Elementare Zahlentheorie

Präsenzübungsaufgaben

Aufgabe 1. Für $n > 1$ ist $n^4 + 4$ nicht prim.

Aufgabe 2. Ein Zahl der Form $m+(m+1)+(m+2)+\dots+(m+k)$ nennen wir „Summe aufeinanderfolgender Zahlen“. Zeige, unter den natürlichen Zahlen lassen sich nur Zweierpotenzen *nicht* als Summe aufeinanderfolgender natürlicher Zahlen darstellen.

Aufgabe 3. Eine ungerade natürliche Zahl $n > 1$ ist prim genau dann, wenn sie sich *nicht* als Summe von drei oder mehr aufeinanderfolgender natürlicher Zahlen darstellen läßt.

Aufgabe 4. Es bezeichne $\pi(x)$ die Anzahl der Primzahlen $\leq x$. Zeige:

$$\sum_{p \leq x, \text{ prim}} \frac{1}{p} = \frac{\pi(x)}{x} + \int_2^x \frac{\pi(u)}{u^2} \, du$$

Aufgabe 5. Zeige, daß $\mathbb{Z}[\sqrt{-5}]$ unzerlegbare Elemente hat, die nicht prim sind. Benutze dazu die Faktorisierungen $6 = 2 \times 3 = (1 + i\sqrt{5})(1 - i\sqrt{5})$ und die Norm $N : a + i\sqrt{5}b \mapsto a^2 + 5b^2$. Hint: Zeige, daß die Norm multiplikativ ist. Da die Norm Werte in $\mathbb{N}$ annimmt, lassen sich damit zu einem Ringelement alle (endlich vielen) möglichen Faktorisierungen angeben.

Aufgabe 6. Zeige: ein Element a in einem Integritätsbereich R ist unzerlegbar, wenn das Hauptideal Ra maximal unter allen echten Hauptidealen ist.

Aufgabe 7. Zeige: ein Element a in einem Integritätsbereich R ist prim, wenn das Hauptideal ra prim ist.

Aufgabe 8. Zeige, daß in $\mathbb{Z}$ die folgende Variante der Kürzungsregel gilt:

$$ac|bc \implies a|b \quad \text{für } c \neq 0$$

Aufgabe 9. Zeige: In einer Matrix aus $\text{GL}_n(\mathbb{Z})$ sind die Einträge einer Zeile teilerfremd.

Aufgabe 10. Die *Fibonacci-Zahlen* sind rekursiv definiert durch:

$$f_1 = 1 \quad f_2 = 1 \quad f_{n+2} = f_{n+1} + f_n$$

Die ersten lauten: 1, 1, 2, 3, 5, 8, 13, 21, ... Zeige: zu jeder natürlichen Zahl N gibt es unendlich viele durch N teilbare Fibonacci-Zahlen.

Aufgabe 11. Berechne die kleinen Potenzen der Matrix

$$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$$

Erkläre das Erscheinen der Fibonacci-Zahlen. Formuliere und beweise eine Vermutung über die höheren Potenzen.

Aufgabe 12. Berechne die Eigenwerte der Matrix

$$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$$

Was hat der goldene Schnitt mit den Fibonacci-Zahlen zu tun?

Aufgabe 13. Seien a und b teilerfremd. Zeige

$$\text{ggT}(a + b, a^2 - ab + b^2) \in \{1, 3\}$$

Aufgabe 14. Zeige: 24 ist die größte natürliche Zahl, die durch alle natürlichen Zahlen unterhalb ihrer Quadratwurzel teilbar ist.

Aufgabe 15. Sei d ein *echter* Teiler von n . Zeige:

$$d - \varphi(d) < n - \varphi(n)$$

Aufgabe 16. Zeige: Aufeinanderfolgende Glieder der Folge $n! + 1$ sind teilerfremd.

Aufgabe 17. Zeige, daß $n \mapsto \sum_{d|n} 1$ eine multiplikative Funktion ist. (Anzahl der Teiler)

Aufgabe 18. Zeige, daß $n \mapsto \sum_{d|n} d$ eine multiplikative Funktion ist. (Summe der Teiler)

Aufgabe 19. Die Funktion $n \mapsto \varphi(n) \sum_{d|n} d$ ist also multiplikativ. Welche Werte nimmt sie auf Primzahlpotenzen an? Folgere: $\varphi(n) \sum_{d|n} d \leq n^2$.

Aufgabe 20. Sei p eine ungerade Primzahl und kein Teiler von a . Ist die Kongruenz

$$x^2 \equiv a \pmod{p}$$

lösbar, so sind alle Kongruenzen

$$x^2 \equiv a \pmod{p^k}$$

lösbar.

Aufgabe 21. Sei $f(x)$ ein Polynom mit ganzzahligen Koeffizienten und p eine Primzahl. Es sei p^k Teiler von $f(a)$ und $f'(a) \not\equiv 0 \pmod{p}$; d.h., a ist reguläre Nullstelle modulo p^k . Wir wissen, wie sich a zu einer Nullstelle modulo p^{k+1} hochheben läßt. Für $k \geq 2$ kann man aber schneller fortschreiten: Sei m ein Inverses zu $f'(a)$ modulo p^{2k} , d.h. $mf'(a) \equiv 1 \pmod{p^{2k}}$. Zeige, daß $b := a - mf(a)$ eine Nullstelle von $f(x)$ modulo p^{2k} ist.

Aufgabe 22. Bestimme alle Lösungen der Kongruenzen

$$\begin{aligned}x^3 + x^2 - 4 &\equiv 0 \pmod{7^3} \\x^3 + x^2 - 5 &\equiv 0 \pmod{7^3} \\x^3 + x + 57 &\equiv 0 \pmod{5^3}\end{aligned}$$

Aufgabe 23. Sei p eine ungerade Primzahl. Wir nennen ein Element $a \in (\mathbb{Z}/p\mathbb{Z})^*$ einen quadratischen Rest, wenn die Kongruenz $x^2 \equiv a \pmod{p}$ eine Lösung hat. Zeige, daß die Hälfte aller Elemente von $(\mathbb{Z}/p\mathbb{Z})^*$ quadratische Reste sind.

Aufgabe 24. Bestimme die primitiven Elemente in $(\mathbb{Z}/23\mathbb{Z})^*$.

Aufgabe 25. Zeige: Ist eine Zahl a teilerfremd zu 6, so ist $a^2 \equiv 1 \pmod{24}$. Hint: behandle das Problem modulo 8 und modulo 3.

Aufgabe 26. Zeige, daß $3^8 \equiv -1 \pmod{17}$ ist. Folgere, daß 3 ein primitives Element der Einheitengruppe modulo 17 ist.

Aufgabe 27. Wieviele Lösungen modulo 17 haben folgende Kongruenzen:

$$\begin{aligned}x^{12} &\equiv 16 \pmod{17} \\x^{48} &\equiv 9 \pmod{17} \\x^{20} &\equiv 13 \pmod{17} \\x^{11} &\equiv 9 \pmod{17}\end{aligned}$$

Aufgabe 28. Sei p eine Primzahl, a sei teilerfremd zu p und definiere eine Restklasse der Ordnung 3. Zeige, daß p ein Teiler von $1 + a + a^2$ ist. Zeige auch, daß $1 + a$ eine Restklasse der Ordnung 6 definiert.

Aufgabe 29. Löse die Kongruenz:

$$x^{99} \equiv 2 \pmod{101}$$

Aufgabe 30. Sei p ein Primfaktor von $\varphi(m)$ aber nicht von m . Zeige, daß mindestens ein Primfaktor von m bei Division durch p den Rest 1 läßt. Hint: Betrachte die Primfaktorzerlegung von m und nutze, daß φ eine multiplikative Funktion ist, deren Werte auf Primzahlpotenzen wir kennen.

Aufgabe 31. Seien k und a natürliche Zahlen mit $a \geq 2$. Zeige, daß k ein Teiler von $\varphi(a^k - 1)$ ist.

Aufgabe 32. Sei p eine Primzahl. Zeige, daß es unendlich viele Primzahlen $q \equiv 1 \pmod p$ gibt. Hint: Nimm an, $q_1, \dots, q_r$ wären alle Primzahlen dieser Form. Benutze die *beiden* vorstehenden Aufgaben mit $m = a^k - 1$ und $k = p$ an bei einer geschickten Wahl von a dazu, die Existenz einer weiteren Primzahl der geforderten Art nachzuweisen.

Aufgabe 33. Löse die Kongruenzen

$$x^2 \equiv 10 \pmod{13}$$

$$x^2 \equiv 5 \pmod{19}$$

Aufgabe 34. Bringe die folgenden Kongruenzen auf die Form $x^2 \equiv d \pmod p$:

$$4x^2 + 2x + 1 \equiv 0 \pmod{5}$$

$$3x^2 - x + 5 \equiv 0 \pmod{7}$$

Aufgabe 35. Sei p eine Primzahl kongruent 2 modulo 3 und sei a teilerfremd zu p . Zeige, daß die Kongruenz $x^3 \equiv a \pmod p$ genau eine Lösung modulo p hat, nämlich $a^{\frac{2p-1}{3}} \pmod p$.

Aufgabe 36. Sei p eine ungerade Primzahl. Zeige, daß die Zahlen $1^2, 2^2, 3^2, \dots, (\frac{p-1}{2})^2$ alle quadratischen Reste repräsentieren und keiner darunter mehrfach vorkommt. Leite daraus her, daß die Summe der quadratischen Reste durch p teilbar ist, sofern $p \geq 5$ ist.

Aufgabe 37. Sei p eine ungerade Primzahl. Zeige, daß das *Produkt* aller quadratischen Reste $\equiv \pm 1 \pmod p$ ist. Hint: fasse die quadratischen Reste $\neq -1$ geschickt zu Paaren zusammen.

Aufgabe 38. Seien p und q teilerfremde Primzahlen und a sei ein quadratischer Rest sowohl modulo p als auch modulo q . Zeige oder widerlege: Dann ist a notwendig ein quadratischer Rest modulo pq .

Aufgabe 39. Bestimme die Primzahlen p , für die 3 quadratischer Rest ist.

Aufgabe 40. Bestimme die Primzahlen p , für die -1 quadratischer Rest ist.

Aufgabe 41. Bestimme die Primzahlen p , für die 5 quadratischer Rest ist.

Aufgabe 42. Bestimme die Primzahlen p , für die 7 quadratischer Rest ist.

Aufgabe 43. Bestimme die Primzahlen p , für die 11 quadratischer Rest ist.

Aufgabe 44. Bestimme diejenigen Primzahlen p , für die es x, y teilerfremd zu p gibt mit

$$x^2 + y^2 \equiv 0 \pmod p$$

Aufgabe 45. Die Primzahl p sei $\equiv 1 \pmod{4}$ und Summe zweier Quadratzahlen: $p = a^2 + b^2$ mit $a > 0$ ungerade. Zeige: $\left(\frac{a}{p}\right) = 1$.

Aufgabe 46. Sei p eine ungerade Primzahl und a teilerfremd zu p . Zeige, daß

$$\sum_{n=1}^p \left(\frac{an+b}{p}\right) = 0$$

ist für jedes feste b .

Aufgabe 47. Berechne $\left(\frac{-a}{p}\right)$.

Aufgabe 48. Zeige: Die Quadratwurzel einer ganzen Zahl ist genau dann rational, wenn sie ganz ist.

Aufgabe 49. Seien $a, b, c \in \mathbb{Z}$ mit $a \neq 0$. Zeige, daß folgende Aussagen äquivalent sind:

1. Eine der Nullstellen von $ax^2 + bx + c$ ist rational.
2. Die Diskriminante $b^2 - 4ac$ ist eine Quadratzahl.
3. Beide Nullstellen von $ax^2 + bx + c$ sind rational.

Bemerkung: 0 zählt in dieser Aufgabe als Quadratzahl.

Aufgabe 50. Faktorisiere die quadratische Form $ax^2 + bxy + cy^2$ in ein Produkt linearer Formen $(kx + ly)(mx + ny)$ mit ganzzahligen Koeffizienten, wenn $b^2 - 4ac$ eine Quadratzahl ist.

Aufgabe 51. Zeige: Die negative Diskriminante der Form $(kx + ly)(mx + ny)$ ist eine Quadratzahl. Hint: Betrachte die Determinante der Matrix $\begin{pmatrix} k & m \\ l & n \end{pmatrix}$.

Aufgabe 52. Zeige: $\text{GL}_2(\mathbb{Z})$ operiert transitiv auf der Menge der Kanten von T .

Aufgabe 53. Zeige: $\text{GL}_2(\mathbb{Z})$ operiert transitiv auf der Menge der Knoten von T . D.h.: $\text{GL}_2(\mathbb{Z})$ operiert transitiv auf der Menge der projektiven Triplets.

Aufgabe 54. Zeige oder widerlege: Zwei quadratische Formen q und q' sind genau dann äquivalent, wenn es zwei Knoten P und Q in $\bar{T}$ gibt, so daß q auf den drei Gebieten um P dieselben Werte annimmt wie q' auf den drei Gebieten um Q .

Aufgabe 55. Finde zwei inäquivalente positiv definite ganze quadratische Formen $ax^2 + hxy + by^2$ mit Diskriminante $\Delta = 4ab - h^2 = 23$.

Aufgabe 56. Entscheide, welche der folgenden Gleichungen ganzzahlige Lösungen in x und y haben:

$$x^2 + 2y^2 = 65$$

$$2x^2 - y^2 = 65$$

$$2x^2 - xy + 3y^2 = 113$$

$$2x^2 - xy + 3y^2 = 37$$

Aufgabe 57. Die Form $q(x, y) := x^2 - 3xy + y^2$ ist eine $+/-$ -Form. Finde eine Matrix A unendlicher Ordnung in $\text{GL}_2(\mathbb{Z})$, die q festhält. Bestimme die Eigenräume von A . Welche Werte nimmt q auf Eigenvektoren von A an?

Aufgabe 58. Finde in T eine Quelle für die positiv definite quadratische Form $q(x, y) = 5x^2 + 3xy + 7y^2$.