AUSGEWÄHLTE KAPITEL DER ZAHLENTHEORIE
7. ÜBUNGSBLATT

PROF. DR. HENNING KRAUSE
DR. JULIA SAUTER

Aufgabe 1. Betrachte die Diophantische Gleichung $f(x) = x^6 - 1 = 0$. Dann ist $c_1 = 2$ eine Lösung der Gleichung modulo 7. Finde $c_2 \in \mathbb{Z}$ mit $f(c_2) \equiv 0 \pmod{49}$ und $c_2 \equiv c_1 \pmod{7}$. Finde dann $c_3 \in \mathbb{Z}$ mit $f(c_3) \equiv 0 \pmod{343}$ und $c_3 \equiv c_2 \pmod{49}$.
Hinweis 1: Du benötigst du voraussichtlich die folgende Faktorisierung
$\frac{30^6-1}{49} = \left(\frac{30^3-1}{49}\right)(30^3+1) = 551 \cdot 27001$
Hinweis 2: Eine ähnliche Aufgabe ist auf der nächsten Seite zur Hilfestellung gelöst.

Aufgabe 2. Finde alle Restklassen modulo 72, die die folgende Kongruenz lösen

$$x^3 + 2x^2 - 1 \equiv 0 \pmod{72}.$$

Hinweis: $72 = 2^3 3^2$.

Aufgabe 3. Finde alle Restklassen modulo 125, die die folgende Kongruenz lösen

$$x^3 - 52x - 21 \equiv 0 \pmod{125}.$$

Aufgabe 4. Es sei $f(x) = 0$ eine Diophantische Gleichung in einer Variablen. Es sei p eine Primzahl und c eine Lösung modulo p^n. Nimm in (1) und (2) an, dass $p | f'(c)$ gilt. Zeige:

(1) Falls $\frac{f(c)}{p^n} \equiv 0 \pmod{p}$, so gilt für jedes $c_k = c + kp^n$ mit $k \in \{0, 1, \ldots, p-1\}$, dass $f(c_k) \equiv 0 \pmod{p^{n+1}}$.
Vergewissere dich durch das folgende Beispiel: Sei $f(x) = x^3 = 0$, und betrachte die Lösung $c = 3$ modulo 9. Finde alle Lösungen modulo 27, die kongruent 3 modulo 9 sind.
(2) Falls p kein Teiler von $\frac{f(c)}{p^n}$ ist, so gibt es keine Lösung modulo p^{n+1}, die kongruent c modulo p^n ist.
Vergewissere dich durch das Beispiel: Sei $f(x) = x^2 - 3 = 0$ und $c = 1$ eine Lösung modulo 2. Zeige, dass es keine Lösungen modulo 4 gibt, die kongruent 1 modulo 2 sind.

Folgere aus (1), (2) und dem Satz von Hensel: Für jede Diophantische Gleichung in einer Variablen mit Lösung c modulo p^n gibt es entweder keine oder genau eine oder genau p Lösungen modulo p^{n+1}, die kongruent c modulo p^n sind.

Hinweis: Sieh dir den Beweis des Satzes von Hensel an.

Abgabe: Freitag, 3. Juni 2016, bis 10.15 Uhr in der Vorlesung.

Beispiele zum Satz von Hensel

Die Aufgabenstellung lautet: Es sei $f(x) = 0$ eine Diophantische Gleichung (in einer Variablen). Finde **eine** Lösung von $f(x) = 0$ modulo p^n ausgehend von einer Lösung c modulo p^{n-1}, die die Extrabedingung p teilt nicht $f'(c)$ erfüllt.
Dies ist genau die Situation in der der Satz von Hensel angewendet werden kann.

(1) Wir betrachten die Diophantische Gleichung $f(x) = x^4 - 1 = 0$, $c = 2$ ist eine Lösung modulo 5. Dann gilt
   1. $f(2) \equiv 2^4 - 1 \equiv 15 \equiv 0 \pmod 5$,
   2. 5 teilt nicht $f'(2) = 4 \cdot 2^3 = 32$.

   Somit sind die Voraussetzungen für den Satz von Hensel erfüllt. Nach dem Satz von Hensel gibt es eine eindeutige Restklasse $[c_2]_{25}$ mit
   1. $f(c_2) \equiv c_2^4 - 1 \equiv 0 \pmod{25}$,
   2. $c_2 = c + k \cdot 5$ mit $\frac{f(c)}{5} + f'(c)k \equiv 0 \pmod 5$.

   Wir berechnen c_2, indem wir erst k berechnen:
$$\frac{f(2)}{5} + f'(2)k \equiv \frac{15}{5} + 32k \equiv 3 + 2k \equiv 0 \pmod 5.$$
   Dies ist äquivalent zu $2k \equiv 2 \pmod 5$. Multiplikation mit 3 gibt $k \equiv 1 \pmod 5$, also wählen wir als Representanten für diese Restklasse zum Beispiel $k = 1$. Dies gibt
$$c_2 = 2 + 1 \cdot 5 = 7.$$
   Also ist 7 eine Lösung von $x^4 - 1$ modulo 25.
   Haben wir uns auch nicht verrechnet?
$$7^4 - 1 \equiv (49)^2 - 1 \equiv (-1)^2 - 1 \equiv 0 \pmod{25}$$
   Somit ist 7 wirklich eine Lösung modulo 25.

(2) Nun wenden wir den Satz nochmal an: Für die Diophantische Gleichung $f(x) = x^4 - 1 = 0$ ist $c_2 = 7$ eine Lösung modulo 25, für die gilt, dass 5 nicht $f'(7) = 4 \cdot 7^3$ teilt. Wir kürzen die obige Auflistung wie folgt ab:
   Nach dem Satz von Hensel gibt es eine eindeutige Lösung c_3 von $x^4 - 1$ modulo 125, die den gleichen Rest wie $c_2 = 7$ modulo 25 läßt. Einen Repräsentanten finden wir, indem wir $k \in \mathbb{Z}$ finden mit
$$\begin{aligned}\frac{f(c_2)}{25} + kf'(c_2) &\equiv \frac{7^4 - 1}{25} + k(4 \cdot 7^3) \equiv \frac{(50-1)^2 - 1}{25} + k(4 \cdot 2^3) \\ &\equiv 2 \cdot (50 - 2) + 2k \equiv -4 + 2k \equiv 0 \pmod 5\end{aligned}$$
   Nun multiplizieren wir $2k \equiv 4 \pmod 5$ mit dem Inversen von 2 modulo 5, d.h. mit 3 und erhalten
$$k \equiv 2 \pmod 5.$$
   Wir wählen $k = 2$ und somit $c_3 = c_2 + kp^2 = 7 + 2 \cdot 25 = 57$.
   Also ist 57 nach dem Satz eine Lösung von $f(x)$ modulo 125.
   Stimmt das denn auch?
$$\begin{aligned}(57)^4 - 1 &\equiv ((50+7)^2)^2 - 1 \equiv (50^2 + 7 \cdot 100 + 49)^2 - 1 \\ &\equiv (7(-25) + 49)^2 - 1 \equiv (-50 + 49)^2 - 1 \equiv 0 \pmod{125}.\end{aligned}$$