

# Quadratische Reste und das quadratische Reziprozitätsgesetz

Alexander Hölzle

03.04.2007

# Inhaltsverzeichnis

|            |  |           |
|------------|--|-----------|
| <b>I</b>   | <b>Motivation und Überblick</b>                                    | <b>3</b>  |
| <b>II</b>  | <b>Quadratische Reste</b>  | <b>4</b>  |
| 1          | Grundlegendes und Beispiele . . . . .                              | 4         |
| 2          | Quadratische Reste modulo Primzahlpotenzen . . . . .               | 8         |
| 2.1        | Gerade Primzahlpotenzen . . . . .                                  | 8         |
| 2.2        | Ungerade Primzahlpotenzen . . . . .                                | 9         |
| 3          | Kriterium von Euler und das Legendre-Symbol . . . . .              | 11        |
| <b>III</b> | <b>Das Reziprozitätsgesetz</b>                                     | <b>14</b> |
| 1          | Das Gaußsche Lemma . . . . .                                       | 14        |
| 2          | Ergänzungssätze und das quadratische Reziprozitätsgesetz . . . . . | 19        |
| 3          | Der Beweis . . . . .   | 21        |
| <b>IV</b>  | <b>Jacobi-Symbol</b>   | <b>24</b> |

# I. Motivation, Überblick und Notation

Ein Schmuckstück der elementaren Zahlentheorie ist die Theorie der quadratischen Reste, welche den hauptsächlichsten Anlass zur Entwicklung der höheren Zahlentheorie gegeben hat. In diesem Dokument werden wir die Grundlagen dieser Theorie elementar vermitteln, d.h. es sind Kenntnisse über algebraische Konstrukte und zahlentheoretische Funktionen (wie die Eulersche  $\phi$ -Funktion) für das Verstehen hilfreich.

Zunächst werden wir die so genannten Legendre- und Jacobisymbole definieren und näher untersuchen. Im Anschluss daran beweisen wir einige grundlegende Sätze, wie z.B. das Eulersche Kriterium oder das Gaußsche Lemma. Der Höhepunkt dieses Dokuments und der elementaren Zahlentheorie ist das quadratische Reziprozitätsgesetz, welches GAUSS in seiner *Disquisitiones* erstmals bewies. GAUSS selbst hat acht Beweise des Reziprozitätsgesetzes für quadratische Reste angegeben, von denen sechs auf voneinander gänzlich verschiedenen Ideen fußen. Wir werden uns mit einem sehr anschaulichen Beweis begnügen.

## II. Quadratische Reste

### 1. Grundlegendes und Beispiele

Bevor wir uns den quadratischen Resten zuwenden eine Bemerkung zur Notation.

Mit  $\mathbb{N} = \{1, 2, \dots\}$  bezeichnen wir die Menge der natürlichen Zahlen (ohne die Null). Das Symbol  $\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$  repräsentiert die Menge der ganzen Zahlen und  $(\mathbb{Z}/n\mathbb{Z}) = \mathbb{Z}_n$ ,  $n \in \mathbb{N}$ , den Restklassenring der ganzen Zahlen. Wie wir wissen besteht der Restklassenring aus einer Menge von Äquivalenzklassen und für  $n > 1$  gilt  $\mathbb{Z}_n = \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}$ , wobei  $\bar{r} = \{r + n \cdot z | z \in \mathbb{Z}\}$ ,  $0 \leq r \leq n - 1$  eine Restklasse (bzw. Nebenklasse) repräsentiert. Sind zwei ganze Zahlen  $a, b \in \mathbb{Z}$  kongruent modulo  $n$ , so notieren wir dies kurz durch  $a \equiv_n b$ ,  $a \equiv b \pmod{n}$  oder  $a \equiv b(n)$ . Die Einheitengruppe des Restklassenringes bezeichnen wir mit  $\mathbb{Z}_n^*$ .

Weiterhin bezeichne  $\phi : \mathbb{N}^\times \rightarrow \mathbb{N}^\times$  die Eulersche  $\phi$ -Funktion (oft auch  $\varphi$ ). Der Funktionswert  $\phi(n)$  gibt die Anzahl der positiven natürlichen zu  $n$  teilerfremden Zahlen kleiner  $n$  an. Die Eulersche  $\phi$ -Funktion ist multiplikativ. Aufgrund des Hauptsatzes der elementaren Zahlentheorie impliziert dies, dass  $\phi(n)$  bereits vollständig beschrieben ist, wenn die Funktionswerte für alle Primzahlpotenzen  $p^m$  bekannt sind. Weiterhin gelten für Primzahlen  $p$  folgende Identitäten

$$\phi(p) = p - 1, \tag{II.1}$$

$$\phi(p^m) = p^m - p^{m-1} = p^{m-1}(p - 1). \tag{II.2}$$

Die Gleichung (2.1) gilt, da Primzahlen in  $\mathbb{N}^\times$  nur die trivialen Teiler 1 und  $p$  besitzen und damit für  $(p - 1)$  Zahlen  $a \leq p$  die Gleichung  $ggT(a, p) = 1$  gilt. Eine Primpotenz  $p^m$  mit  $m \in \mathbb{Z}$  ist zu den Vielfachen von  $p$  nicht teilerfremd. Die Zahlen  $\underbrace{p, 2 \cdot p, 3 \cdot p, \dots, p^{m-1} \cdot p}_{p^{m-1} \text{ Stück}}$  haben mit  $p^m$  den größten gemeinsamen Teiler  $p$ .

**1.1 Definition:** Sei  $n \in \mathbb{N}, n > 1$  vorgegeben. Eine zu  $n$  teilerfremde Zahl  $a \in \mathbb{Z}_n^*$  heißt **quadratischer Rest** modulo  $n$ , wenn ein  $x \in \mathbb{Z}$  existiert, so dass  $x^2 \equiv_n a$ .

Zwei modulo  $n$  quadratische Reste  $a, a' \in \mathbb{Z}$  heißen **verschieden**, wenn gilt  $a \not\equiv_n a'$ . Eine zu  $n$  teilerfremde Zahl  $a$  heißt **quadratischer Nichtrest** modulo  $n$ , wenn  $a$  kein quadratischer Rest modulo  $n$  ist.

Anstatt „quadratischer Rest modulo  $n$ “ sagt man auch „quadratischer Rest nach  $n$ “.

**1.2 Beispiel:** Sei  $n := 9$ , dann sind 1, 4, 7 verschiedene quadratische Reste modulo 9. Der naive Weg ist alle Elemente aus  $(\mathbb{Z}/9\mathbb{Z})^*$  zu berechnen. Gemäß Definition kommen

für quadratische Reste nur die zu  $n = 9$  teulfremden Zahlen kleiner 9 in Frage. Insgesamt existieren davon  $\phi(9) = 6$  Stück und im einzelnen sind dies: 1, 2, 4, 5, 7, 8. Entsprechend berechnen wir die Quadrate:

$$\begin{array}{ll} 1^2 \equiv_9 1, & 2^2 \equiv_9 4 \\ 4^2 \equiv_9 7, & 5^2 \equiv_9 7 \\ 7^2 \equiv_9 7, & 8^2 \equiv_9 1. \end{array}$$

Wir sehen, dass 1,4 und 7 quadratische Reste, dagegen 2,5 und 8 quadratische Nichtreste sind.

Das Problem, bei gegebenem Modul  $n > 1$  alle quadratischen Reste (bzw. Nichtreste) zu bestimmen, ist unser erstes Ziel. Zunächst werden wir dieses Problem für spezielle Moduln lösen, denn oftmals reicht es quadratische Reste modulo  $p$ ,  $p$  eine Primzahl, zu betrachten. Für eine Primzahl  $p$  ist  $a \in \mathbb{Z}_p^*$  genau dann ein quadratischer Rest modulus  $p$ , wenn ein  $x \in \mathbb{Z}$  existiert, so dass die Kongruenz  $x^2 \equiv_p a$  lösbar ist. Man erinnere sich, dass die Einheitengruppe von  $\mathbb{Z}_p$  genau  $\phi(p) = p - 1$  Elemente besitzt und eine besondere Form besitzt:

$$\mathbb{Z}_p^* = \{\overline{0}, \overline{1}, \dots, \overline{p-1}\}$$

Zunächst stellen wir uns die Frage nach der Anzahl der quadratischen Reste:

*Wieviele  $a \in \mathbb{Z}_p^*$  sind Quadratwurzeln, also von der Form  $a = b^2 \pmod p$  für ein  $b \in \mathbb{Z}_p^*$ ?*

Eine Antwort auf diese Frage gibt folgendes

**1.3 Lemma:** Sei  $p > 2$  eine Primzahl. Dann sind die Hälfte der Elemente in  $\mathbb{Z}_p^*$  quadratische Reste, und die andere Hälfte sind quadratische Nichtreste modulo  $p$ .

*Beweis.* Sei  $g$  ein primitives Element von  $(\mathbb{Z}/p\mathbb{Z})^*$ , dann ist  $a = g^j \pmod p$  eine Quadratzahl genau dann, wenn  $j \in \mathbb{Z}$  gerade ist:

„ $\Rightarrow$ “: Ist nämlich  $j \in \mathbb{Z}$  gerade, d.h.  $j = 2k$  für ein  $k \in \mathbb{Z}$ , dann gilt  $a \equiv_p g^j \equiv_p (g^k)^2 \equiv_p g^{2k}$ , also eine Quadratzahl.

„ $\Leftarrow$ “: Ist andererseits  $a$  eine Quadratzahl, also  $a = b^2 \pmod p$  mit  $b \in (\mathbb{Z}/p\mathbb{Z})^*$ , dann gilt  $b = g^k \pmod p$  für ein  $k \in \mathbb{Z}$ , und  $a \equiv_p b^2 \equiv_p (g^k)^2 \equiv_p g^{2k}$ , also ist  $a = g^j \pmod p$  für ein  $k \in \mathbb{Z}$ .

Da  $p$  nach Voraussetzungen stets eine ungerade Primzahl ist, folgt damit unmittelbar, dass die Hälfte, also insgesamt  $\frac{p-1}{2}$  der Elemente aus  $(\mathbb{Z}/p\mathbb{Z})^*$  quadratische Reste sind. Dies sind gerade die Elemente, welche sich mit Hilfe eines primitiven Elements  $g$  und geradem Exponenten  $j = 2k$  darstellen lassen. □

Wir haben also festgestellt, dass mit obiger Notation  $g^1, g^3, \dots, g^{p-2}$  quadratische Nichtreste und  $g^2, g^4, \dots, g^{p-1}$  quadratische Reste  $\pmod p$ ,  $p$  prim, sind. Insbesondere ist also eine primitive Restklasse kein Quadrat - ansonsten würde obiges Lemma seine Gültigkeit verlieren, was nicht sein kann.

Jede ungerade Zahl  $2k + 1 \in \mathbb{Z}$  ist ein quadratischer Rest modulo 2, da  $1^2 \equiv_2 2k + 1$ . Für weitere Überlegungen dürfen wir also für den Moduln  $n \geq 3$  annehmen. Sodann ist  $\phi(n)$  stets gerade, da  $\phi(n) = \prod_{i=1}^r \phi(p_i^{m_i}) = \prod_{i=1}^r \phi(p^{m_i-1}(p-1))$  wobei  $n = \prod_{i=1}^r p_i^{m_i}$  die (bis auf die Reihenfolge und Assoziiertheit) eindeutige Primzerlegung von  $n$  ist.

**1.4 Satz:** Es sei  $n \geq 3$  und es sei die prime Restklassengruppe  $\mathbb{Z}_n^*$  zyklisch; es sei  $g \in \mathbb{Z}$  eine Primitivwurzel (Erzeuger) zu  $n$ . Man setze  $s := \frac{1}{2} \cdot \phi(n)$ . Dann sind

- $1, g^2, g^4, \dots, g^{2s-2}$  verschiedene quadratische Reste und
- $g, g^3, g^5, \dots, g^{2s-1}$  verschiedene quadratische Nichtreste

modulo  $n$ . Insbesondere gibt es genau  $\frac{1}{2} \cdot \phi(n)$  verschiedene quadratische Reste und ebenso viele quadratische Nichtreste modulo  $n$ .

*Beweis.* Nach Voraussetzung gilt  $\langle g \rangle = \{g^k | k \in \mathbb{Z}\} = \mathbb{Z}_n^*$  wobei  $\bar{g}$  die Restklasse des erzeugenden Elements bezeichnen soll. Da

$$\bar{1} = (\bar{g}^0)^2, \bar{g}^2 = (\bar{g}^1)^2, \bar{g}^4 = (\bar{g}^2)^2, \dots, \bar{g}^{2s-2} = (\bar{g}^{s-1})^2$$

Quadrate in  $\mathbb{Z}_n^*$  und paarweise verschieden sind, so ist klar, dass die  $s$  Zahlen  $1, \bar{g}^2, \bar{g}^4, \dots, \bar{g}^{2s-2}$  verschiedene quadratische Reste modulo  $n$  sind.

Würde ein  $k \in \mathbb{Z}$  eine Gleichung  $\bar{b}^2 = \bar{c}^{2k+1}$  mit  $\bar{b} \in \mathbb{Z}_n^*$  bestehen, so müsste, da  $\bar{g}$  die Einheitengruppe  $\mathbb{Z}_n^*$  und damit  $\bar{b}$  erzeugt, die Gestalt  $\bar{b} = \bar{g}^l$  für ein  $l \in \mathbb{Z}$  besitzen. Und damit müsste dann gelten:

$$\begin{aligned} \bar{b}^2 &= (\bar{g}^l)^2 = \bar{g}^{2l}, \\ \Rightarrow \bar{g}^{2(k-l)+1} &= \bar{1}. \end{aligned}$$

Dies hat wegen  $ord(\bar{g}) = ord(\mathbb{Z}_n^*) = \phi(n)$  zur Folge  $\phi(n) | 2(k-l)+1$ , was nach dem oben Bemerkten unmöglich ist, da  $\phi(n)$  für  $n \geq 3$  gerade ist. Die  $s = \frac{1}{2} \cdot \phi(n)$  verschiedenen Restklassen  $g, g^3, g^5, \dots, g^{2s-1}$  sind also verschiedene quadratische Nichtreste modulo  $n$ .

Da die Gruppe  $\mathbb{Z}_n^*$  aus  $\phi(n) = 2s$  Elementen besteht, so ist klar, dass die angegebenen quadratischen Reste bzw. Nichtreste bereits alle quadratischen Reste bzw. Nichtreste modulo  $n$  sind. Insbesondere gibt es also  $s$  verschiedene quadratische Reste und ebenso viele quadratische Nichtreste modulo  $n$ . □

**1.5 Beispiel:** Die Aussage des Satzes ist falsch, wenn  $\mathbb{Z}_n^*$  nicht zyklisch ist. Um dies einzusehen sei  $n := 8$ , d.h. wir betrachten die quadratischen Reste modulo 8. Eine Zahl

$a \in \mathbb{Z}$  ist genau dann ein quadratischer Rest modulo 8, wenn  $a \equiv_8 1$ . Es gibt also nur einen quadratischen Rest modulo 8, aber 3 verschiedene quadratische Nichtreste modulo 8. Zum Beweis dieser Behauptung rechnet man einfach nach. Es ist  $\phi(8) = 4$  mit den primen Restklassen  $\bar{1}, \bar{3}, \bar{5}, \bar{7} \in \mathbb{Z}_8^*$ . Die Behauptung folgt dann aus

$$\bar{1}^2 = \bar{3}^2 = \bar{5}^2 = \bar{7}^2 = \bar{1}.$$

Die Frage, wann eine Zahl  $a \in \mathbb{Z}$  ein quadratischer Rest modulo  $n$  ist, kann durch folgenden Satz auf eine etwas einfachere Frage reduziert werden. Um den folgenden Satz beweisen zu können benötigen wir folgendes

**1.6 Lemma:** Es seien  $n_1, n_2 \in \mathbb{Z}$  und  $v := \text{kgV}(n_1, n_2)$ . Dann gilt:

$$a \equiv_{n_1} b \quad \text{und} \quad a \equiv_{n_2} b \Leftrightarrow a \equiv_v b.$$

Sind speziell  $n_1$  und  $n_2$  teilerfremd, so gilt:

$$a \equiv_{n_1} b \quad \text{und} \quad a \equiv_{n_2} b \Leftrightarrow a \equiv_{n_1 n_2} b.$$

*Beweis.* Wegen  $n_1|v, n_2|v$  ist die Implikation „ $\Leftarrow$ “ trivial, da für  $n \in \mathbb{N}$  die Äquivalenz  $a \equiv_n b \Leftrightarrow n|a-b$  gilt.

„ $\Rightarrow$ “ Die Voraussetzungen besagen  $n_1|(a-b)$  und  $n_2|(a-b)$ . Nach Definition des kleinsten gemeinsamen Vielfachen folgt daraus  $v|(a-b) \Leftrightarrow a \equiv_v b$ . Da  $v = |n_1 n_2|$  im Falle  $\text{ggT}(n_1, n_2) = 1$  gilt ist damit das Lemma bewiesen.  $\square$

Nun die **Problemreduktion** auf teilerfremde Faktoren.

**1.7 Satz:** Es sei  $n \geq 2$  und es sei  $n = n_1 n_2 \cdot \dots \cdot n_r$  eine Faktorisierung von  $n$  in endlich viele natürliche Zahlen  $n_i \geq 2$  derart, dass für alle  $i, j \in \{1, 2, \dots, r\}$  mit  $i \neq j$  gilt:  $\text{ggT}(n_i, n_j) = 1$ . Dann sind folgende Aussagen über eine Zahl  $a \in \mathbb{Z}$  äquivalent:

- i)  $a$  ist ein quadratischer Rest modulo  $n$ .
- ii)  $a$  ist ein quadratischer Rest modulo jeder Zahl  $n_i$  mit  $i = 1, 2, \dots, r$ .

*Beweis.* i)  $\Rightarrow$  ii): Aus  $\text{ggT}(a, n) = 1$  und  $x^2 \equiv_n a \Leftrightarrow n|x^2 - a$  mit  $x \in \mathbb{Z}$  folgt direkt  $\text{ggT}(a, n_i) = 1$  und  $x^2 \equiv_{n_i} a$  für alle  $i \in \{1, 2, \dots, r\}$ , da  $n = n_1 n_2 \cdot \dots \cdot n_r$ .

ii)  $\Rightarrow$  i): Da nach Voraussetzungen für alle  $i = 1, 2, \dots, r$  gilt:  $\text{ggT}(a, n_i) = 1$ , so gilt auch  $\text{ggT}(a, n) = 1$  wegen  $n = n_1 n_2 \cdot \dots \cdot n_r$ . Weiter gibt es nach Voraussetzung zu jedem  $i = 1, 2, \dots, r$  ein  $x_i$ , so dass  $x_i^2 \equiv_{n_i} a$ . Wir betrachten nun das System

$$X \equiv x_1(n_1), \quad X \equiv x_2(n_2), \dots, \quad X \equiv x_r(n_r)$$

simultaner Kongruenzen. Da  $n_1, n_2, \dots, n_r$  paarweise teilerfremde Zahlen sind, so hat dieses System nach dem Hauptsatz über simultane Kongruenzen (Chinesischer Restsatz) eine Lösung  $x \in \mathbb{Z}$ . Es folgt:

$$x^2 \equiv_{n_i} x_i^2 \equiv_{n_i} a \quad \text{für alle } i = 1, 2, \dots, r.$$

Durch Anwendung des Lemma 2.3 und einer evtl. einfachen Induktion folgt die Behauptung.  $\square$

Beachtet man den Hauptsatz der elementaren Zahlentheorie so drängt sich ein Korollar des Satzes geradezu auf.

**1.8 Folgerung:** Es sei  $n = p_1^{m_1} p_2^{m_2} \dots p_r^{m_r}$  die Primzerlegung der natürlichen Zahl  $n \geq 2$ . Sei  $a \in \mathbb{Z}$ , dann gilt:

$a$  ist quadratischer Rest modulo  $n \Leftrightarrow$   
 $a$  ist quadratischer Rest modulo jeder Primzahlpotenz  $p_i^{m_i}$  mit  $i = 1, 2, \dots, r$ .

**1.9 Beispiel:** Es sei  $n := 119 = 7 \cdot 17$  und  $a := 2$ . Da  $3^2 \equiv_7 2$  und  $6^2 \equiv_{17} 2$ , so ist 2 auch ein quadratischer Rest modulo 119. In der Tat gilt  $11^2 \equiv_{119} 2$ .

## 2. Quadratische Reste modulo Primzahlpotenzen

Aufgrund von Folgerung 2.5 darf man sich beim Studium, welche Zahlen quadratische Reste modulo einer vorgegebenen Zahl  $m$  sind, auf den Fall von Primzahlpotenzen beschränken. Zunächst diskutieren wir den Fall einer geraden Primzahlpotenz  $2^k, k \in \mathbb{N}^\times$ .

### 2.1. Gerade Primzahlpotenzen

Ziel dieses Unterabschnittes ist es sämtlichen quadratischen Reste modulo  $2^k$  mit  $k \in \mathbb{N}^\times$  zu bestimmen. Dabei sind die Fälle  $k = 1, 2$  trivial, da man diese einfach berechnen kann. So stellt man fest, dass alle ganzen ungeraden Zahlen, repräsentiert durch die Restklasse  $\bar{1}$ , quadratische Reste modulo 2 sind und für  $k = 2$  genau die Zahlen der Restklassen  $\bar{1}, \bar{3}$  quadratische Reste sind.

Für Exponenten  $k \geq 3$  zeigen wir nun das

**2.1 Lemma:** Es sei  $k \geq 3$ . Dann sind folgende Aussagen über eine ganze Zahl  $a \in \mathbb{Z}$  äquivalent:

- i)  $a$  ist quadratischer Rest modulo  $2^k$ .
- ii)  $a$  ist quadratischer Rest modulo  $2^3$ .
- iii)  $a \equiv 1(8)$ .

*Beweis.* i)  $\Rightarrow$  ii): Trivial, da  $k \geq 3$ .

ii)  $\Rightarrow$  i): Wir führen Induktion nach  $k$ , der Induktionsbeginn  $k = 3$  entspricht der Voraussetzung ii). Vergleichen Sie bitte auch mit dem Beispiel auf Seite 7.

Sei  $k > 3$  und es sei bereits bekannt, dass es zur ungeraden Zahl  $a$  eine Zahl  $x \in \mathbb{Z}$  gibt, so dass gilt

$$\begin{aligned} x^2 &\equiv a \pmod{2^{k-1}}, & \text{d.h.} \\ x^2 - a &= u \cdot 2^{k-1} & \text{mit } u \in \mathbb{Z}. \end{aligned}$$

Wir müssen zeigen, dass es eine Zahl  $y \in \mathbb{Z}$  gibt, so dass  $y^2 \equiv a(2^k)$  gilt. Wir behaupten, dass  $y := x + u2^{k-2}$  die gesuchte Eigenschaft erfüllt. Es gilt

$$\begin{aligned} y^2 - a &= (x + u2^{k-2})^2 - a \\ &= (x^2 - a) + xu2^{k-1} + u^22^{(k-2) \cdot 2} \\ &= u2^{k-1} + xu2^{k-1} + u^22^{2k-4} \\ &= u(1+x)2^{k-1} + u^22^{2k-4}. \end{aligned}$$

Da  $\underbrace{2k-4}_{\in \mathbb{Z}} \geq k$  wegen  $k > 3$ , so sehen wir:

$$y^2 - a \equiv u(1+x)2^{k-1} \pmod{2^k}.$$

Wegen  $x^2 \equiv a(2)$  ist mit  $a$  auch  $x$  ungerade und damit  $1+x$  durch 2 teilbar. Damit folgt wie behauptet

$$y^2 - a \equiv 0 \pmod{2^k},$$

dass  $a$  quadratischer Rest modulo  $2^k$  gilt.

ii)  $\Rightarrow$  iii): Diese Aussage folgt aus dem Beispiel auf Seite 7 oder durch einfaches Nachrechnen.  $\square$

Die Bedingung iii) besagt also, dass eine vorgelegte ganze Zahl  $a$  genau dann ein quadratischer Rest ist, wenn diese in der Restklasse  $\bar{1}$  modulo 8 liegt. Damit haben wir die Frage nach den quadratischen Reste modulo einer geraden Primzahlpotenz vollständig beantwortet.

## 2.2. Ungerade Primzahlpotenzen

Nun untersuchen wir ungerade Primzahlpotenzen  $p^k$  mit  $p \in \mathbb{P} \setminus \{2\}$ . In diesem Fall sind keinerlei Fallunterscheidungen, wie bei den geraden Primzahlpotenzen, notwendig:

**2.2 Satz:** Es sei  $p$  eine ungerade Primzahl, und es sei  $k$  eine positive natürliche Zahl. Dann sind folgende Aussagen über eine ganze Zahl  $a$  äquivalent:

- i)  $a$  ist ein quadratischer Rest modulo  $p^k$ .
- ii)  $a$  ist ein quadratischer Rest modulo  $p$ .

*Beweis.* i)  $\Rightarrow$  ii): Es existiert gemäß Voraussetzungen ein  $x \in \mathbb{Z}$ , so dass die Kongruenzgleichung  $x^2 \equiv a(p^k)$  erfüllt ist, d.h.  $x^2$  und  $a$  liegen in derselben Restklasse und damit gilt  $x^2 - a \in \mathbb{Z}p^k = \{z \cdot p^k | z \in \mathbb{Z}\}$ . Da  $p|p^k$  muss damit  $\mathbb{Z}p^k \subseteq \mathbb{Z}p$  gelten. Deshalb muss  $x$  auch in  $\mathbb{Z}p$  enthalten sein.

ii)  $\Rightarrow$  i): Es sei  $g \in \mathbb{Z}$  ein Erzeuger (Primitivwurzel) der zyklischen Gruppe  $\mathbb{Z}_{p^k}^*$  und  $\mathbb{Z}_p^*$ . Aufgrund von Satz 2.2 ist  $a$  modulo  $p$  als quadratischer Rest zu einer geraden Potenz von  $g$  kongruent:

$$a \equiv g^{2i}(p), \text{ wobei } 0 \leq \frac{1}{2}\phi(p) = \frac{1}{2}(p-1).$$

Da  $g$  auch Primitivwurzel zu  $p^k$  ist, gibt es ein  $l \in \mathbb{N}^\times$ , so dass  $a \equiv g^l(p^k)$  gilt. Daraus ergibt sich insbesondere  $a \equiv g^l(p)$ , also  $g^l \equiv g^{2i}(p)$ . Für die Restklasse  $\mathbb{Z}_p^*$  bedeutet dies:  $\bar{g}^l = \bar{g}^{2i}$  also  $\bar{g}^{l-2i} = \bar{1}$ . Da  $\text{ord}(g) = p-1$  folgt  $(p-1)|(l-2i)$ , also  $l = 2i + n(p-1)$  mit  $n \in \mathbb{Z}$ . Da  $p-1$  gerade ist, so ist mithin  $l = 2v$  (mit  $v \in \mathbb{Z}$ ) gerade. Aus der Gleichung  $(c^v)^2 \equiv a(p^k)$  lesen wir nun ab, dass  $a$  ein quadratischer Rest modulo  $p^k$  ist.  $\square$

**2.3 Beispiel:** 2 ist wegen  $3^2 \equiv 2(7)$  ein quadratischer Rest modulo 7. Daher ist 2 auch ein quadratischer Rest modulo jeder Potenz von 7. Es gilt z.B.  $10^2 \equiv 2(49)$ ,  $108^2 \equiv 2(343)$ .

In diesem Unterabschnitt studieren wir quadratische Reste für den Modul  $p$ , wobei  $p$  eine ungerade Primzahl ist. Deshalb ist  $(p-1)$  eine gerade und  $\frac{1}{2}(p-1)$  eine ganze Zahl ungleich Null.

**2.4 Satz:** Es sei  $a \in \mathbb{Z}$  teilerfremd zu  $p$ . Dann gilt:

- $a$  ist quadratischer Rest modulo  $p \Leftrightarrow a^{\frac{1}{2}(p-1)} \equiv 1(p)$ .
- $a$  ist quadratischer Nichtrest modulo  $p \Leftrightarrow a^{\frac{1}{2}(p-1)} \equiv -1(p)$ .

*Beweis.* Ad 1): Falls  $x^2 \equiv a(p)$  mit  $x \in \mathbb{Z}$ , so ist  $x$  teilerfremd zu  $p$  und es gilt

$$1 \equiv x^{p-1} \equiv (x^2)^{\frac{1}{2}(p-1)}(p),$$

nach dem kleinen Fermatschen Satz. Jeder quadratische Rest modulo  $p$  lässt also die Polynomkongruenz  $X^{\frac{1}{2}(p-1)} - 1 \equiv 0(p)$ . Da es genau  $\frac{1}{2}(p-1)$  verschiedene quadratische Reste modulo  $p$  gibt und da ein Polynom (über einem Integritätsring) maximal  $\frac{1}{2}(p-1)$  inkongruente Lösungen von  $X^{\frac{1}{2}(p-1)} - 1 \equiv 0(p)$  in  $\mathbb{Z}$  gibt, so folgt 1).

Ad 2): Ist  $p$  eine ungerade Primzahl so gilt für jedes  $a \in \mathbb{N}^\times$  mit  $p \nmid a$  eines der beiden folgenden Kongruenzen

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

Es sei  $s := \frac{1}{2}(p-1)$  und  $a^{(p-1)} - 1 = (a^s - 1)(a^s + 1)$ . Aus dem kleinen Fermatschen Satz folgt dann  $(a^s - 1)(a^s + 1) \equiv 0(p)$ . Kürzt man nun jeweils einen der Faktoren, so ist die erste Teilbehauptung klar. Wegen 1) ist damit auch 2) klar.  $\square$

### 3. Kriterium von Euler und das Legendre-Symbol

**3.1 Definition:** Sei  $a \in \mathbb{Z}$  und  $p > 2$  eine Primzahl. Das **Legendre-Symbol**  $\left(\frac{a}{p}\right)$  ist definiert als

$$\left(\frac{a}{p}\right) := \begin{cases} 0 & , \text{ falls } p|a \\ 1 & , \text{ falls } a \pmod p \text{ quadratischer Rest modulo } p \\ -1 & , \text{ falls } a \pmod p \text{ quadratischer Nichtrest modulo } p \end{cases}$$

Das Legendre-Symbol ist nach dem französischen Mathematiker ADRIEN-MARIE LEGENDRE (1752-1833) benannt. Beachten Sie, dass das Legendre-Symbol für Primzahlen definiert ist. Eine Fortführung dieser Definition werden wir weiter unten mit dem Jacobi-Symbol einführen.

**3.2 Beispiel:** Sei  $p = 7$ , also prim. Dann besteht die Einheiten-Gruppe  $(\mathbb{Z}/7\mathbb{Z})^*$  aus  $\phi(7) = 6$  Elementen, nämlich aus den Restklassen  $\{1, 2, 3, 4, 5, 6\}$ . Es gilt

$$\begin{aligned} 1^2 \equiv_7 6^2 \equiv_7 1, & & 2^2 \equiv_7 5^2 \equiv_7 4 \\ 3^2 \equiv_7 4^2 \equiv_7 2, & & 0^2 \equiv_7 7^2 \equiv_7 0 \end{aligned}$$

Es sind also  $\left(\frac{0}{7}\right) = 0$  und  $\left(\frac{1}{7}\right) = \left(\frac{4}{7}\right) = \left(\frac{2}{7}\right) = 1$  und  $\left(\frac{3}{7}\right) = \left(\frac{5}{7}\right) = \left(\frac{6}{7}\right) = -1$ .

Um also festzustellen, für welche von  $0 \pmod p$  verschiedene Restklassen  $a \pmod p$  die Kongruenz

$$x^2 \equiv a \pmod p \tag{II.3}$$

lösbar ist, berechnen wir  $i^2 \pmod p$  für  $i = 1, 2, \dots, (p-1)$ .

Im obigen Beispiel haben wir festgestellt, dass die Kongruenz  $x^2 \equiv a \pmod 7$  für  $a \equiv_7 1, 2$  und  $4$  lösbar ist. Sie besitzt dann jeweils *zwei* differente Lösungen, denn  $x^2 \equiv i^2 \pmod 7$  ist äquivalent mit  $x \equiv i \pmod 7$  oder  $x \equiv -i \pmod 7$ , wobei  $i \not\equiv -i \pmod 7$  und  $i \not\equiv 0 \pmod 7$ .

Bilden wir also die Quadratzahlen von  $1, 2, \dots, (p-1)$  so erhalten wir  $\frac{1}{2}(p-1)$  verschiedene Werte, wobei  $x^2 \equiv_p (p-x)^2$  gilt:

$$\begin{aligned} x^2 \equiv_p y^2 & & \text{mit } 1 \leq x \leq y \leq \frac{1}{2}(p-1) \\ \Rightarrow p|(y^2 - x^2) \Rightarrow p|(x+y)(y-x) & & \text{mit } 0 \leq y-x < x+y < p \\ \Rightarrow y = x \text{ oder } y = (p-x). & & \end{aligned}$$

So ist auch klar, warum die Quadrate von  $1, \dots, \frac{1}{2}(p-1)$  alle paarweise verschieden sind.

Die Restklassen  $a \pmod p$  für welche Kongruenz (2.3) lösbar ist, findet man auch mit Hilfe einer primitiven Restklasse  $\pmod p$ . Allerdings bereitet das Auffinden einer solchen in der Regel große Schwierigkeiten.

Der folgende Satz geht auf Euler und Legendre zurück und ist ein weiteres *notwendiges* aber *nicht hinreichendes* Kriterium für Primzahlen  $p$ .

**3.3 Satz:** (Kriterium von EULER)

Sei  $a \in \mathbb{Z}$  und  $p > 2$  eine Primzahl. Dann gilt

$$a^{\frac{p-1}{2}} \equiv_p \left(\frac{a}{p}\right) \tag{II.4}$$

*Beweis.* Gilt  $p|a$ , dann ist  $a \pmod p = 0$ , also auch  $a^{\frac{p-1}{2}} \equiv_p 0 \equiv_p \left(\frac{a}{p}\right)$ . Wir müssen also noch zeigen, dass (2.4) auch für  $p \nmid a$  gilt. Es sei nun  $p \nmid a$ , dann ist  $a \pmod p \in (\mathbb{Z}/p\mathbb{Z})^*$ . Sei  $g$  ein Erzeuger von  $(\mathbb{Z}/p\mathbb{Z})^*$ , dann ist  $a \pmod p$  ein quadratischer Rest modulo  $p$ , dann gilt  $a \equiv_p g^{2k}$  für ein  $k \in \mathbb{N}_0$ . Also folgt

$$a^{\frac{p-1}{2}} \equiv_p (g^{2k})^{\frac{p-1}{2}} \equiv_p (g^{p-1})^k \equiv_p 1^k \equiv_p 1.$$

Ist  $a \pmod p$  ein quadratischer Nichtrest modulo  $p$ , dann gilt  $a \equiv_p g^{2k+1}$  für ein  $k \in \mathbb{N}_0$ . Also folgt

$$a^{\frac{p-1}{2}} \equiv_p (g^{2k+1})^{\frac{p-1}{2}} \equiv_p g^{k(p-1)+\frac{p-1}{2}} \equiv_p (g^{p-1})^k \cdot g^{\frac{p-1}{2}} \equiv_p 1^k \cdot g^{\frac{p-1}{2}} \equiv_p g^{\frac{p-1}{2}}.$$

Nun ist aber  $g^{\frac{p-1}{2}} \not\equiv_p 1$ , denn die Ordnung von  $g$  in  $(\mathbb{Z}/p\mathbb{Z})^*$  ist  $p-1$ . Andererseits ist  $(g^{\frac{p-1}{2}})^2 \equiv_p g^{p-1} \equiv_p 1$ , also ist  $g^{\frac{p-1}{2}} \equiv_p \pm 1$ . Insgesamt folgt also  $g^{\frac{p-1}{2}} \equiv_p -1$ , also  $a^{\frac{p-1}{2}} \equiv_p -1 \equiv_p \left(\frac{a}{p}\right)$ . □

Ist also  $ggT(a, p) = 1$ , d.h.  $a$  ist kein ganzzahliges Vielfaches von  $p$ , dann muss nach dem Eulerschen Kriterium  $a^{\frac{p-1}{2}} \equiv_p \pm 1$  gelten. Beachten Sie, dass dadurch gerade alle Primzahlen in der Menge  $\{n \in \mathbb{Z} | n = 2k + 1, k \in \mathbb{Z}\} = \{n \in \mathbb{Z} | n = 4k + 1 \text{ oder } n = 4k + 3 \text{ mit } k \in \mathbb{Z}\}$  erfasst werden, d.h. das Eulersche Kriterium gilt für Primzahlen aus  $\mathbb{P} \setminus \{2\}$ , wie oben im Satz formuliert.

**3.4 Folgerung:** Es sei  $p$  eine Primzahl, dann gilt

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

*Beweis.* Man wende das Kriterium von Euler für  $a := -1$  an. □

Die wichtigsten Rechenregeln für Legendre-Symbolen lauten:

**3.5 Lemma:** Sei  $p > 2$  eine Primzahl, und seien  $a, b \in \mathbb{Z}$ .

(i) Gilt  $a \equiv b \pmod{p}$ , dann ist  $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$ .

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

(iii)  $\left(\frac{-1}{p}\right) = \begin{cases} 1, & \text{falls } p \pmod{4} = 1 \\ -1, & \text{falls } p \pmod{4} = 3. \end{cases}$

*Beweis.* (i) Sei  $a \equiv b \pmod{p}$ . Dann ist  $a^{\frac{p-1}{2}} \equiv_p b^{\frac{p-1}{2}}$ , also folgt mit dem Kriterium von Euler, dass  $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$ .

(ii) Es gilt  $\left(\frac{ab}{p}\right) = (ab)^{\frac{p-1}{2}} = a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$ .

(iii) Es gilt  $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$ . Also ist  $\left(\frac{-1}{p}\right) = 1 \Leftrightarrow \frac{p-1}{2}$  ist gerade  $\Leftrightarrow \frac{p-1}{2} = 2k$  für ein  $k \in \mathbb{N}_0$   
 $\Leftrightarrow p - 1 = 4k$  für ein  $k \in \mathbb{N}_0 \Leftrightarrow p = 4k + 1$  für ein  $k \in \mathbb{N}_0 \Leftrightarrow p \pmod{4} = 1$ . Da  $p$  ungerade ist, gilt entweder  $p \pmod{4} = 1$  oder  $p \pmod{4} = 3$ .

□

**3.6 Beispiel:** Mit den eben gewonnenen Rechenregeln können bereits einige der Legendre-Symbole bequem berechnet werden:  $\left(\frac{40}{31}\right) = \left(\frac{9}{31}\right) = \left(\frac{3}{31}\right)^2 = 1$ . Sowie

$\left(\frac{-1}{31}\right) = \left(\frac{-1}{31}\right)\left(\frac{4}{31}\right) = \left(\frac{-1}{31}\right)\left(\frac{2}{31}\right)^2 = -1$ , denn  $31 \pmod{4} = 3$ .

### III. Das Reziprozitätsgesetz

#### 1. Das Gaußsche Lemma

Mit Hilfe des Eulerschen Kriteriums wird nun ein weiteres Restkriterium, das so genannte Gaußsche Lemma, hergeleitet, welches eine Schlüsselrolle im Beweis des quadratischen Reziprozitätsgesetz spielen wird. Zunächst aber das Organisatorische – die notwendigen Definitionen:

**1.1 Definition:** Es sei  $p$  eine Primzahl. Dann heißt eine aus  $(p-1)$  Elementen bestehende Menge

$$\begin{aligned} S_p &:= \{\pm 1, \pm 2, \dots, \pm \frac{1}{2}(p-1)\} \\ &= \{-\frac{1}{2}(p-1), -\frac{1}{2}(p-1)+1, \dots, -1, 1, 2, \dots, \frac{1}{2}(p-1)\}. \end{aligned}$$

die Menge der absolut kleinsten Reste modulo  $p$ . Die Menge  $S_p$  der absolut kleinsten Reste modulo  $p$  ist die disjunkte Vereinigung der Mengen  $S^+ := \{1, 2, \dots, \frac{1}{2}(p-1)\}$  und  $S^- := \{-\frac{1}{2}(p-1), -\frac{1}{2}(p-1)+1, \dots, -1\} = \{-s | s \in S^+\}$ .

**Bemerkung:** Jede zu  $p$  teilerfremde Zahl  $a \in \mathbb{Z}$  ist modulo  $p$  zu genau einem absolut kleinsten Rest  $w$  kongruent. Es gilt also

$$0 < |w| = \min\{|v| : v \in \bar{a}\} \leq \frac{1}{2}(p-1) < \frac{1}{2}p.$$

*Beweis.* Wir wissen, dass jede zu  $p$  teilerfremde Zahl zu genau einem Element der Menge  $\{1, 2, \dots, p-1\}$  modulo  $p$  kongruent ist. Wir müssen also zeigen, dass jedem Element aus  $S^- = \{-\frac{1}{2}(p-1), -\frac{1}{2}(p-1)+1, \dots, -1\}$  bezüglich dem Modul  $p$  ein Element aus  $\{\frac{1}{2}(p-1)+1, \frac{1}{2}(p-1)+2, \dots, (p-1)\}$  entspricht. Nun gilt

$$\frac{1}{2}(p-1) + k \equiv_p -\frac{1}{2}(p-1) + k - 1 \quad \text{für } k = 1, 2, \dots, \frac{1}{2}(p-1);$$

daher ist jedes Element von  $\{1, 2, \dots, (p-1)\}$  zu genau einem Element der Menge

$$S_p = \{-\frac{1}{2}(p-1), -\frac{1}{2}(p-1)+1, \dots, -1, 1, 2, \dots, \frac{1}{2}(p-1)\}$$

kongruent. □

Sind zwei Elemente  $s \in S^+$  und  $a \in \mathbb{Z}$  teilerfremd zu  $p$ , d.h. es gilt  $ggT(a, p) = ggT(a, s) = 1$ , so ist auch das Produkt  $sa$  teilerfremd zu  $p$  also gilt auch  $ggT(sa, p) = 1$ . Aufgrund der letzten Bemerkung und dem eben Gesagten gibt es eindeutig bestimmte Zahlen  $\epsilon_s(a) \in \{+1, -1\}$  und  $s_a \in S^+$  mit

$$s \cdot a \equiv_p \epsilon_s(a) \cdot s_a. \tag{III.1}$$

Es ist  $\epsilon_s(a) = -1$  genau dann, wenn der absolut kleinste Rest des Produkts  $s \cdot a$  modulo  $p$  in  $S^-$  liegt, also negativ ist. Entsprechend ist  $\epsilon_s(a) = +1$  genau dann, wenn der absolut kleinste Rest des Produkts  $s \cdot a$  modulo  $p$  in  $S^+$  liegt, also positiv ist.

Es gilt folgendes

**1.2 Lemma:** Es sei ein zu  $p$  teilerfremdes  $a \in \mathbb{Z}$  fixiert. Dann ist die Abbildung  $S^+ \rightarrow S^+$  definiert durch  $s \mapsto s_a$  bijektiv.

*Beweis.* Da  $S^+$  eine endliche Menge ist, reicht es nachzuweisen, dass aus  $s_a = t_a$  für  $s, t \in S^+$  folgt  $s = t$ . Wegen  $sa \equiv_p \epsilon_s(a) \cdot s_a \Leftrightarrow sa \cdot \epsilon_s(a) \equiv_p s_a$ , da  $\epsilon_s(a) \in \{\pm 1\}$  und daher  $\epsilon_s(a)$  zu sich selbst invers.

Sei nun also  $s_a = t_a$  und mit obiger Gleichung  $sa \cdot \epsilon_s(a) \equiv_p ta \cdot \epsilon_t(a)$ . Nun wendet man die Kürzungsregel für faktorielle Ringe an (jeder Hauptidealring ist ein faktorieller Ring) und erhalten  $s \cdot \epsilon_s(a) \equiv_p t \cdot \epsilon_t(a) \Rightarrow s \cdot \epsilon_s(a) - t \cdot \epsilon_t(a) \equiv_p 0$ , d.h.  $p \mid (s \cdot \epsilon_s(a) - t \cdot \epsilon_t(a))$ . Nun sind  $s, t \in S^+$ , so dass

$$|s \cdot \epsilon_s(a) - t \cdot \epsilon_t(a)| \leq |s \cdot \epsilon_s(a)| + |t \cdot \epsilon_t(a)| = s + t \leq p - 1 < p \tag{III.2}$$

ist. Aus  $p \mid (s \cdot \epsilon_s(a) - t \cdot \epsilon_t(a))$  und  $p$  Primzahl zusammen mit (3.2) folgt  $\epsilon_s(a)s - \epsilon_t(a)t = 0$  und also  $s = t$ . □

Nun kommen wir zum vorläufige Hauptergebnis, dem Restkriterium von Gauß, welches entscheidend für die Beweisführung des quadratischen Reziprozitätsgesetzes. Der Beweis des Gaußschen Lemmas stützt sich entscheidend auf dem Eulersche Kriterium.

**1.3 Satz:** (Gaußsche Lemma)

Es sei  $a \in \mathbb{Z}$  und  $p \in \mathbb{P}$  eine Primzahl mit  $ggT(a, p) = 1$ . Dann gilt

$$\left(\frac{a}{p}\right) = \prod_{s \in S^+} \epsilon_s(a) = (-1)^n,$$

wobei  $n$  die Anzahl der negativen Zahlen unter den absolut kleinsten Resten modulo  $p$  der  $\frac{1}{2}(p-1)$  Vielfachen  $a, 2a, \dots, \frac{1}{2}(p-1)a$ .

*Beweis.* Es ist nur die erste Gleichung zu zeigen. Wir wissen, dass die Abbildung  $S^+ \rightarrow S^+$  mit  $s \mapsto s_a$  bijektiv ist. Es ist  $sa \equiv \underbrace{\epsilon_s(a)}_{\in \{\pm 1\}} \cdot \underbrace{s_a}_{\in S^+}$  wie in (3.1) festgelegt. Aufgrund der

Vorbemerkungen folgt

$$\prod_{s \in S^+} s_a = \prod_{s \in S^+} s = \left[ \frac{1}{2}(p-1) \right]!$$

und mit (3.2) folgt

$$\prod_{s \in S^+} sa \equiv_p \prod_{s \in S^+} (s_a \cdot \epsilon_s(a)) \equiv_p \left( \frac{1}{2}(p-1) \right)! \left( \prod_{s \in S^+} \epsilon_s(a) \right).$$

Da andererseits

$$\begin{aligned} \prod_{s \in S^+} sa &= 1 \cdot a \cdot 2 \cdot a \dots \cdot \frac{1}{2}(p-1) \cdot a \\ &= a^{\frac{1}{2}(p-1)} \cdot \left( \frac{1}{2}(p-1) \right)! \end{aligned}$$

so ergibt sich weiter

$$a^{\frac{1}{2}(p-1)} \cdot \left( \frac{1}{2}(p-1) \right)! \equiv_p \prod_{s \in S^+} (\epsilon_s(a)) \left( \frac{1}{2}(p-1) \right)!.$$

Die Zahl  $\left( \frac{1}{2}(p-1) \right)!$  ist teilerfremd zu  $p$ , daher darf man durch sie kürzen. Es folgt:

$$a^{\frac{1}{2}(p-1)} \equiv_p \prod_{s \in S^+} (\epsilon_s(a)).$$

Da nach dem Eulerschen Kriterium  $\left( \frac{a}{p} \right) \equiv_p a^{\frac{1}{2}(p-1)}$  gilt, so ist das Gaußsche Lemma bewiesen. □

Ein Beispiel wird das Gaußsche Lemma veranschaulichen.

**1.4 Beispiel:** Es soll der Wert des Legendresymbols  $\left( \frac{7}{13} \right)$  mit Hilfe des Gaußschen Lemmas berechnet werden. Wie im Satz spielt die Menge  $S^+ = \{1, 2, 3, 4, 5, 6\}$  eine entscheidende Rolle, denn wir bilden die Produkte  $a \cdot s = 13 \cdot s$  mit allen  $s \in S^+$ . Diese Produkte werden sodann modulo 13 derart reduziert, so dass die Reste in eine der Klassen aus  $S^+$  oder  $S^-$  fallen, d.h. wir müssen zu diesen Produkten die absolut kleinsten Reste bestimmen:

$$\begin{array}{ll} 7 \cdot 1 = 7 \equiv_{13} -6, & 7 \cdot 2 = 14 \equiv_{13} 1 \\ 7 \cdot 3 = 21 \equiv_{13} -5, & 7 \cdot 4 = 28 \equiv_{13} 2 \\ 7 \cdot 5 = 35 \equiv_{13} -4, & 7 \cdot 6 = 42 \equiv_{13} 3 \end{array}$$

Dies ergibt also insgesamt 3 negative absolut kleinsten Reste, womit die Gleichung

$$\left( \frac{7}{13} \right) = (-1)^3 = -1$$

nach dem Lemma von Gauß gilt.

Dieses Beispiel zeigt deutlich, dass die Berechnung eines beliebigen Legendre-Symbols (und damit die Beantwortung der Frage nach den quadratischen Resten) mit Hilfe des Gaußschen Lemmas zwar möglich, aber auch sehr aufwendig ist. Eine wesentliche Verbesserung wird sich durch das quadratische Reziprozitätsgesetz ergeben.

Dem quadratischen Reziprozitätsgesetz werden oftmals sog. Ergänzungssätze zur Seite gestellt. Der folgende Satz wird oftmals auch „zweiter Ergänzungssatz“ zum quadratischen Reziprozitätsgesetz genannt. Er besagt, dass die Zahl  $a := 2$  für alle modulo 8 kongruenten Primzahlen dasselbe quadratische Restverhalten hat.

**1.5 Satz:** (Zweiter Ergänzungssatz)

Für jede Primzahl  $p > 2$  gilt:

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

Es ist also 2 quadratischer Rest modulo aller Primzahlen der Form  $8k+1$  und  $8k+7$ ,  $k \in \mathbb{N}$ , und das quadratischer Nichtrest modulo aller übrigen ungeraden Primzahlen.

Vor dem eigentlichen Beweis eine wichtige

**Bemerkung:** Jede Primzahl  $p \in \mathbb{P}$  ungleich 2 ist ungerade und liegt deshalb in der Menge aller ungeraden natürlichen Zahlen  $2k+1$ ,  $k \in \mathbb{N}$ . Übersetzt man dies in die Sprache der Restklassen, so liegt jede Primzahl  $\neq 2$  in der Restklasse  $\bar{1}$  modulo 2.

Entsprechend kann jede ungerade Primzahl entweder durch  $4k+1$  oder  $4k+3$  mit  $k \in \mathbb{N}$  dargestellt werden. Hier liegt jede ungerade Primzahl entweder in der Restklasse  $\bar{1}$  oder  $\bar{3}$  modulo 4; die übrigen Restklassen  $\bar{0}$  und  $\bar{2}$  enthalten offensichtlich gerade Zahlen.

Nun der Beweis des Ergänzungssatzes:

*Beweis.* Wir bestimmen die Anzahl  $n$  der negativen absolut kleinsten Reste modulo  $p$  der  $\frac{1}{2}(p-1)$  Zahlen  $1 \cdot 2, 2 \cdot 2, \dots, \frac{1}{2}(p-1) \cdot 2$ . Da diese Zahlen sämtlich kleiner als  $p$  sind, liefern genau diejenigen Zahlen  $x \cdot 2$  unter ihnen einen negativen absolut kleinsten Rest, die echt größer als  $\frac{1}{2}(p-1)$  sind. Setzt man  $\lambda := \max\{x \in \mathbb{N} \mid x \cdot 2 \leq \frac{1}{2}(p-1)\}$ , so folgt für die Anzahl der absolut kleinsten Reste modulo  $p$  offensichtlich

$$n = \frac{1}{2}(p-1) - \lambda, \tag{III.3}$$

da  $\lambda$  – gemäß Definition – die Anzahl der positiven absolut kleinsten Reste modulo  $p$  angibt. Unter Benutzung der Gaußklammer, der Definition von  $\lambda$  und der Gleichung (3.3) gilt

$$\begin{aligned}\lambda &= \left[ \frac{1}{4}(p-1) \right] \\ \Rightarrow n &= \frac{1}{2}(p-1) - \left[ \frac{1}{4}(p-1) \right] \\ \Rightarrow \left( \frac{2}{p} \right) &= (-1)^{\frac{1}{2}(p-1) - \left[ \frac{1}{4}(p-1) \right]}.\end{aligned}$$

Wir müssen nun feststellen, für welche Primzahlen  $p$  die Zahl  $n$  gerade bzw. ungerade ist. Jede ungerade Primzahl  $p$  ist von einer der folgenden vier Formen:

$$8k+1, \quad 8k+3, \quad 8k+5, \quad 8k+7$$

mit  $k \in \mathbb{N}$ . Vergleichen Sie auch mit der Bemerkung unmittelbar überhalb dieses Beweises. Setzen wir die verschiedenen Darstellungsformen der Primzahl  $p$  in  $\frac{1}{2}(p-1)$  respektive  $\left[ \frac{1}{4}(p-1) \right]$  ein, so erhalten wir jeweils:

$$4k, 2k \quad 4k+1, 2k \quad 4k+2, 2k+1 \quad 4k+3, 2k+1$$

Damit sehen wir:

$$\begin{aligned}\text{Für } p = 8k+1 \text{ ist } n &= 4k - 2k && \text{gerade;} \\ \text{Für } p = 8k+3 \text{ ist } n &= 4k+1 - 2k && \text{ungerade;} \\ \text{Für } p = 8k+5 \text{ ist } n &= 4k+2 - (2k+1) && \text{ungerade;} \\ \text{Für } p = 8k+7 \text{ ist } n &= 4k+3 - (2k+1) && \text{gerade.}\end{aligned}$$

Demnach ist 2 quadratischer Rest modulo aller Primzahlen der Form  $8k+1$  und  $8k+7$  und quadratischer Nichtrest modulo aller Primzahlen der Form  $8k+3$  und  $8k+5$ .

Wir müssen noch zeigen, dass die soeben gewonnene Aussage äquivalent mit der Formel  $\left( \frac{2}{p} \right) = (-1)^{\frac{p^2-1}{8}}$  ist. Es ist lediglich zu zeigen: Für alle Primzahlen  $p$  der Form  $8k+1$  und  $8k+7$  ist  $\frac{p^2-1}{8}$  eine gerade ganze Zahl; für alle Primzahlen  $p$  der Form  $8k+3$  und  $8k+5$  ist  $\frac{p^2-1}{8}$  eine ungerade ganze Zahl. Dies verifiziert man durch Nachrechnen.  $\square$

Eine jede ganze Zahl  $a \in \mathbb{Z}$  kann, gemäß dem Hauptsatz der elementaren Zahlentheorie, in der Form

$$a = (-1)^j \cdot 2^k \cdot q_1^{m_1} \cdot \dots \cdot q_r^{m_r},$$

wobei  $j \in \{0, 1\}$ ,  $k \in \mathbb{N}$  und  $m_i \in \mathbb{N}^\times$  sowie  $q_i \in \mathbb{P} \setminus \{2\}$  für  $i = 1, \dots, r$ . Entsprechend folgt mit Lemma 2.8 (ii) für das Legendre-Symbol

$$\left( \frac{a}{p} \right) = \underbrace{\left( \frac{-1}{p} \right)^j}_{\text{I}} \cdot \underbrace{\left( \frac{2}{p} \right)^k}_{\text{II}} \cdot \underbrace{\left( \frac{q_1}{p} \right)^{m_1} \cdot \dots \cdot \left( \frac{q_r}{p} \right)^{m_r}}_{\text{III}}.$$

Kennt man in diesen drei Situationen das Legendresche Restsymbol als Funktion des Nenners, so beherrscht man auch den Allgemeinfall auf Grund der Multiplikationsregel für das Legendre-Symbol. Typ I wurde mit Folgerung 2.7 erledigt, Typ II mit Unterabschnitt 2.2.1 bzw. Satz 3.3, bleibt also noch Typ III zu klären; dies wird der folgende Abschnitt.

## 2. Ergänzungssätze und das quadratische Reziprozitätsgesetz

Neben dem bereits beschriebenen Effekt, dass wir das Legendresche-Restsymbol effizient berechnen können wird durch das quadratische Reziprozitätsgesetz die Frage beantwortet, welche Moduln  $m$  so beschaffen sind, dass eine vorgelegte Zahl  $a$  modulo  $m$  ein quadratischer Rest ist. Wie wir bereits festgestellt haben sind dabei insgesamt drei Fälle zu klären. Die ersten beiden Fälle (die bereits umfassend bewiesen wurden) fasst man üblicherweise zu den sog. Ergänzungssätzen zusammen.

### 2.1 Satz: (Ergänzungssätze zum quadr. Reziprozitätsgesetz)

Es sei  $p$  irgendeine Primzahl. Dann gilt:

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

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

Für gewöhnlich nennt man I) bzw. II) den ersten bzw. zweiten Ergänzungssatz. Nun formulieren wir das Hauptergebnis des Dokuments.

### 2.2 Satz: (Quadratische Reziprozitätsgesetz)

Es seien  $p$  und  $q$  verschiedene ungerade Primzahlen. Dann gilt:

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

Für je zwei verschiedene, ungerade Primzahlen  $p, q$  gilt:

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right), \quad \text{wenn } p, q \text{ nicht beide von der Form } 4k + 3 \text{ sind} \quad (\text{III.4})$$

$$\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right), \quad \text{wenn } p, q \text{ beide die Form } 4k + 3 \text{ haben;} \quad (\text{III.5})$$

Da ein Produkt aus zwei Faktoren genau dann ungerade ist, wenn *beide* Faktoren ungerade sind. Ist einer der Faktoren oder beide Faktoren gerade, so ist auch das Produkt gerade. Entsprechend ist  $(-1)^{\frac{p-1}{2}\frac{q-1}{2}} = -1$  genau dann, wenn beide Faktoren in der Potenz gerade sind. Dies ist genau dann der Fall, wenn es  $k, k' \in \mathbb{Z}$  gibt, so dass sich die Primzahlen  $p$  und  $q$  in der Form  $p = 4k + 3$  bzw.  $q = 4k' + 3$  darstellen lassen, denn dann gilt:

$$\begin{aligned} \frac{p-1}{2} \frac{q-1}{2} &= \frac{4k+3-1}{2} \frac{4k'+3-1}{2} \\ &= \frac{4k+2}{2} \frac{4k'+2}{2} \\ &= (2k+1)(2k'+1). \end{aligned}$$

Das quadratische Reziprozitätsgesetz fasst also beide Identitäten (3.4) und (3.5) in einer Formel zusammen. Weiter besagt das quadratische Reziprozitätsgesetz, dass die beiden Fragen

- Ist  $p$  ein quadratischer Rest modulo  $q$ ?
- Ist  $q$  ein quadratischer Rest modulo  $p$ ?

quasi gleichbedeutend sind.

**2.3 Beispiel:** Es soll festgestellt werden, ob 3 ein quadratischer Rest modulo 29 ist. Auf Grund des Reziprozitätsgesetzes gilt

$$\begin{aligned} \left(\frac{3}{29}\right) \left(\frac{29}{3}\right) &= (-1)^{\frac{3-1}{2} \frac{29-1}{2}} = 1 \\ &\Rightarrow \left(\frac{3}{29}\right) = \left(\frac{29}{3}\right), \end{aligned}$$

da ein Produkt genau dann 1 ist, wenn beide Faktoren entweder 1 oder  $-1$  sind. Wegen  $29 \equiv 2(3)$  ergibt sich sodann mit dem zweiten Ergänzungssatz

$$\left(\frac{29}{3}\right) = \left(\frac{2}{3}\right) = (-1)^{\frac{3^2-1}{8}} = -1.$$

Also ist 3 ein quadratischer Nichtrest modulo 29.

Das nächste Anwendungsbeispiel nutzt die Primfaktorzerlegung der zu untersuchenden ganzen Zahl und die Multiplikativität des Legendre-Symbols, wie weiter oben erläutert.

**2.4 Beispiel:** Wir werden nun  $\left(\frac{35}{281}\right)$  berechnen, wobei natürlich 281 eine Primzahl ist. Die Primfaktorzerlegung der Zahl  $35 = 5 \cdot 7$  gibt Anlass die Restsymbole  $\left(\frac{5}{281}\right)$  und  $\left(\frac{7}{281}\right)$  zu berechnen, denn es gilt

$$\left(\frac{35}{281}\right) = \left(\frac{5}{281}\right) \left(\frac{7}{281}\right).$$

Wenden wir das Reziprozitätsgesetz an, so folgt

$$\left(\frac{5}{281}\right) = \left(\frac{281}{5}\right) \quad \text{und} \quad \left(\frac{7}{281}\right) = \left(\frac{281}{7}\right),$$

da offensichtlich (3.4) gilt. Da  $281 \equiv 1(5)$  und  $281 \equiv 1(7)$ , so folgt für  $\left(\frac{35}{281}\right) = 1 \cdot 1 = 1$ , d.h. 35 ist ein quadratischer Rest modulo 281.

### 3. Der Beweis

Der nun folgende Beweis des quadratischen Reziprozitätsgesetzes stützt sich insbesondere auf dem Gaußschen Lemma. Erstmals wurde dieser Beweis im Jahr 1844 von FERDINAND GOTTHOLD EISENSTEIN unter dem Titel „Geometrischer Beweis des Fundamentalsatzes für die quadratischen Reste“ veröffentlicht.

Nun endlich zum

*Beweis.* Es ist zu zeigen, dass

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

wobei  $p, q \in \mathbb{P}, p > 2, q > 2, p \neq q$ . Nun wenden wir auf beide Legendresche Restsymbole das Gaußsche Lemma an. D.h. es existiert  $n, m \in \mathbb{N}$ , so dass

$$\left(\frac{p}{q}\right) = (-1)^m \quad \text{und} \quad \left(\frac{q}{p}\right) = (-1)^n$$

gilt; es ist also  $m$  bzw.  $n$  die Anzahl der negativen Zahlen unter den absolut kleinsten Reste modulo  $q$  bzw. modulo  $p$ . Konkret bedeutet dies, dass  $m$  bzw.  $n$  die Anzahl derjenigen Zahlen aus der Menge  $\{1 \cdot p, 2 \cdot p, \dots, \frac{1}{2}(q-1) \cdot p\}$  bzw.  $\{1 \cdot q, 2 \cdot q, \dots, \frac{1}{2}(p-1) \cdot q\}$  ist, deren absolut kleinster Rest modulo  $q$  bzw.  $p$  negativ ist. Dann folgt also

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{m+n},$$

so dass alles darauf hinausläuft zu zeigen:

$$(-1)^{\frac{p-1}{2}\frac{q-1}{2}} = (-1)^{m+n},$$

also

$$\frac{1}{2}(p-1)\frac{1}{2}(q-1) = m+n+2\delta \quad \text{mit } \delta \in \mathbb{N}.$$

Um diese Gleichung zu beweisen nutzen wir die Struktur der Menge  $S^-$ . Dazu werden wir zunächst die Zahlen  $m$  und  $n$  anders beschreiben. Laut Definition ist  $n$  die Anzahl derjenigen Zahlen  $q \cot s$  mit  $s \in S^+$ , deren absolut kleinster Rest modulo  $p$  negativ ist. Das sind genau die Zahlen  $q \cdot s$  mit  $s \in S^+$ , zu denen es eine Zahl  $t \in \mathbb{Z}$  gibt, so dass gilt

$$-\frac{1}{2} < q \cdot s - p \cdot t < 0.$$

In dieser Ungleichung ist die Zahl  $t$ , wenn sie überhaupt existiert, eindeutig durch  $s$  bestimmt. Es gilt  $t > 0$  und wegen  $s < \frac{1}{2}p$  folgt

$$\begin{aligned} -\frac{1}{2} &< qs - pt < 0 \\ \Rightarrow pt &< qs + \frac{1}{2} < pt + \frac{1}{2} \\ \Rightarrow pt &< qs + \frac{1}{2}p < \frac{1}{2}pq + \frac{1}{2}p = \frac{1}{2}p(q+1), \end{aligned}$$

also

$$t < \frac{1}{2}(q+1), \text{ d.h. } t \leq \frac{1}{2}(q-1).$$

Die Zahl  $t$  ist also, ihre Existenz unterstellt, eine der Zahlen  $1, 2, \dots, \frac{1}{2}(q-1)$ . Damit haben wir festgestellt:

Die Zahl  $n$  ist genau die Anzahl der Paare  $(s, t)$  natürlicher Zahlen, für die gilt:

$$\text{a) } 1 \leq s \leq \frac{1}{2}(p-1), \quad 1 \leq t \leq \frac{1}{2}(q-1), \quad -\frac{1}{2}p < qs - pt < 0.$$

Ebenso sieht man, dass  $m$  genau die Anzahl der Paare  $(u, v)$  natürlicher Zahlen, für die gilt:

$$1 \leq u \leq \frac{1}{2}(q-1), \quad 1 \leq v \leq \frac{1}{2}(p-1), \quad -\frac{1}{2}q < pu - qv < 0.$$

Bringt man die letzte Ungleichung in der Form  $0 < qv - pu < \frac{1}{2}q$  durch Multiplikation mit  $(-1)$  und schreibt noch  $s$  statt  $v$  und  $t$  statt  $u$ , so folgt:

Die Zahl  $m$  ist genau die Anzahl der Paare  $(s, t)$  natürlicher Zahlen, für die gilt:

$$\text{b) } 1 \leq s \leq \frac{1}{2}(p-1), \quad 1 \leq t \leq \frac{1}{2}(q-1), \quad 0 < qs - pt < \frac{1}{2}q.$$

Aus a) und b) folgt nun:

Die Zahl  $m+n$  ist genau die Anzahl der Paare  $(s, t)$  natürlicher Zahlen, für die gilt:

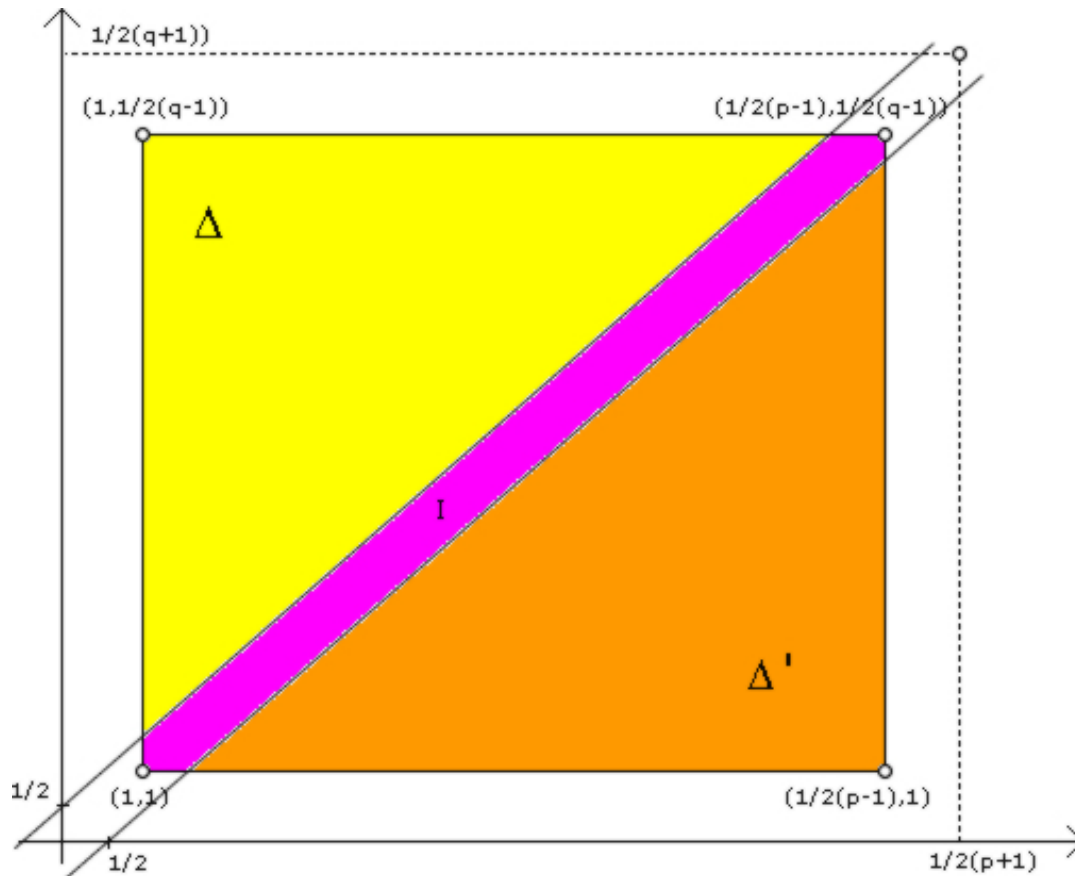
$$\text{c) } 1 \leq s \leq \frac{1}{2}(p-1), \quad 1 \leq t \leq \frac{1}{2}(q-1), \quad -\frac{1}{2}p < qs - pt < \frac{1}{2}q.$$

Zunächst ist klar, dass die  $n$  Paare, die a) erfüllen, sowie die  $m$  Paare, die b) erfüllen, jeweils den Ungleichungen c) genügen. Da jedes Zahlenpaar, welches a) erfüllt, verschieden ist von jedem Zahlenpaar, das b) erfüllt, so sehen wir, dass es mindestens  $m+n$  verschiedene Zahlenpaare gibt, für die c) gilt. Es kann aber auch außer diesen  $m+n$  Paaren kein weiteres Paar  $s', t'$  geben, für welches c) erfüllt ist, denn dann müsste notwendig gelten:  $qs' - pt' = 0$ , d.h. es wäre

$$\frac{p}{q} = \frac{s'}{t'} \quad \text{mit} \quad 1 \leq t' \leq \frac{1}{2}(q-1),$$

was nicht geht, da der Bruch  $\frac{p}{q}$  bereits reduziert ist. Mithin wird c) wie behauptet von genau  $m+n$  Paaren  $s, t$  erfüllt.

Die Ungleichungen c) besagen geometrisch, dass die Zahl  $m+n$  genau die Anzahl der Gitterpunkte (:= Punkte mit ganzzahligen Koordinaten) in der reellen  $x$ - $y$ -Ebene ist, die sowohl im abgeschlossenen Rechteck  $R$  mit vier Eckpunkten  $(1, 1); (\frac{1}{2}(p-1), 1); (\frac{1}{2}(p-1), \frac{1}{2}(q-1)); (1, \frac{1}{2}(q-1))$  als auch im Innern des von den beiden parallelen Geraden  $qx - py = -\frac{1}{2}p$  und  $qx - py = \frac{1}{2}q$  begrenzten Parallelstreifens liegen. Wir bezeichnen diese Menge mit  $I$ .



Im abgeschlossenen Rechteck  $R$  liegen genau die  $\frac{1}{2}(p-1) \cdot \frac{1}{2}(q-1)$  Gitterpunkte  $(s, t)$ , wo  $1 \leq s \leq \frac{1}{2}(p-1), 1 \leq t \leq \frac{1}{2}(q-1)$ . Nun ist  $R$  die Vereinigung der Mengen  $I$  mit den beiden abgeschlossenen Dreiecksflächen  $\Delta$  und  $\Delta'$ :

$$R = I \cup \Delta \cup \Delta'.$$

Die drei Mengen  $I, \Delta, \Delta'$  sind paarweise disjunkt. Bezeichnet daher  $\delta$  bzw.  $\delta'$  die Anzahl der Gitterpunkt in  $\Delta$  bzw.  $\Delta'$ , so folgt

$$\frac{1}{2}(p-1) \cdot \frac{1}{2}(q-1) = m + n + \delta + \delta'.$$

Wir werden nun zeigen, dass in  $\Delta$  und  $\Delta'$  gleich viele Gitterpunkte liegen, dann gilt  $\delta = \delta'$  und wir sind fertig. Das ist anschaulich sofort einleuchtend, denn  $\Delta$  und  $\Delta'$  liegen symmetrisch zum Mittelpunkt  $M$  des Rechtecks  $R$  mit den nicht notwendig ganzzahligen Koordinaten  $(\frac{p+1}{4}, \frac{q+1}{4})$ . Man sieht dies besonders deutlich aus der Figur, wenn man statt  $R$  das in jeder Koordinatenrichtung um 1 vergrößerte Rechteck

$$\{(x, y) \in \mathbb{R}^2 \mid 0 \leq x \leq \frac{1}{2}(p+1), 0 \leq y \leq \frac{1}{2}(q+1)\}$$

mit gleichem Mittelpunkt  $M$  zu Grunde legt und statt  $\Delta$  bzw.  $\Delta'$  die entsprechend vergrößerten Dreiecksflächen betrachtet. Diese Symmetrie von  $\Delta$  bzw.  $\Delta'$  erzwingt  $\delta = \delta'$ . Diese geometrische Schlussweise kann auch rechnerisch mit der Funktion

$$\sigma : \mathbb{R}^2 \rightarrow \mathbb{R}^2, \quad (x, y) \mapsto \left(\frac{1}{2}(p+1) - x, \frac{1}{2}(q+1) - y\right)$$

nachgewiesen werden. Man stellt fest, dass  $\sigma$  bijektiv ist und zu sich selbst invers.  $\square$

## IV. Das Jacobi-Symbol

Abschließend verallgemeinern wir die Definition des Legendre-Symbols auf beliebige *ungerade* Zahlen.

**0.1 Definition:** Sei  $n > 2$  eine ungerade Zahl und sei  $a \in \mathbb{Z}$ . Sei  $n = \sum_{i=1}^r p_i^{\alpha_i}$  die Primfaktorzerlegung von  $n$ , wobei  $p_i \neq p_j$  für  $j \neq i$  und  $1 \leq i, j \leq r$  gilt. Das **Jacobi-Symbol** ist definiert als

$$\left(\frac{a}{n}\right) := \left(\frac{a}{p_1}\right)^{\alpha_1} \cdot \dots \cdot \left(\frac{a}{p_r}\right)^{\alpha_r}.$$

Das Jacobi-Symbol ist nach GUSTAV CARL JACOB JACOBI (1804-1851) benannt.

Das eben entwickelte Reziprozitätsgesetz kann man zwar nicht direkt auf Jacobi-Symbole anwenden, doch auf deren Primfaktorzerlegung, denn diese sind gemäß Definition gerade Legendre-Restsymbole. Im Folgenden untersuchen wir noch grundlegende Eigenschaften des Jacobi-Symbols, das insbesondere in der Kryptographie benötigt wird.

Ist  $n$  eine Primzahl, dann stimmen Jacobi- und Legendre-Symbol überein. Ist  $n$  jedoch zusammengesetzt, dann macht das Jacobi-Symbol *keine* Aussage mehr darüber, ob  $a \bmod n$  in  $(\mathbb{Z}/n\mathbb{Z})^*$  ein quadratischer Rest ist oder nicht, obwohl wir in  $(\mathbb{Z}/n\mathbb{Z})^*$  quadratische Reste definiert haben.

**0.2 Beispiel:** Es sei  $n := 15$  und  $a := 2$ , dann ist  $\left(\frac{2}{15}\right) = \left(\frac{2}{3}\right)\left(\frac{2}{5}\right) = (-1)(-1) = 1$ , denn 2 ist ein quadratischer Nichtrest in  $(\mathbb{Z}/3\mathbb{Z})^*$  und in  $(\mathbb{Z}/5\mathbb{Z})^*$ . Allerdings ist 2 ebenfalls ein quadratischer Nichtrest in  $(\mathbb{Z}/15\mathbb{Z})^*$ , da es kein  $b \in (\mathbb{Z}/15\mathbb{Z})^*$  gibt, so dass  $b^2 \bmod 15 = 2$  gilt.

Ist also  $n > 2$  eine ungerade zusammengesetzte Zahl und  $a \in (\mathbb{Z}/n\mathbb{Z})^*$  vorgegeben. Wie wir im letzten Beispiel gezeigt haben, kann aufgrund von

$$\left(\frac{a}{n}\right) = 1 \tag{IV.1}$$

keine Aussage darüber getroffen werden, ob  $a$  ein quadratischer Rest bzw. Nichtrest in  $(\mathbb{Z}/n\mathbb{Z})^*$  ist. Mit anderen Worten: Bedingung (4.3) ist *nicht hinreichend*, wie wir aber sehen werden ist (4.3) eine *notwendige* Bedingung dafür, dass  $a$  ein quadratischer Rest ist.

**0.3 Lemma:** Sei  $n > 2$  eine ungerade und zusammengesetzt, und sei  $a \in (\mathbb{Z}/n\mathbb{Z})^*$ . Ist  $a$  ein quadratischer Rest in  $(\mathbb{Z}/n\mathbb{Z})^*$ , d.h., es gibt ein  $b \in (\mathbb{Z}/n\mathbb{Z})^*$  mit  $b^2 \bmod n = a$ , dann muss  $\left(\frac{a}{n}\right) = 1$  gelten.

*Beweis.* Sei  $n = \sum_{i=1}^r p_i^{\alpha_i}$  die Primfaktorzerlegung von  $n$ . Für  $1 \leq i \leq r$  gilt dann  $b^2 \equiv_{p_i} a$ , also ist  $a$  ein quadratischer Rest modulo  $p_i$ . Es folgt damit

$$\begin{aligned} \left(\frac{a}{n}\right) &= \left(\frac{a}{p_1}\right)^{\alpha_1} \cdots \left(\frac{a}{p_r}\right)^{\alpha_r} \\ &= 1^{\alpha_1} \cdots 1^{\alpha_r} = 1 \end{aligned}$$

□

Für das Jacobi-Symbol gelten ähnliche Eigenschaften wie für das Legendre-Symbol:

**0.4 Lemma:** Sei  $n > 2$  eine ungerade Zahl und seien  $a, b \in \mathbb{Z}$ .

(i) Gilt  $a \equiv_n b$ , dann folgt  $\left(\frac{a}{n}\right) = \left(\frac{b}{n}\right)$ .

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

(iii)  $\left(\frac{1}{n}\right) = 1$ .

*Beweis.* Sei  $n = \sum_{i=1}^r p_i^{\alpha_i}$  die Primfaktorzerlegung von  $n$ .

(i) Es gelte  $a \equiv_n b$ , dann ist  $a \equiv_{p_i} b$  für  $1 \leq i \leq r$  und

$$\begin{aligned} \left(\frac{a}{n}\right) &= \left(\frac{a}{p_1}\right)^{\alpha_1} \cdots \left(\frac{a}{p_r}\right)^{\alpha_r} \\ &= \left(\frac{b}{p_1}\right)^{\alpha_1} \cdots \left(\frac{b}{p_r}\right)^{\alpha_r} \\ &= \left(\frac{b}{n}\right) \end{aligned}$$

Mit Lemma 4.1.3 folgt damit die Behauptung.

(ii) Es gilt

$$\begin{aligned} \left(\frac{ab}{n}\right) &= \left(\frac{ab}{p_1}\right)^{\alpha_1} \cdots \left(\frac{ab}{p_r}\right)^{\alpha_r} \\ &= \left(\frac{b}{p_1}\right)^{\alpha_1} \cdots \left(\frac{b}{p_r}\right)^{\alpha_r} \left(\frac{a}{p_1}\right)^{\alpha_1} \cdots \left(\frac{a}{p_r}\right)^{\alpha_r} \\ &= \left(\frac{a}{n}\right) \left(\frac{b}{n}\right) \end{aligned}$$

und die Behauptung folgt wieder durch Anwendung von Lemma 4.1.3.

(iii) Es gilt  $\left(\frac{-1}{n}\right) = \left(\frac{-1}{p_1}\right)^{\alpha_1} \cdots \left(\frac{-1}{p_r}\right)^{\alpha_r} = 1$ , denn 1 ist immer ein quadratischer Rest.

□

## **Hinweis:**

Haben Sie einen Fehler oder eine Unstimmigkeit in diesem Dokument entdeckt?  
Falls dem so ist, dann senden Sie mir bitte eine E-Mail an [Alexander@mathematik-netz.de](mailto:Alexander@mathematik-netz.de).

*Vielen Dank!*

Weiterhin viel Spaß mit der Mathematik!

<http://www.mathematik-netz.de>  
<http://www.mathering.de>

## Literaturverzeichnis

- [1] Remmert, R. und Peter, U.; Elementare Zahlentheorie; 1995, 2. Auflage; Birkhäuser Verlag.
- [2] Bosch, S.; Algebra; 2003, fünfte Auflage; Springer Verlag.
- [3] Meyberg, K.; Algebra, Teil 1; 1979, 2. Auflage; Hanser Verlag.
- [4] Meyberg, K.; Algebra, Teil 2; 1979, 2 Auflage; Hanser Verlag.
- [5] Lang, S.; Algebra; 2004, 3. Auflage; Springer Verlag.
- [6] van der Waerden, B.L.; Algebra – Erster Teil; 1967, 5. Auflage; Springer Verlag.
- [7] van der Waerden, B.L.; Algebra – Zweiter Teil; 1966, 7. Auflage; Springer Verlag.
- [8] Scharlau, W.; Algebra I, Kurs 1312; 2004; FernUniversität in Hagen.
- [9] Hartlieb, S. und Unger, L.; Mathematische Grundlagen der Kryptografie, Kurs 1321; 2005; FernUniversität in Hagen.
- [10] Scheja, G. und Storch, U.; Lehrbuch der Algebra, Teil 1; 1993; B.G. Teubner Verlag.