§4. Die Ringe $\mathbb{Z}/m\mathbb{Z}$

In diesem Kapitel beschäftigen wir uns mit Kongruenzen modulo m, für $m \in \mathbb{N}, m > 1$.

1. **Def** Für $m \in \mathbb{N}$, $m \geq 1$, sei $\varphi(m) = \#(\mathbb{Z}/m\mathbb{Z})^*$ die Anzahl der Einheiten des endlichen Rings $\mathbb{Z}/m\mathbb{Z}$. Man nennt φ die Eulersche φ-Funktion.

Lemma Sei $m \in \mathbb{N}$, $m \geq 1$, sei $a \in \mathbb{Z}$. Dann ist $[a]_m$ genau dann eine Einheit in $\mathbb{Z}/m\mathbb{Z}$, wenn gilt $\operatorname{ggT}(a,m) = 1$.

Beweis $[a]_m$ ist Einheit $\Leftrightarrow$ es gibt $b \in \mathbb{Z}$ mit $[a]_m \cdot [b]_m = [1]_m \Leftrightarrow$ es gibt $b \in \mathbb{Z}$ mit $a \cdot b = 1 + k \cdot m$ für ein $k \geq 0 \overset{\S 2.7}{\Leftrightarrow} \operatorname{ggT}(a,m) \mid 1$ $\Leftrightarrow \operatorname{ggT}(a,m) = 1$ $\square$

Korollar Sei $S(m) = \{a \in \mathbb{Z} \mid 1 \leq a \leq m \text{ und } \operatorname{ggT}(a,m) = 1\}$ (für $m \in \mathbb{N}$, $m \geq 1$). Dann gilt $\varphi(m) = \# S(m)$

(vgl. §2.12)

2. Theorem (Euler) Sei $m \in \mathbb{N}$, $m \geq 1$.
Sei $a \in \mathbb{Z}$ mit $\text{ggT}(a,m) = 1$. Dann gilt

$$a^{\varphi(m)} \equiv 1 \pmod m$$

<u>Beweis</u> Nach § 4.1 gilt $[a]_m \in (\mathbb{Z}/m\mathbb{Z})^*$.
Die Gruppe $((\mathbb{Z}/m\mathbb{Z})^*, \cdot)$ hat $\varphi(m)$ Elemente, also teilt $d = o([a]_m)$ die Zahl $\varphi(m)$, d.h.
$\varphi(m) = d \cdot k$ für ein $d \in \mathbb{Z}$. Es folgt

$$\begin{array}{l} [a]_m^{d \cdot k} = [a^{d \cdot k}]_m \\ \shortparallel \\ [1]_m \end{array}$$

$\square$

3. <u>Erinnerung</u> Ein kommutativer Ring $(K, +, \cdot)$ heißt <u>Körper</u>, wenn gilt $K^* = K - \{0\}$.

<u>Bsp</u>
- $(\mathbb{Z}, +, \cdot)$ ist <u>kein</u> Körper, denn
$$\mathbb{Z}^* = \{\pm 1\} \neq \mathbb{Z} - \{0\}$$
- $(\mathbb{N}, +, \cdot)$ ist kein Ring, also auch <u>kein</u> Körper
- $(\mathbb{Q}, +, \cdot)$ und $(\mathbb{R}, +, \cdot)$ sind Körper
- Der Nullring $R = \{0\}$ ist <u>kein</u> Körper, denn $R - \{0\} = \emptyset \neq R^* = R$

4. <u>Satz</u> Sei $m \in \mathbb{N}$. Dann sind äquivalent:

(i) $\mathbb{Z}/m\mathbb{Z}$ ist ein Körper

(ii) $m \in \mathbb{P}$

<u>Beweis</u> Für $m = 0$ gilt $[a]_0 = \{a\}$ und $\mathbb{Z}/0\mathbb{Z}$ ist genau wie $\mathbb{Z}$ kein Körper, $(\mathbb{Z}/0\mathbb{Z})^* = \{[\pm 1]_0\}$

Für $m = 1$ gilt $\mathbb{Z}/\mathbb{Z} = \{[0]_1\}$, das ist der Nullring und kein Körper.

Ist $m \in \mathbb{P}$, so gilt für alle $1 \leq a < m$, dass $ggT(a,m) = 1$ (weil $1, m$ die einzigen Teiler von m sind) $\rightsquigarrow S(m) = \{1, \dots, m-1\}$

$\rightsquigarrow (\mathbb{Z}/m\mathbb{Z})^* = \{[1]_m, \dots, [m-1]_m\} = \mathbb{Z}/m\mathbb{Z} - \{[0]_m\}$.

Ist $m \geq 2$ <u>keine</u> Primzahl, so gibt es k mit $1 < k < m$ mit $k \mid m \rightsquigarrow ggT(k,m) = k \neq 1$

$\Rightarrow [k]_m \notin (\mathbb{Z}/m\mathbb{Z})^* \Rightarrow (\mathbb{Z}/m\mathbb{Z})^* \neq \mathbb{Z}/m\mathbb{Z} - \{[0]_m\}$ $\square$

Also gilt für $m \geq 1$:

$$\varphi(m) = m - 1 \iff m \in \mathbb{P}$$

$(\varphi(1) = 1)$	$\varphi(2) = 1$	$\varphi(3) = 2$
$\varphi(4) = 2$	$\varphi(5) = 4$	$\varphi(6) = 2$
$\varphi(7) = 6$	$\varphi(8) = 4$	$\varphi(9) = 6$

5. <u>Korollar</u> (Satz von Fermat) Sei $p \in \mathbb{P}$.

Ist $a \in \mathbb{Z}$ mit $p \nmid a$, so gilt

$$a^{p-1} \equiv 1 \pmod{p}$$

Für jedes $a \in \mathbb{Z}$ gilt $a^p \equiv a \pmod{p}$

<u>Beweis</u> Die erste Behauptung ist ein Spezialfall von Eulers Satz §4.2, da $\varphi(p) = p-1$.

Es folgt dann auch $a^p \equiv a \pmod{p}$.

Ist $p \mid a$, so ist $a \equiv 0 \pmod{p}$, also gilt auch in diesem Falle $a^p \equiv a \pmod{p}$ $\square$

6. Sei R ein kommutativer Ring. Erinnerung: ein <u>Polynom</u> mit Koeffizienten in R in der Variablen T ist eine Linearkombination

$$f = a_n T^n + a_{n-1} T^{n-1} + \dots + a_0$$

Die $a_j \in R$ heißen <u>Koeffizienten</u> des Polynoms. Zwei Polynome sind gleich, wenn alle ihre Koeffizienten gleich sind. Ist $a_n \neq 0$, so heißt a_n <u>Leitkoeffizient</u> von f und $n = \deg(f)$ der <u>Grad</u> des Polynoms.

Für das <u>Nullpolynom</u> $f = 0$ (alle Koeffizienten sind 0) setzt man $\deg(0) = -\infty$.

Die Menge aller Polynome mit Koeffizienten in R in der Variablen T bildet einen kommutativen Ring

$$R[T] = \{ f = a_n T^n + \dots + a_0 \mid n \geq 0,\ a_0, \dots, a_n \in R \},$$

den Polynomring (mit der üblichen Addition und Multiplikation), vgl. Lin. Algebra.

Lemma Sei K ein Körper, sei $g, f \in K[T]$.
Dann gilt (i) $\deg(f+g) \leq \max\{\deg(f), \deg(g)\}$
(ii) $\deg(f \cdot g) = \deg(f) + \deg(g)$

Beweis Schreibe $f = a_m T^m + \dots + a_0$, $g = b_n T^n + \dots + b_0$
Beh (i) ist klar durch Aufschreiben der Koeffizienten von $f+g$.
Zu (ii) Sei $\deg(f) = m$ und $\deg(g) = n$, also $a_m \neq 0 \neq b_n$. Der Leitkoeffizient von $f \cdot g = a_m b_n T^{m+n} + \dots + a_0 b_0$ ist $a_m \cdot b_n \neq 0$, da $a_m, b_n \neq 0$ $\square$

Bem (i) Gilt auch in $R[T]$, wenn R ein kommutativer Ring ist. Bei (ii) gilt dann aber nur "$\leq$".

7. **Satz** (Teilen mit Rest) Sei $(K,+,\cdot)$ ein Körper, seien $f,g \in K[T]$ Polynome mit $g \neq 0$. Dann gibt es eindeutig bestimmte Polynome h,r in $K[T]$ mit $\deg(r) < \deg(g)$ und

$$f = g \cdot h + r$$

(vgl. §1.5).

Beweis der Existenz von h,r mit Induktion nach $n = \deg(f)$. Für $n < \deg(g) = m$ ist nichts zu zeigen, setze $h = 0$ und $r = f$. (Das gilt auch, wenn $f = 0$.) Sei nun $\deg(f) \geq \deg(g)$.

$f = a_n T^n + \ldots + a_0$, $g = b_m T^m + \ldots + b_0$.

Betrachte $\tilde{f} = f - g \cdot \frac{a_n}{b_m} T^{n-m} \Rightarrow \deg(\tilde{f}) < n$,

also $\tilde{f} = g \cdot \tilde{h} + r$ mit $\deg(r) < m$.

$$\Rightarrow f = \tilde{f} + g \frac{a_n}{b_m} T^{n-m} = g\left(\frac{a_n}{b_m} T^{n-m} + \tilde{h}\right) + r \quad (\checkmark)$$

Zur Eindeutigkeit von h,r: angenommen,

$$f = g h_1 + r_1 = g h_2 + r_2 \qquad \deg(r_1), \deg(r_2) < \deg(g)$$

$$g(h_1 - h_2) = r_2 - r_1$$

$$m + \deg(h_1 - h_2) = \deg(r_2 - r_1) < m \Rightarrow h_1 - h_2 = 0$$

$$\Rightarrow r_1 = r_2$$

$\square$

Def Ein Element $\lambda \in R$ heißt Wurzel (oder Nullstelle) des Polynoms $f \in R[T]$, $f = a_m T^m + \dots + a_0$, wenn

$$f(\lambda) = a_m \lambda^m + \dots + a_0 = 0$$ gilt.

(mit $\deg(f) \geq 1$)

8. **Satz** Sei $(K,+,\cdot)$ ein Körper und sei $f \in K[T]$. Wenn $\lambda \in K$ eine Wurzel von f ist, so gibt es genau ein $h \in K[T]$ mit $f = (T-\lambda)h$.

Beweis Setze $g = T - \lambda \in K[T] \Rightarrow \deg(g) = 1$

Teilen mit Rest:

$$f = g \cdot h + r \qquad \deg(r) < 1 \Rightarrow r \text{ konstantes Polynom}$$

$$\underbrace{f(\lambda)}_{=0} = \underbrace{g(\lambda)\cdot h(\lambda)}_{=0} + r(\lambda) \qquad \Rightarrow r = 0$$

Die Eindeutigkeit folgt aus dem vorigen Satz $\square$

Korollar Ist $(K,+,\cdot)$ ein Körper und $f \in K[T]$ mit $\deg(f) = n \geq 0$, so hat f höchstens n verschiedene Wurzeln.

Beweis Seien $\lambda_1, \dots, \lambda_k$ Wurzeln von f, $\lambda_i \neq \lambda_j$ für $i \neq j$. Es folgt

$$f = (T-\lambda_1)\cdot h_1 \qquad 0 = f(\lambda_2) = \underbrace{(\lambda_2 - \lambda_1)}_{\neq 0} h_1(\lambda_2)$$

$$\Rightarrow h_1(\lambda_2) = 0 \Rightarrow f = (T-\lambda_1)\underbrace{(T-\lambda_2)h_2}_{=h_1} \quad \text{usw}$$

$$\Rightarrow f = (T-\lambda_1)\cdots(T-\lambda_k)\cdot h_k, \qquad h_k \neq 0$$

$\Rightarrow \deg(f) = k + \deg(h_k) \Rightarrow k \leq \deg(f)$ $\square$

9. <u>Theorem</u> (Satz von Wilson)

Sei $m \in \mathbb{N}$ mit $m \geq 2$. Dann sind äquivalent:

(i) $m \in \mathbb{P}$

(ii) $(m-1)! = 1 \cdot 2 \cdot 3 \cdots (m-1) \equiv -1 \pmod m$.

<u>Beweis</u> (ii) $\Rightarrow$ (i) Sei $k = (m-1)!$. Es gilt dann $k \cdot k \equiv 1 \pmod m$. Für $1 \leq a < m$ gilt $a \mid k$, also $k = a \cdot b$ für ein $b \in \mathbb{N}$. Damit $k^2 = a(a \cdot b^2) \equiv 1 \pmod m \Rightarrow [a]_m$ ist Einheit. Nach § 4.1 folgt $ggT(m, a) = 1$. Da das für alle $1 \leq a < m$ gilt, folgt $m \in \mathbb{P}$.

(i) $\Rightarrow$ (ii) Für $m \in \mathbb{P}$ ist $\mathbb{Z}/m\mathbb{Z}$ ein Körper nach § 4.4., also $(\mathbb{Z}/m\mathbb{Z})^* = \mathbb{Z}/m\mathbb{Z} - \{[0]_m\}$. Zu jedem $1 \leq a < m$ gibt es also genau ein b mit $1 \leq b < m$ so, dass $a \cdot b \equiv 1 \pmod m$. $[\Leftrightarrow [a]_m \cdot [b]_m = [1]_m]$. Daher gilt

$$a = b \Leftrightarrow [a]_m^2 = [1]_m \overset{§4.8}{\Leftrightarrow} [a]_m = \pm [1_m]$$

$\Leftrightarrow a = 1, m-1$. Folglich gilt

$$2 \cdot 3 \cdot 4 \cdots (m-2) \equiv 1 \pmod m$$

$\Rightarrow 1 \cdot 2 \cdot 3 \cdots (m-1) \equiv -1 \pmod m$ $\square$

<u>Bem</u> Als Primzahltest ist Wilsons Satz ungeeignet, da die Berechnung von $(n-1)!$ sehr rechenaufwendig ist.

<u>Korollar</u> Sei $p \in \mathbb{P}$ ungerade Primzahl, $p = 2l+1$.

Dann gilt $(l!)^2 \equiv (-1)^{l+1} \pmod p$

<u>Beweis</u> Umschreiben

$$1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-1) = 1 \cdot (p-1) \cdot 2 \cdot (p-2) \cdots l \cdot (p-l)$$

$$\equiv 1 \cdot (-1) \cdot 2(-2) \cdot \ldots \cdot l(-l) \pmod p$$

$$1 \cdot (-1) \cdot 2(-2) \ldots l(-l) = (l!)^2 \cdot (-1)^{l+1}$$

Insgesamt also $(l!)^2 \equiv (-1)^{l+1} \pmod p$ $\square$

<u>Korollar</u> Ist $p \in \mathbb{P}$ von der Form $p = 4k+1$, so gilt $((2k)!)^2 \equiv -1 \pmod p$, d.h. das Polynom T^2+1 hat eine Wurzel in $\mathbb{Z}/p\mathbb{Z}$. $\square$

Um solche Wurzeln geht es im Folgenden. Dazu brauchen wir einen Satz über zyklische Gruppen.

10. <u>Lemma A</u> Sei $m \geq 1$. Für jedes $d \geq 1$ mit $d \mid m$ gibt es <u>genau ein</u> Untergruppe $A_d \subseteq \mathbb{Z}/m\mathbb{Z}$ mit d Elementen, nämlich

$$A_d = \{ [x]_m \mid d \cdot [x]_m = [0]_m \}$$

<u>Beweis</u> Schreibe $m = d \cdot m'$. Nach dem Kriterium §3.4 ist A_d eine Untergruppe und nach §3.15 ist $A_d = \langle [m']_m \rangle$ zyklisch. Für $1 \leq s < d$ ist $s \cdot [m']_m = [s \cdot m']_m \neq [0]_m$ und $d \cdot [m']_m = [0]_m$, also $\# A_d = d = o([m']_m)$.

Ist $H \subseteq \mathbb{Z}/m\mathbb{Z}$ Untergruppe mit d Elementen, so folgt für alle $[x]_m \in H$, dass $d \cdot [x]_m = [0]_m$, also $H \subseteq A_d$. Da $\# H = \# A_d = d$, folgt $H = A_d$ $\square$

#

<u>Lemma B</u> Sei $(G, \cdot)$ eine Gruppe, sei $g \in G$ mit $o(g) = m < \infty$. Sei $k \geq 1$. Es gilt

$o(g^k) = o(g)$ genau dann, wenn $ggT(k, m) = 1$

<u>Beweis</u> Wenn $ggT(k,m) = 1$, so gibt es $u, v \in \mathbb{Z}$ mit $uk + v \cdot m = 1$ $\Rightarrow$ $\underset{\substack{\parallel \\ g}}{g^{uk+v \cdot m}} = (g^k)^u \cdot \underbrace{(g^m)^v}_{=e} = (g^k)^u$

$\Rightarrow \langle g^k \rangle = \langle g \rangle$ und $o(g^k) = o(g)$

Wenn $o(g) = o(g^k)$, so $\langle g^k \rangle = \langle g \rangle$

$\Rightarrow (g^k)^u = g$ für ein $u \in \mathbb{Z}$

Also $k \cdot a \equiv 1 \pmod{m} \Rightarrow ggT(k, m) = 1$ □

Lemma C Sei $m \geq 1$. Dann gilt

$$m = \sum_{\substack{d \geq 1 \\ d | m}} \varphi(d)$$

Beweis Für jeden Teiler $d \geq 1$ von m gibt es genau $\varphi(d)$ Elemente in A_d mit Ordnung d nach Lemma B und Lemma A, und $\mathbb{Z}/m\mathbb{Z}$ hat insgesamt m Elemente. □

Theorem Sei $(G, \cdot)$ eine endliche abelsche Gruppe, $\# G = m$. Wenn es für jedes $d \geq 1$ mit $d | m$ höchstens d Elemente $g \in G$ gibt mit $g^d = e$, so ist G zyklisch.

Beweis Setze $\alpha(d) = \#\{ g \in G \mid o(g) = d \}$

Ist $g \in G$ mit $o(g) = d$, so gilt $d \geq 1$ und $d | m$, vgl. §3,16. Für alle $g^k \in \langle g \rangle$ gilt dann $(g^k)^d = e$, also folgt

$$\langle g \rangle = \{ x \in G \mid x^d = e \} \quad \text{nach Voraussetzung}$$

Damit auch $\alpha(d) = \varphi(d)$ nach Lemma B.

Es folgt

$$m = \sum_{d \geq 1} \alpha(d) = \sum_{\substack{d \geq 1 \\ d \mid m}} \alpha(d) \leq \sum_{\substack{d \geq 1 \\ d \mid m}} \varphi(d) \underset{\substack{\uparrow \\ \text{Lemma 9}}}{=} m$$

Und damit $\alpha(d) = \varphi(d)$ für alle $d \geq 1$ mit $d \mid m$. Insbesondere $\alpha(m) = \varphi(m) \geqq 1$
$\Rightarrow$ es gibt $x \in G$ mit $o(x) = m \Rightarrow \langle x \rangle = G$ □

11. Theorem Sei $(K,+,\cdot)$ ein Körper und sei $G \subseteq K^*$ eine Untergruppe von $(K^*,\cdot)$. Wenn G endlich ist, so ist G zyklisch.

Beweis Sei $g \in G$. Wenn gilt $g^k = 1$, so ist g Wurzel von $T^k - 1$. Nach §4.8 gibt es höchstens k verschiedene Wurzeln dieses Polynoms. Also können wir §4.10 anwenden

□

Korollar Ist $p \in \mathbb{P}$, so ist die Einheitengruppe $(\mathbb{Z}/p\mathbb{Z})^*$ zyklisch. Insbesondere existiert also $\xi \in \mathbb{Z}$ so, dass

$$\underbrace{\{[1]_p, [2]_p, \ldots, [p-1]_p\}}_{(\mathbb{Z}/p\mathbb{Z})^*} = \{[\xi]_p, [\xi^2]_p, \ldots, [\xi^{p-1}]_p\}$$

Achtung, die Reihen-Folgen rechts und links können verschieden sein!

Man nennt ξ eine Primitivwurzel modulo p.

Beispiel $p=5$

(a) $\xi=2 \leadsto \underline{2}, 2^2=\underline{4}, 2^3=5+\underline{3}, 2^4=16=3\cdot 5+\underline{1}$

(b) $\xi=3 \leadsto \underline{3}, 3^2=5+\underline{4}, 3^3=25+\underline{2}, 3^4=80+\underline{1}$

12. Satz Sei $p\in\mathbb{P}$, sei $m\geq 1$ und sei $d=\mathrm{ggT}(m,p-1)$. Sei $a\in\mathbb{Z}$ mit $p\nmid a$.

Dann sind äquivalent:

(i) $T^m-[a]_p$ hat eine Wurzel, d.h. es gibt $x\in\mathbb{Z}$ mit $x^m\equiv a \pmod p$

(ii) $T^d-[a]_p$ hat eine Wurzel, d.h. es gibt $y\in\mathbb{Z}$ mit $y^d\equiv a \pmod p$

(iii) $a^{(p-1)/d}\equiv 1 \pmod p$

Beweis Schreibe $m=m'd$ und $p-1=kd$

(i) $\Rightarrow$ (ii) mit $y=x^{m'}$

(ii) $\Rightarrow$ (iii) $a^{(p-1)/d}\equiv y^{(p-1)}\equiv 1$ nach §4,5 (Satz von Fermat)

(iii) $\Rightarrow$ (i) Sei ξ Primitivwurzel modulo p

Dann gibt es $s \geq 1$ mit $a \equiv \xi^s \pmod p$

Also $a^{(p-1)/d} \equiv \xi^{s \cdot k} \equiv 1 \pmod p$

$\Rightarrow \quad p-1 = k \cdot d \mid s \cdot k \Rightarrow d \mid s$, schreibe $s = s' \cdot d$.

Es gibt $u, v \in \mathbb{Z}$ mit $d = u \cdot m + v \cdot (p-1) = \mathrm{ggT}(m, p-1)$

$$a \equiv \xi^{s' \cdot d} \equiv \xi^{s' \cdot u \cdot m} \cdot \overset{\equiv 1}{\cancel{\xi^{s' \cdot v(p-1)}}} \equiv \left(\xi^{s' u}\right)^m \pmod p$$

also gilt für $x = \xi^{s' u}$, dass $x^m \equiv a \pmod p$ $\square$

<u>Beispiel</u> $p = 7 \quad m = 3 = d$

Die Kongruenz $x^3 \equiv a \pmod 7$ hat eine Lösung genau dann, wenn $a^2 \equiv 1 \pmod 7$

$$\Leftrightarrow a \equiv 1, 6 \pmod 7$$

Wir betrachten jetzt Quadratwurzeln modulo p, d.h. Lösungen von Gleichungen $x^2 \equiv a \pmod p$. Für $p = 2$ ist das einfach, wir konzentrieren uns auf <u>ungerade</u> Primzahlen p.

13. Sei $p \in \mathbb{P}$ mit $p \geq 3$. Eine Zahl $a \in \mathbb{Z}$ heißt <u>quadratisches Residuum modulo p</u>, wenn $p \nmid a$ und wenn es $x \in \mathbb{Z}$ gibt mit

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

Das **Legendre-Symbol** ist definiert als

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{falls es } x \in \mathbb{Z} \text{ gibt mit } x^2 \equiv a \pmod p \\ -1 & \text{sonst} \end{cases}$$

(Das Legendre-Symbol ist nur definiert wenn $p \nmid a$!)
und wenn $p \in \mathbb{P}$ mit $p \geq 3$!)

14. Satz Sei $p \in \mathbb{P}$ ungerade, $p = 2l+1$.
Sei $a \in \mathbb{Z}$ mit $p \nmid a$.
Dann gilt $a^l \equiv \pm 1 \pmod p$

sowie $\left(\frac{a}{p}\right) \equiv a^l \pmod p$

Beweis Für $b = a^l$ gilt $b^2 = a^{2l} = a^{p-1} \equiv 1 \pmod p$
nach Fermats Satz §4.5 und damit $a^l \equiv \pm 1 \pmod p$
Wende jetzt §4.12 an mit $m = 2 = d$
und $l = \frac{p-1}{2}$ □

Korollar Sei $p \in \mathbb{P}$ ungerade. Dann gilt

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{wenn } p \equiv 1 \pmod 4 \quad (\text{vgl. §4.9}) \\ -1 & \text{wenn } p \equiv 3 \pmod 4 \end{cases}$$

Beweis Schreibe $p = 2l+1$. Dann ist l genau
dann gerade, wenn $p \equiv 1 \pmod 4$

und genau dann gilt

$$(-1)^{\ell} \equiv 1 \pmod{p} \qquad \Box$$

15. <u>Def</u> Sei $p \in \mathbb{P}$ ungerade, $p = 2\ell+1$. Eine Menge $\{u_1, \ldots, u_\ell\} \subseteq \mathbb{Z}$ heißt <u>Gauß'sche Menge</u>, wenn gilt

$$(\mathbb{Z}/p\mathbb{Z})^* = \{\pm[u_1]_p, \pm[u_2]_p, \ldots, \pm[u_\ell]_p\}$$

Zum Beispiel ist $\{1, 2, 3, \ldots, \ell\} \subseteq \mathbb{Z}$ eine Gauß'sche Menge, denn $p - k \equiv -k \pmod{p}$

16 <u>Lemma</u> (Gauß) Sei $p \in \mathbb{P}$ ungerade und sei $p = 2\ell+1$. Sei $\{u_1, \ldots, u_\ell\}$ eine Gauß'sche Menge. Sei $a \in \mathbb{Z}$ mit $p \nmid a$.

Wir definieren Zahlen $\varepsilon_1, \ldots, \varepsilon_\ell \in \{\pm 1\}$ durch $a \cdot u_i \equiv \varepsilon_i \cdot u_j \pmod{p}$

Dann gilt $\left(\frac{a}{p}\right) = \varepsilon_1 \cdot \varepsilon_2 \cdots \varepsilon_\ell$

<u>Beweis</u> Zu jedem $x \in \mathbb{Z}$ mit $p \nmid x$ gibt es genau ein i so, dass $x \equiv \pm u_i \pmod{p}$

Denn: $\pm u_i \equiv u_j \pmod{p}$

$$\Rightarrow \#\{\pm[u_1]_p, \ldots, \pm[u_\ell]_p\} < 2\ell \quad ↯$$

Die ε_i sind also wohldefiniert und eindeutig.

Es gilt

$$(a\cdot u_1)(a\cdot u_2)\cdots(a\cdot u_l) = a^l u_1\cdots u_l \equiv \varepsilon_1\cdots\varepsilon_l\, u_1\cdots u_l \pmod p$$

$$\Rightarrow a^l \equiv \varepsilon_1\cdots\varepsilon_l \pmod p.$$

Jetzt wenden wir §4.14 an $\square$

17. Satz Sei $p\in\mathbb{P}$ ungerade. Dann gilt

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{wenn } p\equiv 1,7 \pmod 8 \\ -1 & \text{wenn } p\equiv 3,5 \pmod 8\end{cases}$$

Beweis Schreibe $p = 2l+1$. Wir wenden Gauß Lemma an mit $a=2$ und der Gauß'schen Menge $\{1,2,\dots,l\}$.

1. Fall $l = 4k, 4k+1$

Dann gilt $\varepsilon_i = 1$ für $1\le i\le 2k$, sonst $\varepsilon_i = -1$

$$\Rightarrow \left(\frac{2}{p}\right) = \varepsilon_1\cdots\varepsilon_l = (-1)^{l-2k} = (-1)^l = \begin{cases} -1 & l = 4k+1 \\ 1 & l = 4k\end{cases}$$

$$= \begin{cases} -1 & \text{wenn } p\equiv 3 \pmod 8 \\ 1 & \text{wenn } p\equiv 1 \pmod 8\end{cases}$$

2. Fall $l = 4k+2, 4k+3$

Dann $\varepsilon_i = 1$ für $1\le i\le 2k+1$, sonst $\varepsilon_i = -1$

$$\Rightarrow \left(\frac{2}{p}\right) = \varepsilon_1\cdots\varepsilon_l = (-1)^{l-2k-1} = (-1)^{l-1}$$

$$= \begin{cases} -1 & l = 4k+2 \\ 1 & l = 4k+3\end{cases} = \begin{cases} -1 & \text{wenn } p\equiv 5 \pmod 8 \\ 1 & \text{wenn } p\equiv 7 \pmod 8\end{cases}$$

$\square$

18. <u>Lemma</u> Ist $p \in \mathbb{P}$ ungerade und ist ξ eine Primitivwurzel modulo p, so gilt

$$\left(\frac{\xi^s}{p}\right) = (-1)^s$$

<u>Beweis</u> $\left(\frac{\xi^s}{p}\right) = 1 \Leftrightarrow$ es gibt t mit $\xi^s \equiv \xi^{2t} \pmod p$

$\Leftrightarrow s - 2t \equiv 0 \pmod{p-1}$ für ein $t \in \mathbb{Z}$ geeignet

$\Leftrightarrow s - 2t = k \cdot \underbrace{(p-1)}_{\text{grade}}$ für $t, k \in \mathbb{Z}$ geeignet

$\Leftrightarrow s$ gerade $\square$

<u>Korollar</u> Ist $p \in \mathbb{P}$ ungerade und gilt $p \nmid a, b$, so gilt $\left(\frac{a \cdot b}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$

<u>Beweis</u> Sei ξ Primitivwurzel modulo p.

Schreibe $a \equiv \xi^s \pmod p$ $b \equiv \xi^t \pmod p$

$\Rightarrow a \cdot b \equiv \xi^{s+t} \pmod p$

$\Rightarrow \left(\frac{a \cdot b}{p}\right) = (-1)^{s+t} = (-1)^s \cdot (-1)^t = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$ $\square$

<u>Bem</u> Wir können §4.14 und §4.17 so formulieren:

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

Denn: $(p-1)/2$ ist gerade genau dann, wenn $p \equiv 1 \pmod 4$

$(p^2-1)/8 = (p-1)(p+1)/8$ ist ganze Zahl (!)

und gerade genau dann, wenn $p \equiv 1,7 \pmod 8$ $\square$

Mit diesen Rechenregeln reduziert sich das Berechnen von Legendre-Symbolen auf den Fall $\left(\frac{q}{p}\right)$, wo $p, q \in \mathbb{P}$ ungerade, $p \neq q$.

Für diesen Fall ist Gauß quadratisches Reziprozitätsgesetz entscheidend.

19. <u>Theorem</u> (Gauß) Sei $p, q \in \mathbb{P}$, beide ungerade, mit $p \neq q$. Dann gilt

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

<u>Beweis</u> Schreibe $p = 2n+1$, $q = 2 \cdot m + 1$

Wir wenden Gauß Lemma an auf $a = q$ mit Gauß'scher Menge $\{1, 2, \dots, n\}$

Für $1 \leq x \leq n$ schreibe

$$q \cdot x \equiv \varepsilon_x \cdot u \qquad u \in \{1, \dots, n\} \qquad \varepsilon_x = \pm 1$$

$$\rightsquigarrow \quad q \cdot x = \varepsilon_x \cdot u + p \cdot y \qquad \text{für ein } y \in \mathbb{Z}$$

Dann gilt $\varepsilon_x = -1$ genau dann, wenn

$$p \cdot y = q \cdot x + u$$

Wegen $u \geq 1$, $x \geq 1$ folgt $y \geq 1$. Weiter gilt

$$y = \frac{1}{p}(q \cdot x + u) \underset{x,u \leq n}{\leq} \frac{1}{p}(q+1) \cdot n \underset{\frac{n}{p} < \frac{1}{2}}{<} \frac{q+1}{2} = m+1$$

also $1 \leq y \leq m$.

Ist umgekehrt $y \in \mathbb{Z}$ mit $1 \leq y \leq m$ und

$1 \leq p \cdot y - q \cdot x = u \leq n$, so folgt $\varepsilon_x = -1$.

Sei $M = \{(x,y) \mid 1 \leq x \leq n,\ 1 \leq y \leq m\}$ und

sei $A = \{(x,y) \in M \mid 1 \leq py - qx \leq n\}$.

Es folgt $\left(\frac{q}{p}\right) = (-1)^{\# A}$

Setze $B = \{(x,y) \in M \mid 1 \leq qx - py \leq m\}$, dann

gilt genauso $\left(\frac{p}{q}\right) = (-1)^{\# B}$

Für $1 \leq x \leq n$ gilt $ggT(x,p) = 1$, also

$p \cdot y - q \cdot x \neq 0$.

Es folgt $A \cup B = \{ (x,y) \in M \mid -n \leq qx - py \leq m \}$.

Da $A \cap B = \emptyset$ (nach Definition von A und B)

erhalten wir $(\frac{q}{p})(\frac{p}{q}) = (-1)^{\# A \cup B}$

Sei $C = \{ (x,y) \in M \mid qx - py < -n \}$

$D = \{ (x,y) \in M \mid qx - py > m \}$

Dann gilt $M = A \dot\cup B \dot\cup C \dot\cup D$ (disjunkte Vereinigung)

Betrachte die Abbildung $\varphi(x,y) = (n+1-x, m+1-y)$

Für $(x,y) \in C$ gilt

$$q(n+1-x) + p(m+1-y) = -(qx-py) + q\frac{p+1}{2} + p\frac{q+1}{2}$$

$$= -(qx-py) + m - n > m$$

$\Rightarrow \varphi(C) \subseteq D$

Umkehrabbildung $\psi : D \to C$ genauso, mit

$\psi(x,y) = \varphi(x,y)$. Es folgt $\# C = \# D$

und damit $(-1)^{m \cdot n} = (-1)^{\# A} \cdot (-1)^{\# B} \cdot \underbrace{(-1)^{\# C} \cdot (-1)^{\# D}}_{=1}$

$$= \left(\frac{q}{p}\right) \cdot \left(\frac{p}{q}\right)$$

QED $\square$

Mit dem Gauß'schen Reziprozitätsgesetz lassen sich Legendre-Symbole sehr effektiv berechnen

Beispiel

(a) Hat $x^2 \equiv 17 \pmod{101}$ eine Lösung?

$101 \in \mathbb{P}$ und $17 \in \mathbb{P}$

$$\left(\frac{17}{101}\right) \cdot \left(\frac{101}{17}\right) = (-1)^{\frac{100}{2} \cdot \frac{16}{2}} = 1 \text{ , also}$$

$$\left(\frac{17}{101}\right) = \left(\frac{101}{17}\right) \underset{\substack{\uparrow \\ 101 = 5 \cdot 17 + 16}}{=} \left(\frac{16}{17}\right) = \left(\frac{-1}{17}\right) \underset{\substack{\uparrow \\ \S 4.18}}{=} (-1)^{16/2} = 1$$

Also gibt es $x \in \mathbb{Z}$ mit $x^2 \equiv 17 \pmod{101}$

(b) Hat $x^2 \equiv 12 \pmod{103}$ eine Lösung?

$103 \in \mathbb{P}$ $\quad 12 = 3 \cdot 4$

$$\left(\frac{12}{103}\right) \underset{\substack{\uparrow \\ \S 4.18}}{=} \left(\frac{3}{103}\right) \cdot \left(\frac{4}{103}\right) = \left(\frac{3}{103}\right) \quad \text{denn } \left(\frac{4}{103}\right) = 1$$

$$\left(\frac{3}{103}\right) \cdot \left(\frac{103}{3}\right) = (-1)^{\frac{2}{2} \cdot \frac{102}{2}} = -1$$

$$\left(\frac{3}{103}\right) = -\left(\frac{103}{3}\right) = -\left(\frac{1}{3}\right) = -1$$

Also gibt es keine Lösungen der Kongruenz

$$x^2 \equiv 12 \pmod{103}$$

(c) Bestimme alle Primzahlen $p \in \mathbb{P}$, für die 3 ein quadratisches Residuum ist, d.h. für die es $x \in \mathbb{Z}$ gibt mit $x^2 \equiv 3 \pmod p$.

$p = 2$ $\quad 3 \equiv 1 \pmod 2$ $\rightsquigarrow$ $p = 2$ erfüllt die Bedingung

Sei jetzt $p \geq 3$.

1. Fall $\quad p \equiv 1 \pmod 4$

$$1 \overset{!}{=} \left(\frac{3}{p}\right) \qquad \left(\frac{3}{p}\right)\left(\frac{p}{3}\right) = (-1)^{\frac{2}{2} \cdot \underbrace{\frac{p-1}{2}}_{\text{gerade}}} = 1$$

$$1 = \left(\frac{p}{3}\right) \Leftrightarrow p \equiv 1 \pmod 3$$

Gesucht sind also alle Primzahlen $p \in \mathbb{P}$ mit
$p \equiv 1 \pmod 4$ und $p \equiv 1 \pmod 3$

$$p = 4k+1 \qquad 4k+1 \equiv 1 \pmod 3$$
$$\Leftrightarrow -k+1 \equiv 1 \pmod 3$$
$$\Leftrightarrow k \equiv 0 \pmod 3$$
$$\Leftrightarrow k = 3l$$

Für alle Primzahlen der Form $p \equiv 1 \pmod{12}$ ist also 3 ein quadratisches Residuum.

2. Fall $\quad p \equiv 3 \pmod 4$

$$1 \overset{!}{=} \left(\frac{3}{p}\right) \qquad \left(\frac{3}{p}\right)\left(\frac{p}{3}\right) = (-1)^{\frac{2}{2} \cdot \frac{p-1}{2}} = -1$$

(ungerade)

also: $-1 = \left(\frac{p}{3}\right) \Leftrightarrow p \equiv 2 \bmod 3$

Gesucht sind also alle Primzahlen p mit $p \equiv 2 \pmod 3$ und $p \equiv 3 \pmod 4$

$$p = 4k+3 \qquad 4 \cdot k + 3 \equiv 2 \pmod 3$$
$$\Leftrightarrow k \equiv 2 \pmod 3$$
$$\Leftrightarrow k = 3l+2$$

$$p = 4(3l+2)+3 = 12 \cdot l + 11 = 12(l+1) - 1$$

Für alle Primzahlen der Form $p \equiv -1 \pmod{12}$ ist also 3 ein quadratischer Residuum.

Bsp für beide Fälle: $13 \equiv 1 \pmod{12}$

$$4^2 = 16 \equiv 3 \pmod{13}$$

$11 \equiv -1 \pmod{12}$

$$5^2 = 25 \equiv 3 \pmod{11}$$

Insgesamt: 3 ist quadratischer Residuum modulo $p \in \mathbb{P}$ genau dann, wenn $p = 2$ oder wenn $p \equiv \pm 1 \pmod{12}$.