3 Primzahltests

Eine Frage ist zur Durchführbarkeit des RSA-Verfahrens noch zu klären: Gibt es überhaupt Möglichkeiten, die für die Schlüsselerzeugung nötigen Primzahlen zu finden? Die Antwort wird lauten: Ja, das ist effizient möglich. Man startet mit einer zufälligen Zahl der benötigten Bitlänge und prüft, ob sie eine Primzahl ist. Falls nein, prüft man die nächstgrößere Zahl usw., bis man eine Primzahl gefunden hat.

Nötig sind also Verfahren, die effizient entscheiden, ob eine natürliche Zahl prim ist – sogenannte Primzahltests.

Hierbei tritt ein Phänomen auf, das man auch von anderen mathematischen Problemen (z. B. lineare Optimierung, Bestimmung von Polynomnullstellen) kennt:

- Es gibt einen Algorithmus, der mit polynomialem Aufwand auskommt.
- Es gibt einen „Standard-Algorithmus“ (in den Beispielen: Simplex-Methode, Newton-Verfahren), der in den „meisten“ Fällen deutlich effizienter ist, im schlechtesten Fall („worst case“) allerdings nicht mit polynomialem Aufwand auskommt. Dieser wird in der Praxis bevorzugt.

Bei den Primzahltests ist der neu entdeckte AKS-Algorithmus polynomial, kann aber mit dem etablierten Rabin-Algorithmus nicht mithalten, der sehr effizient ist, aber im schlechtesten Fall nicht einmal das richtige Ergebnis liefert.

Da alle genannten Primzahltests einen beachtlichen Overhead haben, wird man in der praktischen Anwendung stets zuvor die Teilbarkeit durch „kleine“ Primzahlen prüfen, etwa durch Primzahlen $< 10^6$, je nach verfügbarem Speicherplatz: Man legt nämlich dazu eine Liste L dieser Primzahlen an.

Benötigt man nun eine zufällig gewählte Primzahl einer bestimmten Größe, so wählt man zufällig eine Zahl r in diesem Größenbereich – sollte r gerade sein, erhöht man um 1. Dann siebt man nach dem Eratosthenes-Verfahren das Intervall $[r, r + s]$ nach den Vielfachen der Primzahlen in L aus; damit die Chance, noch etwas übrig zu behalten, hinreichend groß ist, sollte man s als deutlich größer als die größte Zahl in der Liste L wählen. Die Zahlen, die übrig bleiben, werden der Reihe nach dem gewünschten Primzahltest unterzogen, bis man eine gefunden hat, die den Test besteht. In den allermeisten Fällen wird das bereits die erste sein.

3.1 Der Pseudoprimzahltest

Woran erkennt man, dass eine Zahl prim ist? Der „naive“ Ansatz, Probedivisionen durch alle Zahlen $\leq \sqrt{n}$ durchzuführen – perfektioniert im Sieb des ERATOSTHENES –, ist nicht effizient, da $\sqrt{n} = \exp(\frac{1}{2}\log n)$ immer noch exponentiell mit der Stellenzahl $\log n$ von n wächst.

Einen Ansatz, Primzahlen ohne Probedivision zu erkennen, bietet der Satz von FERMAT: Ist n prim, so $a^{n-1} \equiv 1 \pmod{n}$ für alle $a = 1, \ldots, n-1$. Umgekehrt sagt man, dass n den **Pseudoprimzahltest zur Basis** a besteht, wenn $a^{n-1} \equiv 1 \pmod{n}$. Eine Primzahl besteht diesen Test also zu jeder Basis $a = 1, \ldots, n-1$. Die Kongruenz $2^{14} \equiv 4 \pmod{15}$ beweist, dass 15 nicht prim ist. Allerdings ist $2^{340} \equiv 1 \pmod{341}$, obwohl $341 = 11 \cdot 31$; aber immerhin ist $3^{340} \equiv 56 \pmod{341}$, so dass 341 durch den Pseudoprimzahltest zur Basis 3 fällt.

Trotzdem reicht dieses Kriterium nicht, um umgekehrt die Primzahleigenschaft zu beweisen. Man nennt n CARMICHAEL**-Zahl**, wenn n den Pseudoprimzahltest zu jeder zu n teilerfremden Basis a besteht, aber nicht prim ist.

Den Pseudoprimzahltest kann man auch dadurch ausdrücken, dass die Ordnung von a in $\mathbb{M}_n$ ein Teiler von $n-1$ ist. Also ist n genau dann CARMICHAEL-Zahl oder prim, wenn $\lambda(n) \mid n-1$ für die CARMICHAEL-Funktion λ. Es gibt zu viele CARMICHAEL-Zahlen, als dass der Pseudoprimzahltest ruhigen Gewissens als für die Praxis ausreichend betrachtet werden könnte. Insbesondere haben ALFORD, GRANVILLE und POMERANCE 1992 bewiesen, dass es unendlich viele CARMICHAEL-Zahlen gibt.

Die kleinste CARMICHAEL-Zahl ist $561 = 3 \cdot 11 \cdot 17$; das folgt leicht aus dem nächsten Satz.

Satz 1 *Eine natürliche Zahl n ist genau dann* CARMICHAEL*-Zahl, wenn sie zuammengesetzt und quadratfrei ist, und $p-1 \mid n-1$ für jeden Primteiler p von n. Eine ungerade* CARMICHAEL*-Zahl hat mindestens 3 Primfaktoren.*

Beweis. „$\Longrightarrow$“: Wäre $p^2 | n$, so enthielte $\mathbb{M}_n$ eine zu $\mathbb{M}_{p^e}$ mit geeignetem $e \geq 2$ isomorphe Untergruppe, also nach Satz 2 in Anhang A.3 auch eine zyklische Gruppe der Ordnung p; also wäre $p \mid n-1$, Widerspruch. Da aber $\mathbb{M}_n$ eine zyklische Gruppe der Ordnung $p-1$ enthält, gibt es ein Element a der Ordnung $p-1$, und $a^{n-1} \equiv 1 \pmod{n}$, also $p-1 \mid n-1$.

„$\Longleftarrow$“: Da n quadratfrei ist, ist nach dem chinesischen Restsatz die multiplikative Gruppe $\mathbb{M}_n$ das direkte Produkt der zyklischen Gruppen $\mathbb{F}_p^\times$, wobei p die Primteiler von n durchläuft. Da stets $p-1 \mid n-1$, hat jedes Element von $\mathbb{M}_n$ eine Ordnung, die $n-1$ teilt.

Zusatz: Angenommen, $n = pq$ mit zwei Primzahlen p und q, etwa $p < q$. Dann ist $q-1 \mid n-1 = pq-1$, also $p-1 \equiv pq-1 \equiv 0 \pmod{q-1}$, Widerspruch zu $p < q$. $\diamond$

3.2 Der strenge Pseudoprimzahltest

Man kann den Pseudoprimzahltest verschärfen, indem man weitere Kennzeichen für Primzahlen auswertet. Sei n zunächst ungerade, zusammengesetzt und keine Primpotenz. Dann gibt es außer ± 1 auch nichttriviale Quadratwurzeln aus 1 in $\mathbb{Z}/n\mathbb{Z}$; findet man eine solche, so hat man nachgewiesen, dass n zusammengesetzt ist. Aber wie soll man nichttriviale Einheitsquadratwurzeln finden, wenn man die Primzerlegung von n nicht kennt? Dazu wird, der Idee aus 2.2 folgend, $n-1$ aufgespalten in $n-1 = 2^s \cdot r$ mit ungeradem r.

Sei $a \in \mathbb{M}_n$. Falls n den Pseudoprimzahltest zur Basis a nicht besteht, ist es als zusammengesetzt erkannt. Andernfalls hat a in der multiplikativen Gruppe $\mathbb{M}_n$ eine Ordnung $\mathrm{Ord}(a) \mid n-1$. In der Folge

$$a^r \bmod n, \quad a^{2r} \bmod n, \quad \ldots, \quad a^{2^s r} \bmod n = 1$$

könnte bereits $a^r \equiv 1 \pmod{n}$ sein. Dann wird a verworfen, ohne dass eine Entscheidung über n getroffen wird. Andernfalls tritt die 1 erstmals an späterer Stelle auf; das davor stehende Element muß dann Einheitswurzel $\neq 1$ sein. Es kann -1 sein; auch dann wird a ohne Entscheidung verworfen. Andernfalls ist eine nichttriviale Einheitswurzel gefunden und n als zusammengesetzt erkannt. Ist dagegen n prim, so gibt es in dieser Situation stets ein k mit $0 \le k < s$, so dass

$$a^{2^k r} \equiv -1 \pmod{n}.$$

Sei nun n eine beliebige positive ganze Zahl, und $n-1$ habe die Zweierordnung s und den ungeraden Teil r. Dann sagt man, n bestehe den **strengen Pseudoprimzahltest zur Basis** a [nach Selfridge ca. 1975], wenn

$$a^r \equiv 1 \pmod{n} \quad \text{oder} \quad a^{2^k r} \equiv -1 \pmod{n} \quad \text{für ein } k = 0, \ldots, s-1.$$

Insbesondere gilt dann $a^{n-1} \equiv 1 \pmod{n}$.

Wir haben also die gleiche Situation wie in Abschnitt 2.3 mit $u = n-1$. Die dortige Menge

$$B_u = \bigcup_{t=0}^{s} \{w \in \mathbb{M}_n \mid w^{r \cdot 2^t} = 1, w^{r \cdot 2^{t-1}} = -1 \text{ (falls } t > 0)\}$$

ist jetzt genau die Menge der Basen, für die n den strengen Pseudoprimzahltest besteht, also die Eigenschaft $(\mathrm{E}_{n,u})$ hat. Diese Basen werden auch **Primzeugen** für n genannt.

Jede Primzahl besteht den strengen Pseudoprimzahltest zu jeder Basis, die kein Vielfaches dieser Primzahl ist. Die Carmichael-Zahl $n = 561$ fällt schon bei $a = 2$ durch: Es ist $n - 1 = 560 = 16 \cdot 35$,

$$2^{35} \equiv 263 \pmod{561}, \qquad 2^{70} \equiv 166 \pmod{561},$$
$$2^{140} \equiv 67 \pmod{561}, \qquad 2^{280} \equiv 1 \pmod{561}.$$

Also ist 561 als zusammengesetzt erkannt. Die kleinste zusammengesetzte Zahl, die den strengen Pseudoprimzahltest für 2, 3 und 5 besteht, ist $25326001 = 2251 \cdot 11251$. Die einzige zusammengesetzte Zahl $< 10^{11}$, die ihn für 2, 3, 5 und 7 besteht, ist 3 215 031 751. Das erweckt die Hoffnung, dass dieser Test zum Erkennen von Primzahlen tatsächlich geeignet ist.

Satz 2 *Sei $n \geq 3$ ungerade. Dann sind äquivalent:*

(i) *n ist prim.*

(ii) *n besteht den strengen Pseudoprimzahltest zu jeder Basis a, die kein Vielfaches von n ist.*

Beweis. „(i) $\Longrightarrow$ (ii)“ wurde oben gezeigt.

„(ii) $\Longrightarrow$ (i)“: Wegen Satz 1 ist n prim oder eine CARMICHAEL-Zahl, insbesondere $\lambda(n) \mid n - 1 = u$; außerdem ist n quadratfrei, erst recht keine Primpotenz. Also ist der Hilfssatz in 2.3 anwendbar; da nach Voraussetzung $B_u = \mathbb{M}_n$, folgt also, dass n Primpotenz, insgesamt also prim ist. $\diamond$

Korollar 3 *Ist n nicht prim, so gibt es höchstens $\frac{\varphi(n)}{2}$ Basen $< n$, für die n den strengen Pseudoprimzahltest besteht.*

Beweis. Falls n CARMICHAEL-Zahl ist, folgt das aus Satz 1 in 2.3. Andernfalls ist $A_u = \{w \in \mathbb{M}_n \mid w^{n-1} = 1\} < \mathbb{M}_n$ echte Untergruppe, und $B_u \subseteq A_u$. $\diamond$

Bei genauerem Hinsehen kann man sogar die Schranke $\frac{\varphi(n)}{4}$ von RABIN/MONIER herleiten (**Übungsaufgabe**).

3.3 Der Primzahltest von Miller

Wie ist das im vorigen Abschnitt entwickelte Kriterium, der strenge Pseudoprimzahltest zu einer oder genügend vielen Basen, praktisch verwertbar? Dazu ist zunächst der Algorithmus für eine Basis a zu formulieren und sein Aufwand zu bestimmen.

Da a^{n-1} sowieso nach dem binären Potenzalgorithmus berechnet wird, ist es effizienter, gleich die ganze Folge der Potenzen ab a^r zu bestimmen; dann ist der Aufwand nicht wesentlich größer als für den „schwachen“ Pseudoprimzahltest. Der strenge Pseudoprimzahltest zur Basis a sieht dann so aus:

Prozedur sPPT(a)
[Strenger Pseudoprimzahltest zu einer Basis a.]
Eingabeparameter:
n = die zu prüfende Zahl (ungerade ≥ 3),
s = Zweierordnung von $n-1$ (vorberechnet),
r = ungerader Teil von $n-1$ (vorberechnet),
a = Basis (im Bereich $[2 \ldots n-1]$).
Ausgabeparameter:
zus = ein Boolescher Wert mit der Bedeutung
TRUE: n ist sicher zusammengesetzt,
FALSE: die Prüfung gab kein definitives Ergebnis
[d. h., n ist strenge Pseudoprimzahl zur Basis a].
Anweisungen:
Bestimme $b = a^r \bmod n$.
Setze $k = 0$.
[Schleife: Am Eingang ist $b = a^{2^k r} \bmod n$;
die Boolesche Variable ‘Ende’, vorbesetzt mit FALSE, entscheidet über das nochmalige Durchlaufen der Schleife.]
Solange nicht Ende:
Falls $b = 1$: Setze Ende = TRUE;
falls $k = 0$, setze zus = FALSE,
sonst setze zus = TRUE. [1 ohne vorherige -1]
Falls $b = n-1$ und $k < s$:
Setze zus = FALSE, Ende = TRUE.
Falls $k = s$ und $b \neq 1$:
Setze zus = TRUE, Ende = TRUE.
In allen anderen Fällen $[k < s, b \neq 1, b \neq n-1]$
ersetze b durch $b^2 \bmod n$,
ersetze k durch $k+1$.

Der Aufwand läßt sich in Einzelschritte aufbrechen, in denen jeweils zwei Zahlen mod n multipliziert werden. Zur Berechnung von $a^r \bmod n$ sind

höchstens $2 \cdot {}^2\log(r)$ solcher Schritte nötig. Bei den höchstens s Schleifendurchläufen wird noch je einmal quadriert. Da ${}^2\log(n-1) = s + {}^2\log(r)$, sind also insgesamt höchstens $2 \cdot {}^2\log(n)$ Quadrate $\bmod n$ zu bilden. Jedes solche Quadrat erfordert höchstens N^2 „primitive“ Ganzzahl-Multiplikationen, wobei N die Stellenzahl von n in der verwendeten Basis des Zahlsystems ist. Die Bestimmung von r bedeutet s Divisionen durch 2 und kann hier vernachlässigt werden. Der Gesamtaufwand ist also, grob geschätzt, $\mathrm{O}(\log(n)^3)$.

Der Primzahltest von MILLER ist nun einfach die Aneinanderreihung der strengen Pseudoprimzahltests zu den Basen $2, 3, 4, 5, \ldots$. Das sieht zunächst nicht effizient aus, denn wenn man tatsächlich eine Primzahl testet, muss man scheinbar alle Basen $< n$ durchlaufen. MILLER hat aber gezeigt, dass man mit entscheidend weniger auskommt – *vorausgesetzt, die erweiterte* RIEMANN*sche Vermutung ist wahr.* Hierzu im nächsten Abschnitt einige Erläuterungen ohne vollständige Beweise.

3.4 Die erweiterte Riemannsche Vermutung (ERH)

Ein **Charakter** mod n ist eine Funktion

$$\chi : \mathbb{Z} \longrightarrow \mathbb{C}$$

mit den Eigenschaften:

(i) χ hat die Periode n.

(ii) $\chi(xy) = \chi(x)\chi(y)$ für alle $x, y \in \mathbb{Z}$.

(iii) $\chi(x) = 0$ genau dann, wenn $\mathrm{ggT}(x, n) > 1$.

Die Charaktere mod n entsprechen kanonisch bijektiv genau den Gruppen-Homomorphismen

$$\bar{\chi} : \mathbb{M}_n \longrightarrow \mathbb{C}^\times.$$

Beispiele sind der **triviale Charakter** $\chi(a) = 1$ für alle zu n teilerfremden a und der aus der Theorie der quadratischen Reziprozität bekannte Jacobi-**Charakter** $\chi(a) = (\frac{a}{n})$, siehe Anhang A.5.

Zu einem Charakter gehört eine **L-Funktion**, die durch die Dirichlet-Reihe

$$L_\chi(z) = \sum_{a=1}^{\infty} \frac{\chi(a)}{a^z}$$

definiert ist. Die Reihe konvergiert absolut und lokal gleichmäßig in der Halbebene $\{z \in \mathbb{C} \mid \mathrm{Re}(z) > 1\}$, weil $a^{i\cdot\mathrm{Im}(z)} = e^{i\cdot\ln(a)\cdot\mathrm{Im}(z)}$ den Betrag 1 hat, also

$$\left|\frac{\chi(a)}{a^z}\right| = \left|\frac{\chi(a)}{a^{\mathrm{Re}(z)} \cdot a^{i\cdot\mathrm{Im}(z)}}\right| = \frac{1}{a^{\mathrm{Re}(z)}} \qquad \text{oder } 0.$$

Sie läßt sich analytisch auf die rechte Halbebene $\mathrm{Re}(z) > 0$ fortsetzen und ist dort holomorph, außer im Fall des trivialen Charakters, wo 1 ein einfacher Pol ist. Die Funktion L_χ hat die Riemann-**Eigenschaft**, wenn sie innerhalb des Streifens $0 < \mathrm{Re}(z) \leq 1$ Nullstellen nur auf der Geraden $\mathrm{Re}(z) = \frac{1}{2}$ hat. Die Riemannsche Vermutung behauptet dies gerade für die Riemannsche Zeta-Funktion, die **erweiterte** Riemannsche **Vermutung** für alle L-Funktionen zu Charakteren mod n. Die Zeta-Funktion ist für $\mathrm{Re}(z) > 1$ definiert durch

$$\zeta(z) := \sum_{a=1}^{\infty} \frac{1}{a^z} = \prod_{p \text{ prim}} \frac{1}{1 - \frac{1}{p^z}},$$

wobei die zweite Gleichung die Produktformel von Euler ist. Für den trivialen Charakter χ_1 mod n gilt also:

$$L_{\chi_1}(z) = \sum_{\mathrm{ggT}(a,n)=1} \frac{1}{a^z} = \zeta(z) \cdot \prod_{p|n \text{ prim}} \left(1 - \frac{1}{p^z}\right);$$

diese L-Funktion hat in $\mathrm{Re}(z) > 0$ die gleichen Nullstellen wie ζ.

Satz 3 (Ankeney/Montgomery/Bach) *Für $c = 2/\ln(3)^2 = 1.65707\ldots$ gilt: Ist χ ein nichttrivialer Charakter $\bmod n$, dessen L-Funktion L_χ die* Riemann*-Eigenschaft hat, so gibt es eine Primzahl $p < c \cdot \ln(n)^2$ mit $\chi(p) \neq 1$.*

Der Beweis soll hier nicht geführt werden.

Korollar 1 *Es gelte die verallgemeinerte* Riemann*sche Vermutung. Sei $G < \mathbb{M}_n$ eine echte Untergruppe. Dann gibt es eine Primzahl p mit $p < c \cdot \ln(n)^2$, deren Restklasse $\bmod n$ im Komplement $\mathbb{M}_n - G$ liegt.*

Beweis. Es gibt einen nichttrivialen Homomorphismus $\mathbb{M}_n/G \longrightarrow \mathbb{C}^\times$, also einen Charakter $\bmod n$ mit $G \subseteq \operatorname{Kern}\chi \subseteq \mathbb{M}_n$. $\diamond$

Satz 4 (Miller) *Die ungerade Zahl $n \geq 3$ bestehe den strengen Pseudoprimzahltest für alle primen Basen $a < c \cdot \ln(n)^2$ mit c wie in Satz 3, und die L-Funktion jedes Charakters für jeden Teiler von n habe die Riemann-Eigenschaft. Dann ist n prim.*

Beweis. Zuerst wird gezeigt, dass n quadratfrei ist. Angenommen $p^2 \mid n$ für eine Primzahl p. Die multiplikative Gruppe $\mathbb{M}_{p^2}$ ist zyklisch von der Ordnung $p(p-1)$; insbesondere ist der Homomorphismus

$$\mathbb{M}_{p^2} \longrightarrow \mathbb{M}_{p^2}, a \mapsto a^{p-1} \bmod p^2,$$

nichttrivial. Sein Bild ist eine Untergruppe $G < \mathbb{M}_{p^2}$ der Ordnung p, die zyklisch, also isomorph zur Gruppe der p-ten Einheitswurzeln in $\mathbb{C}$ ist. Die Zusammensetzung ergibt einen Charakter $\bmod p^2$, und Satz 3 ergibt eine Primzahl $a < c \cdot \ln(p^2)^2$ mit $a^{p-1} \not\equiv 1 \bmod p^2$. Die Ordnung von a in $\mathbb{M}_{p^2}$ teilt $p(p-1)$. Wäre $a^{n-1} \equiv 1 \bmod n$, so müsste die Ordnung auch $n-1$ teilen. Da p zu $n-1$ teilerfremd ist, müsste sie Teiler von $p-1$ sein, was sie ja gerade nicht ist. Also ist $a^{n-1} \not\equiv 1 \bmod n$, und das widerspricht nun wieder dem bestandenen Pseudoprimzahltest. Also ist n quadratfrei.

Jetzt wird gezeigt, dass n auch nicht zwei verschiedene Primfaktoren haben kann. Nehmen wir an, p und q seien zwei solche, o. B. d. A. $\nu_2(p-1) \geq \nu_2(q-1)$. [$\nu_2(x)$ der Exponent des Primfaktors 2 in x.] Sei

$$r = \begin{cases} p, & \text{falls } \nu_2(p-1) > \nu_2(q-1), \\ pq, & \text{falls } \nu_2(p-1) = \nu_2(q-1). \end{cases}$$

Wieder nach dem Satz 3 gibt es ein $a < c \cdot \ln(r)^2$ mit $(\frac{a}{r}) = -1$. Ist u der ungerade Teil von $n-1$ und $b = a^u$, so ist auch $(\frac{b}{r}) = -1$, insbesondere $b \neq 1$. Wegen des strengen Pseudoprimzahltests gibt es also ein k mit $b^{2^k} \equiv -1 \bmod n$. Dann hat also b in $\mathbb{M}_p$ und in $\mathbb{M}_q$ die Ordnung 2^{k+1}. Insbesondere ist $2^{k+1} \mid q-1$.

Falls nun $\nu_2(p-1) > \nu_2(q-1)$ ist, muss sogar $2^{k+1} \mid \frac{p-1}{2}$ sein. Daraus folgt im Widerspruch zum EULER-Kriterium $b^{(p-1)/2} \equiv 1 \pmod{p}$, aber $(\frac{b}{p}) = -1$.

Ist aber $\nu_2(p-1) = \nu_2(q-1)$, so $(\frac{b}{p})(\frac{b}{q}) = (\frac{b}{r}) = -1$; also o. B. d. A. $(\frac{b}{p}) = -1$, $(\frac{b}{q}) = 1$. Nach dem EULER-Kriterium ist $b^{(q-1)/2} \equiv 1 \pmod{q}$, also $2^{k+1} \mid \frac{q-1}{2}$, $k+2 \leq \nu_2(q-1) = \nu_2(p-1)$, also auch $b^{(p-1)/2} \equiv 1 \pmod{p}$, im Widerspruch zu $(\frac{b}{p}) = -1$. $\diamond$

Für den Primzahltest von Miller reicht es also, den strengen Pseudoprimzahltest für alle Primzahlen $a < c \cdot \ln(n)^2$ durchzuführen. Der Gesamtaufwand ist also $O(\log(n)^5)$. Für eine 512-Bit-Zahl, also $n < 2^{512}$, reicht es, die 18698 Primzahlen < 208704 durchzuprobieren. Das dauert natürlich bei aller Effizienz seine Zeit. In der Praxis hat sich daher eine Modifikation dieses Tests durchgesetzt, die (in einem noch zu spezifizierenden Sinne) nicht ganz exakt, aber wesentlich schneller ist. Sie wird im nächsten Abschnitt behandelt.

3.5 Der probabilistische Primzahltest von RABIN

Grundlage ist die Übertragung einer Idee von SOLOVAY und STRASSEN auf den MILLERschen Test, die RABIN vorgeschlagen hat. Anscheinend hatte aber SELFRIDGE schon 1974 diesen Test verwendet. Wählt man a zufällig in $[2 \dots n-1]$, so fällt n „in der Regel“ durch den strengen Pseudoprimzahltest zur Basis a, wenn es zusammengesetzt ist. Was heißt aber „in der Regel“? Wie groß ist die Wahrscheinlichkeit? Diese Frage wurde schon im Korollar zu Satz 2 beantwortet, wobei die schärfere Schranke $\frac{1}{4}$ ohne Beweis angegeben wurde.

Zu bemerken ist, dass die Schranke $\frac{1}{4}$ scharf ist. Das sieht man an den Zahlen der Form

$$n = (1+2t)(1+4t)$$

mit ungeradem t (sofern die Faktoren $p = 1+2t$ und $q = 1+4t$ prim sind – Beispiel: $t = 24969$, $p = 49939$, $q = 99877$). Dann ist $n-1 = 2r$ mit $r = 3t + 4t^2$,

$$B_u = \{a \mid a^r \equiv 1 \pmod{n}\} \cup \{a \mid a^r \equiv -1 \pmod{n}\}.$$

Da $\mathrm{ggT}(r, p-1) = \mathrm{ggT}(3t+4t^2, 2t) = t = \mathrm{ggT}(r, q-1)$, hat jede dieser beiden Kongruenzen genau t^2 Lösungen. Also ist $\#B_u = 2t^2$,

$$\frac{\#B_u}{n-1} = \frac{2t^2}{2 \cdot (3t+4t^2)} = \frac{t}{3+4t} = \frac{1}{4+\frac{3}{t}}.$$

Die Grenze $\frac{1}{4}$ wird allerdings für die meisten zusammengesetzten Zahlen längst nicht erreicht.

Allgemein sei eine Familie $(B_{(n)})_{n \geq 1}$ von Mengen $B_{(n)} \subseteq [1 \dots n-1]$ und ein $\varepsilon \in]0,1[$ gegeben mit

1. $B_{(n)} = [1 \dots n-1]$, wenn n prim,
2. $\#B_{(n)} \leq \varepsilon \cdot (n-1)$ für alle genügend großen ungeraden zusammengesetzten Zahlen n.

Ferner soll die Entscheidung, ob $a \in B_{(n)}$, für alle $a \in [1 \dots n-1]$ effizient möglich sein, also mit einem Aufwand, der höchstens polynomial mit $\ln(n)$ wächst. Dann gibt es einen zugehörigen (abstrakten) Pseudoprimzahltest:

1. Wähle $a \in [1 \dots n-1]$ zufällig.
2. Prüfe, ob $a \in B_{(n)}$.
3. Ausgabe:
   (a) Falls **nein**: n ist sicher zusammengesetzt.
   (b) Falls **ja**: n ist pseudoprim für a.

Der zugehörige **probabilistische Primzahltest** besteht aus der Aneinanderreihung von k solchen Pseudoprimzahltests mit unabhängig voneinander zufällig gewählten Basen a (die sich also auch wiederholen dürfen). Ist stets $a \in B_{(n)}$, so ist n fast sicher prim – man kann diesem Ergebnis die „Irrtumswahrscheinlichkeit“ δ zuweisen, die aber nicht $= \varepsilon^k$ ist, sondern sich so berechnet:

In der Menge der ungeraden Zahlen $< 2^r$, also mit höchstens r Bits sei X die Teilmenge der *zusammengesetzten* Zahlen und Y_k die Menge der Zahlen, die k unabhängige (abstrakte) Pseudoprimzahltests bestehen. Die Wahrscheinlichkeit, dass das einer zusammengesetzten Zahl gelingt, ist dann gegeben durch die bedingte Wahrscheinlichkeit $P(Y_k|X) \leq \varepsilon^k$. Für die praktische Anwendung interessanter ist allerdings die „umgekehrte“ Wahrscheinlichkeit $\delta = P(X|Y_k)$ dafür, dass eine Zahl n, die bestanden hat, trotzdem zusammengesetzt ist. Diese kann man mit Hilfe der Bayesschen Formel abschätzen:

$$P(X|Y_k) = \frac{P(X) \cdot P(Y_k|X)}{P(Y_k)} \leq \frac{P(Y_k|X)}{P(Y_k)} \leq \frac{1}{q} \cdot \varepsilon^k \leq r \cdot \ln(2) \cdot \varepsilon^k,$$

wobei die Dichte der Primzahlen nach dem Primzahlsatz eingeht:

$$P(Y_k) \geq P(\text{prim}) =: q \geq \frac{1}{r \cdot \ln(2)}$$

(die letzte Ungleichung ist sogar großzügig, da wir nur ungerade Zahlen betrachten). Die gesuchte „Irrtumswahrscheinlichkeit“ $\delta = P(X|Y_k)$ könnte also durchaus größer als ε^k sein. Man kann (und) sollte sie dadurch verringern, dass man die Grundmenge, in der man nach Primzahlen sucht, einschränkt und damit $P(Y_k)$ vergrößert, z. B. indem man vor Anwendung des Pseudoprimzahltests durch alle Primzahlen etwa $< 100r$ probeweise dividiert.

Beim **Primzahltest von** Rabin ist $B_{(n)}$ die Menge der Basen a, für die n den strengen Pseudoprimzahltest zur Basis a besteht, und $\varepsilon = \frac{1}{4}$. Übersteht n die 25-fache Anwendung, so ist es mit einer sehr kleinen Irrtumswahrscheinlichkeit prim. Es ist eher wahrscheinlich, dass die Berechnung wegen eines Hard- oder Software-Fehlers falsch ist, als dass der Algorithmus die Primzahl-Eigenschaft falsch schätzt. Knuth bezweifelt auch, dass ein veröffentlichter Beweis der erweiterten Riemannschen Vermutung jemals eine so hohe Glaubwürdigkeit haben kann. Dennoch ist es natürlich mathematisch unbefriedigend, nicht mit absoluter Sicherheit sagen zu können, dass wirklich eine Primzahl vorliegt.

Als weiterführende Literatur zur Frage, wie „gut“ ein probabilistischer Primzahltest ist, sei

- S. H. Kim/ C. Pomerance: The probability that a random probable prime is composite. Math Comp. 53 (1989), 721–741,

empfohlen.

3.6 RSA und Pseudoprimzahlen

Das für die Anwendbarkeit des RSA-Verfahrens grundlegende Problem, wie man Primzahlen findet, wird durch den probabilistischen RABIN-Test zwar hocheffizient, aber nicht restlos befriedigend gelöst: Was passiert, wenn man eine „falsche“ Primzahl erwischt?

Sei dazu $n = pq$ ein vermeintlicher RSA-Modul, für den p und q nicht notwendig Primzahlen – aber zueinander teilerfremd – sind. Bei der Konstruktion der Schlüssel d, e mit

$$de \equiv 1 \pmod{\tilde{\lambda}(n)}$$

werden dann statt der wahren Werte $\varphi(n)$ und $\lambda(n)$ für EULER- und CARMICHAEL-Funktion die möglicherweise davon abweichenden Werte

$$\tilde{\varphi}(n) := (p-1)(q-1), \quad \tilde{\lambda}(n) := \mathrm{kgV}(p-1, q-1)$$

verwendet.

Funktioniert das RSA-Verfahren noch? Sei $a \in \mathbb{Z}/n\mathbb{Z}$ ein Klartext. Der Fall $\mathrm{ggT}(a, n) > 1$ führt – wie auch sonst – zur Faktorisierung des Moduls und wird hier – wie auch sonst – wegen seiner extrem geringen Wahrscheinlichkeit ignoriert. Andernfalls ist $\mathrm{ggT}(a, n) = 1$, und zu fragen ist, ob

$$a^{de-1} \stackrel{?}{\equiv} 1 \pmod{n}$$

gilt. Nun, das ist nach dem chinesischen Restsatz genau dann der Fall, wenn

$$a^{de-1} \equiv 1 \pmod{p} \quad \text{und} \quad \pmod{q}$$

ist. Hinreichend dafür ist

$$a^{p-1} \equiv 1 \pmod{p} \quad \text{und} \quad a^{q-1} \equiv 1 \pmod{q};$$

d. h., eine Nachricht a wird höchstens dann nicht korrekt entschlüsselt, wenn p oder q nicht pseudoprim zur Basis a ist. Also:

- Verwendet man statt einem Primfaktor p eine CARMICHAEL-Zahl, funktioniert das RSA-Verfahren trotz der „falschen“ Parameter korrekt, wenn a zu n teilerfremd ist; allerdings ist die (extrem geringe) Wahrscheinlichkeit, durch einen Klartext a, der nicht zu n teilerfremd ist, zufällig den Modul n zu faktorisieren, geringfügig vergrößert.
- Andernfalls – falls p weder prim noch eine CARMICHAEL-Zahl ist –, gibt es eine geringe Chance, dass eine Nachricht nicht korrekt entschlüsselt werden kann.

Aus diesem Grund werden bei vielen Implementierungen des RSA-Verfahrens nach der Schlüsselerzeugung – wenn der probabilistische Primzahltest von RABIN eingesetzt wird – ein paar Probever- und -entschlüsselungen durchgeführt; das entspricht aber auch nur ein paar zusätzlichen Pseudoprimzahltests. Geht dabei etwas schief, wird der Modul verworfen. Es ist nicht bekannt, ob dieser Fall schon einmal eingetreten ist.

3.7 Der AKS-Primzahltest

Die Frage, ob es einen deterministischen Primzahltest gibt, der **mit polynomialem Aufwand** auskommt, war bisher nur – durch MILLER – auf die erweiterte RIEMANNsche Vermutung zurückgeführt worden. Alle anderen bekannten Primzahltests benötigten einen höheren Aufwand oder waren probabilistisch. Im August 2002 überraschten drei Inder, Manindra AGRAWAL, Neeraj KAYAL und Nitin SAXENA, die Fachwelt mit einem vollständigen Beweis, der auf einem überraschend einfachen Algorithmus beruht. Dieser erhielt sofort den Namen „AKS-Primzahltest". Er benötigt in der schnellsten bisher bekannten Version einen Aufwand von $O(\log(n)^6)$.

Satz 5 (Grundkriterium) *Seien $a, n \in \mathbb{Z}$ teilerfremd, $n \geq 2$. Dann sind äquivalent:*

(i) *n ist prim.*

(ii) *$(X+a)^n \equiv X^n + a \pmod{n}$ im Polynomring $\mathbb{Z}[X]$.*

Beweis. Aus dem binomischen Lehrsatz folgt

$$(X+a)^n = \sum_{i=0}^{n} \binom{n}{i} a^{n-i} X^i$$

in $\mathbb{Z}[X]$.

(i) Ist n prim, so $n | \binom{n}{i}$ für $i = 1, \ldots, n-1$, also $(X+a)^n \equiv X^n + a^n \pmod{n}$, und nach dem Satz von FERMAT ist $a^n \equiv a \pmod{n}$.

(ii) Ist n dagegen zusammengesetzt, so wählt man einen Primfaktor $q | n$ und k mit $q^k | n$ und $q^{k+1} \nmid n$. Dann ist $q \neq n$ und

$$q^k \nmid \binom{n}{q} = \frac{n \cdots (n-q+1)}{1 \cdots q}.$$

Also hat $(X+a)^n$ bei X^q einen Koeffizienten $\neq 0$ in $\mathbb{Z}/n\mathbb{Z}$. $\diamond$

Bemerkungen

1. Der Blick auf das absolute Glied in (ii) zeigt, dass das Grundkriterium eine Verallgemeinerung des Satzes von FERMAT ist.

2. Sei $\mathfrak{q} := (n, X^r - 1) \trianglelefteq \mathbb{Z}[X]$ (Ideal im Polynomring) für $r \in \mathbb{N}$. Ist n prim, so $(X+a)^n \equiv X^n + a \pmod{\mathfrak{q}}$. Also ist gezeigt:

Korollar 1 *Ist n prim, so gilt im Polynomring $\mathbb{Z}[X]$*

$$(X+a)^n \equiv X^n + a \pmod{\mathfrak{q}}$$

für alle $a \in \mathbb{Z}$ mit $\mathrm{ggT}(a, n) = 1$ und alle $r \in \mathbb{N}$.

Die naive Anwendung des Grundkriteriums als Primzahltest würde mit dem binären Potenzalgorithmus etwa ${}^2\log n$ Multiplikationen von Polynomen in $\mathbb{Z}/n\mathbb{Z}[X]$ erfordern, die aber immer aufwendiger werden: Im letzten Schritt sind zwei Polynome vom Grad etwa $\frac{n}{2}$ zu multiplizieren, was einen Aufwand der Größenordnung n erfordert. Das Korollar beschränkt den Grad durch $r-1$, ist aber nicht hinreichend.

Der Kernpunkt des AKS-Algorithmus ist, dass man das Korollar im wesentlichen umkehren kann, wenn man genügend viele, aber insgesamt nur „wenige“ a bei einem geeigneten festen r durchprobiert:

Satz 6 (AKS-Kriterium, Version von H. W. Lenstra**)** *Sei n eine natürliche Zahl ≥ 2. Gegeben sei eine zu n teilerfremde Zahl $r \in \mathbb{N}$. Sei $q := \mathrm{Ord}_r\, n$ die Ordnung von n in der multiplikativen Gruppe $\mathbb{M}_r = (\mathbb{Z}/r\mathbb{Z})^\times$. Ferner sei gegeben eine natürliche Zahl $s \geq 1$ mit $\mathrm{ggT}(n,a) = 1$ für alle $a = 1, \ldots, s$ und*

$$\binom{\varphi(r)+s-1}{s} \geq n^{2d\cdot\lfloor\sqrt{\frac{\varphi(r)}{d}}\rfloor}$$

für jeden Teiler $d|\frac{\varphi(r)}{q}$. Für das Ideal $\mathfrak{q} = (n, X^r-1) \trianglelefteq \mathbb{Z}[X]$ gelte

$$(X+a)^n \equiv X^n + a \pmod{\mathfrak{q}} \quad \text{für alle } a = 1, \ldots s.$$

Dann ist n eine Primzahlpotenz.

Der Beweis (nach D. Bernstein) wird in einige Hilfssätze zerlegt.

Hilfssatz 1 *Für alle $a = 1, \ldots s$ und alle $i \in \mathbb{N}$ gilt:*

$$(X+a)^{n^i} \equiv X^{n^i} + a \pmod{\mathfrak{q}}.$$

Beweis. Das folgt durch Induktion über i, wenn man in

$$(X+a)^n = X^n + a + n\cdot f(X) + (X^r-1)\cdot g(X)$$

in $\mathbb{Z}[X]$ die Substitution $X \mapsto X^{n^i}$ ausführt:

$$\begin{aligned}(X+a)^{n^{i+1}} \equiv (X^{n^i}+a)^n = X^{n^i\cdot n} + a + n\cdot f(X^{n^i}) + (X^{n^i\cdot r}-1)\cdot g(X^{n^i})\\ \equiv X^{n^{i+1}} + a \pmod{\mathfrak{q}},\end{aligned}$$

da $X^{n^i r} - 1 = (X^r)^{n^i} - 1 = (X^r-1)(X^{r\cdot(n^i-1)} + \cdots + X^r + 1)$ Vielfaches von $X^r - 1$ ist. $\diamond$

Sei jetzt $p|n$ ein Primteiler. *Ziel* ist zu zeigen, dass n eine Potenz von p ist.

Das Ideal $\mathfrak{q} = (n, X^r-1) \trianglelefteq \mathbb{Z}[X]$ wird vergrößert zu $\hat{\mathfrak{q}} := (p, X^r-1) \trianglelefteq \mathbb{Z}[X]$. Die Identität aus Hilfssatz 1 gilt dann auch mod $\hat{\mathfrak{q}}$, und es gilt sogar, da jetzt ja mod p gerechnet wird:

Korollar 2 *Für alle $a = 1, \dots s$ und alle $i, j \in \mathbb{N}$ gilt*

$$(X + a)^{n^i p^j} \equiv X^{n^i p^j} + a \pmod{\hat{\mathfrak{q}}}.$$

Sei $H := \langle n, p \rangle \leq \mathbb{M}_r$ die von den Restklassen $n \bmod r$ und $p \bmod r$ erzeugte Untergruppe. Sei

$$d := \#(\mathbb{M}_r / H) = \frac{\varphi(r)}{\#H}.$$

Da $q = \mathrm{Ord}_r\, n \,|\, \#H$, ist $d \,|\, \frac{\varphi(r)}{q}$; also erfüllt d die Voraussetzung von Satz 6. Ein vollständiges Repräsentantensystem $\{m_1, \dots, m_d\} \subseteq \mathbb{M}_r$ von $\mathbb{M}_r / H$ sei für den Rest des Beweises fest gewählt. Korollar 2 wird dann erweitert zu

Korollar 3 *Für alle $a = 1, \dots s$, alle $k = 1, \dots, d$ und alle $i, j \in \mathbb{N}$ gilt*

$$(X^{m_k} + a)^{n^i p^j} \equiv X^{m_k n^i p^j} + a \pmod{\hat{\mathfrak{q}}}.$$

Beweis. Nach dem gleichen Trick wie in Hilfssatz 1 wird $X \mapsto X^{m_k}$ in $\mathbb{Z}[X]$ substituiert:

$$(X + a)^{n^i p^j} = X^{n^i p^j} + a + p \cdot f(X) + (X^r - 1) \cdot g(X) \text{ in } \mathbb{Z}[X],$$

$$(X^{m_k} + a)^{n^i p^j} = X^{m_k n^i p^j} + a + p \cdot f(X^{m_k}) + (X^{m_k \cdot r} - 1) \cdot g(X^{m_k}),$$

und daraus folgt die Behauptung. $\diamond$

Für die Produkte $n^i p^j \in \mathbb{N}$ mit $0 \leq i, j \leq \lfloor \sqrt{\frac{\varphi(r)}{d}} \rfloor$ gilt

$$1 \leq n^i p^j \leq n^{2 \cdot \lfloor \sqrt{\frac{\varphi(r)}{d}} \rfloor}.$$

Es gibt $(\lfloor \sqrt{\frac{\varphi(r)}{d}} \rfloor + 1)^2 > \frac{\varphi(r)}{d}$ solcher Paare $(i, j) \in \mathbb{N}^2$, und alle $n^i p^j \bmod r$ liegen in der Untergruppe H mit $\#H = \frac{\varphi(r)}{d}$; also gibt es verschiedene $(i, j) \neq (h, l)$ mit

$$n^i p^j \equiv n^h p^l \pmod{r},$$

und dafür muss sogar $i \neq h$ sein – sonst wäre $p^j \equiv p^l \pmod{r}$, also $p | r$. Damit ist auch schon der erste Teil des folgenden Hilfssatzes gezeigt:

Hilfssatz 2 *Es gibt i, j, h, l mit $0 \leq i, j, h, l \leq \lfloor \sqrt{\frac{\varphi(r)}{d}} \rfloor$ und $i \neq h$, so dass für $t := n^i p^j$, $u := n^h p^l$ die Kongruenz $t \equiv u \pmod{r}$ erfüllt ist, und $|t - u| \leq n^{2 \cdot \lfloor \sqrt{\frac{\varphi(r)}{d}} \rfloor} - 1$. Damit gilt*

$$(X^{m_k} + a)^t \equiv (X^{m_k} + a)^u \pmod{\hat{\mathfrak{q}}}$$

für alle $a = 1, \dots, s$ und alle $k = 1, \dots d$.

Beweis. Die letzte Kongruenz folgt aus $X^t = X^{u+cr} \equiv X^u \pmod{X^r - 1}$, also

$$(X^{m_k} + a)^t \equiv X^{m_k t} + a \equiv X^{m_k u} + a \equiv (X^{m_k} + a)^u \pmod{\hat{\mathfrak{q}}},$$

für alle a und k. $\diamond$

Da r zu n teilerfremd und p ein Primteiler von n ist, hat $X^r - 1$ im algebraischen Abschluss von $\mathbb{F}_p$ keine mehrfachen Nulstellen, also r verschiedene Nullstellen, die r-ten Einheitswurzeln $\bmod p$. Diese bilden (als endliche multiplikative Untergruppe eines Körpers) eine zyklische Gruppe. Sei ζ ein erzeugendes Element davon, also eine primitive r-te Einheitswurzel. Es gibt einen irreduziblen Teiler $h \in \mathbb{F}_p[X]$ von $X^r - 1$ mit $h(\zeta) = 0$. Sei

$$K = \mathbb{F}_p[\zeta] \cong \mathbb{F}_p[X]/h\mathbb{F}_p[X] \cong \mathbb{Z}[X]/\hat{\hat{\mathfrak{q}}}$$

mit dem Ideal $\hat{\hat{\mathfrak{q}}} = (p, h) \trianglelefteq \mathbb{Z}[X]$. Wir haben also die aufsteigende Kette von Idealen

$$\mathfrak{q} = (n, X^r - 1) \hookrightarrow \hat{\mathfrak{q}} = (p, X^r - 1) \hookrightarrow \hat{\hat{\mathfrak{q}}} = (p, h) \trianglelefteq \mathbb{Z}[X]$$

und umgekehrt die Kette von Surjektionen

$$\mathbb{Z}[X] \longrightarrow \mathbb{Z}[X]/\mathfrak{q} \longrightarrow \mathbb{F}_p[X]/(X^r - 1) \longrightarrow K = \mathbb{F}_p[\zeta] \cong \mathbb{F}_p[X]/h\mathbb{F}_p[X].$$

Hilfssatz 3 *In K gilt:*

(i) $(\zeta^{m_k} + a)^t = (\zeta^{m_k} + a)^u$ *für alle* $a = 1, \ldots, s$ *und alle* $k = 1, \ldots d$.

(ii) *Ist* $G \leq K^\times$ *die von den* $\zeta^{m_k} + a \neq 0$ *erzeugte Untergruppe, so gilt* $g^t = g^u$ *für alle* $g \in \bar{G} := G \cup \{0\}$.

Beweis. (i) folgt aus Hilfssatz 2 mit dem Homomorphismus $\mathbb{Z}[X] \longrightarrow K$, $X \mapsto \zeta$, der den Kern $\hat{\hat{\mathfrak{q}}} \supseteq \hat{\mathfrak{q}}$ hat.

(ii) folgt direkt aus (i). $\diamond$

Die $X + a \in \mathbb{F}_p[X]$ für $a = 1, \ldots s$ sind paarweise verschiedene irreduzible Polynome, da $p > s$ nach der Voraussetzung von Satz 6. Also sind auch alle Produkte

$$f_e := \prod_{a=1}^{s} (X + a)^{e_a} \quad \text{für } e = (e_1, \ldots, e_s) \in \mathbb{N}^s$$

in $\mathbb{F}_p[X]$ verschieden. Was passiert bei der Abbildung

$$\begin{array}{rccl} \Phi\colon \mathbb{F}_p[X] & \longrightarrow & K^d, \\ f & \mapsto & (f(\zeta^{m_1}), \ldots, f(\zeta^{m_d})), \end{array}$$

mit den Polynomen f_e ?

Hilfssatz 4 *Für die f_e mit* $\operatorname{Grad} f_e = \sum_{a=1}^{s} e_a \le \varphi(r) - 1$ *sind die Bilder* $\Phi(f_e) \in K^d$ *paarweise verschieden.*

Beweis. Angenommen, $\Phi(f_c) = \Phi(f_e)$. Nach Korollar 3 gilt für $k = 1, \ldots, d$

$$f_c(X^{m_k})^{n^i p^j} = \prod_{a=1}^{s} (X^{m_k} + a)^{n^i p^j c_a} \equiv \prod_{a=1}^{s} (X^{m_k n^i p^j} + a)^{c_a}$$
$$= f_c(X^{m_k n^i p^j}) \pmod{\hat{\mathfrak{q}}}$$

und ebenso

$$f_e(X^{m_k})^{n^i p^j} \equiv f_e(X^{m_k n^i p^j}) \pmod{\hat{\mathfrak{q}}}.$$

erst recht mod $\hat{\hat{\mathfrak{q}}}$. Anwendung von Φ auf die linken Seiten ergibt

$$f_c(X^{m_k n^i p^j}) \equiv f_e(X^{m_k n^i p^j}) \pmod{\hat{\hat{\mathfrak{q}}}}.$$

Für die Differenz $g := f_c - f_e \in \mathbb{F}_p[X]$ gilt also $g(X^{m_k n^i p^j}) \in h\mathbb{F}_p[X]$ für alle $k = 1, \ldots, d$. Sei $b \in [1 \ldots r-1]$ zu r teilerfremd – also Repräsentant eines Elements von $\mathbb{M}_r$. Dann ist b in einer der Nebenklassen $m_k H$ von $\mathbb{M}_r / H$ enthalten. Es gibt also k, i und j mit $b \equiv m_k n^i p^j \pmod{r}$. Also ist

$$g(X^b) - g(X^{m_k n^i p^j}) \in (X^r - 1)\mathbb{F}_p[X] \subseteq h\mathbb{F}_p[X],$$

also $g(X^b) \in h\mathbb{F}_p[X]$, also $g(\zeta^b) = 0$. Daher hat g in K die $\varphi(r)$ verschiedenen Nullstellen ζ^b. Der Grad von g ist aber $< \varphi(r)$. Also ist $g = 0$, also $f_c = f_e$. $\diamond$

Korollar 4

$$\#\bar{G} \ge \binom{\varphi(r) + s - 1}{s}^{1/d} \ge |t - u| + 1.$$

Beweis. Es gibt $\binom{\varphi(r)+s-1}{s}$ Möglichkeiten, die Exponenten $(e_1, \ldots, e_s)$ wie in Hilfssatz 4 zu wählen. Da alle $\Phi(f_e) \in \bar{G}^d$, folgt

$$\#\bar{G}^d \ge \binom{\varphi(r) + s - 1}{s} \ge n^{2d \cdot \lfloor \sqrt{\frac{\varphi(r)}{d}} \rfloor},$$

nach der Voraussetzung von Satz 6, also

$$\#\bar{G} \ge n^{2 \cdot \lfloor \sqrt{\frac{\varphi(r)}{d}} \rfloor} \ge |t - u| + 1$$

nach Hilfssatz 2. $\diamond$

Damit ist der Beweis von Satz 6 leicht fertigzustellen: Da $g^t = g^u$ für alle $g \in \bar{G} \subseteq K$, hat das Polynom $X^{|t-u|}$ in K mehr als $|t - u|$ Nullstellen. Das geht nur, wenn $t = u$. Nach der Definition von t und u in Hilfssatz 2 ist also n eine Potenz von p.

Damit ist Satz 6 bewiesen. $\diamond$

3.8 Der AKS-Algorithmus

Der Algorithmus wird hier in der Version nach Lenstra/Bernstein beschrieben. Diese ist nicht auf möglichst effiziente Ausführung getrimmt, sondern auf einen möglichst einfachen Nachweis der Polynomialität.

Eingabe

Eingegeben wird eine natürliche Zahl $n \geq 2$.

Die Länge der Eingabe wird durch die Zahl ℓ der Bits in der Darstellung von n zur Basis 2 gemessen, also durch

$$\ell = \begin{cases} \lceil {}^2\log n \rceil, & \text{falls } n \text{ keine Zweierpotenz,} \\ k+1, & \text{falls } n = 2^k. \end{cases}$$

Ausgabe

Ausgegeben wird ein Boolescher Wert, sinngemäß ausgedrückt durch „ZUSAMMENGESETZT“ oder „PRIM“.

Schritt 1

Zweierpotenzen werden vorab abgefangen –

- Falls $n = 2$: Ausgabe „PRIM“, **Ende**.
- (Sonst) Falls n Zweierpotenz: Ausgabe „ZUSAMMENGESETZT“, **Ende**.

  Diesen Fall erkennt man daran, dass ${}^2\log n$ ganzzahlig ist.

Von jetzt an kann man annehmen, dass n keine Zweierpotenz, also $\ell = \lceil {}^2\log n \rceil$, ist.

Schritt 2

Eine große Zahl $N \in \mathbb{N}$ wird vorherberechnet, und zwar

$$N = 2n \cdot (n-1)(n^2-1)(n^3-1)\cdots(n^{4\ell^2}-1) = 2n \cdot \prod_{i=1}^{4\ell^2}(n^i-1).$$

Diese Zahl ist zwar riesengroß, aber, und das ist hier entscheidend:

- Die Zahl $4\ell^2$ der Multiplikationen ist polynomial in ℓ.
- Da
  $$N \leq 2n \cdot n^{\sum_{i=1}^{4\ell^2} i} = 2n \cdot n^{\frac{4\ell^2(4\ell^2+1)}{2}} \leq 2n \cdot n^{16\ell^4},$$
  ist $k := \lceil {}^2\log N \rceil \leq 1 + (16\ell^4+1) \cdot \ell$ polynomial in ℓ.

Die Zahl k wird im folgenden weiterverwendet; es ist $N < 2^k$, und k ist die kleinste natürliche Zahl mit dieser Eigenschaft.

Anforderungen

Es sind jetzt natürliche Zahlen r und s zu finden, die folgende Anforderungen erfüllen:

1. r ist zu n teilerfremd.
2. Im Intervall $[1, \ldots, s]$ hat n keinen Primteiler.
3. Für jeden Teiler $d \mid \frac{\varphi(r)}{q}$ – wobei $q = \mathrm{Ord}_r\, n$ – gilt
$$\binom{\varphi(r) + s - 1}{s} \geq n^{2d \cdot \lfloor \frac{\varphi(r)}{d} \rfloor}.$$
4. Das eigentliche Primzahlkriterium:
$$(X + a)^n \equiv X^n + a \pmod{(n, X^r - 1)}$$
für alle $a = 1, \ldots, s$.

Schritt 3

r wird als die kleinste Primzahl genommen, die kein Teiler von N ist; insbesondere ist r dann auch kein Teiler von n; insbesondere ist die Bedingung 1 erfüllt. Warum wird r mit polynomialem Aufwand gefunden?

Nach einer Erweiterung des Primzahlsatzes gilt für die Summe $\vartheta(x)$ der Logarithmen der Primzahlen $\leq x$,
$$\vartheta(x) = \sum_{p \leq x,\, p \text{ prim}} \ln p\,,$$
die asymptotische Relation
$$\vartheta(x) \sim x$$
sowie die Fehlerabschätzung von Rosser/Schoenfeld
$$x \cdot \left(1 - \frac{1}{\ln x}\right) < \vartheta(x) < x \cdot \left(1 - \frac{1}{2 \ln x}\right) \quad \text{für } x \geq 41.$$
Daher ist
$$\prod_{p \leq 2k,\, p \text{ prim}} p = e^{\vartheta(2k)} > 2^k > N.$$
Es können also nicht alle Primzahlen $< 2k$ Teiler von N sein.

Mit einem Aufwand, der höchstens quadratisch in $2k$, also auch polynomial in in ℓ ist, erhält man daher – etwa mit dem Sieb des Eratosthenes – die Liste aller Primzahlen $\leq r$.

Schritt 4

$s := r$. Die Bedingung 2 ist nicht ohne weiteres erfüllt. Daher wird folgendes Verfahren durchgeführt:

- Die (aus Schritt 3 bekannte) Liste der Primzahlen $p < r$ wird durchlaufen.
  - Falls $p = n$: Ausgabe „PRIM“, **Ende**.
    [Das kann nur für „kleine“ n vorkommen, da n exponentiell mit ℓ wächst, r aber nur polynomial.]
  - (Sonst) Falls $p|n$: Ausgabe „ZUSAMMENGESETZT“, **Ende**.

Falls dieser Punkt im Algorithmus noch erreicht wird, ist die Bedingung 2 für s erfüllt.

Bedingung 3

Der Nachweis der Bedingung 3 beginnt mit der Beobachtung, dass $q := \mathrm{Ord}_r\, n > 4\ell^2$.

> Sonst wäre $n^i \equiv 1 \pmod r$ für ein i mit $1 \le i \le 4\ell^2$, also $r \mid n^i - 1 \mid N$, Widerspruch.

Ist nun d ein Teiler von $\frac{\varphi(r)}{q}$, so

$$\begin{aligned} d &\le \frac{\varphi(r)}{q} < \frac{\varphi(r)}{4\ell^2}\,, \\ 2d \cdot \lfloor\sqrt{\frac{\varphi(r)}{d}}\rfloor &\le 2d \cdot \sqrt{\frac{\varphi(r)}{d}} = \sqrt{4d\varphi(r)} < \frac{\varphi(r)}{\ell} < \frac{\varphi(r)}{{}^2\log n}\,, \\ n^{2d\cdot\lfloor\sqrt{\frac{\varphi(r)}{d}}\rfloor} &< n^{\frac{\varphi(r)}{{}^2\log n}} = 2^{\varphi(r)}. \end{aligned}$$

Andererseits ist, da $\varphi(r) \ge 2$,

$$\binom{\varphi(r)+s-1}{s} = \binom{\varphi(r)+r-1}{r} = \binom{2\varphi(r)}{\varphi(r)+1} \ge 2^{\varphi(r)}.$$

Also ist die Bedingung 3 erfüllt.

Schritt 5

Nun wird die Bedingung 4,

$$(X+a)^n \equiv X^n + a \pmod{(n, X^r-1)}$$

in einer Schleife für $a = 1, \ldots, r$ überprüft. Die Anzahl der Schleifendurchläufe ist höchstens r, also $\le 2k$, also polynomial in ℓ. Bei jedem Schleifendurchlauf wird zweimal binär potenziert, also insgesamt höchstens 4ℓ Mal

multipliziert; multipliziert werden dabei Polynome von einem Grad $< r$ – der also polynomial in ℓ ist – mit Koeffizienten, deren Größe $< n$, deren Bitlänge also auch polynomial in ℓ ist.

- Falls für ein a die Bedingung 4 verletzt ist, wird „ZUSAMMENGESETZT“ ausgegeben, **Ende**.

Ansonsten ist für alle a die Bedingung 4 erfüllt, also n nach dem AKS-Kriterium eine Primzahlpotenz.

Schritt 6

Nun ist noch zu entscheiden, ob n eine echte Primzahlpotenz ist. Da die Primzahlen $\leq r$ keine Teiler von n sind, ist in einer Schleife über t mit $1 \leq t <^r \log n$ zu prüfen:

- Falls $\sqrt[t]{n}$ ganzzahlig: Ausgabe „ZUSAMMENGESETZT“, **Ende**.

Die Zahl der Schleifendurchläufe ist $\leq \ell$, und die Prüfung in jedem Durchlauf ist ebenfalls mit polynomialem Aufwand durchzuführen, wenn man $\lfloor \sqrt[t]{n} \rfloor$ mit einer binären Suche im Intervall $[1 \ldots n-1]$ sucht.

Falls der Algorithmus bis an diese Stelle kommt, wird „PRIM“ ausgegeben, **Ende**.

Damit ist gezeigt:

Hauptsatz 1 *Der AKS-Algorithmus bestimmt, ob n eine Primzahl ist, mit einem Aufwand, der polynomial von $\log n$ abhängt.*