UNIVERSITÄT DES SAARLANDES
Fachrichtung 6.1 - Mathematik
Christian Bopp

Übungen zur Elementaren Zahlentheorie

Sommersemester 2018

Die Lösungen des Übungsblattes sind bis spätestens 14.00 Uhr, am 27.06.2018, in die Briefkästen vor dem Zeichensaal in Geb. E2 5, einzuwerfen.
Alle Übungsblätter und Informationen zur Vorlesung werden auf der Seite unserer Arbeitsgruppe unter *Teaching* zu finden sein: www.math.uni-sb.de/ag-schreyer/

Blatt 11 — 20.05.2018

Aufgabe 1. Ist die folgende simultane Kongruenz lösbar? Falls ja, bestimmen Sie die kleinste positive Lösung.

$$x \equiv 1 \bmod 10$$
$$x \equiv 13 \bmod 22$$
$$x \equiv 46 \bmod 55$$

Aufgabe 2. Wir bezeichnen mit $\varphi : \mathbb{N} \to \mathbb{N}$ die Eulersche φ–Funktion.

(a) Für welche $n \in \mathbb{N}$ gilt $\varphi(n) = \varphi(2n)$?
(b) Gibt es ein $n \in \mathbb{N}$ mit $\varphi(n) = 14$?

Aufgabe 3. Sei $m \in \mathbb{N}^*$ und sei $a \in (\mathbb{Z}/m\mathbb{Z})^\times$. Zeigen Sie, dass

$$\mathrm{ord}_m(a^k) = \frac{\mathrm{ord}_m(a)}{\mathrm{ggT}(\mathrm{ord}_m(a), k)}.$$

Aufgabe 4. (a) Diskutieren Sie das Verfahren der schnellen Exponentation (siehe nächste Seite).
(b) Berechnen Sie die folgenden modularen Potenzen mittels schneller Exponentation:
(i) $5^{31} \bmod 12$
(ii) $6^{101} \bmod 25$

Schnelle Exponentation:

Die Berechnung von $a^e \mod m$ kann sehr Zeit aufwendig sein. Ein effektives Verfahren um solche modularen Potenzen zu berechnen, ist die schnelle Exponentation. Um $a^e \mod m$ zu berechnen, gehen wir wie folgt vor:

Schritt 1. Wir berechnen die binäre Entwicklung des Exponenten e, d.h. wir schreiben den Exponenten als

$$e = \sum_{i=0}^{k} e_i \cdot 2^i \quad \text{mit } e_i \in \{0, 1\}.$$

Um die binäre Entwicklung zu berechnen, benutzen wir den folgenden Algorithmus:

(i) Setze $i = 0$

(ii) Ist e ungerade, so setzen wir $e_i = 1$ und ersetzen e durch $e := \frac{(e-1)}{2}$. Ist e gerade, so setzen wir $e_i = 0$ und ersetzen e durch $e := \frac{e}{2}$.

(iii) Ersetze i durch $i := i+1$ und wiederhole die Schritte (ii) und (iii) bis schließlich $e = 0$ ist.

Schritt 2. Wir berechnen nun $a^{2^i} \mod m$ für $i = 0, \ldots, k$ indem wir benutzen, dass $a^{2^{i+1}} = a^{2^i \cdot 2} = (a^{2^i})^2$.

Schritt 3. Wir benutzen dass $a^e = a^{\sum_{i=1}^{k} e_i \cdot 2^i} = \prod_{i=0}^{k} a^{2^i \cdot e_i} = \prod_{i: e_i \neq 0} a^{2^i}$.

Beispiel. Wir wollen $6^{73} \mod 100$ berechnen.
Schritt 1. Wir berechnen die binäre Entwicklung von e:
Da e ungerade ist, ist $e_0 = 1$ und wir ersetzen e durch $e := \frac{e-1}{2} = 36$.
Es ist $e = 36$ gerade, also ist $e_1 = 0$ und wir ersetzen e durch $e := \frac{e}{2} = 18$.
Es ist $e = 18$ gerade, also ist $e_2 = 0$ und wir ersetzen e durch $e := \frac{e}{2} = 9$.
Es ist $e = 9$ ungerade, also ist $e_3 = 1$ und wir ersetzen e durch $e := \frac{e-1}{2} = 4$.
Es ist $e = 4$ gerade, also ist $e_4 = 0$ und wir ersetzen e durch $e := \frac{e}{2} = 2$.
Es ist $e = 2$ gerade, also ist $e_5 = 0$ und wir ersetzen e durch $e := \frac{e}{2} = 1$.
Es ist $e = 1$ ungerade, also ist $e_6 = 1$ und wir ersetzen e durch $e := \frac{e-1}{2} = 0$.
Da nun $e = 0$ ist sind wir fertig. Die binäre Entwicklung von 73 ist also

$$73 = \sum_{i=0}^{6} e_i 2^i = 1 + 2^3 + 2^6.$$

Schritt 2. In diesem Schritt berechnen wir die Potenzen 6^{2^i} für $i = 1, \ldots, 6$.

$$6^2 \equiv 36 \mod 100 \qquad 6^{2^2} \equiv (6^2)^2 \equiv -4 \mod 100$$

$$6^{2^3} \equiv (6^{2^2})^2 \equiv 16 \mod 100 \qquad 6^{2^4} \equiv 16^2 \equiv 56 \mod 100$$

$$6^{2^5} \equiv (56)^2 \equiv 36 \mod 100 \qquad 6^{2^6} \equiv 36^2 \equiv -4 \mod 100$$

Schritt 3. Wir können nun $6^{73} \mod 100$ berechnen:

$$6^{73} \equiv 6^1 \cdot 6^{2^3} \cdot 6^{2^6} \equiv 6 \cdot 16 \cdot (-4) \equiv 16 \mod 100$$

Hätten wir $6^{73} \mod 100$ als $6 \cdot \cdots \cdot 6 \mod 100$ berechnet und in jedem Schritt modulo 100 gerechnet, dann hätten wir 72 Multiplikationen durchführen müssen. Mit Hilfe der schnellen Exponentation waren lediglich $6 + 2 = 8$ Multiplikationen notwendig. Die schlechteste Strategie wäre es gewesen zuerst 6^{73} zu berechnen und erst im letzten Schritt modulo 100 zu rechnen, da 6^{73} eine Zahl mit 57 Dezimalstellen ist.