Goethe-Universität Frankfurt
Institut für Mathematik

Prof. Dr. Jakob Stix
Theresa Kumpitsch

Elementare Zahlentheorie

Wintersemester 2021/22

Übungsblatt 2 29.10.21

Aufgabe 1 (Lemma von Bézout, 5 Punkte)**.**

(a) Bestimmen Sie alle Lösungen $(x, y) \in \mathbb{Z}^2$ der linearen diophantischen Gleichung

$$6x - 9y = 15.$$

(b) (i) Begründen Sie, warum die lineare diophantische Gleichung

$$2x - 3y + 6z = 5$$

eine Lösung $(x, y, z) \in \mathbb{Z}^3$ besitzt.

(ii) Finden Sie eine Lösung (x_0, y_0, z_0).

(iii) Bestimmen Sie nun alle Lösungen. Gehen Sie dazu wie folgt vor. Überlegen Sie sich Bedingungen an $\Delta_x, \Delta_y, \Delta_z$, damit

$$x = x_0 + \Delta_x, y = y_0 + \Delta_y \text{ und } z = z_0 + \Delta_z$$

eine Lösung ist. Versuchen Sie schließlich Δ_x, Δ_y, und Δ_z in Abhängigkeit zweier Parameter darzustellen d.h. finden Sie eine Parametrisierung der Form

$$(\Delta_x, \Delta_y, \Delta_z)^T = sv + tu \text{ für } t, s \in \mathbb{Z} \text{ und } v, u \in \mathbb{Z}^3.$$

Aufgabe 2 (Binomischer Lehrsatz mod p, 5 Punkte)**.** Sei p eine Primzahl.

(a) Sei $k \in \mathbb{N}$ mit $k < p$. Zeigen Sie, dass gilt $p \mid \binom{p}{k}$.

(b) Folgern Sie, dass für alle x, y die folgende Kongruenz gilt:

$$(x + y)^p \equiv x^p + y^p \bmod p.$$

(c) Nutzen Sie dies für einen (zur Vorlesung alternativen) Beweis des kleinen Satzes von Fermat: Für jede ganze Zahl a ist

$$a^p \equiv a \pmod p.$$

(d) Zeigen Sie auf eine weitere Art, dass es unendlich viele Primzahlen gibt. Gehen Sie dazu wie folgt vor.

(i) Seien $a, b, n, m \in \mathbb{Z}$ und $n, m \geq 1$. Angenommen $a|b^n - 1$ und $a|b^m - 1$. Zeigen Sie, dass gilt

$$a|b^{\mathrm{ggT}(n,m)} - 1.$$

(ii) Sei p eine Primzahl. Zeigen Sie, dass für alle Primteiler q von $2^p - 1$ gilt:

$$q \equiv 1 \pmod p.$$

(iii) Nehmen Sie an, dass es eine größte Primzahl p gibt und führen Sie das zu einem Widerspruch.

Aufgabe 3 (EAN-Code, 5 Punkte)**.** Der EAN-Code (Strichcode) arbeitet mit 13 Ziffern $a = (a_1, \ldots, a_{13})$ aus $\{0, 1, \ldots, 9\}$. Gültige Code-Wörter erfüllen die Prüfbedingung

$$a_1 + 3a_2 + a_3 + 3a_4 + \ldots + 3a_{12} + a_{13} \equiv 0 \pmod{10}$$

(a) Zeigen Sie, dass es immer erkannt werden kann, dass kein korrekter EAN-code vorliegt, wenn wir uns bei der Eingabe einer EAN an genau einer Stelle vertan haben.

(b) Welche Ziffernvertauschungen können erkannt werden (und welche nicht)?

Aufgabe 4 (Primzahlen, 5 Punkte)**.**

(a) Benutzen Sie das Sieb des Eratosthenes, um alle Primzahlen bis 400 zu bestimmen.
(b) Wieviele Primzahlen gibt es bis 100, von 100 bis 200, von 200 bis 300 und von 300 bis 400?
(c) Ein *Primzahlzwilling* ist ein Paar aus Primzahlen, deren Abstand 2 ist. Wieviele Primzahlzwillinge gibt es bis 400?
(d) Wie verteilen sich die Primzahlen ≤ 400 auf die Kongruenzklassen modulo 10 bzw. modulo 12?
(e) Freiwillige Zeitverschwendung: https://isthisprime.com/game/

Abgabe: Am kommenden Freitag, den **05.11.21**, bis um 12:00 digital auf OLAT.
