

Prof. Dr. M. Reineke
Dr. R. Olbricht
Dipl.-Math. M. Boos

25. September 2009

Nachklausur zur Elementaren Zahlentheorie

Aufgabe 1: (8 Punkte)

Sind $a, b \in \mathbf{N}$ teilerfremd, so gibt es $x, y \in \mathbf{Z}$ mit $ax + by = 2$. □ □

Wahr: Satz über die Teilersummendarstellung.

Für genügend großes n ist die n -te Fibonacci-Zahl größer als n^{22} . □ □

Wahr: nach Korollar der Binet-Formel wachsen die Fibonacci-Zahlen wie $(\frac{1+\sqrt{5}}{2})^n$, also (Analysis I) schneller als jedes n^C .

Eine prime Restklasse $[a]$ modulo m ist primitiv, falls $a^{\varphi(m)} \equiv 1 \pmod{m}$. □ □

Falsch: die Bedingung rechts gilt für jede prime Restklasse (Euler-Fermat).

Für die Euler- φ -Funktion gilt $\varphi(m) = |\mathbf{Z}/m\mathbf{Z}|$. □ □

Falsch: $\varphi(m) = |(\mathbf{Z}/m\mathbf{Z})^*|$.

Es gilt stets $\varphi(2n) = \varphi(n)$. □ □

Falsch: z.B. $\varphi(2) = 1$, $\varphi(4) = 2$.

Es gibt unendlich viele Primzahlen $\equiv -1 \pmod{3}$. □ □

Wahr: Proposition 1.3.17 aus der Vorlesung (Spezialfall des Satzes von Dirichlet).

Die Restklasse $[7]$ besitzt ein Inverses in $\mathbf{Z}/98\mathbf{Z}$. □ □

Falsch, da 7 nicht teilerfremd zu 98.

Für $\text{ggT}(a, m) = 1$ gilt: $\text{ord}_m[a]$ teilt $m - 1$. □ □

Falsch, z.B. hat $[3]$ die Ordnung $2 \pmod{4}$, aber $2 \nmid 3$.

Die Dezimalbruchentwicklung von $\frac{27}{52}$ besitzt eine Vorperiode der Länge 2. □ □

Wahr: siehe Beispiel in der Vorlesung.

$\left(\frac{9}{101}\right) = 1$. □ □

Wahr, denn $\left(\frac{a^2}{p}\right) = 1$.

Die diophantische Gleichung $x^2 - y^2 + z^2 = 0$ für $x, y, z \in \mathbf{Z}$ besitzt unendlich viele Lösungen. □ □

Wahr: diese Gleichung kann man zu $x^2 + z^2 = y^2$ umstellen, dies sind gerade die pythagoräischen Zahlentripel.

$\left(\frac{a \cdot b}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$ falls $p \nmid a, b$. □ □

Wahr: Satz aus der Vorlesung.

$m_p(\text{kgV}(m, n)) = \min(m_p(m), m_p(n))$. □ □

Falsch, mit ggT statt kgV wäre es richtig.

Eine Zahl besitzt so viele verschiedene maximale echte Teiler wie verschiedene Primfaktoren. □ □

Wahr: ist nämlich p Primfaktor von n , so ist n/p maximaler echter Teiler, und jeder solche ist von dieser Form.

Genau die geraden Potenzen einer primitiven Restklasse \pmod{p} sind quadratische Reste \pmod{p} . □ □

Wahr: Resultat aus der Vorlesung.

Es gilt stets $\text{ggT}(n, m) = \text{ggT}(m, n - km)$. □ □

Wahr: darauf beruht der Euklidische Algorithmus.

Aufgabe 2: (4 Punkte) Bestimmen Sie die kleinste natürliche Zahl $n > 2$ mit $2|n$, $3|n+1$, $4|n+2$, $5|n+3$, $6|n+4$.

Man schreibt dies zu einem System von Kongruenzen um:

$$n \equiv 0 \pmod{2}, \quad n \equiv 2 \pmod{3}, \quad n \equiv 2 \pmod{4}, \quad n \equiv 2 \pmod{5}, \quad n \equiv 2 \pmod{6}.$$

Die letzte Kongruenz ist äquivalent zu $n \equiv 2 \pmod{2}$ und $n \equiv 2 \pmod{3}$, kann also weggelassen werden. Aus $n \equiv 2 \pmod{4}$ folgt schon $n \equiv 0 \pmod{2}$, also reduziert sich das System auf

$$n \equiv 2 \pmod{3}, \quad n \equiv 2 \pmod{4}, \quad n \equiv 2 \pmod{5}.$$

Die Lösung 2 sieht man sofort, nach dem chinesischen Restesatz sind alle Lösungen dann genau die Zahlen $n \equiv 2 \pmod{60 = 3 \cdot 4 \cdot 5}$. Also ist $n = 62$ die gesuchte Lösung.

Aufgabe 3: (4 Punkte) Charakterisieren Sie die Primzahlen p , für die die Kongruenz $x^2 + 6x + 4 \equiv 0 \pmod{p}$ eine Lösung x besitzt.

Wir führen quadratische Ergänzung durch:

$$0 \equiv x^2 + 6x + 4 = (x + 3)^2 - 5 \pmod{p},$$

also ist die Kongruenz äquivalent zu $(x + 3)^2 \equiv 5 \pmod{p}$. Die Lösbarkeit dieser Kongruenz liest man an $\left(\frac{5}{p}\right)$ ab. Um das Quadratische Reziprozitätsgesetz anwenden zu dürfen, nehmen wir zunächst $p \neq 2, 5$ an, dann $\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right)$. Quadratische Reste $\pmod{5}$ sind gerade 1 und 4, also ist die Kongruenz lösbar falls $p \equiv 1, 4 \pmod{5}$. Die Fälle $p = 2, 5$ untersucht man direkt und erhält in beiden Fällen Lösbarkeit. Insgesamt ist die Kongruenz also genau dann lösbar, wenn $p = 2$ oder $p = 5$ oder $p \equiv 1, 4 \pmod{5}$.

Aufgabe 4: (4 Punkte) Bestimmen Sie alle Vielfachen von 12 mit genau 2 verschiedenen Primfaktoren und genau 14 Teilern.

Da die gesuchte Zahl n genau 2 Primfaktoren hat, ist sie von der Form $n = p^a q^b$. Da $2^2 \cdot 3 = 12|n$, müssen die beiden Primfaktoren von n gerade 2 und 3 sein, also $n = 2^a 3^b$ mit $a \geq 2$ und $b \geq 1$. Die Anzahl der Teiler von n ist dann $(a + 1)(b + 1) = 14$. Wegen der Ungleichungen an a und b ist die einzige Lösung $a = 6$, $b = 1$, also $n = 2^6 \cdot 3 = 192$ die einzige Lösung.

Aufgabe 5: (4 Punkte) Bestimmen Sie eine primitive Restklasse modulo 17.

Wieviele solche gibt es?

Wegen $\varphi(17) = 16$ ist eine prime Restklasse genau dann primitiv $\pmod{17}$, wenn ihre achte Potenz nicht [1] ist. Wir probieren die Restklasse [3]: es ist $[3]^2 = [9]$, $[3]^4 = [9]^2 = [81] = [-4]$, $[3]^8 = [-4]^2 = [16] = [-1] \neq [1]$, also ist [3] primitiv. Die Anzahl aller solchen ist $\varphi(\varphi(17)) = \varphi(16) = 8$.

Aufgabe 6: (4 Punkte) Beweisen Sie, dass $7 \nmid \binom{82}{12}$, aber $7 \mid \binom{82}{36}$.

Nach dem Satz von Kummer erhält man die Multiplizität von 7 in diesen Binomialkoeffizienten als die Zahl der Überträge bei 7-adischer Addition von 12 und 70 bzw. von 36 und 46. Es gilt $12 = 7 + 5 = (15)_7$, $70 = 49 + 3 \cdot 7 = (130)_7$, $36 = 5 \cdot 7 + 1 = (51)_7$ und $46 = 6 \cdot 7 + 4 = (64)_7$. Wir führen die Additionen durch: $(15)_7 + (130)_7 = (145)_7$ ohne Übertrag, $(51)_7 + (64)_7 = (145)_7$ mit einem Übertrag. Dies zeigt die Behauptung.