Goethe-Universität Frankfurt
Institut für Mathematik

Prof. Dr. Jakob Stix

# Elementare Zahlentheorie

Sommersemester 2017

**Übungsblatt 6** 29. Mai 2017

**Aufgabe 27.** (Fermat-Pseudoprimzahlen)

(a) Zeigen Sie, daß 341 eine Fermat-Pseudoprimzahl zur Basis 2 ist.

(b) Es gibt unendlich viele Fermat-Pseudoprimzahlen zur Basis 2.
*Hinweis: Zeigen Sie: mit $n$ ist auch $2^n - 1$ eine Fermat-Pseudoprimzahl zur Basis 2.*

**Aufgabe 28.** (Carmichaelzahlen)

Zeigen Sie die folgenden Aussagen:

(a) Wenn $p \mid n$, dann existiert in $(\mathbb{Z}/n\mathbb{Z})^\times$ ein Element der Ordnung $p-1$.

(b) Wenn $p^2 \mid n$, dann existiert in $(\mathbb{Z}/n\mathbb{Z})^\times$ ein Element der Ordnung $p$.

(c) Die Zahl $n$ ist Carmichaelzahl, wenn $n$ quadratfrei ist und für jeden Primteiler $p \mid n$ gilt: $p-1 \mid n-1$.

(d) Die 2 ist die einzige gerade Carmichaelzahl.

(e) Die 561 ist Carmichaelzahl.

*Tipp:* Verwenden Sie, daß für jede Primzahl $p$ und $k \geq 2$ die Gruppe $(\mathbb{Z}/p^k\mathbb{Z})^\times$ ein Element der Ordnung $p$ enthält, beispielsweise als Konsequenz des Satzes von Cauchy.

**Aufgabe 29.** (Primitivwurzeln)

(a) Bestimmen Sie alle Primitivwurzeln modulo 11, 13 und 17.

(b) Zeigen Sie: Es gibt keine Primzahl $p$, so dass 4 eine Primitivwurzel modulo $p$ ist.

(c) Nutzen Sie ein Computeralgebrasystem, um die kleinste Primzahl zu berechnen, für die die kleinste Primitivwurzel größer als 100 ist.

**Aufgabe 30.** (RSA-Verfahren)

Alice will sich mit Bob zu einem geheimen Treffen verabreden. Dazu hat Bob einen öffentlichen RSA-Schlüssel $(n, e) = (4141, 127)$ ausgegeben, und Alice hat ihre RSA-verschlüsselte Nachricht an Bob gesendet. Inzwischen haben Sie doch einen Zugriff auf diese Nachricht, die folgendermaßen lautet:

2993 3130 1627

Können Sie diese hacken? Sie sollten für diese Aufgabe einen Computer benutzen.

*Erläuterung: Zur Verschlüsselung werden die Buchstaben gemäß folgender Tabelle in Zahlen umgewandelt. Anschließend wurde die Ziffernfolge in 4-stellige Blöcke unterteilt. Bei Bedarf wird der letzte Block mit Leerzeichen " " = 36 aufgefüllt.*

| A | B | C | D | E | F | G | H | I | J | K | L | M |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 |

| N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 | 32 | 33 | 34 | 35 |

**Aufgabe 31.** (Quadratische Kongruenzen)

(a) Sei $p$ eine ungerade Primzahl. Weiter seien $a, b, c \in \mathbb{N}$ mit $p \nmid a$. Zeigen Sie: Die Kongruenz

$$ax^2 + bx + c \equiv 0 \pmod{p}$$

besitzt genau $\left(\frac{b^2-4ac}{p}\right) + 1$ viele Lösungen in $\mathbb{Z}/p\mathbb{Z}$.

(b) Untersuchen Sie, wieviele Lösungen in $\mathbb{Z}/n\mathbb{Z}$ folgende Kongruenzen besitzen:

(i) $2x^2 + 3x - 1 \equiv 0 \mod n$, wobei $n = 133$.

(ii) $5x^2 + 3x + 1 \equiv 0 \mod n$, wobei $n = 235$.

---

**Abgabe:** Am kommenden Dienstag, den **6. Juni 2017**, bis zur Vorlesung in den Kasten im 3. Stock, Institut für Mathematik, Robert-Mayer-Straße 6-8. Downloads von Übungsblättern und Informationen zur Vorlesung unter

`http://www.uni-frankfurt.de/65113368/17_SS_Elementare-Zahlentheorie`