diese Kurven $E_p(K)$ *elliptische Kurven.*



Die elliptische Kurve $y^2 = x^3 - 3x + 18$ über $\mathbb{R}$.



Die elliptische Kurve $y^2 = x^3 + 3x^2 + 2x$ über $\mathbb{R}$.

Wir könnten nun versucht sein, allgemeiner einen Ring mit Nullteiler (etwa $\mathbb{Z}/n\mathbb{Z}$ für zusammengesetztes n) zu Grunde zu legen, von der geometrischen Konstruktion von $P+Q$ abzusehen und die Addition wie oben durch $P+Q = (f(x_1, y_1, x_2, y_2), g(x_1, x_2, y_1 \cdot y_2))$ zu definieren. Dann könnten aber im Nenner der rationalen Funktionen Nullteiler (das sind Faktoren von n) auftreten, und bei der Berechnung von $f(x_1, x_2, y_1, y_2)$ bzw. $g(x_1, x_2, y_1, y_2)$ erleiden wir Schiffbruch. Insbesondere gilt das für die Berechnung von $f_m(x, y)$ und $g_m(x, y)$. Wir erhalten auf diese Weise keine Gruppe mehr.

Genau darauf beruht nun dieses Verfahren: gegeben sei ein n, das faktorisiert werden soll. Wir wählen eine zufällige Zahl a, die wir mod n betrachten und einen Punkt $P = (x, y) \in \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. Dieser soll auf der Kurve $y^2 = x^3 + ax + b$ liegen. Dadurch ist $b \in \mathbb{Z}/n\mathbb{Z}$ bestimmt. Wir wählen jetzt ein $m \in \mathbb{N}$; dieses ist Produkt von Potenzen der ersten r Primzahlen und (i.w.) $< \sqrt{n}$, wobei die Exponenten und r in einer gewissen optimalen Weise gewählt werden, auf die ich hier nicht eingehen will. Dann berechnen wir mP mit Hilfe der Formeln $(f_m(x, y), g_m(x, y))$. Geht die Berechnung gut, haben wir Pech gehabt und starten mit einem neuen a und einem neuen P. Geht aber die Berechnung schief, weil im Nenner von $f_m(x, y), g_m(x, y)$ ein Nullteiler auftritt, so haben wir einen Faktor von n gefunden. Dieses Verfahren arbeitet in $e^{(1+c_n)\sqrt{\log n \log\log n}}$ Schritten, wobei c_n eine Folge ist, die gegen 0 strebt. Für genauere Informationen siehe [KO].

Es gelingt neuerdings, sehr große Zahlen zu faktorisieren. Wir diskutieren dazu das obige Beispiel aus dem Scientific American. Damals (1977) ergab eine grobe Abschätzung, daß es etwa 40 000 000 000 000 000 Jahre dauern würde, um n zu faktorisieren, also den Text zu entschlüsseln. Der Fortschritt hat aber 1994 zu einer neuerlichen Abschätzung der Rechenzeit geführt. Es ergab sich für sie 4 000 bis 6 000 Jahre. Daraufhin begannen drei Amerikaner und ein Brite ([AGLL]) die größte Kalkulation in der Geschichte der Menschheit. Via Internet wurden mehrere tausend Besitzer von PCs gebeten, sich zu beteiligen. Mit deren Hilfe (es haben 600 mitgemacht) und einiger sehr schneller Rechenanlagen ist es nach einem halben Jahr Rechenzeit gelungen, n zu faktorisieren. Es ist $n = p \cdot q$, wobei

$p =$ 3490 5295 1084 7650 9491 4784 9619 9038 9813
3417 7646 3849 3387 8439 9082 0577 und

q = 3 2769 1329 9326 6709 5499 6198 8190 8344
6141 3177 6429 6799 2942 5397 9828 8533.

Die verschlüsselte Botschaft konnte nun leicht ermittelt werden und lautet

THE MAGIC WORDS ARE SQUEAMISH OSSIFRAGE

Die Autoren vermuten, daß mit einem Einsatz von 30 bis 40 Millionen Dollar viele der heute für das RSA-Verfahren verwendeten n faktorisiert werden könnten. Will man also vor der amerikanischen Regierung etwas geheim halten, ist es ratsam, sich vorzusehen und 200-stellige n zu verwenden.

Der Große Fermatsche Satz

Frey [FR] hatte die Idee, elliptische Kurven $y^2 = x(x-a^p)(x-c^p)$ über $\mathbb{Q}$ zu studieren, wobei $p > 3$ eine Primzahl und (a, b, c) eine Lösung der Fermatschen Gleichung $a^p + b^p = c^p$ bezeichnet. Serre [SE] äußerte eine Vermutung, die besagt, daß aus der Richtigkeit einer weiteren Vermutung, die Tanyama-Shimura Vermutung heißt, folgt, daß es die Kurven $y^2 = x(x-a^p)(x-c^p)$ gar nicht geben dürfte, d.h. der Große Fermatsche Satz folgte. Ribet [RI] bewies diese Vermutung, d.h. er bewies: ist die Tanyama-Shimura Vermutung richtig, so gilt der Große Fermatsche Satz. Diese Tanyama-Shimura Vermutung wurde schließlich in einem Spezialfall, der den Großen Satz von Fermat impliziert, in ganz großen Arbeiten von Wiles [WI] und Taylor und Wiles [TW] bewiesen.

LITERATUR:

[AGLL] Atkins, D., Graff, M., Lenstra, A.K., Leyland, P.C.: The magic words are squeamish ossifrage. Preprint.

[BA] Bach, E.: Analytic methods in the analysis and design of number theoretic algorithms. MIT Press, 1985.

[CH] Chen, J.: The lattice points in a circle. Sci. Sinica 12 (1963), 633-649. Acta Math. Sinica (1963), 299-313 (Chinesisch). Übersetzt in Chinese Math. 4 (1963), 322-339.

[CO] Van der Corput, J.G.: Neuere zahlentheoretische Abschätzungen. Math. Ann. 89 (1923), 215-254.

[DH] Diffie, W., Hellman, M.: New Directions in Cryptography. IEEE Trans. Information Theory 22 (1976), 644-654.

[FR] Frey, G.: Links between stable elliptic curves and certain Diophantine equations. Annales Universitatis Saraviensis, Series Mathematicae 1 (1986), 1-40.

[HA] Hardy, G.H.: On the expression of a number as the sum of two squares. Quart. J. Math. 46 (1915), 263-283.

[HU] Hua, L.-K.: The lattice points in a circle. Quart. J. of Math., Oxford Ser., 13 (1942), 18-29.

[HUX] Huxley, M.N.: Exponential sums and lattice points II. Proc. London Math. Soc. 66, No.2 (1993), 279-301.

[IM] Iwaniec, H., Mozzochi, C.J.: On the divisor and circle problems. J. Number Theory 29, No. 1 (1988), 60-93.

[KOB] Koblitz, N.: Number Theory and Cryptography. Preprint.

[KOL] Kolesnik, G.: On the method of exponent pairs. Acta Arith. 45 (1985). 115-143.

[LA1] Landau, E.: Über die Gitterpunkte in einem Kreise (Erste, zweite Mitteilung). Nachr. K. Gesellschaft Wiss. Göttingen, Math.-Phys. Klasse 1915, 148-160, 161-171.

[LA2] Landau, E.: Note on the preceding paper. Proc. Royal Soc. London, Ser. (A), 106 (1924), 487-488.

[LLMP] Lenstra, A.K., Lenstra, H.W. Jr., Manasse, M.S., Pollard, J.M.: The number field sieve. Preprint.

[LRW] Lune, J. van de, Riele, H.J.J. te, Winter, D.T.: On the zeros of the Riemann zeta function in the critical strip IV. Math. Comp. 46 (1986), 667-681.

[LW] Littlewood, J.E., Walfisz, A.: The lattice points of a circle. Proc. Royal Soc. London, Ser. (A), 106 (1924), 478-487.

[MI] Miller, G.L.: Riemann's hypothesis and tests for primality. J. Comp. System Sci. 13 (1976), 300-317.

[NI] Nieland, L.W.: Zum Kreisproblem. Math. Ann. 98 (1928), 717-736.

[NO] Nowak, W.-G.: Lattice points in a circle and divisors in arithmetic progressions. Manuscr. Math. 49 (1984), 195-205.

[OR] Odlytzko, A.M., Riele, H.J.J. te: A disproof of Mertens conjecture. J. Reine u. Angew. Math 357 (1985), 138-160.

[PSW] Pomerance, C.:, Selfridge, J.L., Wagstaff, S.S. Jr.: The pseudoprimes to $25 \cdot 10^9$. Math. Comp. 35 (1980), 1003-1026.

[RI] Ribet, K.A.: On modular representations of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ arising from modular forms. Invent. Math. 100 (1990), 431-476.

[RSA] Rivest, R., Shamir, A., Adleman, L.: A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM 21 (1978), 120-126.

[SE] Serre, J.P.: Sur les répresentations modulaires de degré 2 de $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Duke Math. J. 54 (1987), 179-230.

[SI] Sierpiński, W.: O pewnem zagadnieniu z rachunku funckcyj asymptotycznych. Prace mat.-fiz. 17 (1906), 77-118.

[TI] Titchmarsh, E.C.: The lattice-points in a circle. Proc. London Math. Soc. (2) 38 (1934), 96-115. Corrigendum 555.

[TW] Taylor, R., Wiles, A.: Ring-theoretic properties of certain Hecke-algebras. Ann. of Math. 141, No.3 (1995), 553-572.

[VI] Vinogradov, I.M.: The Method of Trigonometrical Sums in Number Theory. Moscow, Nauka, 1980.

[WA] Walfisz, A.: Über zwei Gitterpunktprobleme. Math. Ann. 95 (1926), 69-83.

[WI] Wiles, A.: Modular elliptic curves and Fermat's Last Theorem. Ann. of Math. 141, No. 3 (1995), 443-551.