Übungen zu Zahlentheorie für TM, SS 2013

zusammengestellt von Johannes Morgenbesser

Übungsmodus: Ausarbeitung von 10 der Beispiele 1–38, 5 der Beispiele A–O und 15 der Beispiele i–xxxi.

1. Zeigen Sie, dass
   (a) $p^2 + 2$ keine Primzahl ist für $p > 3$ prim,
   (b) $n^4 + 4^n$ keine Primzahl ist für $n > 1$.

2. Zeigen Sie: Sind $a, b \in \mathbb{Z}^+$, sodass $a \mid b^2$, $b^2 \mid a^3$, $a^3 \mid b^4, \ldots$ gilt, dann folgt $a = b$.

3. Zeigen Sie, dass $1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}$ für $n > 1$ keine ganze Zahl ist.

4. Zeigen Sie, dass für alle $n \geqslant 1$ gilt: $(n! + 1, (n + 1)! + 1) = 1$.

5. (Legendre) Zeigen Sie, dass die Zahl $n!$ den Primfaktor p genau
$$\sum_{k \geqslant 1} \left\lfloor \frac{n}{p^k} \right\rfloor$$
   Mal enthält.

6. Lösen Sie mit Hilfe der letzten Aufgabe:
   (a) Auf wieviel Nullen endet $(169!)$?
   (b) $\sqrt[n]{n!} \leqslant \prod_{p \mid n!} p^{\frac{1}{p-1}}$.

7. Sei p eine Primzahl. Zeigen Sie, dass jeder Primteiler der Mersenne-Zahl $2^p - 1$ größer als p ist (Hinweis: Satz von Lagrange).

8. Zeigen Sie: Die Zahl $2^s - 1$ ist höchstens dann eine (Mersennsche) Primzahl, wenn der Exponent s selbst eine Primzahl ist.

9. Zeigen Sie, dass es unendlich viele Primzahlen der Form $4k + 3$ gibt.

10. Zeigen Sie, dass es unendlich viele Primzahlen der Form $4k + 1$ gibt.

11. Bestimmen Sie alle Lösungen p, q, $r \in \mathbb{Z}^+$ der Gleichung
$$\frac{1}{p} + \frac{1}{q} + \frac{1}{r} = 1.$$

12. Sei $F_n = 2^{2^n} + 1$ die n-te Fermat Zahl ($n \geqslant 0$).
    (a) Zeigen Sie, dass je zwei Fermat Zahlen relativ prim zueinander sind.

(b) Zeigen Sie, dass F_5 nicht prim ist (Hinweis: $F_5 = 20449^2 + 62264^2$).

13. (Fermat) Zeigen Sie, dass 21 nicht als Summe von Quadraten zweier rationaler Zahlen dargestellt werden kann.

14. Sei $\alpha\beta = \gamma^n$, wobei α, β, $\gamma \in \mathbb{Z}[i]$ und α und β relativ prim zueinander sind. Zeigen Sie, dass Gaußsche Zahlen $\varepsilon \in \{\pm 1, \pm i\}$ und $\delta \in \mathbb{Z}[i]$ existieren, sodass $\alpha = \varepsilon\delta^n$.

15. Benützen Sie das vorherige Beispiel um zu zeigen, dass die einzigen Lösungen von $x^2 + y^2 = z^2$ mit $(x, y) = 1$ und $x \equiv 0 \bmod 2$ gegeben sind durch

$$x = 2ab, \quad y = a^2 - b^2 \quad \text{und } z = a^2 + b^2,$$

wobei a, $b \in \mathbb{Z}$ mit $(a, b) = 1$ (Hinweis: $x^2 + y^2 = (x + iy)(x - iy)$).

16. Zeigen Sie, dass jede Zahl $n \in \mathbb{Z}^+$ dargestellt werden kann als Summe von Zahlen der Form $n = 2^i 3^j$, wobei kein Summand einen anderen teilt.

17. Zeigen Sie, dass für m, $n \in \mathbb{Z}^+$ mit $(m, n) = 1$ folgendes gilt: $m^{\varphi(n)} + n^{\varphi(m)} \equiv 1 \bmod mn$.

18. Berechnen Sie $2^{10^{10^{10}}} \bmod 77$.

19. Sei $f(x) = x^{99} + x^{98} + \cdots x + 1$. Wieviele Lösungen hat die Kongruenz $f(x) \equiv 0 \bmod 101$?

20. Zeigen Sie, dass die Kongruenz $(x^2 - 2)(x^2 - 17)(x^2 - 34) \equiv 0 \bmod p$ für jedes $p \in \mathbb{P}$ lösbar ist.

21. Sei $p > 3$, prim. Zeigen Sie, dass

$$\sum_{\substack{1 \leqslant a < p \\ \left(\frac{a}{p}\right) = 1}} a \equiv 0 \bmod p.$$

22. Zeigen Sie: Es gibt unendlich viele Dreieckszahlen (d.h. ganze Zahlen von der Form $(n(n + 1)/2$ mit $n \in \mathbb{Z}^+$), die gleichzeitig Quadratzahlen sind.

23. Zeigen Sie: Die Diophantische Gleichung $x^4 - 4y^4 = z^2$ hat keine Lösung mit $x, y, z \in \mathbb{Z}^+$.

24. Berechnen Sie $\left(\frac{70}{97}\right)$, $\left(\frac{-14}{83}\right)$ und $\left(\frac{55}{89}\right)$.

25. (a) Berechnen Sie die Kettenbruchdarstellung von $\sqrt{3}$ und $\sqrt{5}$.
    (b) Zeigen Sie, dass die Gleichung $x^2 - 3y^2 = -1$ nicht lösbar ist.
    (c) Ist die Gleichung $x^2 - 5y^2 = -1$ lösbar?

26. Sei $n \in \mathbb{Z}^+$. Zeigen Sie, dass es ein Vielfaches ($\neq 0$) von n gibt, welches in der Dezimaldarstellung nur Nuller und Einser enthält. Zeigen Sie weiters, dass 2^n ein Vielfaches besitzt, das nur aus Einser und Zweier besteht (Dezimaldarstellung).

27. Seien $m_1, \ldots, m_l$ und $a_1, \ldots, a_l$ ganze Zahlen. Zeigen Sie: Das Kongruenzsystem
$$x \equiv a_i \bmod m_i, \quad 1 \leqslant i \leqslant l,$$
ist genau dann lösbar, wenn $a_i \equiv a_j \bmod (m_i, m_j)$ für alle $1 \leqslant i, j \leqslant l$. Im Falle der Lösbarkeit ist die Lösung eindeutig modulo $kgV(m_1, \ldots, m_l)$.

28. Lösen Sie das folgende System simultaner Kongruenzen:
    - $x \equiv 1 \bmod 4$
    - $2x \equiv 3 \bmod 5$
    - $4x \equiv 5 \bmod 7$

29. Zeigen Sie, dass $x^2 + 1 = y^3$ nur die Lösung $(0, 1)$ besitzt.

30. Angenommen es existiert eine Primitivwurzel modulo m. Zeigen Sie, dass es genau $\varphi(\varphi(m))$ inkongruente Primitivwurzeln modulo m gibt.

31. (Verallgemeinerung des Satzes von Wilson) Sei $m \in \mathbb{Z}^+$. Zeigen Sie, dass
$$\prod_{\substack{1 \leqslant k \leqslant m \\ (k,m)=1}} k \equiv \begin{cases} -1 \bmod m, & \text{wenn } m \in \{1, 2, 4, p^n, 2p^n \, (p \in \mathbb{P} \setminus \{2\}, n \in \mathbb{Z}^+)\} \\ 1 \bmod m, & \text{sonst.} \end{cases}$$

32. Zeigen Sie: Sei a ungerade. Dann ist die Kongruenz $x^2 \equiv a \bmod 2$ immer lösbar, die Kongruenz $x^2 \equiv a \bmod 4$ nur im Fall $a \equiv 1 \bmod 4$ lösbar und die Kongruenz $x^2 \equiv a \bmod 2^e$ für $e \geqslant 3$ nur im Fall $a \equiv 1 \bmod 8$ lösbar.

33. Zeigen Sie, dass $2^{1019} - 1$ keine (Mersenne-) Primzahl ist. (Hinweis: 2039 ist eine Primzahl).

34. Gibt es eine Quadratzahl der Form $55k - 1$?

35. Sei $p > 5$ prim. Zeigen Sie: p ist ein Faktor von $\underbrace{11\ldots1}_{p-1}$ (Dezimaldarstellung).

36. Sei p eine Primzahl und $c \in \mathbb{Z}$. Zeigen Sie, dass es unendlich viele Zahlen $x \in \mathbb{Z}^+$ gibt, die folgende simultanen Kongruenzen lösen:
$$x \equiv c \bmod p, \quad x^x \equiv c \bmod p, \quad x^{x^x} \equiv c \bmod p, \quad \ldots$$

37. Zeigen Sie, dass jede Zahl $n > 169$ als Summe von fünf (!) positiven (!) Quadratzahlen dargestellt werden kann.

38. In der Dezimaldarstellung hat 2^{29} genau 9 verschiedene Ziffern. Welche Ziffer fehlt? (Hinweis: Ziffernsumme).

(A) Sei $\mathbb{Z}[\omega] = \{a + b\omega : a, b \in \mathbb{Z}\}$ mit $\omega = \frac{1}{2}(-1 + i\sqrt{3})$.

  (a) Zeigen Sie, dass $\mathbb{Z}[\omega]$ ein euklidischer Ring mit Normabbildung $N(a + b\omega) = a^2 - ab + b^2$ ist.

  (b) Berechne alle Einheiten von $\mathbb{Z}[\omega]$.

  (c) Zeigen Sie, dass 3 in $\mathbb{Z}[\omega]$ durch $(1 - \omega)^2$ teilbar ist.

(B) Finden Sie alle $n \in \mathbb{Z}^+$ mit $\varphi(5n) = 5\varphi(n)$.

(C) Bestimmen Sie $123456789101112\ldots19781979 \bmod 1980$.

(D) Finden Sie alle Lösungen von $x^7 - 14x - 2 \equiv 0 \bmod 49$.

(E) Zeigen Sie, dass es unendlich viele natürliche Zahlen gibt, die nicht als Summe von vier positiven (!) Quadraten dargestellt werden können.

(F) Sei $p \in \mathbb{P}$ ungerade. Zeigen Sie, dass

$$\left(\frac{1 \cdot 2}{p}\right) + \left(\frac{2 \cdot 3}{p}\right) + \cdots + \left(\frac{(p-2)(p-1)}{p}\right) = -1.$$

(G) Zeigen Sie:

  (a) Unter $n+1$ positiven ganzen Zahlen kleiner gleich $2n$, gibt es zwei, sodass eine die andere teilt.

  (b) Angenommen wir haben n positive ganze Zahlen kleiner gleich $2n$, sodass das kleinste gemeinsame Vielfache von je zwei Zahlen größer ist als $2n$. Dann sind alle Zahlen größer als $2n/3$.

(H) Zeigen Sie:

  (a) Unter $n+1$ positiven ganzen Zahlen kleiner gleich $2n$ gibt es zwei Zahlen die relativ prim zueinander sind.

  (b) Seien $1 \leqslant a_1 < a_2 < \cdots < a_l \leqslant n$ ganze Zahlen mit $l > (n+2)/2$. Zeigen Sie, dass es dann Indizes $1 \leqslant i < j < k \leqslant l$ gibt, sodass $a_i + a_j = a_k$.

(I) Finden Sie die kleinste positive ganze Zahl, sodass $x \equiv 5 \bmod 12$, $x \equiv 17 \bmod 20$ und $x \equiv 23 \bmod 42$.

(J) Berechnen Sie die ersten acht Zahlen der Kettenbruchentwicklung von π sowie die ersten 5 Konvergenten p_k/q_k, $k = 0, \ldots, 4$. Zeigen Sie weiters, dass wenn $\frac{r}{s}$ eine rationale Zahl mit $\pi < \frac{r}{s} < 22/7$ ist, $s > 106$ sein muss.

(K) Lösen Sie die folgenden quadratischen Kongruenzen:

  (a) $x^2 + 5x + 3 \equiv 0 \bmod 11$

  (b) $x^2 + 7x + 4 \equiv 0 \bmod 10$

  (c) $2x^2 + 3x + 7 \equiv 0 \bmod 12$

(L) Zeigen Sie, dass es in einer vorgegebenen arithmetischen Progression beliebig viele aufeinanderfolgende zusammengesetzte natürliche Zahlen gibt (Hinweis: Faktorielle).

(M) (a) Zeigen Sie, dass $\lfloor x \rfloor + \lfloor y \rfloor \leqslant \lfloor x + y \rfloor$ für alle $x, y \in \mathbb{R}$.

(b) Zeigen Sie mit Hilfe von (i) und Beispiel 5, dass $n!$ das Produkt von n beliebigen aufeinanderfolgenden Zahlen teilt.

(c) Wie kann man (ii) mit Hilfe von Binomialkoeffizienten zeigen?

(N) Finden Sie die kleinste positive ganze Zahl x, sodass x geteilt durch $10, 9, \ldots, 2$ die Reste $9, 8, \ldots, 1$ hat.

(O) Sei n eine vollkommene Zahl ($\sum_{d|n} d = 2n$). Zeigen Sie, dass

$$\left(\sum_{\substack{(r,s)=1 \\ 1 \leqslant r < s \leqslant n \\ r+s > n}} \frac{1}{rs} \right) \cdot \left(\sum_{d|n} \frac{1}{d} \right) = 1.$$

Hinweis: Leiten Sie für den ersten Faktor eine allgemeine Formel für $n > 1$ her.

(i) Bestimmen Sie alle Lösungen $x, y > 0$ des Gleichungssystems

$$\begin{cases} x + y = 5432 \\ \mathrm{kgV}(x, y) = 223020. \end{cases}$$

(ii) Auf wieviel Nuller endet

$$\frac{500!}{200!}?$$

(iii) Zeigen Sie, dass für alle $a, b, c > 0$

$$[a, b, c] = \frac{abc\,(a, b, c)}{(a, b)(b, c)(c, a)}.$$

(iv) Bestimmen Sie die Lösungen der Gleichung $9x^2 - 24x + 13 \equiv 0 \bmod 59$.

(v) Sei $q > 2$ eine Primzahl. Ist $p = 2^q - 1$ auch eine Primzahl, dann besitzt $x^2 \equiv 3 \bmod p$ keine Lösungen.

(vi) Sei $p = 4k + 1$ eine Primzahl. Zeigen Sie, dass für ungerade $d \mid k$ die Gleichung $x^2 \equiv d \bmod p$ Lösungen besitzt.

(vii) Komet A ist alle 5 Jahre von der Erde aus sichtbar und wurde das letzte Mal vor einem Jahr gesehen. Komet B ist alle 8 Jahre sichtbar und wurde das letzte Mal vor 2 Jahren gesehen. Komet C ist alle 11 Jahre sichtbar und wurde das letzte Mal vor 8 Jahren gesehen. In wie vielen Jahren können alle drei Kometen frühestens gleichzeitig gesehen werden? Und in wie vielen Jahren darauf das nächste Mal?

(viii) Bestimmen Sie alle Lösungen von $\varphi(n) = 80$.

(ix) Es sei $p = 2q + 1$ eine Primzahl, wobei q auch eine Primzahl ist. Weiters sei a eine ganze Zahl welche $a^3 - a \not\equiv 0 \bmod p$ erfüllt. Zeigen Sie, dass a oder $-a$ eine Primitivwurzel modulo p ist.

(x) Berechnen Sie $(2^n - 1, 2^{n^k} + 1)$ für alle $k, n \geqslant 1$.

(xi) Geben Sie alle Paare $(x, y) \in \mathbb{Z}^2$ an, sodass $40x + 64y = 56$.

(xii) Geben Sie eine Zahl kleiner oder gleich 1000 an, welche dividiert durch 7 Rest 4, dividiert durch 9 Rest 7 und dividiert durch 10 Rest 6 ergibt.

(xiii) Was sind die beiden letzten Ziffern (in Basis 10) der Zahl 3^{3333}?

(xiv) Es sei p eine ungerade Primzahl und g_1 und g_2 zwei Primitivwurzeln modulo p. Zeigen Sie, dass $g_1 g_2$ keine Primitivwurzel modulo p ist.

(xv) Zeigen Sie, dass es unendlich viele Primzahlen der Form $6k - 1$ gibt.

(xvi) Es sei p eine ungerade Primzahl. Berechnen Sie $\left(\frac{\frac{p+1}{2}}{p}\right)$ und $\left(\frac{\frac{p-1}{2}}{p}\right)$.

(xvii) Es sei p eine Primzahl und k eine natürliche Zahl welche $0 \leqslant k \leqslant p - 1$ erfüllt. Zeigen Sie

$$k!(p - 1 - k)! \equiv (-1)^{k+1} \bmod p.$$

(xviii) Es seien p und q Primzahlen, sodass $p = 2q + 1$ und m sei eine natürliche Zahl welche $1 \leqslant m \leqslant p - 2$ erfüllt. Zeigen Sie, dass m eine Primitivwurzel modulo p ist, genau dann wenn m ein quadratischer Nichtrest modulo p ist.

(xix) Es seien a und b zwei teilerfremde natürliche Zahlen und $m, n, r, s \in \mathbb{Z}$, sodass $ms - nr = \pm 1$. Berechnen Sie $(ma + nb, ra + sb)$.

(xx) Es seien a und b zwei teilerfremde natürliche Zahlen. Berechnen Sie $(a^3 - b^3, a^2 - b^2)$.

(xxi) Angenommen p und $8p - 1$ sind Primzahlen. Kann $8p + 1$ auch prim sein?

(xxii) Es sei n eine natürliche Zahl p eine Primzahl. Zeigen Sie, dass

- $11 \mid n^{11} + 10n$,
- $42 \mid n^7 - 7$,

- $p \mid n^{p^p} - n$.

(xxiii) Es seien m und n natürliche Zahlen. Zeigen $\varphi(m) \mid \varphi(n)$ falls $m \mid n$.

(xxiv) Es sei n eine ungerade natürliche Zahl. Zeigen Sie, dass $n \mid 2^{n!} - 1$.

(xxv) Berechnen Sie den Exponenten von 2 in $(2^n - 1)!$.

(xxvi) Es sei F_n die n-te Fermat-Zahl. Zeigen Sie, dass alle Teiler von F_n von der Form $2^{n+1}k + 1$ sind.

(xxvii) Sei $p > 2$ eine Primzahl. Zeigen Sie, dass genau dann jeder quadratische Nichtrest modulo p eine Primitivwurzel modulo p ist, wenn p eine Fermatsche Primzahl ist.

(xxviii) Es sei n eine natürliche Zahl. Zeigen Sie, dass alle Primteiler von $4n^2 + 1$ von der Form $4k + 1$ sind.

(xxix) Berechnen Sie Näherungsbrüche der Kettenbruchentwicklung von $(1 + \sqrt{5})/2$. ?????

(xxx) Es sei $a/b = [a_0, a_1, \ldots, a_n]$ mit $(a, b) = 1$ und $b > 0$. Zeigen Sie: Ist n gerade, dann ist $x = -cq_{n-1}$ und $y = cp_{n-1}$ eine Lösung der Gleichung $ax + by = c$. Ist n ungerade, dann ist $x = cq_{n-1}$ und $y = -cp_{n-1}$ eine Lösung der Gleichung $ax + by = c$.

(xxxi) Finden Sie eine Lösung der Gleichung $1255x + 177y = 1$.