Übungen zur Vorlesung Angewandte Diskrete Mathematik

Institut für Reine Mathematik WS 08/09 – Blatt 06

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

---

Auf diesem Blatt sind 4 Zusatzpunkte zu erreichen!

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)

   (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)

2. Berechnen Sie alle Quadratwurzeln von 135 modulo 473. (4 P)

3. Führen Sie den Test von Rabin durch für die Zahl $N = 3277$ und die Basis $a = 2$. (4 P)
   Hinweis: Bestimmen Sie zunächst den Exponenten von 2 modulo N (ohne N zu faktorisieren).

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

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

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

   (c) Für wie viele $a \in (\mathbb{Z}/\mathbb{Z}N)^\times$ gilt $a^{(N-1)/2} \equiv -1 \mod N$?
   Hinweis: Eine solche Lösung ist z.B. $a_0 = 3$ (Dies brauchen Sie nicht zu zeigen). Wie konstruiert man mit Hilfe von a_0 aus einer Lösung für (b) eine Lösung für (c)?

   (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 $\varphi(N)$.

5. Sei $p > 3$ eine Primzahl, so dass $2p-1$ und $3p-2$ ebenfalls Primzahlen sind.

   (a) Zeigen Sie: 6 teilt $p-1$. (2 P)

   (b) Zeigen Sie: $p \cdot (2p-1) \cdot (3p-2)$ ist eine Carmichael-Zahl. (4 P)

   (c) Finden Sie mit dem Kriterium aus (b) zwei Carmichael-Zahlen. (2 P)