UNIVERSITÄT ULM
Institut für Zahlentheorie und Wahrscheinlichkeitstheorie

Übungen zur Angewandten Diskreten Mathematik

Prof. Dr. Helmut Maier, Hans- Peter Reck

Gesamtpunktzahl: 48 Punkte

Übungsblatt 8

Abgabe: **Freitag, 18. Februar 2011**, vor den Übungen im **H 6**

Die Punte dieses Blattes sind Zusatzpunkte, gehen also nicht in die Wertung der notwendig zu erreichenden Punkte ein. Zur Klausurzulassung benötigt man also 156 Punkte.

1. Es sei K ein endlicher Körper. Zeige: die multiplikative Gruppe $K^* = (K\backslash\{0\}, \cdot)$ ist zyklisch.
(4 Punkte)

2. Es ist $11^2 \equiv 14 \mod 107$. Zudem sind 53 und 107 Primzahlen. Bestimme damit $ord_{107}14$. (6 Punkte)

3. Es sei $m = 341 = 11 \cdot 31$.
   (a) Zeige, daß $ord_m a \leq 30$ für alle a mit $ggT(a, m) = 1$.
   (b) Gibt es ein a mit $ord_m a = 30$? (6 Punkte)

4. (a) Zeige: Die Menge der Restklassen $a \mod m$, die k- te Reste $\mod m$ sind, bildet eine Gruppe bzgl. der Multiplikation.
   (b) Es sei p eine Primzahl. Zeige:
   Das Produkt zweier quadratischer Nichtreste $\mod p$ ist ein quadratischer Rest $\mod p$.
(8 Punkte)

5. Die Folge der Lucas- Zahlen L_n ist für alle $n \in \mathbb{N}$ folgendermaßen definiert:
$$\begin{pmatrix} L_{n+2} & L_{n+1} \\ L_{n+1} & L_n \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^n \begin{pmatrix} 3 & 1 \\ 1 & 2 \end{pmatrix}$$
   (a) Bestimme L_n für alle $1 \leq n \leq 10$.
   (b) Zeige, daß $L_n L_{n+2} - L_{n+1}^2 = 5 \cdot (-1)^n$ ist.
   (c) Zeige, daß zwei aufeinanderfolgende Lucas- Zahlen teilerfremd sind.
   (d) Zeige:
$$L_n = \left(\frac{1+\sqrt{5}}{2}\right)^n + \left(\frac{1-\sqrt{5}}{2}\right)^n.$$
(8 Punkte)

6. Untersuche folgende Zusammenhänge zwischen den Lucas- und den Fibonacci- Zahlen u_n. Zeige, daß für alle $m, n \in \mathbb{N}$ gilt:

   (a) $u_n + u_{n+2} = L_{n+1}$

   (b) $2u_{n+m} = u_m L_n + u_n L_m$

   (c) $L_n^2 - 5u_n^2 = 4 \cdot (-1)^n$. (6 Punkte)

7. Bestimme die Höhe dieses schmalen Parallelogramms aus Aufgabe 5 von Übungsblatt 7. (4 Punkte)

8. Ein Teilnehmer T eines RSA- Systems hat den öffentlichen Schlüssel

$$(e, n) = (11, 35).$$

   Er erhält von einem anderen Teilnehmer S den Geheimtext $C = 22$.
   Was war die ursprüngliche Botschaft?

   Hinweis:
   Es ist $22^2 \equiv -6 \mod 35$. (6 Punkte)