Kapitel 3. Potenzreste, insbesondere quadratische Reste

In diesem Kapitel werden, wie schon im Vorwort zum letzten in Aussicht gestellt, die Untersuchungen über Kongruenzen fortgeführt. Wie erinnerlich wurde in § 4 von Kap. 2 eine Methode vorgestellt, die die Gewinnung sämtlicher Wurzeln eines ganzzahligen Polynoms in einer Unbestimmten nach einem natürlichen Modul m auf die Ermittlung aller Wurzeln des Polynoms modulo aller in m aufgehenden Primzahlen reduziert.

Jetzt sollen die spezielleren polynomialen Kongruenzen $X^n \equiv c \pmod{m}$ bei ganzem $n \geq 2$ und zu m teilerfremdem, ganzem c genauer auf ihre Lösbarkeit untersucht werden. Dabei ist § 1 dem allgemeinen Fall gewidmet, während der Spezialfall $n = 2$ einer sehr eingehenden Diskussion in § 2 unterzogen wird.

Zentrales Ergebnis von § 2 ist das von GAUSS gefundene quadratische Reziprozitätsgesetz mit seinen beiden Ergänzungssätzen, für das GAUSS selbst acht methodisch verschiedene Beweise geliefert hat. § 2 endet mit Anwendungen dieser Sätze auf die Fragen nach der Existenz unendlich vieler Primzahlen in gewissen arithmetischen Progressionen und nach der möglichen Form von Primfaktoren von FERMAT– bzw. MERSENNE–Zahlen. Seit längerer Zeit spielen diejenigen MERSENNE–Zahlen, die Primzahlen sind, in den aktuellen Primzahlrekordlisten eine führende Rolle.

In § 3 schließlich wird noch die Problematik angeschnitten, wie sich bei ungerader Primzahl p die $c \in \{1, 2, \ldots, p-1\}$ verteilen, für die die Kongruenz $X^2 \equiv c \pmod{p}$ lösbar ist. Die Beantwortung dieser spezielleren Fragestellung wirft als Nebenergebnis ab, daß unter den Primzahlen p genau die $p \not\equiv 3 \pmod{4}$ als Summe zweier Quadratzahlen darstellbar sind. Dies leitet dann über zu den anfangs von Kap. 4 zu besprechenden Problemen.

§ 1. Indexrechnung und Potenzreste

1. Indizes. Sei m eine natürliche Zahl, so daß es nach dem GAUSSschen Satz 2.5.5 eine Primitivwurzel a modulo m gibt. Wie in 2.5.6 festgestellt, gibt

es zu jedem ganzen c mit $(c,m) = 1$ genau ein $i = i(c) \in \{0,\dots,\varphi(m)-1\}$, so daß $a^i \equiv c \pmod m$ gilt. Offenbar sind daher $c \equiv c' \pmod m$ und $i(c) = i(c')$ miteinander gleichwertig; $i(c)$ ist also eine Invariante der ganzen, durch c repräsentierten primem Restklasse modulo m, die selbstverständlich auch noch von der gewählten Primitivwurzel a mod m abhängt. Sind a, c wie hier beschrieben, so heißt $i(c)$ der *Index von c bezüglich a*, der als $\operatorname{ind}_a c$ notiert wird.

In 2.5.1 wurde beispielsweise festgestellt, daß 3 und 5 die beiden Primitivwurzeln modulo 14 sind; nach diesem Modul sind $3^0, 3^1, \dots, 3^5$ kongruent 1, 3, 9, 13, 11, 5 bzw. $5^0, 5^1, \dots, 5^5$ kongruent 1, 5, 11, 13, 9, 3, jeweils in der angegebenen Reihenfolge. Man hat somit folgende kleine Tabelle

$c \pmod{14}$	1	3	5	9	11	13
$\operatorname{ind}_3 c$	0	1	5	2	4	3
$\operatorname{ind}_5 c$	0	5	1	4	2	3

Eine umfangreiche Indextabelle bezüglich der zu den Primzahlpotenzen unterhalb 1000 gehörigen Primitivwurzeln findet sich bereits in dem in 2.5.3 erwähnten *Canon Arithmeticus* von JACOBI. Der Begriff des Index selbst wurde bei Primzahlmoduln von GAUSS (*Disquisitiones Arithmeticae*, Art. 57ff.) eingeführt.

In der folgenden Proposition sind einige einfache Regeln für das Rechnen mit Indizes zusammengestellt.

Proposition. *Gibt es modulo $m \in \mathbb{N}$ Primitivwurzeln, ist a (und auch $\hat a$) eine solche und sind $c_1, c_2, c \in \mathbb{Z}$ zu m teilerfremd, so gilt modulo $\varphi(m)$*

(i) $\operatorname{ind}_a c_1c_2 \equiv \operatorname{ind}_a c_1 + \operatorname{ind}_a c_2$,

(ii) $\operatorname{ind}_a c^n \equiv n \operatorname{ind}_a c$ *für alle* $n \in \mathbb{N}_0$,

(iii) $\operatorname{ind}_a 1 \equiv 0, \quad \operatorname{ind}_a a \equiv 1$,

(iv) $\operatorname{ind}_{\hat a} c \equiv (\operatorname{ind}_{\hat a} a)(\operatorname{ind}_a c)$,

(v) $(\operatorname{ind}_{\hat a} a,\ \varphi(m)) = 1$.

Beweis. Ist nämlich $i_k := \operatorname{ind}_a c_k$ für $k = 1, 2$, so bedeutet dies $a^{i_k} \equiv c_k \pmod m$, also $a^{i_1+i_2} \equiv c_1c_2 \equiv a^{\operatorname{ind}_a c_1c_2} \pmod m$, woraus (i) folgt. Aus (i) ergibt sich induktiv bei $(c_k, m) = 1$ für $k = 1, \dots, n$

$$\operatorname{ind}_a \prod_{k=1}^{n} c_k \equiv \sum_{k=1}^{n} \operatorname{ind}_a c_k \pmod{\varphi(m)}$$

und (ii) folgt für $n \geq 1$ hieraus durch Spezialisierung. Die beiden Aussagen in (iii) sind klar; die erstere gibt (ii) auch für $n = 0$. Für (iv) hat man zu beachten, daß

$$\hat{a}^{\mathrm{ind}_{\hat{a}}a} \equiv a \pmod{m} \tag{1}$$

gilt, was modulo m sofort zu

$$\hat{a}^{\mathrm{ind}_{\hat{a}}c} \equiv c \equiv a^{\mathrm{ind}_a c} \equiv \hat{a}^{(\mathrm{ind}_{\hat{a}}a)(\mathrm{ind}_a c)}$$

führt; die Kongruenz der beiden Potenzen ganz außen gibt (iv). Ist $d := (\mathrm{ind}_{\hat{a}}a, \varphi(m))$, so folgt aus (1)

$$1 \equiv \hat{a}^{\varphi(m)(\mathrm{ind}_{\hat{a}}a)/d} \equiv a^{\varphi(m)/d} \pmod{m};$$

da a Primitivwurzel modulo m ist, muß $d = 1$ sein, und das ist (v). □

Bemerkungen. 1) Betrachtet man nochmals obiges Beispiel mit $m = 14$ und setzt $a = 3$, $\hat{a} = 5$, so ist $\mathrm{ind}_5 c \equiv 5\,\mathrm{ind}_3 c \equiv -\mathrm{ind}_3 c \pmod 6$ für $(c, 14) = 1$; dies zeigt gerade, wie die dritte Zeile der obigen Tabelle aus der zweiten hervorgeht.

2) Die Regeln der Proposition erinnern stark an die geläufigen Rechenregeln für Logarithmen, z.B. (iv) an die Umrechnung von Logarithmen zu verschiedenen Basen. Weiter ist bei festen m und a die Abbildung ind_a der primen Restklassengruppe modulo m auf die additive Gruppe des Restklassenrings modulo $\varphi(m)$ ein Isomorphismus; die Homomorphieeigenschaft von ind_a steht gerade in (i).

2. Ein Beispiel. Die in Proposition 1 zusammengestellten Regeln für das Rechnen mit Indizes sollen nun benutzt werden, um an einem Beispiel zu zeigen, wie man damit gewisse Typen von polynomialen Kongruenzen behandeln kann. Sei etwa die Kongruenz

$$9X^5 \equiv 11 \pmod{14} \tag{1}$$

vorgelegt. Falls sie eine ganzzahlige Lösung x besitzt, ist offenbar $(x, 14) = 1$. Weiter muß, wenn man etwa mit der Primitivwurzel 3 modulo 14 argumentiert, die Gleichung $\mathrm{ind}_3 9x^5 = \mathrm{ind}_3 11$ gelten. Daraus folgt mittels (i), (ii) der Proposition $\mathrm{ind}_3 9 + 5\,\mathrm{ind}_3 x \equiv \mathrm{ind}_3 11 \pmod 6$; entnimmt man $\mathrm{ind}_3 9$, $\mathrm{ind}_3 11$ der Tabelle aus 1, so ist die letzte Kongruenz zu $5\ \mathrm{ind}_3 x \equiv 2 \pmod 6$ äquivalent, woraus $\mathrm{ind}_3 x = 4$ und $x \equiv 11 \pmod{14}$ folgt. Umgekehrt lösen diese x die Kongruenz (1). Arbeitet man anstelle von 3 mit 5 als Primitivwurzel modulo 14, so ergibt sich dasselbe Endresultat, da sich alle Kongruenzen für die Indizes bezüglich 3

bzw. 5 nur um den zu $\varphi(14) = 6$ teilerfremden Faktor $\mathrm{ind}_5 3 = 5$ unterscheiden (vgl. (iv) und (v) der Proposition).

3. n–te Potenzreste, quadratische Reste und Nichtreste. Sind $m, n \in \mathbb{N}$, $c \in \mathbb{Z}$, so sollen im weiteren die speziellen polynomialen Kongruenzen

$$X^n \equiv c \pmod{m} \tag{1}$$

untersucht werden. Ist $(c, m) = 1$ und (1) lösbar, so heißt c *n–ter Potenzrest modulo* m. Ist $(c, m) = 1$, so heißt c *quadratischer Rest modulo* m, falls (1) im Spezialfall $n = 2$ lösbar ist; ist jedoch (1) unter denselben Bedingungen an c, m, n unlösbar, so heißt c *quadratischer Nichtrest modulo* m. Die zu m nicht teilerfremden c werden hier nicht klassifiziert.

Beispiel. Da 2(1) zu $X^5 \equiv 9 \pmod{14}$ äquivalent ist, hat das Beispiel in 2 insbesondere gezeigt, daß 9 ein fünfter Potenzrest modulo 14 ist.

4. Kriterium für n–te Potenzreste. Der folgende Satz enthält ein einfaches Kriterium zur Entscheidung der Lösbarkeit von 3(1) im Falle solcher Moduln m, zu denen es Primitivwurzeln gibt.

Satz. *Seien $m, n \in \mathbb{N}$, $c \in \mathbb{Z}$, $(c, m) = 1$, $d := (n, \varphi(m))$ und modulo m gebe es eine Primitivwurzel. Dann sind folgende Aussagen äquivalent:*

(i) *c ist n–ter Potenzrest modulo m.*

(ii) *Es ist $c^{\varphi(m)/d} \equiv 1 \pmod{m}$.*

(iii) *d teilt $\mathrm{ind}_a c$ für alle Primitivwurzeln a modulo m.*

Trifft eine dieser Aussagen zu, so hat 3(1) genau d modulo m inkongruente Lösungen.

Beweis. (i) $\Rightarrow$ (ii): Nach Voraussetzung gibt es ein 3(1) lösendes $x \in \mathbb{Z}$ und wegen $(c, m) = 1$ ist auch $(x, m) = 1$. Wegen $n/d \in \mathbb{N}$ hat man nach dem FERMAT–EULERschen Satz 2.3.4

$$c^{\varphi(m)/d} \equiv (x^{\varphi(m)})^{n/d} \equiv 1 \pmod{m}.$$

(ii) $\Rightarrow$ (iii): Ist a irgendeine Primitivwurzel modulo m, so ergibt Proposition 1(ii), (iii) die Teilbarkeitsbeziehung $\varphi(m) | \frac{\varphi(m)}{d} \mathrm{ind}_a c$, also $d | \mathrm{ind}_a c$.

(iii) $\Rightarrow$ (i): Sei a eine beliebige Primitivwurzel modulo m; nach Satz 2.1.5 ist die lineare Kongruenz $nY \equiv \mathrm{ind}_a c \pmod{\varphi(m)}$ lösbar und besitzt genau d modulo

$\varphi(m)$ inkongruente Lösungen $y_1, \ldots, y_d \in \{0, \ldots, \varphi(m) - 1\}$. Setzt man nun $x_\delta := a^{y_\delta}$, so sind die $x_1, \ldots, x_d$ modulo m inkongruent und erfüllen

$$x_\delta^n = a^{ny_\delta} \equiv a^{\operatorname{ind}_a c} \equiv c \pmod{m}.$$

Somit hat 3(1) mindestens die modulo m inkongruenten Lösungen $x_1, \ldots, x_d$ und (i) gilt.

Erfüllt umgekehrt ein ganzzahliges x die Kongruenz 3(1), so gilt nach Proposition 1(ii)

$$n \operatorname{ind}_a x \equiv \operatorname{ind}_a c \pmod{\varphi(m)}.$$

Nach den vorherigen Überlegungen muß dann aber $\operatorname{ind}_a x$ gleich einem der y_δ sein, also x kongruent dem entsprechenden x_δ modulo m. □

Bemerkung. Für Primzahlen m war die Äquivalenz von (i) und (ii) bereits EULER bekannt.

5. Folgerungen aus dem Kriterium. Aus Satz 4 werden in diesem und dem nächsten Abschnitt einige interessante und wichtige Konsequenzen abgeleitet.

Korollar A. *Seien $m, n \in \mathbb{N}$ so gewählt, daß es modulo m Primitivwurzeln gibt und daß $(n, \varphi(m)) = 1$ gilt. Bilden dann $x_1, \ldots, x_{\varphi(m)}$ ein primes Restsystem modulo m, so gilt dies auch für $x_1^n, \ldots, x_{\varphi(m)}^n$.*

Beweis. Zunächst sind alle x_j^n zu m teilerfremd, da dies für die x_j zutrifft. Wegen $(n, \varphi(m)) = 1$ und dem FERMAT–EULERschen Satz ist Bedingung (ii) von Satz 4 für jedes zu m teilerfremde ganze c erfüllt und daher ist 3(1) für jedes dieser c modulo m eindeutig lösbar, woraus die Behauptung folgt. □

Eine unmittelbare Konsequenz aus der Äquivalenz (i) $\Leftrightarrow$ (iii) des Satzes 4 ist folgendes

Korollar B. *Genügen m, n, c, d den Bedingungen von Satz 4, so gilt: c ist n–ter Potenzrest modulo m genau dann, wenn c bei beliebig gewählter Primitivwurzel a modulo m einer der durch a^{jd}, $j = 1, \ldots, \varphi(m)/d$, bestimmten primen Restklassen modulo m angehört.*

Korollar C. *Modulo einer ungeraden Primzahl p gibt es $\frac{1}{2}(p-1)$ quadratische Reste und ebensoviele quadratische Nichtreste.*

Beweis. Sei c ganz und nicht durch p teilbar. Nach Korollar B ist c quadratischer Rest modulo p genau dann, wenn c modulo p kongruent einer der Zahlen $a^2, a^4, \ldots, a^{p-1}$ ist, a eine beliebig gewählte Primitivwurzel modulo p. Demnach ist c quadratischer Nichtrest modulo p genau für $c \equiv a, a^3, \ldots, a^{p-2} \pmod{p}$. □

Bemerkung. Ist m wieder gleich einer ungeraden Primzahl p und ist $n = 2$, so hat man $d = 2$ in Satz 4 und für $c \equiv -1 \pmod{p}$ lautet die Kongruenz in (ii) jenes Satzes $(-1)^{(p-1)/2} \equiv 1 \pmod{p}$, was mit $p \equiv 1 \pmod 4$ äquivalent ist. Genau für diese ungeraden p ist also die quadratische Kongruenz $X^2 \equiv -1 \pmod{p}$ lösbar. Damit hat man einen weiteren Beweis für den wesentlichen Teil von Satz 2.3.9.

6. n-te Potenzreste, Modulzerlegung in Primzahlpotenzen. Wenn man *sämtliche* modulo m inkongruenten Lösungen von

$$X^n \equiv c \pmod{m} \tag{1}$$

explizit ermitteln will, so kann man dazu selbstverständlich das in den Sätzen 2.4.2 und 2.4.4 beschriebene Reduktionsverfahren auf das spezielle Polynom $f = X^n - c$ anwenden. Will man jedoch *nur* entscheiden, ob ein zu m teilerfremdes c ein n–ter Potenzrest ist oder nicht, so kann man dafür notwendige und hinreichende Bedingungen folgendem Satz entnehmen.

Satz. *Sind $m, n \in \mathbb{N}$, $c \in \mathbb{Z}$, $(c, m) = 1$ und ist $2^{\alpha_0} \prod_{\kappa=1}^{k} p_\kappa^{\alpha_\kappa}$ mit $\alpha_0 \in \mathbb{N}_0$, $\alpha_1, \ldots, \alpha_k \in \mathbb{N}$ die kanonische Zerlegung von m, so ist das Bestehen folgender Kongruenzen notwendig und hinreichend dafür, daß c ein n–ter Potenzrest modulo m ist:*

$$c^{\varphi(q_\kappa)/(n, \varphi(q_\kappa))} \equiv 1 \pmod{q_\kappa} \tag{2}$$

für $\kappa = 0, \ldots, k$, falls $\alpha_0 \leq 2$; dabei ist $q_\kappa := p_\kappa^{\alpha_\kappa}$, $p_0 := 2$. Ist jedoch $\alpha_0 > 2$, so ist (2) nur für $\kappa = 1, \ldots, k$ zu fordern, dafür müssen aber zusätzlich die beiden Kongruenzen

$$nI \equiv i \pmod 2, \qquad nJ \equiv j \pmod{2^{\alpha_0 - 2}} \tag{3}$$

lösbar sein, wobei i bzw. j modulo 2 bzw. $2^{\alpha_0 - 2}$ eindeutig bestimmt sind derart, daß bei festem $u \equiv \pm 3 \pmod 8$ gilt

$$c \equiv (-1)^i u^j \pmod{2^{\alpha_0}}. \tag{4}$$

Beweis. Offenbar ist c ein n–ter Potenzrest modulo m genau dann, wenn c ein n–ter Potenzrest modulo q_κ für $\kappa = 0, \ldots, k$ ist. Wegen $(c, q_\kappa) = 1$ und weil es Primitivwurzeln modulo q_κ gibt, ist die letzte Bedingung nach Satz 4(ii) äquivalent mit (2) und zwar für $\kappa = 1, \ldots, k$ stets, für $\kappa = 0$ nur dann, wenn $\alpha_0 \leq 2$, vgl. den GAUSSschen Satz 2.5.5 über die Existenz von Primitivwurzeln.

Ist aber $\alpha_0 > 2$, so kann man sich auf Korollar 2.5.6 stützen, um zu entscheiden, ob das (nun sicher ungerade) c ein n–ter Potenzrest modulo 2^{α_0} ist: Ist u wie im Satz vorgegeben, bestimmt man i, j gemäß (4) nach dem Korollar 2.5.6 und genügt ein ganzes x der Kongruenz $x^n \equiv c \pmod{2^{\alpha_0}}$, so ist x ungerade und analog zu (4) darstellbar in der Form

$$x \equiv (-1)^I u^J \pmod{2^{\alpha_0}} \tag{5}$$

mit modulo 2 bzw. $2^{\alpha_0 - 2}$ eindeutig bestimmten I, J. Daher müssen die beiden Kongruenzen (3) gelten. Sind umgekehrt die Kongruenzen (3) für I, J lösbar und definiert man x durch (5), so ist $x^n \equiv c \pmod{2^{\alpha_0}}$. □

Nach den letzten Feststellungen im Beweis ist ein ungerades c genau dann n–ter Potenzrest modulo 2^{α_0} mit $\alpha_0 > 2$, wenn (3) für I, J lösbar ist. Daraus folgt die erste Aussage im nachstehenden

Korollar. *Seien $n, \alpha_0 \in \mathbb{N}$, $\alpha_0 > 2$ und $c \in \mathbb{Z}$ ungerade. Ist n ungerade, so ist c ein n–ter Potenzrest modulo 2^{α_0}. Sei jetzt n gerade. Ist $c \not\equiv 1 \pmod 8$, so ist es nicht n–ter Potenzrest modulo 2^{α_0}; ist $c \equiv 1 \pmod 8$, so ist es n–ter Potenzrest modulo 2^{α_0} genau dann, wenn $(n, 2^{\alpha_0 - 2}) | j$ für j wie im Satz gilt.*

Beweis. Bei geradem n ist $x^n \equiv 1 \pmod 8$ für jedes ungerade ganze x, weshalb bei $c \not\equiv 1 \pmod 8$ sicher $x^n \not\equiv c$ modulo 8, erst recht also modulo 2^{α_0}, für alle genannten x gilt. Ist $c \equiv 1 \pmod 8$, so sind in (4) beide i, j gerade und daher ist in (3) die erste Kongruenz (für I) lösbar; die zweite (für J) ist lösbar genau für $(n, 2^{\alpha_0 - 2}) | j$. □

Bemerkung. Wegen $(2, 2^{\alpha_0 - 2}) | j$ kann aus der letzten Feststellung gefolgert werden: *Eine ungerade ganze Zahl c ist quadratischer Rest bzw. Nichtrest modulo 2^{α_0}, $\alpha_0 > 2$, je nachdem, ob $c \equiv 1$ bzw. $\not\equiv 1 \pmod 8$ gilt.*

§ 2. Quadratische Reste

1. Quadratische Kongruenzen und quadratische Reste. Während im vorigen Paragraphen allgemein n–te Potenzreste behandelt wurden, wird in diesem der Spezialfall $n = 2$ genauer diskutiert. Es ist plausibel, daß in diesem

Fall der quadratischen Reste die Theorie weiter entwickelt ist als im allgemeinen Fall.

Zunächst jedoch soll in diesem ersten Abschnitt der Zusammenhang zwischen der Frage nach der Existenz von Wurzeln quadratischer Polynome nach Moduln und zwischen quadratischen Resten geklärt werden.

Sei dazu $m'' \in \mathbb{N}$ und $f \in \mathbb{Z}[Z]$, $\partial(f) = 2$, etwa $f(Z) = rZ^2 + sZ + t$, wobei man o.B.d.A. $r \in \mathbb{N}$ voraussetzen darf. Quadratische Ergänzung zeigt, daß $f(Z) \equiv 0 \pmod{m''}$ genau dann lösbar ist, wenn

$$(2rZ + s)^2 \equiv s^2 - 4rt \pmod{4rm''}$$

lösbar ist. Setzt man noch $c' := s^2 - 4rt$, $m' := 4rm''$, so hat man folgende

Proposition A. *Löst $y \in \mathbb{Z}$ die Kongruenz*

$$Y^2 \equiv c' \pmod{m'} \tag{1}$$

und ist $y \equiv s \pmod{2r}$, so ist $z := \frac{y-s}{2r}$ ganz und Wurzel von f modulo m''. Ist umgekehrt ein ganzes z Wurzel von f modulo m'', so löst $y := 2rz + s$ die Kongruenz (1) und es ist $y \equiv s \pmod{2r}$.

In dem hier präzisierten Sinne ist die Frage nach der Existenz von Wurzeln von f modulo m'' äquivalent mit der Frage nach der Lösbarkeit der speziellen quadratischen Kongruenz (1). Diese letzte Kongruenz ist vom Typ 1.6(1) mit $n = 2$; allerdings werden im allgemeinen c' und m' nicht teilerfremd sein. Wie man die Frage nach der Lösbarkeit von (1) dennoch auf den teilerfremden Fall reduzieren kann, soll nun besprochen werden. Dazu ist es bequem, noch folgende Definition zu vereinbaren: Ist $d \in \mathbb{N}$, $d = \prod_p p^{\nu_p(d)}$, so heißt $\prod_{\substack{p \\ \nu_p(d)\ ungerade}} p$ der *quadratfreie Kern von d.* Beispielsweise ist $3 \cdot 7$ der quadratfreie Kern von $2^8 \cdot 3^{11} \cdot 5^6 \cdot 7$. (Vorsicht! Manche Autoren nennen $\prod_{\substack{p \\ \nu_p(d)>0}} p$ den quadratfreien Kern von d.)

Proposition B. *Sind c', m' wie in Proposition A, ist b der quadratfreie Kern von $d := (c', m')$ und setzt man $e := c'/d$, $m := m'/d$, so gilt: Die Kongruenz (1) ist lösbar genau dann, wenn $(b, m) = 1$ gilt und be quadratischer Rest modulo m ist.*

Beweis. Ist nämlich (1) lösbar und $y \in \mathbb{Z}$ eine solche Lösung, so gilt $d|y^2$; wegen der Definition von b ist $d = a^2 b$ bei geeignetem $a \in \mathbb{N}$, also $a|y$. Setzt man

$x := y/a$, so ist $x^2 \equiv be \pmod{bm}$ und also auch $x^2 \equiv be \pmod{m}$. Dabei ist $(b, m) = 1$, somit ebenfalls $(be, m) = 1$. Denn wäre p eine b und m teilende Primzahl, so wäre $p|x$ und also wegen $x^2 \equiv be \pmod{bm}$ auch $p^2|be$; wegen $p \not| e$ wäre dann aber b durch p^2 teilbar und somit nicht quadratfrei.

Ist umgekehrt be quadratischer Rest modulo m und gilt $(b, m) = 1$, so gibt es ein ganzes x mit $x^2 \equiv be \pmod{m}$ und dazu auch ein ganzes y mit $by \equiv x \pmod{m}$. Damit hat man $by^2 \equiv e \pmod{m}$ und also $(aby)^2 \equiv de \pmod{dm}$, d.h. die Kongruenz (1) ist lösbar. □

2. Kriterium für quadratische Reste. Die Frage, wann bei ganzen, zueinander teilerfremden $m > 0$ und c die Kongruenz

$$X^2 \equiv c \pmod{m} \tag{1}$$

lösbar ist oder nicht, wann also c quadratischer Rest oder Nichtrest modulo m ist, wird nun weiter untersucht.

Satz. *Seien $m \in \mathbb{N}$, $c \in \mathbb{Z}$, $(c, m) = 1$ und sei $2^{\alpha_0} \prod_{\kappa=1}^{k} p_\kappa^{\alpha_\kappa}$ wie in Satz 1.6 die kanonische Zerlegung von m. Es ist (1) lösbar genau dann, wenn c quadratischer Rest modulo p_κ für $\kappa = 1, \ldots, k$ ist und gilt*

$$c \equiv 1 \quad \left(\mathrm{mod}\ 2^{\mathrm{Min}(\alpha_0, 3)}\right). \tag{2}$$

Beweis. Es werde (1) von $x \in \mathbb{Z}$ gelöst. Daher gilt $x^2 \equiv c \pmod{p_\kappa}$ für $\kappa = 1, \ldots, k$ und im Falle $\alpha_0 \geq 1$ ist c wegen $(c, m) = 1$ ungerade; dann ist wegen (1) auch x ungerade, also $x^2 \equiv 1 \pmod 8$ und man hat (2).

Für die Umkehrung beachtet man folgendes: Ist $\alpha_0 \geq 3$, so hat man $c \equiv 1 \pmod 8$ nach (2); nach der Bemerkung am Ende von 1.6 ist c quadratischer Rest modulo 2^{α_0}. Ist jedoch α_0 gleich 0, 1 oder 2, so gilt $c \equiv 1 \pmod{2^{\alpha_0}}$ nach (2) und so ist c auch hier quadratischer Rest modulo 2^{α_0}. Da weiter c quadratischer Rest modulo p_κ für $\kappa = 1, \ldots, k$ ist, liefert die Implikation (i) $\Rightarrow$ (ii) von Satz 1.4 die Kongruenzen $c^{(p_\kappa - 1)/2} \equiv 1 \pmod{p_\kappa}$, was induktiv leicht zu $c^{(p_\kappa - 1)p_\kappa^{\alpha_\kappa - 1}/2} \equiv 1 \pmod{p_\kappa^{\alpha_\kappa}}$ führt. (Dies ist übrigens wieder (2) in Satz 1.6.) Die Implikation (ii) $\Rightarrow$(i) von Satz 1.4 zeigt nun, daß c quadratischer Rest modulo $p_\kappa^{\alpha_\kappa}$ ist, insgesamt jetzt sogar für $\kappa = 0, 1, \ldots, k$ ($p_0 := 2$) und man hat die Lösbarkeit von (1). (Stillschweigend wurde hier der Gaußsche Satz 2.5.5 berücksichtigt: Modulo $p_\kappa, p_\kappa^2, \ldots$ gibt es Primitivwurzeln, wenn $\kappa = 1, \ldots, k$.)
□

Bemerkungen. 1) Die zuletzt bewiesene Tatsache, daß für ungerade, c nicht teilende Primzahlen p aus der Lösbarkeit von $X^2 \equiv c \pmod{p}$ diejenige von $X^2 \equiv c \pmod{p^\alpha}$ für alle $\alpha \in \mathbb{N}$ folgt, kann auch mit Satz 2.4.4 anstatt unter Rückgriff auf Satz 1.4 eingesehen werden: Wendet man (ii) des erstgenannten Satzes nämlich mit $f(X) := X^2 - c$, $a = 2$ und einer Wurzel y_1 von f modulo p an, so ist $p \nmid f'(y_1) = 2y_1$ und also hat f modulo p^2 eine Wurzel y_2 mit $p \nmid y_2$. Induktiv stellt man fest, daß f modulo p^α eine Wurzel y_α mit $p \nmid y_\alpha$ hat, was wieder genau besagt, daß c quadratischer Rest modulo p^α ist.

2) In den ersten Abschnitten dieses Paragraphen zeigte sich insbesondere, wie die Lösbarkeit quadratischer Kongruenzen zusammenhängt mit der Frage, ob eine ganze Zahl quadratischer Rest oder Nichtrest modulo einer ungeraden Primzahl ist. In 6 (vgl. auch die Anwendungen in 8 bis 12) werden überaus wirkungsvolle Hilfsmittel zur Entscheidung dieser Frage vorgestellt; die Ausführungen in 3 bis 5 haben mehr vorbereitenden Charakter.

3. Das Legendre–Symbol. Ist c ganz, aber nicht durch die ungerade Primzahl p teilbar, so setzt man nach dem Vorgang von Legendre (*Essai sur la Théorie des Nombres*, 1798)

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

Dieses $\left(\frac{c}{p}\right)$ heißt Legendre–*Symbol*; man liest es als *c nach p*. Eine erste Zusammenstellung wichtiger Eigenschaften des Legendre–Symbols findet sich im folgenden

Satz. *Für $c, c' \in \mathbb{Z}$ und Primzahlen p mit $p \nmid 2cc'$ gilt:*

(i) $\quad c \equiv c' \pmod{p} \Rightarrow \left(\frac{c}{p}\right) = \left(\frac{c'}{p}\right)$,

(ii) $\quad \left(\frac{cc'}{p}\right) = \left(\frac{c}{p}\right)\left(\frac{c'}{p}\right)$,

(iii) $\quad \left(\frac{c}{p}\right) = (-1)^{\operatorname{ind}_a c}$ *für alle Primitivwurzeln a modulo p,*

(iv) $\quad \sum_{c=1}^{p-1} \left(\frac{c}{p}\right) = 0.$

Beweis. (i): Nach Voraussetzung sind hier ja c, c' gleichzeitig quadratischer Rest oder Nichtrest modulo p und so folgt die Behauptung direkt aus der Definition des Legendre–Symbols.

(iii): Nach (i) $\Leftrightarrow$ (iii) von Satz 1.4 ist $(\frac{c}{p}) = 1$ genau dann, wenn $\mathrm{ind}_a c$ gerade ist (für alle Primitivwurzeln a modulo p).

(ii) ist nun wegen Proposition 1.1(i) und dem soeben gezeigten (iii) einsichtig, man beachte die Geradheit von $\varphi(p) = p - 1$.

(iv) ist die Kurzfassung von Korollar 1.5C. □

Bemerkungen. 1) Regel (ii) wird bisweilen in der folgenden lässigen Form zitiert: Rest mal Rest und Nichtrest mal Nichtrest ergibt Rest; Nichtrest mal Rest ergibt Nichtrest. Generell bringt die Einführung des LEGENDRE–Symbols offenbar den Vorteil, daß man mit dem quadratischen Restverhalten ganzer Zahlen modulo ungerader Primzahlen richtiggehend *rechnen* kann. In diesem Zusammenhang sei darauf hingewiesen, daß noch GAUSS in seinen *Disquisitiones Arithmeticae* cRp bzw. cNp notierte, wenn c quadratischer Rest bzw. Nichtrest modulo p ist.

2) Manchmal ist es zweckmäßig, das LEGENDRE–Symbol $(\frac{c}{p})$ unter der alleinigen Voraussetzung zu definieren, daß p eine ungerade Primzahl ist: Für $p \not| c$ geschieht dies dann genau wie oben, während man für $p|c$ zusätzlich $(\frac{c}{p}) := 0$ festsetzt. Man prüft unmittelbar nach, daß (i) und (ii) des Satzes bei dieser erweiterten Definition gültig bleiben; dies trifft auch für (iv) zu, wo jetzt die Summation über c wahlweise von 0 bzw. von 1 bis $p - 1$ erstreckt ist.

4. Eulers Kriterium. Hier wird eine notwendige und hinreichende Bedingung dafür angegeben, daß eine ganze nicht durch die ungerade Primzahl p teilbare Zahl c quadratischer Rest modulo p ist. Dies Kriterium wurde von EULER (Opera Omnia Ser. 1, II, 493–518) mit Beweis um 1760 herum publiziert, nachdem er es schon gut zehn Jahre früher angekündigt hatte (Opera Omnia Ser. 1, II, 62–85).

Satz. *Für ganze c und ungerade Primzahlen p mit $p \not| c$ gilt* $c^{(p-1)/2} \equiv (\frac{c}{p}) \pmod{p}$.

Beweis. Bei $(\frac{c}{p}) = 1$ folgt aus (i) $\Rightarrow$ (ii) von Satz 1.4 die Kongruenz $c^{(p-1)/2} \equiv 1 \pmod{p}$, insgesamt also die behauptete Kongruenz. Ist $(\frac{c}{p}) = -1$, so liefert (ii) $\Rightarrow$ (i) des zitierten Satzes $c^{(p-1)/2} \not\equiv 1 \pmod{p}$; da jedoch nach dem FERMAT–EULERschen Satz 2.3.4 gilt

$$p|(c^{p-1} - 1) = (c^{(p-1)/2} + 1)(c^{(p-1)/2} - 1) \ ,$$

muß die Kongruenz $c^{(p-1)/2} \equiv -1 \pmod{p}$ bestehen. Somit gilt die behauptete Kongruenz auch in diesem Fall. □

In Art. 106 seiner *Disquisitiones Arithmeticae* stellt GAUSS seinem eigenen Beweis des EULERschen Kriteriums die Bemerkung voran, daß es "in praxi nullum fere usum habeat", aber dennoch "propter simplicitatem atque generalitatem memoratu dignum est". Warum es praktisch fast keinen Nutzen habe, erläutert er ein paar Zeilen später: " ... quoties numeri examinandi mediocriter sunt magni, hoc criterium ob calculi immensitatem prorsus inutile erit."

Mittels dieses vor allem für theoretische Zwecke geeigneten Kriteriums soll hier ein weiterer Beweis für Satz 3(ii) gegeben werden:

Sind nämlich die dortigen Voraussetzungen erfüllt, so ist nach EULERs Kriterium die Differenz $(\frac{cc'}{p}) - (\frac{c}{p})(\frac{c'}{p})$ eine durch p teilbare ganze Zahl; nach Definition des LEGENDRE–Symbols ist diese Differenz aber gleich -2, 0 oder 2, woraus die Behauptung schon folgt. □

Bemerkung. Erweitert man die Definition des LEGENDRE–Symbols wie in Bemerkung 2 zu 3 angegeben, so ist das EULER–Kriterium für *alle* ganzen c gültig, wenn nur p eine ungerade Primzahl ist.

5. Gauss'sches Lemma. In diesem Abschnitt wird ein weiteres notwendiges und hinreichendes Kriterium für quadratisches Restverhalten modulo ungerader Primzahlen vorgestellt, welches auf GAUSS (Werke II, S. 4ff.) zurückgeht. Dies Kriterium wird dann in 7 zum Beweis des in 6 zu formulierenden zentralen Ergebnisses dieses Paragraphen benutzt.

Folgende Bezeichnungsweise ist bei festem $m \in \mathbb{N}$ zweckmäßig: Jedem ganzen c werde dasjenige r aus dem absolut kleinsten Restsystem S_m^* modulo m (vgl. Ende von 2.1.4) zugeordnet, für das $r \equiv c \pmod m$ gilt; für r werde ausführlicher $r_m(c)$ geschrieben. Dann hat man folgendes

Gauss'sche Lemma. *Ist c ganz, p eine ungerade, nicht in c aufgehende Primzahl und $\mu_p(c) := \#\{j \in \mathbb{N} : j \le \frac{1}{2}(p-1),\ r_p(jc) < 0\}$, so gilt*

$$(\frac{c}{p}) = (-1)^{\mu_p(c)}.$$

Beweis. Gilt nämlich $|r_p(jc)| = |r_p(j'c)|$ für $j, j' \in \{1, \dots, \frac{1}{2}(p-1)\}$, so ist $r_p(jc) = r_p(j'c)$ oder $r_p(jc) = -r_p(j'c)$, also $p|(j-j')c$ oder $p|(j+j')c$. Wegen $0 < j + j' < p$ und $p \not| c$ ist hier die zweite Alternative unmöglich und man hat $p|(j-j')$, d.h. $j = j'$. Mit Rücksicht auf $p \not| jc$ für alle zugelassenen j sind sämtliche $|r_p(jc)|$ aus $\{1, \dots, \frac{1}{2}(p-1)\}$ und so stimmen diese $\frac{1}{2}(p-1)$

Zahlen in irgendeiner Reihenfolge mit den Zahlen $1, \dots, \frac{1}{2}(p-1)$ überein. Wegen $r_p(jc) = -|r_p(jc)|$ genau für $r_p(jc) < 0$ hat man, jeweils modulo p

$$\big(\frac{p-1}{2}\big)!\,c^{(p-1)/2} \equiv \prod_{j=1}^{(p-1)/2} jc \equiv (-1)^{\mu_p(c)} \prod_{j=1}^{(p-1)/2} |r_p(jc)| = (-1)^{\mu_p(c)}\big(\frac{p-1}{2}\big)!\ ,$$

also $c^{(p-1)/2} \equiv (-1)^{\mu_p(c)}$. Das EULER–Kriterium 4 führt dann zu $(\frac{c}{p}) \equiv (-1)^{\mu_p(c)}$ (mod p) und damit zur behaupteten Gleichung, da in der letzten Kongruenz beide Seiten nur der Werte 1 und -1 fähig sind. □

Bemerkung. Kombiniert man das GAUSSsche Lemma mit Satz 3(iii), so kann man bei $p \not| 2c$ sagen: Für alle Primitivwurzeln a modulo p sind $\mathrm{ind}_a c \equiv \mu_p(c)$ (mod 2), d.h. $\mathrm{ind}_a c$ und $\mu_p(c)$ haben dieselbe Parität.

6. Quadratisches Reziprozitätsgesetz, Ergänzungssätze. Sind c und p wie zuletzt im GAUSSschen Lemma vorausgesetzt, so soll nun das LEGENDRE–Symbol $(\frac{c}{p})$ berechnet werden; diese Aufgabe wird mit Hilfe der Ergebnisse der letzten drei Abschnitte entscheidend weiter reduziert. Ist nämlich $c \in \mathbb{N}$ und

$$2^{\beta_0} \prod_{\lambda=1}^{\ell} q_\lambda^{\beta_\lambda} \tag{1}$$

seine kanonische Zerlegung mit $\beta_0 \in \mathbb{N}_0$, $\beta_1, \dots, \beta_\ell \in \mathbb{N}$ und paarweise verschiedenen ungeraden Primzahlen $q_1, \dots, q_\ell$ (alle $\neq p$), so gilt aufgrund der eventuell mehrfach angewandten Multiplikativitätseigenschaft aus Satz 3(ii)

$$(\frac{c}{p}) = \prod_{\lambda=0}^{\ell} (\frac{q_\lambda}{p})^{\beta_\lambda} \tag{2}$$

mit $q_0 := 2$. Ist aber $-c \in \mathbb{N}$ und (1) seine kanonische Zerlegung, so ist $(\frac{-c}{p}) = (\frac{-1}{p})(\frac{c}{p})$ gleich der rechten Seite von (2) und somit wegen $(\frac{-1}{p})^2 = 1$

$$(\frac{c}{p}) = (\frac{-1}{p}) \prod_{\lambda=0}^{\ell} (\frac{q_\lambda}{p})^{\beta_\lambda}.$$

Daher reicht es, für ungerade Primzahlen p die speziellen LEGENDRE–Symbole $(\frac{-1}{p})$, $(\frac{2}{p})$ sowie $(\frac{q}{p})$ für ungerade, von p verschiedene Primzahlen q zu berechnen. Den Wert der ersten beiden Symbole entnimmt man dem

1. bzw. 2. Ergänzungssatz zum quadratischen Reziprozitätsgesetz. *Für ungerade Primzahlen p ist*

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

Also ist -1 quadratischer Rest modulo p genau für $p \equiv 1 \pmod 4$; 2 ist quadratischer Rest modulo p genau für $p \equiv 1$ oder $7 \pmod 8$.

Beweis. Nach EULERs Kriterium 4 ist die Differenz $\left(\frac{-1}{p}\right) - (-1)^{(p-1)/2}$ durch p teilbar; andererseits ist sie gleich -2, 0 oder 2 und dies gibt schon den ersten Ergänzungssatz. Wegen $\mu_p(-1) = \frac{1}{2}(p-1)$ folgt dieser übrigens auch sofort aus dem GAUSSschen Lemma 5, welches sogleich erneut für den zweiten Ergänzungssatz angewandt wird.

Genau für diejenigen $j \in \{1, \ldots, \frac{1}{2}(p-1)\}$ mit $j < \frac{1}{4}p$ ist $0 < r_p(2j) < \frac{1}{2}p$, somit hat man $-\frac{1}{2}p < r_p(2j) < 0$ genau für die j mit $\frac{1}{4}p < j \leq \frac{1}{2}(p-1)$, deren Anzahl das gesuchte $\mu_p(2)$ ist. Man bestätigt leicht

$$\mu_p(2) = \begin{cases} \frac{1}{4}(p-1) & \text{für } p \equiv 1, 5 \pmod 8, \\ \frac{1}{4}(p+1) & \text{für } p \equiv 3, 7 \pmod 8, \end{cases}$$

weshalb $\mu_p(2)$ genau dann gerade ist, wenn $p \equiv \pm 1 \pmod 8$ gilt. Dieselbe Eigenschaft hat offenbar $\frac{1}{8}(p^2-1)$ und damit liefert das GAUSSsche Lemma den zweiten Ergänzungssatz. □

Bemerkung. Der erste Ergänzungssatz sagt über ungerade Primzahlen p: Die Kongruenz $X^2 \equiv -1 \pmod p$ ist genau für $p \equiv 1 \pmod 4$ lösbar. Dies ist erneut der wesentliche Teil von Satz 2.3.9.

Wie bereits weiter oben bemerkt, bleibt $\left(\frac{q}{p}\right)$ noch für voneinander verschiedene ungerade Primzahlen p, q zu berechnen. Man kann nun aber nicht analog zu $\left(\frac{-1}{p}\right)$ oder $\left(\frac{2}{p}\right)$ einen geschlossenen Ausdruck für $\left(\frac{q}{p}\right)$ angeben, sondern lediglich für das Produkt $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)$. Dies geschieht in dem von GAUSS 1796 entdeckten sogenannten

Quadratischen Reziprozitätsgesetz. *Für voneinander verschiedene ungerade Primzahlen p, q gilt*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4}.$$

Ist also p oder q kongruent 1 modulo 4, so gilt $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)$; sind p und q beide kongruent 3 modulo 4, so hat man $\left(\frac{q}{p}\right) = -\left(\frac{p}{q}\right)$.

Wie man dennoch $(\frac{q}{p})$ mit Hilfe dieses Satzes ermitteln kann, wird in 8 anhand eines Beispiels erläutert.

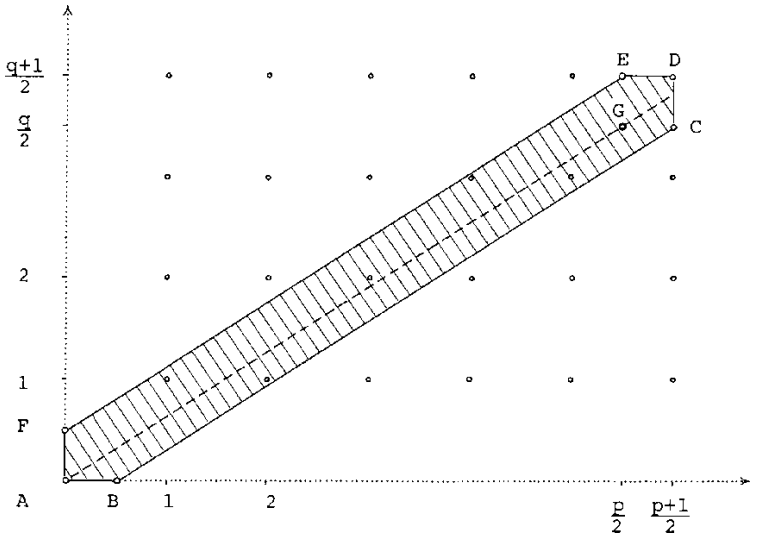
7. Beweis des Reziprozitätsgesetzes. Nach dem GAUSSschen Lemma 5 ist das quadratische Reziprozitätsgesetz gleichwertig mit der Aussage

$$(1) \qquad 2 \nmid (\mu_p(q) + \mu_q(p)) \;\Leftrightarrow\; p \equiv q \equiv 3 \pmod 4 ,$$

die hier gezeigt werden soll. Dazu sei definiert

$$\Omega := \{(x,y) \in \mathbb{R}_+^2 : \; x < \frac{p+1}{2},\; y < \frac{q+1}{2},\; y < \frac{2qx+p}{2p},\; x < \frac{2py+q}{2q}\};$$

Ω ist das Innere des (nachstehend im Fall $p = 11$, $q = 7$ skizzierten, schraffierten) Sechsecks $ABCDEF$.



Ist $(x,y) \in \Omega$ und setzt man $x' := \frac{p+1}{2} - x$, $y' := \frac{q+1}{2} - y$, so prüft man leicht nach, daß auch $(x',y') \in \Omega$ gilt: Aus $(x,y) \in \Omega$ folgt ja z.B.

$$\frac{2py'+q}{2q} = \frac{p+1}{2} - \frac{p}{q}\big(y - \frac{1}{2}\big) > \frac{p+1}{2} - \frac{p}{q} \cdot \frac{qx}{p} = x'.$$

Weiter ist $(x',y') = (x,y)$ genau dann, wenn $x = \frac{p+1}{4}$, $y = \frac{q+1}{4}$ gilt; die Richtigkeit von $(\frac{p+1}{4}, \frac{q+1}{4}) \in \Omega$ ist sofort einzusehen.

Nennt man ganz allgemein $(x, y) \in \mathbb{R}^2$ einen *Gitterpunkt* genau dann, wenn sogar $(x, y) \in \mathbb{Z}^2$ gilt, so werden nun die in Ω gelegenen Gitterpunkte abgezählt: $(\frac{p+1}{4}, \frac{q+1}{4})$ ist Gitterpunkt genau dann, wenn die beiden Kongruenzen rechts in (1) gelten. Ist (x, y) ein in Ω gelegener, von $(\frac{p+1}{4}, \frac{q+1}{4})$ verschiedener Gitterpunkt, so hat (x', y') dieselbe Eigenschaft; außerdem ist (x', y') von (x, y) verschieden. Indem man nun die Gitterpunkte in Ω in naheliegender Weise zu Paaren zusammenfaßt, ist klar:

$$\#\Omega \cap \mathbb{Z}^2 \text{ ungerade} \quad \Leftrightarrow \quad p \equiv q \equiv 3 \pmod 4.$$

Wenn nun noch

$$\#\Omega \cap \mathbb{Z}^2 = \mu_p(q) + \mu_q(p) \tag{2}$$

gezeigt ist, ist (1) und somit das Reziprozitätsgesetz bewiesen.

Kein Gitterpunkt $(x, y) \in \Omega$ kann der Bedingung $py = qx$ genügen, d.h. auf der Geraden durch $A := (0, 0)$ und $G := (\frac{1}{2}p, \frac{1}{2}q)$ liegen. Denn $p|qx$ würde $p|x$ implizieren; für die natürliche Zahl x müßte also $p \leq x < \frac{1}{2}(p+1)$ gelten, was unmöglich ist.

Nun wird die Anzahl der oberhalb der Geraden durch A und G gelegenen Gitterpunkte von Ω bestimmt. Es ist (x, y) genau dann ein solcher, wenn gilt:

$$x \in \{1, \ldots, \frac{1}{2}(p-1)\}, \quad y \in \mathbb{Z}, \quad \frac{qx}{p} < y < \frac{2qx+p}{2p};$$

dabei ist die letzte Doppelungleichung mit $-\frac{1}{2}p < qx - py < 0$ äquivalent. In der vor dem Gaussschen Lemma 5 eingeführten Terminologie bedeutet dies aber $-\frac{1}{2}p < r_p(qx) < 0$. So ist die Anzahl der oberhalb der Geraden durch A und G gelegenen Gitterpunkte von Ω gleich der Anzahl aller $x \in \{1, \ldots, \frac{1}{2}(p-1)\}$ mit $r_p(qx) < 0$, also gleich $\mu_p(q)$.

Analog ist die Anzahl der unterhalb dieser Geraden gelegenen Gitterpunkte von Ω gleich $\mu_q(p)$, womit (2) insgesamt bewiesen ist. □

Bemerkung. Der hier gegebene geometrische Beweis des quadratischen Reziprozitätsgesetzes geht zurück auf G. Eisenstein (Mathematische Werke I, 164–166), selbst Schüler von Gauss. Weitere historische Bemerkungen zum Reziprozitätsgesetz folgen in 13.

8. Ein numerisches Beispiel. Gauss beschließt Art. 146 seiner *Disquisitiones Arithmeticae* mit der Lösung folgender Aufgabe: "Quaeritur relatio

numeri +453 ad 1236." Er möchte also die Frage behandeln, ob die Kongruenz $Y^2 \equiv 453 \pmod{1236}$ lösbar ist. Hier ist $(453, 1236) = 3$ und man sieht leicht, daß die vorgelegte Kongruenz mit folgender neuen äquivalent ist: $3X^2 \equiv 151 \pmod{412}$. Wegen $2 \cdot 412 = 3 \cdot 275 - 1$ ist 275 modulo 412 zu 3 invers und so ist die letzte Kongruenz weiterhin gleichwertig mit

$$X^2 \equiv -87 \pmod{412}. \tag{1}$$

Diese Kongruenz ist von der Form 2(1) mit $c = -87$, $m = 412 = 2^2 \cdot 103$, die zueinander teilerfremd sind. Nach Satz 2 ist (1) genau dann lösbar, wenn -87 quadratischer Rest modulo 103 ist; $-87 \equiv 1 \pmod 4$ ist ja erfüllt. Man hat also noch das LEGENDRE–Symbol $(\frac{-87}{103})$ zu berechnen.

Nach Satz 3(ii) ist $(\frac{-87}{103}) = (\frac{-1}{103})(\frac{3}{103})(\frac{29}{103}) = (-1)(-1)(\frac{29}{103})$, wenn man für $(\frac{3}{103}) = -(\frac{103}{3}) = -(\frac{1}{3}) = -1$ das Reziprozitätsgesetz und Satz 3(i) investiert und für $(\frac{-1}{103}) = -1$ den ersten Ergänzungssatz. Erneut nach dem Reziprozitätsgesetz ist $(\frac{29}{103}) = (\frac{103}{29}) = (\frac{3 \cdot 29 + 16}{29}) = (\frac{16}{29}) = (\frac{2}{29})^4 = 1$, wo nochmals Satz 3(i), (ii) zum Zuge kamen. Damit ist $(\frac{-87}{103})$ zu 1 festgestellt, weshalb (1) und damit auch die Ausgangskongruenz lösbar ist.

Offenbar wird (1) von einem $x \in \mathbb{Z}$ genau dann gelöst, wenn dieses ungerade ist und $x^2 \equiv -87 \pmod{103}$ genügt, was offenbar mit $x^2 \equiv 16 \pmod{103}$ oder eben $x \equiv \pm 4 \pmod{103}$ äquivalent ist. Modulo 412 hat somit (1) genau die vier Lösungen ± 99, ± 107; dies führt modulo 1236 zu den sämtlichen Lösungen ± 297, ± 321 von $Y^2 \equiv 453$. Tatsächlich beschließt GAUSS a.a.O. seine Ausführungen "... est autem revera $453 \equiv 297^2 \pmod{1236}$."

Bemerkung. Hier sollte insbesondere gezeigt werden, wie man $(\frac{c}{p})$ unter Verwendung von Reziprozitätsgesetz, Ergänzungssätzen und den Regeln in Satz 3(i), (ii) *stets* berechnen kann. Manchmal kürzt eine umsichtige Beobachtung der speziellen Situation das Ganze erheblich ab. So ist z.B. oben $(\frac{-87}{103}) = (\frac{103-87}{103}) = (\frac{16}{103}) = (\frac{2}{103})^4 = 1$ und man kommt *hier* gänzlich ohne Reziprozitätsgesetz und Ergänzungssätze aus; $(\frac{2}{103})$ tritt ja nur in gerader Potenz auf.

9. Quadratische Nichtreste modulo Primzahlen. Ein erster Beitrag zu der in § 3 anzuschneidenden Frage nach der Verteilung quadratischer Reste und Nichtreste ist enthalten in

Proposition A. *Zu jeder Primzahl $p > 3$ mit $p \equiv 3 \pmod 4$ gibt es eine natürliche Zahl unterhalb $2\sqrt{p} + 1$, die quadratischer Nichtrest modulo p ist.*

Dies ist eine unmittelbare Folgerung aus

Proposition B. *Zu jedem p wie in Proposition A gibt es eine Primzahl $q \leq 2[\sqrt{p}]+1$ mit $q \equiv 3 \pmod 4$ und $(\frac{q}{p}) = -1$.*

Beweis. Sei $a := [\sqrt{p}]$. Bei geradem a ist $p - a^2 \in \mathbb{N}$ und $p - a^2 \equiv 3 \pmod 4$. Daher hat $p - a^2$ nur ungerade Primfaktoren, insgesamt aber mindestens einen $\equiv 3 \pmod 4$. Ist q ein solcher, so ist $q \leq p - a^2 < p - (\sqrt{p}-1)^2 = 2\sqrt{p} - 1$ und $a^2 \equiv p \pmod q$; d.h. p ist quadratischer Rest modulo q, also $(\frac{p}{q}) = 1$ und somit wegen $p \equiv q \equiv 3 \pmod 4$ nach dem quadratischen Reziprozitätsgesetz $(\frac{q}{p}) = -1$.

Ab jetzt sei a ungerade. Ist $p \equiv 7 \pmod 8$, so hat man $p - a^2 \equiv 7 - 1 = 6 \pmod 8$, also gilt $\frac{1}{2}(p - a^2) \equiv 3 \pmod 4$. Nun hat $\frac{1}{2}(p - a^2)$ einen Primfaktor $q \equiv 3 \pmod 4$, mit dem man wie vorher zu Ende argumentiert.

Ist $p \equiv 3 \pmod 8$, so ist $(a+2)^2 - p$ positiv ganz und kongruent $1 - 3 \equiv 6 \pmod 8$. Daher ist die natürliche Zahl $\frac{1}{2}\big((a+2)^2 - p\big) \equiv 3 \pmod 4$ und hat einen Primfaktor q der gewünschten Art. Dabei hat man nur noch die in Aussicht gestellte obere Schranke für q zu bestätigen: Wegen der Irrationalität von $\sqrt{p}$ (vgl. Korollar 1.1.9) ist in $a \leq \sqrt{p}$ das Gleichheitszeichen unmöglich, also gilt $a^2 \leq p-1$. Da hier die linke Seite ungerade, die rechte gerade ist, kann noch genauer $a^2 \leq p-2$ gesagt werden, also $q \leq \frac{1}{2}(a^2+4a+4-p) \leq 2a+1 = 2[\sqrt{p}]+1$ wie behauptet. □

Bemerkungen. 1) Die Größenbeschränkung für q in Proposition B kann man im allgemeinen nicht weiter verbessern. Für die Primzahlen $p = 11$, 83, 227 z.B. ist $2[\sqrt{p}]+1 = 7$, 19, 31 jeweils tatsächlich die kleinste Primzahl $\equiv 3 \pmod 4$, die quadratischer Nichtrest modulo p ist.

2) Die soeben aufgeführten drei Primzahlen sind sämtliche bei ungeradem $a > 1$ von der Form $a^2 + 2$ (also $\equiv 3 \pmod 8$), wobei überdies a durch 3 teilbar sein muß, da andernfalls $a^2 + 2$ größer als 3 und ein Vielfaches von 3 wäre. Die Folge $a^2 + 2$ mit durch 3 teilbarem ungeradem a beginnt mit 11,83, 227,433,731,1093,1523,2027,2603,3251, ... Die angegebenen zehn Zahlen sind alle, bis auf die fünfte und neunte, Primzahlen. Es ist aber unbekannt, ob in dieser Folge unendlich viele Primzahlen vorkommen.

10. Primzahlen in arithmetischen Progressionen.

Hier sollen einige einfache Illustrationen gegeben werden zum nachstehenden

Satz von Dirichlet. *Sind $k, \ell \in \mathbb{N}$ zueinander teilerfremd, so gibt es unendlich viele Primzahlen p mit $p \equiv \ell \pmod k$.*

Die Richtigkeit dieses Satzes hat EULER 1775 im Spezialfall $\ell = 1$ als Vermutung ausgesprochen, im allgemeinen Fall LEGENDRE 1785, der auch einen Beweis versucht hat. Den ersten vollständigen Beweis konnte jedoch erst 1837 DIRICHLET (Werke I, 313–342) liefern, dessen diesbezügliche Arbeit den Beginn der analytischen Zahlentheorie markiert.

Offenbar ist die Teilerfremdheit von k und ℓ notwendig für die Existenz unendlich vieler Primzahlen $p \equiv \ell \pmod{k}$. Ist nämlich q eine k und ℓ teilende Primzahl, so gilt $q|(kn + \ell)$ für alle ganzen n; daher kann höchstens das kleinste positive dieser $kn + \ell$ eine Primzahl (und damit gleich q) sein. Überdies darf o.B.d.A. $\ell \leq k$ vorausgesetzt werden.

Es sollen hier sämtliche Spezialfälle $k = 1, 2, 3, 4, 6$ des DIRICHLET*schen Satzes bewiesen werden.*

Ist k gleich 1 oder 2, so ist die Aussage im Satz identisch mit derjenigen des EUKLIDschen Satzes 1.1.4. Zur Behandlung der restlichen Fälle seien jeweils $p_1, \ldots, p_r$ paarweise verschiedene Primzahlen $\equiv \ell \pmod{k}$; mit mehr oder weniger Geschick, je nach Unterfall, wird zu diesen eine ganze Zahl $n_r > \ell$ so konstruiert, daß man zeigen kann: n_r hat einen von $p_1, \ldots, p_r$ verschiedenen Primfaktor $p_{r+1} \equiv \ell \pmod{k}$, womit man dann fertig ist.

Sei zuerst $k = 4$; dann hat man $\ell = 1, 3$ zu diskutieren. Im zweiten Unterfall folgt man dem EUKLIDschen Beweisgedanken in 1.1.4, indem man setzt

$$n_r := 4p_1 \cdot \ldots \cdot p_r - 1. \tag{1}$$

Da hier $n_r \equiv 3 \pmod 4$ gilt, können dessen (sämtliche ungerade) Primfaktoren nicht alle $\equiv 1 \pmod 4$ sein; somit hat n_r einen Primfaktor $p_{r+1} \equiv 3 \pmod 4$, der wegen (1) von $p_1, \ldots, p_r$ verschieden ist. Im ersten Unterfall $\ell = 1$ arbeitet man mit

$$n_r := (2p_1 \cdot \ldots \cdot p_r)^2 + 1. \tag{2}$$

Jeder Primfaktor p_{r+1} von n_r ist wegen (2) von $2, p_1, \ldots, p_r$ verschieden und wegen (2) ist -1 quadratischer Rest modulo p_{r+1}. Nach dem ersten Ergänzungssatz ist $(-1)^{(p_{r+1}-1)/2} = 1$, also $p_{r+1} \equiv 1 \pmod 4$.

Für $k = 6$ ist $\ell = 1, 5$ möglich. Im zweiten Unterfall schließt man genau wie für $k = 4$, $\ell = 3$; dies kann dem Leser überlassen bleiben. Im ersten Unterfall $\ell = 1$ arbeitet man hier mit

$$n_r := (2p_1 \cdot \ldots \cdot p_r)^2 + 3; \tag{3}$$

jeder Primfaktor p_{r+1} von n_r ist wegen (3) von $2, 3, p_1, \ldots, p_r$ verschieden und wegen (3) ist -3 quadratischer Rest modulo $p_{r+1} =: p$, also ist $(\frac{-3}{p}) = 1$.

Benutzt man hier Satz 3(i), (ii), das quadratische Reziprozitätsgesetz und seinen ersten Ergänzungssatz, so ist

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

Aus $p \equiv 2 \pmod 3$ würde $(\frac{p}{3}) = (\frac{2}{3}) = -1$ nach dem zweiten Ergänzungssatz folgen, also ist $p \equiv 1 \pmod 3$, wegen der Ungeradheit von $p = p_{r+1}$ also $p_{r+1} \equiv 1 \pmod 6$.

Schließlich sind bei $k = 3$ die Unterfälle $\ell = 1, 2$ möglich. Da für ungerade Primzahlen p die Kongruenzen $p \equiv 1$ bzw. $5 \pmod 6$ mit den Kongruenzen $p \equiv 1$ bzw. $2 \pmod 3$ äquivalent sind, werden diese Fälle schon durch $k = 6$, $\ell = 1, 5$ abgedeckt. □

Bemerkungen. 1) Die Fragestellung im DIRICHLETschen Satz kann man wie folgt verallgemeinern: Sei $f \in \mathbb{Z}[X]$ nicht konstant, in $\mathbb{Z}[X]$ irreduzibel, mit positivem Leitkoeffizienten und $(*)$: es gebe keine Primzahl, die alle $f(n)$ mit $n \in \mathbb{Z}$ teilt. (Die Bedingung $(*)$ verlangt mindestens die Teilerfremdheit sämtlicher Koeffizienten von f, d.h. dessen *Primitivität*; bei $\partial(f) = 1$ sind $(*)$ und die Primitivität von f offenbar äquivalent.) Da die Folge $(f(n))_{n=0,1,\ldots}$ ganzer Zahlen von einer Stelle an streng wächst, ist die Frage sinnvoll, ob es unendlich viele $n \in \mathbb{N}$ gibt, für die $f(n)$ Primzahl ist. Im Fall $\partial(f) = 1$ beantwortet der DIRICHLETsche Satz die gestellte Frage positiv, während sie für $\partial(f) \geq 2$ noch offen ist. Wenigstens konnte H.–E. RICHERT (1968) die Existenz unendlich vieler $n \in \mathbb{N}$ zeigen, für die $f(n)$ Produkt von höchstens $\partial(f)+1$ (nicht notwendig verschiedenen) Primzahlen ist; bei $\partial(f) = 2$ kann man nach H. IWANIEC (1978) "Produkt dreier" durch "Produkt zweier" Primzahlen ersetzen.

2) Der Leser möge sich klarmachen, daß die in Bemerkung 2 zu 9 offen gelassene Frage genau mit folgender äquivalent ist: Sei f das spezielle Polynom $36X^2 + 36X + 11$ von der Art wie in Bemerkung 1; gibt es unendlich viele $n \in \mathbb{N}$, für die $f(n)$ Primzahl ist?

11. Primfaktoren von Fermat–Zahlen. LUCAS bewies 1877 mit Hilfe des zweiten Ergänzungssatzes aus 6 ein Ergebnis, welches die Form der möglichen Primfaktoren der in 2.1.2 eingeführten FERMAT–Zahlen $F_n := 2^{2^n} + 1$ stark einschränkt.

Satz. *Teilt eine Primzahl p die* FERMAT*–Zahl F_n mit $n \geq 2$, so gilt $p = 2^{n+2}k + 1$ mit natürlichem k.*

Beweis. Nach Voraussetzung ist $2^{2^n} \equiv -1 \pmod p$, also $2^{2^{n+1}} \equiv 1 \pmod p$ und somit gilt $\mathrm{ord}_p 2 = 2^{n+1}$. Nach Korollar 2.3.4 wird $p-1$ von 2^{n+1} geteilt und wegen $n \geq 2$ ist $p \equiv 1 \pmod 8$. Nach dem zweiten Ergänzungssatz ist dann $(\frac{2}{p}) = 1$, d.h. es gilt $x^2 \equiv 2 \pmod p$ bei geeignetem ganzem, nicht durch p teilbarem x. Die letzte Kongruenz impliziert $x^{2^{n+2}} \equiv 2^{2^{n+1}} \equiv 1 \pmod p$, weshalb $\mathrm{ord}_p x = 2^j$ mit einem natürlichen $j \leq n+2$ sein muß. Aus $x^2 \equiv 2 \pmod p$ folgt dann $1 \equiv 2^{2^{j-1}} \pmod p$, weshalb auch $j \geq n+2$ gelten muß. Nach Korollar 2.3.4 teilt $\mathrm{ord}_p x \ (= 2^{n+2})$ die Zahl $p-1$ wie behauptet. □

Die Aussage dieses Satzes liefert eines der wenigen bekannten theoretischen Hilfsmittel für die Suche nach Primfaktoren von FERMAT–Zahlen. Danach hat man die Primfaktoren von F_5 in der arithmetischen Folge $(128k+1)_{k=1,2,\ldots}$ zu suchen, die mit 129,257,385,513,641,... beginnt. Offensichtlich sind hier nur $(F_3 =)257$ und 641 Primzahlen und wegen $(F_3, F_5) = 1$, vgl. Satz 2.1.2, ist 641 die *erste* mögliche Primzahl, die F_5 teilen kann. Daß sie es tatsächlich tut, wurde schon in 2.1.2 vorgeführt; der dort angegebene zweite Primfaktor von F_5 ist in Übereinstimmung mit obigem Satz gleich $2^7 \cdot 3 \cdot 17449 + 1$.

Ähnlich konnten 1877 unabhängig voneinander LUCAS und J. PERVUSIN einen Primfaktor von F_{12} entdecken. Nach obigem Satz ist jeder solche von der Form $d_k := 2^{14}k + 1$. Wegen $5|(d_1, d_6)$, $3|(d_2, d_5)$, $13|d_3$ und $d_4 = F_4$ ist $k = 7$ die früheste Möglichkeit und in der Tat erweist sich d_7 als F_{12} teilende Primzahl.

Die F_n mit $5 \leq n \leq 32$ sind zusammengesetzt, allerdings kennt man nur für $5 \leq n \leq 11$ die vollständige Faktorisierung von F_n; bei $n \in \{14, 20, 22, 24\}$ ist kein einziger Primfaktor von F_n bekannt. F_{33} ist derzeit die kleinste FERMAT–Zahl, bei der man nicht weiß, ob sie prim oder zusammengesetzt ist.

12. Mersenne–Primzahlen. Wie in Proposition 1.1.8 gesehen, können höchstens solche MERSENNE–Zahlen $M_p := 2^p - 1$ Primzahlen sein, für die p selbst Primzahl ist. Mit Hilfe des zweiten Ergänzungssatzes wird sogleich ein Ergebnis bewiesen, welches gewisse M_p sofort als zusammengesetzt erkennen läßt.

Satz A. *Ist p eine Primzahl, so daß auch $q := 2p+1$ Primzahl ist, so gilt $q|M_p \Leftrightarrow q \equiv \pm 1 \pmod 8$ bzw. $q|(M_p+2) \Leftrightarrow q \equiv \pm 3 \pmod 8$.*

Beweis. Man hat $q|M_p \Leftrightarrow 2^{(q-1)/2} \equiv 1 \pmod q \Leftrightarrow (\frac{2}{q}) \equiv 1 \pmod q$, letzteres nach dem EULER–Kriterium 4. Damit ist $(\frac{2}{q}) = 1$, was nach dem zweiten Ergänzungssatz mit $q \equiv \pm 1 \pmod 8$ äquivalent ist.

Weiter gilt $q|(M_p+2) \Leftrightarrow 2^{(q-1)/2} \equiv -1 \pmod q \Leftrightarrow (\frac{2}{q}) = -1 \Leftrightarrow q \equiv \pm 3 \pmod 8$. □

Korollar. *Ist $p \equiv 3 \pmod 4$ eine Primzahl, so daß auch $q := 2p+1$ Primzahl ist, so wird M_p von q geteilt; bei $p > 3$ ist also M_p unter den vorstehenden Bedingungen zusammengesetzt.*

Beweis. Wegen $p \equiv 3 \pmod 4$ ist $q \equiv -1 \pmod 8$ und Satz A liefert die erste Behauptung. Weiter tritt in $2p+1 \leq 2^p - 1$ genau für $p = 3$ Gleichheit ein. □

Es folgt noch ein Resultat über die mögliche Form von Primfaktoren der M_p.

Satz B. *Sei p eine ungerade Primzahl und q ein Primfaktor von M_p. Dann gilt $q \equiv 1 \pmod{2p}$ und $q \equiv \pm 1 \pmod 8$.*

Beweis. Nach Voraussetzung ist $2^p \equiv 1 \pmod q$, also $(\mathrm{ord}_q 2) | p$. Da $\mathrm{ord}_q 2$ nicht gleich 1 ist, hat man $\mathrm{ord}_q 2 = p$. Nach dem "kleinen" FERMATschen Satz ist $2^{q-1} \equiv 1 \pmod q$, also $p | (q-1)$; wegen $2 | (q-1)$ hat man die erste Behauptung. Die ganze Zahl $x := 2^{(p+1)/2}$ genügt $x^2 - 2 = 2M_p \equiv 0 \pmod q$ und man hat $(\frac{2}{q}) = 1$; die zweite Behauptung folgt aus dem zweiten Ergänzungssatz. □

Aufgrund des Korollars ist M_p zusammengesetzt für die Primzahlen $p = 11, 23, 83, 131, 179, 191$. Es gibt genau 54 Primzahlen $\equiv 3 \pmod 4$ unterhalb 4000, für die auch $2p+1$ Primzahl ist; die Anzahl aller Primzahlen unterhalb 4000 ist 550. Es ist allerdings offen, ob gleichzeitig $4k+3$ und $8k+7$ für unendlich viele natürliche k Primzahlen sein können.

Die Faktorzerlegung von $M_{11} = 2047$ findet man mittels Satz B leicht wie folgt: Jeder Primfaktor von M_{11} muß $\equiv 1 \pmod{22}$ und $\equiv \pm 1 \pmod 8$ sein und die erste sich daraus ergebende Möglichkeit 23 teilt tatsächlich M_{11}; man hat $M_{11} = 23 \cdot 89$ und natürlich genügt auch 89 den Kongruenzen des Satzes B. Diese Zerlegung wurde von CATALDI (1588) gefunden, der auch zeigte, daß M_{13}, M_{17} und M_{19} Primzahlen sind.

Für M_{19} sei dies hier exemplarisch vorgeführt. Die Voraussetzungen des Korollars sind hier nicht erfüllt, so daß man Chancen hat, M_{19} als Primzahl nachzuweisen. Aufgrund von Satz B kommen als M_{19} teilende Primzahlen unterhalb $M_{19}^{1/2}$ (d.h. unterhalb 724) höchstens noch 191, 457 und 647 in Frage; daß M_{19} von diesen nicht geteilt wird, rechnet man schließlich direkt nach.

In der folgenden Tabelle sind alle bisher bekannten 36 MERSENNEschen Primzahlen M_p mit $p > 31$ aufgelistet; hinzu kommen die acht bis EULER bekannten mit $p \in \{2, 3, 5, 7, 13, 17, 19, 31\}$. Der zweiten Spalte entnimmt man die jeweilige Anzahl der Dezimalstellen von M_p. In der dritten werden die jeweiligen Entdecker ab 2001 nicht mehr aufgeführt, zumal die Suche nach immer größeren

Primzahlen M_p seit 1996 im Rahmen des weltweiten GIMPS–Projekts (*Great Internet Mersenne Prime Search*, http://www.mersenne.org) abläuft.

p	Stellenanzahl	Entdecker (Jahr)
61	19	Pervusin (1883)
89	27	Fauquembergue, Powers (1911)
107	33	" " (1914)
127	39	Lucas (1876)
521	157	Lehmer & Robinson (1952)
607	183	"
1279	386	"
2203	664	"
2281	687	"
3217	969	Riesel (1957)
4253	1281	Hurwitz & Selfridge (1961)
4423	1332	"
9689	2917	Gillies (1963)
9941	2993	"
11213	3376	"
19937	6002	Tuckerman (1971)
21701	6533	Nickel & Noll (1978)
23209	6987	"
44497	13395	Slowinski (1979)
86243	25962	" (1982)
110503	33265	Colquitt & Welsh (1988)
132049	39751	Slowinski (1983)
216091	65050	" (1985)
756839	227832	Slowinski & Gage (1992)
859433	258716	" (1994)
1257787	378632	" (1996)
1398269	420921	Armengaud & Woltman (1996)
2976221	895932	Spence & Woltman (1997)
3021377	909526	Clarkson & Woltman (1998)
6972593	2098960	Hajratwala & Woltman (1999)
13466917	4053946	Cameron & Woltman (2001)
20996011	6320430	(2003)
24036583	7235733	(2004)
25964951	7816230	(2005)
30402457	9152052	(2005)
32582657	9808358	(2006)

Aus der umseitigen Tabelle kann der Leser gut die historische Entwicklung immer verbesserter Primzahltests einerseits und immer schnellerer Computer andererseits ablesen. Der Computerausdruck von $M_{32582657}$ im Dezimalsystem würde etwa den 10000–fachen Platz benötigen wie der in 5.1.11 reproduzierte Ausdruck des Beginns der Dezimalbruchentwicklung der Zahl π, also mindestens 11 Exemplare des vorliegenden Buchs.

Bemerkung. Aktuelle Primzahlrekorde gehören offenbar zu den wenigen Ergebnissen mathematischer Forschung, die der Öffentlichkeit in dieser oder jener Form regelmäßig zur Kenntnisnahme angeboten werden. So ging Mitte Februar 1985 durch die deutsche Presse, W. KELLER in Hamburg habe mit $5 \cdot 2^{23473} + 1$ die fünftgrößte damals bekannte Primzahl (7067 Dezimalstellen) gefunden. Auch die Entdeckung von M_{216091} als seinerzeit größte bekannte Primzahl wurde Mitte September 1985 in Presse und Rundfunk gemeldet und kommentiert. Die holländische Tageszeitung "Haarlems Dagblad" hatte am 5. Oktober 1983 den bald darauf entthronten Rekordinhaber M_{132049} in Dezimaldarstellung in voller Länge abgedruckt.

Gegenüber der Tagespresse ungewöhnlicher ist das nachfolgend abgebildete, 1968 von der U.S.–Post in Urbana (Illinois) gewählte Informationsmedium.

Wenn hier schon die Problematik "Mathematik und ihre Publicity" angesprochen ist, so sollte trotz der generell dürftigen Repräsentanz nicht vergessen werden, daß sowohl die Schweizerische Nationalbank als (bis zur Euro-Einführung) auch die Deutsche Bundesbank mit EULER bzw. GAUSS auf ihren 10 Franken– bzw. 10 Mark–Scheinen die bedeutendsten Mathematiker (und Zahlentheoretiker) des 18. bzw. 19. Jahrhunderts ehren bzw. ehrten. Dem tut die Tatsache kaum Abbruch, daß allerlei physikalisch–technische Skizzen und Apparaturen die Rückseiten beider Scheine zieren: Solche mehr praktischen Dinge sind der Allgemeinheit eben viel leichter nahezubringen als noch so schöne Ergebnisse der abstrakten Mathematik.

13. Historisches zum Reziprozitätsgesetz. Die beiden Ergänzungssätze zum quadratischen Reziprozitätsgesetz (hier kurz q.Rg.) waren bereits FERMAT bekannt, aber erst EULER (Opera Omnia Ser. 1, II, 328–337) bzw. LAGRANGE (Oeuvres III, 695–795) lieferten Beweise für den ersten bzw. zweiten. Das q.Rg. selbst scheint von EULER gefunden, von ihm etwa 1745 implizit benützt, spätestens aber 1772 (Opera Omnia Ser. 1, III, 497–512) erstmals klar ausgesprochen worden zu sein. Offenbar unabhängig von EULER hat auch LEGENDRE (Hist. Acad. Paris *1785*, 465ff.) das q.Rg. entdeckt und zu zeigen versucht. Sein Beweisversuch hatte allerdings insofern eine in jener Zeit unbehebbare Lücke, als er die Existenz unendlich vieler Primzahlen in gewissen arithmetischen Folgen *voraussetzte*, vgl. 10. In LEGENDREs in 3 erwähntem *Essai* ... (S. 186) findet sich dann die in 6 angegebene elegante, symmetrische Formulierung des q.Rg. mit Hilfe des von ihm eingeführten Symbols $(\frac{p}{q})$. Ebenfalls von LEGENDRE stammt die in die spätere Literatur eingegangene Bezeichnung für das Gesetz ("loi de réciprocité"), während GAUSS generell vom "theorema fundamentale" spricht.

GAUSS selbst hat als Achtzehnjähriger aus umfangreichem Beispielmaterial das q.Rg. herauspräpariert, ganz unabhängig von seinen Vorgängern EULER und LEGENDRE. Nach einem Jahr härtester Arbeit war ihm dann der erste komplette Beweis gelungen. Über diese Phase seiner Forschungen schreibt er (Werke II, S. 4): "Adiicere liceat tantummodo, in confirmationem eorum, quae in art. praec. prolata sunt, quae ad meos conatus pertinent. In ipsum theorema proprio marte incideram anno 1795, dum omnium, quae in arithmetica sublimiori iam elaborata fuerant, penitus ignarus et a subsidiis literariis omnino praeclusus essem: sed per integrum annum me torsit, operamque enixissimam effugit, donec tandem demonstrationem in Sectione quarta operis illius traditam nactus essem."*)

Während GAUSS seinen ersten Beweis des q.Rg. (8. April 1796) mittels vollständiger Induktion und ganz im Rahmen der Theorie der quadratischen Reste führte, gab er bald darauf (27. Juni 1796) einen weiteren an, der sich auf seine Untersuchungen über quadratische Formen stützte (*Disquisitiones Arithmeticae*, Art. 257ff.). Insgesamt lieferte GAUSS selbst acht methodisch verschiedene Beweise für das q.Rg., ein Zeichen für die zentrale Bedeutung, die er diesem für

*) (Es mögen nur zur Bestätigung dessen, was im vorigen Artikel gesagt wurde, einige Bemerkungen zu meinen Versuchen gestattet sein. Auf jenen Satz kam ich im März 1795 selbständig. Damals waren mir alle schon erzielten Resultate der höheren Arithmetik völlig unbekannt und zu den Hilfsmitteln der Literatur hatte ich keinerlei Zugang. Doch quälte mich jener Satz ein ganzes Jahr lang und entzog sich den angestrengtesten Bemühungen, bis mir endlich der im vierten Abschnitt jenes Werkes [*Disquisitiones Arithmeticae*, Art. 135ff.] aufgeschriebene Beweis gelang.)

die Zahlentheorie zumaß.

In der Folgezeit sind zahlreiche weitere Beweise angegeben worden. Alleine 45 entfallen auf die Jahre zwischen 1796 und 1896. Diese Beweise sind chronologisch geordnet und mit der jeweils verwendeten Methode bei P. BACHMANN (*Niedere Zahlentheorie* I, Teubner, Leipzig, 1902, S. 203/4) zitiert; davon operieren 28 mit dem GAUSSschen Lemma 5 oder mit geeigneten Modifikationen. Bis heute sind deutlich über 150 Beweise des q.Rg. publiziert worden; 1963 erschien eine Note mit dem Titel "The 152nd proof of the law of quadratic reciprocity" von M. GERSTENHABER (Amer. Math. Monthly *70*, 397–398 (1963)).

Parallel mit der Suche nach immer neuen Beweisvarianten für das *quadratische* Rg. hat schon GAUSS damit begonnen, analoge Reziprozitätsgesetze für Kongruenzen *höheren als zweiten Grades* aufzustellen. Den ersten Beweis für das von GAUSS 1825 gefundene biquadratische Rg. konnte EISENSTEIN 1844 liefern, der im gleichen Jahr das 1827 erstmals von JACOBI gezeigte kubische Rg. bewies. Um die Wende zum 20. Jahrhundert hat vor allem HILBERT diese Entwicklung entscheidend gefördert und zwar sowohl durch einige bedeutende Arbeiten als auch dadurch, daß er die Frage nach möglichst weitgehender Verallgemeinerung des q.Rg. in den Katalog seiner "Mathematischen Probleme" aufnahm.

Unter diesem Titel hielt HILBERT 1900 auf dem Internationalen Mathematiker–Kongreß in Paris seinen inzwischen berühmt gewordenen Vortrag. Dort formulierte er insbesondere 23 seinerzeit offene Fragestellungen explizit, die die ganze damalige Mathematik umspannten und die er als Schlüsselprobleme für weitere Fortschritte in den einzelnen mathematischen Teildisziplinen erachtete. Das "neunte HILBERTsche Problem" stellt unter der Überschrift *Beweis des allgemeinsten Reziprozitätsgesetzes im beliebigen Zahlkörper* folgende Aufgabe:

"Für einen beliebigen Zahlkörper soll das Reziprozitätsgesetz der ℓ–ten Potenzreste bewiesen werden, wenn ℓ eine ungerade Primzahl bedeutet und ferner, wenn ℓ eine Potenz von 2 oder eine Potenz einer ungeraden Primzahl ist. Die Aufstellung des Gesetzes sowie die wesentlichen Hilfsmittel zum Beweise desselben werden sich, wie ich glaube, ergeben, wenn man die von mir entwickelte Theorie des Körpers der ℓ–ten Einheitswurzeln und meine Theorie des relativ–quadratischen Körpers in gehöriger Weise verallgemeinert."

Dieses Problem wurde vor allem durch Arbeiten von T. TAGAKI (1920/2), H. HASSE (1926), E. ARTIN (1928) und I.R. SAFAREVIC (1948/50) gelöst.

Bemerkung. Den genannten HILBERTschen Vortrag findet man nebst hervorragender Kommentierungen über den Anfang bzw. Mitte der 1970er Jahre aktuellen Stand der 23 Einzelprobleme in: *Die Hilbertschen Probleme*, Ostwalds Klassiker Band 252, Leipzig, 1971 bzw. *Mathematical developments arising from Hilbert problems*, Proc. Symp. Pure Math. *28* (1976).

Viele wertvolle Informationen zum q.Rg., zu seiner Behandlung von GAUSS, zu seinen interessantesten Beweisvarianten ebenso wie zu den zuletzt diskutierten algebraischen Verallgemeinerungen entnimmt man dem zum 200. Geburtstag von GAUSS erschienenen Bändchen von H. PIEPER (*Variationen über ein zahlentheoretisches Thema von Carl Friedrich Gauss*, Birkhäuser, Basel–Stuttgart, 1978).

§ 3. Verteilung quadratischer Reste

1. Summen über gewisse Legendre–Symbole. Für ungerade Primzahlen p und natürliche $d < p$ interessiert nun die Anzahl der d–Tupel sukzessiver natürlicher Zahlen unterhalb p, die *sämtlich* quadratische Reste modulo p sind. Schreibt man diese Anzahl als $Q_p(d)$, so ist offenbar $Q_p(d) = 0$ für $\frac{1}{2}(p-1) < d$ wegen Korollar 1.5C. Uninteressant ist auch die aus demselben Grund geltende Gleichung $Q_p(1) = \frac{1}{2}(p-1)$. In 2 wird $Q_p(2)$ ermittelt, in 3 dann $Q_p(3)$. Für die Durchführung dieses Programms benötigt man zunächst folgendes

Lemma. *Ist p eine ungerade Primzahl, so gilt bei ganzen a, b*

$$S_p(a,b) := \sum_{t=0}^{p-1}\Big(\frac{(t+a)(t+b)}{p}\Big) = \begin{cases} p-1, & \text{falls } a \equiv b \pmod p \\ -1 & \text{sonst.} \end{cases}$$

Bemerkung. Derartige Summen sind in diesem Paragraphen stets über die im Sinne von Bemerkung 2 in 2.3 *erweiterten* LEGENDRE–Symbole zu verstehen; sonst müßte man einen oder zwei t–Werte von der Summation ausschließen, was einfach unbequemer wäre.

Beweis. Mit $k := b - a$ ist

$$S_p(a,b) = \sum_{i=a}^{p-1+a}\Big(\frac{i(i+k)}{p}\Big) = \sum_{i=0}^{p-1}\Big(\frac{i(i+k)}{p}\Big) = \sum_{i=1}^{p-1}\Big(\frac{i(i+k)}{p}\Big). \tag{1}$$

Dabei ist die Tatsache benutzt, daß in den beiden ersten Summen jeweils über ein vollständiges Restsystem modulo p summiert wird, weiter ist $(\frac{0}{p}) := 0$ beachtet. Ist $j(i)$ modulo p invers zu $i \in \{1,\dots,p-1\}$, so durchlaufen i und $j(i)$ gleichzeitig ein primes Restsystem modulo p. Daher kann die Summe rechts in (1) folgendermaßen umgearbeitet werden:

$$S_p(a,b) = \sum_{i=1}^{p-1}\Big(\frac{j(i)}{p}\Big)^2\Big(\frac{i(i+k)}{p}\Big) = \sum_{i=1}^{p-1}\Big(\frac{1+j(i)k}{p}\Big) = \sum_{j=1}^{p-1}\Big(\frac{1+jk}{p}\Big). \tag{2}$$

Nun ist $a \equiv b \pmod p$ mit $p|k$ äquivalent und in diesem Fall sind alle in der Summe rechts in (2) vorkommenden LEGENDRE–Symbole gleich $(\frac{1}{p}) = 1$, woraus der erste Teil des Lemmas folgt. Für $p\not|k$ sind alle ganz rechts in (2) vorkommenden $1 + jk$ modulo p paarweise inkongruent und sämtliche inkongruent 1. Wegen Satz 2.3(iv) (vgl. die dortige Bemerkung 2) ist damit nach (2)

$$S_p(a,b) = \sum_{\ell=0}^{p-1} (\frac{\ell}{p}) - (\frac{1}{p}) = -1. \qquad \square$$

2. Paare sukzessiver quadratischer Reste. Hier soll der folgende, auf GAUSS zurückgehende Satz bewiesen werden.

Satz. *Für ungerade Primzahlen p gibt es genau $\frac{1}{4}(p - 4 + (-1)^{(p+1)/2})$ Paare aufeinanderfolgender quadratischer Reste modulo p, die überdies natürliche Zahlen unterhalb p sind.*

Beweis. Man sieht sofort, daß $\frac{1}{4}(1 + (\frac{t}{p}))(1 + (\frac{t+1}{p}))$ gleich 1 ist, falls t *und* $t+1$ quadratische Reste modulo p sind, und gleich 0 sonst; dies gilt für $t = 1, \ldots, p-2$. Mit der Bezeichnung anfangs von 1 folgt daraus, wenn man noch Satz 2.3(iv), den ersten Ergänzungssatz aus 2.6 sowie Lemma 1 beachtet,

$$\begin{aligned} 4Q_p(2) &= \sum_{t=1}^{p-2} \Big(1 + (\frac{t}{p})\Big)\Big(1 + (\frac{t+1}{p})\Big) \\ &= p - 2 + \sum_{t=1}^{p-2} \Big(\frac{t}{p}\Big) + \sum_{t=2}^{p-1} \Big(\frac{t}{p}\Big) + \sum_{t=0}^{p-1} \Big(\frac{t(t+1)}{p}\Big) \\ &= p - 2 - (-1)^{(p-1)/2} - 1 - 1. \end{aligned}$$

Daraus liest man die Behauptung ab. $\square$

Beispiel. Nach dem Satz ist $Q_{29}(2) = 6$. Tatsächlich sind 1, 4, 5, 6, 7, 9, 13, 16, 20, 22, 23, 24, 25, 28 alle 14 quadratischen Reste modulo 29 in $\{1, \ldots, 28\}$ und für $Q_{29}(2)$ werden also genau die Paare $(4,5)$, $(5,6)$, $(6,7)$, $(22,23)$, $(23,24)$ und $(24,25)$ gezählt.

Bemerkung. Der Beweis des Satzes legt nahe, daß man mit Leichtigkeit analog z.B. die Anzahl der Paare sukzessiver natürlicher Zahlen unterhalb p bestimmen kann, die beide quadratische Nichtreste modulo p sind (oder die beiden restlichen möglichen Kombinationen von Resten und Nichtresten).

3. Tripel sukzessiver quadratischer Reste. Definiert man für ungerade Primzahlen p und ganze t die sogenannten JACOBSTHALschen *Summen* $T_p(t)$ durch

$$T_p(t) := \sum_{c=1}^{p-1} \Big(\frac{c(c^2-t)}{p}\Big), \tag{1}$$

so gilt der folgende

Satz. *Für ungerade Primzahlen p existieren genau*

$$Q_p(3) = \begin{cases} \frac{1}{8}(p + T_p(1) - 11 - 4(-1)^{(p-1)/4}), & \text{falls } p \equiv 1 \pmod 4, \\ [\frac{1}{8}p], & \text{falls } p \equiv 3 \pmod 4, \end{cases}$$

Tripel aufeinanderfolgender quadratischer Reste modulo p, die überdies natürliche Zahlen unterhalb p sind.

Beweis. Für $p = 3$ ist die behauptete Formel richtig, da Tripel der genannten Art hier nicht auftreten können. Ist $p \geq 5$, so sieht man völlig analog zum Beweisbeginn in 2

$$\begin{aligned} 8Q_p(3) &= \sum_{c=2}^{p-2} \Big(1 + \big(\frac{c-1}{p}\big)\Big)\Big(1 + \big(\frac{c}{p}\big)\Big)\Big(1 + \big(\frac{c+1}{p}\big)\Big) \\ &= p - 3 - \Big(\frac{p-1}{p}\Big) - \Big(\frac{p-2}{p}\Big) - \Big(\frac{1}{p}\Big) - \Big(\frac{p-1}{p}\Big) - \Big(\frac{1}{p}\Big) - \Big(\frac{2}{p}\Big) \\ &\quad + S_p(-1,0) - \Big(\frac{(p-1)(p-2)}{p}\Big) + S_p(0,1) - \Big(\frac{2}{p}\Big) + S_p(-1,1) - \Big(\frac{-1}{p}\Big) \\ &\quad + T_p(1). \end{aligned}$$

Nach Lemma 1 sowie den beiden Ergänzungssätzen aus 2.6 ist somit

$$8Q_p(3) = p - 8 - 3(-1)^{(p-1)/2} - 3(-1)^{(p^2-1)/8} - (-1)^{(p-1)/2+(p^2-1)/8} + T_p(1),$$

was für $p \equiv 1 \pmod 4$ direkt die Behauptung liefert. Ist $p \equiv 3 \pmod 4$, so hat man nach dem folgenden Lemma 4(iii)

$$8Q_p(3) = p - 5 - 2(-1)^{(p^2-1)/8} = \begin{cases} p-3 & \text{für } p \equiv 3 \pmod 8 \\ p-7 & \text{für } p \equiv 7 \pmod 8), \end{cases}$$

was auch in diesem Fall die Behauptung des Satzes ergibt. □

Beispiel. Nach dem Satz ist $Q_{29}(3) = 4$ und in der Tat werden dabei genau die Tripel $(4,5,6)$, $(5,6,7)$, $(22,23,24)$ und $(23,24,25)$ gezählt, vgl. das Beispiel in 2. Dabei findet man $T_{29}(1) = 10$ relativ leicht aus Lemma 4(ii).

Bemerkung. Bei der Anwendung der Formel des Satzes muß man im Fall $p \equiv 1 \pmod 4$ generell $T_p(1)$ berechnen. Für kleine p ist das ziemlich mühelos; man kann Lemma 4(ii) verwenden. Für große p wird man sich im allgemeinen mit einer Abschätzung für $T_p(1)$ zufrieden geben, vgl. das folgende Korollar 4.

4. Eigenschaften Jacobsthalscher Summen. Über die durch 3(1) eingeführten Summen $T_p(t)$ gibt folgender Hilfssatz die erforderlichen Auskünfte.

Lemma.

(i) *Es gilt* $T_p(0) = 0$.

(ii) *Für ganze* t *ist* $T_p(t) = (1 + (\frac{-1}{p})) \sum_{c=1}^{(p-1)/2} (\frac{c(c^2-t)}{p})$.

(iii) *Bei* $p \equiv 3 \pmod 4$ *ist* $T_p(t) = 0$ *für alle ganzen* t.

(iv) *Für ganze* s,t *ist* $T_p(s^2 t) = (\frac{s}{p}) T_p(t)$.

(v) $T_p(t)^2$ *ist konstant für alle quadratischen Reste (bzw. Nichtreste) modulo* p.

(vi) *Ist* $p \equiv 1 \pmod 4$ *und* t_0 *irgendein quadratischer Nichtrest modulo* p, *so gilt*

$$T_p(1)^2 + T_p(t_0)^2 = 4p.$$

Beweis. (i) ist wegen $(\frac{c^3}{p}) = (\frac{c}{p})$ für $c = 1, \ldots, p-1$ äquivalent mit Satz 2.3(iv).

(ii) folgt direkt aus

$$\sum_{c=(p+1)/2}^{p-1} \Big(\frac{c(c^2-t)}{p}\Big) = \sum_{d=1}^{(p-1)/2} \Big(\frac{-d(d^2-t)}{p}\Big),$$

wenn man $c = p - d$ setzt und Satz 2.3(i), (ii) beachtet.

(iii) ergibt sich aus (ii) wegen $(\frac{-1}{p}) = -1$ genau für $p \equiv 3 \pmod 4$; (iii) folgt aber auch aus (iv) mit $s := -1$.

(iv) ist bei $p|s$ klar wegen $(\frac{s}{p}) = 0$, wegen (i) und der sich aus Satz 2.3(i) ergebenden Gleichung $T_p(t) = T_p(t')$ für ganze, modulo p kongruente t, t'. Ist

$p \nmid s$, so durchläuft mit c auch sc ein primes Restsystem modulo p und man entnimmt die Behauptung der folgenden Gleichung.

$$\Big(\frac{s}{p}\Big)T_p(t) = \Big(\frac{s^3}{p}\Big)T_p(t) = \sum_{c=1}^{p-1}\Big(\frac{sc((sc)^2 - s^2t)}{p}\Big) = \sum_{d=1}^{p-1}\Big(\frac{d(d^2 - s^2t)}{p}\Big) = T_p(s^2t).$$

Für (v) sei a eine feste Primitivwurzel modulo p. Nach Korollar 1.5B sind sämtliche quadratischen Reste bzw. Nichtreste modulo p kongruent $a^2, a^4, \ldots$ $\ldots, a^{p-1}$ bzw. $a, a^3, \ldots, a^{p-2}$. Sind t_1, t_2 entweder beides Reste oder beides Nichtreste modulo p, so ist $t_2 \equiv a^{2m}t_1 \pmod p$ mit geeignetem natürlichem m. Wendet man (iv) mit $s := a^m$, $t := t_1$ an, so ist $T_p(t_2)^2 = (\frac{a^m}{p})^2 T_p(t_1)^2 = T_p(t_1)^2$ wie behauptet.

(vi): Nach (i), (v) und den Definitionen von $S_p(a,b)$ bzw. $T_p(t)$ in 1 bzw. 3(1) ist

$$\begin{aligned}\frac{p-1}{2}(T_p(1)^2 + T_p(t_0)^2) &= \sum_{t=0}^{p-1} T_p(t)^2 = \sum_{t=0}^{p-1}\sum_{c,d=1}^{p-1}\Big(\frac{c(c^2-t)}{p}\Big)\Big(\frac{d(d^2-t)}{p}\Big)\\ &= \sum_{c,d=1}^{p-1}\Big(\frac{cd}{p}\Big)\sum_{t=0}^{p-1}\Big(\frac{(t-c^2)(t-d^2)}{p}\Big) \qquad (1)\\ &= \sum_{c,d=1}^{p-1}\Big(\frac{cd}{p}\Big)S_p(-c^2,-d^2).\end{aligned}$$

Wegen Lemma 1 ist hier die letzte Summe weiter gleich

$$(p-1)\sum_{\substack{c,d=1\\ p\mid(c^2-d^2)}}^{p-1}\Big(\frac{cd}{p}\Big) - \sum_{\substack{c,d=1\\ p\nmid(c^2-d^2)}}^{p-1}\Big(\frac{cd}{p}\Big). \qquad (2)$$

Nun ist $p|(c^2 - d^2)$ gleichbedeutend damit, daß modulo p *entweder* $d \equiv c$ *oder* $d \equiv -c$ gilt; wegen $p \equiv 1 \pmod 4$ und dem ersten Ergänzungssatz ist in jedem Fall $(\frac{cd}{p}) = (\frac{c^2}{p}) = 1$ und so ist die erste Summe in (2) gleich $2(p-1)$. Die zweite Summe in (2) ist unter Berücksichtigung von Satz 2.3(ii), (iv)

$$\sum_{c=1}^{p-1}\Big(\frac{c}{p}\Big)\sum_{\substack{d=1\\ d\not\equiv\pm c(p)}}^{p-1}\Big(\frac{d}{p}\Big) = \sum_{c=1}^{p-1}\Big(\frac{c}{p}\Big)\Big(0 - \big(\frac{c}{p}\big) - \big(\frac{-c}{p}\big)\Big) = -2\sum_{c=1}^{p-1}\Big(\frac{c}{p}\Big)^2 = -2(p-1).$$

Beachtet man die Gleichheit von (1) und (2) sowie die zuletzt gefundenen Werte der Summen in (2), so folgt

$$\frac{p-1}{2}(T_p(1)^2 + T_p(t_0)^2) = (p-1)(2(p-1)+2)\ ,$$

was unmittelbar zu (vi) führt. □

Aus (vi) folgt jetzt $|T_p(1)| \leq 2\sqrt{p}$ bei $p \equiv 1 \pmod 4$, was bei großem p natürlich viel besser ist als das sich aus 3(1) trivial mit Dreiecksungleichung ergebende $|T_p(1)| \leq p-1$. Damit kann man aus Satz 3 gewinnen das

Korollar. *Für alle großen Primzahlen p gilt*

$$Q_p(3) = \frac{1}{8}p + O(\sqrt{p}).$$

Dies hat gegenüber Satz 3 den Vorteil einer einheitlichen Formulierung, die überdies die maximale Größenordnung des Anteils $T_p(1)$ in Satz 4 in Evidenz setzt. Dafür aber hat man jetzt für $Q_p(3) - \frac{1}{8}p$ nur noch eine Abschätzung, jedoch keine Gleichheit mehr.

Bemerkung. Nach 3(1) sind alle $T_p(1)$ ganzzahlig und somit sind bei $p \equiv 1 \pmod 4$ in (vi) des Lemmas $T_p(1)$, $T_p(t_0)$ aus Kongruenzgründen beide gerade. Setzt man daher $x := \frac{1}{2}T_p(1)$, $y := \frac{1}{2}T_p(t_0)$, so ist (x, y) eine ganzzahlige Lösung der diophantischen Gleichung

$$X^2 + Y^2 = p. \tag{3}$$

Proposition 1.6.10 lehrt, daß man damit im wesentlichen alle ganzzahligen Lösungen von (3) kennt. An diese Gleichung wird in 4.1.1 unmittelbar angeknüpft.