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

29.06.2006

Übungen zur Vorlesung

Elementare Zahlentheorie

SoSe 2006

Musterlösung Blatt 8

Aufgabe 1.

Zeige:

(a) *Für alle ungeraden Primzahlen* $q < 41$ *gilt* $\left(\dfrac{-163}{q}\right) = -1$.

Beh.: $\forall q < 41$ prim, $q > 2$ gilt: $\left(\frac{-163}{q}\right) = -1$

Bew.: $\left(\frac{-163}{3}\right) = \left(\frac{2}{3}\right) = -1$, $\left(\frac{-163}{5}\right) = \left(\frac{2}{5}\right) = -1$, $\left(\frac{-163}{7}\right) = \left(\frac{-2}{7}\right) = -\left(\frac{2}{7}\right) = -1$, $\left(\frac{-163}{11}\right) = \left(\frac{2}{11}\right) = -1$, $\left(\frac{-163}{13}\right) = \left(\frac{6}{13}\right) = \left(\frac{2}{13}\right)\cdot\left(\frac{3}{13}\right) = -\left(\frac{13}{3}\right) = -1$, $\left(\frac{-163}{19}\right) = \left(\frac{8}{19}\right) = -1$, $\left(\frac{-163}{23}\right) = \left(\frac{-2}{23}\right) = -\left(\frac{2}{23}\right) = -1$, $\left(\frac{-163}{29}\right) = \left(\frac{11}{29}\right) = \left(\frac{29}{11}\right) = \left(\frac{-4}{11}\right) = -1$, $\left(\frac{-163}{31}\right) = \left(\frac{-8}{31}\right) = \left(\frac{2}{31}\right)\cdot\left(\frac{-1}{31}\right) = -1$, $\left(\frac{-163}{37}\right) = \left(\frac{22}{37}\right) = \left(\frac{2}{37}\right)\cdot\left(\frac{11}{37}\right) = -\left(\frac{27}{11}\right) = -\left(\frac{4}{11}\right) = -1$.

(b) *(Euler) Das Polynom* x^2-x+41 *nimmt an den* 41 *Stellen* $x = 0, 1, \ldots, 40$ *nur Primzahlen als Werte an.*
Hinweis: $4n^2 - 4n + 4\cdot 41 = (2n-1)^2 + 4\cdot 41 - 1$.

Beh.: $x^2 - x + 41$ nimmt an $x = 0, 1, \ldots, 40$ nur PZ als Werte an.

Bew.: Annahme: n^2-n+41 zusammengesetzt mit kleinstem Primteiler q. Dann $2 < q < 41$, da $n^2 - n + 41 = n(n-1) + 41 \leq 40\cdot 39 + 41 < 41^2$. Wegen $4n^2 - 4n + 41\cdot 4 = (2n-1)^2 + 4\cdot 41 - 1 = (2n-1)^2 + 163 \equiv 0\ (q)$ folgt, daß -163 ein qR mod q ist, d.h. $\left(\frac{-163}{q}\right) = 1$ im Widerspruch zu (a).

Aufgabe 2.

(a) *Bestimme alle Lösungen der Kongruenz* $x^4 - 6x^2 + 35 \equiv 0\ (43)$.

Beh.: Die Kongruenz $x^4 - 6x^2 + 35 \equiv 0\ (43)$ hat keine Lösung $x \in \mathbb{Z}$.

Bew.: Quadratische Ergänzung zeigt:
$x^4 - 6x^2 + 35 \equiv 0\ (43) \Leftrightarrow x^4 - 2\cdot 3x^2 + 9 \equiv -35 + 9 \equiv 17\ (43) \Leftrightarrow (x^2-3)^2 \equiv 17\ (43)$.
Die Kongruenz $y^2 \equiv 17\ (43)$ ist lösbar, denn

$$\left(\frac{17}{43}\right) = \left(\frac{43}{17}\right)\cdot(-1)^{\frac{42}{2}\cdot\frac{16}{2}} = \left(\frac{9}{17}\right) = 1$$

Sie hat dann auch genau 2 Lösungen, nämlich: $x_0 \equiv 17^{\frac{43+1}{2}} = 17^{11} \equiv 24\ (43)$ und $x_1 \equiv 43 - 24 = 19\ (43)$. Nun sind die Kongruenzen $x^2 - 3 \equiv 24\ (43)$ und $x^2 - 3 \equiv 19\ (43)$ auf Lösbarkeit zu überprüfen, also $x^2 \equiv 27\ (43)$ und $x^2 \equiv 22\ (43)$.
Da $\left(\frac{27}{43}\right) = \left(\frac{3}{43}\right) = -\left(\frac{43}{3}\right) = -\left(\frac{1}{3}\right) = -1$ und $\left(\frac{22}{43}\right) = \left(\frac{2}{43}\right) \cdot \left(\frac{11}{43}\right) = (-1) \cdot (-1) \cdot \left(\frac{43}{11}\right) = \left(\frac{-1}{11}\right) = -1$ sind diese Kongruenzen unlösbar, also ist auch die ursprüngliche Kongruenz unlösbar.

(b) *Sei $p > 2$. Zeige: Dann hat die Kongruenz $ax^2 + bx + c \equiv 0\ (p)$, $p \nmid a$, genau $1 + \left(\frac{b^2 - 4ac}{p}\right)$ viele Lösungen. Wie berechnet man diese?*
***Bemerkung:** Das Legendresymbol wird $= 0$ gesetzt, falls $p \mid (b^2 - 4ac)$.*

Vor.: $p > 2$ prim.

Beh.: Die Kongruenz $ax^2 + bx + c \equiv 0\ (p)$, $p \nmid a$ hat genau $1 + \left(\frac{b^2 - 4ac}{p}\right)$ viele Lösungen. (Berechnung der Lösungen im Beweis)
(Bem.: Legendresymbol $:= 0$, falls $p \mid (b^2 - 4ac)$.)

Bew.: Es ist

$$\begin{aligned} & ax^2 + bx + x \equiv 0\ (p) \\ \Leftrightarrow\ & 4a^2x^2 + 4abx + 4ac \equiv 0\ (p) \\ \Leftrightarrow\ & (2ax + b)^2 \equiv b^2 - 4ac\ (p) \qquad (*) \end{aligned}$$

1.Fall $p \mid (b^2 - 4ac)$, dann ist die rechte Seite von $(*) \equiv 0\ (p)$, zu lösen ist dann $2ax + b \equiv 0\ (p) \Leftrightarrow x \equiv -b \cdot (2a)^*\ (p)$, da $p \nmid (2a)$ und dem Inversen $(2a)^*$ von $2a$ mod p. Dies ist dann die einzige Lösung.

2.Fall $p \nmid (b^2 - 4ac)$ und $\left(\frac{b^2-4ac}{p}\right) = -1$, dann ist $(*)$ unlösbar, da $b^2 - 4ac$ in diesem Fall kein qR ist. $\rightsquigarrow$ keine Lösung.

3.Fall $p \nmid (b^2 - 4ac)$ und $\left(\frac{b^2-4ac}{p}\right) = 1$, dann ist $(*)$ lösbar:
Die Kongruenz $y^2 \equiv b^2 - 4ac\ (p)$ hat genau 2 Lösungen (Wurzelziehalgorithmus), und mit $2ax + b \equiv y\ (p) \Leftrightarrow x \equiv (y - b) \cdot (2a)^*\ (p)$ gibt es dann genau 2 Lösungen für $(*)$ bzw. die Ausgangskongruenz.

Aufgabe 3.

Zeige, daß es unendlich viele Primzahlen der Form $5k - 1$ gibt.
***Hinweis:** Für jedes $n > 1$ hat $5(n!)^2 - 1$ einen Primteiler $p > n$ der Form $5k - 1$.*

Beh.: Es gibt unendlich viele Primzahlen der Form $5k - 1$, d.h. p mit $p \equiv -1\ (5)$.

Bew.: Die Zahl $5(n!)^2 - 1$ ist ungerade, hat also nur Primfaktoren > 2. Sei p ein solcher Primfaktor, also: $5(n!)^2 \equiv 1\ (p) \rightsquigarrow (5n!)^2 \equiv 5\ (p)$, d.h. 5 ist qR mod p, also hat p entweder die Form $5k + 1$ oder $5k - 1, k \geq 2$, da

$\left(\frac{p}{5}\right) = \left(\frac{5}{p}\right)$ und die einzigen Quadrate mod 5 sind 1 und $-1 = 2^2$ (von der 0 abgesehen).
Nun hat $5(n!)^2 - 1$ die Form $5k-1$, also können nicht alle Primfaktoren davon die Form $5k+1$ haben, denn deren Produkt wäre ebenfalls von der Form $5k+1$. Nun gilt für alle Primfaktoren p von $5(n!)^2 - 1$ die Ungleichung $p > n$. [Wäre sonst $p \leq n$, gälte $5(n!)^2 \equiv 0\ (p)$, da p in $n!$ enthalten wäre, im Widerspruch zu $5(n!)^2 \equiv 1\ (p)$.] Also existiert ein Primfaktor $p > n$ von $5(n!)^2 - 1$ der Form $5r - 1$, d.h.

$$\forall n > 1\ \exists\ p \text{ prim }, p = 5k - 1 : n < p < 5(n!)^2.$$

Also gibt es unendlich viele PZ $\equiv -1\ (5)$.

Aufgabe 4.

*Sei $p > 2$ prim. Wieviele Reste mod p sind sowohl Quadrat als auch Quadrat plus 1? **Beispiel:** Für $p = 7$ gibt es genau zwei solcher Reste, nämlich $1 = 1^2 = 0^2 + 1$ und $2 \equiv 3^2 \equiv 1^2 + 1\ (7)$.*

Vor.: $p > 2$ prim

Beh.: Genau $\left[\frac{p}{4}\right] + 1$ Reste h mod p sind sowohl Quadrat als auch Quadrat $+1$, d.h. $h \equiv x^2\ (p), h \equiv y^2 + 1\ (p)$ lösbar.

Bew.: Wir fordern

$$x^2 \equiv y^2 + 1\ (p) \Leftrightarrow (x-y)(x+y) \equiv 1\ (p)$$

d.h. $x - y$ ist das Inverse von $x + y$ mod p.
Jeder Rest $\neq 0$ hat ein eind. Inverses mod p, mit $k = x + y$ darf k also alle Werte $1, 2, \ldots, p-1$ annehmen, damit sind dann x, y bestimmt durch $x + y = k, x - y = k^{-1}(\text{ mod } p) \Leftrightarrow 2x = k + k^{-1}, 2y = k - k^{-1}$ mod p (k^{-1} das Inverse von k mod p).
Somit gibt es die $p-1$ vielen Lösungspaare

$$(x, y) = 2^{-1} \cdot (k + k^{-1}), 2^{-1} \cdot (k - k^{-1})), k = 1, 2 \ldots, p-1$$

(2^{-1} ist das Inverse von 2 mod p). Gefragt ist nun nach der Anzahl der verschiedenen Reste $h \equiv x^2 \equiv y^2 + 1\ (p)$, und manche Paare (x, y) geben den selben Wert h:
$z^2 \equiv s\ (p)$ hat 1 Lösung $= 0$, falls $s = 0$, 0 oder 2 Lösungen sonst.
d.h. für ein h gibt es i.a. 4 Lösungspaare $(\pm x_0, \pm y_0)$, außer:
zu $h = 1$ gibt es die 2 Lösungspaare $(\pm 1, 0)$,
zu $h = 0$ gibt es 2 Lösungspaare $(0, \pm y_0)$, falls -1 qR mod p ($\Leftrightarrow p \equiv 1\ (4)$) oder 0 Lösungspaare, falls $p \equiv 3\ (4)$.
Somit:

- $p \equiv 1\ (4) \Rightarrow$ Anzahl h ist $= \frac{p-1-4}{4} + 2 = \frac{p+3}{4} = \left[\frac{p}{4}\right] + 1$, wobei die 4 in $p - 1 + 4$ aus den 4 Paaren zu $h = 0, 1$ und die $+2$ aus $h = 0, 1$ kommt.
- $p \equiv 3\ (4) \Rightarrow$ Anzahl h ist $= \frac{p-1-2}{4} + 1 = \frac{p+1}{4} = \left[\frac{p}{4}\right] + 1$, wobei die 2 in $p - 1 - 2$ aus den 2 Paaren zu $h = 1$ und die 1 aus $h = 1$ kommt.