Universität des Saarlandes
Fachrichtung 6.1, Mathematik
Prof. Dr. Ernst-Ulrich Gekeler
M.Sc. Philipp Stopp

9. Übung zu Einführung in die Algebra und Zahlentheorie, WS 2015/2016

Aufgabe 1. *(1 + 1 + 2 + 2 + 4 + 5 = 15 Punkte)*
Die ISBN (Internationale Standardbuchnummer) eines Buches bestand bis 2006 aus 10 Ziffern, z.B.:

$$2 - 070 - 61275 - 9\,.$$

Dabei beschreibt der erste Block die Sprache (z.B. 0 oder 1 für Englisch, 2 für Französisch, 3 für Deutsch, 88 für Italienisch,...), der zweite Block den Verlag und der dritte Block die Buchnummer innerhalb des Verlags. Die letzte Ziffer ist eine sogenannte Prüfziffer.
Bezeichnet man die 10 Ziffern mit $a_1, \ldots, a_{10}$, so erfüllt eine gültige ISBN immer

$$a_1 + 2a_2 + 3a_3 + \ldots + 10a_{10} \equiv 0 \pmod{11}\,.$$

Dabei steht ein eventuell auftretendes "X" für die Ziffer 10.
(i) Testen Sie die Gültigkeit der ISBN an mindestens einem Buch Ihrer Wahl.
(ii) Begründen Sie: Sind die Ziffern $a_1, \ldots, a_9$ vorgegeben, so kann man die Prüfziffer ($\in \{0, 1 \ldots, 9, X\}$) immer so wählen, dass eine gültige ISBN entsteht.
(iii) Begründen Sie: Wird bei der Eingabe einer ISBN (genau) eine Ziffer falsch eingetippt, so entsteht immer eine ungültige Nummer.
(iv) Begründen Sie: Werden bei der Eingabe einer ISBN zwei Ziffern vertauscht, so entsteht immer eine ungültige Nummer.
(v) Wieso wurde bei der ISBN ein Prüfverfahren mod 11 und nicht mod 10 verwendet?
(vi) Seit 2007 wird ein neues System mit 13 Ziffern verwendet (ISBN-13).
Die 13-te Ziffer ist die Prüfziffer. Damit eine ISBN-13 gültig ist, muss sie

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

erfüllen.
Welche Vor- und Nachteile hat das neue System gegenüber dem alten?

- Bitte wenden -

Aufgabe 2. *(4 + 4 + 2 = 10 Punkte)*
Es sei p eine Primzahl. Zeigen Sie:
(i)

$$\prod_{1 \le a < p} a \equiv -1 \pmod{p}.$$

(ii) Für $a \in \mathbb{N}$ teilerfremd zu p sei $F(a) := (a^{p-1} - 1)/p$. Dann ist $F(a) \in \mathbb{Z}$ und

$$F(ab) \equiv F(a) + F(b) \pmod{p}.$$

(iii) Definiert F einen Homomorphismus von $(\mathbb{Z}/p)^\star$ nach $(\mathbb{Z}/p, +)$?

Aufgabe 3. *(10 Punkte)*
Es sei p eine Primzahl und

$$m := m_0 + m_1 p + m_2 p^2 + \ldots + m_r p^r$$

sowie

$$n := n_0 + n_1 p + n_2 p^2 + \ldots + n_s p^s$$

mit $m_i, n_j \in \{0, \ldots, p-1\}$, für $0 \le i \le r$ und $0 \le j \le s$, sowie $m_i = 0$ für $i > r$ und $n_j = 0$ für $j > s$.
Zeigen Sie die folgende Kongruenz:

$$\binom{m}{n} \equiv \prod_k \binom{m_k}{n_k} \pmod{p}.$$

Erinnerung: Es ist $\binom{m}{n} = 0$, falls $m < n$ und $\binom{0}{0} = 1$.

Aufgabe 4. *(5 Punkte)*
Die Zahl 2 ist Primitivwurzel modulo 83 und 6 ist Primitivwurzel modulo 41 (das müssen Sie nicht nachprüfen).
Bestimmen Sie eine natürliche Zahl a mit

$$\begin{aligned} a &\equiv 2 \pmod{83} \\ a &\equiv 6 \pmod{41} \end{aligned}$$

und berechnen Sie die Ordnung der Restklasse von a in der primen Restklassengruppe modulo $3403 = 41 \cdot 83$.

Abgabe bis Donnerstag, den 07.01.2016
vor der Vorlesung in die Briefkästen

Wir wünschen Ihnen ein frohes Weihnachtsfest
und einen guten Rutsch ins neue Jahr!