ELEMENTARE ZAHLENTHEORIE
8. ÜBUNGSBLATT

DR. BAPTISTE ROGNERUD

Aufgabe 1. [4 Punkte] Sei $n \in \mathbb{N}_{>1}$. Seien $p_1, \cdots, p_n$ die Primfaktoren von $n-1$. Angenommen es gibt ein $a \in \mathbb{N}$ mit $a^{n-1} \equiv 1(\mod n)$ und $a^{\frac{n-1}{p_i}} \not\equiv 1(\mod n)$.

Zeigen Sie, dass n Primzahl ist.

(Hinweis: Berechnen Sie die Ordnung von $\overline{a}$ in $(\mathbb{Z}/n\mathbb{Z})^\times$.)

Aufgabe 2. [1+1+2 Punkte]

(a) Berechnen Sie die Ordnung alles Gruppenelemente in $(\mathbb{Z}/12\mathbb{Z})^\times$
(b) Ist $(\mathbb{Z}/12\mathbb{Z})^\times$ eine zyklische Gruppe?
(b) Zeigen Sie:

$$(\mathbb{Z}/12\mathbb{Z})^\times \cong \big(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, +\big)$$

Aufgabe 3. [4 Punkte] Sei $t \in \mathbb{N}_{>0}$.

(a) Zeigen Sie: Wenn $6t+1$, $12t+1$ and $18t+1$ Primzahlen sind, dann ist $n = (6t+1)(12t+1)(18t+1)$ eine Carmichael-Zahl.
(b) Finden Sie 2 Carmichael-Zahlen mit Hilfe von (a)[1].

Aufgabe 4. [4 Punkte]

Der Geheimtext

$$2466|1320|1307|2426|1307|1401|1307|2466|1025.$$

wurde mit dem RSA-Verfahren chiffriert. Dazu wurde der folgende öffentliche Schlüssel verwendet:

$$(e, n) = (703, 2573).$$

Bestimmen Sie den privaten Schlüssel und den Klartext ($A = 1, B = 2, \cdots, Z = 26$).

(Hinweis: $2573 = 31 \times 83$. Sie sollten für diese Aufgabe einen Taschenrechner oder Online-Taschenrechner benutzen, z.B.:

https://www.mtholyoke.edu/courses/quenell/s2003/ma139/js/powermod.html)

Abgabe: Freitag, 8. Juni 2018, bis 10 Uhr in die Postfächer der Tutoren in V3-126.

[1]Es gibt 246683 Carmichael-Zahlen kleiner gleich 10^{16} aber nur 256 davon sind der From wie in (a).