Übungen zur Vorlesung Angewandte Diskrete Mathematik

Institut für Reine Mathematik WS 08/09 – Blatt 06 (Lösung)

Abgabetermin: Freitag, 28.11.2008 um 14:15 Uhr vor Beginn der Übung

---

1. Sei N von der Größenordnung 10^{200}. Sie suchen Primzahlen, die nahe bei N liegen. Dazu durchsuchen Sie das Intervall von N bis $N+b$.

   (a) Wie groß würden Sie b wählen, um mit großer Wahrscheinlichkeit mindestens eine Primzahl zwischen N und $N+b$ zu finden? (2 P)

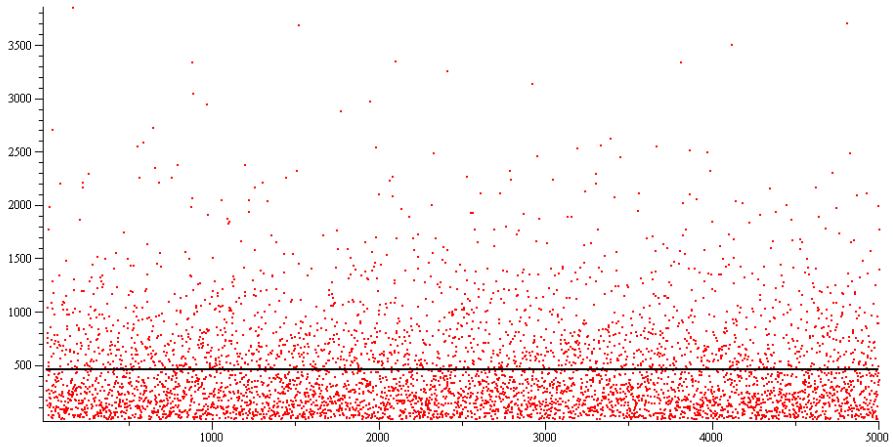
   Lösung: Gesucht ist also ein b, so dass $\pi(N+b)-\pi(N) \geqslant 1$; dabei ist π die Primzahlzählfunktion. Es ist ungefähr $\pi(N) \approx N//\log(N)$, und $\pi(N+b) \approx (N+b)/\log(N+b)$. Falls b im Vergleich zu N klein ist, gilt $\log(N+b) \approx \log(N)$, also $\pi(N+b) \approx (N+b)/\log(N)$. Setzen wir diese Asymptotik in unsere Bedingung ein, so erhalten wir

   $$1 = \frac{N+b}{\log(N)} - \frac{N}{\log(N)} = \frac{b}{\log(N)}.$$

   Man sollte also ungefähr $b = \log(N)$ wählen. In unserem Fall:

   $$\log(10^{200}) = 200 \cdot \log(10) \approx 200 \cdot 2,3 = 460.$$

   Zum Vergleich: Im der folgenden Grafik sieht man für die ersten 5000 Primzahlen ab 10^{200} die Abstände zwischen zwei aufeinanderfolgenden Primzahlen aufgetragen. Der Anteil derjenigen Abstände, die unter 460 liegen, beträgt ungefähr 62%. Im Mittel liegen allerdings ca. $0,996$ Primzahlen in einem Intervall der Länge 460. Obwohl die Abstände stark schwanken und oft oberhalb von 460 liegen, ist 460 damit eine sehr gute Näherung für den *mittleren* Abstand; bzw. die relative Häufigkeit der Primzahlen der Größenordnung 10^{200}.



   (b) Angenommen, Sie haben alle Zahlen zwischen N und $N+b$ schon auf Teilbarkeit durch 2, 3, 5 und 11 überprüft. Wie viele Zahlen (ungefähr) sind noch Kandidaten für Primzahlen? (2 P)

   Lösung: Wir müssen noch alle Zahlen auf Primalität überprüfen, die zu $2 \cdot 3 \cdot 5 \cdot 11 = 330$ teilerfremd sind. Im Intervall $[N, N+329]$ kommen alle Reste modulo 330 genau einmal vor; daher finden sich genau $\varphi(330) = 2 \cdot 4 \cdot 10 = 80$ teilerfremde Zahlen im Intervall $[N, N+329]$. Vergrößern wir das Intervall, skaliert sich das ungefähr. D.h. auf einem Intervall der Länge 460 erwarten wir ca. $460 \cdot 80/330 \approx 112$ Zahlen, die zu 330 teilerfremd sind.

4. Sei $N = 1891 = 31 \cdot 61$. (4 P)

(a) Für wie viele $a \in (\mathbb{Z}/\mathbb{Z}N)^\times$ gilt $a^{N-1} \equiv 1 \mod N$?

Lösung: Nach Notiz 2.3.7 aus dem Skript gibt es genau $\mathrm{ggT}(N-1, p-1) \cdot \mathrm{ggT}(N-1, q-1)$ Lösungen. In unserem Fall ist $N-1 = 1890$, $p-1 = 30$, $q-1 = 60$; damit gibt es $30 \cdot 30 = 900$ Lösungen.

(b) Für wie viele $a \in (\mathbb{Z}/\mathbb{Z}N)^\times$ gilt $a^{(N-1)/2} \equiv 1 \mod N$?

Lösung: Ebenfalls nach Notiz 2.3.7 gibt es genau $\mathrm{ggT}((N-1)/2, p-1) \cdot \mathrm{ggT}((N-1)/2, q-1)$ Lösungen. In unserem Fall ist $(N-1)/2 = 945$; damit gibt es $15 \cdot 15 = 225$ Lösungen.

(c) Für wie viele $a \in (\mathbb{Z}/\mathbb{Z}N)^\times$ gilt $a^{(N-1)/2} \equiv -1 \mod N$?

Lösung: Eine solche Lösung ist z.B. $a_0 = 3$. Ist nun a eine Lösung aus (b); d.h. es gilt $a^{(N-1)/2} \equiv 1 \mod N$, dann betrachtet man $b := a_0 \cdot a$. Es gilt dann $b^{(N-1)/2} = (a_0 a)^{(N-1)/2)} \equiv (-1) \cdot 1 \equiv -1$; d.h. b ist eine Lösung für (c). Ist umgekehrt b eine Lösung für (c), so setzt man analog $a := a_0 b$ und erhält $a^{(N-1)/2} = (a_0 b)^{(N-1)/2)} \equiv (-1)(-1) \equiv 1$; d.h. a ist eine Lösung für (b). Wir können also aus jeder Lösung von (b) eine eindeutige Lösung von (c) konstruieren und umgekehrt. D.h. also, (c) hat die gleiche Anzahl Lösungen wie (b), nämlich 225 .

(d) Für wie viele $a \in (\mathbb{Z}/\mathbb{Z}N)^\times$ besteht N zur Basis a den Test von Rabin? Vergleichen Sie dies mit $\varphi(N)$.

Lösung: Wegen $N - 1 = 1890 = 2 \cdot 945$ besteht $N - 1$ den Test zu Basis a genau dann, wenn

$$a^{(N-1)/2} \equiv 1 \mod N \quad \text{oder}$$
$$a^{(N-1)/2} \equiv -1 \mod N;$$

d.h. wenn a eine Lösung aus (b) oder (c) ist. Davon gibt es insgesamt $2 \cdot 225 = 450$ Lösungen. Zum Vergleich: Es gilt $\varphi(N) = (p-1)(q-1) = 30 \cdot 60 = 1800$; d.h. es gibt 1800 teilerfremde Basen. Der Anteil der Basen a , für die N den Test besteht, ist also $450/1800 = 1/4$. Nach Satz 2.3.6 ist dies der größtmögliche Anteil (also der worst-case).