Aufgabe 1: (4 Punkte)

1. Berechnen Sie $3^{1000} \pmod 7$.

   $\varphi(7) = 7 - 1 = 6$, also $3^{1000} \equiv 3^{6k+4} \equiv 1^k 3^4 \equiv (3^2)^2 \equiv 81 \equiv 4 \pmod 7$.

2. Geben Sie alle ganzzahligen Lösungen der Gleichung $x^2 - 11x - 11 \equiv 0 \pmod{77}$ an.

   Mod 11: $x^2 \equiv 0 \pmod{11}$.

   Mod 7: $x^2 - 4x - 4 \equiv (x-2)^2 - 8 \pmod 7 \Leftrightarrow (x-2)^2 \equiv 1 \pmod 7$

x		1	2	3	4	5	6	7
$(x-2)^2$	$\pmod 7$	1	0	1	4	2	2	4

   Es ist also $x \equiv 0 \pmod{11}$ und $x \equiv 1$ oder $\equiv 3 \pmod 7$: Es ist dann $x = 22$ und $x = 66$ eine Lösung modulo 77.

Aufgabe 2: (4 Punkte) Entscheiden Sie, welche der beiden Kongruenzen in $\mathbb{Z}$ lösbar bzw. unlösbar sind. Im Falle der Lösbarkeit, geben Sie eine Lösung an, im anderen Fall eine Begründung für die Unlösbarkeit.

1. $82x \equiv 1 \pmod{101}$, man bestimmt 85 als Inverses modulo 101 (z.B. mit dem erw. euklid. Alg).
2. $1105x \equiv 5 \pmod{442}$

   Hier ist der $\mathrm{ggT}(1105, 442) = 221 \neq 1$, es gibt kein Inverses von 1105 modulo 442.

Aufgabe 3: (2 Punkte) Welche der folgenden Zahlen sind Summe zweier Quadrate? Geben Sie jeweils eine Begründung an.

Wir prüfen bei den Primzahlen jeweils, ob sie kongruent 1 mod 4 sind. Nach einem Satz der Vorlesung sind sie dann eine Summe von Quadraten

1. $n_1 = 104729$, n_1 ist prim, $n_1 \equiv 1 mod 4$: Ja
2. $n_2 = 104723$, n_2 ist prim, $n_2 \equiv -1 mod 4$: Nein
3. $n_3 = 307961$, mit der Faktorisierung in Primzahlen: $n_3 = 547 \cdot 563$. Beide Faktoren sind kongruent -1 modulo 4. Damit ist das Produkt nicht als Summe von zwei Quadraten darstellbar.

Aufgabe 4: (6 Punkte) Entscheiden Sie, ob die folgende diophantische Gleichung eine nichttriviale Lösung besitzt:

$$0 = -37X^2 + 27Y^2 + 43Z^2$$

$27 = 3^2 * 3$ ist nicht quadratfrei, deswegen machen wir eine Variablentransformation $x = X, z = Z, y = 3Y$ und betrachten die Gleichung

$$0 = -37x^2 + 3y^2 + 43z^2$$

Wir prüfen die Bedingungen des Satzes von Legendre:

- nicht alle Koeffizienten haben das gleiche Vorzeichen: Ja
- $\left(\frac{-(-37)3}{43}\right) = 1$

- $\left(\frac{-(-37)43}{3}\right) = 1$
- $\left(\frac{(-3)43}{37}\right) = -1$, diese Bedingung ist verletzt.

Es folgt: die diophantische Gleichung hat keine nichttriviale Lösung.

Bei der Berechnung der Jacobi-Symbole sind diese Zwischenergebnisse hilfreich: (jeweils eins berechnen und das andere über quadratische Reziprozität bestimmen.)

$$\left(\frac{37}{43}\right) = -1, \quad \left(\frac{3}{43}\right) = -1, \quad \left(\frac{37}{3}\right) = 1,$$
$$\left(\frac{43}{37}\right) = -1, \quad \left(\frac{43}{3}\right) = 1, \quad \left(\frac{3}{37}\right) = 1$$

Aufgabe 5: (6 Punkte) Bestimmen Sie alle rationalen Lösungen von $x^2 + 23y^2 = 1$.

Eine Lösung ist $x_0 = 1, y_0 = 0$. Die Gerade durch diesen Punkt ist $y = m(x-1)$. Einsetzen der Geradengleichung in die Kurve ergibt:

$$\begin{aligned} 1 = x^2 + 23y^2 &= x^2 + 23m^2(x-1)^2 \Leftrightarrow x^2 - 1 + 23m^2(x-1)^2 = 0 \\ &\Leftrightarrow (x-1)(x+1) + 23m^2(x-1)^2 = (x-1)((x+1) + 23m^2(x-1)) = 0 \end{aligned}$$

Wir suchen Lösungen mit $x \neq 1$, also mit $((x+1) + 23m^2(x-1)) = 0$:

$$0 = ((x+1) + 23m^2(x-1)) \Leftrightarrow x(1 + 23m^2) = 23m^2 - 1 \Leftrightarrow x = \frac{23m^2 - 1}{23m^2 + 1}$$

Einsetzen in die Geradengleichung liefert dann noch $y = \frac{-2m}{23m^2+1}$. Das ist, mit $m \in \mathbb{Q}$, eine Parametrisierung der rationalen Lösungen mit $x \neq 1$, es gibt noch die Lösung $x = 1, y = 0$.

Aufgabe 6: (6 Punkte) Eine rationale Lösung der Gleichung $y^2 = x^3 - 2x$ ist $(-1, 1)$. Finden Sie eine weitere rationale Lösung mit $x \neq -1$, indem Sie die Tangente durch den Punkt $(-1, 1)$ legen und den zweiten Schnittpunkt ermitteln.

Ein Punkt der elliptischen Kurve ist $x_0 = -1, y_0 = 1$. Die Steigung der Tangenten im Punkt x_0, y_0 berechnet sich über:

$$\frac{\partial}{\partial x} y^2 = 2yy' = 3x^2 - 2$$

Einsetzen von x_0, y_0 ergibt: $2y' = 1$, also $y' = 1/2$. Die Tangente an die Kurve in dem Punkt hat also die Gleichung $y = \frac{1}{2}x + b$. Erneutes Einsetzen der Koordinaten x_0, y_0 ergibt $y = \frac{x}{2} + \frac{3}{2}$. Einsetzen der Tangentengleichung in die Gleichung der Kurve:

$$\begin{aligned} \left(\frac{x}{2} + \frac{3}{2}\right)^2 = x^3 - 2x &\Leftrightarrow \frac{1}{4}x^2 + \frac{3}{2}x + \frac{9}{4} = x^3 - 2x \\ &\Leftrightarrow x^3 - \frac{1}{4}x^2 - \frac{7}{2}x - \frac{9}{4} = 0 \\ &\Leftrightarrow (x+1)\left(x^2 - \frac{5}{4}x - \frac{9}{4}\right) = 0 \Leftrightarrow (x+1)^2\left(x - \frac{9}{4}\right) = 0 \end{aligned}$$

Die letzte Zeile folgt durch Polynomdivision mit dem Faktor $(x+1)$ und pq-Formel bzw. durch Polynomdivision mit dem Faktor $(x+1)^2$. Die x-Koordinate des zweiten Schnittpunktes der Tangente mit der Kurve ist $x_1 = \frac{9}{4}$, dazu gehört die y-Koordinate $y_1 = \frac{21}{8}$.