Ungelöste Probleme der Zahlentheorie

Teil 7: Die (GRH) und Primzahltests

Aus Teil 6:
Die (GRH) für die L-Fkt. $L(s,\chi)$ zu dem Dirichlet-Charakter χ mod k besagt, dass alle Nullstellen $L(s,\chi)$ im Streifen $0 < \operatorname{Re} s < 1$ den Realteil $\frac{1}{2}$ haben.

Wir geben nun einen in der Praxis schnellen Primzahltest an, der nachweislich schnell ist, falls die (GRH) stimmt.
Dazu stellen wir erst ein wenig Theorie über quadratische Nichtreste zusammen.

Legendre-Symbol

Für $p > 2$ prim sei $n_2(p) := \min\{a \in \{1,\dots,p-1\};\ \left(\frac{a}{p}\right) = -1\}$
der kleinste quadratische Nichtrest mod p. (qNR)

Die Gleichung $\sum_{a=1}^{p-1} \left(\frac{a}{p}\right) = 0$ zeigt, dass $n_2(p) \leq \frac{p-1}{2}$ ist.

Die Pólya-Vinogradov-Unglg. $\sum_{1 \leq a \leq x} \left(\frac{a}{p}\right) = O(p^{\frac{1}{2}} \log p)$ zeigt $n_2(p) = O(p^{\frac{1}{2}e^{-1/2}+\varepsilon})$, $\varepsilon > 0$ bel.

Die bislang beste Abschätzung für $n_2(p)$ ist $n_2(p) = O(p^{\frac{1}{4}e^{-1/2}+\varepsilon})$
(D. Burgess, 1957).

Wir zeigen nun:
Die (GRH) für den Charakter $\chi = \left(\frac{\cdot}{p}\right)$ (d.h. die dazugehörige L-Fkt.) verschärft dies zu:

$$n_2(p) = O(\log^2 p).$$

Sagen wir mal, die implizite Konstante hier sei $c_1 > 0$.

Das heißt, durch Probieren der ersten $C_1 \log^2 p$ vielen $a \geq 1$ trifft man auf einen quadratischen Nichtrest mod p, wenn die (GRH) stimmt; darauf kann man sich in der Praxis natürlich verlassen:
Wenn man bis $C_1 \cdot \log^2 p$ keinen qu. NR gefunden haben sollte, kann demnach die (GRH) für den Charakter $\chi = (\frac{\cdot}{p})$ nicht stimmen!

Genaue Formulierung:

Satz von Ankeny-Montgomery (1952):

Sei $\chi \neq \chi_0$ ein Charakter mod k. Es gelte für $L(s,\chi)$ die Riemannsche Vermutung. Dann ex. mit einer absoluten, berechenbaren Konstanten C_1 ein $n \leq C_1 \log^2 k$ mit $\chi(n) \neq 0$ und $\chi(n) \neq 1$.

(Für χ reell ist dann $\chi(n) = -1$.)

Hinweis zum Beweis:

Es besteht die explizite Formel:

$$\underbrace{\sum_{p \leq x} \left(1 - \frac{p}{x}\right) \chi(p) \log p}_{\substack{\text{Mit } x = A\log^2 k \text{ mit } A \text{ groß} \\ \text{und } \chi(p) \in \{0,1\} \text{ für alle } p \leq x}} = \underbrace{- \sum_{\substack{\varrho \in \mathbb{C} \\ L(\varrho,\chi)=0}} \frac{x^\varrho}{\varrho(\varrho+1)}}_{\substack{\text{stimmt die (GRH),} \\ \text{ist dies } = O(x^{1/2} \log k)}} + O(x^{1/2}) + O(\log k).$$

folgte, dass dies $\geq C \cdot x$ wäre, $C > 0$, im $\lightning$ zur oberen Absch. mit der (GRH).
(Es gibt höchstens $O(\log k)$ PZen $p \leq x$, die k teilen)
Beachten, dass $x = O(x^{1/2} \log k)$ für kleinere x keinen $\lightning$ liefert! $\square$

Nun zu der Frage, wie dieser Satz bei PZtests zum Einsatz kommt:
Gegeben sei eine (große) natürliche Zahl n mit $O(\log n)$ vielen Ziffern (in irgendeinem Ziffernsystem, für den Computer am besten im Binär- oder Hexadezimalsystem). Es soll mit einem möglichst schnellen algorithmischen Verfahren entschieden werden, ob n prim oder zusammengesetzt ist, zumindest in einer polynomiellen Laufzeit $O((\log n)^c)$ für ein $C > 0$.

Ein mögliches Testverfahren ist folgender

$\left(\frac{a}{n}\right)$: Jacobi-symbol

Solovay-Strassen-Primzahltest: Für $n>1$, $2\nmid n$, sind äquivalent:

(i) n ist prim, (ii) $\forall a\in\mathbb{Z}_n^*$: $a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \bmod n$.

$\left(\mathbb{Z}_n^* := \{a\in\{1,\dots,n-1\};\ (a,n)=1\}\right)$

Bew.: (i) $\Rightarrow$ (ii) ist der Satz von Euler (vgl. elementare ZT),

(ii) $\Rightarrow$ (i): 1.) Beh.: $\forall a\in\mathbb{Z}_n^*$: $a^{n-1}\equiv 1\,(n) \Rightarrow n$ quadratfrei.

Sei $p^t \,\|\, n$ und g eine Primitivwurzel mod p^t, d.h. $\langle g\rangle = \mathbb{Z}_{p^t}^*$.

(die $\mathbb{Z}_{p^t}^*$ sind zyklische Gruppen)

CRS = Chinesischer Restsatz

$\overset{CRS}{\Longrightarrow} \exists a\in\mathbb{Z}_n^*$: $a\equiv g \bmod p^t$ & $a\equiv 1 \bmod \frac{n}{p^t}$. Nach Vor.: $a^{n-1} = g^{n-1}\equiv 1 \bmod p^t$.

Somit: $\mathrm{ord}_{p^t}(g) = \varphi(p^t) = p^{t-1}(p-1) \mid (n-1)$,

für $t>1$ zeigt dies $p \mid (n-1)$ im ↯ zu $p\mid n$.

2.) Wegen (ii) und 1.) ist n quadratfrei, etwa $n=p_1\cdots p_r$ mit $2<p_1<\dots<p_r$,

Ann.: $r\geq 2$. Dann wähle a mit $\left(\frac{a}{p_1}\right)=-1$ und sei $x\in\mathbb{Z}_n^*$ mit

$x\equiv a\,(p_1)$, $x\equiv 1\,(p_j)$ für $2\le j\le r$.

Jacobi-Symbole! →

Dann ist $\left(\frac{x}{n}\right) = \left(\frac{x}{p_1}\right)\cdots\left(\frac{x}{p_m}\right) = \left(\frac{a}{p_1}\right)\cdot\left(\frac{1}{p_2}\right)\cdots\left(\frac{1}{p_m}\right) = -1$.

Nach (ii) ist

$\left(\frac{x}{n}\right)\equiv x^{\frac{n-1}{2}}\,(n)$, also $x^{\frac{n-1}{2}}\equiv -1\,(n)$, insb. $x^{\frac{n-1}{2}}\equiv -1\,(p_2)$

im ↯ zu $x^{\frac{n-1}{2}} \equiv 1^{\frac{n-1}{2}} \equiv 1\,(p_2)$. □

Der Solovay-Strassen-Test taugt in dieser Form nicht für die Praxis, da alle $a\in\mathbb{Z}_n^*$ (und das sind $\varphi(n)$ viele, für n prim also $\varphi(n)=n-1$) getestet werden müssen. Mit der (GRH) kann die Zahl der a gedrückt werden:

Satz: Sei $n>1$, $2\nmid n$, es gelte die (GRH) für alle reellen Charaktere $\chi\neq\chi_0$ zum Modul n. Weiter gelte: $\forall a\in\mathbb{Z}_n^*$, $1\le a\le C_1\log^2 n$: $a^{\frac{n-1}{2}}\equiv\left(\frac{a}{n}\right) \bmod n$. Dann ist n prim. (C_1 aus A-M.)

A-M = Ankeny-Montgomery

Bew.: Ann.: n nicht prim. Betr. den Charakter $\chi:\mathbb{Z}_n^*\to\{1,-1\}$, $\chi(a):=a^{\frac{n-1}{2}}\left(\frac{a}{n}\right) \bmod n$

S-S = Solovay-Strassen

(und den zugeh. Zahlcharakter χ), $\chi\neq\chi_0$ wegen S-S. Nach A-M. ex. ein $a\in\mathbb{Z}_n^*$, $a\le C_1\log^2 n$ mit $\chi(a)=-1$, also $a^{\frac{n-1}{2}}\equiv -\left(\frac{a}{n}\right) \bmod n$, im ↯ zur Vor. des Satzes. □

Bem.: ist $\chi : \mathbb{Z} \to \mathbb{C}$ multiplikativ, $\chi(m)=0$ genau für m mit $(m,k)>1$, so ist $|\chi(m)|=1$ für $(m,k)>1$.

⌈ Ist $m^\ell = 1$ mit $\ell = \mathrm{ord}_k(m)$, so ist $|\chi(m)|^\ell = |\chi(m^\ell)| = |\chi(1)| = 1$, also $|\chi(m)|=1$. ⌋

Reelle Charaktere nehmen daher nur Werte $\in \{1,-1,0\}$ an.

Die folgende Verfeinerung des Solovay-Strassen-Tests liefert einen in der Praxis schnellen probabilistischen Test:

Satz (Rabin): Sei $n \geq 3$ ungerade, $n-1 = 2^t \cdot u$, u ungerade.

Für alle a mit $(a,n)=1$ gelte $a^u \equiv 1$ oder $\exists \ell \in \{0,\dots,t-1\}: a^{2^\ell u} \equiv -1 \bmod n$. ⊛

Dann ist n prim.

Ist umgekehrt n nicht prim, so gilt für die Menge

$A := \{a;\ 0<a<n,\ (a,n)=1,\ ⊛ \text{ gilt}\}$ dann $\#A \leq \frac{1}{4}\cdot\varphi(n)$.

[Beweis vgl. Satz 12.4., [Forster: Algorithmische ZT]]

Dieser Satz ist die Grundlage für den probabilistischen Rabin-Test (1980):

Geg. $n \geq 3$ ungerade. Wähle eine Zufallszahl $1<a<n$, $(a,n)=1$, und prüfe damit ⊛.

Gilt ⊛ nicht, so ist n zusammengesetzt. ("a ist Zeuge für die Nicht-Primheit von n")

Andernfalls ist n mit einer Fehlerwahrscheinlichkeit $\leq \frac{1}{4}$ prim.

Wiederholtes, zufälliges Testen einer Zufallszahl a drückt diese Fehlerwahrscheinlichkeit wiederum um $\frac{1}{4}$, usw. Da $(\frac{1}{4})^j$ schnell gegen 0 geht, reichen wenige Test-a für eine vernünftige Fehler-W. Mit der Aussage, n ist mit Wahrscheinlichkeit $\leq (\frac{1}{4})^j$ nicht prim, ist man dann in der Praxis auch zufrieden.

W. = Wahrscheinlichkeit

PZ-Tests werden in der Kryptographie vor allem auch zur Erzeugung von PZen benutzt: Wähle zufällig eine große Zahl n, nicht durch alle kleine PZen teilbar. Teste dann mit einem schnellen PZ-Test, ob diese prim bzw. "primgenug" ist. = (wahrscheinlich prim)

Mit zwei großen PZen p, q (etwa gleicher Größe) kann dann ein RSA-Modul $p \cdot q$ erzeugt werden.

Def.: Eine Zahl $n \geq 3$ heißt starke Pseudoprimzahl zur Basis a, wo $(a,n)=1$, falls $\otimes$ gilt.

Bsp.: $n = 2^{400} - 593$, $k := 100$. Der Rabin-Test zeigte:
n ist mit W. $\leq \left(\frac{1}{4}\right)^{100} < 10^{-60}$ keine PZ.
(Mit deterministischen Test wurde später auch $n \in \mathbb{P}$ bestätigt.)

Ist $W(n)$ die kleinste Zahl a mit $1 < a < n$, $(a,n)=1$, so, dass $\otimes$ nicht gilt (d.h. Zeuge, W wie "witness" für die Nicht-Primheit), so kann gezeigt werden:

Satz: Gilt die (GRH), so ist $W(n) \leq 2\log^2(n)$ für alle zusammengesetzten $n \geq 3$.

Im Jahr 2003 wurde ein deterministischer PZ-Test entdeckt, der polynomiell schnelle Laufzeit hat: von den drei indischen Mathematikern Agrawal, Kayal und Saxena. Dieser Test heißt AKS-Test und beantwortete die bis dahin offene Frage nach der Existenz eines solchen Test.
Die Entscheidung, ob n prim ist oder nicht, ist demnach ein P-Problem.
("P" für in polynomieller Zeit entscheidbar, eine Komplexitätsklasse. Eine wichtige, ungelöste Vermutung der Komplexitätstheorie lautet "P ≠ NP" ...)

Der AKS-Test ist leicht zugänglich, aber für die Praxis bislang ohne Relevanz, wo bis heute die probalistischen Tests benutzt werden.

Der AKS-Test ist wie folgt durchführbar:

1. Schritt: Entscheide, ob n eine echte Potenz $n = p^k$ zu einer Primzahlbasis p ist.
2. Schritt: Wähle (q,r,s) mit $(q,n)=(r,n)=1$, $s \leq n$, $q \mid r-1$, $n^{(r-1)/q} \not\equiv 0,1 \pmod r$ und $\binom{q+s-1}{s} \geq n^{2\lfloor\sqrt{r}\rfloor}$ (Problem bei der Laufzeit; s nicht zu groß!)
3. Schritt: Für $a = 1, \ldots, s-1$: (i) ist $a \mid n$, gehe zu 5., (ii) ist $(X+a)^n \not\equiv X^n + a \pmod{X^r - 1, n}$, gehe zu 5.
4. Schritt: Ausgabe: "n ist prim"
5. Schritt: Ausgabe: "n ist zusammengesetzt".

kongruent in: $\mathbb{Z}_n[X]/(X^r - 1)$.