

Aufgabenzettel 7.

7.1. 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. (Man nennt dies 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.

7.2. Die Zweifachen in einer abelschen Gruppe $(G, +)$, die Quadrate in einer abelschen Gruppe $(G, \cdot)$ (Fortführung der Aufgabe 6.4):

(a) Sei $(G, +)$ eine abelsche Gruppe, additiv geschrieben. Wir betrachten $2G := \{2g \mid g \in G\}$ (dabei ist natürlich $2g = g + g$), also die Menge der *Zweifachen* in G . Zeige:

- (1) Es ist $2G$ immer eine Untergruppe von G .
- (2) Ist G endlich, und ist $|G|$ ungerade, so ist $2G = G$.
- (3) Ist G zyklisch, und ist $|G|$ gerade, so ist $|2G| = \frac{1}{2}|G|$.
- (4) Sind $(G, +), (H, +)$ abelsche Gruppen, so ist $2(G \times H) = 2G \times 2H$.

(b) Nun sei $(G, \cdot)$ eine multiplikativ geschriebene abelsche Gruppe. Man formuliere die entsprechenden Aussagen (1) - (4). Hier betrachten wir also $G^2 = \{g^2 \mid g \in G\}$ - die Menge der *Quadratzahlen* (oder einfach *Quadrate*) in G .

(c) Man gebe eine Formel für die Anzahl der Quadrate in $(\mathbb{Z}/n)^*$ an für $n \in \mathbb{N}$ (natürlich mit Beweis).

7.3. 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.

Wieviele Primitivwurzeln modulo p gibt es also für jede der Primzahlen $p < 50$?

7.4. Mit C_n bezeichnen wir eine zyklische Gruppe der Ordnung n .

(a) Sei $G = C_{n_1} \times \cdots \times C_{n_t}$ mit geraden Zahlen $n_1, \dots, n_t$. Zeige: in G gibt es genau $2^t - 1$ Elemente der Ordnung 2.

(b) Folgere daraus: G lässt sich nicht als Produkt von $t - 1$ zyklischen Gruppen schreiben.

(c) Gesucht sind Zahlen $n_1, \dots, n_{10}$, sodass sich $(\mathbb{Z}/n_i)^*$ als Produkt von i zyklischen Gruppen, nicht aber von $i - 1$ zyklischen Gruppen schreiben lässt.

7.1. Let n be a natural number. (a) Show by induction on n : we can write $n = \sum_{i=0}^{\infty} a_i 2^i$ with numbers $a_i \in \{0, 1\}$ (of course, almost all $a_i = 0$), and this representation is unique. (This is called the *dyadic expansion* of n).

(b) Use (a) in order to provide an algorithm in order to calculate powers x^n fast (here x is any real number). One wants to minimize the number of multiplication! For example, in order to calculate x^7 , one may use $x^7 = (x^2 x)^2 x$ — in this way, only 4 multiplications are needed.

7.2. Doubling in an abelian group $(G, +)$, squaring in an abelian group $(G, \cdot)$ (This is related to exercise 6.4):

(a) Let $(G, +)$ be an abelian group, written with addition. Let $2G := \{2g \mid g \in G\}$ (here $2g = g + g$). Show:

(1) $2G$ is a subgroup of G .

(2) If G is finite, and $|G|$ is odd, then $2G = G$.

(3) If G is cyclic and $|G|$ is even, then $|2G| = \frac{1}{2}|G|$.

(4) If $(G, +), (H, +)$ are abelian groups, then $2(G \times H) = 2G \times 2H$.

(b) Now let $(G, \cdot)$ be an abelian group, written with multiplication. Formulate the corresponding assertions (1) - (4), now using $G^2 = \{g^2 \mid g \in G\}$ - this set is called the set of squares in G .

(c) Determine the number of squares in $(\mathbb{Z}/n)^*$ for $n \in \mathbb{N}$ (with proof!).

7.3. Show: If g is a primitive root modulo n and $a \in \mathbb{Z}$ 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.

Show that this implies that the number of primitive roots modulo n is $\phi(\phi(n))$, provided there is at least one primitive root.

Calculate the number of primitive roots modulo p for all the primes $p < 50$.

7.4. Let C_n denote a cyclic group of order n .

(a) Let $G = C_{n_1} \times \cdots \times C_{n_t}$ with even numbers $n_1, \dots, n_t$. Show: in G there are precisely $2^t - 1$ elements of order 2.

(b) Show that this implies that G cannot be written as a product of $t - 1$ cyclic groups.

(c) Exhibit numbers $n_1, \dots, n_{10}$, such that $(\mathbb{Z}/n_i)^*$ can be written as a product of i cyclic groups, but not as a product of $i - 1$ cyclic groups.