5 Quadratische Kongruenzen

5.1 Einführende Diskussion

Problem: Gegeben $a, b, c \in \mathbb{Z}$. Wann ist die quadratische Kongruenz $ax^2 + bx + c \equiv 0 \mod m$ lösbar und wann nicht? In diesem Rahmen wird nur der Fall $a = 1$ behandelt (andere Wahl von a ergibt keine schönen Ergebnisse).

1. Gedanke: Mittels des Chinesischen Restsatzes reicht die Betrachtung des Falls $m = p^t,\ p \in \mathbb{P},\ t \in \mathbb{N}_+$ aus.
$p = 2$: Explizite Aussage möglich (Übung). Hier betrachten wir nur $p > 2$. Dann gilt aber ohne Beschränkung der Allgemeinheit $2 \mid b$, denn $\overline{b} = \overline{2}\underbrace{(\overline{2}^{-1}b)}_{=:b_0} = 2\overline{b}_0$.

$$x^2 + 2b_0x + c = \underbrace{(x + b_0)^2}_{=:x'} + \underbrace{c - b_0^2}_{=:-k} = x' - k$$

Dann genügt zu zeigen: Wann ist $x^2 \equiv k \mod p^t$ lösbar. $k = p^{v_p(k)}k_0,\ p \nmid k_0$, falls $v_p(k) \geq t \implies$ lösbar mit $x = 0$. Falls $v_p(k) = u < t$: Ansatz $x = p^{v_p(x)}x_0,\ p \nmid x_0$, falls x Lösung ist, dann gilt für ein $c \in \mathbb{Z}$:

$$p^{2v_p(x)}x_0^n = p^k k_0 + cp^t = p^k(\underbrace{k_0 + cp^{t-u}}_{\not\equiv 0 \mod p}),\ t - u > u \implies u = wv_p(x),$$

also $2 \mid u$ und $x_0 \equiv k_0 \mod p^{t-u}$ mit $p \nmid k_0$. Die Umkehrung gilt auch. Ergebnis: Die Kongruenz $x^2 \equiv k \mod p^t$ ist lösbar, wenn $v_p(k) \geq t$, wenn $v_p(k) < t$, so genau dann lösbar, wenn $2 \mid v_p(k)$ und die Kongruenz $x_0^2 \equiv k_0 \mod p^{t-u}$ lösbar ist. Hiernach genügt es, den Fall $x^2 \equiv k \mod p^t$ mit $p \nmid k$ zu behandeln, also $\overline{k} \in G = (\mathbb{Z}/p^t\mathbb{Z})^\times$.

Hilfssatz
Sei $t \in \mathbb{N}_+,\ p \in \mathbb{P},\ p > 2,\ p \nmid k$. Dann gilt:

$$x^2 \equiv k \mod p^t \text{ lösbar} \iff x^2 \equiv k \mod p \text{ lösbar.}$$

Beweis
„$\implies$“ trivial
„$\impliedby$“ Induktion nach t. $t = 1$ ist klar. Sei also $t > 1$ und $x_0 \in \mathbb{Z}$ mit $x_0^2 \equiv k \mod p^{t-1}$. Gesucht x, nötig $x \equiv x_0 \mod p^{t-1}$.
Ansatz: $x = x_0 + cp^{t-1},\ x_0^2 = k + vp^{t-1}\ (c, v \in \mathbb{Z})$.
Idee: Bestimme c, so dass $x^2 \equiv k \mod p^t$.

$$x^2 = \left(x_0 + cp^{t-1}\right)^2 = k + vp^{t-1} + 2x_0cpt - 1 + c^2 + \underbrace{p^{2t-2}}_{\equiv 0 \mod p^t}$$

$$\begin{aligned} &\overset{!}{\equiv} k \mod p^t \\ \iff\ & vp^{t-1} \equiv -2x_0cp^{t-1} \mod p^t \\ \iff\ & v \equiv -2x_0c \mod p \end{aligned}$$

Klappt mit $\overline{c} = \overline{v}(\overline{-2x_0})^{-1}$ in $\mathbb{F}_p$, da $p \nmid x_0$ (wegen $x_0^2 \equiv k \neq 0 \mod p$), $p \nmid 2 \implies \overline{-2x_0} \in \mathbb{F}_p^\times$. ■

Resultat der Diskussion: Frage der Lösbarkeit von quadratischen Kongruenzen lässt sich zurückführen auf die Frage, welche k mit $p \nmid k$ für prime p größer zwei quadratische Reste sind oder nicht. Erinnerung an Eulers Quadratkriterium!

5.2 Grundaussagen über Potenzreste

Bezeichnung

(1) $(G, \cdot)$ abelsche Gruppe, $l \in \mathbb{N}_+ : \ G^{(l)} := \{x^l : \ x \in G\}$, $G^{(l)}$ ist Untergruppe von G (Ist mit Untergruppenkriterium schnell gezeigt).

(2) $k \in \mathbb{Z}$ heißt l-ter *Potenzrest* $\mod m$, $m \in \mathbb{N}_+ \iff k \in ((\mathbb{Z}/m\mathbb{Z})^\times)^{(l)} \iff \mathrm{ggT}(m,k) = 1$ und es existiert $x \in \mathbb{Z}$ mit $x^l \equiv k \mod m$.

Lemma 5.1
$(G, \cdot)$ abelsche Gruppe, $n = \#G < \infty$.
$d := \mathrm{ggT}(n, l)$. Dann ist $G^{(l)} = G^{(d)}$.

Beweis
$x \in G$, $\underbrace{x^l}_{\in G^{(l)}} = \underbrace{x^{\frac{l}{d}d}}_{\in G^{(d)}}$, also ist $G^{(l)} \subset G^{(d)}$. Der LinKom-Satz 1.10 liefert $d = un + vl$ mit $u, v \in \mathbb{Z}$.
$\underbrace{x^d}_{\in G^{(d)}} = \underbrace{x^{nu}}_{=1(\mathrm{EOS})} \ x^{lv} = (x^v)^l \in G^{(l)}$, also ist $G^{(d)} \subset G^{(l)}$. Folglich sind beide Mengen gleich. ■

Nächste Frage: Was ist $\#\left(((\mathbb{Z}/p^t\mathbb{Z})^\times)^{(d)}\right)$?

Klar: Falls $G = \langle\zeta\rangle = \left\{1, \zeta, \ldots, \zeta^{m-1}\right\}$ dann $d = \mathrm{ggT}(k, m)$
$G^{(k)} = G^{(d)} = \left\{1, \zeta^d, \zeta^{2d}, \ldots, \zeta^{\left(\frac{m}{d}-1\right)d}\right\}$
$\implies \#G^{(k)} = \#G^{(d)} = \frac{m}{d}$
Ergebnis also

Satz 5.2 (Potenzrestklassenanzahlsatz)
(i) Sei $p \in \mathbb{P}$, $p > 2$, $k, t \in \mathbb{N}_+$. Dann gilt

$$\#\left(\left(\mathbb{Z}/p^t\mathbb{Z}\right)^\times\right)^{(k)} = \frac{\varphi(p^t)}{\mathrm{ggT}(\varphi(p^t), k)}$$

(In Worten: Es gibt genau $\frac{\varphi(p^t)}{\mathrm{ggT}(\varphi(p^t),k)}$ k-te Potenzrestklassen.

(ii) Für $2 \nmid k$ ist $\left(\left(\mathbb{Z}/2^t\mathbb{Z}\right)^\times\right)^{(k)} = \left(\mathbb{Z}/2^t\mathbb{Z}\right)^\times$.
Für $t > 2$ und $2 \mid k$ ist $\left(\left(\mathbb{Z}/2^t\mathbb{Z}\right)^\times\right)^{(k)}$ zyklisch und hat $\frac{2^{t-2}}{\mathrm{ggT}(2^{t-1},k)}$ Elemente.

(iii) (Potenzrestkriterium a la Euler)
Sei $p \in \mathbb{P}$, $p > 2$, $t, k \in \mathbb{N}_+$, $d = \mathrm{ggT}(\varphi(p^t), k)$
r ist k-ter Potenzrest mod $p^t \iff r^{\frac{\varphi(p^t)}{d}} \equiv 1 \bmod p^t$.

Beweis
Beweise (iii) wie Eulerkriterium, benutze primitives Element!

Folge: $p \in \mathbb{P}$, $p > 2 \implies$ Es gibt genau $\frac{p-1}{2}$ quadratische Reste und $\frac{p-1}{2}$ quadratische Nichtreste.
Grund: (i) mit $k = d = 2$, $t = 1$, $\varphi(p) = p - 1$
Bsp: $p = 11$

x	±1	±2	±3	±4	±5
$x^2 \bmod 11$	1	4	9	5	3

$\leftarrow$ quadratische Reste
$\{2, 6, 7, 8, 10\} \leftarrow$ quadratische Nichtreste

5.3 Quadratische Reste und das quadratische Reziprozitätsgesetz

$p \in \mathbb{P}$, $p > 2$

Definition
(1)

$$k \text{ quadratischer Rest} \mod p \iff \overline{k} \in \left(\left(\mathbb{F}_p\right)^\times\right)^{(2)}$$
$$k \text{ quadratischer Nichtrest} \mod p \iff \overline{k} \in \mathbb{F}_p^x \setminus \left(\left(\mathbb{F}_p\right)^\times\right)^{(2)}$$

(2) Die Frage der Lösbarkeit quadratischer Kongruenzen lässt sich zurückführen auf die Frage, ob k quadratischer Rest ist oder nicht ($\bmod p$).

Definition
Sei $p \in \mathbb{P}$, $p > 2$, $u \in \mathbb{Z}$, so sei

$$\left(\frac{u}{p}\right) = \begin{cases} 1 & u \text{ quadratischer Rest} \mod p \\ -1 & u \text{ quadratischer Nichtrest} \mod p \\ 0 & \text{sonst, d. h. } p \mid u \end{cases}$$

$\left(\frac{u}{p}\right)$ heißt *Legendre-Symbol*.

Satz 5.3 (Legendre-Symbol-Satz)
Sei $a, b \in \mathbb{Z}$, $p \in \mathbb{P}$, $p > 2$, dann gelten

(i) $a \equiv b \bmod p \implies \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$, und $\left(\frac{a}{p}\right) \in \{0, \pm 1\}$

(ii) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$, insbesondere hat man den Gruppenhomomorphismus

$$\chi_p : \mathbb{F}_p^\times \to \mathbb{C}^\times,\ \chi_p(\overline{a}) = \left(\frac{a}{p}\right) =: \left(\frac{\overline{a}}{p}\right)$$

(Homomorphismen $G \to \mathbb{C}^\times$, G abelsche Gruppe, heißen traditionell Charaktere der Gruppe G, χ_p heißt Dirichlet-Charakter)

(iii) $\left(\frac{ab^2}{p}\right) = \left(\frac{a}{p}\right)$ falls $p \nmid b$.

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

Beweis

(i) Definition.

(iv) Eulerkriterium:

$$a \text{ quadratischer Rest} \iff \overline{a}^{\frac{p-1}{2}} = 1 \text{ in } \mathbb{F}_p$$
$$a \text{ quadratischer Nichtrest} \iff \overline{a}^{\frac{p-1}{2}} = -1 \text{ in } \mathbb{F}_p$$

$p \mid a \iff p \mid a^{\frac{p-1}{2}}$

(ii) $\left(\frac{ab}{p}\right) \overset{\text{(iv)}}{\equiv} (ab)^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$. Wegen $-\frac{p}{2} < \left(\frac{a}{p}\right) < \frac{p}{2} \implies \left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$

(iii) $\left(\frac{ab^2}{p}\right) \overset{\text{(ii)}}{=} \left(\frac{a}{p}\right)\left(\frac{b^2}{p}\right) = \left(\frac{a}{p}\right) \underbrace{\left(\frac{b}{p}\right)^2}_{=1} = \left(\frac{a}{p}\right)$ ∎

Satz gibt Algorithmus zur Berechnung von $\left(\frac{a}{p}\right)$.

Skizze:

(1) $\left(\frac{a}{p}\right) = \left(\frac{a \bmod p}{p}\right) = \left(\frac{r}{p}\right) = \left(\frac{\operatorname{sgn}(r)}{p}\right)\left(\frac{|r|}{p}\right)$

(2) Primzerlegung von $|r| = p_1^{n_1} \cdot \ldots \cdot p_t^{n_t}$
$\left(\frac{2}{p}\right)$ elementar „Ergänzungssatz“
$\left(\frac{q}{p}\right)$ $q \in \mathbb{P}$, $q > 2$, $q \neq p$ geht zurück auf $\left(\frac{p}{q}\right)$ mittels des quadratischen Reziprozitätsgesetzes.

Nämlich:

Legendre: Experimente zeigen unerwartete und „unerklärliche“ Zusammenhänge zwischen $\left(\frac{p}{q}\right)$ und $\left(\frac{q}{p}\right)$. Zum Beispiel $\left(\frac{p}{5}\right) = \left(\frac{5}{p}\right)$ $(\star)$ oder $\left(\frac{p}{7}\right) = -\left(\frac{7}{p}\right)$ und Ähnliche.
$(\star)$ Beweisversuch: Wenn $x \in \mathbb{Z}$ mit $x^2 \equiv 5 \bmod p$ $(p \mid x^2 - 5)$ so konstruiere $y \in \mathbb{Z}$, $y = y(x, 5, p)$ mit $y^2 \equiv p \bmod 5$ $(5 \mid y^2 - p)$.
Bis heute eine Formel für so ein y unbekannt!

Der folgende Satz ist der berühmteste Satz der Elementaren Zahlentheorie.

Satz 5.4 (Quadratisches Reziprozitätsgesetz von Gauß)
(i) Es seinen $p, q \in \mathbb{P}$, $p > 2$, $q > 2$, $p \neq q$. Dann gilt

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

(ii) „Ergänzungssätze“ $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1 & p \equiv 1 \bmod 4 \\ -1 & p \equiv -1 \bmod 4 \end{cases}$

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1 & p \equiv \pm 1 \bmod 8 \\ -1 & p \equiv \pm 3 \bmod 8 \end{cases}$$

Gauß gab 7 wesentlich verschiedene Beweise, heute 200 bekannt. Kein „Eselsbeweis“ dabei. Heute befriedigender Beweis via „Artins“ Reziprozitätsgesetz.

Artins Hauptsatz der sog. „Klassenkörpertheorie“ stellt eine Isomorphie her zwischen den Automorphismusgruppen („Galoisgruppen“), sog. abelschen Zahlkörper und sog. Strahlklassengruppen (verallg. Restklassengruppen).

Beweis
Hier: Raffinierter Beweis mit endlichen Körpern
In $L = \mathbb{F}_{p^{q-1}}$ existiert $\omega \in L^\times$ mit $\operatorname{ord}(\omega) = q$
Dann ist für $\alpha \in \overline{a}$ in $\mathbb{F}_q$ wohldefiniert $\omega^\alpha := \omega^a$ (Elementordnungssatz)
Fasse $\left(\frac{a}{q}\right) =: \left(\frac{\alpha}{q}\right)$ als Element von L auf $\begin{pmatrix} = & 0_L \\ & \pm 1_L \end{pmatrix}$
Bezeichung $\tau := \sum_{\alpha \in \mathbb{F}_q} \left(\frac{\alpha}{q}\right) \cdot \omega^\alpha$ $(\in L)$ heißt Gaußsche Summe.
$\left[\text{Gauß benutzte statt } \omega\ \zeta = e^{\frac{2\pi i}{q}} \in \mathbb{C} \ (\operatorname{ord} \zeta = q \text{ in } \mathbb{C}^\times)\right]$

Formeln a la Gauß $\tau^2 = q \cdot \left(\frac{-1}{q}\right) \cdot 1_L$ (a)

$$\tau^{p-1} = \left(\frac{p}{q}\right) \cdot 1_L \quad \text{(b)}$$

Aus diesen Formeln ergibt sich das Gesetzt mit dem Eulerkriterium
$\left(\frac{q}{p}\right) \equiv q^{\frac{p-1}{2}} \bmod p$ (also $\left(\frac{q}{p}\right) \cdot 1_L = q^{\frac{p-1}{2}} \cdot 1_L$)

$$\left(\tfrac{q}{p}\right)\cdot 1_L = (q\cdot 1_L)^{\frac{p-1}{2}}$$
$$\overset{\text{(a)}}{=} \left(\left(\tfrac{-1}{q}\right)\tau^2\right)^{\frac{p-1}{2}} = \left(\tfrac{-1}{q}\right)^{\frac{p-1}{2}}\tau^{p-1} \overset{\text{(ii)}}{=} (-1)^{\frac{q-1}{2}\cdot\frac{p-1}{2}}\cdot\tau^{p-1}$$
$$\overset{\text{(b)}}{=} (-1)^{\frac{q-1}{2}\cdot\frac{p-1}{2}}\cdot\left(\tfrac{p}{q}\right)\cdot 1_L$$
$$\Longrightarrow \left(\tfrac{p}{q}\right)\left(\tfrac{q}{p}\right) = (-1)^{\frac{q-1}{2}\cdot\frac{p-1}{2}}$$

$$\left[\text{Hinweis: } \left(\tfrac{p}{q}\right)\in\{\pm 1\} \Longrightarrow \left(\tfrac{p}{q}\right)^{-1} = \left(\tfrac{p}{q}\right)\right]$$

Details: 1. Man verschaffe sich ω: $L = \mathbb{F}_{p^{q-1}}$ enthält primes Element ζ, ord $\zeta = p^{q-1}-1$. Bekanntlich $p^{q-1}\equiv 1 \bmod q$ wegen $\overline{p}\in\mathbb{F}_q^x$ (Euler)

$\Longrightarrow q \mid p^{q-1}-1 = \text{ord }\zeta$. Setze $\omega = \zeta^{\frac{\text{ord }\zeta}{q}}$

$\Longrightarrow$ ord $\omega = q$.

Nachrechnen (b): Verwende: In Körper L mit $\mathbb{F}_p$ Teilkörper ist $(\alpha+\beta)^p = \alpha^p+\beta^p$

$\tau^p = \sum_{\alpha\in\mathbb{F}_q} \underbrace{\left(\frac{\alpha}{p}\right)^p}_{=\left(\frac{\alpha}{q}\right)} \omega^{\alpha p} \quad \{\alpha p \mid \alpha\in\mathbb{F}_q\} = \mathbb{F}_q$ da $p\in\mathbb{F}_q^x$.

$$\left[\text{Summationstransfer: } \beta=\alpha p \Longrightarrow \left(\tfrac{\alpha}{q}\right) = \left(\tfrac{\beta\overline{p}^{-1}}{q}\right) = \left(\tfrac{\beta}{q}\right)\left(\tfrac{\overline{p}}{q}\right)^{-1} (\text{ da } \chi_q \text{ Homomorphismus})\right]$$

$$\Longrightarrow \tau^p = \sum_{\beta\in\mathbb{F}_q} \underbrace{\left(\frac{\overline{p}}{q}\right)^{-1}}_{\left(\frac{p}{q}\right)} \left(\tfrac{\beta}{q}\right)\omega^\beta = \left(\tfrac{p}{q}\right)\sum_{\beta\in\mathbb{F}_q}\left(\tfrac{\beta}{q}\right)\omega^\beta = \left(\tfrac{p}{q}\right)\tau$$

Wegen $\tau\neq 0$ (folgt aus a) (b) OK.

(a) später

Zu den Ergänzungssätzen

$\left(\tfrac{-1}{q}\right)\equiv(-1)^{\frac{p-1}{2}} \bmod p$, $-\frac{p}{2} < \left(\tfrac{-1}{q}\right), (-1)^{\frac{p-1}{2}} < \frac{p}{2}$

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

Demnach
-1 quadratischer Rest mod p $\iff p\equiv 1 \bmod 4$, also für $p = 5, 13, 17, 23, \ldots$
-1 quadratischer Nichtrest mod p $\iff p\equiv -1 \bmod 4$, also für $p = 3, 7, 11, \ldots$

Bsp: $-1\in\mathbb{F}_{13}$ $5^2\equiv -1 \bmod 13$ ∎

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

$\tau = \sum_{\alpha\in\mathbb{F}_q}\left(\tfrac{\alpha}{q}\right)\omega^\alpha$, ord$(\omega) = q$, Gaußsche Summe

Berechnung τ^2:

Sei $\left(\frac{0}{q}\right) = 0,\ \alpha \in \mathbb{F}_q^\times$:

$$\begin{aligned}
\tau^2 &= \sum_{\alpha\in\mathbb{F}_q} \left(\frac{\alpha}{q}\right)\omega^\alpha \cdot \sum_{\beta\in\mathbb{F}_q}\left(\frac{\beta}{q}\right)\omega^\beta \\
&= \sum_{\alpha\in\mathbb{F}_p^\times}\sum_{\beta\in\mathbb{F}_q}\left(\frac{\alpha}{q}\right)\left(\frac{\beta}{q}\right)\omega^{\alpha+\beta}, \qquad (\mathbb{F}_q = \{\underbrace{\alpha+\beta}_{:=\gamma}\big|\beta\in\mathbb{F}_q) \\
&= \sum_{\alpha\in\mathbb{F}_q^\times}\sum_{\gamma\in\mathbb{F}_q}\left(\frac{\alpha}{q}\right)\left(\frac{\gamma-\alpha}{q}\right)\omega^\gamma \\
&= \sum_{\gamma\in\mathbb{F}_q}\underbrace{\sum_{\alpha\in\mathbb{F}_q^\times}\left(\frac{\alpha}{q}\right)\left(\frac{\gamma-\alpha}{q}\right)}_{=:C_\gamma}
\end{aligned}$$

$\underline{\gamma = 0}$: $C_0 = \sum_{\alpha\in\mathbb{F}_q^\times}\underbrace{\left(\frac{-\alpha^2}{q}\right)}_{\left(\frac{-1}{q}\right)} = (q-1)\left(\frac{-1}{q}\right)\cdot 1_L$

$\underline{\gamma \neq 0}$: $\left(\frac{\alpha}{q}\right)\left(\frac{\gamma-\alpha}{q}\right) = \underbrace{\left(\frac{\alpha}{q}\right)\left(\frac{\alpha}{q}\right)}_{=1}\left(\frac{\gamma\alpha^{-1}-1}{q}\right)$

$$\begin{aligned}
C_\gamma &= \sum_{\alpha\in\mathbb{F}_q^\times}\left(\frac{\gamma\alpha^{-1}-1}{q}\right) \\
&\quad \left[X := \{\gamma\alpha^{-1}\big|\underbrace{\alpha\in\mathbb{F}_q^\times,\ \alpha\neq\gamma}_{q-2\ \alpha\text{'s}}\} \subseteq \mathbb{F}_q^\times \implies \#X = q-2,\ -1\notin X \implies X = \mathbb{F}_q^\times\setminus\{-1\}\right] \\
&= \sum_{\sigma\in\mathbb{F}_q^\times\setminus\{-1\}}(\frac{\sigma}{q}) \\
&= \underbrace{\sum_{\sigma\in\mathbb{F}_q^\times}(\frac{\sigma}{q})}_{\substack{=\left(\frac{q-1}{2}\right)\cdot 1-(\frac{q-1}{2}) \\ \text{(da gleich viele quadratische} \\ \text{Reste wie Nichtreste)}}} - \left(\frac{-1}{q}\right) \\
&= -\left(\frac{-1}{q}\right)
\end{aligned}$$

$$\begin{aligned}\tau^2 &= \sum_{\gamma\in\mathbb{F}_q} C_\gamma \omega^\gamma \\ &= (q-1)\left(\frac{-1}{q}\right)\cdot 1_L + \sum_{\gamma\in\mathbb{F}_q^\times} -\left(\frac{-1}{q}\right)\omega^\gamma \\ &= (q-1)\left(\frac{-1}{q}\right)\cdot 1_L - (\frac{-1}{q})\sum_{j=0}^{q-1}\omega^j + \underbrace{\left(\frac{-1}{q}\right)}_{\text{Kompensiert } j=0} \\ &= q\left(\frac{-1}{q}\right)\cdot 1_L - \underbrace{\left(\frac{-1}{q}\right)\frac{\omega^q-1}{\omega-1}}_{=0, q=\mathrm{ord}(\omega), \text{ da } \omega^q=1}\end{aligned}$$

Ergebnis: $\tau^2 = q\left(\frac{-1}{q}\right)\dot{1}_L$ (a)
Ergänzungssatz $\left(\frac{2}{q}\right)$: Übung

Anwendung der Eulerformel und des quadratischen Reziprozitätsgesetzes Hiervon gibt es viele. Hier über $\mathbb{F}_n$.
Euler: $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \mod p, p>2, p\nmid a \implies \overline{a}^{\frac{p-1}{2}} = \left(\frac{a}{p}\right)$ in $\mathbb{F}_p$
$\left(\frac{a}{p}\right) = -1 \implies \mathrm{ord}(\overline{a}) \nmid \frac{p-1}{2}$, immer $\mathrm{ord}(\overline{a}) \mid p-1$
Also: $v_2(\mathrm{ord}(\overline{a})) = v_2(p-1)$
Sagt am Meisten, wenn $p-1 = 2^k, k>0$. Dann $\mathrm{ord}(\overline{a}) \mid 2^k, \mathrm{ord}(\overline{a}) \nmid 2^{k-1} \implies \mathrm{ord}(\overline{a}) = p-1 = 2^k \implies \overline{a}$ ist primitiv.

Falls $2^k+1 = p \in \mathbb{P}$, so ist a Primitivwurzel $\iff (\frac{a}{p}) = -1 (p\in\mathbb{P} \implies k = 2^n, n\in\mathbb{N}_+, p = F_n = 2^{2^n}+1$ n-te Fermatzahl (1. Übungsblatt).

Falls das so ist, so ist 3 eine Primitivwurzel $\mod p$.
Berechne $(\frac{3}{p})$. $p = 2^k+1 \equiv 1 \mod 4 (k\geq 2) \implies (-1)^{\frac{p-1}{2}} = 1 \implies (\frac{3}{p})(\frac{p}{3}) = (-1)^{\frac{2}{2}\cdot\frac{p-1}{2}} = 1 \implies (\frac{3}{p}) = (\frac{p}{3})$ (quadratisches Reziprozitätsgesetz!)
Berechne $p \mod 3$. $p = F_n = 2^{2^n}+1, n\geq 1$. (Folgende Äquivalenz stimmt wohl nicht ganz, bitte überprüft das jemand) $2\equiv -1 \mod 3, p \equiv (-1)^{2^n}+1 \equiv 1+1 \equiv -1 \mod 3 \implies \left(\frac{3}{p}\right) = \left(\frac{p}{3}\right) = \left(\frac{-1}{3}\right)$

Satz 5.5 (Fermat-Zahl-Satz)
(1) Sei $k\in\mathbb{N}_+, p = 2^k+1$. Dann gilt $p\in\mathbb{P} \implies k = 2^n (n\in\mathbb{N}) \implies p = F_n = 2^{2^n}+1$
(2) Ist $p = F_n \in \mathbb{P}, a\in\mathbb{Z}, p\nmid a, n\geq 1$, so gilt: a Primitivwurzel $\mod a \iff (\frac{a}{p}) = -1$. Trifft zu auf $a=3$
(3) Pepins-Test: Sei $n\in\mathbb{N}_+$. Dann gilt: $F_n = 2^{2^n}+1 \in \mathbb{P} \iff 3^{2^{(2^n-1)}} \equiv -1 \mod F_n$

Beweis
(1) ✓

(2) ✓

(3) „$\Longrightarrow$“: $F_n = p \in \mathbb{P} \implies 3$ Primitivwurzel $\mod p$, $\operatorname{ord}(\overline{3}) \mid p-1 = 2^{2^n} \implies \overline{3}^{2^{2^n-1}} = \overline{3}^{\frac{2^{2^n}}{2}} = \pm 1$. Bei $+1$ keine Primitivwurzel.
„$\Longleftarrow$“: Sei $p \in \mathbb{P}, p \mid F_n = 2^{2^n}+1$. $3^{2^{2^n-1}} \equiv -1 \mod F_n \implies 3^{2^{2^n-1}} \equiv -1 \mod p, 3^{2^{2^n}} \equiv 1 \mod F_n \implies 3^{2^{2^n}} \equiv 1 \mod p$. $F_n - 1 = \operatorname{ord}(\overline{3}) = 2^{2^n} \leq p-1$ ($\operatorname{ord}(\overline{3})$ in $\mathbb{F}_p$ teilt $\#\mathbb{F}_p^\times = p-1$) ∎

5.3.1 Jacobi-Symbol

Definition
Sei $a \in \mathbb{Z},\ m \in \mathbb{N}_+,\ 2 \nmid n,\ \operatorname{ggT}(a,m) = 1$ $(\star)$. Definiere in diesem Fall das Jacobi-Symbol $\left(\frac{a}{m}\right)$ durch:

$$\left(\frac{a}{m}\right) = \prod_{\substack{p \in \mathbb{P} \\ p \mid m}} \left(\frac{a}{p}\right)_L^{v_p(m)},$$

andernfalls ist $\left(\frac{a}{m}\right)$ nicht definiert. Hierbei ist $\left(\frac{a}{p}\right)_L$ das Legendre-Symbol.

Klar:

$\left(\frac{a}{1}\right) = \left(\frac{1}{m}\right) = 1$

$m \in \mathbb{P}, m > 2$, so ist Jacobi $\left(\frac{a}{m}\right)$ = Legendre $\left(\frac{a}{m}\right)$

Satz 5.6 (Jacobi-Symbolsatz)
Falls $a, a' \in \mathbb{Z}, m, m' \in \mathbb{Z}$, so gelten, falls die vorhandenen Jacobi-Symbole definiert sind:

(i) $a \equiv b \mod m \implies \left(\frac{a}{m}\right) = \left(\frac{b}{m}\right)$

(ii) $\left(\frac{aa'}{m}\right) = \left(\frac{a}{m}\right)\left(\frac{a'}{m}\right),\ \left(\frac{a}{mm'}\right) = \left(\frac{a}{m}\right)\left(\frac{a}{m'}\right)$

(iii) $\left(\frac{a}{m}\right)\left(\frac{m}{a}\right) = (-1)^{\frac{a-1}{2}\cdot\frac{m-1}{2}}$ (Reziprozitätsgesetz)

(iv) $\left(\frac{-1}{m}\right) = (-1)^{\frac{m-1}{2}}, \left(\frac{2}{m}\right) = (-1)^{\frac{m-1}{8}}$ (Ergänzungssätze)

Algorithmus-Skizze zur Berechnung von $\left(\frac{a}{m}\right)$

0. $m = 1 : \left(\frac{a}{m}\right) = \left(\frac{a}{1}\right) = 1$
1. $m > 1, 2 \nmid m, \left(\frac{a}{m}\right) = \left(\frac{r}{m}\right)$ mit $r = a \bmod m$ (also $|r| < \frac{m}{2}$)
2. Stelle r dar als $r = \operatorname{sign}(r) 2^{v_2(r)} r_0$ (also $r_0 > 0, 2 \nmid r_0, |r| < \frac{m}{2}$)
   Rechenaufwand minimal!

$$\left(\frac{r}{m}\right) = \underbrace{\left(\frac{\operatorname{sign}(r)}{m}\right)\left(\frac{2}{m}\right)^{v_2(r)}}_{=:\Upsilon}\left(\frac{r_0}{m}\right)$$

Rechenaufwand für Υ ist ebenfalls minimal.

3. $\left(\frac{r_0}{m}\right) = \left(\frac{m}{r_0}\right)(-1)^{\frac{r_0-1}{2}\cdot\frac{m-1}{2}}$, wende Verfahren auf $\left(\frac{m}{r_0}\right.$ an. Problem reduziert von m auf r_0 mit $0 < r_0 < \frac{m}{2}$. Schleife wird ca. $\log_2 m$ mal durchlaufen.
   ! Primzerlegung kommt nirgends vor **!**

Bemerkung Aus $\left(\frac{a}{m}\right) = 1$ folgt nicht, dass a quadratischer Rest mod m ist.

Beispiel
$\left(\frac{2}{15}\right) = \left(\frac{2}{3}\right)\left(\frac{2}{5}\right) = (-1)(-1) = 1$. 2 ist quadratischer Nichtrest mod 3 und erst recht quadratischer Nichtrest von mod 15

Beweis (Jacobi-Symbolsatz 5.6)

(i) $p \mid m, p \in \mathbb{P}, a \equiv b \mod m \implies a \equiv b \mod p \implies \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right) \implies \left(\frac{a}{m}\right) = \left(\frac{b}{m}\right)$

(ii) $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$ (Legendre Symbol) $\implies \left(\frac{a}{m}\right)\left(\frac{b}{m}\right) = \left(\frac{ab}{m}\right)$
$\left(\frac{a}{mm'}\right) = \prod_{p\in\mathbb{P}}\left(\frac{a}{p}\right)^{v_p(mm')} = \prod_{p\in\mathbb{P}}\left(\frac{a}{p}\right)^{v_p(m)+v_p(m')} = \prod_{p\in\mathbb{P}}\left(\left(\frac{a}{p}\right)^{v_p(m)}\left(\frac{a}{p}\right)^{v_p(m')}\right) =$
$\prod_{p\in\mathbb{P}}\left(\frac{a}{p}\right)^{v_p(m)} \cdot \prod_{p\in\mathbb{P}}\left(\frac{a}{b}\right)^{v_p(m')} = \left(\frac{a}{m}\right)\left(\frac{a}{m'}\right)$

(iii) $\left(\frac{a}{m}\right)\left(\frac{m}{a}\right) = (-1)^{\frac{a-1}{2}\cdot\frac{m-1}{2}}$ klar für $m = 1$ oder $a = 1$. Also $m > 1, a > 1$ voraussetzbar. $2 \nmid m, 2 \nmid a$.
Falls $m \in \mathbb{P}$ und $a \in \mathbb{P}(\text{ggT}(m, n) = 1)$, so steht das quadratische Reziprozitätsgesetz für das Legendre Symbol da.
Also nur noch zu beweisen, wenn a oder $m \notin \mathbb{P}$ etwa $m = uv,\ 1 < v < m$.
Induktion nach a, m:
Induktionhypothese: $\left(\frac{a}{u}\right)\left(\frac{u}{a}\right) = (-1)^{\frac{a-1}{2}\cdot\frac{u-1}{2}}$, $\left(\frac{a}{v}\right)\left(\frac{v}{a}\right) = (-1)^{\frac{a-1}{2}\cdot\frac{v-1}{2}}$
$\left(\frac{a}{uv}\right)\left(\frac{uv}{a}\right) \overset{(ii)}{=} \left(\frac{a}{u}\right)\left(\frac{a}{v}\right)\left(\frac{u}{a}\right)\left(\frac{v}{a}\right) \overset{\text{I.H.}}{=} (-1)^{\frac{a-1}{2}\cdot\frac{u-1}{2}}(-1)^{\frac{a-1}{2}\cdot\frac{v-1}{2}} \overset{?}{=} (-1)^{\frac{a-1}{2}\cdot\frac{uv-1}{2}}$

Genügt: $n-1+v-1 = uv-1 \mod 4$. Das stimmt, weil $2 \nmid u, 2 \nmid v$ und $u, v \equiv \pm 1 \mod 4$

(iv) Ähnliche Induktion ∎