

Der Ring $\mathbb{Z}_n[\sqrt{q}]$. Mersenne Primzahlen

Definition des Ringes $\mathbb{Z}_n[\sqrt{q}]$. Sei n eine natürliche Zahl und sei $q = -1$ oder q ein Produkt verschiedener Primzahlen in ersten Potenzen: $q = p_1 \dots p_k$.

$$\mathbb{Z}_n[\sqrt{q}] = \{a + b\sqrt{q} \mid a, b \in \mathbb{Z}_n\}.$$

Definieren wir eine Abbildung

$$N : \mathbb{Z}_n[\sqrt{q}] \rightarrow \mathbb{Z}_n$$

mit der Regel: $N(a + b\sqrt{q}) = a^2 - qb^2$. Das Element $N(a + b\sqrt{q})$ des Ringes \mathbb{Z}_n heißt *Norm* des Elementes $a + b\sqrt{q}$.

Aufgabe 1. Beweisen Sie, daß die Norm zweier Elemente des Ringes $\mathbb{Z}_n[\sqrt{q}]$ gleich das Produkt ihrer Normen ist.

Aufgabe 2. Beweisen Sie, daß ein Element des Ringes $\mathbb{Z}_n[\sqrt{q}]$ ein Inverses nur dann hat, wenn seine Norm ein Inverses in dem Ring \mathbb{Z}_n hat.

Aufgabe 3. Finden Sie die Ordnung der multiplikativen Gruppe des Ringes $\mathbb{Z}_5[\sqrt{3}]$.

Definition. Eine Mersenne-Zahl M_n ist die Zahl der Form $2^n - 1$.

Aufgabe 4. Beweisen Sie: wenn M_n eine Primzahl ist, dann ist n auch eine Primzahl.

Aufgabe 5. Prüfen Sie nach, daß M_{23} eine zusammengesetzte Zahl ist.

Definition. Lucas Folge L_1, L_2, \dots definiert man mit der Formel:

$$L_1 = 4, \quad L_{n+1} = L_n^2 - 2.$$

Satz. Sei $n > 2$ eine natürliche Zahl. Die Zahl M_n ist eine Primzahl nur dann, wenn L_{n-1} durch M_n teilbar ist.

Aufgabe 6. Prüfen Sie nach, daß M_{31} (Euler, Jahr 1772), M_{61} (Perwuschin, Jahr 1883) und M_{521} (Robinson+Computer, Jahr 1952) Primzahlen sind.