Primes ist in P – Der AKS-Primzahltest
Notizen zum Vortrag auf dem MCAT-6 in Halle/S.

Hans-Gert Gräbe
Institut für Informatik, Universität Leipzig

10. Oktober 2003

Anfang August 2002 verbreitete sich die Nachricht, dass einige bis dahin unbekannte Inder einen deterministischen Primzahltest mit polynomialer Laufzeit entdeckt hatten. Die Anerkennung und Beweisglättung durch führende Experten folgte im Laufe einer Woche, so dass damit eines der großen Probleme der Komplexitätstheorie eine Lösung gefunden hat.

Besonders erstaunlich ist die Tatsache, dass – etwa im Gegensatz zum Beweis des „großen Fermat“ – der Beweis nur relativ einfache algebraische Argumente verwendet und gut auch von Mathematikern mit „durchschnittlichen“ Kenntnissen der Zahlentheorie nachvollzogen werden kann. Darum soll es in dem Vortrag gehen.

Doch zunächst eine Referenz an die Entdecker dieses Beweisansatzes. Dies sind

[A] Manindra Agrawal, Professor am Indian Institute of Technology in Kanpur seit 1996,

[K] Neeraj Kayal und

[S] Nitin Saxena, zwei Studenten und Mitglieder der indischen Mannschaft bei der Internationalen Mathematik-Olympiade 1997.

1. Der klassische Fermat-Test

Sei $n \in N$ eine natürliche Zahl und $m = \log_2(n)$ deren Bitlänge.

Es gilt folgender

Satz 1 (Kleiner Satz von Fermat) *Ist n prim, so gilt*

$$a^{n-1} \equiv 1 \pmod{n} \text{ für alle } a \in \mathbf{Z}_n^*$$

Kontraposition:

Satz 2 *Gilt $a^{n-1} \not\equiv 1 \pmod{n}$ für eine ganze Zahl $1 < a < n$, so ist n garantiert zusammengesetzt.*

Komplexität: $O(m^3)$

Las-Vegas-Verfahren:

- Wähle zufällige Werte $1 < a < n$ und berechne $a^{n-1} \pmod{n}$.
- Ist $a^{n-1} \not\equiv 1 \pmod{n}$ für **einen** Wert a, so ist n **garantiert** zusammengesetzt.

- Ist $a^{n-1} \equiv 1 \pmod{n}$ für **alle** Werte a, so ist n **wahrscheinlich** zusammengesetzt. (Fermat pseudo prime)

$$P_n := \{a \in \mathbf{Z}_n^* \ : \ a^{n-1} \equiv 1 \pmod{n}\}$$

ist eine Untergruppe von $\mathbf{Z}_n^*$. Also

Wenn $P_n \neq Z_n^*$, dann Fehlerwahrscheinlichkeit nach c Tests höchstens 2^{-c}.

Leider gilt es zusammengesetzte n mit $P_n = Z_n^*$ (Carmichael-Zahlen).

2. Verfeinerungen

(a) Verfeinerte Tests mit Gruppen P_n', wo immer $P_n' \neq Z_n^*$ gilt (Solovay-Strassen, Rabin-Miller).

(b) Andere Gruppen als $\mathbf{Z}_n^*$ (elliptische Kurven).

(c) Suche nach kleinen „Testmengen“ (der Größe $O(m^k)$) für deterministische Verfahren.

3. Erweiterungen von $\mathbf{Z}_n$

Satz 3 *Sei $n \in \mathbf{N}, a \in \mathbf{Z}_n^*$. Dann gilt die Gleichung*

$$(x-a)^n = x^n - a \pmod{n} \qquad (T)$$

genau dann, wenn n eine Primzahl ist.

(T) enthält $n = 2^m$ Terme in expandierter Form, ist also bereits als Datenstruktur exponentiell. Rechne deshalb das Ganze $\pmod{f(x)}$ mit einem (monischen) Polynom $f(x) \in \mathbf{Z}_n[x]$ vom Grad $\deg f(x) = r$, also in $R = \mathbf{Z}_n[x]/(f(x))$.

Für primes n und irreduzibles $f(x)$ ist das der endliche Körper $GF(n^r)$.

Rechnen in R ist so einfach wie Rechnen mit $\mathbf{Z}_n$-Vektoren der Länge r, weil $f(x)$ einer algebraischen Ersetzungsregel für x^r entspricht.

Besonders einfach wird die Rechnung für $f(x) = x^r - a$ und $a \in \mathbf{Z}_n^*$. Es gilt

$$n \text{ prim } \Rightarrow \ (x-a)^n \equiv x^n - a \mod (x^r - 1, n).$$

Gefragt sind Werte (r, a), für welche die Umkehrung dieser Aussage richtig ist.

(3a) Zunächst wurde diese Frage für festes $a = 1$ und variierendes r untersucht.

(3b) Der Durchbruch wurde für variierendes a bei festem r erreicht.

4. Der Satz von [AKS], 14.08.2002

Satz 4 *Für $n \in \mathbf{N}$ seien r, q so gewählt, dass $q | r-1$ und $n^{(r-1)/q} \pmod{r} \notin \{0, 1\}$ gilt.*

Sei weiter S eine genügend große Menge von Restklassen aus $\mathbf{Z}_n$ mit $gcd(n, a - a') = 1$ für alle $a, a' \in S$.

Genügend groß bedeutet dabei ($s = \# S$)

$$\binom{q+s-1}{s} \geq n^{2\lfloor\sqrt{r}\rfloor}.$$

Gilt dann

$$(x-a)^n \equiv x^n - a \mod (x^r - 1, n) \qquad (T_{r,a})$$

für alle $a \in S$, so ist n eine Primzahlpotenz.

Eine Wahl für die Parameter ist z.B. (Existenz von entsprechenden q und r vorausgesetzt):

$$q \geq 4\sqrt{r} \cdot m, \qquad S = \{1, \ldots, s\} \text{ mit } s = 2\sqrt{r} \cdot m, \qquad m = \log_2(n)$$

Beweis:

$$\binom{q+s-1}{s} \geq \left(\frac{q}{s}\right)^s \geq 2^{2\sqrt{r} \cdot m} = n^{2\sqrt{r}}$$

Primtest-Algorithmus

1. Wenn n echte Primzahlpotenz $\Rightarrow$ `return false`
2. Wähle geeignete (q, r, S)
3. Für $a \in S$ prüfe
   (a) Ist $gcd(a, n) > 1 \Rightarrow$ `return false`
   (b) Ist $(x-a)^n \not\equiv x^n - a \mod (x^r - 1, n) \Rightarrow$ `return false`
4. `return true`

Kosten:

1. kann mit Newton-Iteration in polynomialer Laufzeit erledigt werden.

Die größten Kosten verursacht Schritt (3b). Diese sind bei schneller FFT-Arithmetik bis auf logarithmische Faktoren wie das Rechnen mit $\mathbf{Z}_n$-Vektoren der Länge r, also $\tilde{O}(r\, s\, m^2)$

Gesamtkosten sind bei obiger Wahl von s also gerade $\tilde{O}(r^{3/2}\, m^3)$.

Zum Abschluss des Beweises ist damit zu untersuchen, ob es geeignete $r \in m^{O(1)}$ gibt.

Es zeigt sich, dass dazu maximal $O(m^6)$ Zahlen getestet werden müssen.

5. Zur Wahl von q und r

Gesucht sind Primzahlen r, welche einen „großen“ Faktor besitzen.

Dazu wird ein Ergebnis der analytischen Zahlentheorie über die Dichte von Primzahlen r mit großem Faktor von $r-1$ verwendet. Für

$$P(x) = \{r \leq x \ : \ \exists\, q \ (q, r \text{ prim}); (q | r-1); q > x^{2/3}\}$$

gilt

$$\#\, P(x) \gtrsim \pi(x) \sim \frac{x}{\log(x)}.$$

Für den größten Primfaktor q von $r \in P(x)$ gilt $\frac{r-1}{q} < x^{1/3}$.

Wir müssen für [AKS] also solche r ausschließen, die Teiler eines $n^k - 1, k < x^{1/3}$ sein können.

$n^k - 1$ hat bei festem k höchstens $O(k \cdot \log(n))$ Teiler. Also sind insgesamt höchstens $O(x^{2/3}\, \log(n))$ Teiler zu vermeiden.

Es reicht also, x so groß zu wählen, dass

$$x^{2/3}\, \log(n) \gtrsim \frac{x}{\log(n)}, \text{ also } x \gtrsim \log(n)^6$$

gilt, um ein r mit der geforderten zusätzlichen Teilbarkeitseigenschaft zu finden.

6. Zum Beweis des Satzes von [AKS]

Kreisteilungspolynome

In $\mathbf{Z}[x]$ gilt $(x^r - 1) = \prod_{d|r} \Phi_d(x)$.

$\Phi_r(x) = \prod_{a \in \mathbf{Z}_m^*} (x - \zeta^a)$ heißt *r-tes Kreisteilungspolynom* und ist über $\mathbf{Z}$ irreduzibel. ζ ist hier eine primitive r-te Einheitswurzel.

$\Phi_r(x)$ kann aber in $\mathbf{Z}_p[x]$ (p prim) weiter zerfallen.

Beispiel ($p = 2, r = 7$):

$$\Phi_7(x) = (x^6 + \ldots + 1) \equiv (x^3 + x^2 + 1)(x^3 + x + 1) \pmod 2.$$

Genauer gilt (mit $(r, p) = 1$)

$$\Phi_r(x) = h_1(x) \cdot \ldots \cdot h_s(x)$$

mit Polynomen $h_i(x)$ vom Grad $deg\, h_i = d = ord(p \in \mathbf{Z}_r^*)$ und

$$h_i(x) = \prod_{k=0}^{d-1} (x - \zeta^{c_i\, p^k})$$

für geeignete $c_i \in \mathbf{Z}_p^*$.

Der Beweis

Nimm einen Primfaktor $p|n$ mit $p^{(r-1)/q} \pmod r \notin \{0, 1\}$. Damit ist $d = ord(p \in \mathbf{Z}_r^*)$ ein Vielfaches von q.

Nach Voraussetzung ist $(x - a)^n = x^n - a$ in $R = \mathbf{Z}_p[x]/(x^r - 1)$ für alle $a \in S$.

Daraus folgt $(x^{n^i} - a)^n = x^{n^{i+1}} - a$ in $\mathbf{Z}_p[x]/(x^{n^i r} - 1)$ und wegen $(x^r - 1)|(x^{n^i r} - 1)$ auch in R.

Da $f(x^p) = f(x)^p$ generell in $\mathbf{Z}_p[x]$ gilt, folgt $(x - a)^t = x^t - a$ in R für alle $t = n^i p^j$.

Betrachte die $n^i p^j$ mit $0 \le i, j \le \lfloor \sqrt{r} \rfloor$. Dabei ist $n^i p^j < n^{i+j} \le n^{2\lfloor \sqrt{r} \rfloor}$ und es gibt wenigstens $r + 1$ solche Paare (i, j).

Es gibt also $t = n^{i_1} p^{j_1} \ne u = n^{i_2} p^{j_2}$ mit $|t - u| < n^{2\lfloor \sqrt{r} \rfloor}, t \equiv u \pmod r$ und folglich $x^t = x^u$ in R. Damit gilt auch $(x - a)^t = (x - a)^u$ in R für alle $a \in S$.

Sei $h(x) \in \mathbf{Z}_p[x]$ ein irreduzibler Faktor von $\Phi_r(x) = \frac{x^r - 1}{x - 1}$ (dieser hat Grad $d \ge q \ge 2$) und $K = \mathbf{Z}_p[x]/(h(x))$ der Restklassenkörper. Dann gilt $(x - a)^t = (x - a)^u$ für alle $a \in S$ auch in K und $(x - a) \in K^*$ aus Gradgründen.

Betrachte die Gruppe $G \subset K^*$, die von $\{x - a \ : \ a \in S\}$ erzeugt wird. Dann gilt $g^t = g^u$ für alle $g \in G$.

G hat wenigstens $\binom{q+s-1}{s} \ge n^{2\lfloor \sqrt{r} \rfloor} > |t - u|$ Elemente:

> Die Produkte $\prod_{a \in S} (x - a)^{e_a}$ mit $\sum_{a \in S} e_a < q$ sind paarweise verschieden (sie sind verschieden in $\mathbf{Z}_p[x]$ und haben alle einen Grad $< q \le d = deg\, h(x)$).

Also gilt $t = u$ und damit $n = p^k$ mit $k = \dfrac{j_2 - j_1}{i_2 - i_1}$.

Literatur

[1] D. J. Bernstein: Proving primality after Agrawal-Kayal-Saxena. Version vom 25.01.2003, `http://cr.yp.to/papers.html#aks`

[2] F. Bornemann: Ein Durchbruch für „Jedermann“. DMV-Mitteilungen 4/2002, S. 14-21 (und die Literaturliste dort)

[3] S. Wehmeier: Der AKS-Primzahltest. Notizen zum Seminarvortrag, 16.12.2002, `http://math-www.uni-paderborn.de/~stefanw`