Blatt 6

Prof. Dr. N-P. Skoruppa und C. Math. L. Fischer Abgabe: Mi 30-05-2007

Für jede richtig gelöste Aufgabe werden 4 Punkte vergeben.

Aufgabe 1. Inplementieren Sie für Ihr CAS die Funktion `myLegendre(a,p)`, die für eine Primzahl p und eine zu p teilerfremde Zahl a das Legendre-Symbol $\left(\frac{a}{p}\right)$ berechnet. Dabei dürfen Sie nur Grundrechenarten (ggfs. einschl. Potenzieren und Teilen mit Rest) benutzen. Erzeugen Sie dann zufällig 10000 Inputs (a, p), wobei p mindestens 6 Dezimalstellen besitzt und ermitteln Sie die mittlere Laufzeit[1] Ihrer Implementierung.

Aufgabe 2. Sei A eine ganzzahlige 2×2-Matrix mit $\det(A) \neq 0$. Finden und beweisen Sie eine einfache Formel für die Zahlenfolge

$$a(m) = \#\left\{\begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} : A\begin{pmatrix} x \\ y \end{pmatrix} = 0\right\}.$$

(Hinweis: Sie dürfen ohne Beweis benutzen, dass es Matrizen $M, N \in \mathrm{GL}(2, \mathbb{Z})$ gibt, sodass MAN eine Diagonalmatrix ist.)

Aufgabe 3. Für eine ungerade Primzahl p und eine nicht durch p teilbare Zahl $a > 0$ sei n die Anzahl der Zahlen $1 \leq j < \frac{p}{2}$, sodass $(aj)\%p > \frac{p}{2}$ gilt[2]. Zeigen sie:

$$n = \sum_{k=1}^{\lfloor a/2 \rfloor} \#\left]\frac{(2k-1)p}{2a}, \frac{2kp}{2a}\right[\cap \mathbb{Z}.$$

Aufgabe 4. Leiten Sie folgende Behauptung aus dem *Gausschen Kriterium* unter Benutzung der Formel aus der vorangehen Aufgabe ab: Für jede ungerade Primzahl p gilt

$$\left(\frac{7}{p}\right) = \left(\frac{(-1)^{\frac{p-1}{2}}p}{7}\right).$$

Aufgabe 5. Sei $m > 0$ eine ganze Zahl. Zeigen Sie, dass die Menge $\mathbb{D}_m$ der Dirichletcharaktere modulo m versehen mit der üblichen Multiplikation von Funktionen eine abelsche Gruppe bildet. Beweisen Sie, dass diese Gruppe für ungerade Primzahlpotenzen m zyklisch ist (Hinweis: Ein Dirichletcharakter χ ist schon durch den Wert $\chi(w)$ für irgendeine Primitivwurzel modulo m eindeutig festgelegt). Bestimmen Sie die Elemente der Ordnung 2 in den Gruppen $\mathbb{D}_p$, wo p alle ungeraden Primzahlen durchläuft.

---

[1] In PARI/GP können Sie hierzu `gettime()` benutzen.

[2] $x\%p$ ist der Rest von x bei Division durch p