Der indische Primzahltest (Primes is in $\mathcal{P}$)

Seminarvortrag

Eberhard Oeljeklaus

Im Sommer 2002 wurde bekannt, daß die indischen Mathematiker M. Agrawal, N. Kayal und N. Saxena gemeinsam einen deterministischen Algorithmus entwickelt haben, welcher für jede natürliche Zahl n in polynomialer Laufzeit entscheiden kann, ob n eine Primzahl ist. Sie haben damit ein berühmtes Problem der Komplexitätstheorie gelöst, bekannt in der Formulierung: *Is Primes in $\mathcal{P}$?* Der Begriff polynomiale Laufzeit bezieht sich auf die Länge (Stellenzahl) von n. Das Ergebnis lautet genauer: :
Es gibt einen deterministischen Algorithmus, der für jede Zahl $n \in \mathbb{N}$ in höchstens $O(log^{\kappa} n)$ Rechenschritten entscheidet, ob n eine Primzahl ist. Der Exponent κ ist eine von n unabhängige positive Zahl.
Wir wollen in diesem Vortrag das theoretische Ergebnis der genannten Mathematiker vorstellen, welches die Grundlage für ihren Algorithmus bildet. Eine wesentliche Rolle für den Beweis des theoretischen Resultats spielt der folgende Satz von E. Fouvry (Invent. math. 79, 383-407(1985)) über die Verteilung von Primzahlen mit speziellen Eigenschaften.
Für alle $n \in \mathbb{N}, n \geq 2,$ sei $P(n)$ der größte Primteiler von n.

Satz 1. (Fouvry): *Es gibt ein $n_0 \in \mathbb{N}$, so dass für alle $n \geq n_0$ gilt:*

$$\# \left\{ p \in \mathbb{N} \mid p\ prim, p \leq n, P(p-1) \geq \sqrt[3]{n^2} \right\} \geq \frac{2}{3}\ \frac{n}{\log n}.$$

Diese Abschätzung war bereits in den achtziger Jahren ein wichtiger Baustein für das folgende Ergebnis im Zusammenhang mit dem Fermat-Problem: Sind $x, y, z \in \mathbb{N}$, so gilt für unendlich viele Primzahlen p : Besteht eine Gleichung $x^p + y^p = z^p$, so ist p ein Teiler des Produktes xyz.
Der Satz von Fouvry wird in unserem Zusammenhang benötigt, um das folgende Lemma zu beweisen:

Lemma 1. *Es gibt ein $n_1 \in \mathbb{N}$, so dass für alle $n \geq n_1$ gilt:*
Das Intervall $[(4\log n)^6,\ 15 \cdot (4\log n)^6]$ enthält eine Primzahl r mit der Eigenschaft

$$ggT\ (r, n) = 1,\ q := P(r-1) \geq 4\sqrt{r}\log n, \quad n^{\frac{r-1}{q}} \not\equiv 1\ mod\ r.$$

Für $x \in \mathbb{R}$ sei $\pi(x) := \#\{p \in \mathbb{N} \mid p \text{ prim},\ p \leq x\}$. Zum Beweis des Lemmas benötigen wir die folgende Ungleichung von Tschebyschew (1852):
Für alle $x \in \mathbb{R},\ x \geq 2,$ gilt:

$$\frac{x}{6\log x} \leq \pi(x) \leq \frac{8x}{\log x}.$$

(vgl. A. Leutbecher: Zahlentheorie, Springer Verlag Berlin, 1996, S. 28).

Beweis des Lemmas. Sei $n_0 \in \mathbb{N}$ wie im Satz von Fouvry gewählt.
Sei $n \in \mathbb{N},\ n \geq n_0$.

Es sei $x := 15(4\log n)^6$, und für $\alpha > 0$ sei
$S_\alpha := \{r \in \mathbb{N} \mid r \text{ prim},\ \alpha \leq r \geq x,\ P(r-1) \geq \sqrt[3]{x^2}\}$,
$S := S_{(4\log n)^6}$.
Wir geben zunächst eine Abschätzung für die Anzahl der Elemente in der Menge S. Es gilt:

$$\begin{aligned} \#S &\geq \#S_1 - \pi((4\log n)^6) \\ &\geq \tfrac{2}{3} \cdot \tfrac{15(4\log n)^6}{\log(15\cdot(4\log n)^6)} - \pi((4\log n)^6) && (Fouvry) \\ &\geq \tfrac{10\cdot 4^6\cdot(\log n)^6}{\log 15 + 6\log 4 + 6\log\log n} - \tfrac{8\cdot 4^6(\log n)^6}{6\log 4 + 6\log\log n} && (Tschebyschew) \end{aligned}$$

Es gibt also ein $n_2 \in \mathbb{N}$, so dass für $n \geq n_2$ gilt:

$$\begin{aligned} \#S &\geq \tfrac{10\cdot 4^6(\log n)^6}{7\log\log n} - \tfrac{8\cdot 4^6(\log n)^6}{6\log\log n} \\ &= 4^6(\tfrac{10}{7} - \tfrac{4}{3})\ \tfrac{(\log n)^6}{\log\log n} \\ &= \tfrac{4^6\cdot 2}{21}\ \tfrac{(\log n)^6}{\log\log n}. \end{aligned}$$

Nun sei für $1 \leq k \in \mathbb{N}$:

$$N(k) :=\ n \cdot \prod_{\nu=1}^{k}(n^\nu - 1).$$

Wir wollen zeigen, dass die Anzahl der Primfaktoren von $N(k)$ kleiner ist als die Anzahl der Elemente von S. Sei allgemein $A(m)$ die Anzahl der Primfaktoren von $m \in \mathbb{N}, m \geq 2$. Eine leichte Rechnung zeigt, dass $A(m) \leq \log_2 m$ ist.

Wir beweisen zunächst, dass $A(N(k)) \leq k^2 \log n$ ist für $k \geq 5$: Wegen

$$A(n^\nu - 1) \leq \log_2(n^\nu - 1) < \log_2 n^\nu = \nu \cdot \log_2 n$$

ist

$$A(N(k)) < \log_2 n + \sum_{\nu=1}^{k} \nu \log_2 n = (1 + \frac{k}{2}(k+1))\log_2 n = (1 + \frac{k}{2}(k+1))\frac{\log n}{\log 2}$$

$$= (\frac{k^2 + k + 2}{2\log 2})\log n \leq k^2 \log n$$

für $k \geq 5$.
Für $k := \lfloor \sqrt[3]{x} \rfloor$ folgt daher:

$$A(N(\lfloor \sqrt[3]{x} \rfloor) \leq \sqrt[3]{x^2}\log n \leq 4^4\sqrt[3]{15^2}(\log n)^5.$$

Es gibt ein $n_3 \in \mathbb{N}$, so dass für alle $n \geq n_3$ gilt:

$$\#S \geq \frac{4^6 \cdot 2}{21} \frac{(\log n)^6}{\log\log n} > 4^4 \sqrt[3]{15^2} \cdot (\log n)^5 \geq A(N(\lfloor \sqrt[3]{x} \rfloor)).$$

Es gibt somit eine Primzahl $r \in S$, welche die Zahl $N(\lfloor x^{\frac{1}{3}} \rfloor)$ nicht teilt. Diese Zahl r hat die Eigenschaft:

$$\mathrm{ggT}(r,n) = 1,\ (4\log n)^6 \leq r \leq x,\ q := P(r-1) \geq x^{\frac{2}{3}} \geq r^{\frac{2}{3}}.$$

Es folgt: $\quad q \geq r^{\frac{2}{3}} = r^{\frac{1}{2}} \cdot r^{\frac{1}{6}} \geq r^{\frac{1}{2}}(4\log n).$

Weil r die die Zahlen $n^\nu - 1, 1 \leq \nu \leq \lfloor x^{\frac{1}{3}} \rfloor$, nicht teilt, und weil

$$\frac{r-1}{q} \leq \frac{r-1}{r^{\frac{2}{3}}} < r^{\frac{1}{3}} \leq x^{\frac{1}{3}}$$

und $\frac{r-1}{q} \in \mathbb{N}$ ist, erhalten wir $\frac{r-1}{q} \leq \lfloor x^{\frac{1}{3}} \rfloor$, also $n^{\frac{r-1}{q}} \not\equiv 1 \mathrm{mod}\ r.$ $\square$

Für $n \in \mathbb{N}, n \geq 2$, setzen wir

$S(n) := \{r \mid r$ Primzahl $, r \nmid n, r \leq 15(4\ \log n)^6, q := P(r-1) \geq 4\sqrt{r}\log n, n^{\frac{r-1}{q}} \not\equiv 1 \bmod r\}.$

Das Lemma besagt, dass es ein $n_1 \in \mathbb{N}$ gibt mit $S(n) \neq \emptyset$ für alle $n \geq n_1$.
Es gilt der folgende

Satz 2. *(Agrawal-Kayal-Saxena, 2002)*
Es sei $r \in S(n)$. Wenn für alle $a \in \mathbb{N}$ mit $1 \leq a < 2\sqrt{r}\ \log n$ die Beziehungen

1) $ggT(a,n) = 1$,

2) $(x-a)^n \equiv x^n - a \bmod ((x^r - 1)\mathbb{Z}[X] + n\mathbb{Z}[X])$,

gelten, dann ist $n = p^k$ für eine Primzahl $p \geq 2\sqrt{r}\ \log n$ und $k \in \mathbb{N}$.
Umgekehrt gilt: Ist n eine Primzahl, so sind die Bedingungen 1) und 2) für jedes $a \in \mathbb{N}, 1 \leq a < n$, und alle $r \in \mathbb{N}$ erfüllt.

Beweis. Um die erste Aussage des Satzes zu beweisen, nehmen wir an, dass die Bedingungen 1) und 2) für ein $r \in S(n)$ mit $q := P(r-1)$ erfüllt seien. Es gibt dann einen Primteiler p von n mit der Eigenschaft $p^{\frac{r-1}{q}} \not\equiv 1 \bmod r$. Weil $1 = \mathrm{ggT}(n,r) = \mathrm{ggT}(p,r)$ ist, gilt nach dem kleinen Satz von Fermat:
$p^{r-1} \equiv 1 \bmod r$.
Daraus folgt:

$$q \mid \mathrm{ord}_r p, \quad \text{wobei } \mathrm{ord}_r p := \min\{k \in \mathbb{N} \mid k \geq 1, p^k \equiv 1 \bmod r\}.$$

Weiter gilt wegen $(1 + \lfloor\sqrt{r}\rfloor)^2 > r$: Es gibt $(i_1, j_1), (i_2, j_2) \in \{0,1,2,...,\lfloor\sqrt{r}\rfloor\} \times \{0,1,2,...,\lfloor\sqrt{r}\rfloor\}, (i_1,j_1) \neq (i_2,j_2)$, so dass

$$t_1 := n^{i_1} p^{j_1} \equiv n^{i_2} p^{j_2} (=: t_2) \mathrm{mod}\ r$$

ist. Sei etwa $t_1 \geq t_2 = t_1 - cr$ für ein $c \in \mathbb{N}$.
Wegen $\mid j_1 - j_2 \mid < 2\lfloor\sqrt{r}\rfloor < q$ ist $\mid j_1 - j_2 \mid < \mathrm{ord}_r p$ und damit $i_1 \neq i_2$.

Wir werden zeigen, dass $t_1 = t_2$ ist, und das liefert $1 \neq n^{i_1 - i_2} = p^{j_2 - j_1}$, also $n = p^k$ für ein $k \in \mathbb{N}$.
Weil p ein Teiler von n ist, gilt gemäß 1), dass $\mathrm{ggT}(a,p) = 1$ ist für alle $1 \leq a < 2\sqrt{r}\log n$. Gemeinsam mit 2) liefert dies

$$(x-a)^{p^{j_\nu}} \equiv x^{p^{j_\nu}} - a \bmod ((x^r - 1)\mathbb{Z}[x] + p\mathbb{Z}[x])$$
$$(x-a)^{n^{i_\nu}} \equiv x^{n^{i_\nu}} - a \; mod((x^r - 1)\mathbb{Z}[x] + p\mathbb{Z}[x]), \qquad \nu = 1, 2,$$

also

$$(x-a)^{t_\nu} \equiv x^{t_\nu} - a \; mod((x^r - 1)\mathbb{Z}[x] + p\mathbb{Z}[x]), \qquad \nu = 1, 2.$$

Daraus folgt

$$\begin{aligned}(x-a)^{t_1} &\equiv (x-a)^{t_2} + (x^{t_1} - x^{t_2}) \; mod((x^r - 1)\mathbb{Z}[x] + p\mathbb{Z}[x]) \\ &\equiv (x-a)^{t_2} + x^{t_2}(x^{cr} - 1) \; mod((x^r - 1)\mathbb{Z}[x] + p\mathbb{Z}[x]) \\ &\equiv (x-a)^{t_2} + x^{t_2}(x^r - 1)\sum_{\alpha=0}^{c-1} x^\alpha \; mod((x^r - 1)\mathbb{Z}[x] + p\mathbb{Z}[x]) \\ &\equiv (x-a)^{t_2} \; mod((x^r - 1)\mathbb{Z}[x] + p\mathbb{Z}[x])\end{aligned}$$

Da diese Beziehung für alle $a \in \mathbb{N}$ mit $1 \leq a \leq l := \lfloor 2\sqrt{r}\log n \rfloor$ gilt, ergibt sich

$$\left(\prod_{1 \leq a \leq \ell} (x-a)^{m_a}\right)^{t_1} \equiv \left(\prod_{1 \leq a \leq \ell} (x-a)^{m_a}\right)^{t_2} \bmod ((x^r - 1)\mathbb{Z}[x] + p\mathbb{Z}[x])$$

für alle $m_a \in \mathbb{N}$.
Es sei

$$T := \left\{ \prod_{1 \leq a \leq \ell} (x-a)^{m_a} \mid \sum_{1 \leq a \leq \ell} m_a \leq ord_r p - 1 \right\} \subset \mathbb{Z}[X].$$

Dann ist
$(*)$ $\qquad \#T = \binom{\ell + ord_r p - 1}{\ell} > 2^{ord_r p - 1} \geq 2^{q-1}$

wegen $q \mid \mathrm{ord}_r p$ und weil allgemein gilt für $d, \ell \in \mathbb{N}, d \geq 1, \ell \geq 2$:

$$\#\{(s_1, ..., s_\ell) \in \mathbb{N}^\ell \mid \sum_{i=1}^{\ell} s_i \leq d\} = \binom{\ell + d}{\ell} > 2^d.$$

Wir betten nun T in die (zyklische) multiplikative Gruppe eines endlichen Körpers ein, um eine Abschätzung von $\#T$ nach unten zu erhalten. Diese Abschätzung wird sich unter der Annahme $t_1 > t_2$ als unverträglich zu $(*)$ erweisen, womit dann $t_1 = t_2$ gezeigt ist.

Es sei ζ eine primitive r-te Einheitswurzel und

$$\Phi_r(x) = \frac{x^r - 1}{x - 1} = \sum_{i=0}^{r-1} x^i = \prod_{\nu=1}^{k} f_\nu \in \mathbb{F}_p[X],\ \mathbb{F}_p := \mathbb{Z}/p\mathbb{Z},$$

eine Zerlegung des Kreisteilungspolynoms Φ_r in irreduzible Faktoren $f_1, ..., f_k \in \mathbb{F}_p[X]$. Sei etwa $f := f_1$ das Minimalpolynom von ζ in $\mathbb{F}[X]$. Wegen grad$f = ord_r p$ ist $k := \mathbb{F}_p[X]/f\mathbb{F}_p[X]$ ein Körper mit $p^{\mathrm{ord}_r p}$ Elementen. Wir betrachten den kanonischen Ringepimorphismus

$$\psi : \mathbb{Z}[X] \xrightarrow{\psi_1} \mathbb{F}_p[X] \xrightarrow{\psi_2} K.$$

Offensichtlich ist $\psi(x^r - 1) = 0 = \psi(p)$. Für $1 \leq a \leq \ell$ gilt:

$$(x-a)^{t_1} - (x-a)^{t_2} = (h_1(x^r - 1) + ph_2), \qquad h_1, h_2 \in \mathbb{Z}[X].$$

Daher folgt

$$\psi((x-a)^{t_1} - (x-a)^{t_2}) = \psi(h_1)\psi(x^r - 1) + \psi(p)\psi(h_2) = 0,$$

also

$$(\psi(x-a))^{t_1} = (\psi(x-a))^{t_2}$$

und damit auch

$$(\psi(g))^{t_1} = (\psi(g))^{t_2}$$

für alle $g \in T$. Die Abbildung

$$\psi_{|T} : T \to K^* = K \backslash \{0\}$$

ist außerdem injektiv, wie wir jetzt sehen werden. Wir bemerken zunächst: Ist $g = \prod_{1 \leq a \leq \ell} (x-a)^{m_a} \in T$ und gilt für ein $a_0 \in \{1, 2, ..., \ell\}$ die Beziehung $p \mid g(a_0)$, so folgt $g(a_0) = 0$ wegen $\mid a_0 - a \mid < p$ für $1 \leq a \leq \ell$.

Seien $g_1, g_2 \in T$ mit $\psi(g_1) = \psi(g_2)$, also $\psi(g_1 - g_2) = \psi_2 \circ \psi_1(g_1 - g_2) = 0$. Dann ist $\psi_1(g_1 - g_2) = 0$, denn wegen grad $\psi_1(g_1 - g_2) \leq$ord$_r p - 1 <$grad f wäre sonst $\psi_2(\psi_1(g_1 - g_2)) \neq 0$. Mithin ist $g_1 - g_2 \in p\mathbb{Z}[X]$, und somit haben g_1 und g_2 nach der obigen Bemerkung die gleichen Nullstellen. Sei etwa $g_1 = (x-a)^{m_a} \cdot h_1, g_2 = (x-a)^{n_a} h_2$ mit $m_a \geq n_a \geq 1$ und $h_2(a) \neq 0$. Dann folgt $g_1 - g_2 = (x-a)^{n_a}((x-a)^{m_a - n_a} h_1 - h_2) \in p\mathbb{Z}[X]$.

Weil $p\mathbb{Z}[X]$ ein Primideal in $\mathbb{Z}[X]$ ist, folgt hieraus $(x-a)^{m_a - n_a} h_1 - h_2 \in p\mathbb{Z}[X]$. Also haben h_2 und $(x-a)^{m_a - n_a} h_1$ die gleichen Nullstellen, und somit ist $m_a = n_a$ wegen $h_2(a) \neq 0$. Insgesamt ist damit gezeigt, dass $g_1 = g_2$ ist.

Zusammenfassend stellen wir fest: $\psi(T)$ ist eine Teilmenge von K^*, und es ist $\#\psi(T) = \#T, g^{t_1 - t_2} = 1$ für alle $g \in \psi(T)$; insbesondere ist ord g ein Teiler von $t_1 - t_2$.
Die Menge $\psi(T)$ erzeugt eine zyklische Untergruppe G der multiplikativen Gruppe K^*, daher gilt also ord $G \mid (t_1 - t_2)$. Wir wollen zeigen, dass $t_1 = t_2$ ist und schließen indirekt. Wäre $t_1 > t_2$, so erhielten wir

$2^{q-1} < \#T = \#\psi(T) \leq$ord $G \leq t_1 - t_2$,

$$t_1 - t_2 = n^{i_1}p^{j_1} - n^{i_2}p^{j_2} \leq n^{\lfloor\sqrt{r}\rfloor}p^{\lfloor\sqrt{r}\rfloor} \leq n^{\lfloor\sqrt{r}\rfloor}n^{\lfloor\sqrt{r}\rfloor} = n^{2\lfloor\sqrt{r}\rfloor},$$

also insgesamt

$$2^{q-1} < n^{2\lfloor\sqrt{r}\rfloor}, \text{ d.h. } (q-1)\log 2 < 2\lfloor\sqrt{r}\rfloor \log n.$$

Nach Voraussetzung ist aber $q \geq 4\sqrt{r}\log n$, und somit hätten wir die Ungleichung

$$(4\sqrt{r}\ \log n - 1)\ \log 2 < 2\sqrt{r}\ \log n,$$

die aber wegen $\log 2 > \frac{69}{100}$ und $\sqrt{r}\log n > 1$ nicht bestehen kann. Mithin ist $t_1 = t_2$ und der Satz bewiesen. □