Universität Karlsruhe (TH)
Mathematisches Institut II
Prof. Dr. H.-W. Leopoldt

Karlsruhe, 31.5.1990

Elementare Zahlentheorie — Übungsblatt 6

Aufgabe 25 (4 Punkte)

(a) Man bestimme alle $x \in \mathbb{Z}$, für die das folgende System simultaner Kongruenzen erfüllt ist:
$x \equiv 1 \pmod 2$, $x \equiv 2 \pmod 3$, $x \equiv 4 \pmod 7$, $x \equiv 3 \pmod{11}$.

(b) Eine Pillenfabrik A möchte wissen, wieviele Pillen einer bestimmten Sorte die Konkurrenzfirma B pro Stunde herstellt. Ein Informant teilt A über B folgendes mit: Verpackte B die in einer Stunde produzierten Pillen in Packungen zu je i Pillen, so blieben jeweils $i-1$ Pillen übrig. Dies gelte für alle $i \in \{2, 3, \ldots, 10\}$.
Man bestimme die kleinstmögliche Zahl von Pillen, die B pro Stunde herstellt.

Aufgabe 26 (4 Punkte)

Geben Sie alle Lösungen der folgenden Kongruenzen an:

(a) $6 \cdot x^{23} \equiv 4 \pmod{31}$,

(b) $19 \cdot 20^x \equiv 7 \pmod{31}$.

(Hinweis: Benutzen Sie eine Primitivwurzel modulo 31.)

Aufgabe 27 (3 Punkte)

Sei $f \in \mathbb{Z}[T]$ ein Polynom. Für $m \in \mathbb{N}$ sei $N(m)$ die Anzahl der Lösungen in $\mathbb{Z}/_{\mathbb{Z}m}$ von $f(x) \equiv 0 \pmod m$.
Zeigen Sie: Ist $m = m_1 \cdot \ldots \cdot m_r$ mit paarweise teilerfremden $m_i \in \mathbb{N}$, so gilt $N(m) = N(m_1) \cdot \ldots \cdot N(m_r)$.

Aufgabe 28 (3 Punkte)

Sei $f(x, y) = 6xy - 3x - 2y + 1$. Zeigen Sie:
Die Gleichung $f(x, y) = 0$ hat keine Lösung über $\mathbb{Z}$.
Jedoch hat für jedes $m \in \mathbb{N}$ die Kongruenz $f(x, y) \equiv 0 \pmod m$ eine Lösung über $\mathbb{Z}/_{\mathbb{Z}m}$.

Aufgabe 29 (8=2+1+1+2+2 Punkte)

Ein Verfahren zum Wurzelziehen in $\mathbb{F}_p$:
Sei eine Primzahl $p > 2$ und ein $a \in \mathbb{F}_p{}^\times$ gegeben. Wir suchen ein $b \in \mathbb{F}_p{}^\times$ mit $b^2 = a$.

1. Verfahren:
Bestimme eine Primitivwurzel g und stelle eine Tabelle aller Potenzen von g auf. Aus $a = g^{2k}$ mit $k \in \mathbb{Z}$ kann man schließen, daß $b = g^k$ eine Quadratwurzel von a ist.
Dieses Verfahren ist für große p unbrauchbar.

2. Verfahren (*Cantor, Zassenhaus* 1981):
Nehmen wir an, es gibt ein $b_1 \in \mathbb{F}_p{}^\times$ mit ${b_1}^2 = a$. Dann hat das Polynom $f(T) := T^2 - a \in \mathbb{F}_p[T]$ die Primfaktorzerlegung $f(T) = (T - b_1)(T - b_2)$ mit $b_2 = -b_1 \neq b_1$.
Zeigen Sie:

(a) Zu gegebenen $u_1, u_2 \in \mathbb{F}_p$ gibt es genau eine Polynom-Restklasse $\overline{u(T)} \in \mathbb{F}_p[T]/_{\mathbb{F}_p[T] \cdot f(T)}$ mit $u(b_1) = u_1$ und $u(b_2) = u_2$. (Nach Polynomdivision durch $f(T)$ können wir o.B.d.A. mit einem $u(T) \in \mathbb{F}_p[T]$ mit $\deg(u) < 2$ rechnen.)

(b) Für $v(T) := u(T)^{\frac{p-1}{2}} \bmod f(T)$ gilt $v(b_1), v(b_2) \in \{0, 1, -1\}$.

(c) $f(T) = \mathrm{ggT}(v(T)-1, f(T)) \cdot \mathrm{ggT}(v(T), f(T)) \cdot \mathrm{ggT}(v(T)+1, f(T))$ (bis auf Einheit in $\mathbb{F}_p[T]^\times = \mathbb{F}_p{}^\times$).

(d) Bei gleichverteilter zufälliger Auswahl von $u(T) = c_0 + c_1 \cdot T \in \mathbb{F}_p + \mathbb{F}_p \cdot T$ bekommen wir durch (b) und (c) mit Wahrscheinlichkeit $> \frac{1}{2}$ eine *nichttriviale* Faktorisierung von $f(T)$ und damit b_1 und b_2 explizit.

(e) Bestimmen Sie eine Quadratwurzel von $a = 122$ in $\mathbb{F}_{257}$.

Abgabe: Bis spätestens Donnerstag, 7.6.1990, 15.30 Uhr in den Kasten bei Zi. 308 des Mathematikgebäudes oder in der Übung im Hörsaal Hauptbau.