**Mathematisches Institut**
**Abt. für Reine Mathematik**
Dr. K. Halupczok

14.06.2006

Übungen zur Vorlesung

# Elementare Zahlentheorie

SoSe 2006

## Musterlösung Blatt 6

**Aufgabe 1.**

(a) *Ein Ei wiegt* 55 *g, ein Eßlöffel Mehl* 10 *g, ein Eßlöffel Zucker und Butter je* 15 *g. Es soll ein Rührteig hergestellt werden, der aus gleichen Teilen Eier, Mehl, Zucker und Butter besteht. Es ist noch ein Eigelb (*20 *g) und ein halbes Päckchen Backpulver übrig, die mitverwendet werden sollen; ein Päckchen Backpulver reicht für* 500 *g Mehl. Wie läßt sich mit diesen Angaben ein Rührteig abmessen? Dabei sind nur ganzzahlig viele zusätzliche Eier, ganze zusätzliche Backpulverpäckchen und ganzzahlig viele Eßlöffel Mehl, Zucker und Butter erlaubt. Eine Kuchenform faßt gut* 1.5 *kg Teig. Wieviele Kuchen lassen sich aus dem Rührteig backen?*

Beh.: Man braucht 1575 EL Mehl, 286 Eier, 1050 EL Zucker. 1050 EL Butter und 31 Päckchen Backpulver. Dies ergibt 42 Kuchen.

Bew.: Sei $5x$ die benötigte Mehlmenge (= Menge an Eiern, Zucker und Butter) in Gramm. Dann gilt:

$$\begin{aligned} 5x - 250 &\equiv 0 \ (500) \quad \text{(Mehl, wegen Backpulver)} \\ 5x - 20 &\equiv 0 \ (55) \quad \text{(Eier)} \\ 5x &\equiv 0 \ (15) \quad \text{(Zucker, Butter)} \end{aligned}$$

und $5x \equiv 0 \ (10)$ (Mehl, wird durch $5x - 250 \equiv 0 \ (500)$ schon erfüllt.) Also:

$$\begin{aligned} x &\equiv 50 \ (100) \\ x &\equiv 4 \ (11) \\ x &\equiv 0 \ (3) \end{aligned}$$

Lösen mit CRS: $m = 100 \cdot 11 \cdot 3 = 3300, M_1 = 33, M_2 = 300, (M_3 = 1100.)$
$M_i M_i^* \equiv 1 \ (m_i)$ ergibt: $M_1^* = -3, M_2^* = 4, (M_3^* = 2)$.
Dann: $x_0 = 33 \cdot (-3) \cdot 50 + 300 \cdot 4 \cdot 4 + 1100 \cdot 2 \cdot 0 = -150 \equiv 3150 \ (m)$
Mit dieser Lösung $x$ ist:

$$\begin{aligned} 5x &= 15750 = 1575 \cdot 10 \rightsquigarrow 1575 \text{ EL Mehl} \\ 5x - 20 &= 15730 = 286 \cdot 55 \rightsquigarrow 286 \text{ Eier} \\ 5x &= 15750 = 1050 \cdot 15 \rightsquigarrow 1050 \text{ EL Zucker und Butter} \end{aligned}$$

Anzahl Backpulverpäckchen: $\frac{5x-250}{500} = 31$
Teigmenge insgesamt (ohne Backpulver): $x \cdot 5 \cdot 4 = 6300$, also 63 kg Teig, macht $\frac{63}{1.5} = 42$ Kuchen.

(b) *Aus einem alten chinesischen Rechenbuch:* 19 *Räuber stehlen einen Sack mit Goldstücken. Beim Versuch, die Beute gerecht aufzuteilen, bleiben fünf Goldstücke übrig. Es kommt darüber zum Streit, bei dem ein Räuber erschlagen wird. Die restlichen* 18 *versuchen erneut, gerecht aufzuteilen. Diesmal bleiben* 12 *Goldstücke übrig. Erneuter Streit. Wieder wird einer erschlagen. Unter den restlichen* 17 *Räubern geht die Teilung auf. Wieviele Goldstücke waren mindestens im Sack?*

Beh. Es waren mindestens 5610 Goldstücke im Sack.

Bew. Es gebe $x$ Goldstücke, dann ist also

$$x \equiv 5\ (19)$$
$$x \equiv 12\ (18)$$
$$x \equiv 0\ (17)$$

zu lösen. CRS mit paarweise teilerfremden Moduln $m_1 = 19, m_2 = 18, m_3 = 17, m = 19 \cdot 18 \cdot 17 = 5814$ anwenden:
$M_1 = m_2 m_3 = 306, M_2 = m_1 m_3 = 323$ und $M_1^* = 10, M_2^* = 17$. (Berechnung mit Eukl. Algorithmus: $a, b$ mit $1 = aM_1 + bm_1$, also $M_1^* = a$, ebenso $M_2^*$.)
Dann ist $x = M_1 \cdot M_1^* \cdot 5 + M_2 \cdot M_2^* \cdot 12 + M_3 \cdot M_3^* \cdot 0 = 306 \cdot 5 \cdot 10 + 323 \cdot 12 \cdot 17$
$\Rightarrow x = 81192 \equiv 5610\ (m)$, also waren mindestens 5610 Goldstücke im Sack.

**Aufgabe 2.**

(a) *Zeige: Das Kongruenzensystem* $x \equiv a\ (m), x \equiv b\ (n)$ *kann unlösbar in* $x$ *sein, falls* $m$ *und* $n$ *nicht teilerfremd sind. Gilt hingegen* $(m, n) \mid (b - a)$, *so ist es lösbar.*

Beh.: $x \equiv a\ (m), x \equiv b\ (n)$ kann unlösbar in $x$ sein, falls $(m, n) > 1$.

Bew.: z.B. ist $x \equiv 1\ (2) \wedge x \equiv 2\ (4)$, also $x$ sowohl gerade als auch ungerade unlösbar.

Beh.: Gilt $(m, n) | (b - a)$, so ist $x \equiv a\ (m) \wedge x \equiv b\ (n)$ lösbar.

Bew.: $(m, n) | (b - a) \Rightarrow \exists u, v : mu + nv = b - a$.
Sei $x := a + mu \equiv a\ (m)$, dann: $x = a + (b - a) - nv = b - nv \equiv b\ (n)$.
Also ist $x$ Lösung.

(b) *Zeige: Ist das Kongruenzensystem*

$$x \equiv a_i\ (m_i), \quad i = 1, \ldots, r,$$

*lösbar, so gilt* $\forall\ i \neq j : (m_i, m_j) \mid (a_j - a_i)$. *Wie erhält man dann aus einer speziellen Lösung alle Lösungen?*

Beh.: $\forall i = 1, \ldots, r : x \equiv a_i\ (m_i)$ lösbar $\Rightarrow \forall i \neq j : (m_i, m_j) | (a_j - a_i)$

Bew.: Sei $i \neq j, d := (m_i, m_j)$
Aus $x \equiv a_i\ (m_i)$, d.h. $m_i|(x-a_i)$ folgt dann $d|(x-a_i)$, ebenso: $d|(x-a_j)$.
Also: $d|(x-a_i)-(x-a_j) = a_j - a_i$.

Beh.: Ist $s$ Lösung, so sind die $s + k \cdot [m_1, \ldots, m_r], k \in \mathbb{Z}$, alle Lösungen.

Bew.: $x$ Lösung $\Leftrightarrow x \equiv s\ (m_i)$ für alle i $\Leftrightarrow x \equiv s\ ([m_1, \ldots, m_r])$. (Kongruenzrechnen)

(c) *Bestimme die kleinste natürliche Zahl, die bei Division durch* $10, 9, \ldots, 3, 2$ *die Reste* $9, 8, \ldots, 2, 1$ *läßt.*

Beh.: $n = 2519$ ist die kleinste natürliche Zahl, die bei Division durch $10, \ldots, 3, 2$ die Reste $9, \ldots, 2, 1$ läßt.

Bew.: Gesucht ist eine Lösung der Kongruenz $x \equiv 9\ (10), x \equiv 8\ (9), \ldots, x \equiv 1\ (2)$. Also $x \equiv -1\ (k)$ für $k = 2, 3, \ldots, 10$. Eine Lösung ist $x = -1$, alle Lösungen sind nach (b) die Elemente aus $-1 + \mathbb{Z} \cdot [2, \ldots, 10]$. Wir haben $[2, \ldots, 10] = 2^3 \cdot 3^2 \cdot 5 \cdot 7 = 2520$, also tut's 2519.

**Aufgabe 3.**

*Sei* $f \in \mathbb{Z}[x]$, $m \in \mathbb{N}$, $0 \leq a < m$, $f_a(x) = f(x) + a$. *Mit* $\rho_a(m)$ *sei die Lösungsanzahl der Kongruenz* $f_a(x) \equiv 0\ (m)$ *bezeichnet. Dann gilt*

$$\sum_{a=0}^{m-1} \rho_a(m) = m.$$

Vor.: $f \in \mathbb{Z}[X], m \in \mathbb{N}, 0 \leq a < m, f_a(x) = f(x) + a$. Mit $\rho_a(m)$ sei die Lösungszahl der Kongruenz $f_a(x) \equiv 0\ (m)$ bezeichnet.

Beh.:

$$\sum_{a=0}^{m-1} \rho_a(m) = m.$$

Bew.: Definiere für $b = 0, 1, \ldots, m-1$ eine Einteilung in Klassen $K_0, \ldots, K_{m-1}$ gemäß $b \in K_a :\Leftrightarrow f(b) \equiv -a\ (m) \Leftrightarrow f_a(b) \equiv 0\ (m) \Leftrightarrow b$ Lösung von $f_a(x) \equiv 0\ (m)$. Die Klassen sind paarweise disjunkt [ $b \in K_a \cap K_{a'} \Rightarrow -a \equiv f(b) \equiv -a'(m)$, d.h. $a = a'$.] und jede Zahl $b$ liegt in einer solchen Klasse! [$f(b)$ muss zu einem $-a$ Kongruent sein mod $m$]
Für $m$, der Anzahl aller Zahlen $b = 0, 1, \ldots, m-1$ folgt:
$m = \#(K_0 \cup \ldots \cup K_{m-1}) = \sum_{a=0}^{m-1} \#(K_a) = \sum_{a=0}^{m-1} \rho_a(m)$ (Da $K_i$ p.w. disjunkt und $\#K_a = \rho_a(m)$ aus obiger Äquivalenz)

**Aufgabe 4.**

*Sei* $P := \{3, 7, 5, 17, 13, 241\}$. *Konstruiere eine Restklasse* $r + m\mathbb{Z}$, *so daß es für jedes* $N \in r + m\mathbb{Z}$ *und jede Zweierpotenz* $2^k$ *eine Primzahl* $p \in P$ *gibt mit* $N \equiv 2^k\ (p)$.

*Hinweis: Verwende Aufgabe 2 von Blatt 3.*

Vor.: $P := \{3, 7, 5, 17, 13, 241\}$, alles Primzahlen, seinen diese $p_1, \ldots, p_6$, sei $r := 2.036.812$ und $m := p_1 \cdot \ldots \cdot p_6 = 5.592.405$.

Beh.: $\forall N \in r + m\mathbb{Z} \forall k \geq 0 \exists p \in P : N \equiv 2^k \ (p)$

Bew.: Die Kongruenzen aus Aufgabe 2, Blatt 3, seien $x \equiv a_i \ (m_i)$, also

$$\begin{array}{lllll} a_1 = 0, & a_2 = 0, & a_3 = 1, & a_4 = 3, & a_5 = 7, \quad a_6 = 23 \\ m_1 = 2, & m_3 = 3, & m_3 = 4, & m_4 = 8, & m_5 = 12, \quad m_6 = 24 \end{array}$$

Wir haben: $2^{m_i} \equiv 1 \ (p_i)$ für alle $i, p_i \in P$, nämlich:

$$2^2 \equiv 1 \ (3), 2^3 \equiv 1 \ (7), 2^4 \equiv 1 \ (5), 2^8 \equiv 1 \ (17), 2^{12} \equiv 1 \ (13)$$

und $2^{24} \equiv 1 \ (241)$ [Nachrechnen!]
Nach dem CRS existiert ein $r \in \mathbb{Z}$ mit $r \equiv a^{a_i} \ (p_i)$ für alle $i$ (siehe unten)
Dieses $r$ und $m := p_1 \cdot \ldots \cdot p_6$ tun's:
Sei $N \in r + m\mathbb{Z}$ und $k \geq 0$.
Nach Aufgabe 2, Blatt 3, ex. dann ein $i \in 1, \ldots, 6$ mit $k \equiv a_i \ (m_i)$, etwa $k = a_i + m_i u$.
Dann: $2^k \equiv 2^{a_i} \cdot 2^{m_i u} \equiv 2^{a_i} \ (p_i)$ und $N \equiv r \ (p_i), r \equiv 2^{a_i} \ (p_i)$, also ist $N \equiv 2^k \ (p_i)$.

Zur Konstruktion von $r$ mit CRS:

$$\begin{array}{lll} M_1 = 1864135, & M_2 = 798915, & M_3 = 1118481 \\ M_4 = 328965, & M_5 = 430185, & M_6 = 23205 \end{array}$$

Also folgt:

$$\begin{array}{lll} M_1 \equiv 1 \ (3), M_1^* = 1, & M_2 \equiv 5 \ (7), M_2^* = 3, & M_3 \equiv 1 \ (5), M_3^* = 1 \\ M_4 \equiv -2 \ (17), M_4^* = 8, & M_5 \equiv 2 \ (13), M_5^* = 7, & M_6 \equiv 69 \ (421), M_6^* = 7 \end{array}$$

$A_i$ mit $A_i \equiv 2^{a_i} \ (p_i)$ sind $A_1 = 1, A_2 = 1, A_3 = 2, A_4 = 8, A_5 = -2, A_6 = 12$.
Lösung: $r = M_1 M_1^* A_1 + \ldots + M_6 M_6^* A_6 = \ldots = 2.036.812$