Goethe-Universität Frankfurt
Institut für Mathematik

Prof. Dr. Jakob Stix
Theresa Kumpitsch

Elementare Zahlentheorie

Wintersemester 2021/22

Übungsblatt 10 07.01.21

Aufgabe 1 (Unendlich viele Primzahlen (mal wieder), 4 Punkte)**.**

(a) Sei $f \in \mathbb{Z}[T]$ ein nicht-konstantes Polynom. Zeigen Sie, dass es unendlich viele Primzahlen p gibt, sodass f eine Nullstelle mod p besitzt, d.h. es gibt ein $n \in \mathbb{Z}$ mit $f(n) \equiv 0 \bmod p$.
Tipp: Begründen Sie zunächst, warum wir ohne Einschränkung annehmen können, dass f irreduzibel ist, teilerfremde Koeffizienten besitzt und $f(0) \neq 0$. Führen Sie dann den Beweis per Widerspruch. Angenommen also, es gibt nur endlich viele Primzahlen $p_1, \ldots, p_r$ für die sich ein n findet, sodass p_i ein Teiler von $f(n)$ ist. Betrachten Sie dann für $a_0 = f(0)$ und eine natürliche Zahl m den Wert $f(a_0 m p_1 \cdots p_r)$.

(b) Folgern Sie, dass jede ganze Zahl $a \neq 0$ quadratische Rest mod unendlich vieler Primzahlen ist.

Aufgabe 2 (Lösbarkeit diophantischer Gleichungen, 2 Punkte)**.**
Zeigen Sie, dass die Gleichung

$$(2X - 1)(3Y - 1) = 0$$

für alle natürlichen Zahlen n Lösungen mod n besitzt, allerdings keine ganzzahligen Lösungen $(x, y) \in \mathbb{Z}^2$.

Aufgabe 3 (Quadratische und kubische Reste, 4 Punkte)**.**
Manchmal ist es nützlich, eine Diophantische Gleichung modulo einer geeigneten natürlichen Zahl n zu betrachten, um festzustellen, ob sie ganzzahlige Lösungen besitzen kann. Hierzu ein paar Aufgaben.

(a) Zeigen Sie, dass die Gleichung $15X^2 - 7Y^2 = 9$ keine ganzzahligen Lösungen $(x, y) \in \mathbb{Z}^2$ besitzt.

(b) (i) Bestimmen Sie alle möglichen kubischen Reste modulo 9.
(ii) Sei $n \geq 0$ und sei

$$n = x^3 + y^3 + z^3$$

ganzzahlig lösbar. Dann ist eine notwendige Bedigung für n, dass $n \not\equiv \pm 4 \bmod 9$.

Bemerkung: Die Frage, welche Zahlen sich als Summe von drei Kubikzahlen darstellen lassen ist ein offenes Problem, d.h. es ist insbesondere nicht bekannt, ob die Bedingung aus (b) hinreichend ist und es ist ebenfalls schwierig, entsprechende Darstellungen zu bestimmen. So war es z.B. lange unklar, ob sich 33 oder 42 so darstellen lassen. Dieses Problem wurde von Andrew Booker und Andrew Sutherland 2019 gelöst, 2020 haben diese auch die Fälle 165, 795 und 906 knacken können. Beispielsweise hat die Gleichung $X^3 + Y^3 + Z^3 = 42$ eine Lösung, nämlich

$$(-80\,538\,738\,812\,075\,974)^3 + 80\,435\,758\,145\,817\,515^3 + 12\,602\,123\,297\,335\,631^3 = 42.$$

Aufgabe 4 (Quadratisch Henseln, 5 Punkte)**.**

(a) Bestimmen Sie die Lösungen von der Kongruenzgleichung $x^2 \equiv 2 \bmod 7$. Nutzen Sie das Ergebnis um eine Lösung der Kongruenzgleichung $x^2 \equiv 2 \bmod 49$ zu finden.

(b) Sei p eine ungerade Primzahl und $p \nmid m$. Angenommen $x^2 \equiv m \bmod p$ besitzt eine Lösung. Zeigen Sie, dass es eine Folge ganzer Zahlen $(x_1, x_2, x_3, \ldots)$ gibt mit $0 \leq x_n \leq p^n - 1$ und $x_{n+1} \equiv x_n \bmod p^n$, sodass x_n eine Lösung der Gleichung mod p^n ist, d.h. $x_n^2 \equiv m \bmod p^n$.
Tipp: Nutzen Sie die Idee aus (i) und konstruieren Sie die Folge der Lösungen induktiv.

Aufgabe 5 (Pythagoräische Tripel und rationale Parametrisierung, 5 Punkte)**.**
Gegeben Sie die diophantische Gleichung

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

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

(a) Zeigen Sie: (a, b, c) ist genau dann ein pythagoräisches Tripel, wenn $x = \frac{a}{c}$ und $y = \frac{b}{c}$ ein rationaler Punkt auf dem Einheitskreis ist, d.h. ein Punkt $(x, y) \in \mathbb{Q}^2$ mit $x^2 + y^2 = 1$. Zeigen Sie ferner, dass die Steigung der Geraden durch die Punkte $(-1, 0)$ und (x, y) eine rationale Zahl $t \in (0, 1)$ ist.

(b) Bestimmen Sie für $t \in (0, 1) \cap \mathbb{Q}$ die Schnittpunkte der Geraden der Steigung t durch den Punkt $(-1, 0)$ mit dem Einheitskreis.

(c) Zeigen Sie, dass die Menge der primitiven pythagoräischen Tripel gegeben ist durch

$$a = 2rs, \quad b = r^2 - s^2, \quad c = r^2 + s^2 \qquad \text{mit } r, s \in \mathbb{Z} \text{ so dass } r \not\equiv s \pmod 2.$$

Tipp: Nutzen Sie (b) und schreiben Sie t zunächst als gekürzten Bruch $t = r/s \in (0, 1)$, d.h. $r < s$ (Warum?). Was passiert, wenn r und s beide ungerade sind?

(e*) (freiwillig, keine Punkte) Wie viele rationale Punkte kann ein Kreis im $\mathbb{R}^2$ mit irrationalem Mittelpunkt (x_0, y_0) (d.h. $x_0 \in \mathbb{R} \setminus \mathbb{Q}$ oder $y_0 \in \mathbb{R} \setminus \mathbb{Q}$) haben?

Abgabe: Am kommenden Freitag, den **14.01.21**, bis um 12:00 digital auf OLAT.
