Faktorisierung mit elliptischen Kurven

Das RSA-Verfahren beruht auf der Schwierigkeit des Problems, eine große Zahl in ihre Primfaktoren zu zerlegen. Dieses Problem interessierte Mathematiker schon lange vor RSA. So vermutete etwa FERMAT 1650, daß jede Zahl der Form $2^{2^n} + 1$ eine Primzahl sei und zeigte dies auch für $n \leq 4$; 1742 zeigte dann aber EULER, daß

$$2^{32} + 1 = 4\,294\,967\,297 = 641 \times 6\,700\,417$$

eine zusammengesetzte Zahl ist. (Bis heute ist kein $n > 4$ bekannt, für das $2^{2^n} + 1$ eine Primzahl ist, aber es ist auch nicht bekannt, ob es nicht vielleicht doch unendlich viele Primzahlen dieser Form gibt.)

Eine andere berühmte Faktorisierung lange vor Aufkommen der ersten Computer erregte 1903 Aufsehen: Am 31. Oktober dieses Jahres schrieb FRANK NELSON COLE (1861–1926) auf einer Sitzung der American Mathematical Society auf eine der beiden Tafeln die Zahl

$$2^{67} - 1 = 147\,573\,952\,589\,676\,412\,927\,,$$

und auf die andere schrieb er

$$193\,707\,721 \times 761\,838\,257\,287\,.$$

Dieses Produkt rechnete er wortlos aus nach der üblichen Schulmethode zur schriftlichen Multiplikation, und als er dieselbe Zahl erhielt, die auf der anderen Tafel stand, schrieb er ein Gleichheitszeichen zwischen die beiden Zahlen und setzte sich wieder. Das Ergebnis, d.h. die Faktorisierung von M_{67}, findet ein Computeralgebrasystem heute in weniger als einer Sekunde; für die damalige Zeit war sie eine Sensation! COLE gab später zu, daß er drei Jahre lang jeden Sonntag Nachmittag daran gearbeitet hatte, wobei er mit verschiedenen Methoden versuchte möglichst viele Kongruenzen zu finden, die ein Teiler von $2^{67} - 1$ erfüllen muß, Einzelheiten findet man in

F. N. COLE: On the factoring of large numbers, *Bull. Am. Math. Soc.* **10** (1903), 134–137 *oder* `http://www.ams.org/bull/1903-10-03/S0002-9904-1903-01079-9/home.html`

Der Auftritt von COLE schlug selbst außerhalb der Mathematik so hohe Wellen, daß seine Faktorisierung noch fast ein Jahrhundert später

vorkommt in einer New Yorker (off-Broadway) Show von RINNE GROFF mit dem Titel *The five hysterical girls theorem.* Dort bringt sich ein junger Mathematiker um, weil er in einem Beweis von der *Primzahl* $2^{67} - 1$ ausgeht, und die Tochter des Professors die obige Faktorisierung an die Tafel schreibt. Einzelheiten kann man, so man unbedingt möchte, unter `http://www.playscripts.com/play.php3?playid=551` nachlesen. (Die Show verschwand nach zwei Monaten Ende Mai 2000 in der Versenkung; sie wurde seither nur noch zweimal von Amateurgruppen aufgeführt.)

DERRICK NORMAN LEHMER (1867–1938) veröffentlichte ebenfalls 1903 eine Liste der Primzerlegungen alle Zahlen bis 10 017 000; er baute eine Reihe von Maschinen, teils mit Fahrradketten und Zahnrädern, teils auch elektromechanisch, zur Faktorisierung von Zahlen. Mit dem Aufkommen der ersten Computer in der zweiten Hälfte des zwanzigsten Jahrhundert wurden auch diese fast sofort zur Faktorisierung eingesetzt. Benutzt wurden dazu die verschiedensten Algorithmen, und 1987 schlug der niederländische Mathematiker HENDRIK WILLEM LENSTRA auch einen mit elliptischen Kurven vor:

> H.W. LENSTRA JR.: Factoring integers with elliptic curves, *Annals of Mathematics* **126**, 649–673, pdf unter doi:10.2307/1971363

Es gibt kein „bestes“ Faktorisierungsverfahren; für Zahlen verschiedener Größenordnungen haben jeweils andere Verfahren ihre Stärken, und auch Vorwissen über die zu faktorisierende Zahl kann bei der Wahl eines geeigneten Verfahrens helfen.

LENSTRAs Methode ist bis heute das beste Verfahren, um etwa zwanzig- bis sechzigstellige Faktoren großer Zahlen zu finden; der bisherige Rekord ist ein 2013 von R. PROPPER gefundener 83-stelliger Faktor der 285-stelligen Zahl $3^{337} + 1$. (Für kleinere Faktoren gibt es einfachere Methoden; speziell für Faktoren mit bis zu etwa acht Stellen gibt es wohl nichts schnelleres als Probedivisionen durch alle Primzahlen unter dieser Schranke.)

Wie viele Verfahren, die elliptische Kurven verwende, hat auch der Faktorisierungsalgorithmus von LENSTRA einen „klassischen“ Vorgänger; es ist die 1974 von JOHN POLLARD vorgestellte $(p - 1)$-Methode.

(JOHN POLLARD ist ein britischer Mathematiker, der den größten Teil seines Berufslebens bei British Telecom arbeitete, dabei aber über zwanzig mathematische Arbeiten veröffentlichte, größtenteils aus dem Gebiet der algorithmischen Zahlentheorie.)

POLLARDs $(p-1)$-Methode beruht auf dem kleinen Satz von FERMAT: Für einen Primteiler p von N, ein Vielfaches r von $p-1$ und eine zu p teilerfremde natürliche Zahl a ist $a^r \equiv 1 \bmod p$; der ggT von $(a^r - 1) \bmod N$ und N ist also durch p teilbar.

Natürlich ist $p-1$ nicht bekannt, wir können aber hoffen, daß $p-1$ nur durch vergleichsweise kleine Primzahlen teilbar ist. Sei etwa B eine Schranke mit der Eigenschaft, daß $p-1$ durch keine Primzahlpotenz größer B teilbar ist. Dann ist das Produkt r *aller* Primzahlpotenzen q^e, die höchstens gleich B sind, sicherlich ein Vielfaches von $p-1$, wenn auch ein extrem großes, das sich kaum mit realistischem Aufwand berechnen läßt. Für jedes konkrete a kann $a^r \bmod N$ jedoch verhältnismäßig einfach berechnet werden: Man ersetzt einfach a nacheinander für jede Primzahl $q \leq B$ die Zahl a durch $a^{q^e} \bmod N$; wobei q^e die größte q-Potenz kleiner oder gleich B ist.

Insgesamt funktioniert POLLARDs $(p-1)$-Methode zur Faktorisierung einer natürlichen Zahl N also folgendermaßen:

0. Schritt: Wähle eine Schranke B und eine Basis a zwischen 1 und N.

1. Schritt: Erstelle (z.B. nach ERATOSTHENES) eine Liste aller Primzahlen $q \leq B$.

2. Schritt: Berechne für jede dieser Primzahlen q den größten Exponenten e derart, daß auch noch $q^e \leq B$ ist, d.h. $e = [\log B / \log q]$. Ersetze dann den aktuellen Wert von a durch $a^{q^e} \bmod N$.

3. Schritt: Berechne ggT$(a-1, N)$. Falls ein Wert ungleich eins oder N gefunden wird, war das Verfahren erfolgreich, ansonsten nicht.

Es ist klar, daß der Erfolg dieses Verfahrens wesentlich davon abhängt, daß N einen Primteiler p hat mit der Eigenschaft, daß alle Primfaktoren

von $p-1$ relativ klein sind. Ob dies der Fall ist, läßt sich im Voraus nicht sagen; die $(p-1)$-Methode liefert daher gelegentlich ziemlich schnell sogar 20- oder 30-stellige Faktoren, während sie andererseits deutlich kleinere Faktoren oft nicht findet.

Als Beispiel betrachten wir noch einmal $N = 2^{67} - 1$. Wenn wir mit der Basis $a = 17$ und der Schranke $B = 3\,000$ arbeiten, wird a modulo n potenziert zum neuen

$$a = 111\,153\,665\,932\,902\,146\,348 \text{ mit } \operatorname{ggT}(a-1, N) = 193\,707\,721\,.$$

Damit ist (in Sekundenbruchteilen auf einem Standard-PC) eine nichttriviale Faktorisierung gefunden, und ein Primzahltest zeigt, daß sowohl der gefundene Faktor als auch sein Komplement prim sind.

Warum die Methode Erfolg hatte, sehen wir an der Faktorisierung der um eins verminderten Faktoren:

$$193\,707\,720 = 2^3 \cdot 3^3 \cdot 5 \cdot 67 \cdot 2\,677 \quad \text{und}$$

$$761\,838\,257\,286 = 2 \cdot 3^2 \cdot 29 \cdot 67 \cdot 2\,551 \cdot 8\,539\,.$$

Für jede Schranke $B \geq 2\,677$ ist also der erste Faktor ein Teiler des endgültigen $a-1$, aber für $B < 8\,539$ ist der zweite Faktor mit hoher Wahrscheinlichkeit keiner.

Falls $p-1$ nicht nur relativ kleine Primfaktoren hat, führt die $(p-1)$-Methode nicht zum Erfolg. In solchen Fällen kann man aber hoffen, daß vielleicht $p+1$ oder irgendeine andere Zahl in der Nähe von p nur kleine Primfaktoren hat. Wir brauchen daher Varianten der $(p-1)$-Methode, bei denen es nicht auf die Primfaktoren von $p-1$ ankommt, sondern auf die anderer Zahlen in der Nähe von p.

Um solche Varianten zu finden, empfiehlt es sich, zunächst die $(p-1)$-Methode etwas abstrakter unter gruppentheoretischen Gesichtspunkten zu betrachten.

Dort rechnen wir in der primen Restklassengruppe $(\mathbb{Z}/N)^\times$ und damit implizit auch in $(\mathbb{Z}/p)^\times$ für jeden Primteiler p von N – egal ob wir ihn kennen, oder nicht. In $(\mathbb{Z}/p)^\times$ ist für jedes Element a die $(p-1)$-te Potenz gleich dem Einselement; genau dasselbe gilt für jede r-te Potenz,

für die der Exponent r ein Vielfaches von $(p-1)$ ist. Bei der $(p-1)$-Methode wird ein r berechnet, das durch alle Primzahlpotenzen bis zu einer gewissen Schranke teilbar ist; falls in der Primzerlegung von $p-1$ keine Primzahlpotenz oberhalb der Schranke liegt, ist r ein Vielfaches von $p-1$.

Allgemeiner können wir statt in $(\mathbb{Z}/N)^\times$ und $(\mathbb{Z}/p)^\times$ auch in einem anderen Paar von Gruppen rechnen: Wir gehen aus von einer endlichen Gruppe G_N, deren Elemente sich in irgendeiner Weise als r-tupel über $(\mathbb{Z}/N)$ auffassen lassen; außerdem nehmen wir an, daß sich die Gruppenmultiplikation für zwei so dargestellte Elemente auf Grundrechenarten über $\mathbb{Z}/N$ zurückführen läßt. Dann können wir die Elemente von G_N zu Tupeln über $\mathbb{Z}/p$ reduzieren, und die Menge aller so erhaltenen Tupel bildet eine Gruppe G_p. Wieder ist jede Rechnung in G_N implizit auch eine Rechnung in G_p.

Die Elementanzahl von G_p sei $N(p)$.

Wir wählen irgendein Element von G_N und potenzieren es mit demselben Exponenten r, mit dem wir bei der $p-1$-Methode die Zahl a modulo N potenziert haben. Falls r ein Vielfaches von $N(p)$ ist, erhalten wir ein Element $b \in G_N$, dessen Reduktion modulo p das Einselement von G_p ist. Ist daher b_i die i-te Koordinate von b und e_i die von e, so muß die Differenz $b_i - e_i$ durch p teilbar sein, und mit etwas Glück können wir p als ggT von n und $b_i - e_i$ bestimmen.

Bleibt nur noch das Problem, geeignete Gruppen zu finden. Bei der $(p-1)$-Methode ist $G_N = (\mathbb{Z}/N)^\times$ und $N(p) = p-1$.

1982 entwickelte der kanadische Mathematiker HUGH COWIE WILLIAMS eine $(p+1)$-Methode, die darauf beruht, daß es für jede Primzahl p auch einen Körper $\mathbb{F}_{p^2}$ mit p^2 Elementen gibt, so daß die multiplikative Gruppe $\mathbb{F}_{p^2}^\times$ aus $p^2-1 = (p+1)(p-1)$ Elementen besteht. 1987 schließlich kam LENSTRA auf die Idee, als Gruppe eine elliptische Kurve über einem endlichen Körper zu verwenden.

G_p ist also die Gruppe bestehend aus den Punkten einer elliptischen Kurve über $\mathbb{F}_p$. Da p und damit auch der Körper $\mathbb{F}_p$ nicht bekannt sind,

werden die die Punkte repräsentiert durch Paare $(x, y) \in (\mathbb{Z}/N)^2$, die einer vorgegebenen WEIERSTRASS-Gleichung $y^2 = x^3 - ax - b$ genügen, wobei auch a, b als Elemente von $\mathbb{Z}/N$ gegeben sind. Sie müssen so gewählt werden, daß $\Delta = 4a^3 + 27b^2$ teilerfremd zu N ist; dann definiert die Gleichung für jedem Primteiler p von N modulo p eine elliptische Kurve über $\mathbb{F}_p$. G_p ist also die entsprechende Punktmenge in $\mathbb{F}_p^2$ zusammen mit dem Punkt O. Nach einem Satz, den der deutsche Mathematiker HELMUT HASSE (1898–1979) in mehreren Arbeit zwischen 1933 und 1935 bewies, ist

$$p + 1 - 2\sqrt{p} \leq N(p) \leq p + 1 + 2\sqrt{p}\,,$$

und nach einem 1969 von WILLIAM C. WATERHOUSE veröffentlichten Satz gibt es für eine Primzahl $p > 3$ und eine ganze Zahl t vom Betrag kleiner $2\sqrt{p}$ genau dann eine elliptische Kurve E über $\mathbb{F}_p$ mit $p + 1 + t$ Punkten, wenn t nicht durch p teilbar ist. Wenn man mit hinreichend vielen verschiedenen Kurven arbeitet, ist daher die Chance recht groß, daß der Exponent r wenigstens für eine davon ein Vielfaches von $N(p)$ ist.

Betrachten wir als einfaches Beispiel (bei dem naives Abdividieren billiger wäre) die Faktorisierung von $N = 4453$ mit der elliptischen Kurve E mit WEIERSTRASS-Gleichung $y^2 = x^3 + 10x - 2$. Wir rechnen modulo N in der von $P = (1, 3)$ erzeugten zyklischen Untergruppe von E, und da es hier nur ums Prinzip gehen soll, wählen wir keine große Suchschranke, sondern berechnen einfach den Punkt $3P$.

Dazu bestimmen wir zunächst nach der Verdoppelungsformel den Punkt $2P$:

Die Tangentensteigung im Punkt (x, y) ist $m = \frac{3x^2+10}{2y}$, in $(1, 3)$ also $13/6 \bmod p$. Da wir p nicht kennen, versuchen wir dies modulo N zu berechnen, d.h. wir wenden den erweiterten EUKLIDischen Algorithmus an auf $N = 4453$ und 6:

$$4453 : 6 = 742 \quad \text{Rest } 1 \Longrightarrow 1 = 4453 - 6 \cdot 742\,.$$

Sechs hat also modulo N den Kehrwert $-742 \equiv 3711 \bmod N$, und damit ist $m = 13 \cdot 3711 \equiv 3713 \bmod N$ und $2P = (4332, 3230)$.

$3P$ wird als $2P + P$ berechnet. Die Gerade durch P und $2P$ hat die Steigung

$$m = \frac{3230 - 3}{4332 - 1} \bmod p = \frac{3227}{4331} \bmod p\,.$$

Wieder wenden wir den erweiterten Euklidischen Algorithmus an auf den Nenner 4331 und $N = 4453$:

$$4453 : 4331 = 1 \text{ Rest } 122 \Longrightarrow 122 = 4453 - 4331$$

$$4331 : 122 = 35 \text{ Rest } 61 \Longrightarrow 61 = 4431 - 35 \cdot 122 = 36 \cdot 4331 - 235 \cdot 4453$$

$$122 : 61 = 2\,.$$

Da die letzte Division ohne Rest aufgeht, ist ggT$(4331, N) = 61$, d.h. 4331 ist nicht teilerfremd zu N und hat somit kein Inverses modulo N.

Der ggT 61 ist eine Primzahl; betrachten wir die Situation modulo $p = 61$. Wir hatten die Koordinaten von $2P$ modulo N berechnet als $(4332, 3230)$; nachdem wir nun den Primteiler 61 von N gefunden haben, können wir sie modulo 61 reduzieren und erhalten $2P = (1, 58)$ über $\mathbb{F}_{61}$. Die Punkte $P = (1, 3)$ und $2P = (1, 58)$ haben also dieselbe x-Koordinate, aber verschiedene y-Koordinaten. (Natürlich ist $58 = -3$ in $\mathbb{F}_{61}$.) Somit ist auf der über $\mathbb{F}_{61}$ betrachteten elliptischen Kurve mit WEIERSTRASS-Gleichung $y^2 = x^3 + 10x - 2$ die Summe von P und $2P$ gleich O, d.h. $3P = O$.

Der Kofaktor $N/p = 4453/61 = 73$ ist auch eine Primzahl; wenn wir den Punkt P auf der elliptischen Kurve über F_{73} mit WEIERSTRASS-Gleichung $y^2 = x^3 + 10 - 2$ betrachten, können wir die Koordinaten von $2P$ durch ihre Restklassen modulo 73 ersetzen und erhalten $2P = (18, 25)$. Auf dieser Kurve ist $3P$ also von O verschieden, denn P und $2P$ haben verschiedene x-Koordinaten.

Der EUKLIDische Algorithmus lieferte beim Versuch, die Steigung der Geraden durch P und $2P$ zu berechnen, einen von eins verschiedenen ggT, weil die Steigung auf der Kurve über $\mathbb{F}_{73}$ ein Wert aus diesem Körper ist, während die Gerade durch P und $2P$ für die Kurve über $\mathbb{F}_{61}$ parallel zur y-Achse verläuft. Dies führte dazu, daß wir den Faktor 61 von N finden konnten.

Allgemeine funktioniert LENSTRAs Methode wie folgt:

Gegeben sei eine natürliche Zahl N; gesucht ist ein Faktor p von N.

Man wähle zunächst zufällig einige WEIERSTRASS-Gleichungen

$$y^2 = x^3 + a_i x + b_i \bmod N \quad \text{mit} \quad \text{ggT}(N, 4a_i^3 + 27b_i^2) = 1\,,$$

und für jede davon ein Paar $(x_i, y_i) \in \left(\mathbb{Z}/N\right)^2$, das diese Gleichung erfüllt. Meist rechnet man mit etwa zehn bis zwanzig WEIERSTRASS-Gleichungen.

Als nächstes wird, wie bei der $p-1$-Methode, eine Suchschranke B festgelegt, und nacheinander wird für jede Primzahl $p < B$ jeder der Punkte P_i auf „seiner“ Kurve ersetzt durch $p^e P_i$, wobei p^e die größte p-Potenz ist, die noch kleiner als B ist.

Das Verfahren beruht auf der Hoffnung, daß bei mindestens einer Gleichung und mindestens einer Primzahl p der Punkt $p^e P_i$ nicht berechenbar ist, da er modulo p gleich O wäre, modulo eines anderen Primteilers q von N aber nicht. Bei der Berechnung der Steigung der Geraden für eine der Zwischensummen stellt sich dann heraus, daß der Nenner nicht teilerfremd zu N ist, und wir erhalten einen Faktor. Der Algorithmus ist also genau dann erfolgreich, wenn es *nicht* gelingt, das angestrebte Vielfache zu berechnen.

Man beachte, daß der gefundene Faktor nicht unbedingt eine Primzahl sein muß: Es könnte schließlich sein, daß ein zu berechnendes Vielfaches modulo mehrerer Primteiler von N gleich O ist, aber modulo mindestens eines weiteren Primteilers nicht.