§4 Quadrate in $E(\mathbb{Z}/n\mathbb{Z})$

Wir wollen die Quadratzahlen in $E(\mathbb{Z}/n\mathbb{Z})$ studieren. Dabei betrachten wir insbesondere den Fall $E(\mathbb{Z}/p\mathbb{Z})$ für eine Primzahl p. Wie bereits bekannt, ist

$$E := E(\mathbb{Z}/p\mathbb{Z}) \cong C_{p-1},$$

also

$$E = \langle \bar{t} \rangle$$

für ein $\bar{t} = t + p\mathbb{Z} \in E(\mathbb{Z}/p\mathbb{Z}) \smallsetminus \{p\mathbb{Z}\}$. Die Zahl $t \in \mathbb{Z}$ heißt dann Primitivwurzel modulo p. Die Menge der Quadrate aus E sei im Folgenden mit E^2 bezeichnet. Es ist

$$E^2 = \{\bar{x}^2 \in E \ \mid \ \bar{x} \in E\} \leq E.$$

Einen Ansatz liefert der Gruppen-Homomorphismus

$$\sigma := (\bar{x} \mapsto \bar{x}^2) \colon E \to E.$$

Der Kern zu diesem Gruppen-Homomorphismus ist gegeben durch

$$\mathrm{Kern}(\sigma) = \{\bar{x} \in E \ \mid \ \bar{x}^2 = \bar{1} = 1 + p\mathbb{Z}\} = \langle -\bar{1} \rangle$$

Nach dem Homomorphiesatz für Gruppen gilt nun

$$E/\langle \bar{1} \rangle >= E/\mathrm{Kern}(\sigma) \cong \mathrm{Bild}(\sigma) = E^2,$$

woraus

$$|E^2| = |E/\langle \bar{1} \rangle| = \frac{p-1}{2}$$

folgt. Doch welche Elemente liegen nun in E^2? Gibt es zu einem gegebenen $\bar{a} \in E$ ein $\bar{b} \in E$ mit $\bar{a} = \bar{b}^2$?

Ist zum Beispiel stets $\bar{a} = -\bar{1} \in E^2$? - Dem ist nicht so, es ist etwa

$$\langle \bar{1} \rangle > \leq E(\mathbb{Z}/5\mathbb{Z})^2,$$

aber

$$\langle \bar{1} \rangle > \not\leq E(\mathbb{Z}/7\mathbb{Z})^2.$$

Definition 1 ***(Legendre-Symbol)***
Es seien $a \in \mathbb{N}$ beliebig, p eine Primzahl und $E^2 := \{\bar{x}^2 \in E(\mathbb{Z}/p\mathbb{Z}) \ \mid \ \bar{x} \in E(\mathbb{Z}/p\mathbb{Z})\}$. Wir setzen

$$\left(\frac{a}{p}\right) := \begin{cases} +1, & \text{falls } \bar{a} \in E^2, \\ -1, & \text{falls } \bar{a} \notin E^2. \end{cases}$$

Für $p = 7$ ergibt sich zum Beispiel

$$\left(\frac{1}{7}\right) = \left(\frac{2}{7}\right) = \left(\frac{4}{7}\right) = 1 \text{ und } \left(\frac{3}{7}\right) = \left(\frac{5}{7}\right) = \left(\frac{6}{7}\right) = -1.$$

Satz 1 ***(Eigenschaften von*** $\left(\frac{a}{p}\right)$***)***
Es seien $a, b \in \mathbb{N}$ beliebig sowie p eine Primzahl.
(1) Aus $a \equiv b \bmod p$ folgt $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.
(2) Für alle $a \in \mathbb{Z}$ ist $\left(\frac{a^2}{p}\right) = 1$.
(3) Es ist $\left(\frac{1}{p}\right) = 1$.
(4) $\left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$.
Beweis. Es sei $E := E(\mathbb{Z}/p\mathbb{Z})$ und $E^2 := \{\bar{x}^2 \in E \ \mid \ \bar{x} \in E\}$.
(1) Aus $a \equiv b \bmod p$ folgt $\bar{a} = \bar{b}$ und damit $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

(2) Für alle $a \in \mathbb{Z}$ ist $\overline{a^2} = \bar{a}^2 \in E^2$, also $\left(\frac{a^2}{p}\right) = 1$.

(3) Es ist $\bar{1} = \bar{1}^2 \in E^2$, somit folgt $\left(\frac{1}{p}\right) = 1$.

(4) Da $|E^2| = \frac{p-1}{2}$ ist, folgt $[E : E^2] = 2$, also

$$E = E^2 \,\dot{\cup}\, \bar{t}E^2.$$

(Es gibt kein $\bar{x} \in E$ mit $\bar{t} = \bar{x}^2$, denn $\mathrm{o}(\bar{t}) = |E|$.)

1. Fall: Es sei $\bar{a}, \bar{b} \in E^2$. Dann ist $\bar{a}\bar{b} = \overline{ab} \in E^2$, also folgt

$$\left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right) = 1 \cdot 1 = 1 = \left(\frac{ab}{p}\right).$$

2. Fall: Es sei $\bar{a}, \bar{b} \notin E^2$. Dann ist $\bar{a}\bar{b} = \overline{ab} \in E^2$, also folgt

$$\left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right) = (-1) \cdot (-1) = 1 = \left(\frac{ab}{p}\right).$$

3. Fall: Es sei $\bar{a} \in E^2, \bar{b} \notin E^2$. Dann ist $\bar{a}\bar{b} = \overline{ab} \notin E^2$, also folgt

$$\left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right) = 1 \cdot (-1) = -1 = \left(\frac{ab}{p}\right). \qquad ||$$

Bemerkung 1 Die Abbildung

$$\left(\frac{\cdot}{p}\right) := \left(a \mapsto \left(\frac{a}{p}\right)\right) : \mathbb{Z} \setminus \{0\} \to \{\pm 1\}$$

ist also ein Monoidhomomorphismus.

Satz 2 ***(Eulers Kriterium)***
Es sei $p \neq 2$ eine Primzahl und $a \in \mathbb{Z} \setminus p\mathbb{Z}$ beliebig. Dann gilt

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \bmod p.$$

Beweis. Es sei $\bar{a} \in E := E(\mathbb{Z}/p\mathbb{Z})$ beliebig. Dann ist

$$\bar{a}^{p-1} = \bar{1},$$

denn $\mathrm{o}(\bar{a}) \mid p-1$. Daraus folgt

$$(\bar{a}^{\frac{p-1}{2}} - \bar{1}) \cdot (\bar{a}^{\frac{p-1}{2}} + \bar{1}) = \bar{a}^{p-1} - \bar{1} = \bar{0},$$

also, da $\mathbb{Z}/p\mathbb{Z}$ ein Körper ist,

$$\bar{a}^{\frac{p-1}{2}} \in \{\pm 1\}.$$

1. Fall: Es sei $\left(\frac{a}{p}\right) = 1$. Dann gibt es also ein $\bar{x} \in E$ mit $\bar{a} = \bar{x}^2$. Somit folgt

$$\overline{a^{\frac{p-1}{2}}} = \bar{a}^{\frac{p-1}{2}} = (\bar{x}^2)^{\frac{p-1}{2}} = \bar{x}^{p-1} = \bar{1}$$

und damit

$$a^{\frac{p-1}{2}} \equiv 1 \bmod p.$$

2. Fall: Es sei $\left(\frac{a}{p}\right) = -1$. Weiter sei $\bar{t} \in E$ mit $E = <\bar{t}>$. Dann ist

$$\bar{a} = \bar{t}^k \text{ für ein ungerades } k \in \{0, \ldots, p-1\}.$$

Außerdem ist $\bar{t}^{\frac{p-1}{2}} = -\bar{1}$ das Element der Ordnung 2 in E. Daraus folgt

$$\overline{a^{\frac{p-1}{2}}} = \bar{a}^{\frac{p-1}{2}} = (\bar{t}^j)^{\frac{p-1}{2}} = (\bar{t}^{\frac{p-1}{2}})^j = (-\bar{1})^j = -\bar{1},$$

also

$$a^{\frac{p-1}{2}} \equiv -1 \bmod p. \qquad ||$$

Beispiel 1 Es sei $a = -1$ und p eine Primzahl. Dann ist

$$\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} = \begin{cases} +1, & \text{für } p \equiv 1 \bmod 4, \\ -1, & \text{für } p \equiv 3 \bmod 4, \end{cases} \quad \bmod p.$$

Satz 3 ***(quadratisches Reziprozitätsgesetz von Legendre und Gauss)***
Es seien $p, q \neq 2$ Primzahlen mit $p \neq q$. Dann ist

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$

Beweis. Siehe Literatur über Elementare Zahlentheorie. ||

Beispiel 2 *Es ist*

$$\begin{aligned}
\left(\frac{23}{59}\right) &= \left(\frac{59}{23}\right)\cdot(-1)^{29\cdot 11} \\
&= (-1)\cdot\left(\frac{13}{23}\right) \\
&= (-1)\cdot\left(\frac{23}{13}\right)\cdot(-1)^{11\cdot 6} \\
&= (-1)\cdot\left(\frac{10}{13}\right) \\
&= (-1)\cdot\left(\frac{-3}{13}\right) \\
&= (-1)\cdot\left(\frac{-1}{13}\right)\left(\frac{3}{13}\right) \\
&= (-1)\cdot\left(\frac{13}{3}\right)\cdot(-1)^{6\cdot 1} \\
&= (-1)\cdot\left(\frac{1}{3}\right) \\
&= -1.
\end{aligned}$$

Satz 4 ***(zweite Komplementärformel)*** Es sei $p \neq 2$ eine Primzahl. Dann ist

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

Beweis. Siehe Literatur über Elementare Zahlentheorie. ||

§6 Der Hauptsatz der Arithmetik

Frage 1 Warum gilt der Satz über die Existenz und Eindeutigkeit der Darstellung von natürlichen Zahlen als Produkt von Primzahlen?

Frage 2 Was ist eine Primzahl?

Satz 5 $\sqrt{2}$ ist eine irrationale Zahl.
Beweis. (nach Euklid, ca. 340 - 270 v. Chr.)
Angenommen, $\sqrt{2}$ ist eine rationale Zahl. Dann gibt es $m, n \in \mathbb{N}$ mit $\mathrm{ggT}(m, n) = 1$, so dass

$$\sqrt{2} = \frac{m}{n}.$$

Es folgt

$$2 = \frac{m^2}{n^2}$$

also

$$m^2 = 2n^2.$$

Dann gilt aber $2 \mid m$, es gibt also ein $x \in \mathbb{N}$ mit $m = 2x$. Somit erhalten wir

$$4x^2 = 2n^2$$

also

$$2x^2 = n^2,$$

also $2 \mid n$ im Widerspruch dazu, dass $\mathrm{ggT}(m, n) = 1$ ist. $\qquad ||$

Zur Erinnerung:

Definition 2 ***(größter gemeinsamer Teiler)***
Es seien M ein Monoid und $a, b \in M$. Ein größter gemeinsamer Teiler von a, b ist ein $g \in M$ für das gilt:
(1) $g \mid a$ und $g \mid b$.
(2) Ist $u \in M$ mit $u \mid a$ und $u \mid b$, so folgt $u \mid g$.

Der Beweis zum vorigen Satz benutzte die Existenz und Eindeutigkeit der Primfaktorzerlegung einer natürlichen Zahl.
Gilt in $\mathbb{N}$ stets „aus $2 \mid xy$ folgt $2 \mid x$ oder $2 \mid y$“?

Definition 3 ***(unzerlegbare Elemente)***
Es sei M ein Monoid. Ein Element $u \in M$ heißt *unzerlegbar*, wenn
(1) u kein Nullelement ist ($n \in M$ heißt Nullelement, wenn $nx = n$ für alle $x \in M$),
(2) $u \notin E(M)$ ist und
(3) aus $u = ab$ folgt, dass $a \in E(M)$ oder $b \in E(M)$ ist.

Definition 4 ***(prime Elemente)***
Es sei M ein Monoid. Ein Element $p \in M$ heißt *prim*, wenn
(1) p kein Nullelement ist,
(2) $p \notin E(M)$ ist und
(3) aus $p = ab$ folgt, dass $p \mid a$ oder $p \mid b$.

Frage 3 Ist unzerlegbar gleich prim in allgemeinen Monoiden?

Beispiel 3 (1) In $\mathbb{N}$ ist unzerlegbar gleich prim. Ebenso in $M_1 := 2\mathbb{N}_0 + 1$ und $M_2 := 3\mathbb{N}_0 + 1$.
(2) Betrachten wir jedoch als Gegenbeispiel

$$M := 2\mathbb{N}_0 \cup \{1\}.$$

In diesem Monoid ist 42 unzerlegbar (denn $21 \notin M$), aber nicht prim, denn

$$420 = 6 \cdot 70$$

und

$$42 \nmid 6 \text{ und } 42 \nmid 70.$$

Frage 4 Woran liegt es, dass in $\mathbb{N}$ unzerlegbare Element auch prim sind (und umgekehrt), in allgemeinen Monoiden jedoch nicht?