Übungen zur Zahlentheorie, WWU Münster, Mathematisches Institut, SoSe 2016
U. Hartl, K. Halupczok **Blatt Nr. 3**, 28.04.16

Abgabe: **Mittwoch, 04. Mai 2016**, bis 11:30 Uhr in die Briefkästen im Hörsaalgebäude

---

Leseaufgabe: Kapitel 1.6 und 1.7 bis Montag 2.5., Kapitel 2.1 bis Montag 9.5.

Aufgabe 1

(a) Geben Sie die Einheitengruppen der Ringe $\mathbb{Z}/24\mathbb{Z}$ und $\mathbb{Z}/13\mathbb{Z}$ explizit an.

(b) Zeigen Sie unter Verwendung des Satzes von Euler mod $9n$: Jede ungerade natürliche Zahl n, die kein Vielfaches von 5 ist, teilt eine Repetier-Eins (vgl. Aufgabe 2 auf Blatt 1).

Aufgabe 2

(a) Wieviele Lösungen kann die Kongruenz $x^3 - 54x^2 - 5x + 3^{41} \equiv 0 \bmod 55$ maximal haben? Berechnen Sie alle Lösungen durch Zerlegung des Polynoms in Linearfaktoren mod 55, welche in diesem Beispiel (nach Reduktion der Koeffizienten) leicht zu machen ist.

(b) Sei p eine Primzahl. Zeigen Sie die Polynomkongruenzen

$$X^{p-1} - 1 \equiv (X-1)(X-2)\cdots(X-(p-1)) \bmod p$$

und

$$(X-1)^p - (X-1) \equiv X^p - X \bmod p.$$

Aufgabe 3

(a) Bestimmen Sie folgende Ordnungen: $\operatorname{ord}(\overline{6})$ in $(\mathbb{Z}/31\mathbb{Z})^\times$, $\operatorname{ord}(\overline{4})$ in $(\mathbb{Z}/53\mathbb{Z})^\times$.

(b) Bestimmen Sie alle primitiven Wurzeln mod 19.

(c) Untersuchen Sie, ob es primitive Wurzeln in $\mathbb{Z}/26\mathbb{Z}$ und in $\mathbb{Z}/12\mathbb{Z}$ geben könnte.

(d) Sei r eine primitive Wurzel mod p und $k \in \mathbb{N}$. Zeigen Sie, dass r^k genau dann eine primitive Wurzel mod p ist, wenn $\operatorname{ggT}(k, p-1) = 1$ ist.