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".

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. $\diamond$