

AUSGEWÄHLTE KAPITEL: ELEMENTARE ZAHLENTHEORIE BLATT 7

Aufgabe 1. (4) 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: Du benötigst voraussichtlich die folgende Faktorisierung

$$\frac{30^6 - 1}{49} = \left(\frac{30^3 - 1}{49} \right) (30^3 + 1) = 551 \cdot 27001.$$

Eine ähnliche Aufgabe ist auf der nächsten Seite zur Hilfestellung gelöst.

Aufgabe 2. (4) Finde alle Restklassen modulo 72, die die folgende Kongruenz lösen

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

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

Aufgabe 3. (4) Finde alle Restklassen modulo 125, die die folgende Kongruenz lösen

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

Aufgabe 4. (2 + 2) Es sei $f(x) = x^3 + x^2$.

(1) Zeige, dass (die Restklasse von) $c = 1$ eine Lösung der Kongruenz

$$f(c) \equiv 0 \pmod{2}$$

ist. Wende den Satz von Hensel an, um eine Lösung modulo 2^2 zu finden. Wende danach den Satz von Hensel auf die so erhaltene Lösung an, um eine Lösung modulo 2^3 zu erhalten. Wende den Satz nochmal an, um eine Lösung modulo 2^4 zu erhalten.

(2) Begründe: Für jede positive natürliche Zahl n gilt, dass (die Restklasse von) $c_n := \sum_{i=0}^{n-1} 2^i$ eine Lösung der Kongruenz

$$f(x) \equiv 0 \pmod{2^n}$$

ist.

Hinweis: Es gilt

$$1 + 2 + 2^2 + \dots + 2^{n-1} = \sum_{i=0}^{n-1} 2^i = 2^n - 1$$

für jede positive natürliche Zahl n . Dies kannst du ohne Begründung beim lösen der Aufgabe benutzen.

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:

$$0 \equiv \frac{f(2)}{5} + f'(2)k \equiv \frac{15}{5} + 32k \equiv 3 + 2k \pmod{5}.$$

Dies ist äquivalent zu $2k \equiv 2 \pmod{5}$. Multiplikation mit 3 gibt $k \equiv 1 \pmod{5}$, also wählen wir als Repräsentanten 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

$$\begin{aligned} 0 &\equiv \frac{f(c_2)}{25} + k f'(c_2) \\ &\equiv \frac{7^4 - 1}{25} + k(4 \cdot 7^3) \\ &\equiv \frac{(50 - 1)^2 - 1}{25} + k(4 \cdot 2^3) \\ &\equiv 2 \cdot (50 - 2) + 2k \\ &\equiv -4 + 2k \pmod{5} \end{aligned}$$

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?

$$\begin{aligned}(57)^4 - 1 &\equiv ((50 + 7)^2)^2 - 1 \equiv (50^2 + 7 \cdot 100 + 49)^2 - 1 \\ &\equiv (7(-25) + 49)^2 - 1 \equiv (-50 + 49)^2 - 1 \equiv 0 \pmod{125}.\end{aligned}$$

- (3) Wir können den Satz von Hensel nun auf $f(x) = x^4 - 1$ und die Lösung $c_3 = 57$ modulo 125 anwenden, denn 5 teilt nicht

$$f'(57) = 4 \cdot (57^3).$$

Dazu lösen wir wieder (diesmal mit Taschenrechner)

$$0 \equiv \frac{f(57)}{125} + kf'(57) \equiv 84448 + k4 \cdot 57^3 \equiv 3 + 2k \pmod{5}.$$

Somit können wir wieder $k = 1$ wählen und $c_4 = 57 + k \cdot 125 = 182$ ist die Lösung modulo 625, die uns der Satz von Hensel liefert.

Die Probe dazu (mit Taschenrechner):

$$(182)^4 - 1 = 625 \cdot 1755519$$

Also ist 182 eine Lösung modulo 625.