ulm university universität
uulm

Probeklausur zur Angewandten Diskreten Mathematik

Dr. Hartmut Lanzinger, Hans- Peter Reck

Gesamtpunktzahl: 114 Punkte, 100 Punkte= 100 %, keine Abgabe

1. Es seien $m = 1155$ und $n = 1280$.

   (a) Bestimme die Primfaktorzerlegung von m und n

   (b) Leite daraus $ggT(m, n)$ und $kgV(m, n)$ als Produkt von Primfaktoren her. (7 Punkte)

2. Es seien $n, m \in \mathbb{N}$. Zeige: Ist 3 ein Teiler von $n^2 + m^2$, so teilt 3 bereits n und m. (5 Punkte)

3. (a) Bestimme den größten gemeinsamen Teiler von 6141 und 3243.

   (b) Ist die Diophantische Gleichung $6141x + 3243y = 207$ lösbar?
   Falls ja, gib hierfür eine Lösung an. (10 Punkte)

4. (a) Gib alle Lösungen der linearen Kongruenz $23x \equiv 31 \bmod 47$ an.

   (b) Bestimme das multiplikative Inverse von 19 mod 71. (8 Punkte)

5. Es gilt $839 \in \mathbb{P}$, $840 = 2^3 \cdot 3 \cdot 5 \cdot 7$ und $841 = 29^2$.

   (a) Bestimme den Wert der Eulerschen φ- Funktion dieser drei Zahlen.

   (b) Berechne $29^{1696} \bmod 839$. (7 Punkte)

6. Für einen Primteiler der zusammengesetzten Mersenne- Zahl M_{251} muss $251|(p-1)$ gelten.

   (a) Bestimme die kleinste Primzahl dieser Art.

   (b) Zeige, dass diese Primzahl auch ein Teiler von M_{251} ist. (8 Punkte)

7. An welchen Wochentagen fanden folgende Ereignisse statt?

   (a) die Stürmung der Lufthansa- Maschine Landshut in Mogadischu (18. Oktober 1977)

   (b) der Orkan Lothar (26. Dezember 1999)

   Hinweis:
   Es gilt dabei für den Oktober $f(8) = 6$ und für den Dezember $f(10) = 4$. (6 Punkte)

8. Bestimme die Faktorisierung der Zahl 1729 mittels des Pollard- Rho- Verfahrens. (6 Punkte)

9. (a) Bestimme die kleinste positive Zahl, die die folgenden Eigenschaften erfüllt:

$$\begin{aligned} x &\equiv 4 \bmod 5 \\ x &\equiv 2 \bmod 11 \\ x &\equiv 1 \bmod 12^2. \end{aligned}$$

   (b) Stellt die Lösung eine Carmichael- Zahl dar (mit Begründung)? (9 Punkte)

10. Zeige, dass die Diophantische Gleichung $x^6 - 11x^4 + 36x^2 - 36 + 27^n = 0$ für alle $n \in \mathbb{N}$ unlösbar ist. (8 Punkte)

11. (a) Berechne $\mathrm{ord}_{13}\, 3$ und zeige, dass 3 keine Primitivwurzel modulo 13 ist.

    (b) Bestimme eine Primitivwurzel modulo 13.

    (c) Stelle jedes $g \in (\mathbb{Z}/13\mathbb{Z})^*$ als Potenz der in Teilaufgabe b) gefundenen Primitivwurzel dar.

    (d) Löse die Kongruenz $x^5 \equiv 11 \bmod 13$.

    (e) Löse die Kongruenz aus Teilaufgabe d) mit der Methode der schnellen Exponentiation.

    (12 Punkte)

12. Es seien $n \in \mathbb{N}$ ungerade mit $n \geq 2$ und $m \in \mathbb{N}_0$.

    (a) Zeige, dass $(n - 1 + n \cdot m)^{n-1} \equiv 1 \bmod n$ gilt.

    (b) Folgt daraus, dass n eine Pseudoprimzahl zur Basis $n - 1 + n \cdot m$ ist? (6 Punkte)

13. Es sei $n = pq$ mit $p = 17$ und $q = 19$.
    Als öffentlichen Schlüssel wähle ein Teilnehmer eines RSA- Systems $(e, n) = (11, 323)$ und versende die Botschaft $C = 3$. Bestimme den Klartext B. (6 Punkte)

14. Michael und Vito wollen einen geheimen Schlüssel vereinbaren. Sie wählen dazu $p = 23$ und $r = 5$. Michael wählt $a \in \{1, 2, \ldots, 22\}$, Vito $b \in \{1, 2, \ldots, 22\}$. Damit berechnen sie $A = r^a \equiv 2 \bmod 23$ und $B = r^b \equiv 3 \bmod 23$.

    (a) Bestimme a und b mit dem diskreten Logarithmus.

    (b) Berechne den geheimen Schlüssel k.

    Mit Vitos öffentlichem Schlüssel $(23, 5, 3)$ möchte Michael ihm nun geheime Nachrichten verschicken. Mit dem geheimen Schlüssel k bestimmt er zuerst das Paar $(c_1, c_2) = (5^k \bmod 23, mB^k \bmod 23)$. Marta möchte die Nachricht ebenfalls lesen, kann aber nur $c_2 = 19$ abfangen und ohne Kenntnis des geheimen Schlüssels k die Nachricht nicht entschlüsseln.

    (c) Bestimme den Klartext m. (12 Punkte)

15. Überprüfe, ob $1241 = 17 \cdot 73$ ein quadratischer Rest modulo der Primzahl 4801 ist. (4 Punkte)

Viel Erfolg!