Lösungen der Nachklausur in Elementarer Zahlentheorie, SoSe 2006

Aufgabe 1

(a) Zeige, daß für alle $a \in \mathbb{Z}$ gilt: $(2a+1, 9a+4) = 1$.

(b) Zeige, daß für alle $a, b \in \mathbb{Z}$ gilt: $(a,b) = [a,b] \Leftrightarrow a = \pm b$.

Lösung:

Zu (a): Ist $b \in \mathbb{Z}$ ein gemeinsamer Teiler von $2a+1$ und $9a+4$, etwa $2a+1 = bc$ mit $c \in \mathbb{Z}$, so teilt b auch die Differenz $8a+3 = 4(2a+1)-1 = 4bc-1$, also folgt $b \mid 1$. Demnach ist $(2a+1, 9a+4) = 1$ der größte gemeinsame Teiler. □

Zu (b): Ist $d := (a,b)$ und $m := [a,b]$, sowie $d = m$, so folgt mit $|a| = dr$ und $|b| = ds$, $r, s \in \mathbb{N}$, also $(r,s) = 1$, daß $d = m = [a,b] = [dr, ds] = drs$ ist. Es folgt $rs = 1$, also $r = s = 1$ und somit $|a| = d = |b|$, d. h. $a = \pm b$. □

Aufgabe 2

Zeige: Ist für $k \geq 1$ die k-te Fermatzahl $F_k = 2^{2^k} + 1$ prim, so gilt

$$\left(\frac{3}{F_k}\right) = -1.$$

Lösung:

Da $F_k \equiv 1 \ (4)$ ist, gilt nach dem quadratischen Reziprozitätsgesetz

$$\left(\frac{3}{F_k}\right) = \left(\frac{F_k}{3}\right).$$

Modulo 3 gilt nun $F_k \equiv (-1)^{2^k} + 1 \equiv 2 \ (3)$, also folgt

$$\left(\frac{F_k}{3}\right) = \left(\frac{2}{3}\right) = -1.$$

□

Bemerkung: Die Voraussetzung "F_k prim" ist abschwächbar, es genügt, hier $3 \nmid F_k$ zu fordern und das QRG für das Jacobi-Symbol zu verwenden.

Aufgabe 3

Für welche $n \in \mathbb{N}$ ist $\varphi(n) = 18$?

Lösung:

Sei n mit $\varphi(n) = 18 = 2 \cdot 3^2$ gegeben. Für die PFZ $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ ist $\varphi(n) = p_1^{\alpha_1 - 1} \cdots p_r^{\alpha_r - 1}(p_1 - 1) \cdots (p_r - 1)$, und da die Faktoren $p_i - 1$ außer für $p_i = 2$ alle gerade sind, folgt $r \leq 2$.

1.Fall: $r = 1$. Dann ist $n = p^\alpha$ und $\varphi(n) = p^{\alpha-1}(p-1)$. Soll dies $= 18$ sein, so folgt nur $p = 3$ (dann $\alpha = 3$) oder $p = 19$ (dann $\alpha = 1$), also ist nur $n = 3^3 = 27$ oder $n = 19$ möglich, für die tatsächlich $\varphi(n) = 18$ gilt, wovon man sich überzeugt.

2.Fall: $r = 2$. Dann ist $n = p^\alpha q^\beta$, $\alpha, \beta \geq 1$, nur möglich, wenn eine der Primzahlen $= 2$ ist, denn sonst wäre $\varphi(n)$ mehrmals durch 2 teilbar. Und aus demselben Grund ist dann nur 2 oder 2^2 die in n aufgehende 2er-Potenz. Sei also $p = 2$. Wäre nun $2^2|n$, so ist wegen dem geraden Faktor $q-1$ wieder eine 2er-Potenz zuviel in $\varphi(n)$.

Also ist $n = 2q^\beta$ mit $2 < q \leq 19$. Dann ist $\varphi(n) = q^{\beta-1}(q-1) = 3^2 \cdot 2$. Also ist (a) $q - 1 = 2$ oder (b) $q - 1 = 6$ oder (c) $q - 1 = 18$. Im Fall (a) ist $q = 3$, und $\beta = 3$, also $n = 2 \cdot 3^3 = 54$, eine Lösung. Im Fall (b) ist $q = 7$, und β müßte $= 1$ sein, aber dann wäre $n = 14$, was keine Lösung ist, weil in $\varphi(14) = 6$ eine 3er-Potenz fehlt. Im Fall (c) ist $q = 19$ und $\beta = 1$, also $n = 2 \cdot 19 = 38$, was eine Lösung ist.

Alle Lösungen sind also $\{19, 27, 38, 54\}$. □

Aufgabe 4

Bestimme alle Lösungen der Kongruenz

$$x^3 - 4x - 5 \equiv 0 \ \ (50).$$

Lösung:

Es ist $50 = 2 \cdot 5^2$. Modulo 2 ist 1 einzige Lösung, und alle Lösungen modulo 5 sind 0, 2 und $-2 \equiv 3\,(5)$, denn modulo 5 ist das Polynom $= x^3 - 4x = x(x^2 - 4) = x(x-2)(x+2)$.

Von den Lösungen mod 5 steigen wir nun auf zu Lösungen mod $5^2 = 25$: Dazu bilden wir die Ableitung $f'(x) = 3x^2 - 4$ des Polynoms $f(x)$ der linken Seite der Kongruenz. Es ist $f'(0) = -4 \not\equiv 0\,(5)$ und $f'(\pm 2) = 8 \not\equiv 0\,(5)$, also läßt sich zu jeder Lösung mod 5 genau eine zugehörige Lösung mod 25 konstruieren.

Zu 0 mod 5: Der Ansatz $\frac{f(0)}{5} + b \cdot f'(0) \equiv 0\,(5)$ liefert $-4b \equiv 1\,(5)$, also $b = 1$ und die Lösung $0 + 1 \cdot 5 = 5$ mod $5^2 = 25$.

Zu ± 2 mod 5: Der Ansatz $\frac{f(\pm 2)}{5} + b \cdot f'(\pm 2) \equiv 0\,(5)$ liefert $-1 + 8b \equiv 0\,(5)$, also $b = 2$ und die Lösungen $\pm 2 + 2 \cdot 5$, d. h. 12 und 8 mod 5.

Gesucht sind nun die Lösungen von $x \equiv 1\,(2), x \equiv a\,(25)$ mit $a = 5, 8, 12$, also sind 5, 33 und 37 alle Lösungen der Kongruenz mod 50. □

Aufgabe 5

Sei $p > 3$ eine Primzahl. Zeige:

$$\left(\frac{-3}{p}\right) = 1 \quad \Longleftrightarrow \quad p \equiv 1\,(6).$$

Lösung:

Nach dem QRG und seinem 1. EG ist

$$\begin{aligned}\left(\frac{-3}{p}\right) &= \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}}(-1)^{\frac{3-1}{2}\cdot\frac{p-1}{2}}\left(\frac{p}{3}\right) \\ &= (-1)^{p-1}\left(\frac{p}{3}\right) = \left(\frac{p}{3}\right) = \begin{cases} 1, & \text{falls } p \equiv 1\ (3), \\ -1, & \text{falls } p \equiv -1\ (3). \end{cases}\end{aligned}$$

Da p prim, ist $p \equiv 1\,(3)$ äquivalent zu $p \equiv 1\,(6)$, und $p \equiv -1\,(3)$ ist äquivalent zu $p \equiv 5\,(6)$. Dies zeigt die Behauptung, denn eine Primzahl > 3 liegt immer in einer der beiden Restklassen 1 und 5 mod 6. □

Aufgabe 6

Zeige: Für alle $n, k \in \mathbb{N}$ gilt

$$n^k = \sum_{d|n} \mu\left(\frac{n}{d}\right) \sum_{t|d} t^k$$

Lösung:

Es sei P_k die k-te Potenzfunktion und σ_k die k-te Teilersummenfunktion. Es gilt $\sigma_k = \underline{1} * P_k$, also $P_k = \sigma_k * \mu$ nach Anwendung der Möbiusschen Umkehrformel. Es folgt

$$n^k = \sum_{d|n} \sigma_k(d)\, \mu\left(\frac{n}{d}\right) = \sum_{d|n} \mu\left(\frac{n}{d}\right) \sum_{t|d} t^k.$$

□

Aufgabe 7

Bestimme die kleinste positive ganze Zahl $a > 2$ mit

$$2 \,|\, a, \quad 3 \,|\, (a+1), \quad 4 \,|\, (a+2), \quad 5 \,|\, (a+3), \quad 6 \,|\, (a+4).$$

Lösung:

Zu bestimmen ist a ganz mit

$$\begin{aligned}
&a \equiv 0\,(2), && \text{etwa } a = 2b,\\
&a \equiv -1\,(3), && \text{also } b \equiv -2 \equiv 1\,(3),\\
&a \equiv -2\,(4), && \text{also } b \equiv -1 \equiv 1\,(2),\\
&a \equiv -3\,(5), && \text{also } 2b \equiv -3\,(5),\ \text{d. h. } b \equiv -9 \equiv 1\,(5),\\
&a \equiv -4\,(6), && \text{also } b \equiv -2 \equiv 1\,(3).
\end{aligned}$$

Die drei Kongruenzen $b \equiv 1\,(2)$, $b \equiv 1\,(3)$, und $b \equiv 1\,(5)$ haben modulo $2 \cdot 3 \cdot 5 = 30$ die Lösung 1 (CRS), die kleinste positive Lösung > 1 ist also $b = 31$, und somit ist $a = 62$ die gesuchte ganze Zahl > 2. □

Aufgabe 8

Zeige: Eine Zahl $n \in \mathbb{N}$ kann genau dann als Differenz zweier Quadrate geschrieben werden, wenn sie das Produkt zweier Faktoren, die beide gerade oder beide ungerade sind, ist.

Lösung:

Sei zunächst $n = a^2 - b^2$, also folgt $n = (a+b)(a-b)$. Angenommen, $a+b = 2k$ wäre gerade und $a - b = 2\ell + 1$ ungerade, dann wäre $2a = 2k + 2\ell + 1$ gerade und ungerade, ein Widerspruch. Ebenso folgt dieser Widerspruch, wenn $a+b$ ungerade und $a - b$ gerade wäre. Also haben $a + b$ und $a - b$ gleiche Parität.

Sei umgekehrt $n = uv$ mit u und v beide gerade oder beide ungerade. Dann sind $u + v$ und $u - v$ beide gerade, und es folgt, daß

$$n = uv = \left(\frac{u+v}{2}\right)^2 - \left(\frac{u-v}{2}\right)^2$$

eine Differenz zweier Quadrate ist. □