§4 Polynome und Primitivwurzeln

1. Erinnerung. Sei R ein kommutativer Ring.

Ein Polynom f in der Variablen X ist ein formaler Ausdruck $F = a_n \cdot X^n + a_{n-1} \cdot X^{n-1} + \ldots + a_1 \cdot X + a_0$ mit $a_0, a_1, \ldots, a_n \in R$. Man nennt die a_j die Koeffizienten des Polynoms. Ist $a_n \neq 0$, so heißt a_n Leitkoeffizient von F und man sagt, f hat Grad n,

$$\deg(f) = n$$

(für das Nullpolynom $f = 0$ setzt $\deg(f) = -\infty$)

Wenn der Leitkoeffizient $a_n = 1$ ist, so heißt f normiertes Polynom. Polynome werden nach den "üblichen" Regeln addiert und multipliziert, etwa

$$(a_n X^n + \ldots + a_0) \cdot (b_m X^m + \ldots + b_0)$$

$$= a_n b_m X^{n+m} + (a_n \cdot b_{m-1} + a_{n-1} \cdot b_m) X^{m+n-1} + \ldots + a_0 \cdot b_0$$

Zwei Polynome sind gleich genau dann, wenn sie die gleichen Koeffizienten haben.

2. Lemma Sei R ein kommutativer Ring, sei $R[X]$ die Menge aller Polynome mit der Variablen X. Dann ist $R[X]$ ein kommutativer Ring. Für alle $f, g \in R[X]$ gilt

$$\deg(f+g) \leq \max\{\deg(f), \deg(g)\}$$
$$\deg(f \cdot g) \leq \deg(f) + \deg(g)$$

und wenn R zusätzlich ein Körper ist, gilt

$$\deg(f \cdot g) = \deg(f) + \deg(g).$$

Beweis Dass $R[X]$ ein kommutativer Ring ist, rechnet man direkt nach. Einselement ist $f = 1$, Nullelement ist das Nullpolynom $f = 0$.

Ansatz, $f = a_n X^n + \dots + a_0$, $g = b_m X^m + \dots + b_0$

OE $n \geq m$. Dann setze $b_j = 0$ für $m < j \leq n$

$$f+g = (a_n + b_n) X^n + \dots + (a_0 + b_0)$$
$$\Rightarrow \deg(f+g) \leq n$$
$$f \cdot g = a_n \cdot b_m X^{n+m} + \dots + a_0 b_0$$
$$\Rightarrow \deg(f \cdot g) \leq n \cdot m.$$

Falls R ein Körper ist und $a_n, b_m \neq 0$,
so ist auch $a_n \cdot b_m \neq 0$ $\Rightarrow \deg(f \cdot g) = m+n$ $\square$

3. Satz (vom Teilen mit Rest)

Sei K ein Körper, seien $f, g \in K[x]$
Polynome mit $g \neq 0$. Dann gibt es
eindeutig Polynome $h, r \in K[x]$ mit

$$f = g \cdot h + r \quad \text{und} \quad \deg(r) < \deg(g). \quad \#$$

Beweis Existenz von h, r

Wenn $\deg(f) < \deg(g)$ setze $h = 0, r = f$
$\Rightarrow$ fertig.
Wenn $\deg(f) \geq \deg(g)$ Induktion und
$\deg(f) = n \geq 0$.
Induktionsanfang: $n = 0$ $\Rightarrow$ $f = a_0 \neq 0$
$g = b_0 \neq 0$
Setze $h = \frac{a_0}{b_0}$ $\Rightarrow$ $f = g \cdot h + 0$ $(\checkmark)$

Induktionsschritt Sei $g = b_m X^m + \dots + b_0$

$f = a_n X^n + \dots + a_0$

$b_m, a_n \neq 0$, $n \geq m$

Betrachte $\tilde{f} = f - g \cdot \frac{a_n}{b_m} \cdot X^{n-m}$

$= a_n X^n - a_n X^n +$ Restterme

$\Rightarrow \deg(\tilde{f}) < \deg(f)$. Nach Induktionsannahme gibt es $\tilde{h}, r \in K[X]$ mit

$$\tilde{f} = g \cdot \tilde{h} + r \qquad \deg(r) < \deg(g)$$

$$= f - g \cdot \frac{a_n}{b_m} X^{n-m}$$

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

Eindeutigkeit Angenommen, $f = g \cdot h_1 + r_1$

$= g \cdot h_2 + r_2$

$\deg(r_1), \deg(r_2) < \deg(g)$

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

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

$\Rightarrow \deg(h_1 - h_2) < 0 \Rightarrow h_1 = h_2$ und

$r_1 = r_2$ □

4. Def Sei R ein kommutativer Ring, sei $f = a_n X^n + \dots + a_0 \in R[X]$ Polynom. Ein Element $u \in R$ heißt Nullstelle von f, falls

$$a_n u^n + \dots + a_0 = f(u) = 0$$ gilt.

Lemma Sei K ein Körper, sei $f \in K[X]$ Polynom. Wenn $u \in K$ eine Nullstelle von f ist, so gibt es $h \in K[X]$ mit

$$f = h \cdot (X - u)$$

Beis Wir machen Teilen mit Rest,

$$f = h \cdot (X-u) + r \qquad h, r \in K[X]$$

mit $\deg(r) < \deg(X-u) = 1 \Rightarrow \deg(r) \leq 0$,

$r = b_0 \in K$ konstantes Polynom. Einsetzen von

u liefert $f(u) = 0 = h(u) \cdot \underbrace{(u-u)}_{=0} + \underbrace{r(u)}_{=b_0}$.

$\Rightarrow b_0 = 0$, r Nullpolynom □

Satz Sei K ein Körper, sei $F \in K[X]$ Polynom mit $n = \deg(f) \geq 1$. Dann gibt es eindeutig bestimmt $u_1, \dots, u_m \in K$ sowie $h \in K[X]$ mit

$f = (X-u_1)\cdot(X-u_2)\cdots(X-u_m)\cdot h$ so, dass h keine Nullstellen in K hat. Die Nullstellen von f sind genau $u_1, \dots, u_m$ (wobei Wiederholungen vorkommen können). Insbesondere hat f höchstens n verschiedene Nullstellen.

Beweis: Mit dem Lemma folgt sofort die Existenz von $u_1, \dots, u_m$ und h, etwa

$f = (X-u_1)\cdot h_1$ u_1 Nullstelle von f

$= (X-u_1)\cdot(X-u_2)\cdot h_2$ u_2 Nullstelle von h_1 $\{\deg(h_2) < \deg(h_1)$

$\vdots$

$= (X-u_1)\cdots(X-u_m)\cdot h_m$ h_m ohne Nullstellen.

Angenommen, $v \in K$ ist Nullstelle von f. Es folgt

$f(v) = (v-u_1)\cdots(v-u_m)\cdot \underbrace{h(v)}_{\neq 0} = 0 \Rightarrow v-u_j = 0$

für ein $j \in \{1, \dots, m\}$, da K Körper ist.

Also sind $\{u_1, \dots, u_m\}$ genau die Nullstellen von f.

Zur Eindeutigkeit der Zerlegung mit Induktion nach $\deg(f) = n \geq 1$. Wenn $\deg(f) = 1$, dann $f = a(X-u)$, $a, u \in K$, $a \neq 0$

$\Rightarrow$ fertig.

Induktionsschritt: $f = (X-u_1)\cdots(X-u_m)\cdot h$
$= (X-v_1)\cdots(X-v_\ell)\cdot \tilde{h}$

a) es gibt j mit $u_1 = v_j$ OE $j=1$, also

$f = (X-u_1)\cdots(X-u_m)\cdot h = (X-u_1)(X-v_2)\cdots(X-v_\ell)\cdot\tilde{h}$

Teilen ohne Rest $\Rightarrow$ $(X-u_2)\cdots(X-u_m)\cdot h = (X-v_2)\cdots(X-v_\ell)\cdot\tilde{h}$

Ind. Ann. $\Rightarrow$ $m=\ell$, $h=\tilde{h}$, nach Umsortieren $u_2=v_2$, $u_3=v_3$, ..., $u_m=v_m$ □

Wir brauchen nun einige Ergebnisse über zyklische Gruppen.

5. Def Eine abelsche Gruppe $(G,*)$ heißt zyklisch, wenn es ein Element $g\in G$ gibt mit $\langle g\rangle = G$, also $G = \{g^k \mid k\in\mathbb{Z}\}$

Beispiele
- $(\mathbb{Z},+)$ ist zyklisch, $\langle 1\rangle = \mathbb{Z}$, denn $\mathbb{Z} = \{k\cdot 1 \mid k\in\mathbb{Z}\}$
- $(\mathbb{Z}/m,+)$ ist zyklisch, $\langle [1]_m\rangle = \mathbb{Z}/m$, denn $\mathbb{Z}/m = \{k\cdot[1]_m \mid k\in\mathbb{Z}\} = \{[k]_m \mid k\in\mathbb{Z}\}$
- $(\mathbb{Q},+)$ ist nicht zyklisch, für $q=\frac{a}{b}\in\mathbb{Q}$ $a,b\in\mathbb{Z}$, $b\geq 1$ folgt $\langle q\rangle = \{\frac{k\cdot a}{b} \mid k\in\mathbb{Z}\} \neq \mathbb{Q}$

Lemma A Sei $(G,*)$ eine zyklische Gruppe und sei $H \subseteq G$ eine Untergruppe. Dann ist H zyklisch.

Beweis Sei $G = \langle g \rangle = \{ g^k \mid k \in \mathbb{Z} \}$, betrachte den surjektiven Homomorphismus $f: \mathbb{Z} \to G$, $f(k) = g^k$. Für $k, l \in \mathbb{Z}$ mit $f(k), f(l) \in H$ folgt $f(k+l) \in H$ und $f(-k) \in H \Rightarrow f^{-1}(H) \subseteq \mathbb{Z}$ ist Untergruppe. Nach §2.5 gibt es $d \in \mathbb{N}$ mit $f^{-1}(H) = d \cdot \mathbb{Z}$. Also

$$H = f(f^{-1}(H)) = \{ g^{d \cdot k} \mid k \in \mathbb{Z} \} = \langle g^d \rangle.$$

(f surjektiv!) □ #

Lemma B Sei $(G,*)$ eine endliche zyklische Gruppe, $\#G = n$. Für jeden Teiler $m \in \mathbb{N}$ von n gibt es genau eine Untergruppe $G_m \subseteq G$ mit $\#G_m = m$ und $G_m = \{ x \in G \mid x^m = e \}$

Beweis Schreibe $n = m \cdot d$, $m, d \in \mathbb{N}$. Sei $G = \langle g \rangle$, $\operatorname{ord}(g) = n$ vgl. §3.8. Für $x \in G$, $x = g^k$ gilt: $x^m = e \Leftrightarrow g^{m \cdot k} = e$

$\Leftrightarrow n \mid m \cdot k \Leftrightarrow d \mid k \Leftrightarrow x \in \langle g^d \rangle$

Folglich gilt $\langle g^d \rangle = \{ x \in G \mid x^m = e \}$.

Weiter gilt $\operatorname{ord}(g^d) = m$, also $\#\langle g^d \rangle = m$.

Ist $H \leq G$ eine beliebige Untergruppe mit $\#H = m$, so folgt $x^m = e$ für alle $x \in H$ nach §3.8, d.h. $H \leq G_m = \langle x^d \rangle$. Da $\#H = m = \#G_m$ folgt $H = G_m$ □

Lemma 6 Sei $(G, *)$ endliche zyklische Gruppe, $\#G = n \geq 1$. Sei $k \in \mathbb{N}$ und sei $\langle g \rangle = G$. Dann sind äquivalent:

(i) $\langle g^k \rangle = G$

(ii) $\operatorname{ggT}(k, n) = 1$.

Beweis (i) $\Rightarrow$ (ii) $\langle g^k \rangle = G \Rightarrow$ es gibt $l \in \mathbb{Z}$ mit $g^{k \cdot l} = g \Rightarrow k \cdot l \equiv 1 \pmod{n} \Rightarrow \operatorname{ggT}(k, n) = 1$ §1.10

(ii) $\Rightarrow$ (i) $\operatorname{ggT}(k, n) = 1 \Rightarrow$ es gibt $u, v \in \mathbb{Z}$ mit

$$uk + vn = 1 \Rightarrow g^{\overbrace{u \cdot k}} \underbrace{g^{v \cdot n}}_{= e} = g \Rightarrow \langle g^k \rangle = G$$ □

Lemma D Sei G eine zyklische Gruppe mit $\#G = n < \infty$. Dann gilt

$$\#\{x \in G \mid \langle x \rangle = G\} = \varphi(n)$$

Beis Das folgt direkt aus Lemma G', denn $\varphi(n) = \#\{k \in \mathbb{N} \mid 0 \le k < n \text{ und } ggT(k,n)=1\}$, vgl. §2.15 □

Lemma E Sei $n \in \mathbb{N}$, $n \ge 1$. Dann gilt

$$\sum_{\substack{d \ge 1 \\ d \mid n}} \varphi(d) = n$$

Beis Für jeden Teiler d von n gibt $\varphi(d)$ nach Lemma D die Anzahl der $x \in \mathbb{Z}/n$ an, für die gilt $\operatorname{ord}(x) = d$. Jedes $x \in \mathbb{Z}/n$ hat einen Ordnung, die n teilt. Also zählt die linke Seite die Anzahl der Elemente von $\mathbb{Z}/n$ □

Lemma F Sei $(G,*)$ eine endliche abelsche Gruppe, $\#G = n$. Wenn für jeden Teiler $d \geq 0$ von n gilt

$$\#\{x \in G \mid x^d = e\} \leq d$$

dann ist G zyklisch.

Beweis Sei $\alpha(d) = \#\{x \in G \mid \mathrm{ord}(x) = d\}$.

Zu zeigen ist $\alpha(n) > 0$. Es gilt

$$\sum_{\substack{d \geq 1 \\ d \mid n}} \alpha(d) = n.$$

Angenommen, $\alpha(d) > 0$. Dann gibt es $x \in G$ mit $H = \langle x \rangle$, $\#H = d$. Für jedes $y \in H$ gilt $y^d = e$, also $H = \{y \in G \mid y^d = e\}$.

Es folgt, dass H alle Elemente $y \in G$ mit $\mathrm{ord}(y) = d$ enthält, also $\alpha(d) = \varphi(d)$ nach Lemma D. Insgesamt also: $\alpha(d) \neq 0 \Rightarrow \alpha(d) = \varphi(d)$

$$n = \sum_{d \mid n} \varphi(d) \geq \sum_{d \mid n} \alpha(d) = n$$

Es folgt $\alpha(d) = \varphi(d)$ für alle Teiler d von n.

Insbesondere ist $\alpha(n) = \varphi(n) \geq 1$ □

6. Satz Sei $(K,+,\cdot)$ ein Körper, sei $H \subseteq K^*$ eine endliche Untergruppe von $(K^*,\cdot)$. Dann ist H zyklisch, d.h. es gibt $u \in H$ mit $H = \{u^k \mid k \in \mathbb{Z}\}$

Bew. Sei $n = \#H$. Für $u \in H$ mit $\mathrm{ord}(u) = d$ gilt: $u^d - 1 = 0$, d.h. u ist Nullstelle des Polynoms $X^d - 1$. Nach §4.4 gibt es höchstens d solcher Nullstellen in K, also $\#\{v \in H \mid v^d = 1\} \leq d$. Nach §4.5 Lemma F ist H zyklisch □

Korollar Ist $(K,+,\cdot)$ ein endlicher Körper, so ist $(K^*,\cdot)$ eine zyklische Gruppe.

Insbesondere ist für $p \in \mathbb{P}$ die multiplikative Grp $(\mathbb{Z}/p)^* = \{[1]_p, [2]_p, \ldots, [p-1]_p\}$ zyklisch,

Bem. Wenn $m \in \mathbb{N}$ kein Primzahl ist, dann ist $(\mathbb{Z}/m)^*$ nicht unbedingt zyklisch. Zum Beispiel ist $(\mathbb{Z}/8)^*$ nicht zyklisch, für jedes $[a]_8 \in (\mathbb{Z}/8)^*$ gilt $[a^2]_8 = [1]_8$ $(a = 1, 3, 5, 7)$.

7. Def Sei $p \in \mathbb{P}$. Eine Zahl $\xi \in \mathbb{Z}$ heißt Primitivwurzel modulo p, falls gilt $\{[\xi]_p, [\xi^2]_p, \ldots, [\xi^{p-1}]_p\} = (\mathbb{Z}/p)^*$

Beispiel $p = 5$, $\xi = 3$

$$\xi^2 = 9 \equiv 4 \pmod 5$$
$$\xi^3 = 27 \equiv 2 \pmod 5$$
$$\xi^4 = 81 \equiv 1 \pmod 5$$

Wenn ξ Primitivwurzel modulo p ist, so auch $\xi + k \cdot p$, für jedes $k \in \mathbb{Z}$.

8. Satz Sei $p \in \mathbb{P}$, sei $m \geq 1$ natürliche Zahl, sei $d = ggT(m, p-1)$.

Für $a \in \mathbb{Z}$ mit $p \nmid a$ sind äquivalent:

(i) Es gibt $x \in \mathbb{Z}$ mit $x^m \equiv a \pmod p$

(ii) Es gibt $y \in \mathbb{Z}$ mit $y^d \equiv a \pmod p$

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

Beweis: Schreibe $m = m' \cdot d$, $p-1 = l \cdot d$ mit $l \neq 0$

(i) $\Rightarrow$ (ii) Setze $y = x^{m'} \Rightarrow y^d \equiv a \pmod p$

(ii) $\Rightarrow$ (iii) $a^l \equiv y^{l \cdot d} \equiv y^{p-1} \equiv 1 \pmod p$

nach Eulers Satz §3, 9.

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

Es gibt $s \geq 1$ mit $\xi^s \equiv a \pmod p$,

da $ggT(a,p) = 1$ ($[a]_p \in (\mathbb{Z}/p)^*$).

Nach Voraussetzung gilt $a^l \equiv \xi^{s \cdot l} \equiv 1 \pmod p$

also $s \cdot l \equiv 0 \pmod{p-1} \Rightarrow \underbrace{(p-1)}_{l \cdot d} \cdot k = s \cdot l$

für ein $k \in \mathbb{Z} \Rightarrow d \cdot k = s$ (weil $l \neq 0$).

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

$[a]_p = [\xi^s]_p = [\xi]_p^{k(um + v(p-1))}$

$= [\xi]_p^{kum}$. Wähle also $x \in \mathbb{Z}$ mit

Eulers $\uparrow$ $[x]_p = [\xi]_p^{ku} \Rightarrow x^m \equiv a \pmod p$ □

Bsp $p=7$, $m=3$. Die Kongruenz $d=3$

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

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

Wir betrachten jetzt die Existenz von Quadratwurzeln modulo p, d.h. Lösungen der Kongruenz $x^2 \equiv a \pmod p$, für $p \nmid a$. Für $p=2$ ist das trivial, betrachte Primzahlen $p \geq 3$, d.h. p ist ungerade.

9. Def Sei $p \in \mathbb{P}$ und $p \geq 3$. Eine Zahl $a \in \mathbb{Z}$ heißt quadratischer Rest modulo p, wenn $p \nmid a$ und wenn es $x \in \mathbb{Z}$ gibt mit $x^2 \equiv a \pmod p$. Anders gesagt: $[a]_p \neq [0]_p$ und $X^2 - [a]_p$ hat eine Nullstelle in $\mathbb{Z}/p$.

Wir definieren das Legendre-Symbol

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{falls } a \text{ quadr. Res. mod } p \\ -1 & \text{sonst} \end{cases}$$

Achtung: das Legendre-Symbol nicht mit dem Bruch a/p verwechseln! Das Legendre-Symbol $\left(\frac{a}{p}\right)$ ist nur definiert für $p \in \mathbb{P}$, $p \geq 3$ und $a \in \mathbb{Z}$, $p \nmid a$.

10. Satz Sei $p \in \mathbb{P}$, $p \geq 3$. Schreibe $p = 2 \cdot l + 1$. Sei $a \in \mathbb{Z}$ mit $p \nmid a$. Dann gelten

$$a^l \equiv \pm 1 \pmod{p}$$

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

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

Beweis Sei $b = a^l$. Dann gilt $b^2 = a^{2l} = a^{p-1} \equiv 1 \pmod{p}$

nach Eulers Theorem § 3.9, folglich $b = a^l \equiv \pm 1 \pmod{p}$, weil $\mathbb{Z}/p$ Körper ist. Wende nun § 4.7 an mit $m = 2$ und $d = \mathrm{ggT}(m, p-1) = 2$, $(p-1)/2 = l$ □

Korollar Sei $p \in \mathbb{P}$, $p \geq 3$. Dann gilt

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

Bew. Da p ungerade ist, ist $p \equiv \pm 1 \pmod 4$.
Schr. $p = 2l+1$. Dann ist l gerade genau dann, wenn $p \equiv 1 \pmod 4$ und genau dann gilt für $a = -1$, dass $a^l \equiv 1 \pmod p$ □

Unser nächstes Ziel ist eine praktische Formel zur Berechnung von Legendre-Symbolen.

11. Def Sei $p \in \mathbb{P}$, $p \geq 3$. Schr. $p = 2l+1$.
Ein Mengensystem $\{u_1, \dots, u_l\}$ heißt
Gauß'sche Menge (bzgl. p), wenn gilt

$$(\mathbb{Z}/p)^* = \{[\pm u_1]_p, \dots, [\pm u_l]_p\}.$$

Zum Beispiel ist $\{1, 2, \dots, l\}$ eine Gauß'sche Menge, denn $p - k \equiv -k \pmod p$.

12. Satz (Gauß' Lemma) Sei $p \in \mathbb{P}$, $p \geq 3$, $p = 2l+1$. Sei $\{u_1, \dots, u_l\}$ Gauß'sches System. Sei weiter $a \in \mathbb{Z}$ mit $p \nmid a$. Dann ist auch $\{au_1, \dots, au_l\}$ ein Gauß'sches System. Zu jedem $i = 1, \dots, l$ gibt es folglich genau ein $j \in \{1, \dots, l\}$ so, dass $au_i \equiv \varepsilon_i u_j \pmod{p}$, mit $\varepsilon_i \in \{\pm 1\}$. Es gilt $\left(\frac{a}{p}\right) = \varepsilon_1 \cdot \varepsilon_2 \cdots \varepsilon_l$.

Beweis: Da $[a]_p \in (\mathbb{Z}/p)^*$ einheitlich ist, gilt $\mathbb{Z}/p = \{[\pm au_1]_p, \dots, [\pm au_l]_p\}$. Also gibt es zu jedem i genau ein j mit $au_i \equiv \pm u_j \pmod{p}$. Die $\varepsilon_1, \dots, \varepsilon_l$ sind dadurch eindeutig bestimmt. Nun gilt

$$(au_1)(au_2)\cdots(au_l) = a^l u_1 \cdots u_l \equiv \varepsilon_1 \cdots \varepsilon_l \cdot u_1 \cdots u_l \pmod{p},$$

insgesamt $a^l \equiv \varepsilon_1 \cdots \varepsilon_l \pmod{p}$. Lehl §4.10. □

#

13. Satz Sei $p \in \mathbb{P}$, $p \geq 3$. Dann gilt

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

Beis Schon $p = 2l+1$, betrachte die Gauß'sche Menge $\{1, 2, \ldots, l\}$ und $a = 2$, wende §4.12 an.

1. Fall $l = 4 \cdot k$ oder $l = 4 \cdot k + 1$
$p \equiv 1 \pmod 8$ $p \equiv 3 \pmod 8$

Beh: $\varepsilon_i = 1$ für $i = 1, \ldots, 2k$ $\varepsilon_i = -1$ für $i > 2k$.

Denn: $2 \cdot i \leq l$ für $i \leq k$ $\Rightarrow \varepsilon_i = 1$

Für $i = 2k + h$, $h \geq 1$ gilt $2 \cdot i = 4k + 2h$

$$= \begin{cases} l + 2 \cdot h > l \Rightarrow \varepsilon_i = -1 & \text{wenn } l = 4k \\ l - 1 + 2 \cdot h > l \Rightarrow \varepsilon_i = -1 & \text{wenn } l = 4k+1 \end{cases}$$

Also $\varepsilon_1 \cdots \varepsilon_l = \begin{cases} 1 & \text{wenn } p \equiv 1 \pmod 8 \\ -1 & \text{wenn } p \equiv 3 \pmod 8 \end{cases}$

2. Fall $l = 4k + 2$ oder $l = 4k + 3$
$p \equiv 5 \pmod 8$ $p \equiv 7 \pmod 8$

$\varepsilon_i = 1$ für $i = 1, \ldots, 2k+1$, $\varepsilon_i = -1$ für $i > 2k+1$

(genauso)

$$\Rightarrow \varepsilon_1 \cdots \varepsilon_l = \begin{cases} -1 & l = 4k+2 \\ 1 & l = 4k+3 \end{cases}$$

□

Bem Man kann §4.10 und §4.13 auch so formulieren:

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

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

denn: $p = 2l+1 \Rightarrow (p-1)/2 = l$

$p = 2l+1 \Rightarrow (p^2-1)/8 = \frac{4l(l+1)}{8} = \frac{l(l+1)}{2}$ □

14. Lemma Sei $p \in \mathbb{P}$, $p \geq 3$ und sei ζ ein Primitivwurzel modulo p. Für $s \in \mathbb{N}$ gilt dann

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

Bew: $\left(\frac{\zeta^s}{p}\right) = 1 \Leftrightarrow$ es gibt $t \in \mathbb{N}$ mit

$$\zeta^{2t} \equiv \zeta^s \pmod p \Leftrightarrow 2t \equiv s \pmod{p-1}$$

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

$\Leftrightarrow s$ gerade $\Leftrightarrow (-1)^s = 1$ □

15. Theorem Ist $p \in \mathbb{P}$ ungerade und gilt $p \nmid a, b$, so gilt

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

Beweis Sei ξ Primitivwurzel modulo p. Schreibe

$$a \equiv \xi^s, \quad b \equiv \xi^t \pmod{p} \quad \text{für } s, t \in \mathbb{N}.$$

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

Moderne Formulierung: Das Legendre-Symbol liefert ein Homomorphismus

$$(\mathbb{Z}/p)^* \xrightarrow{f} \{\pm 1\}$$
$$[a]_p \longmapsto \left(\frac{a}{p}\right)$$

Mit §4.10, §4.13 und §4.15 ist die Berechnung eines Legendre-Symbols $\left(\frac{q}{p}\right)$ auf den Fall zurückgeführt, wo $q \in \mathbb{P}$ eine ungerade Primzahl ist. Der letzte fehlende Schritt ist Gauß' Theorem über Quadratische Reziprozität.

16. Theorem (Gauß) Das quadratische Reziprozitätsgesetz.

Sei $p, q \in \mathbb{P}$, $p, q \geq 3$, $p \neq q$. Dann gilt

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

Beweis: Schon $p = 2\cdot n+1$ und $q = 2\cdot m+1$.

Wir wenden Gauß' Lemma §4.12 an mit $a = q$.

Die Gauß'sche Menge ist $\{1, \dots, n\}$. Also

$$q\cdot i \equiv \varepsilon_i \cdot k \pmod{p} \quad 1 \leq i, k \leq n, \quad \varepsilon_i = \pm 1$$

$$q\cdot i = \varepsilon_i \cdot k + j\cdot p \quad \text{für ein } j \in \mathbb{Z}.$$

$$\varepsilon_i = -1 \iff q\cdot i + k = j\cdot p$$

Dann: $1 \leq j = \frac{1}{p}(q\cdot i + k) \leq \frac{1}{p}(q\cdot n + n) = \frac{n}{p}(q+1)$

$$< \frac{1}{2}(q+1) = m+1, \text{ d.h. } 1 \leq j \leq m.$$

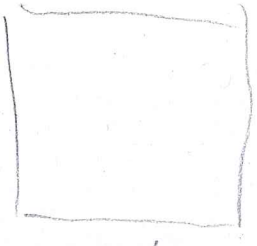
Ist umgekehrt $1 \leq j \leq m$ und gilt

$$1 \leq k = j\cdot p - q\cdot i \leq n,$$

so ist $\varepsilon_i = -1$.

Sei $M = \{(i,j) \in \mathbb{N}\times\mathbb{N} \mid 1 \leq i \leq n,\ 1 \leq j \leq m\}$

$\#M = m\cdot n$



$-n \le qi - pj \le -1$

$A = \{ (i,j) \in M \mid 1 \le pj - qi \le n \}$

dann gilt $\varepsilon_1 \cdots \varepsilon_n = (-1)^{\#A} = \left(\frac{q}{p}\right)$

Entsprehl $B = \{ (i,j) \in M \mid 1 \le qi - pj \le m \}$

$-m \le pj - qi \le -1$

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

Weiter gilt für $1 \le j \le n$, dann ggT $(j,p) = 1$,

also $p \cdot j - q \cdot i \neq 0$. Damit

$A \cup B = \{ (i,j) \in M \mid -n \le q \cdot i - p \cdot j \le m \}$

sowie $A \cap B = \emptyset$, damit

$(-1)^{\#A} \cdot (-1)^{\#B} = (-1)^{\#(A \cup B)} = \left(\frac{p}{q}\right)\left(\frac{q}{p}\right)$

Sei $C = \{ (i,j) \in M \mid q \cdot i - p \cdot j < -n \}$

$D = \{ (i,j) \in M \mid q \cdot i - p \cdot j > m \}$

Dann $M = A \dot\cup B \dot\cup C \dot\cup D$

Sei $f(i,j) = (n+1-i,\ m+1-j)$

$(i,j) \in C \Rightarrow q(n+1-i) - p(m+1-j)$

$= -(qi - pj) + q\frac{p+1}{2} - p\frac{q+1}{2}$

$= -(qi - pj) + \frac{q-p}{2}$

$= -\underbrace{(qi - pj)}_{<-n} + m - n > m$

$\Rightarrow f(C) \subseteq D$

Ganz ähnlich folgt $f(D) \subseteq G$. Wir

gilt $f(f(i,j)) = f(n+1-i, m+1-j)$

$= (i,j) \Rightarrow f$ ist injektiv.

Damit $\#G \leq \#D \leq \#G \Rightarrow \#C = \#D$ und

$$\underset{(-1)}{m \cdot n} = \underset{(-1)}{\#M} = \underset{(-1)}{\#A} \cdot \underset{(-1)}{\#B} \cdot \underbrace{\underset{(-1)}{\#C} \cdot \underset{(-1)}{\#D}}_{=1}$$

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

□ #

17. Beispiel (a) Hat $x^2 \equiv 17 \pmod{107}$ eine Lösung? $17, 107 \in \mathbb{P}$

$$\left(\frac{17}{107}\right) = ?$$

$$\left(\frac{17}{107}\right)\cdot\left(\frac{107}{17}\right) = (-1)^{8 \cdot 53} = 1, \text{ also}$$

$$\left(\frac{17}{107}\right) = \left(\frac{107}{17}\right) = \left(\frac{5}{17}\right) = \left(\frac{17}{5}\right) = \left(\frac{2}{5}\right) = -1 \quad \text{da } 5 \equiv 5 \pmod 8$$

$107 = 6 \cdot 17 + 5$

$$\left(\frac{5}{17}\right)\left(\frac{17}{5}\right) = (-1)^{2 \cdot 8} = 1$$

Also gibt es kein $x \in \mathbb{Z}$ mit $x^2 \equiv 17 \pmod{107}$.

(b) Hat $x^2 \equiv 12 \pmod{107}$ eine Lösung?

$$\left(\frac{12}{107}\right) = \left(\frac{3\cdot 4}{107}\right) = \left(\frac{3}{107}\right)\cdot \underbrace{\left(\frac{2}{107}\right)^2}_{=1} = -\left(\frac{107}{3}\right) = -\left(\frac{2}{3}\right) = 1 \qquad (3 \equiv 3 \bmod 8)$$

$$\left(\frac{3}{107}\right)\left(\frac{107}{3}\right) = (-1)^{1\cdot 53} = -1$$

also hat $x^2 \equiv 12 \pmod{107}$ eine Lösung,

z.B. $36^2 = 12\cdot 107 + 12$

Wir wissen aus §4.10, dass -1 genau dann quadratischer Rest modulo p ist, für $p \in \mathbb{P}$, $p \geq 3$, wenn gilt $p \equiv 1 \pmod 4$.

Diese Frage lässt sich auch für andere Zahlen systematisch behandeln.

18 <u>Anwendung/Lemma</u> Sei $p \in \mathbb{P}$, $p \geq 5$. Dann ist 3 quadratischer Rest modulo p genau dann, wenn $p \equiv \pm 1 \pmod{12}$.

Also z.B. für $p = 11$: $5^2 = 25 \equiv 3 \pmod{11}$

oder für $p = 13$: $4^2 = 16 \equiv 3 \pmod{13}$

Beis. 1. Fall $p \equiv 1 \pmod 4$: $1 \overset{!}{=} \left(\frac{3}{p}\right)$

$\left(\frac{3}{p}\right)\left(\frac{p}{3}\right) = (-1)^{1 \cdot \frac{p-1}{2}} = 1$, da $\frac{p-1}{2}$ gerade ist

also $\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right)$.

Wit: $\left(\frac{p}{3}\right) = 1 \iff p \equiv 1 \pmod 3$,

denn -1 ist kein quadratischer Rest modulo 3.

Sei $p = 4k+1$. $4k+1 \equiv 1 \pmod 3$

$\iff 4k \equiv 0 \pmod 3$

$\iff k = 3n \quad n \in \mathbb{N}, n \geq 1$

also $p = 12n+1$, $p \equiv 1 \pmod{12}$

2. Fall $p \equiv 3 \pmod 4$: $1 \overset{!}{=} \left(\frac{3}{p}\right)$

$\left(\frac{3}{p}\right)\left(\frac{p}{3}\right) = (-1)^{1 \cdot \frac{p-1}{2}} = -1$, also $1 = \left(\frac{3}{p}\right) \iff$

$-1 = \left(\frac{p}{3}\right) \iff p \equiv 2 \pmod 3$

$p = 4k+3 \equiv 2 \pmod 3$

$\iff k+1 \equiv 2 \pmod 3$

$\iff k = 3n+2$

$p = 12n + 8 + 3 = 12n + 11$

also $p \equiv -1 \pmod{12}$