ELEMENTARE ZAHLENTHEORIE
8. Übungsblatt

Julia Sauter, Andrew Hubery

Aufgabe 1.

Der folgende Geheimtext wurde empfangen. Er war mit dem RSA-Verfahren durch den öffentlichen Schlüssel $(n, e) = (3239, 1783)$ verschüsselt. (Hinweis: $41 \mid 3239$.)

$$0143 \mid 2333 \mid 2149 \mid 0822 \mid 1531 \mid 2304 \mid 2934 \mid 2164$$

Bestimmen Sie den privaten Schlüssel (n, d) und den Klartext (A=2,B=3,...,Z=27).

(4 Punkte)

Aufgabe 2.

(a) Sei $t \geq 1$ sodass $6t + 1$, $12t + 1$ und $18t + 1$ alle Primzahlen sind. Zeigen Sie, dass $C \coloneqq (6t + 1)(12t + 1)(18t + 1)$ eine Carmichael-Zahl ist.

(b) Finden Sie mit Hilfe von (a) drei Carmichael Zahlen.

(4 Punkte)

Aufgabe 3.

(a) Sei $n \geq 1$. Zeigen Sie per Induktion, dass

$$3^{2^n} \equiv 1 + 2^{n+2} \pmod{2^{n+3}}.$$

(b) Für $n \geq 3$ zeigen Sie, dass $3 \pmod{2^n}$ die Ordnung 2^{n-2} hat.

(3+2 Punkte)

Aufgabe 4.

(a) Finden Sie die Ordnungen alle Elemente aus $(\mathbb{Z}/12\mathbb{Z})^\times$. Ist $(\mathbb{Z}/12\mathbb{Z})^\times$ eine zyklische Gruppe?

(b) Finden Sie alle Primitivwurzeln modulo 5 und modulo 25.

(c) Sei $p > 2$ eine Primzahl und a eine Primitivwurzel modulo p. Zeigen Sie, dass $a+pb$ eine Primitivwurzel modulo p^2 ist genau dann, wenn $(a + pb)^{p-1} \not\equiv 1 \pmod{p^2}$.

Zeigen Sie weiter, dass es genau eine $b \pmod{p}$ gibt, sodass $a + pb$ keine Primitivwurzel modulo p^2 ist. (Sie dürfen annehmen, dass $(\mathbb{Z}/p^2\mathbb{Z})^\times$ zyklish ist.)

Hinweis: Schreiben Sie $a^{p-1} = 1 + pt$ und berechnen Sie $a(a + pb)^{p-1} \pmod{p^2}$.

(2+2+3 Punkte)

Abgabe: Montag 10. Juni, bis 12 Uhr in die Postfächer der Tutoren im V3–126