Angewandte diskrete Mathematik

Einige ehemalige Klausuraufgaben

Im folgenden bezeichnet φ die Eulersche φ–Funktion.

1. Zeige, daß für zwei ganze Zahlen a, b genau dann $13 \mid (10a+b)$ gilt, wenn $13 \mid (a+4b)$ gilt.

2. Zeige, daß $n^7 - n$ für jede ganze Zahl n durch 42 teilbar ist.

3. Es seien $m=960$ und $n=1280$.

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

   b) Stelle die Werte von $\varphi(m)$ und $\varphi(n)$ als Produkt von Primfaktoren dar.

   Die Werte der Produkte bruachen nicht berechnet werden.

4. Bestimme mit Hilfe des Euklidischen Algorithmus' den größten gemeinsamen Teiler von 10013 und 992.

5. Entscheide jeweils, ob die angegebene Diophantische Gleichung lösbar ist, und finde gegebenenfalls eine Lösung.

   a) $10013x + 992y = 62$ b) $341x + 55y + 121z = 10$

6. Finde das multiplikative Inverse von 59 modulo 113.

7. Welchen Rest modulo 3 kann das Quadrat einer ganzen Zahl n annehmen. Wie hängt dieser Rest von n ab?

8. Berechne $\varphi(359)$, $\varphi(360)$ und $\varphi(361)$.

9. Betrachte den Restklassenring $R = \mathbb{Z}/111\mathbb{Z}$.

   a) Ist R ein Körper?

   b) Bestimme $\varphi(111)$.

   c) Berechne $5^{145} \bmod 111$.

   d) Was ist das multiplikative Inverse von $19 \bmod 111$?

10. Finde die kleinste natürliche Zahl, welche die Kongruenzen

$$x \equiv 3 \bmod 4\,, \quad x \equiv 5 \bmod 7 \quad \text{und} \quad x \equiv 9 \bmod 11$$

    erfüllt.

11. Zeige: $F_n = 2^{2^n} + 1$ $(n \in \mathbb{N} \setminus \{1\})$ eine Primzahl, so ist 2 keine Primitivwurzel modulo F_n.

12. Entscheide für jeden der folgenden Moduln m, ob 3 eine Primitivwurzel modulo m ist.

    a) $m = 5$ b) $m = 11$

13. Ist die Kongruenz $x^6 \equiv 5 \bmod 71$ lösbar?

14. Es sei $K = \mathbb{Z}/5\mathbb{Z}$ der (bis auf Isomorphie eindeutig bestimmte) Körper mit fünf Elementen. Und es sei $P = x^2 + x + \overline{1} \in K[x]$, wobei $\overline{a} = \overline{a \bmod 5}$ bedeute. Zeige:

    a) Das Polynom P hat keine Nullstelle in K und ist irreduzibel.

    b) Der Restklassenring $K[x]/(P)$ ist ein Körper. Wieviele Elemente hat er?

    c) Finde ein Polynom $p \in K[x]$ vom Grade ≤ 1 mit $(x^2 + x + \overline{2})(x^2 + \overline{1}) \equiv p(x) \bmod P$.

15. Ein Teilnehmer eines RSA–Systems hat den öffentlichen Schlüssel $(e, n) = (13, 77)$. Er erhält von einem anderen Teilnehmer den Geheimtext $C = 5$. Was war die ursprüngliche Botschaft B?