Aufgabenzettel 4.

4.1. Zwei Beweise für den Kleinen Fermat. Sei p Primzahl.

(a) 1. Beweis (wohl der einfachste!) Zeige mit Induktion nach n: Es gilt $n^p \equiv n \mod p$. Folgere daraus: Ist p kein Teiler von n, so ist $n^{p-1} \equiv 1 \mod p$. (Dabei verwendet man die Regel $(\overline{a} + \overline{b})^p = \overline{a}^p + \overline{b}^p$. Sie gilt für alle Elemente $\overline{a}, \overline{b} \in \mathbb{Z}/p$, warum?)

(b) 2. Beweis. Zeige: Ist $1 \leq a < p$, so liefert die Multiplikation mit $\overline{a}$ eine Permutation der Menge $(\mathbb{Z}/p)^* = \{\overline{1}, \ldots, \overline{p-1}\}$. Folgere daraus: $\prod_{i=1}^{p-1} \overline{ai} = \prod_{i=1}^{p-1} \overline{i}$. Daraus folgt die Behauptung — wieso?.

Zusatz. Man verallgemeinere den Beweis in (b), um den Satz von Euler zu zeigen: Ist $(a, n) = 1$, so ist $a^{\phi(n)} \equiv 1 \mod n$.

4.2. Man bestimme eine Primitivwurzel modulo 17, lege eine Indextabelle an und löse damit die folgenden Gleichungen:

$$x^{20} \equiv 13 \mod 17, \qquad x^{12} \equiv 13 \mod 17,$$
$$x^{48} \equiv 9 \mod 17, \qquad x^{11} \equiv 9 \mod 17.$$

4.3. Schnelles Potenzieren. Sei n eine natürliche Zahl. (a) Zeige per Induktion: n lässt sich eindeutig in der Form $n = \sum_{i=0}^{\infty} a_i 2^i$ mit Zahlen $a_i \in \{0, 1\}$ (natürlich fast alle $a_i = 0$) schreiben (die *dyadische Darstellung* von n).

(b) Zeige, dass man (a) verwenden kann, um für eine reelle Zahl x relativ schnell x^n zu berechnen: Wie sollte man vorgehen? Man möchte die Anzahl der notwendigen Multiplikationen minimieren - Beispiel: Um $x^7 = (x^2 x)^2 x$ zu berechnen, braucht man 4 Multiplikationen.

4.4. (a) Sei $m \in \mathbb{N}$. Zeige: Die Menge $M(m) = \{mz + 1 \mid z \in \mathbb{Z}\}$ ist eine Unterhalbgruppe von $(\mathbb{Z}, \cdot)$.

(b) Zeige: Es gibt unendlich viele Primzahlen der Form $4n-1$ mit $n \in \mathbb{N}$. [Hilfe: Angenommen es gibt nur endlich viele derartige Primzahlen, sagen wir $q_1, \ldots, q_t$. Betrachte die Primteiler der Zahl $4q_1 \cdots q_t - 1$. Zusätzlich verwende (a).]

Präsenz-Aufgaben.

1. Man zeige, dass 2 eine Primitivwurzel modulo 13 ist, lege eine Indextabelle an und löse damit die folgenden Gleichungen:

$$x^{24} \equiv 5 \mod 13, \qquad x^5 \equiv 6 \mod 13,$$
$$x^5 \equiv 9 \mod 13, \qquad x^{28} \equiv 7 \mod 13.$$

2. Zeige: Ist g eine Primitivwurzel modulo n und ist $a \in \mathbb{Z}$ mit $(a, \phi(n)) = 1$, so ist auch g^a eine Primitivwurzel modulo n und man erhält auf diese Weise alle Primitivwurzeln modulo n.

Folgere daraus: Die Anzahl der Primitivwurzeln modulo n ist $\phi(\phi(n))$, sofern es überhaupt Primitivwurzeln gibt.

3. Zeige: Es gibt keine Primitivwurzel modulo 8.

4.1. Let p be a prime.

(a) Use induction on n to show that $n^p \equiv n \mod p$ for all $n \in \mathbb{N}$. Show that this implies: If p does not divide n, then $n^{p-1} \equiv 1 \mod p$. (Hint: Use $(\overline{a} + \overline{b})^p = \overline{a}^p + \overline{b}^p$ for all $\overline{a}, \overline{b} \in \mathbb{Z}/p$, why is this true?)

(b) Show: Multiplication by $\overline{a}$, for any $1 \leq a < p$, yields a permutation of the set $(\mathbb{Z}/p)^* = \{\overline{1}, \ldots, \overline{p-1}\}$; thus $\prod_{i=1}^{p-1} \overline{ai} = \prod_{i=1}^{p-1} \overline{i}$, this yields the little Fermat.

Addition. Generalize the proof (b), in order to get a proof of Euler's theorem: If $(a, n) = 1$, then $a^{\phi(n)} \equiv 1 \mod n$.

4.2. Determine a primitive root modulo 17, and the corresponding index table. Use the table in order to solve the following equations:

$$x^{20} \equiv 13 \mod 17, \quad x^{12} \equiv 13 \mod 17, \quad x^{48} \equiv 9 \mod 17, \quad x^{11} \equiv 9 \mod 17.$$

4.3. Fast calculation of powers. Let $n \in \mathbb{N}$. (a) Use induction in order to show: n can be written uniquely in the form $n = \sum_{i=0}^{\infty} a_i 2^i$ with $a_i \in \{0, 1\}$, almost all $a_i = 0$ (this is the *dyadic presentation* of n).

(b) Use (a) in order to calculate quickly x^n for any $x \in \mathbb{R}$, using a small number of multiplications: For example, in order to calculate $x^7 = (x^2 x)^2 x$, we need 4 multiplications.

4.4. (a) Show that for $m \in \mathbb{N}$, the set $M(m) = \{mz + 1 \mid z \in \mathbb{Z}\}$ is a subsemigroup of $(\mathbb{Z}, \cdot)$.

(b) Show that there are infinitely many primes of the form $4n - 1$ with $n \in \mathbb{N}$. [Hint: Assume that $q_1, \ldots, q_t$ are the only primes of this form. Consider the prime divisors of $4q_1 \cdots q_t - 1$ and use (a).]

1. Show that 2 is a primitive root modulo 13 and determine the corresponding index table. Use the table in order to solve the equations

$$x^{24} \equiv 5 \mod 13, \quad x^5 \equiv 6 \mod 13, \quad x^5 \equiv 9 \mod 13, \quad x^{28} \equiv 7 \mod 13.$$

2. If g is a primitive root modulo n and if $a \in \mathbb{Z}$ satisfies $(a, \phi(n)) = 1$, then also g^a is a primitive root modulo n and all primitive roots modulo n are obtained in this way.

The number of primitive roots modulo n ist either 0 or $\phi(\phi(n))$.

3. There is no primitive root modulo 8.