Das Quadratische Reziprozitätsgesetz

Anna Sökeland, Natalie Graßmuck

26.04.2007

1 Vorbemerkungen

$3 \equiv 4^2 \bmod 13$, d.h. modulo 13 ist 3 ein Quadrat.

Definition : Sei $p \neq 2$ eine Primzahl. $x \in F_p^*$ ist Quadrat modulo p, wenn $\exists y \in F_p^*$ mit

$$x = y^2 \tag{1}$$

Frage : Welche ganze Zahlen sind modulo p Quadrate ?

2 Das Quadratische Reziprozitätsgesetz

2.1 Quadrate in F_q

Im Folgenden sei $q = p^n$, $n \in \mathrm{N}$ und p prim. Dann gilt folgender

Satz :
a) Ist $p = 2$, dann sind alle Elemente von F_q Quadrate.
b) Ist $p \neq 2$, dann gilt :

$$\#\{x \in F_q^* | \exists y \in F_q^* : y^2 = x\} \; = \; \frac{q-1}{2} \tag{2}$$

Beweis :
a) Folgt aus der Tatsache dass $f : F_{2^n} \longrightarrow F_{2^n}$ mit $f(x) = x^2$ ein Automorphismus auf F_{2^n} ist.

b) Sei Ω eine algebraische Abgeschlossenheit von F_q ; wenn $x \in F_q^*$ dann soll $y \in \Omega$, sodass $y^2 = x$.
Man hat : $y^{(q-1)} = x^{\frac{q-1}{2}} = \pm 1$ da $x^{(q-1)} = 1$.
Damit x ein Quadrat in F_q ist es notwendig und hinreichend, dass y zu F_q^* gehört, d.h. $y^{(q-1)} = 1$. Deshalb ist F_q^{*2} der Kern von $x \mapsto x^{\frac{q-1}{2}}$. D.h. also, wenn $x \in F_q^{*2}$ dann $\exists y \in F_q^*$ mit $y^2 = x$.
$x \mapsto x^{\frac{q-1}{2}} = (y^2)^{\frac{q-1}{2}} = 1 \Rightarrow x \in$ Kern.
$x \in$ Kern $\Leftrightarrow x^{\frac{q-1}{2}}$, d.h. im Kern sind die Elemente die auf 1 abgebildet werden.
Daraus folgt, das Polynom $x^{\frac{q-1}{2}} - 1$ hat höchstens $\frac{q-1}{2}$ Nullstellen

bzw. die # Elemente im Kern $\leq \frac{q-1}{2}$. (*)
Außerdem wissen wir, dass F_q^* zyklisch ist und die Ordnung $q-1$ hat.
Das bedeutet : $F_q^* := \{a, a^2, a^3, \ldots, a^{q-1}\}$, mit $a \in F_q^*$.
Man sieht, dass F_q^* mindestens $\frac{q-1}{2}$ Quadrate hat,
d.h. # Quadrate $\geq \frac{q-1}{2}$. (**)
Aus (*) und (**) $\Rightarrow \#\{x \in F_q^* | \exists y \in F_q^* : y^2 = x\}$

2.2 Legendre Symbol

Definition : Sei $p \neq 2$ und $x \in F_p^*$. Das Legendre Symbol $\left(\frac{x}{p}\right)$ ist definiert durch

$$\left(\frac{x}{p}\right) := x^{\frac{(p-1)}{2}} = \begin{cases} +1, & x \text{ ist Quadrat modulo } p \\ -1, & \text{sonst} \end{cases} \tag{3}$$

Satz 2.2.1 : Das Legendre Symbol ist multiplikativ, d.h. es gilt für $x, y \in F_p^*$:

$$\left(\frac{xy}{p}\right) = \left(\frac{x}{p}\right) \cdot \left(\frac{y}{p}\right) \tag{4}$$

Beweis :
Aus voriger Definition folgt :

$$\left(\frac{xy}{p}\right) = (xy)^{\frac{p-1}{2}} = (x)^{\frac{p-1}{2}} (y)^{\frac{p-1}{2}} = \left(\frac{x}{p}\right) \cdot \left(\frac{y}{p}\right) \tag{5}$$

2.3 Das QRG und seine Ergänzungssätze

Das Quadratische Reziprozitätsgesetz ist einer der wichtigsten Sätze der elementaren Zahlentheorie. Euler vermutete es bereits um 1740, lieferte jedoch keinen Beweis. Die vereinfachte Formulierung des QRGs stammt von Legendre, aber erst Gauß gelang der erste vollständige Beweis.

Satz 2.3.1 : Seien $l, p \neq 2$ zwei verschiedene Primzahlen. Dann gilt :

$$\left(\frac{l}{p}\right) = \left(\frac{p}{l}\right) (-1)^{\frac{l-1}{2} \cdot \frac{p-1}{2}} \tag{6}$$

Beweis :
Sei $S \subseteq F_p^*$, so dass sich F_p^* als disjunkte Vereinigung schreiben lässt :
$F_p^* = S \cup (-S)$. Im Folgenden setzen wir $S := \{1, \ldots, \frac{p-1}{2}\}$. Für $a \in F_p^*$, $s \in S$ ist auch $a \cdot s \in F_p^*$, d.h. es gibt eindeutig bestimmte Zahlen $e_s(a) \in \{+1, -1\}$ und $s_a \in S$ mit

$$a \cdot s = e_s(a) \cdot s_a \tag{7}$$

Dann gilt :

(i) **Gaußlemma :**

$$\left(\frac{a}{p}\right) = \prod_{s\in\ S} e_s(a) \tag{8}$$

Beweis von (i) :
Beh. : Die s_a sind paarweise verschieden, d.h. für $s, t \in S$ mit $s \neq t$ gilt $s_a \neq t_a$.
Denn angenommen $s_a = t_a$, dann würde gelten :

$$a^2 \cdot s^2 = s_a^2 = t_a^2 = a^2 \cdot t^2 \tag{9}$$

Mit $a \in F_p^*$ folgt $s^2 = t^2$, also $s = \pm t$. Die Behauptung ergibt sich daher nach Definition von S. Aufgrund der Endlichkeit von S und der gezeigten Injektivität der Abbildung $s \mapsto s_a$ ist diese eine Bijektion von S in sich selbst.
Zur Erinnerung :

$$a \cdot s = e_s(a) \cdot s_a \tag{10}$$

Durch Produktbildung über alle $s \in S$ liefert dies folgende Gleichung :

$$a^{\frac{p-1}{2}} \prod_{s\in\ S} s = \quad \left(\prod_{s\in\ S} e_s(a)\right) \prod_{s\in\ S} s_a = \quad \left(\prod_{s\in\ S} e_s(a)\right) \prod_{s\in\ S} s \tag{11}$$

Daher gilt (Beachte $s \in F_p^*$) :

$$a^{\frac{p-1}{2}} = \quad \prod_{s\in\ S} e_s(a) \tag{12}$$

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

(ii) **Ergänzungssätze :** Im Folgenden sei $p \neq 2$ eine Primzahl.
1.Ergänzungssatz :

$$\left(\frac{-1}{p}\right) \quad = \quad \begin{cases} +1, & p \equiv +1 \bmod 4 \\ -1, & p \equiv -1 \bmod 4 \end{cases} \tag{13}$$

Beweis :
Es gilt $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$. Die Behauptung folgt nun aus der Tatsache, dass $\frac{p-1}{2}$ gerade $\iff p \equiv +1 \bmod 4$.

2.Ergänzungssatz :

$$\left(\frac{2}{p}\right) \quad = \quad \begin{cases} +1, & p \equiv \pm 1 \bmod 8 \\ -1, & p \equiv \pm 5 \bmod 8 \end{cases} \tag{14}$$

Beweis :
Nach dem Gaußlemma gilt für $a = 2 \ \in F_p^*$:

$$\left(\frac{2}{p}\right) = \prod_{s \in \ S} e_s(2) \tag{15}$$

Betrachte $2s = e_s(2) \cdot s_2$. Für $2s \leq \frac{p-1}{2}$ ist $2s \in S$. Setze $s_2 := 2s$, dann folgt $e_s(2) = +1$. Andernfalls ist $2s \notin S$, also $2s \neq s_2$, da $s_2 \in S$. Also $e_s(2) = -1$.
Also gilt für $s \in S$:

$$e_s(2) \quad = \quad \begin{cases} +1, & s \leq \frac{p-1}{4} \\ -1, & s > \frac{p-1}{4} \end{cases} \tag{16}$$

Definiere

$$n(p) := \quad \# \left\{ s \in \mathbf{Z}, \quad \frac{p-1}{4} < s \leq \frac{p-1}{2} \right\} \tag{17}$$

Dann gilt :

$$\left(\frac{2}{p}\right) = (-1)^{n(p)} \tag{18}$$

Fallunterscheidungen :

Fall 1) $p \equiv 1 \bmod 4$, d.h. $p = 4k + 1$ für $k \in \mathbf{N}$

Dann ist $n(p) = \#\left\{s \in \mathbf{Z},\ k < s \leq 2k\right\} = 2k - k = k$.
Also gilt :

$$\left(\frac{2}{p}\right) = (-1)^k = \begin{cases} +1, & p \equiv +1 \bmod 8 \\ -1, & p \equiv +5 \bmod 8 \end{cases} \tag{19}$$

Denn für k gerade gilt : $p = 4 \cdot (2l) + 1 = 8l + 1$,
und für k ungerade gilt : $p = 4 \cdot (2l + 1) + 1 = 8l + 5$.

Fall 2) $p \equiv -1 \bmod 4$, d.h. $p = 4k + 3$ für $k \in \mathbf{N}$

Dann ist $n(p) = \#\left\{s \in \mathbf{Z},\ k + \frac{1}{2} < s \leq 2k + 1\right\} = (2k + 1) - k = k + 1$.
Also gilt :

$$\left(\frac{2}{p}\right) = (-1)^{k+1} = \begin{cases} +1, & p \equiv -1 \bmod 8 \\ -1, & p \equiv -5 \bmod 8 \end{cases} \tag{20}$$

Denn für $k + 1$ gerade, d.h. k ungerade gilt : $p = 4 \cdot (2l + 1) + 3 = 8l + 7$,

und für $k+1$ ungerade, d.h. k gerade gilt : $\qquad p = 4 \cdot (2l) + 3 = 8l + 3.$

Damit folgt die Behauptung :

$$\left(\frac{2}{p}\right) \quad = \quad \begin{cases} +1, & p \equiv \pm 1 \bmod 8 \\ -1, & p \equiv \pm 5 \bmod 8 \end{cases} \tag{21}$$

Dies ist äquivalent zu

$$\left(\frac{2}{p}\right) = (-1)^{\frac{(p+1)\cdot(p-1)}{8}} = (-1)^{\frac{p^2-1}{8}} \tag{22}$$

(iii) **Trigonometrisches Lemma**
Zum Beweis des QRGs benötigen wir folgende Identität :

$$\frac{sinmx}{sinx} = (-4)^{(m-1)/2} \prod_{1 \le j \le (m-1)/2} \left(sin^2 x - sin^2 \frac{2\pi j}{m} \right) \tag{23}$$

wobei m eine ungerade ganze Zahl ist.
Der Leser möge sich das im Buch von H.-D. Ebbinghaus et al. : Zahlen (Grundwissen Mathematik 1, Springer) veranschaulichen.

(iv) **Beweis des quadratischen Reziprozitätsgesetzes**

Seien l und p zwei verschiedene Primzahlen und $l, p \neq 2$. Sei $S = \left\{1, ..., \frac{p-1}{2}\right\}$ wie vorher.
Nach dem Gauss Lemma gilt :

$$\left(\frac{l}{p}\right) = \prod_{s \in S} e_s(l). \tag{24}$$

Nun ergibt sich aus der Gleichheit von $ls = e_s(l) s_l$:

$$sin\frac{2\pi}{p} ls = e_s(l) sin\frac{2\pi}{p} s_l \tag{25}$$

Formt man diese Gleichung um und unter Beachtung, dass $s \mapsto s_l$ eine Bijektion ist, ergibt sich folgender Ausdruck :

$$\left(\frac{l}{p}\right) = \prod_{s \in S} e_s(l) = \prod_{s \in S} sin\frac{2\pi ls}{p} / sin\frac{2\pi s}{p} \tag{26}$$

Unter Verwendung des Trigonometrischen Lemmas mit $m = l$ können wir die Gleichung auch schreiben als :

$$\begin{aligned} \left(\frac{l}{p}\right) &= \prod_{s \in S} (-4)^{(l-1)/2} \prod_{t \in T} \left(sin^2 \frac{2\pi s}{p} - sin^2 \frac{2\pi t}{l} \right) \\ &= (-4)^{(l-1)(p-1)/4} \prod_{s \in S, t \in T} \left(sin^2 \frac{2\pi s}{p} - sin^2 \frac{2\pi t}{l} \right) \end{aligned} \tag{27}$$

wobei T die Menge der ganzen Zahlen zwischen 1 und $(l-1)/2$ kennzeichnet. Vertauscht man l und p, erhält man einen ähnlichen Ausdruck :

$$\left(\frac{p}{l}\right) = (-4)^{(l-1)(p-1)/4} \prod_{s\in S, t\in T} \left(sin^2 \frac{2\pi t}{l} - sin^2 \frac{2\pi s}{p} \right) \tag{28}$$

$\left(\frac{l}{p}\right)$ und $\left(\frac{p}{l}\right)$ sind identisch bis auf ihr Vorzeichen.
Da es $\frac{1}{2}(p-1)\frac{1}{2}(l-1)$ Faktoren davon gibt, unterscheiden sich die Gleichungen nur um den Faktor $(-1)^{\frac{1}{4}(p-1)(l-1)}$, womit das quadratische Reziprozitätsgesetz bewiesen wäre.

2.4 Beispiel

$$\begin{aligned} \left(\frac{29}{43}\right) &\overset{\text{(i)}}{=} \left(\frac{43}{29}\right) \overset{\text{(ii)}}{=} \left(\frac{14}{29}\right) \overset{\text{(iii)}}{=} \left(\frac{2}{29}\right) \cdot \left(\frac{7}{29}\right) \\ &\overset{\text{(iv)}}{=} -\left(\frac{7}{29}\right) \overset{\text{(i)}}{=} -\left(\frac{29}{7}\right) \overset{\text{(ii)}}{=} -\left(\frac{1}{7}\right) \overset{\text{(v)}}{=} -1 \end{aligned} \tag{29}$$

Hierbei wurde verwendet :
(i) QRG ($29 \equiv 1 \bmod 4$)
(ii) $\left(\frac{a}{p}\right)$ ist nach Definition nur von der Restklasse a modulo p abhängig
(iii) Satz 2.2.1 Multiplikativität des Legendre Symbols
(iv) Satz 2.3.1 Teil(ii) : 2.Ergänzungssatz ($29 \equiv 5 \bmod 8$)
(v) 1 ist als Quadratzahl für jede Primzahl $p \neq 2$ Quadrat modulo p