Primzahltests mit elliptischen Kurven

Die Suche nach Primzahlen beschäftigte schon die klassischen griechischen Mathematiker und geht bis heute unvermindert weiter. Die im Augenblick größte bekannt Primzahl wurde im Dezember 2018 gefunden und ist $2^{82\,589\,933} - 1$, eine Zahl mit 24 862 048 Dezimalstellen. Seit Aufkommen der Kryptographie mit öffentlichen Schlüsseln braucht man auch dafür Primzahlen; deren Stellenzahl sollte zwar nicht in die Millionen gehen, aber doch in die Hunderte. Speziell für RSA müssen diese Primzahlen zufällig gewählt werden; es ist daher wichtig, für eine Zufallszahl schnell entscheiden zu können, ob sie prim ist oder nicht.

Die größte bekannte Primzahl war in den letzten fünfzig Jahren außer zwischen 1985 und 1992 stets eine sogenannte MERSENNE-Zahl, d.h. von der Form $2^p - 1$ mit einer Primzahl p. Für solche Zahlen gibt es spezielle sehr effiziente Testverfahren, die allerdings auch nur für diese Zahlen geeignet sind. Für zufällig gewählte Zahlen der Größenordnung, die man für RSA und für Verfahren auf der Grundlage diskreter Logarithmen benötigt, ist derzeit ein Test mit elliptischen Kurven das beste bekannte Verfahren.

Natürlich hat auch dieses Verfahren klassische Vorgänger, so daß wir uns zunächst mit diesen beschäftigen wollen. Ausgangspunkt dafür ist der kleine Satz von FERMAT, wonach für eine Primzahl p und eine nicht durch p teilbare Zahl a die Kongruenz $a^{p-1} \equiv 1 \bmod p$ gilt. Im Umkehrschluß folgt sofort

Lemma: Wenn es zu einer natürlichen Zahl p eine dazu teilerfremde Zahl a gibt, für die $a^{p-1} \not\equiv 1 \bmod p$ ist, kann p keine Primzahl sein. ∎

Die Umkehrung dieses Lemmas gilt leider nicht: Es gibt, wie man inzwischen weiß, unendlich viele zusammengesetzte Zahlen n, für die trotzdem $a^{n-1} \equiv 1 \bmod n$ für jedes zu n teilerfremde a gilt; das sind die sogenannten CARMICHAEL-Zahlen. Trotzdem wird es für große Zahlen zunehmend unwahrscheinlich, daß eine Zahl p für auch nur ein zufällig gewähltes a den obigen Test besteht, ohne Primzahl zu sein.

SU HEE KIM, CARL POMERANCE: The probability that a Random Probable Prime is Composite, *Math. Comp.* **53** (1989), 721–741

geben folgende obere Schranke für die Fehlerwahrscheinlichkeit ε:

$p \approx 10^{60}$	10^{70}	10^{80}	10^{90}	10^{100}
$\varepsilon \leq 7{,}16 \cdot 10^{-2}$	$2{,}87 \cdot 10^{-3}$	$8{,}46 \cdot 10^{-5}$	$1{,}70 \cdot 10^{-6}$	$2{,}77 \cdot 10^{-8}$
$p \approx 10^{120}$	10^{140}	10^{160}	10^{180}	10^{200}
$\varepsilon \leq 5{,}28 \cdot 10^{-12}$	$1{,}08 \cdot 10^{-15}$	$1{,}81 \cdot 10^{-19}$	$2{,}76 \cdot 10^{-23}$	$3{,}85 \cdot 10^{-27}$
$p \approx 10^{300}$	10^{400}	10^{500}	10^{600}	10^{700}
$\varepsilon \leq 5{,}8 \cdot 10^{-29}$	$5{,}7 \cdot 10^{-42}$	$2{,}3 \cdot 10^{-55}$	$1{,}7 \cdot 10^{-68}$	$1{,}8 \cdot 10^{-82}$
$p \approx 10^{800}$	10^{900}	10^{1000}	10^{2000}	10^{3000}
$\varepsilon \leq 5{,}4 \cdot 10^{-96}$	$1{,}0 \cdot 10^{-109}$	$1{,}2 \cdot 10^{-123}$	$8{,}6 \cdot 10^{-262}$	$3{,}8 \cdot 10^{-397}$

(Sie geben natürlich auch eine allgemeine Formel an, jedoch ist diese zu grausam zum Abtippen.)

Um zu testen, ob eine vorgegebene Zahl p prim ist, empfiehlt es sich daher immer, zunächst zu testen, ob für ein zufälliges a die Kongruenz $a^{p-1} \equiv 1 \bmod p$ gilt; falls ja, ist damit nichts bewiesen, aber falls das Ergebnis ungleich eins ist, wissen wir sicher, daß p nicht prim sein kann.

Der französische Mathematiker FRANÇOIS EDOUARD ANATOLE LUCAS (1842–1891) fand 1876 eine Umkehr des FERMAT-Tests:

Lemma: Falls es zu einer natürlichen Zahl p eine dazu teilerfremde Zahl a gibt derart, daß $a^{p-1} \equiv 1 \bmod p$ ist, aber $a^{(p-1)/q} \not\equiv 1 \bmod p$ für jeden Primteiler q von $p-1$, ist p eine Primzahl.

Beweis: n sei die Ordnung von a modulo p, also die kleinste natürliche Zahl, für die $a^n \equiv 1 \bmod p$ ist. Da $a^{p-1} \equiv 1 \bmod p$ ist, muß n ein Teiler von $p-1$ sein. Falls n ein echter Teiler von $p-1$ ist, gibt es mindestens einen Primteiler q von $p-1$ derart, daß n auch ein Teiler von $(p-1)/q$ ist, denn diese Zahlen sind die maximalen echten Teiler von $p-1$. Daher muß dann mindestens eine der Potenzen $a^{(p-1)/q}$ kongruent eins modulo p sein, was nach Voraussetzung nicht der Fall ist. Somit ist $n = p-1$. Damit sind die Zahlen $a^i \bmod p$ für $i = 1, \ldots, p-1$ allesamt verschieden, es sind also die sämtlichen natürlichen Zahlen

von eins bis $p-1$. Da $a^i \cdot a^{(p-1)-i} = a^{p-1} \equiv 1 \bmod p$ ist, hat also jede natürliche Zahl $r < p$ ein multiplikatives Inverses modulo p und ist somit teilerfremd zu p. Somit muß p eine Primzahl sein.

■

Für kleine Zahlen p ist dieses Kriterium leicht anzuwenden; für große p ist es aber im Allgemeinen nicht mit vertretbarem Aufwand möglich, die Primteiler von $p-1$ zu finden. Der britische Mathematiker und Physiker HENRY CABOURN POCKLINGTON (1870–1952) fand 1914 eine Version, für die man nur noch einen Teil dieser Primteiler kennen muß:

Lemma: p sei eine natürliche Zahl, und $p-1 = km$ mit $m \geq \sqrt{p}$ und ggT$(m,k) = 1$. Die Primzerlegung von m sei $m = p_1^{e_1} \cdots p_r^{e_r}$. Falls es zu jeder der Primzahlen p_i eine zu p teilerfremde Zahl a_i gibt mit $a_i^{p-1} \equiv 1 \bmod p$ und ggT$(a_i^{(p-1)/p_i} - 1, p) = 1$, ist p eine Primzahl.

Beweis: q sei der kleinste Primteiler von p. Wir müssen zeigen, daß $q = p$ ist.

Da alle a_i teilerfremd zu p sind, sind sie erst recht teilerfremd zu q; wir können also von der Ordnung n_i von a_i reden. Nach FERMAT ist $a_i^{q-1} \equiv 1 \bmod q$, daher ist n_i ein Teiler von $q-1$.

Wäre n_i auch ein Teiler von $(p-1)/p_i$, so wäre $a_i^{(p-1)/p_i} \equiv 1 \bmod q$, so daß q ein gemeinsamer Teiler von $a_i^{(p-1)/p_i} - 1$ und p wäre, was nach Voraussetzung ausgeschlossen ist. Somit kann n_i kein Teiler von $(p-1)/p_i$ sein. Andererseits ist aber $a^{p-1} \equiv 1 \bmod p$ und damit erst recht $a^{p-1} \equiv 1 \bmod q$, so daß n_i ein Teiler von $p-1$ sein muß.

Jeder Teiler n_i von $p-1$ ist von der Form $n_i = p_1^{f_1} \cdots p_r^{f_r} k'$ mit $0 \leq f_j \leq e_j$ und einem Teiler k' von k, der, genau wie k, teilerfremd zu m und somit insbesondere nicht durch p_i teilbar ist. Da n_i kein Teiler von $(p-1)/p_i$ ist, muß also $f_i = e_i$ sein, d.h. n_i und damit erst recht $q-1$ ist durch $p_i^{e_i}$ teilbar. Dies gilt für alle i, also ist $q-1$ auch durch das Produkt $m = p_1^{e_1} \cdots p_r^{e_r}$ teilbar. Nach Voraussetzung ist $m \geq \sqrt{p}$, d.h. $q > q-1 \geq m \geq \sqrt{p}$. Der kleinste Primteiler von p ist also größer als $\sqrt{p}$, was nur möglich ist, wenn $p = q$ eine Primzahl ist,

■

Für den Beweis dieses Satzes war es wichtig, daß wir die Elementanzahl der multiplikativen Gruppe modulo einer Primzahl kannten, daß wir also wußten, daß $\mathbb{F}_q^\times$ aus $q-1$ Elementen besteht. Für eine beliebige elliptische Kurve kennen wir deren Elementanzahl im Allgemeinen nicht. Andererseits war im Beweis ja nur wichtig, daß q echt größer als diese Elementanzahl ist, und eine untere Schranke für die Anzahl der Punkte auf einer elliptischen Kurve gibt uns der bereits im Zusammenhang mit der Faktorisierung zitierte Satz von HASSE: Für eine elliptische Kurve E über einem Körper $\mathbb{F}_p$ ist

$$p+1-2\sqrt{p} \leq \#E(\mathbb{F}_p) \leq p+1+2\sqrt{p}\,.$$

Der Beweis dieses Satzes verwendet Methoden der analytischen Zahlentheorie, sogenannte DIRICHLET-Reihen; in der Tat bewies ihn HASSE über eine Aussage, die man als ein Analogon der RIEMANNschen Vermutung für den Fall elliptischer Kurven auffassen kann. Für diese Methoden fehlt uns leider die Zeit, so daß wir den Satz ohne Beweis akzeptieren müssen.

Immerhin können wir uns, völlig unexakt und rein heuristisch, überlegen, warum die Elementanzahl ungefähr in dieser Größenordnung liegen sollte: Wir betrachten für eine WEIERSTRASS-Gleichung

$$y^2 = x^3 + ax + b$$

für jedes $x \in \mathbb{F}_p$ den Wert $x^3 + ax + b \in \mathbb{F}_p$. Wie wir bereits wissen, sind in $\mathbb{F}_p$ unter den p Elementen $(p+1)/2$ Quadrate. Nun wissen wir natürlich nicht, wie viele Werte $x^3 + ax + b$ überhaupt annimmt und ob darunter die Quadrate oder die Nichtquadrate überwiegen, aber als erste Hypothese können wir doch davon ausgehen, daß etwa die Hälfte der Werte Quadrate sind und die andere Hälfte nicht. Zu den Quadraten gibt es dann Werte y, für die $y^2 = x^3 + ax + b$ ist, wobei wir für die meisten x zwei solche Werte bekommen. Damit sollte es ungefähr $2 \cdot \frac{p}{2} = p$ affine Punkte geben, zusammen mit O also $p+1$ Punkte. Wie der Satz von HASSE zeigt, ist das ungefähr richtig, wobei HASSE sogar noch genaue Fehlerschranken angibt.

Bei der Übertragung des Primzahltests von POCKLINGTON auf elliptische Kurven haben wir das Problem, daß wir mit einer Zahl p arbeiten,

von der wir nicht wissen, ob sie prim ist. Wir können also nicht von einer elliptischen Kurve über $\mathbb{F}_p$ sprechen. Wie bei der Faktorisierung gehen wir stattdessen aus von einer WEIERSTRASS-Gleichung modulo p und können versuchen, auch auf deren Punkte die Additions- und die Verdoppelungsformel anwenden, wobei es allerdings passieren kann, daß wir eine notwendige Division nicht durchführen können. In diesem Fall haben wir einen echten Faktor von p gefunden und wissen daher, daß p nicht prim ist. In diesem Sinne ist es zu verstehen, wenn im folgenden Satz von den Vielfachen eines Punktes die Rede ist, obwohl dessen Koordinaten zumindest *a priori* nicht in einem Körper liegen müssen.

Satz: p sei eine natürliche Zahl und $y^2 = x^3 + ax + b$ sei eine WEIERSTRASS-Gleichung modulo p. Weiter seien $P_1 \dots P_r \in \mathbb{Z}/p \times \mathbb{Z}/p$ Punkte, deren Koordinaten der WEIERSTRASS-Gleichung genügen, und $p_1, \dots, p_r$ seien verschiedene Primzahlen derart, daß $p_i P_i = O$ für alle i und

$$\prod_{i=1}^{r} p_i > \left(\sqrt[4]{p} + 1\right)^2 .$$

Dann ist p eine Primzahl.

Beweis: Wieder sei q der kleinste Primfaktor von p, und $p = q^e \cdot k$ mit einem zu q teilerfremden Kofaktor k. Jedes Paar $P_i = (x_i, y_i)$ definiert einen Punkt $Q_i = (x_i \bmod q, y_i \bmod q)$ auf der durch die WEIERSTRASS-Gleichung definierten elliptischen Kurve E über $\mathbb{F}_q$. Da die Q_i affine Punkte sind, also ungleich O, und die p_i Primzahlen, hat der Punkt Q_i die Ordnung p_i auf E. Somit hat E eine Untergruppe der Ordnung p_i; die Elementenzahl von E ist also ein Vielfaches von p_i. Da die p_i verschiedene Primzahlen sind, ist $\#E$ sogar durch das Produkt der p_i teilbar, das nach Voraussetzung größer ist als $\left(\sqrt[4]{p}+1\right)^2$. Zusammen mit dem Satz von HASSE erhalten wir die Ungleichung

$$\left(\sqrt[4]{q} + 1\right)^2 < \prod_{i=1}^{k} p_i \le \#E < q + 1 + 2\sqrt{q} = (\sqrt{q} + 1)^2 .$$

Somit ist $\sqrt[4]{p} + 1 < \sqrt{q} + 1$, d.h. $\sqrt{p} < q$. Der kleinste Primteiler von p

ist also größer als $\sqrt{p}$, was nur im Fall $q = p$ möglich ist. Damit ist p als Primzahl erkannt. ∎

Für die Anwendung dieses Satzes stellt sich die Frage, wie man geeignete Punkte P_i von Primzahlordnung findet. Meist startet man einfach mit irgendwelchen Punkten und berechnet deren Ordnungen. Falls die Ordnung eines Punktes P keine Primzahl ist, hat sie Primteiler p, für die man sie als $n = pm$ schreiben kann, und der Punkt mP hat die Ordnung p.

Bleibt die Frage, wie man die Ordnung eines Punktes P bestimmt. Die p_i sind zwar deutlich kleiner als p, aber doch zu groß, als daß man die Ordnung einfach durch sukzessive Berechnung aller Potenzen bestimmen könnte.

Wenn wir die Ordnung eines Elements von $\mathbb{F}_p^\times$ bestimmen wollen, wissen wir nach dem kleinen Satz von FERMAT, daß sie ein Teiler von $p - 1$ ist, so daß es reicht, für diese Teiler das entsprechende Vielfache zu berechnen.

Für eine elliptische Kurve über $\mathbb{F}_p$ haben wir als allgemeine Aussage nur den Satz von HASSE, der uns eine Ungleichung gibt, die von rund $4\sqrt{p}$ Zahlen erfüllt wird. Für eine konkrete elliptische Kurve gibt es aber einen Algorithmus von SCHOOF, der (über die Ideen, die zum Beweis des Satzes von HASSE führten) die genaue Elementanzahl effizient berechnet, und sobald man sie kennt, kann man sich wieder auf deren Teiler beschränken.