Vortrag zum Thema Quadratische Reste und Quadratische Reziprozität

Aran Salih

19. Mai 2017

In den folgenden Seiten werden die ersten beiden Paragraphen des Kapitels 5, des Buches " A Classical Introduction to Modern Number Theory" (second edition, Springer 1990) von Kenneth Ireland und Michael Rosen behandelt.

Vorwort

Allgemein betrachten wir p, wobei p Primzahl ist (Notation: $p \in Prim$) und die *Kongruenz* $x^2 \equiv a\ (p)$ (in Worten: x^2 ist kongruent zu a modulo p). In den folgenden Seiten wird die Kenntnis der Definition von Kongruenzen vorausgesetzt. Die Kongruenz $x^2 \equiv a\ (p)$ ist genau dann lösbar, wenn gilt $a^{\frac{p-1}{2}} \equiv 1\ (p)$. Die Rückrichtung dieses Satzes "Für welche$p$ ist $x^2 \equiv a\ (p)$ lösbar?", ist um einiges komplizierter zu klären. Eine Antwort auf diese Frage liefert das sogenannte *Quadratic law*, welches von Legendre und Euler formuliert wurde. Der vollständige Beweis stammt jedoch von Gauß, der es auch als *goldenes Theorem* bezeichnet hat.

1 Quadratische Reste

Definition 1.1

Sei $(a, p) = 1$ (d.h. a und p sind teilerfremd).
So wird a als *quadratischer Rest mod* p^k bezeichnet, falls die Kongruenz $x^2 \equiv a\ (p^k)$ $(k \in \mathbb{N})$ eine Lösung besitzt.

Sonst wird a als *quadratischer Nicht-Rest mod* p^k bezeichnet.

Beispiel 1.2

Die Zahl 2 ist ein quadratischer Rest modulo 7. Die Zahl 3 ist ein quadratischer Nicht-Rest mod 7. Somit besitzt die Kongruenz $x^2 \equiv 2\ (7)$ eine Lösung und die Kongruenz $x^2 \equiv 3\ (7)$ keine. Die Berechnung der quadratischen Reste modulo 7 lässt sich folgender Tabelle entnehmen:

k <7	1	2	3	4	5	6
k quadrieren	1	4	9	16	25	36
k^2 mod 7	1	4	2	2	4	1

Die Zahlen 2 und 4 sind quadratische Reste mod 7, während 3, 5 und 6 quadratische Nicht-Reste mod 7 sind. Es existieren andere Wege, quadratische Reste zu berechnen und analysieren. Wir werden später sehen, dass es kein Zufall ist in diesem Beispiel, dass wir die gleiche Anzahl an quadratischen Resten mod 7 haben wie quadratische Nicht-Reste mod 7. In Korollar 1.7 wird darauf näher eingegangen.

Proposition 1.3

Sei $m = 2^e p_1^{k_1} \cdot \ldots p_n^{k_n}$ $(k_i \in \mathbb{N})$ die Primfaktorzerlegung von m. Zudem gelte $(a, m) = 1$. Dann ist $\mathrm{x}^2 \equiv a\ (m)$ genau dann lösbar, wenn folgende Bedingungen erfüllt sind

a) Falls $e = 2$, dann gilt $a \equiv 1\ (4)$.
   Falls $e \geqslant 3$, dann gilt $a \equiv 1\ (8)$.

b) Es gilt $a^{\frac{p_i - 1}{2}} \equiv 1\ (p_i)$ für alle $i \in \{1, \ldots, \ell\}$

Beweis

Im Beweis wird die Aussage des *chinesischen Restsatz-Theorems* verwendet, den wir jetzt näher betrachten werden.
Eine kurze Definition des chinesischen Restsatz-Theorems (kurz CRST):
Für das System von Kongruenzen

$$\begin{cases} x \equiv a_1\ (p_1), \\ x \equiv a_2\ (p_2), \\ \vdots \\ x \equiv a_k\ (p_k). \end{cases}$$

wobei $ggT(p_1, \ldots, p_k) = 1$ ist, existiert eine Lösung.
Wir zeigen, dass die Kongruenz $x^2 \equiv a\ (2^e p_1^{k_1} \ldots p_\ell^{k_\ell})$ äquivalent ist zu der Lösbarkeit der folgenden Kongruenzen :

$$\begin{aligned} x^2 &\equiv a\ (2^e), \\ x^2 &\equiv a\ (p_1^{k_1}), \\ &\vdots \\ x^2 &\equiv a\ (p_\ell^{k_\ell}). \end{aligned}$$

Es genügt somit die Lösungen der einzelnen Kongruenzen zu finden.
Seien b_i die Lösung der jeweiligen Kongruenz für alle $i \in \{1, \ldots \ell\}$.

$$\begin{cases} b_0^2 \equiv a\ (2^e), \\ b_1^2 \equiv a\ (p_1^{k_1}), \\ \vdots \\ b_l^2 \equiv a\ (p_\ell^{k_\ell}). \end{cases}$$

Das CRST verlangt in seinen Voraussetzungen, ein System von Kongruenzen, welches auf der linken Seite des Gleichheitszeichens, das selbe x hat. Es berechnet also eine gemeinsame Lösung für die Kongruenzen im System. Nun konstruiert man sich ein System aus Kongruenzen, welche auf der linken Seite des Gleichheitszeichens, das gleiche x hat,während auf der rechten Seite die b_i stehen. So erhalten wir das folgende System

$$\begin{cases} x \equiv b_0\ (2^e), \\ x \equiv b_1\ (p_1^{k_1}), \\ \vdots \\ x \equiv b_\ell\ (p_\ell^{k_\ell}). \end{cases}$$

Nach der Definition des CRST existiert eine Lösung y für dieses System von Kongruenzen. Es gilt

$$\begin{cases} (y)^2 \equiv b_0^2 \equiv a\ (2^e), \\ (y)^2 \equiv b_1^2 \equiv a\ (p_1^{k_1}), \\ \vdots \\ (y)^2 \equiv b_\ell^2 \equiv a\ (p_\ell^{k_\ell}). \end{cases}$$

Damit haben wir gezeigt, dass die Lösbarkeit der einzelnen Kongruenzen, die Lösbarkeit der Kongruenz $x^2 \equiv a\ (2^e p_1^{k_1} \dots p_\ell^{k_\ell})$ impliziert. Wir müssen nun nur zeigen, wann jede einzelne Kongruenz eine Lösung besitzt. Im folgenden ist es sehr wichtig, dass gilt $(a, m) = 1$.

Fall 1: Sei $x^2 \equiv a\ (2^e)$.
Man sieht, dass die Zahl 1 der einzige quadratische Rest mod 4 und mod 8 ist. Beachte, dass 4 als quadratischer Rest mod 8, nicht in Betrachtung gezogen wird, da gelten muss $(a, 2^3 = 8) = 1$. Somit erhält man die Lösbarkeit des Systems, falls gilt $a \equiv 1\ (4)$ für $e = 2$ und $a \equiv 1\ (8)$ für $e = 3$.

Wir müssen noch den Fall für $n > 3$ untersuchen.
Zu zeigen: $x^2 \equiv a\ (2^{n+1})$ lösbar für $n > 3$.
Wir nutzen die Induktion nach n. Als *Induktionsanfang* nehmen wir den bereits gezeigten Fall für $n > 3$. Sei ein x_0 gegeben mit $x_0^2 \equiv 1\ (2^n)$ für n=3 .
Induktionschritt: Gesucht ist eine Lösung für die Kongruenz $x^2 \equiv 1\ (2^{n+1})$. Als Lösungsansatz nehmen wir $L = x_0 + 2^{n-1} \cdot c$, wobei $c \in \{0, 1\}$ist. Nun setzen wir L in die Kongruenz $x^2 \equiv 1\ (2^{n+1})$ ein. Wir erhalten:

$$\begin{aligned} (x_0 + 2^{n-1} \cdot c)^2 &\equiv x_0^2 + 2^n \cdot x_0 \cdot c + 2^{2n-2} \cdot c^2 && (1) \\ &\equiv 1 + 2^n \cdot m + 2^n \cdot x_0 \cdot c + 2^{2n-2} \cdot c^2 && (2) \\ &\equiv 1 + 2^n \cdot (m + x_0 \cdot c) + 2^{2n-2} \cdot c^2 && (3) \end{aligned}$$

Anschließend wird die rechte Seite auf mod 2^{n+1} bezogen.Die Zahl $2^{2n-2} \cdot c^2$ fällt weg, da gilt :

$$\begin{aligned} 2n - 2 &\geq n + 1 \\ n &\geq 3 \end{aligned}$$

Es muss nun für die Klammer in Zeile (3), im mittleren Teil des Terms eine Fallunterscheidung für m gemacht werden. Falls m gerade sein sollte, kann

$c = 0$ gewählt werden. Somit würde auch der mittlere Teil aufgrund von mod 2^{n+1} wegfallen. Falls m ungerade sein sollte, kann $c = 1$ gewählt werden, s.d. $m + x_0$ gerade ist und wie zuvor wegfallen würde (Beachte: $x_0^2 \equiv 1\ (2^n)$ daraus folgt, dass x_0 ungerade ist). Die Zahl c nimmt somit eine regulatorische Rolle ein, s.d. der Rest 1 übrig bleibt in allen Fällen.

Wir müssen noch die Lösbarkeit der einzelnen Kongruenzen klären.
Fall 2: Sei $p \in Prim$ und $(a, p) = 1$. Wann sind $x^2 \equiv a\ (p^e)$ und $x^2 \equiv a\ (p^{e+1})$ lösbar? Konkreter stellt man sich die Frage wann $x^2 \equiv a\ (p)$ lösbar ist. Der Rest von a ist nach Voraussetzung in $\mathbb{Z}_p^{\cdot}$ enthalten. Es ist bekannt, dass $\mathbb{Z}_p$ ist ein Körper für $p \in Prim$ und dass ein Isomorphismus φ existiert, der von $(Z_p^*, \cdot)$ auf $(\mathbb{Z}_{p-1}, +)$ abbildet.

Behauptung: Sei p ungerade $\in$ Prim und $(a, p) = 1$. Dann ist $x^2 \equiv a\ (p)$ genau dann lösbar, wenn $a^{\frac{p-1}{2}} \equiv 1\ (p)$ gilt.

Beweis: Sei also ein x_0 gegeben mit $x_0^2 \equiv a\ (p)$. Da $(a, p) = 1$, gilt

$$\begin{aligned} a^{\frac{p-1}{2}} &\equiv (x_0^2)^{\frac{p-1}{2}} && (4)\\ &\equiv x_0^{p-1} && (5)\\ &\equiv 1\ (p) && (6) \end{aligned}$$

Die letzte Gleichung in Zeile (6) folgt, aus dem Satz von Lagrange und da $|\mathbb{Z}_p^*| = p - 1$ gilt.
Nun müssen wir untersuchen für welche $a \in \mathbb{Z}_{p-1}$, die Kongruenz $x^2 \equiv a\ (p)$ lösbar ist. Die Menge $\mathbb{Z}_{p-1} = \{0, 1, 2, 3, \ldots, p-2\}$ enthält alle möglichen Kandidaten für a die in $x^2 \equiv a\ (p)$ eingesetzt werden können. Bilden wir die Gleichung $a^{\frac{p-1}{2}} \equiv 1\ (p)$ mit der oben genannten Isomorphie φ auf $\mathbb{Z}_{p-1}$ ab, erhält man die Gleichung $0 = \frac{p-1}{2} \cdot \varphi(a)$. Setzt man für a jeden einzelnen möglichen Kandidaten nun ein, erhält man die Menge

$$\{0, \tfrac{p-1}{2}, p-1, p-1+\tfrac{p-1}{2}, 2(p-1), \ldots\}.$$

Diese Menge kann,aufgrund von mod $p - 1$ umgeschrieben werden als

$$\{0, \tfrac{p-1}{2}, 0, \tfrac{p-1}{2}, 0, \tfrac{p-1}{2} \ldots\}.$$

Jedes zweite Element ist Null und nur die a erfüllen die Gleichung $0 = \frac{p-1}{2} \cdot \varphi(a)$ in $\mathbb{Z}_{p-1}$, für die $\varphi(a)$ gerade ist. Dies ist sehr wichtig bei der Beantwortung der Frage für welche a, die Kongruenz $x^2 \equiv a\ (p)$ lösbar ist. Wir nutzen den

Isomorphismus φ ein weiteres Mal aus und bilden $x^2 \equiv a\ (p)$ auf $\mathbb{Z}_{p-1}$ ab. Man erhält die Gleichung $2x = \varphi(a)$. Diese ist lösbar für die oben genannten $\varphi(a)$,welche gerade sind. Somit ist $x^2 \equiv a\ (p)$ lösbar.

Bemerkung 1.4

Für den Fall $e = 1$, gilt a) ebenfalls. Als Voraussetzung gilt, dass $(a, m) = 1$, s.d. a ungerade und somit auch lösbar ist. Außerdem ist das Quadrat einer ungeraden Zahl, wieder ungerade.

Definition 1.5

Das Symbol $\left(\frac{a}{p}\right)$ wird Legendre Symbol genannt und erhält den Wert 1, falls a ein quadratischer Rest mod p ist. Im Fall, dass a ein quadratischer Nicht-Rest mod p ist erhält es den Wert -1. Falls $p \mid a$, gilt $\left(\frac{a}{p}\right) = 0$. Das Legendre Symbol ist eines der wichtigsten Werkzeuge, um quadratische Reste zu analysieren. In der folgenden Proposition werden wir einige seiner Vorteile darstellen.

Proposition 1.6

Sei $p \in Prim$ und $a \in \mathbb{Z}$. Dann gilt:

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

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

c) Falls $a \equiv b\ (p)$ gilt, so ist $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

Beweis

Falls $p \mid a$ oder $p \mid b$ gilt, sind alle drei Aussagen trivial. Das Legendre Symbol nimmt in diesem Fall den Wert 0 an. Im folgenden gelte $p \nmid a$ und $p \nmid b$.
Zu a): Wir wissen es gilt $a^{p-1} \equiv 1\ (p)$, daraus folgt:

$$(a^{\frac{p-1}{2}} + 1) \cdot (a^{\frac{p-1}{2}} - 1) \equiv a^{p-1} - 1 \equiv 0\ (p).$$

Dies impliziert, dass

$$a^{\frac{p-1}{2}} \equiv \pm 1\ (p) \text{ gilt.}$$

Nach Proposition 1.3 b) gilt $a^{\frac{p-1}{2}} \equiv 1\ (p)$, falls a quadratischer Rest mod p ist. Das heißt die Gleichheit für des Legendre Symbol $\left(\frac{a}{p}\right)$ (welches den Wert 1 annimmt, falls a quadratischer Rest mod p ist) mit $a^{\frac{p-1}{2}}$ ist wahr für a quadratischem Rest mod p. Falls $a^{\frac{p-1}{2}}$ nicht den Wert 1 beträgt, kann es nur gleich -1 sein, nach obiger Rechnung und a wäre ein quadratischer Nicht-Rest mod p. Gleichzeitig erhält das Legendre Symbol $\left(\frac{a}{p}\right)$ für dieses a und p auch den Wert -1. Die Behauptung aus a) wäre gezeigt.
Zu b): Es gilt nach a): $(ab)^{\frac{p-1}{2}} \equiv \left(\frac{ab}{p}\right)\ (p)$. Weiterhin gilt:

$$(ab)^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} \cdot b^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right), \text{ auch nach a).}$$

Somit ist

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

Zu c): Dieser Beweis folgt direkt aus der Definition des Legendre Symbols und der Kongruenz.

Korollar 1.7

Es existieren so viele quadratische Reste mod p, wie quadratische Nicht-Reste mod p.

Beweis

Sei $x^2 \equiv a\ (p)$ gegeben, wobei $a \in \mathbb{Z}$, $p \in Prim$. Nutzen wir den Isomorphismus aus dem Beweis von Proposition 1.3 und greifen die Argumentation aus dem genannten Beweis auf, sehen wir, dass nur die a (aus der Menge $\mathbb{Z}_{p-1} = \{0, 1, 2, 3, \ldots p-2\}$), die Gleichung $2x = \varphi(a)$ erfüllen für die $\varphi(a)$ gerade ist. Dies sind die Hälfte der Zahlen, der Menge $\mathbb{Z}_{p-1}$, welche eine gerade Anzahl von Elementen enthält, denn p ist ungerade und somit $p-1$ gerade. Die Anzahl der quadratischen Nicht-Reste mod p die für a in Frage kommen ist genau so groß wie die, der quadratischen Reste mod p.

Korollar 1.8

Sei $p \in Prim$.

(i) Das Produkt von zwei quadratischen Resten mod p ist ein quadratischer Rest mod p.

(ii) Das Produkt von zwei quadratischen Nicht-Resten mod p ist ein quadratischer Rest mod p.

(iii) Das Produkt eines quadratischen Rest mod p und einem quadratischen Nicht-Rest mod p ist ein quadratischer Nicht-Rest mod p.

Beweis

Seien $a, b \in \mathbb{Z}_p$. Wir nutzen für den Beweis die bereits gezeigte Eigenschaft aus Proposition 1.6 b) aus: $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$.

Zu i): Seien a und b zwei quadratische Reste mod p. Es gilt:

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

Also

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

Nach der Definition des *Legendre-Symbols* ist ab ein quadratischer Rest mod p.

Zu ii): Analog zum Beweis von i). Seien a und b zwei quadratische Nicht-Reste mod p. Es gilt:

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

Zu iii): Analog. Sei a ein quadratischer Rest mod p und b ein quadratischer Nicht-Rest mod p (Analog, falls a Nicht-Rest und b Rest ist). Es gilt:

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

Nach Legendre ist ab ein quadratischer Nicht-Rest mod p.

Korollar 1.9

Es gilt $(-1)^{\frac{p-1}{2}} = -1$. Das bedeutet, dass -1 genau dann ein quadratischer Rest mod p ist, wenn $p \equiv 1\ (4)$ gilt.

Beweis

Durch Substitution von $a = -1$ in Proposition 1.6 a) erhalten wir die gewünschte Gleichung.

Folgerungen zu Korollar 1.9

Es ist bekannt, dass ungerade Zahlen die Form $4k+1$ oder $4k+3$ haben können. So kann Korollar 1.9, wie folgt umformuliert werden :

$x^2 \equiv -1\ (p)$ hat genau dann eine Lösung, wenn p die Form $4k+1$ hat.

So ist -1 ein quadratischer Rest der Primzahlen $5, 13, 17, 29, \ldots$ und ein quadratischer Nicht-Rest der Primzahlen $3, 7, 11, 19, \ldots$. Mit Korollar 1.9 kann bewiesen werden, dass es unendlich viele Primzahlen der Form $4k+1$ gibt. Sei hier zu $\{p_1 \ldots p_m\}$ eine endliche Menge bestehend aus Primzahlen der Form $4k+1$. Man betrachte $(2p_1 \ldots p_m)^2 + 1$ und $p \in \mathbb{Z}$, für das gilt $p \mid (2p_1 \ldots p_m)^2 + 1$. Daraus folgt, dass -1 ein quadratischer Rest mod p ist, denn es gilt $(2p_1 \ldots p_m)^2 + 1 \equiv 0\ (p)$, da $p \mid a$.
Mit Korollar 1.9 folgt nun, dass p von der Form $4k+1$ sein muss. Jedoch ist $p \notin \{p_1 \ldots p_m\}$, da man den Rest 1 erhält, falls $(2p_1 \ldots p_m)^2 + 1$ durch p_i geteilt wird für alle $i \in \{1, \ldots m\}$. Da p jedoch $(2p_1 \ldots p_m)^2 + 1$ teilt, ist es nicht in der $\{p_1 \ldots p_m\}$ enthalten. So wird p, welches die Form $4k+1$ hat aus einer endlichen Menge von Primzahlen derselbigen Form ausgeschlossen. So existieren unendliche viele Primzahlen p, die ausgeschlossen werden aus solchen Mengen.

Definition 1.10

Definiere die Menge $S = \{-\frac{p-1}{2}, -\frac{p-3}{2}, \ldots, -1, 1, 2, \ldots \frac{p-1}{2}\}$. Sei μ die Anzahl an negativen Resten aus S, der ganzzahligen Zahlen $a, 2a, 3a, \ldots, \frac{p-1}{2}\ a$, falls gilt $p \nmid a$.

Lemma 1.11 (Gauß-Lemma)

Das *Gauß-Lemma* besagt, dass

$$\left(\frac{a}{p}\right) = (-1)^{\mu} \text{ gilt.}$$

Gauß definiert das *Legendre-Symbol* mithilfe von μ.

Beweis

Sei $\pm m_\ell$ der kleinste Rest von $\ell \cdot a \bmod p$, wobei $m_\ell \geqslant 0$ und $\ell \in \{1, \ldots, \frac{p-1}{2}\}$. Sei m_k analog für $k \cdot a$ definiert. Man behauptet $m_\ell \neq m_k$, falls $\ell \neq k$ ist.
Wir nehmen an, dass $m_\ell = m_k$ gilt. Dann ist $\ell \cdot a \equiv \pm k \cdot a\ (p)$. Außerdem impliziert $p \nmid a$, dass $\ell \pm k \equiv 0\ (p)$ gilt. Diese Kongruenz kann aber nicht auftreten, da $\ell \neq k$ ist und $|\ell \pm k| \ < \ |\ell| + |k| \ < \ p - 1$. Es folgt, dass

die Mengen $\{1, 2, \ldots \frac{p-1}{2}\}$ und $\{m_1, \ldots m_{\frac{p-1}{2}}\}$ identisch sind (Beachte: Man bildet ℓ auf m_ℓ ab, wobei beide Elemente aus der Menge $\{1, 2, \ldots, \frac{p-1}{2}\}$ stammen). Wir multiplizieren nun die Kongruenzen

$$\begin{aligned} 1 \cdot a &\equiv \pm m_1 \ (p), \\ &\vdots \\ \frac{p-1}{2} \cdot a &\equiv \pm m_{\frac{p-1}{2}} \ (p) \end{aligned}$$

miteinander und erhalten die Gleichung

$$\tfrac{p-1}{2}! \cdot a^{\frac{p-1}{2}} \equiv (-1)^\mu \cdot \tfrac{p-1}{2}! \ (p).$$

Daraus folgt

$$a^{\frac{p-1}{2}} \equiv (-1)^\mu \ (p).$$

Außerdem gilt nach Proposition 1.6 a) $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \ (p)$. Damit ist die Gleichheit des Legendre Symbols $\left(\frac{a}{p}\right)$ mit $(-1)^\mu$ bewiesen.

Proposition 1.12

Die Zahl 2 ist ein quadratischer Rest mod p, falls p der Form $8k + 1$ oder $8k+7$ angehört. Falls p die Form $8k+3$ oder $8k+5$ hat ist 2 ein quadratischer Nicht-Rest mod p. Zusammengefasst heißt das:

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

Also ist 2 genau dann ein quadratischer Nicht-Rest mod p, wenn
$p \equiv \pm 1 \ (8)$ gilt.

Beweis

Es kann leicht nachgewiesen werden, dass die beiden Aussagen der Proposition 1.12 äquivalent sind zur Formel $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$. Beispielsweise, wählt man für p, eine Primzahl der Form $8k + 7$ und setzt dieses p in die Potenz $\frac{p^2-1}{8}$ (von (-1)) aus der obigen Formel ein. So erhält man:

$$\tfrac{(8k+7)^2-1}{8} = \tfrac{64k^2+112k+49-1}{8} = 8k^2 + 14k + 6.$$

Letzteres ist *gerade*, so dass gilt $(-1)^{\frac{p^2-1}{8}} = 1$ für $p = 8k+7$, also $\left(\frac{2}{p}\right) = 1$. Für die anderen Formen, die p annehmen kann erfolgt die Rechnung analog.

Sei nun p ungerade Primzahl und μ wie in Definition 1.10 definiert. Als Hilfe für die Berechnung von μ setzen wir ein m voraus, welches folgende Bedingungen erfüllen soll:

(1) $2m \leqslant \frac{p-1}{2}$,

(2) $2(m+1) > \frac{p-1}{2}$.

Daraus folgt:

$$\mu = \tfrac{p-1}{2} - m.$$

Erinnerung: μ ist die Anzahl an negativen Resten, der ganzzahligen Zahlen $a, 2a, 3a, \ldots, \frac{p-1}{2} \cdot a$. Also betrachte die Menge

$$\{2 \cdot 1, 2 \cdot 2, \ldots, 2 \cdot \tfrac{p-1}{2}\},$$

denn in Proposition 1.12 ist $a = 2$. Darüber hinaus geht die Menge über $\frac{p-1}{2}$, wie man sieht. Im folgenden werden wir eine Fallunterscheidung für jede einzelne der oben genannten Formen, die p annehmen kann machen.

Fall 1: Sei $p = 8k+1$.
Wir erhalten durch umformen

$$p - 1 = 8k \Leftrightarrow \tfrac{p-1}{2} = 4k.$$

Wegen den beiden Bedingungen die m erfüllen muss, gilt $m = 2k$. Somit ist

$$\mu = \tfrac{p-1}{2} - m \Leftrightarrow \mu = 4k - 2k \Leftrightarrow \mu = 2k.$$

$\mu = 2k$ ist gerade und daraus folgt $\left(\frac{2}{p}\right) = 1$.

Fall 2: Sei $p = 8k+7$. Analog zu Fall 1.

$$p - 1 = 8k + 6 \Leftrightarrow \tfrac{p-1}{2} = 4k + 3.$$

Mit den Bedingungen 1) und 2) für m, folgt $m = 2k+1$. Also gilt

$$\mu = 4k + 3 - (2k+1) \Leftrightarrow \mu = 2k + 2.$$

μ ist wie in Fall 1 gerade. Somit ist $\left(\frac{2}{p}\right) = 1$.

Allgemein sucht man für m den Wert, ab den man negative Reste erhält. Dabei orientiert man sich an der Menge $\{1, 2, \ldots, \frac{p-1}{2}\}$ und kann sich als Anhaltspunkt, das Element in der Mitte, der Menge aussuchen (im Fall 2 ist es $2k + 2$). Da jede Zahl nach Definition 1.10 mit a multipliziert wird, multipliziert man $2k + 1$ mit 2. Man erhält $4k + 2$. Dies ist kleiner als $\frac{p-1}{2} = 4k + 3$. Als nächstes wählt man die nächst größere Zahl, welche $2k + 2$ ist und multipliziert diese mit 2. So erhält man $4k + 4$ was nun größer ist als $\frac{p-1}{2} = 4k + 3$. Auf diese Art findet man die *kritische Stelle*, ab der man negative Reste erhält. Die Differenz aus $\frac{p-1}{2}$ mit der kritischen Stelle gibt uns μ.

Fall 3: Sei $p = 8k + 3$.
$p - 1 = 8k + 2 \Leftrightarrow \frac{p-1}{2} = 4k + 1$. So erhält man $m = 2k$ und $\mu = 2k + 1$.
Da μ ungerade ist und folgt $\left(\frac{2}{p}\right) = (-1)$.

Fall 4: Sei $p = 8k + 5$. Es folgt $\frac{p-1}{2} = 4k + 2$ und $m = 2k + 1$.
Dann ist $\mu = 2k + 1$. Wie in Fall 3 gilt, $\left(\frac{2}{p}\right) = (-1)$.

Folgerungen zu Proposition 1.12

Ähnlich wie in den Folgerungen zu Korollar 1.9, können wir mithilfe von Proposition 1.12 zeigen, dass es unendlich viele Primzahlen der Form $8k + 7$ gibt. Wir nehmen an, dass $\{p_1, \ldots, p_m\}$ eine endliche Menge aus Primzahlen, der Form $8k + 7$ sei. Man betrachte $(4p_1p_2 \ldots p_m)^2 - 2$. Der ungerade Primzahlen-Divisor, dieser Zahl hat die Form $8k+1$ oder $8k+7$, da für solche Prim-Divisoren 2 ein quadratischer Rest mod p ist (nach Proposition 1.12).
Genauer: Sei p ungerade Primzahl, die $(4p_1p_2 \ldots p_m)^2 - 2$ teilt, dann gilt
$(4p_1p_2 \ldots p_m)^2 - 2 \equiv 0\ (p) \Leftrightarrow (4p_1p_2 \ldots p_m)^2 \equiv 2\ (p)$.
Daraus folgt die Behauptung, dass 2 ein quadratischer Rest mod p ist für solche Prim-Divisoren.
Nun sei p Prim-Divisor der Form $8k + 7$. Dann ist $p \notin \{p_1, \ldots, p_m\}$, denn es gilt $p_i \nmid ((4p_1p_2 \ldots p_m)^2 - 2)$ für alle $i \in \{1, \ldots, m\}$.

2 Das Gesetz der quadratischen Reziprozität

Proposition 2.1

Seien p und q ungerade Primzahlen. Dann gelten:

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

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

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

Beweis

Der Beweis wird in kommenden Vorträgen zum Kapitel 6 behandelt. a) und b) wurden bereits im ersten Abschnitt, dieser Ausarbeitung gezeigt.

Beispiel 2.2

Berechne $\left(\frac{79}{101}\right)$.
Es gilt $101 \equiv 1\ (4)$ und $101 \equiv 22\ (79)$.
Daraus folgt:

$$\left(\tfrac{79}{101}\right) = \left(\tfrac{101}{79}\right) = \left(\tfrac{22}{79}\right).$$

Die erste Umformung folgt aus Proposition 2.1 c). Somit haben wir das eigentliche *Legendre-Symbol* $\left(\frac{79}{101}\right)$ minimiert auf $\left(\frac{22}{79}\right)$. Mit Proposition 1.6 b) können wir $\left(\frac{22}{79}\right)$ umschreiben als

$$\left(\tfrac{2}{79}\right) \cdot \left(\tfrac{11}{79}\right) = \left(\tfrac{22}{79}\right).$$

Wir berechnen jetzt die beiden *Legendre-Symbole*, um das Ergebnis von $\left(\frac{22}{79}\right)$ beziehungsweise $\left(\frac{79}{101}\right)$ zu erhalten.
Aus $79 \equiv 7\ (8)$ folgt, dass$\left(\frac{2}{79}\right) = 1$ ist nach Proposition 1.12. Da 11 und 79 beide kongruent zu 3 mod 4 sind, gilt:

$$\left(\tfrac{11}{79}\right) = -\left(\tfrac{79}{11}\right) = -\left(\tfrac{2}{11}\right).$$

Anschließend liefert uns $11 \equiv 3\ (8)$, dass $\left(\frac{2}{11}\right) = (-1)$ ist (auch nach Prop. 1.12). Also $\left(\frac{11}{79}\right) = -\left(\frac{2}{11}\right) = -(-1) = 1$. Zusammengefasst heißt das

$$\left(\tfrac{79}{101}\right) = \left(\tfrac{22}{79}\right) = \left(\tfrac{2}{79}\right) \cdot \left(\tfrac{11}{79}\right) = 1 \cdot 1 = 1.$$

79 ist ein quadratischer Rest mod 101 nach der Definition des *Legendre-Symbols*.

Definition 2.3

Das *Jacobi-Symbol* ist eine Erweiterung, des *Legendre-Symbols* $\left(\frac{a}{p}\right)$.
Sei b ungerade positive ganze Zahl und $a \in \mathbb{Z}$. Darüber hinaus sei
$b = p_1 \dots p_m$ eine Zerlegung von b. Dann wird

$$\left(\tfrac{a}{b}\right) = \left(\tfrac{a}{p_1}\right) \cdot \left(\tfrac{a}{p_2}\right) \cdot \left(\tfrac{a}{p_3}\right) \cdot \dots \cdot \left(\tfrac{a}{p_m}\right)$$

als *Jacobi-Symbol* bezeichnet.

Bemerkung 2.4

Das *Jacobi-Symbol* besitzt ähnliche Vorteile, wie das *Legendre-Symbol*. Wichtig ist zu erwähnen: $\left(\frac{a}{b}\right)$ kann den Wert 1 annehmen (nach der Definition des *Jacobi-Symbols*) ohne dass die Bedingung erfüllt sein muss, dass a quadratischer Rest mod b ist. Ein kurzes Beispiel hierfür ist $\left(\frac{2}{15}\right)$.
Mithilfe von Proposition 1.6 b) gilt:

$$\left(\tfrac{2}{15}\right) = \left(\tfrac{2}{3}\right) \cdot \left(\tfrac{2}{5}\right) = (-1) \cdot (-1) = 1.$$

$\left(\frac{2}{15}\right)$ nimmt den Wert 1 an, obwohl 2 ein quadratischer Nicht-Rest mod 15 ist.

Proposition 2.5

Seien $a, a_1, a_2 \in \mathbb{Z}$ und b, b_1, b_2 ungerade positive ganze Zahlen. Dann gilt:

a) $\left(\frac{a_1}{b}\right) = \left(\frac{a_2}{b}\right)$, falls $a_1 \equiv a_2 \ (b)$.

b) $\left(\frac{a_1 \cdot a_2}{b}\right) = \left(\frac{a_1}{b}\right) \cdot \left(\frac{a_2}{b}\right)$.

c) $\left(\frac{a}{b_1 \cdot b_2}\right) = \left(\frac{a}{b_1}\right) \cdot \left(\frac{a}{b_2}\right)$.

Beweis

a) und b) folgen unmittelbar aus den Vorteilen des *Legendre- Symbols*. c) folgt aus der Definition 2.3.

Proposition 2.6

a) $\left(\frac{-1}{b}\right) = (-1)^{\frac{b-1}{2}}$.

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

c) Falls a ungerade positive Zahl, wie b sein sollte , gilt $\left(\frac{a}{b}\right) \cdot \left(\frac{b}{a}\right) = (-1)^{\frac{a-1}{2} \cdot \frac{b-1}{2}}$.

Proposition 2.7

Sei a nicht quadratische ganze Zahl. Dann existieren unendlich viele Primzahlen p, so dass a ein quadratischer Nicht-Rest mod p ist.

Beweis

Wir nehmen an, dass a *quadrat-frei* ist und $a = 2^e q_1 \dots q_n$ Primfaktorzerlegung von a ist, wobei $e \in \{0, 1\}$.
Fall 1 : Sei $a = 2$.
Sei $\{\ell_1, \dots, \ell_m\}$ endliche Menge von Primzahlen, wobei die 3 nicht enthalten sein soll und für alle $i \in \{1, \dots, m\}$ gilt $\left(\frac{2}{\ell_i}\right) = (-1)$.
Da $b \equiv 3\ (8)$ gilt, erhalten wir

$$\left(\frac{2}{b}\right) = (-1)^{\frac{b^2-1}{8}} = (-1) \text{ nach Proposition 1.12.}$$

Sei $b = p_1 \cdot \dots \cdot p_m$ die Primfaktorzerlegung von b. So kann $\left(\frac{2}{b}\right)$ mithilfe der Definition 2.3 (nach *Jacobi*):

$$\left(\frac{a}{p}\right) = \left(\frac{a}{p_1}\right) \cdot \left(\frac{a}{p_2}\right) \cdot \left(\frac{a}{p_3}\right) \cdot \dots \cdot \left(\frac{a}{p_m}\right)$$

umgeschrieben werden als:

$$\left(\frac{2}{b}\right) = \left(\frac{2}{p_1}\right) \cdot \left(\frac{2}{p_2}\right) \cdot \left(\frac{2}{p_3}\right) \cdot \dots \cdot \left(\frac{2}{p_m}\right)$$

Das impliziert

$$\left(\frac{2}{p_i}\right) = (-1) \text{ für einige } i \in \{1, \dots, m\}.$$

Somit sind die $p_i \notin \{3, \ell_1, \ldots, \ell_m\}$.

Fall 2: Sei $a = 2^e \cdot q_1 \cdot \cdots \cdot q_n$ $(n \geqslant 1)$ und teilbar durch eine ungerade Primzahl. Sei $\{\ell_1, \ldots, \ell_k\}$ eine endliche Menge ungerader Primzahlen, welche die q_i für $i \in \{1, \ldots, \ell\}$ nicht enthält. Zusätzlich setzt man ein s voraus, welches ein quadratischer Nicht-Rest mod q_n ist. Nun versuchen wir eine Lösung für das folgende System aus Kongruenzen zu finden :

$$\begin{cases} x \equiv 1 \ (l_i) \\ x \equiv 1 \ (8) \\ x \equiv 1 \ (q_i) \\ x \equiv s \ (q_n). \end{cases}$$

Nach dem *chinesischen Rest Satz Theorem* existiert eine Lösung für dieses System. Wir bezeichnen die Lösung mit b. Die Zahl b ist ungerade und habe die Primfaktorzerlegung $b = p_1 \cdot \cdots \cdot p_m$. Da b das obige System löst, gilt $b \equiv 1 \ (8)$. Daraus folgt

$$\left(\tfrac{2}{b}\right) = 1 \text{ und } \left(\tfrac{q_i}{b}\right) = \left(\tfrac{b}{q_i}\right) \text{ mit Proposition 2.6.}$$

Beziehen wir dies auf Proposition 2.5 b), so gilt:

$$\begin{aligned} \left(\frac{a}{b}\right) &= \left(\frac{2}{b}\right)^e \cdot \left(\frac{q_1}{b}\right) \cdot \cdots \cdot \left(\frac{q_{n-1}}{b}\right) && (7) \\ &= \left(\frac{b}{q_1}\right) \cdot \cdots \cdot \left(\frac{b}{q_{n-1}}\right) \cdot \left(\frac{b}{q_n}\right) && (8) \\ &= \left(\frac{1}{q_1}\right) \cdot \cdots \cdot \left(\frac{1}{q_{n-1}}\right) \cdot \left(\frac{s}{q_n}\right) && (9) \\ &= (-1). && (10) \end{aligned}$$

In Zeile (9) nimmt $\left(\frac{s}{q_n}\right)$ nach unserer Konstruktion den Wert -1 an und die restlichen Klammern den Wert 1. Letzteres gilt, da b das Kongruenz System löst welches $x \equiv 1 \ (p_i)$ enthält. Also gilt:

$$\left(\tfrac{a}{b}\right) = (-1).$$

Mit der Definition 2.3 von $\left(\frac{a}{b}\right)$ folgt, dass $\left(\frac{a}{p_i}\right) = (-1)$ ist für einige i $\in \{1, \ldots, m\}$. Weiterhin gilt, $b \nmid \ell_j$, da b die Kongruenz $x \equiv 1\ (\ell_j)$ löst. Daraus folgt, dass

$$p_i \notin \{\ell_1, \ldots, \ell_k\}.$$

Zusammengefasst bedeutet das: Wenn a quadratischer Nicht-Rest mod p und teilbar durch ungerade Primzahlen ist, findet man eine Primzahl p außerhalb einer gegebenen endlichen Menge von Primzahlen $\{2, \ell_1, \ldots, \ell_k\}$, so dass gilt $\left(\frac{a}{p}\right) = (-1)$.