Einführung in die Zahlentheorie
Blatt 7

hhu Düsseldorf
WiSe 2021/22

Abgabe: bis Montag 29.11.2021

Vorlesungswebseite: `http://reh.math.uni-duesseldorf.de/~khalupczok/EZ/`
Die folgenden Aufgaben sind schriftlich zu bearbeiten und abzugeben. Wie üblich sind dabei alle Behauptungen zu beweisen. Resultate aus der Vorlesung dürfen verwendet werden, die zugehörigen Referenznummern können Sie zur Klarstellung dann mit angeben.

Aufgabe 1 (5 Punkte):

(1) Wie können die Lösungen eines Kongruenzensystems $x \equiv a_1 \ (m_1)$ und $x \equiv a_2 \ (m_2)$, wo $(m_1, m_2) = 1$ ist, direkt mit dem erweiterten euklidischen Algorithmus bestimmt werden?

(2) Seien $a, b \in \mathbb{Z}$ und $m, n \in \mathbb{N}$. Dann ist das Kongruenzensystem $x \equiv a \ (m),\ x \equiv b \ (n)$ genau dann lösbar, wenn $(m, n) \mid (a - b)$ gilt. Beschreiben Sie in diesem Fall die Lösungsmenge.

Aufgabe 2 (3 Punkte):

Für die Eulersche φ-Funktion zeige man: (1) Aus $a \mid b$ folgt $\varphi(a) \mid \varphi(b)$.
(2) Für jedes n gibt es ein a mit $\varphi(a) = n!$ (Tipp nach Erdős: $\prod_{p \le n}(p-1) \mid n!$).

Aufgabe 3 (5 Punkte):

(1) Berechnen Sie die Ordnungen der Restklassen 6 mod 31 und 5 mod 108.

(**Hinweis**: Sie können Teil (2) benutzen.)

(2) Für $m, a, c \in \mathbb{N}$ mit $m > 1$ gelte $a^c \equiv 1 \bmod m$. Zeigen Sie: Genau dann ist c die Ordnung von a mod m, wenn gilt: Für jeden Primteiler q von c ist $a^{c/q} \not\equiv 1 \bmod m$.

Aufgabe 4 (5 Punkte):

Es sei p eine Primzahl, sei $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ der (bis auf Isomorphie eindeutig bestimmte) endliche Körper mit p Elementen, weiter bezeichne $\mathbb{F}_p[X]$ den Polynomring in einer Unbestimmten über dem Körper $\mathbb{F}_p$.

(1) Zeigen Sie mittels Grad- und Nullstellenvergleich, dass in $\mathbb{F}_p[X]$ gelten:
$$X^{p-1} - 1 = (X+1)(X+2)\cdots(X+(p-1)), \qquad (X+1)^p - (X+1) = X^p - X.$$

(2) Aus der zweiten Gleichung folgt die Gültigkeit von
$$\binom{p}{j} \equiv 0 \bmod p \text{ für } 1 \le j \le p-1.$$

(3) Für $m, n \in \mathbb{N}$ und für $k \in \mathbb{N}_0$ mit $0 \le k \le m$ gilt
$$\binom{mp^n}{kp^n} \equiv \binom{m}{k} \bmod p.$$

(**Hinweis**: Warum ist $(X+1)^{p^n m} = (X^{p^n}+1)^m$ in $\mathbb{F}_p[X]$?)

Aufgabe 5 (2 Punkte):

(1) Für $a, b \in \mathbb{N}$ mit $(ab, 70) = 1$ gilt $a^{12} - b^{12} \equiv 0 \ (280)$.

(2) Für $(m, n) = 1$ gilt $n^{\varphi(m)} + m^{\varphi(n)} \equiv 1 \ (mn)$.