Probeklausur zur Elementaren Zahlentheorie

Prof. Dr. Helmut Maier, Hans- Peter Reck

Gesamtpunktzahl: 130 Punkte, 100 Punkte= 100 %

keine Abgabe

1. Es seien $m = 630$ und $n = 62 \cdot p$ mit $p \in \mathbb{P}$ und $5 < p < 12$.

   (a) Bestimme die Primfaktorzerlegung von m und n.

   (b) Leite daraus den größten gemeinsamen Teiler und das kleinste gemeinsame Vielfache von m und n als Produkt von Primfaktoren her. (7 Punkte)

2. (a) Zeige, dass die Summe dreier aufeinanderfolgender Kubikzahlen durch 9 teilbar ist.

   (b) Es sei $n = \sum_{j=0}^{k} b_j \cdot 1000^j$ mit $b_j \in \mathbb{Z}$ und $0 \leq b_j \leq 999$.
   Zeige, dass n genau dann durch 7 teilbar ist, wenn $\sum_{j=0}^{k} (-1)^j \cdot b_j$ durch 7 teilbar ist.
   (7 Punkte)

3. Eine Stadtkapelle möchte sich anlässlich ihres 150jährigen Jubiläums neue Uniformen anschaffen. Ihr steht dafür der Betrag von 1280 Euro zur Verfügung. In der erwünschten Qualität kosten Damenuniformen 51 Euro und Herrenuniformen 27 Euro.

   (a) Warum kann der zur Verfügung stehende Betrag nicht komplett ausgegeben werden?

   (b) Welches ist der höchste Betrag, der ausgegeben werden kann?

   (c) Wieviele Uniformen beider Arten werden für diesen Höchstbetrag angeschafft? (10 Punkte)

4. In der Simpsons- Folge "Im Schatten des Genies" kritzelt Homer auf eine Tafel die Gleichung

$$3987^{12} + 4365^{12} = 4472^{12},$$

   ein offensichtlicher Widerspruch zum (bewiesenen) Großen Fermatschen Satz.
   Rette die Situation und weise nach, dass die obige Gleichung falsch ist (wenn auch nur ganz knapp).
   (5 Punkte)

5. Berechne

   (a) $15^{40} \bmod 49$

   (b) $3^{1280} \bmod 256$. (7 Punkte)

6. (a) Bestimme die betragsmäßig kleinste Zahl $x \in \mathbb{Z}$, die die drei Kongruenzen $x \equiv 4 \bmod 9$, $x \equiv 3 \bmod 10$ und $x \equiv 7 \bmod 11$ erfüllt.

   (b) Wie viele Lösungen hat die Kongruenz $x^{21} \equiv 1 \bmod N$ mit $N = 31 \cdot 49 \cdot 64$?

   (c) Gib alle Lösungen der Kongruenz $x^8 + x^4 + 7x^2 + 1 \equiv 0 \bmod 10$ an. (15 Punkte)

7. (a) Bestimme die Faktorisierung von 51 mittels des Pollardschen- Rho- Verfahrens.

   (b) Berechne $\varphi(51)$ und $\varphi(51^2)$. (8 Punkte)

8. (a) Zeige, dass die Menge $M = \{1, 2, 15, 30, 71, 117\}$ nicht mit Quadraten zu einem reduzierten Restsystem modulo 11 ergänzt werden kann.

   (b) Es sei $n \in \mathbb{N}$ und $d(n)$ die Anzahl der Teiler von n.
   Zeige, dass die zahlentheoretische Funktion d multiplikativ ist. (10 Punkte)

9. (a) Gib eine Definition folgender Begriffe an:
      i. vollständiges Restsystem modulo m
      ii. Ordnung von a mod m
      iii. Pseudoprimzahl zur Basis $a \in \mathbb{N}$

   (b) Formuliere den Fundamentalsatz der Arithmetik. (12 Punkte)

10. (a) Begründe, warum zum Modul 25 eine Primitivwurzel existiert.

    (b) Wieviele teilerfremde Restklassen modulo 25 gibt es?

    (c) Gib diese teilerfremden Restklassen modulo 25 explizit an.

    (d) Bestimme das multiplikative Inverse von 19 mod 25.

    (e) Welche Ordnung besitzt das Element 13 modulo 25?

    (f) Zeige, dass 3 eine Primitivwurzel modulo 25 ist.

    (g) Löse die Kongruenz $21x \equiv 7 \bmod 25$.

    (h) Wieviele achte Potenzreste gibt es modulo 25?

    (i) Überprüfe, ob 17 achter Potenzrest modulo 25 ist.

    (j) Wieviele Lösungen besitzt dann die Kongruenz $x^8 \equiv 17 \bmod 25$? (20 Punkte)

11. Es sei $k \in \mathbb{N}_0$. Den Fermatzahlen $F_k := 2^{2^k} + 1$ sind wir bereits auf Übungsblatt 6 begegnet.

    (a) Es sei nun $k \geq 2$ und $p \in \mathbb{P}$ mit $p|F_k$. Berechne $\mathrm{ord}_p\, 2$.

    (b) Zeige: $p \equiv 1 \bmod 2^{k+2}$.

    (c) Folgere die Existenz unendlich vieler Primzahlen $p \equiv 1 \bmod 8$.

    (d) Folgere aus Teilaufgabe b), dass 641 ernsthafter Kandidat für einen Primfaktor von F_5 ist.

    (e) Folgere $641|F_5$ aus den Gleichungen $641 = 5 \cdot 2^7 + 1$ und $641 = 5^4 + 2^4$. (12 Punkte)

12. (a) Es gilt $5009 \in \mathbb{P}$. Berechne das Legendre- Symbol

$$\left(\frac{2016}{5009}\right).$$

    (b) Ist die Kongruenz $x^2 \equiv 101 \bmod 2017$ mit $2017 \in \mathbb{P}$ lösbar. (9 Punkte)

13. Tomo und Vito wollen beide einer dritten Person Marta Nachrichten versenden.
    Marta veröffentlicht ihren öffentlichen Schlüssel $S = (e, n)$ mit $e = 19$ und $n = 11 \cdot 13 = 143$.

    (a) Prüfe, ob die Voraussetzungen für das RSA- Verfahren vorliegen.

    (b) Tomo möchte die Botschaft $B = 21$ verschlüsselt an Marta senden.
    Welchen Wert C schickt er weiter?

    (c) Von Vito erhält Marta die Botschaft $C = 31$. Was war die ursprüngliche Information?
    (8 Punkte)

Viel Erfolg!