Ü 1. Bestimmen Sie alle $x \in \mathbb{Z}$, für die gilt

$$2x \equiv 1 \mod 3, \quad x \equiv 2 \mod 5, \quad 3x \equiv 4 \mod 7 \quad \text{und} \quad x \equiv 3 \mod 4.$$

Ü 2. Sei $p \in \mathbb{P}$.

(1) Zeigen Sie: Für $j \in [0, p]$ gilt

$$p \mid \binom{p}{j} \Leftrightarrow j \in [1, p-1].$$

(2) Beweisen Sie, dass für a, $b \in \mathbb{Z}$ gilt: $(a+b)^p \equiv a^p + b^p \mod p$.

(3) Geben Sie einen Beweis für den *kleinen Satz von Fermat*, d.h.,

$$a^p \equiv a \mod p \quad \text{für alle } a \in \mathbb{Z},$$

indem Sie $(a+1)^p$ modulo p betrachten.

***Ü 3.** Die Suche nach rechtwinkligen Dreiecken mit ganzzahliger Seitenlänge führt auf die diophantische Gleichung

$$X^2 + Y^2 = Z^2. \tag{$\star$}$$

Ein Lösung $(a, b, c) \in \mathbb{N}^3$ von $(\star)$ heißt *pythagoräisches Tripel*. Ein pythagoräisches Tripel heißt *primitiv* wenn gilt $\operatorname{ggT}(a, b, c) = 1$.

(1) Bestimmen Sie alle $(a, b, c) \in \mathbb{Z}^3$ mit $abc = 0$ die $(\star)$ lösen (triviale Lösungen).

Im Weiteren setzen wir stets voraus $abc \neq 0$.

(2) Zeigen Sie: Ist $(a, b, c) \in \mathbb{Z}^3$ eine nicht-triviale Lösung von $(\star)$, so existiert ein $d \in \mathbb{Z}$ und ein primitives pythagoräisches Tripel $(a_0, b_0, c_0) \in \mathbb{N}^3$ mit $(a, b, c) = (\pm da_0, \pm db_0, \pm dc_0)$.

(3) Zeigen Sie: Ein pythagoräisches Tripel (a, b, c) ist genau dann primitiv, wenn a, b, c paarweise teilerfremd sind. Ist (a, b, c) ein primitives pythagoräisches Tripel, so ist genau eines von a und b gerade.

(4) Überlegen Sie sich, dass primitive pythagoräische Tripel in Bijektion zu rationalen Punkten $(x, y) \in \mathbb{Q}^2$ am Einheitskreis (d.h. $x^2 + y^2 = 1$) mit $x > 0$ und $y > 0$ stehen.

(5) Die rationalen Punkte am Einheitskreis lassen sich parametrisieren, indem man einen festen rationalen Punkt am Einheitskreis wählt, alle Geraden mit rationaler Steigung durch diesen Punkt betrachtet, und jeweils den zweiten Schnittpunkt dieser Geraden mit dem Einheitskreis bestimmt.

Tun Sie das, ausgehend vom Punkt $(-1, 0)$. (Die Gerade $x = -1$ hat keinen weiteren Schnittpunkt mit dem Einheitskreis; der Schnittpunkt an der Stelle $(-1, 0)$ ist ein Doppelpunkt.)

(6) Bestimmen Sie nun alle primitiven pythagoräischen Tripel. (Ist ihr rationaler Parameter im vorigen Schritt k, so setzen Sie $k = \frac{a}{b}$ mit $\mathrm{ggT}(a, b) = 1$. Sie werden noch weitere Einschränkungen an a, b machen müssen, um tatsächlich immer primitive Tripel zu erhalten.)

Für die folgenden Aufgaben ist Stoff aus der Vorlesungseinheit vom 10.1. hilfreich (insbesondere der kleine Satz von Fermat (siehe auch Übung 2) und die Teilbarkeitskriterien).

Ü 4. Sei $a \in \mathbb{N}$. Zeigen Sie, dass die Zahlen a^5 und a mit derselben Dezimalziffer enden.

Ü 5. Geben Sie, basierend auf der Dezimaldarstellung einer natürlichen Zahl, Teilbarkeitsregeln für die Teilbarkeit durch d für alle $d \in [2, 11]$.

Hinweis: Für $d = 7$ betrachten Sie 10^d modulo 7 und finden Sie ein passendes gewichtetetes Analogon der Ziffernsumme. (Die Regel für $d = 7$ ist etwas komplizierter.)