Mathematisches Institut
Abt. für Reine Mathematik
Dr. K. Halupczok

06.07.2006

Übungen zur Vorlesung

Elementare Zahlentheorie

SoSe 2006

Musterlösung Blatt 9

Aufgabe 1.

Beweise die beiden Ergänzungsgesetze für das Jacobi-Symbol.

1.Beh.: Für $m \in \mathbb{N}$ ungerade gilt $(\frac{-1}{m}) = (-1)^{\frac{m-1}{2}}$, das 1. EG für das Jacobi-Symbol.

Bew.: Sei $m = \prod_{i=1}^{r} p_i, \quad p_i > 2$ prim, nicht notwendig verschieden.
Dann ist

$$\left(\frac{-1}{m}\right) = \prod_i \left(\frac{-1}{p_i}\right) \overset{1.\text{EG}}{=} \prod_i (-1)^{\frac{p_i-1}{2}} = (-1)^{\sum_i \frac{p_i-1}{2}} \overset{!}{=} (-1)^{\frac{m-1}{2}}$$

Zu zeigen ist also: $\sum_{i=1}^{r} \frac{p_i-1}{2} \equiv \frac{m-1}{2}$ (2), d.h. die Exponenten haben dieselbe Parität.
Vollständige Induktion nach r, $r = 1$✓
OBdA $r \geq 2, r-1 \rightsquigarrow r$: Es gilt:

$$\begin{aligned}\frac{p_1 \cdots p_{r-1} - 1}{2} - \frac{p_r + 1}{2} + \frac{p_1 \cdots p_{r-1} p_r - 1}{2} &\equiv \frac{p_1 \cdots p_{r-1}(1+p_r) - p_r - 1}{2} \\ &= \frac{1}{2}(p_1 \cdots p_{r-1} - 1)(1 + p_r) \\ &\equiv 0 \ (2)\end{aligned}$$

da $(p_1 \cdots p_{r-1} - 1)$ und $(1 + p_r)$ gerade. Also ist:

$$\begin{aligned}\frac{m-1}{2} = \frac{p_1 \cdots p_{r-1} - 1}{2} &\equiv \frac{p_r - 1}{2} \overset{(*)}{-} \frac{p_1 \cdots p_{r-1} - 1}{2} \\ &\overset{\text{I.A.}}{\equiv} \frac{p_r - 1}{2} + \sum_{i=1}^{r-1} \frac{p_i - 1}{2} \ (2)\end{aligned}$$

wobei bei $(*)$ + oder − bezgl. mod 2 egal ist.

2.Beh.: Für $m \in \mathbb{N}$ ungerade gilt $(\frac{2}{m}) = (-1)^{\frac{m^2-1}{8}}$, das 2. EG für das Jacobi-Symbol

Bew.: Sei $m = \prod_{i=1}^{r} p_i, p_i > 2$ prim, nicht notwendig verschieden.
Dann ist:

$$\left(\frac{2}{m}\right) = \prod_i \left(\frac{2}{p_i}\right) \overset{2.\text{EG}}{=} \prod_i (-1)^{\frac{p_i^2-1}{8}} = (-1)^{\sum_i \frac{p_i^2-1}{8}} \overset{!}{=} (-1)^{\frac{m^2-1}{8}}$$

Zu zeigen ist also: $\sum_{i=1} r\frac{p_i^2-1}{8} \equiv \frac{m^2-1}{8}$ (2), d.h. die Exponenten haben dieselbe Parität.
Vollständige Induktion nach r, $r = 1$✓
OBdA $r \geq 2, r-1 \rightsquigarrow r$: Es gilt:

$$\begin{aligned}\frac{p_1^2 \cdots p_{r-1}^2 - 1}{8} + \frac{p_r^2 - 1}{8} + \frac{p_1^2 \cdots p_r^2 - 1}{8} &= \frac{p_1^2 \cdots p_{r-1}^2(1 + p_r^2) + (p_r^2 + 1) - 4}{8} \\ &= \frac{1}{8}((p_1^2 \cdots p_{r-1}^2 + 1)(p_r^2 + 1) - 4) \\ &= \frac{1}{8}(16k + 16l + 8^2 \cdot lk) \equiv 0\ (2)\end{aligned}$$

mit $(p_1^2 \cdots p_{r-1}^2 + 1) := 2 + 8l$ und $(p_r^2 + 1) := 2 + 8k$, denn ungerade Quadrate sind $\equiv 1$ (8). Also ist:

$$\begin{aligned}\frac{m-1}{8} = \frac{p_1^2 \cdots p_r^2 - 1}{8} &\overset{(*)}{\equiv} \frac{p_r^2 - 1}{8} + \frac{p_1^2 \cdots p_{r-1}^2 - 1}{8} \\ &\overset{\text{I.A.}}{\equiv} \frac{p_r^2 - 1}{8} + \sum_{i=1}^{r-1} \frac{p_i^2 - 1}{8}\ (2)\end{aligned}$$

wobei die Vorzeichen in $(*)$ mod 2 egal sind.

Aufgabe 2. *Zeige:*

(a) *Für jedes $n \geq 3$ gibt es ein pythagoräisches Tripel (x, y, z), so daß n gleich einer der Zahlen x, y oder z ist.*

Beh.: $\forall n \geq 3 \exists$ pyth. Tripel $(x, y, z) : n = x \vee n = y \vee n = z$

Bew.: 1.Fall: $2 \nmid n$, etwa $n = 2k + 1$.
Dann: $n = (k+1)^2 - k^2$ mit $a = k + 1, b = k$ tut's dann $(n = a^2 - b^2, 2ab, a^2 + b^2)$.
2.Fall: $2 \mid n$, etwa $n = 2^t m, 2 \nmid m$.
Fall a): $t \geq 2 \rightsquigarrow$ wähle $a = 2^{t-1}m, b = 1$, dann tut's $(a^2 - b^2, 2ab = n, a^2 + b^2)$.
Fall b): $t = 1 \rightsquigarrow n = 2m$ mit $2 \nmid m$. Für m gibt es nach Fall 1 ein pyth. Tripel (x, y, z) mit $x = m$, dann tut's $(2x = n, 2y, 2z)$.

(b) *Ist n nicht als Summe zweier Quadrate darstellbar, so kann sie auch nicht als Summe von zwei Quadraten rationaler Zahlen darstellt werden.*

Beh.: n nicht Summe von zwei Quadraten $\Rightarrow n$ nicht Summe von zwei Quadraten rationaler Zahlen.

Bew.: Sonst: $n = (\frac{x_1}{y_1})^2 + (\frac{x_2}{y_2})^2 \Leftrightarrow n(y_1y_2)^2 = (x_1y_2)^2 + (x_2y_2)^2$.
Da n nicht als Summe von 2 Quadraten geschrieben werden kann, gibt es nach dem Satz von Euler einen Primfaktor $p \equiv 3\ (4)$ von m mit: $p^k \mid n, p^{k+1} \nmid n, k$ ungerade.
In der Gleichung $n(y_1y_2)^2 = (x_1y_2)^2+(x_2y_2)^2$ tritt auf der linken Seite der Primfaktor p mit ungeradem Exponenten auf, auf der rechten Seite mit geradem Exponenten, da die rechte Seite ja Summe von 2 Quadraten ist.
$\rightsquigarrow$ Widerspruch, also läßt sich n auch nicht als Summe von 2 Quadraten rationaler Zahlen schreiben.

Aufgabe 3.

Zeige:

(a) *Sei n auf zwei verschiedene Arten in eine Summe von zwei Quadraten zerlegt:*

$$n = s^2 + t^2 = u^2 + v^2,\ s \geq t > 0,\ u \geq v > 0,\ s > u.$$

Dann ist $d := (su - tv, n)$ ein nichttrivialer Teiler von n.

Vor.: $n = s^2 + t^2 = u^2 + v^2, s \geq t > 0, u \geq v > 0, s > u.$

Beh.: $d := (su - tv, n)$ ist nicht trivialer Teiler von n, d.h. $d \neq 1, d \neq n$.

Bew.: Klar: $d \mid n$. Da $s^2 \equiv -t^2\ (n), u^2 \equiv -v^2\ (n)$, ist $s^2u^2 \equiv t^2v^2\ (n)$, also gilt $n \mid (su + tv)(su - tv)$.
Es ist $n^2 = (s^2 + t^2)(u^2 + v^2) = (su + tv)^2 + (sv - tu)^2$ mit $su + tv < n \Rightarrow sv - tu > 0$ und $sv > tu$, da $s > u$ und $v > t$ aus $v > s$ und Glg., also $0 < su + tv < n$.
Weiter ist $0 < su - tv$ (da $s > u \geq v, t < v \leq u \rightsquigarrow su > tv$) und $su-tv < n$ (da $n^2 = (sv+tv)^2+(su-tv)^2$ mit $sv+tv > 0 \Rightarrow su-tv < n$)
Wegen $n \mid (su-tv)(su-tv)$ mit $0 < su-tv < n, 0 < su-tv < n$ haben dann $su-tv\ (< n)$ und n einen nichttrivialen gemeinsamen Teiler, somit ist $d = (su - tv, n)$ nichttrivialer Teiler von n.

(b) *Ist $n = pq$ mit $p, q \equiv 1\ (4)$, so läßt sich n auf zwei verschiedene Arten als Summe von zwei Quadraten schreiben.*

** Liefert (a) dann ein geeignetes Faktorisierungsverfahren?*

Beh.: Ist $n = pq$ mit $p, q \equiv 1\ (4)$, so läßt sich n auf zwei verschiedene Arten als Summe von 2 Quadraten schreiben.

Bew.: p und q lassen sich als Summe von 2 Quadraten schreiben, etwa $p = x_1^2 + x_2^2$, und $q = y_1^2 + y_2^2$ mit $x_1, x_2, y_1, y_2 > 0$.
Dann ist $n = pq = (x_1y_1 - x_2y_2)^2 + (x_1y_2 + x_2y_1)^2 = (x_1y_1 + x_2y_2)^2 + (x_2y_1 - x_1y_2)^2$.
Die Darstellungen sind verschieden:
Es ist $x_1y_1 - x_2y_2 \neq x_1x_1 + x_2y_2$, sonst wäre $2x_2y_2 = 0$, ein Widerspruch und $x_1y_1 - x_2y_2 \neq -x_1y_1 - x_2y_2$, sonst wäre $2x_1y_1 = 0$, ein Widerspruch sowie $x_1y_1-x_2y_2 \neq x_2y_1-x_1y_2$, sonst wäre $0 = (x_1-x_2)y_1+(x_1-x_2)y_2 =$

$(x_1 - x_2)(y_1 + y_2)$ mit $x_1 - x_2 \neq 0$, sonst p gerade und $y_1 + y_2 \neq 0$ sonst q gerade
und $x_1y_1 - x_2y_2 \neq -x_2y_1 + x_1y_2$, sonst wäre $0 = (y_1 - y_2)x_1 + (y_1 - y_2)x_2 = (y_1 - y_2)(x_1 + x_2)$ mit $y_1 - y_2 \neq 0$, sonst q gerade und $x_1 + x_2 \neq 0$ sonst p gerade.

* Zur Frage, ob (a) ein geeignetes Faktorisierungsverfahren liefern würde: Ja, falls es einfach wäre, für $n = pq$ die zwei Darstellungen als Summe von zwei Quadraten zu finden. Dafür gibt es - außer Probieren - kein Verfahren, und Probieren geht zu lange. Obiger Existenzbeweis in (b) geht davon aus, daß die Faktorisierung von n in Faktoren p und q bekannt ist.

Aufgabe 4.

Zeige:

(a) *Die diophantische Gleichung $x^4 - y^4 = z^2$ hat keine Lösung in natürlichen Zahlen x, y und z.*

Beh.: $x^4 - y^4 = z^2$ hat keine Lösung $(x, y, z) \in \mathbb{N}^3$

Bew.: Sei sonst (x, y, z) Lösung mit x minimal
Dann: $(x, y) = 1$, sonst: $d := (x, y) > 1 \rightsquigarrow x = dx_1, y = dy_1 \rightsquigarrow d^4(x_1^4 - y_1^4) = z^2$ mit $(x_1, y_1) = 1 \rightsquigarrow$ Gleichung ist mit d^4 kürzbar und $x_1^4 - y_1^4 = z_1^4$ im Widerspruch zur Minimalität von x.
Weiter ist x ungerade. Es ist:
$z^2 + (y^2)^2 = (x^2)^2$ mit $(x^2, y^2) = 1 \rightsquigarrow (z, y^2) = 1 \rightsquigarrow (z, y^2, x^2)$ phytagoräisches Tripel mit $(z, y^2) = 1 \rightsquigarrow x^2$ ungerade $\rightsquigarrow x$ ungerade.

1.Fall y ungerade
Dann: z gerade und (z, y^2, x^2) phyt. Tripel mit $(z, y^2) = 1, 2 \mid z$, also $z = 2ab, y^2 = a^2 - b^2, x^2 = a^2 + b^2$ für $a > b > 0, (a, b) = 1, a + b \equiv 1\ (2)$. $\rightsquigarrow a^4 - b^4 = (a^2 + b^2)(a^2 - b^2) = x^2y^2 = (xy)^2$, d.h. (a, b, xy) Lösung, aber $0 < a < \sqrt{a^2 + b^2} = x$, im Widerspruch zu x minimal.

2.Fall y gerade
Dann: z ungerade und (z, y^2, x^2) pyth. Tripel mit $(z, y^2) = 1, 2 \mid y^2$, also $y^2 = 2ab, z = a^2 - b^2, x^2 = a^2 + b^2$ für $a > b > 0, (a, b) = 1, a + b \equiv 1\ (2)$. Sei OBdA a gerade, b ungerade (sonst folgendes analog).
Mit $y^2 = (2a)b$ und $(2a, b) = 1$ folgt dann:
$2a = w^2, b = v^2$ und $w = 2u$, also $a = 2u^2$.
Somit: $x^2 = a^2 + b^2 = 4u^4 + v^4 \rightsquigarrow$ pyth. Tripel $(2u^2, v^2, x)$ mit $(2u^2, v^2) = (4u^2, v^2) = (w^2, v^2) = (2a, b) = 1$
$\rightsquigarrow$ es ex. $s > t > 0$ mit $2u^2 = 2st, v^2 = s^2 - t^2, x = s^2 + t^2$ und $(s, t) = 1$. Aus $u^2 = st$ folgt $s = c^2, t = d^2$, sowie $v^2 = s^2 - t^2 = c^4 - d^4$, d.h. (c, d, v) Lösung mit $0 < c < s^2 + t^2 = x$ im Widerspruch zur Minimalität von x.

(b) *Die Fläche eines pythagoräischen Dreiecks (rechtwinklig mit ganzzahligen Seitenlängen) kann nie eine Quadratzahl sein.*

Beh.: Es existiert kein pythagoräisches Dreieck, dessen Flächeninhalt Quadratzahl ist.

Bew.: Sonst $x^2 + y^2 = z^2$ mit $\frac{1}{2}xy = u^2 \rightsquigarrow 2xy = 4u^4$, also $(x+y)^2 = z^2 + 4u^2, (x-y)^2 = z^2 - 4u^2$. Die Gleichungen miteinander Multiplizieren ergibt: $(x^2 - y^2)^2 = ((x+y)(x-y))^2 = (x+y)^2(x-y)^2 = z^4 - 16u^4 = z^4 - (2u)^4$ im Widerspruch zu (a)