UNIVERSITÄT ULM
Institut für Zahlentheorie und Wahrscheinlichkeitstheorie

Probeklausur zur Angewandten Diskreten Mathematik

Prof. Dr. Helmut Maier, Hans- Peter Reck

Gesamtpunktzahl: 130 Punkte, 100 Punkte= 100 %

keine Abgabe

1. Es sei $m = 2^4 \cdot 3^3 \cdot 7 \cdot 11^2 \cdot 13$ und $n = 2 \cdot 5^2 \cdot 7 \cdot 11$.

   (a) Gib die Primfaktorzerlegung für $ggT(m, n)$ und $kgV(m, n)$ an.

   (b) Gib eine Darstellung der Werte $\varphi(m)$ und $\varphi(n)$ als Produkt von Primfaktoren.

   (c) Zeige: Aus $ggT(a, b, c) = 1$, $ggT(a, b) = d$ und $ggT(a, c) = f$ folgt $ggT(a, bc) = df$.

   Die Werte der Produkte brauchen jeweils nicht berechnet werden. (9 Punkte)

2. Zeige:

   (a) $7|(10a + b) \Leftrightarrow 7|(a - 2b)$ mit $a, b \in \mathbb{Z}$.

   (b) Die Zahl $111 \ldots 111$, bestehend aus k Ziffern des Wertes 1 mit $k \geq 2$ ist keine Quadratzahl.

   (9 Punkte)

3. (a) Bestimme mit Hilfe des Euklidischen Algorithmus den größten gemeinsamen Teiler der beiden Zahlen 969 und 221.

   (b) Entscheide über die Lösbarkeit der folgenden Diophantischen Gleichungen. Gib im positiven Falle eine Lösung an.

   i. $969x + 221y = 748$.

   ii. $414x + 713y = 100$. (14 Punkte)

4. Es ist $43 \cdot 38 = 15 \cdot 109 - 1$.
   Benütze dies, um das multiplikative Inverse von 43 mod 109 zu berechnen. (6 Punkte)

5. Bestimme die kleinste positive Lösung der Kongruenz $1193x \equiv 367 \bmod 31500$ mittels des Chinesischen Restsatzes.

   (10 Punkte)

6. Gib eine Definition für die folgenden Begriffe an:

   (a) zyklische Gruppe

   (b) Integritätsring

   (c) Körper (12 Punkte)

7. Es ist $83 = 2 \cdot 41 + 1$, und 41 ist prim. Welche Werte kann $\operatorname{ord}_{83} a$ annehmen? (12 Punkte)

8. Die Mersennesche Zahl M_{251} ist zusammengesetzt. Für einen Primteiler muß $251|(p-1)$, also $p \equiv 1 \bmod 251$ gelten. Die kleinste Primzahl dieser Art ist $p = 503$.
   Zeige: 503 ist ein Teiler von M_{251}. (10 Punkte)

9. (a) Welche Untergruppen hat die Gruppe $(\mathbb{Z}/12\mathbb{Z}, +)$?
   (b) Es sei G eine beliebige Gruppe der Ordnung 12, d.h. auch möglicherweise nichtabelsch. Welche Ordnungen können die Untergruppen von G haben? (10 Punkte)

10. Zeige durch Nachrechnen (und nicht durch Benützung von Satz 1.16.13 der Vorlesung), daß die Gruppe $G = ((\mathbb{Z}/15\mathbb{Z})^*, \cdot)$ nicht zyklisch ist. (8 Punkte)

11. Es sei $K = (\mathbb{Z}/5\mathbb{Z}, +, \cdot)$ der (bis auf Isomorphie eindeutig bestimmte) Körper mit fünf Elementen. Es sei $f_0 \in K[x]$ durch $f_0(x) = x^2 + x + \overline{1}$ definiert, wobei $\overline{a} = a \bmod 5$ bedeute.

    Zeige:

    (a) Das Polynom f_0 hat keine Nullstelle in K.
    (b) Zudem ist es irreduzibel.
    (c) Der Ring der Restklassen modulo f_0, also $K[x]/(f_0)$ ist ein Körper. Wieviele Elemente hat er?
    (d) Es sei $t = x \bmod f_0$.
    Finde ein Polynom p vom Grad ≤ 1, so daß $(t^2 + t + \overline{2}) \cdot (t^2 + \overline{1}) = p(t)$ gilt. (14 Punkte)

12. Ein Code C über einem Körper mit q Elementen haben eine Kontrollmatrix vom Typ $(4, 10)$. Bestimme die Mächtigkeit $|C|$. (8 Punkte)

13. Zeige folgenden Zusammenhang zwischen den Fibonaccizahlen u_n und dem Binomialkoeffizienten:

$$u_n = \sum_{k=0}^{n} \binom{n-k}{k}.$$

(8 Punkte)

Viel Erfolg!