§ 15. Quadratische Gleichungen modulo m

15.1. In diesem Paragraphen beschäftigen wir uns mit Gleichungen der Gestalt

$$x^2 + Ax + B \equiv 0 \bmod m,$$

wobei a, b und $m \geq 2$ vorgegebene ganze Zahlen sind. Dies lässt sich auch als eine Gleichung im Ring $\mathbb{Z}/m$ auffassen. Ist

$$m = p_1^{k_1} \cdot \ldots \cdot p_r^{k_r}$$

die Primfaktor-Zerlegung von m, so gilt die Isomorphie

$$\mathbb{Z}/m \cong \mathbb{Z}/p_1^{k_1} \times \ldots \times \mathbb{Z}/p_1^{k_1}.$$

Deshalb kann man den allgemeinen Fall auf den Fall, wo $m = p^k$ eine Primzahlpotenz ist, zurückführen. Die Primzahl 2 spielt bei quadratischen Gleichunge eine Sonderrolle; wir behandeln hier nur den Fall ungerader Primzahlen p. Dann ist 2 modulo p^k invertierbar, wir können also im Ring $\mathbb{Z}/p^k$ folgende Umformung vornehmen.

$$x^2 + Ax + B = x^2 + Ax + \frac{A^2}{4} - \frac{A^2}{4} + B = \Big(x + \frac{A}{2}\Big)^2 - \Big(\frac{A^2}{4} - B\Big).$$

Deshalb ist $x^2 + Ax + B = 0$ äquivalent zu

$$\Big(x + \frac{A}{2}\Big)^2 = \frac{A^2}{4} - B.$$

Die Gleichung ist deshalb genau dann lösbar, falls das Element $\Delta := A^2/4 - B$ im Ring $\mathbb{Z}/p^k$ eine Wurzel besitzt. Wir sind deshalb auf den Fall rein-quadratischer Gleichungen

$$x^2 \equiv a \bmod p^k$$

zurückgeführt. Wir behandeln zunächst den Fall $k = 1$. Es interessiert also die Frage, ob für ein vorgegebenes $a \in \mathbb{Z}$ die Kongruenz

$$x^2 \equiv a \bmod p$$

eine Lösung besitzt. In diesem Fall nennt man a einen *quadratischen Rest* modulo p (Abkürzung QR), sonst einen *quadratischen Nicht-Rest* (NR) modulo p.

15.2. Definition. Sei $a \in \mathbb{Z}$ und p eine ungerade Primzahl. Dann wird das *Legendre-Symbol* $\left(\frac{a}{p}\right)$ wie folgt definiert:

$$\Big(\frac{a}{p}\Big) := \begin{cases} 0, & \text{falls } p \mid a, \\ +1, & \text{falls } p \nmid a \text{ und } a \text{ ist QR mod} p, \\ -1, & \text{falls } p \nmid a \text{ und } a \text{ ist NR mod} p. \end{cases}$$

Die Gleichung $x^2 \equiv a \bmod p$ ist also genau dann lösbar, wenn $(\frac{a}{p}) \geqslant 0$. Offenbar gilt

$$a \equiv b \bmod p \quad \Longrightarrow \quad \Big(\frac{a}{p}\Big) = \Big(\frac{b}{p}\Big).$$

15.3. Satz (Euler-Kriterium). *Sei p eine ungerade Primzahl. Dann gilt für jede ganze Zahl a*

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

Beweis. Falls $p \mid a$, sind beide Seiten $\equiv 0 \bmod p$. Wir können also im folgenden voraussetzen, dass $p \nmid a$.

1. Fall: a ist quadratischer Rest modulo p. Dann gibt es eine ganze Zahl b mit $a \equiv b^2 \bmod p$. Natürlich gilt auch $p \nmid b$. Daher folgt aus dem kleinen Satz von Fermat

$$a^{(p-1)/2} \equiv b^{p-1} \equiv 1 \equiv \Big(\frac{a}{b}\Big) \bmod p.$$

2. Fall: a ist quadratischer Nichtrest. Sei g eine Primitivwurzel modulo p. Dann ist $a \equiv g^m$ mit einer ungeraden Zahl $m = 2k+1$. Damit folgt

$$a^{(p-1)/2} \equiv g^{(2k+1)(p-1)/2} \equiv g^{k(p-1)} g^{(p-1)/2} \equiv g^{(p-1)/2} \equiv -1 \equiv \Big(\frac{a}{b}\Big) \bmod p.$$

Bemerkung. Wegen des schnellen Potenzierungs-Algorithmus liefert Satz 15.3 eine effiziente Methode, das Legendre-Symbol zu berechnen. Wir werden aber im nächsten Paragraphen sehen, dass man mittels des quadratischen Reziprozitätsgesetzes das Legendre-Symbol noch schneller berechnen kann.

15.4. Corollar. *Für jede ungerade Primzahl p und alle ganzen Zahlen a, b gilt*

$$\Big(\frac{a}{p}\Big)\Big(\frac{b}{p}\Big) = \Big(\frac{ab}{p}\Big).$$

Insbesondere liefert das Legendre-Symbol einen surjektiven Homomorphismus multiplikativer Gruppen

$$\mathbb{F}_p^* \longrightarrow \{\pm 1\}, \quad a \mapsto \Big(\frac{a}{p}\Big).$$

Aus der Multiplikativität des Legendre-Symbols folgt z.B. dass das Produkt zweier quadratischer Nichreste ein quadratischer Rest ist. Aus dem Corollar folgt ferner, dass es in $\mathbb{F}_p^*$ ebenso viele quadratische Reste wie Nichtreste gibt.

15.5. Berechnung von Quadratwurzeln modulo p. Sei p eine ungerade Primzahl und a eine ganze Zahl mit $(\frac{a}{p}) = 1$. Wir wollen untersuchen, wie man eine Lösung der Kongruenz $x^2 \equiv a \bmod p$ effizient berechnen kann. Wir müssen zwei Fälle unterscheiden.

1. Fall: $p \equiv 3 \bmod 4$. Nach dem Euler-Kriterium ist

$$a^{(p-1)/2} \equiv 1 \bmod p.$$

Multiplikation dieser Gleichung mit a ergibt

$$a^{(p+1)/2} \equiv a \bmod p.$$

Da $p \equiv 3 \bmod 4$, ist $(p+1)/2$ eine gerade Zahl, also

$$x := a^{(p+1)/4} \bmod p$$

eine Lösung der Kongruenz $x^2 \equiv a \bmod p$.

2. Fall: $p \equiv 1 \bmod 4$. Hier kann der obige Trick nicht verwendet werden. Wir schreiben

$$p - 1 = 2^s u, \quad \text{wobei } s \geqslant 2, \text{ und } u \text{ ungerade.}$$

Nach dem Euler-Kriterium ist

$$a^{2^{s-1}u} \equiv 1 \bmod p, \quad \text{also} \quad (a^u)^{2^{s-1}} \equiv 1 \bmod p.$$

Nach Satz 13.3 liegt also das Element $b := a^u \bmod p$ in der zyklischen Untergruppe

$$G(2^{s-1}) := \{x \in \mathbb{F}_p^* : x^{2^{s-1}} = 1\} \subset \mathbb{F}_p^*$$

der Ordnung 2^{s-1} von $\mathbb{F}_p^*$. Um zu einem erzeugenden Element von $G(2^{s-1})$ zu kommen, wählen wir einen quadratischen Nichtrest $y \bmod p$. Dann gilt

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

Es folgt für $z := y^{2u} \bmod p$, dass

$$z^{2^{s-2}} \equiv -1 \bmod p.$$

Daraus folgt, dass $z \bmod p$ die Ordnung 2^{s-1} hat, also ein erzeugendes Element von $G(2^{s-1})$ ist. Nach der in 13.6 besprochenen Methode lässt sich das diskrete Logarithmus-Problem in $G(2^{s-1})$ effizient lösen, wir können also eine ganze Zahl k konstruieren, so dass

$$a^u \equiv b \equiv z^k \equiv y^{2ku} \bmod p \quad \Longrightarrow \quad a^u y^{-2ku} \equiv 1 \bmod p.$$

(Das Inverse von $y \bmod p$ lässt sich entweder mit dem erweiterten Euklidischen Algorithmus bestimmen, oder man verwendet $y \cdot y^{p-2} \equiv 1 \bmod p$.) Aus der letzten Gleichung folgt durch Multiplikation mit a

$$a^{u+1} y^{-2ku} \equiv a \bmod p \quad \Longrightarrow \quad (a^{(u+1)/2} y^{-ku})^2 \equiv a \bmod p,$$

d.h. $x := a^{(u+1)/2}y^{-ku} \bmod p$ ist eine Quadratwurzel von $a \bmod p$.

15.6. Berechnung von Quadratwurzeln modulo p^n. Trivialerweise folgt aus einer Kongruenz $x^2 \equiv a \bmod p^n$ die Kongruenz $x^2 \equiv a \bmod p$. Umgekehrt kann man aus einer Lösung der Kongruenz modulo p eine Lösung modulo p^n konstruieren. Es gilt nämlich:

Sei p eine ungerade Primzahl, $n \geq 2$ und a mit $p \nmid a$ ein quadratischer Rest $\bmod p$*, d.h. $x_0^2 \equiv a \bmod p$ mit einer ganzen Zahl x_0. Dann gibt es eine* $\bmod\ p^n$ *eindeutig bestimmte ganze Zahl x mit*

$$x^2 \equiv a \bmod p^n \quad \textit{und} \quad x \equiv x_0 \bmod p.$$

Beweis. a) Eindeutigkeit. Es seien x, y zwei Lösungen. Aus $x^2 \equiv y^2 \bmod p^n$ folgt

$$(x-y)(x+y) \equiv 0 \bmod p^n.$$

Da $x \equiv y \equiv x_0 \bmod p$, folgt $x + y \equiv 2x_0 \bmod p$. Daher ist $x + y$ invertierbar $\bmod p^n$, also $x \equiv y \bmod p^n$.

b) Existenz. Wir verwenden das bekannte Newtonsche Näherungs-Verfahren (siehe z.B. Forster, Analysis 1, §6) zur Bestimmung der Quadratwurzel. Ausgehend von dem Anfangswert x_0 definieren wir die Folge

$$x_{k+1} := \frac{1}{2}\left(x_k + \frac{a}{x_k}\right) \quad \text{in } \mathbb{Z}/p^n.$$

Man beachte, dass x_0 invertierbar $\bmod p^n$ ist. Durch Induktion ergibt sich $x_k \equiv x_0 \bmod p$ für alle k, also ist a/x_k als Element von $\mathbb{Z}/p^n$ wohldefiniert. Aus der Rekursionsformel erhält man

$$x_{k+1}^2 - a = \frac{(x_k^2 - a)^2}{4x_k^2} \quad \text{in } \mathbb{Z}/p^n,$$

woraus folgt

$$x_{k+1}^2 - a \equiv 0 \bmod p^m \quad \text{mit } m := \min(2^k, n).$$

Sobald $2^k \geq n$, hat man also $x_{k+1}^2 \equiv a \bmod p^n$ und damit die gesuchte Lösung gefunden.

Es ist bemerkenswert, dass das für die reelle Analysis entwickelte Newtonsche Näherungs-Verfahren auch hier für endliche Ringe anwendbar ist und nach endlich vielen Schritten eine exakte Lösung liefert.