$|G_1| = \sum_{x=1}^{\frac{p-1}{2}} \left\lfloor \frac{qx}{p} \right\rfloor = T(q,p)$. Ebenso ist

$|G_2| = \sum_{y=1}^{\frac{q-1}{2}} \left\lfloor \frac{py}{q} \right\rfloor = T(p,q)$

$\Rightarrow$ Da $|G| = \frac{(p-1)(q-1)}{4}$ ist $T(p,q) + T(q,p) = \frac{(p-1)(q-1)}{4}$. ∎

Beispiel 6.12 18.07.2018

Wir möchten mit Hilfe der Rechenregeln & dem QR einige Legendre Symbole berechnen:

(a) Wir bestimmen, ob 7 ein quadr. Rest modulo 19 ist.

$\left(\frac{7}{19}\right) \overset{QR}{=} -\left(\frac{19}{7}\right) \overset{6.4\,b)}{=} -\left(\frac{5}{7}\right) \overset{QR+6.4}{=} -\left(\frac{2}{5}\right) \overset{6.8}{=} (-1)^{\frac{5^2-1}{8}} = (-1)^3 = -1$

(b) Wir möchten bestimmen, ob 713 quadr. Rest modulo 1009 ist

Es ist 1009 ist prim & $713 = 23 \cdot 31$

Es ist:

$\left(\frac{23}{1009}\right) \overset{QR}{=} \left(\frac{1009}{23}\right) \overset{6.4\,b)}{=} \left(\frac{2^2 \cdot 5}{23}\right) \overset{6.4\,a)}{=} \left(\frac{5}{23}\right) \overset{QR}{=} \left(\frac{23}{5}\right) \overset{6.4\,b)}{=} \left(\frac{3}{5}\right)$

$\overset{QR}{=} \left(\frac{5}{3}\right) \overset{6.4\,b)}{=} \left(\frac{2}{3}\right) \overset{6.8}{=} -1$

$\left(\frac{31}{1009}\right) \overset{QR+6.4\,b)}{=} \left(\frac{17}{31}\right) \overset{QR+6.4\,b)}{=} \left(\frac{14}{17}\right) \overset{6.4\,a)}{=} \left(\frac{2}{17}\right)\left(\frac{7}{17}\right) \overset{6.8}{=} (-1)^{36}\left(\frac{7}{17}\right)$

$\overset{QR+6.4\,b)}{=} \left(\frac{3}{7}\right) \overset{QR+6.4\,b)}{=} -\left(\frac{1}{3}\right) = -1$

$\Rightarrow \left(\frac{713}{1009}\right) = (-1)\cdot(-1) = 1$

(c) Wir möchten überprüfen, ob die Gleichung $x^2 \equiv 13 \bmod 76$ lösbar ist. Es ist $76 = 4 \cdot 19$ & nach CRS ist die obige Gleichung genau dann lösbar, wenn das System

$$\begin{cases} x^2 \equiv 13 \bmod 4 \\ x^2 \equiv 13 \bmod 19 \end{cases}$$ lösbar ist.

Wir berechnen: $\left(\frac{13}{19}\right) \overset{QR+6.4}{=} \left(\frac{6}{13}\right) = \left(\frac{2}{13}\right)\left(\frac{3}{13}\right) \overset{6.8}{=} (-1)\left(\frac{3}{13}\right) \overset{QR\ 6.4}{=} (-1)\underbrace{\left(\frac{1}{3}\right)}_{=1} = -1$

Damit ist das System nicht lösbar & somit auch nicht die ursprüngliche Gleichung $x^2 \equiv 13 \bmod 76$.

Das Jacobi-Symbol

Definition 6.13

Sei $n \in \mathbb{N}$ & $a \in \mathbb{Z}$ mit $ggT(a,n) = 1$. Sei ferner $n = p_1 \cdot \ldots \cdot p_r$ die Primfaktorzerlegung von n.

Das Jacobi-Symbol $\left(\frac{a}{n}\right)$ ist definiert als: $\left(\frac{a}{n}\right) = \prod_{i=1}^{r} \underbrace{\left(\frac{a}{p_i}\right)}_{\text{Legendre-Symbol}}$

Bemerkung 6.14

- Ist $\left(\frac{a}{n}\right) = -1$, so ist die Kongruenz $x^2 \equiv a \bmod n$ nicht lösbar
- Ist $\left(\frac{a}{n}\right) = 1$, so folgt lediglich, dass die Anzahl der Primzahlen p_i mit $\left(\frac{a}{p_i}\right) = -1$ gerade ist.

Dies verrät uns also nichts über die Lösbarkeit der Gleichung $x^2 \equiv a \bmod n$.

Satz 6.15

Seien n und n' ungerade natürliche Zahlen

a) Falls $a \equiv a' \bmod n$, so ist $\left(\frac{a}{n}\right) = \left(\frac{a'}{n}\right)$

b) $\left(\frac{a}{n}\right)\left(\frac{a}{n'}\right) = \left(\frac{a}{n \cdot n'}\right)$, $\left(\frac{a}{n}\right) \cdot \left(\frac{a'}{n}\right) = \left(\frac{a \cdot a'}{n}\right)$

Beweis:

Folgt aus den Rechengesetzen für das Legendre Symbol (+Def $\left(\frac{a}{n}\right)$)

Satz 6.16 (Quadratisches Reziprozitätsgesetz für das Jacobi-Symbol)

Es gilt:

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

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

c) $\left(\frac{n}{m}\right) \cdot \left(\frac{m}{n}\right) = (-1)^{\frac{(n-1)(m-1)}{4}}$

Beweis:

Rosen 9.5 + 9.6

Beispiel 6.17

Mit dem Jacobi-Symbol kann man effizient Legendre-Symbole berechnen. (383 & 443 sind PZ)

$$\left(\frac{383}{443}\right) \overset{QR}{=} -\left(\frac{443}{383}\right) \overset{6.15\ a)}{=} -\left(\frac{2^2 \cdot 15}{383}\right) \overset{6.4\ c)}{=} -\left(\frac{15}{383}\right) \overset{QR}{=} \left(\frac{383}{15}\right) \overset{6.15}{=} \left(\frac{2^3}{15}\right)$$

$$= \left(\frac{2}{15}\right) = 1$$

Da man Jacobi-Symbole & modulare Potenzen effizient ausrechnen kann, ist der folgende Primzahltest entwickelt worden.

Algorithmus 6.18 (Solovey-Strassen-Primzahltest)

Wollen testen, ob $n \in \mathbb{N}$ eine Primzahl ist

(1) Wähle $0 < a < n$ & berechnen $ggT(a,n)$. Ist $ggT \neq 1$, so kann n nicht prim sein

(2) Falls $ggT(a,n) = 1$ berechne $[b] = [a^{\frac{n-1}{2}}] \in (\mathbb{Z}/n\mathbb{Z})^*$

Ist $[b] \neq [1]$ oder $[-1]$, so kann n nach dem kleinen Satz von Fermat keine Primzahl gewesen sein. (Bem. $a^{p-1} \equiv 1 \bmod p$ $\Rightarrow a^{\frac{p-1}{2}} \equiv \pm 1 \bmod p$ vgl. Bew. von 6.3)

(3) Teste für das Jacobi-Symbol die Kongruenz $\left(\frac{a}{n}\right) \equiv b \bmod n$

$$\equiv a^{\frac{n-1}{2}}$$

Gilt dies nicht, so ist das Eulersche Krit. (6.3) verletzt & n ist nicht prim.

(4) Andernfalls kann man keine Aussage machen & man fängt erneut mit (1) an.

Nach k Durchläufen ist die Wahrscheinlichkeit, dass n zus. gesetzt ist $\leq \left(\frac{1}{2}\right)^k$ (siehe Rosen 9.11)

Bemerkung / Definition:

Sei n eine zusammengesetzte Zahl & $b \in \mathbb{Z}$. Dann heißt n Eulersche Pseudoprimzahl zur Basis b, falls $\left(\frac{b}{n}\right) \equiv b^{\frac{n-1}{2}} \bmod n$

Welche Zahlen sind Summe von zwei Quadraten?

$1 = 0^2 + 1^2$	$6 =$ Nein!	$11 =$ Nein!
$2 = 1^2 + 1^2$	$7 =$ Nein!	$12 =$ Nein!
$3 =$ Nein!	$8 = 2^2 + 2^2$	$13 = 2^2 + 3^2$
$4 = 0^2 + 2^2$	$9 = 0^2 + 3^2$	$14 =$ Nein!
$5 = 1^2 + 2^2$	$10 =$ Nein!	

Sehen kein erkennbares Schema.

Die Primzahlen < 30, die sich als Summe von zwei Quadraten schreiben lassen sind 2, 5, 13, 17, 29

→ Für alle diese Primzahlen ist $p=2$ oder $p \equiv 1 \bmod 4$

Lemma 6.19

Sei $n = a^2 + b^2$ $(a, b \in \mathbb{Z})$, dann ist $n \not\equiv 3 \bmod 4$

Beweis: Die quadr. Reste modulo 4 sind 0 und 1

Falls $n = a^2 + b^2$ so ist n kongruent zu $0+0, 0+1, 1+0, 1+1 \bmod 4$.

Bemerkung 6.20

Für eine Primzahl $n=p$ können wir das obige Lemma auch wie folgt beweisen:

Sei $p = a^2 + b^2$. Da p prim sind a, b teilerfremd

$$\Rightarrow (a^2) \equiv (-b)^2 \bmod p \Rightarrow 1 = \left(\frac{a^2}{p}\right) = \left(\frac{-b}{p}\right) = \left(\frac{-1}{p}\right)\underbrace{\left(\frac{b^2}{p}\right)}_{=1} = \left(\frac{-1}{p}\right)$$

Kor. 6.5 sagt

"$1 = \left(\frac{-1}{p}\right)$" $\Leftrightarrow$ "$p \equiv 1 \bmod 4$"

Genauer gilt für Primzahlen auch die Umkehrung von Lemma 6.19

Satz 6.21

Eine Primzahl p ist genau dann Summe von zwei Quadraten, wenn $p=2$ oder $p \equiv 1 \bmod 4$ gilt.

Beweis:

Es bleibt zu zeigen, dass sich p als $p = a^2 + b^2$ schreiben lässt, falls $p \equiv 1 \mod 4$. Die Beweismethode hierzu nennt man Fermat's Abstiegsargument.

Sei also p eine Primzahl mit $p \equiv 1 \mod 4$. Aus Bem. 6.20 folgt, dass $\left(\frac{-1}{p}\right) = 1$

$\Rightarrow$ Es ex. also ein A mit $0 < A < p$ & $A^2 \equiv -1 \mod p$

Wir wählen $m \in \mathbb{Z}$ mit $A^2 + 1 = m \cdot p$

Wegen $m \leq \frac{A^2+1}{p}$ & $0 \leq A < p$ folgt $m \leq \frac{(p-1)^2+1^2}{p} = p - \frac{2(p-1)}{p} < p$

Ist $m = 1$ so sind wir fertig denn dann ist $A^2 + 1^2 = 1 \cdot p$

Sei also $m > 1$. Wir definieren $a_0 := A$ & $b_0 = 1$ & $m_0 = m$

Wir wollen Zahlen a_1, b_1 & m_1 finden mit $a_1^2 + b_1^2 = m_1 \cdot p$ & $m_1 < m_0 = m$. Dies wiederholen wir dann bis schließlich $m_r = 1$ ist.

(Dann ist $m_r \cdot p = p = a_r^2 + b_r^2$)

Wir werden im Folgenden die folgende Identität benutzen

$(*)$ $(u^2+v^2)(A^2+B^2) = (u \cdot A + v \cdot B)^2 + (v \cdot A - u \cdot B)^2$

Fermat's Abstiegsargument: Gegeben sei ein Tripel von Zahlen (a_i, b_i, m_i) mit $1 < m_i < p$ & $a_i^2 + b_i^2 = m_i \cdot p$.

Wir suchen $(a_{i+1}, b_{i+1}, m_{i+1})$ mit $a_{i+1}^2 + b_{i+1}^2 = m_{i+1} p$ & $m_{i+1} < m_i$.

Wähle u_i, v_i mit $-\frac{m_i}{2} < u_i, v_i \leq \frac{m_i}{2}$ & $u_i \equiv a_i \mod m_i$, $v_i \equiv b_i \mod m_i$

Es gilt also $0 \equiv a_i^2 + b_i^2 \equiv u_i^2 + v_i^2 \mod m_i$

Schreiben $u_i^2 + v_i^2 = m_i \cdot r_i$. Es gilt

1) $1 \leq r_i < m_i$

2) $m_i \mid (u_i a_i + v_i b_i)$ } klar, wegen Def. der u_i, v_i

3) $m_i \mid (u_i a_i - v_i b_i)$ }

zu 1) Wir bemerken, dass $r_i = \frac{u_i^2 + v_i^2}{m_i} \leq \frac{\left(\frac{m_i}{2}\right)^2 + \left(\frac{m_i}{2}\right)^2}{m_i} = \frac{1}{2} m_i < m_i$

/A: $r_i = 0 \Rightarrow u_i^2 + v_i^2 = 0 \Rightarrow u_i = v_i = 0$

$\Rightarrow a_i \equiv b_i \equiv 0 \mod m_i \Rightarrow m_i^2$ ist ein Teiler von $a_i^2 + b_i^2 = m_i \cdot p$

$\Rightarrow m_i = 1$ ↯ zu $1 < m_i < p$

Also gilt $1 < r_i < m_i$

Mit Hilfe von (*) schreiben wir

(*2) $m_i^2 \cdot r_i \cdot p = \underbrace{(u_i^2 + v_i^2)}_{m_i \cdot r_i} \cdot \underbrace{(a_i^2 + b_i^2)}_{m_i \cdot p} \overset{(*)}{=} (u_i \cdot a_i + v_i \cdot b_i)^2 + (v_i a_i - u_i b_i)^2$

Wir definieren:

$a_{i+1} := \frac{u_i \cdot a_i + v_i b_i}{m_i}$, $b_{i+1} := \frac{v_i \cdot a_i - u_i b_i}{m_i}$, $m_{i+1} = r_i$

Mit (*2) folgt $(a_{i+1})^2 + (b_{i+1})^2 = m_{i+1} \cdot p$ mit $m_{i+1} \overset{(1)}{<} m_i$

Induktiv folgt nun die Existenz eines Tripels (a_r, b_r, m_r)

mit $m_r = 1$ & $m_r \cdot p = p = a_r^2 + b_r^2$ □

Satz 6.22

Sei $n \in \mathbb{N}$ mit Primfaktorzerlegung $n = \prod_i p_i^{e_i}$ (mit $p_i \neq p_j$ für $i \neq j$)

Die Zahl n lässt sich genau dann als Summe von zwei Quadraten schreiben, wenn eine der folgenden Bedingungen erfüllt ist:

(1) $p_i = 2$ $\forall i$

(2) e_i ist gerade $\forall i$

(3) $p_i \equiv 1 \mod 4$ $\forall i$

} Für alle p_i in der Primfaktorzerlegung von n mit $p_i \equiv 3 \mod 4$ ist e_i gerade.

Beweis:

Ist $n_1 = a^2 + b^2$ & $n_2 = c^2 + d^2$ so ist wegen der Identität (*) auch $n_1 \cdot n_2$ eine Summe von 2 Quadraten. Der Satz folgt also aus Satz 6.21. & wiederholtes Anwenden von (*) □

Man kann ähnliche Sätze auch für Summen von drei bzw. vier Quadraten beweisen.

Satz 6.23 (Drei Quadrate Satz von Gauß)

$n \in \mathbb{N}$ ist genau dann Summe von 3 Quadraten, wenn n nicht von der Form $n = 4^i \cdot (7+8k)$ für $i,k \in \mathbb{N}$.

Satz 6.24 (Vier Quadrate Satz von Lagrange)

Jede natürliche Zahl lässt sich als Summe von 4 Quadraten schreiben.

Für die Beweise: siehe Müller-Stach & Piontkowski "Elementare & algebraische Zahlentheorie" → Satz 9.4 & 9.6 □