Lösungen der Klausur in Elementarer Zahlentheorie, SoSe 2006

Aufgabe 1

Zeige für $m, n \in \mathbb{N}$, $a, b, c, d \in \mathbb{Z}$:
Aus $ab \equiv cd \ (m)$, $b \equiv d \ (n)$, $(b, n) = 1$ folgt $a \equiv c \ ((m, n))$.

Lösung:

Die Kongruenzen der Voraussetzungen gelten auch modulo (m, n), da (m, n) ein gemeinsamer Teiler von n und m ist. Es folgt $ab \equiv cd \equiv cb \ ((m, n))$, und da $(b, n) = 1$ ist auch $(b, (m, n)) = 1$, also läßt sich die Kongruenz $ab \equiv cb \ ((m, n))$ mit b kürzen und man erhält $a \equiv c \ ((m, n))$. □

Aufgabe 2

Zeige: Für $n \geq 1$ ist die Zahl

$$1! + 2! + \cdots + n!$$

genau dann eine Quadratzahl, wenn $n = 1$ oder $n = 3$ ist.

Lösung:

Für $n = 1$ und $n = 3$ ist die Zahl eine Quadratzahl, da $1! = 1^2$ und $1! + 2! + 3! = 9 = 3^2$. Für $n = 2$ ist $1! + 2! = 3$ und $n = 4$ ist $1! + 2! + 3! + 4! = 33$ keine Quadratzahl. Da nun für $n \geq 5$ die Kongruenz $n! \equiv 0 \ (10)$ gilt (denn $n!$ hat dann die Teiler 2 und 5), hat man für $n \geq 5$

$$1! + 2! + \cdots + n! \equiv 33 + 5! + 6! + \cdots + n! \equiv 33 \equiv 3 \ (10).$$

Alle Quadrate mod 10 sind aber $0, 1, 4, 9, 6, 5$, also können die Zahlen $1! + \cdots + n!$ für $n \geq 5$ keine Quadratzahlen sein, da ihr Rest 3 mod 10 ist. □

Aufgabe 3

Zeige: Ist $p > 2$ prim, $a \in \mathbb{Z}$, $(a, p) = 1$, $\mathrm{ord}_p(a) = 2k$, $k \in \mathbb{N}$,
so folgt $a^k \equiv -1 \ (p)$.

Lösung:

Ist $\mathrm{ord}_p(a) = 2k$, so gilt $a^{2k} \equiv 1 \ (p)$, also ist $(a^k - 1)(a^k + 1)$ durch die Zahl p teilbar. Da p prim, teilt p (mind.) einen der beiden Faktoren. Der Faktor

$a^k - 1$ wird aber nicht von p geteilt, weil sonst $2k$ nicht die Ordnung von a mod p wäre, also teilt p den anderen Faktor $a^k + 1$, d.h. es gilt $a^k \equiv -1\ (p)$. □

Aufgabe 4

Bestimme alle Lösungen der Kongruenz

$$x^3 + 9x - 4 \equiv 0\ (100).$$

Lösung:

Es ist $100 = 4 \cdot 5^2$, und die einzige Lösung mod 4 ist die 0, die einzige Lösung mod 5 ist die 3, wie man durch Probieren feststellt. Wir untersuchen nun mit dem Aufsteigesatz, welche Lösung mod 25 durch die Lösung 3 mod 5 induziert wird. Ist $f(x) := x^3 + 9x - 4$, so ist $f'(x) = 3x^2 + 9$, und $f'(3) = 36 \not\equiv 0(5)$, also gibt es genau eine Lösung mod 25. Mit dem Ansatz

$$\frac{f(3)}{5} + b \equiv 0\ (5) \Leftrightarrow b \equiv -\frac{f(3)}{5} = -10 \equiv 0\ (5)$$

erhält man also mit $b = 0$ die Lösung $3 + 0 \cdot 5 = 3$ mod 25.

Nun sind nur noch die Kongruenzen $x \equiv 0\ (4)$ und $x \equiv 3\ (25)$ simultan zu lösen. Nach dem Chinesischen Restsatz ist die gemeinsame Lösung $x \equiv 0 \cdot M_1 M_1^* + 3 \cdot M_2 M_2^* \equiv 3 \cdot 4 \cdot M_2^*\ (100)$ mit dem Inversen M_2^* von $M_2 = 4$ mod 25, das ist -6, da $4 \cdot (-6) \equiv (-1) \cdot 24 \equiv (-1)(-1) = 1\ (25)$. Es folgt $x \equiv -72 \equiv 28\ (100)$, das ist dann also die einzige Lösung der Kongruenz mod 100. □

Aufgabe 5

Sei $p > 5$ eine Primzahl. Zeige:

$$\left(\frac{6}{p}\right) = 1 \quad \Longleftrightarrow \quad p \equiv k\ (24) \text{ mit } k \in \{1, 5, 19, 23\}.$$

Lösung:

Es gilt

$$\left(\frac{6}{p}\right) = \left(\frac{2}{p}\right) \cdot \left(\frac{3}{p}\right),$$

und dies ist $= 1$, gewenn beide Faktoren $= 1$ oder beide Faktoren $= -1$ sind. Es gilt zunächst

$$\left(\frac{3}{p}\right) = 1 \Longleftrightarrow p \equiv \pm 1\ (12)$$

und

$$\left(\frac{3}{p}\right) = -1 \Longleftrightarrow p \equiv \pm 5 \ (12),$$

denn nach dem QRG ist

$$\left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}} \left(\frac{p}{3}\right) = \begin{cases} 1, & \text{falls } p \equiv 1 \ (4), p \equiv 1 \ (3), \text{d. h. } p \equiv 1 \ (12), \\ -1, & \text{falls } p \equiv 1 \ (4), p \equiv -1 \ (3), \text{d. h. } p \equiv 5 \ (12), \\ -1, & \text{falls } p \equiv -1 \ (4), p \equiv 1 \ (3), \text{d. h. } p \equiv -5 \ (12), \\ 1, & \text{falls } p \equiv -1 \ (4), p \equiv -1 \ (3), \text{d. h. } p \equiv -1 \ (12). \end{cases}$$

Somit gilt

$$\begin{aligned} \left(\frac{2}{p}\right) = 1 \text{ und } \left(\frac{3}{p}\right) = 1 &\Longleftrightarrow p \equiv \pm 1 \ (8) \text{ und } p \equiv \pm 1 \ (12) \\ &\Longleftrightarrow p \equiv \pm 1 \ (24), \end{aligned}$$

(denn die Kongruenzen $p \equiv -1 \ (8)$ und $p \equiv 1 \ (12)$ sowie $p \equiv 1 \ (8)$ und $p \equiv -1 \ (12)$ sind unerfüllbar, da $4 = (8, 12) \nmid (-1 - 1) = -2$, s. Blatt 6 Aufg. 2b) und

$$\begin{aligned} \left(\frac{2}{p}\right) = -1 \text{ und } \left(\frac{3}{p}\right) = -1 &\Longleftrightarrow p \equiv \pm 5 \ (8) \text{ und } p \equiv \pm 5 \ (12) \\ &\Longleftrightarrow p \equiv \pm 5 \ (24), \end{aligned}$$

(denn die Kongruenzen $p \equiv -5 \ (8)$ und $p \equiv 5 \ (12)$ sowie $p \equiv 5 \ (8)$ und $p \equiv -5 \ (12)$ sind unerfüllbar, da $4 = (8, 12) \nmid (-5 - 5) = -10$, s. Blatt 6, Aufg. 2b). Dies zeigt, daß genau die Reste $\pm 1, \pm 5$ mod 24 in Frage kommen, also die Reste $\{1, 5, 19, 23\}$ mod 24, wie behauptet. □

Aufgabe 6

Zeige: Ist $n > 1$ quadratfrei, so gilt

$$\sum_{d|n} \sigma(d^{k-1})\varphi(d) = n^k$$

für alle $k \geq 2$.

Lösung:

Sei $n = p_1 p_2 \cdots p_r > 1$ eine quadratfreie Zahl. Die durch $f(m) = \sigma(m^t)\varphi(m)$, $t \geq 1$, definierte Funktion ist multiplikativ, da sie aus solchen zusammengesetzt ist. Damit ist auch die Funktion $F(n) = \sum_{d|n} f(d) = \sum_{d|n} \sigma(d^{k-1})\varphi(d)$

multiplikativ. Da n quadratfrei ist, genügt es, für alle Primzahlen p die Gleichung $F(p) = p^k$ nachzuweisen, denn daraus und aus der Multiplikativität von F folgt dann $F(n) = p_1^k \cdots p_r^k = n^k$.

Da 1 und p die einzigen Teiler von p sind, erhält man sofort

$$F(p) = \sum_{d|p} \sigma(d^{k-1})\varphi(d) = 1 + \sigma(p^{k-1})\varphi(p) = 1 + \frac{p^k - 1}{p-1}(p-1) = p^k,$$

was zu zeigen war. □

Aufgabe 7

Zeige: Keine der Zahlen

$$11, 111, 1111, 11111, \ldots$$

läßt sich als Summe zweier Quadrate schreiben.

Lösung:

Die Zahlen sind alle $\equiv 11$ (100), also $\equiv 3$ (4). Eine Zahl $\equiv 3$ (4) hat in ihrer Primfaktorzerlegung aber mindestens einen Primteiler $p \equiv 3(4)$, der in ungerader Potenz auftritt, da ansonsten die Zahl die Form $4k+1$ haben müßte (Produkte von Zahlen der Gestalt $4k+1$ haben wieder diese Gestalt, und Quadrate von Zahlen der Gestalt $4k+3$ sind ebenso von der Gestalt $4k+1$). Nach dem Satz von Euler über Summen von zwei Quadraten sind diese Zahlen also nicht als Summe zweier Quadrate schreibbar. □

Aufgabe 8

Für alle teilerfremden natürlichen Zahlen m und n zeige

$$m^{\varphi(n)} + n^{\varphi(m)} \equiv 1\ (mn).$$

Lösung:

Da $(m,n) = 1$ ist nach dem Satz von Euler einerseits $m^{\varphi(n)} \equiv 1\ (n)$ und andererseits $n^{\varphi(m)} \equiv 1\ (m)$. Trivialerweise gelten auch die Kongruenzen $m^{\varphi(n)} \equiv 0\ (m)$ und $n^{\varphi(m)} \equiv 0\ (n)$. Deswegen folgt

$$m^{\varphi(n)} + n^{\varphi(m)} \equiv 1\ (n) \quad \text{und} \quad m^{\varphi(n)} + n^{\varphi(m)} \equiv 1\ (m).$$

Die Kongruenz gilt dann auch mod $[m,n] = mn$, da $(m,n) = 1$. □