**Übungen zur Zahlentheorie, WWU Münster, Mathematisches Institut, SoSe 2016**
**U. Hartl, K. Halupczok** **Blatt Nr. 4**, 06.05.16

Abgabe: **Donnerstag, 12. Mai 2016**, bis 8:30 Uhr in die Briefkästen im Hörsaalgebäude

**Leseaufgabe:** Kapitel 2.2 bis Donnerstag 12.5.

### Aufgabe 1

(a) Bestimmen Sie alle quadratischen Reste und Nichtreste mod 7 und mod 19.

(b) Bestimmen Sie alle Lösungen der Kongruenz $(x-2)^2 \equiv -3 \bmod 7 \cdot 19$.

(c) Bestimmen Sie alle Lösungen der Kongruenz $x^2 - 4x + 3 \equiv -4 \bmod 7 \cdot 19$.

(d) Beschreiben Sie allgemeiner eine Lösungsstrategie für die quadratische Kongruenz $x^2 + ax + b \equiv 0 \bmod m$, wenn $a, b \in \mathbb{Z}$ ist und $m \in \mathbb{N}$, $m > 1$, ein quadratfreier Modul ist. (Vgl. Aufgabe 3 auf Blatt 1 zum Begriff quadratfrei.)

### Aufgabe 2

(a) Stellen Sie alle Reste mod 19 als Potenz der primitiven Wurzel 2 mod 19 dar.

(b) Berechnen Sie das Legendresymbol

$$\left(\frac{6513}{19}\right) = \left(\frac{15}{19}\right)$$

durch Zerlegung der Zahl 15 in ihre Primteiler und Ausnutzung der Multiplikativität des Legendresymbols,

1. einmal durch Verwendung von Aufgabe 1 (a),
2. einmal durch Verwendung von Teil (a) dieser Aufgabe.

Warum ist es vorteilhaft, erst die Reduktion von 6513 auf 15 vorzunehmen? Ginge das noch einfacher? Sind diese Methoden bei sehr großen Zahlen noch praktisch durchführbar?

(c) Berechnen Sie das in (b) genannte Legendresymbol unter Verwendung der Eulerkongruenz Satz 2.1.9. Ist dies auch bei sehr großen Zahlen praktisch durchführbar?

### Aufgabe 3

(a) Sei $n = pq$ das Produkt zweier (womöglich großer) verschiedener Primzahlen $p$ und $q$ mit $p \equiv q \equiv 3 \bmod 4$, und es sei ein Rest $b$ mod $n$ zufällig gewählt. Zeigen Sie, dass die Kongruenz $x^2 \equiv b^2 \bmod n$ insgesamt vier Lösungen mod $n$ besitzt, wobei zwei Lösungen von der Form $\pm c$ mod $n$ sind, die von $\pm b$ mod $n$ jeweils verschieden sind.

(b) Zeigen Sie: Sind $n$, $b$ und $c$ explizit bekannt, so können auch die beiden Primfaktoren von $n$ explizit durch Ermittlung von $\mathrm{ggT}(b+c, n)$ berechnet werden.

(c) Führen Sie dies in der Praxis durch am Beispiel $n = 209$, $b = 16$ und $c = 60$. Warum wird die Rechnung auch bei sehr großen Zahlen schnell durchführbar sein?