WiSe '21/'22, hhu
K. Halupczok

Vorlesung Einführung in die Zahlentheorie

EZ8: Polynomielle Kongruenzen (mit beliebigen Moduln)

Stichworte: Lösungszahl, Multiplikativität der Lösungszahl laut CRS, Satz von Lagrange, Satz von Wilson, Aufstiegsatz (Hensels Lemma)

8.1. Einleitung: Die Anzahl der Lösungen einer polynomiellen Gleichung $f(x)=0$, mit $f \in \mathbb{Z}[X]$, in $\mathbb{Z}/m$ ist multiplikativ im Modul m. Von den Lösungen modulo p ausgehend kann zu den Lösungen modulo $p^2, p^3, p^4, \dots$ aufgestiegen werden.
Ist die PFZ $m = p_1^{k_1} \cdots p_r^{k_r}$ bekannt, können mit den Lösungen modulo $p_1^{k_1}, p_2^{k_2}, \dots, p_r^{k_r}$ alle Lösungen modulo m "chinesisch" zusammengesetzt werden.

8.2. Def. (Lösungszahl einer polynomiellen Kongruenz): Sei $f \in \mathbb{Z}[X]$ und $m \in \mathbb{N}$.
Dann heißt $S(m) := S(m,f) := \#\{x \in \mathbb{N}_0;\ x<m \text{ und } f(x) \equiv 0 \ (m)\}$ die Lösungszahl der polynomiellen Kongruenz $f(x) \equiv 0 \ (m)$.
Diese kann auch als die Anzahl Lösungen der polynomiellen Gleichung $f(x)=0$ im Restklassenring $\mathbb{Z}/m$ verstanden werden.

Zu linearen Kongruenzen erhalten wir die folgende Aussage über S:

8.3. Satz (Lösungszahl linearer Kongruenzen): Sei $f = aX + b \in \mathbb{Z}[X]$, $a \neq 0$, sei $m \in \mathbb{N}$. Falls $(a,m) \mid b$ (d.h. falls $f(x) \equiv 0 \ (m)$ lösbar ist), so gilt $S(m) = (a,m)$. Für $(a,m) \nmid b$ hat $f(x) \equiv 0 \ (m)$ keine Lösungen.
Schreiben wir $L = \{x \bmod m;\ ax+b \equiv 0 \ (m)\}$ für die Lösungsmenge, so haben wir

$$L = \left\{x_0,\ x_0 + \tfrac{m}{d},\ x_0 + 2\tfrac{m}{d}, \dots,\ x_0 + (d-1)\tfrac{m}{d}\right\},$$

wenn $d := (a,m)$, $x_0 := -\frac{b}{d} a^* \left(\frac{m}{d}\right)$, und wenn a^* das Inverse von $\frac{a}{d}$ mod $\frac{m}{d}$ ist.

Bew.: Es handelt sich bei der Kongruenz $ax+b \equiv 0 \ (m)$ um die diophantische lineare Gleichung $ax + my = -b$, wobei nur die Reste mod m der ersten Komponente der Lösungspaare $(x,y) \in \mathbb{Z}^2$ gefragt sind.

Das Kriterium $(a,m) \mid b$ ist zur Lösbarkeit notwendig und hinreichend, wie schon in 3.13/3.14 gezeigt.

Falls $d := (a,m) \mid b$, erhalten wir alle Lösungen für x mod m so:

Haben $ax+b \equiv 0 \ (m) \iff \frac{a}{d} x + \frac{b}{d} \equiv 0 \ (\frac{m}{d})$ (⊛)

Mit $(\frac{a}{d}, \frac{m}{d}) = 1$ hat $\frac{a}{d}$ eine inverse Restklasse mod $\frac{m}{d}$ (explizit mit Bézout-Lemma),

somit ex. $a^* \in \mathbb{Z}$ mit $a^* \cdot \frac{a}{d} \equiv 1 \ (\frac{m}{d})$

so dass (⊛) $\iff x \equiv -\frac{b}{d} \cdot a^* \ (\frac{m}{d})$ folgt,

d.h. (⊛) hat genau eine Lösung $x_0 := -\frac{b}{d} \cdot a^*$ mod $\frac{m}{d}$.

Die d Zahlen $x_0, \ x_0 + \frac{m}{d}, \ \dots, \ x_0 + (d-1)\frac{m}{d}$ sind mod m verschieden.

Jedes x, das (⊛) erfüllt, ist mod m zu einer dieser Zahlen kongruent.

Die einzige Lösung x_0 mod $\frac{m}{d}$ induziert somit d Lösungen mod m. □

Bem.: Im Fall $(a,m) = 1$ ex. genau 1 Lösung $x_0 \equiv -b\bar{a}^{\varphi} \ (m)$.

Damit sind lineare Kongruenzen vollständig verstanden. Für höhere polynomielle Kongruenzen untersuchen wir zunächst die Abhängigkeit vom Modul.

Der CRS gibt uns eine Möglichkeit, die Lösungen polynomieller Kongruenzen zu verschiedenen Moduln "chinesisch" zusammenzusetzen.

8.4. Satz (S ist multiplikativ im Modul): Sind $m_1, m_2 \in \mathbb{N}$, $(m_1, m_2) = 1$, so folgt für alle $f \in \mathbb{Z}[X]$, dass $S(m_1 m_2) = S(m_1) S(m_2)$.

Bew.: Wir wenden den CRS aussagenlogisch an. Sei $k := S(m_1)$, $l := S(m_2)$ und seien $x_1, \dots, x_k$ Vertreter der Lösungsrestklassen mod m_1, und $y_1, \dots, y_l$ Vertreter der Lösungsrestklassen mod m_2.

Wegen $(m_1, m_2) = 1$ ist $f(x) \equiv 0 \ (m_1 m_2)$ für alle $x \in \mathbb{Z}$ äquivalent zu

$$f(x) \equiv 0 \ (m_1) \ \wedge \ f(x) \equiv 0 \ (m_2)$$

$$\Leftrightarrow \ \big(x \equiv x_1 (m_1) \vee \dots \vee x \equiv x_k (m_1)\big) \wedge \big(x \equiv y_1 (m_2) \vee \dots \vee x \equiv y_l (m_2)\big)$$

$$\Leftrightarrow \ \bigvee_{j=1}^{k} \bigvee_{h=1}^{l} \big(x \equiv x_j (m_1) \wedge x \equiv y_h (m_2)\big)$$

$$\overset{\text{CRS, da } (m_1, m_2) = 1}{\Leftrightarrow} \ x \equiv x_{j,h} \ (m_1 m_2) \quad \text{für ein } x_{j,h} \in \mathbb{Z}.$$

Verschiedenen Paaren (x_j, y_h) entsprechen dabei laut CRS verschiedenen $x_{j,h}$ modulo $m_1 \cdot m_2$. Damit hat die zuletzt genannte Disjunktion von $k \cdot l$ vielen Zweier-Kongruenzsystemen genau $kl = S(m_1) S(m_2)$ viele Lösungen, und damit auch die polynomielle Kongruenz zu Beginn. □

8.5. Bsp.: Wir zeigen, wie die Lösungen einer quadratischen Kongruenz laut Beweis von 8.4 explizit "chinesisch" zusammengesetzt werden können:

Bsp. $x^2 \equiv 4 \ (15)$. Dann ist $x \equiv \pm 2 \ (3)$ und $x \equiv \pm 2 \ (5)$. 13

Die Systeme $\{x \equiv 2 (3), x \equiv 2 (5)\}$ bzw. $\{x \equiv -2 (3), x \equiv -2 (5)\}$ führen direkt auf $x \equiv 2 (15)$ bzw. $x \equiv -2 \overset{=}{=} 13 (15)$.

Haben darüberhinaus $\{x \equiv 2 (3), x \equiv -2 (5)\} \Leftrightarrow x \equiv 8 \ (15)$ und $\{x \equiv -2 (3), x \equiv 2 (5)\} \Leftrightarrow x \equiv 7 \ (15)$, also 4 Lösungen.

Dass die Kongruenz mod den Primzahlen $p = 3$ und $p = 5$ hier jeweils 2 Lösungen besitzt und nicht mehr, folgt einem allgemeinen Prinzip, das in 8.6 formuliert ist. Die Lösungszahl einer Kongruenz $f(x) \equiv 0 \ (p)$ kann aber auch stark schwanken.

8.6. Bsp.: • Für $f(x) \equiv x^3 + 2x - 7 \equiv 0 \ (p)$ findet man $S(2) = 1$, $S(3) = 0$, $S(5) = 2$, $S(7) = 1$.

• Die Kongruenz $x^p - x \equiv 0 \ (p)$ hat nach dem Kleinen Satz von Fermat genau p Lösungen (mod p).

8.6. **Satz (von Lagrange, über polynomielle Kongruenzen mod $p \in \mathbb{P}$):**
Sei $f \in \mathbb{Z}[X]$, $\deg(f) = n$, $p \in \mathbb{P}$, und p kein Teiler des Leitkoeffizienten von f.
Dann ist $S(p,f) \leq n = \deg(f)$, d.h. die Lösungszahl von $f(x) \equiv 0 \ (p)$ ist höchstens so groß wie der Grad von f.

Bem.: Die Aussage ist klar, wenn man bedenkt, dass "$\equiv \bmod p$ in $\mathbb{Z}$" dasselbe bedeutet wie "$=$ im Körper $\mathbb{Z}/p$". Die Bedingung an den Leitkoeffizienten besagt, dass f als Polynom über $\mathbb{Z}/p$ den Grad n hat. Nach dem allgemeineren Satz der Algebra über Nullstellen eines Polynoms über einem Körper hat f über $\mathbb{Z}/p$ höchstens n Nullstellen.

Bew.: Wir geben im Prinzip den Beweis des allgemeineren Satzes, schreiben ihn aber um für $\mathbb{Z}/p$.

- Sei ein vollständiges Restsystem R mod p gegeben, und betrachte o.E. den Fall, dass überhaupt Lösungen existieren, d.h. ex. $x_1 \in R$ mit $f(x_1) \equiv 0 \ (p)$. Polynomdivision ergibt $f(X) = (X - x_1) g(X) + b_1$ mit einem Polynom g, $\deg(g) \leq n-1$, dessen Leitkoeff. $\not\equiv 0 \ (p)$ ist. Und $X = x_1$ zeigt $b_1 \equiv 0 \ (p)$.
Für alle $x \in R \setminus \{x_1\}$ mit $f(x) \equiv 0 \ (p)$ ist nun $(x - x_1) \cdot g(x) = f(x) \equiv 0 \ (p)$. Da $x - x_1 \not\equiv 0 \ (p)$ folgt also $g(x) \equiv 0 \ (p)$ für alle $x \in R \setminus \{x_1\}$ mit $f(x) \equiv 0 \ (p)$. Die Beh. ergibt sich nun induktiv.
- Für $n = 0$ gibt es wegen $a_0 \not\equiv 0 \ (p)$ keine Lösung (a_0 das Absolutglied).
- Für $n = 1$ werden Lösungen von $a_1 x + a_0 \equiv 0 \ (p)$ gesucht, was wegen $p \nmid a_1$ genau 1 Lösung hat laut 8.3. □

Eine Anwendung, die für praktische Primzahltests aber leider ungeeignet ist, ist 8.7.

8.7. **Satz (von Wilson):** Für alle $n \in \mathbb{N}$, $n > 1$, gilt: n ist Primzahl $\Leftrightarrow (n-1)! \equiv -1 \ (n)$.

Bew.: "$\Leftarrow$": Sei $n \in \mathbb{N}$ zus.gesetzt. Dann ex. $q \in \mathbb{P}$, $q \mid n$, $q < n$.
Also teilt q die Zahlen n und $(n-1)! = 1 \cdot 2 \cdot \ldots \cdot (n-1)$.
Die Kongruenz der r.S. kann wegen $q \nmid -1$ deshalb nicht bestehen.

"$\Rightarrow$": Es ist $(2-1)! = 1! = 1 \equiv -1 \ (2)$. Sei nun $p > 2$ eine ungerade Primzahl.
Die Kongruenz $-(x^{p-1} - 1) + \prod_{j=1}^{p-1} (x - j) = (x-1) \cdot (x-2) \cdot \ldots \cdot (x-(p-1)) - (x^{p-1} - 1) \equiv 0 \ (p)$
wird nach dem Kleinen Satz von Fermat von den $p-1$ vielen Zahlen $x = 1, 2, \ldots, p-1$ gelöst.
Die l.S., als Polynom geschrieben, hat einen Grad von höchstens $p-2$.
Ist eines der Koeffizienten davon $\not\equiv 0 \ (p)$, ergibt sich deshalb ein Widerspruch zum Satz von Lagrange 8.6. Insbesondere folgt durch Betrachtung des Absolutglieds
$1 + \prod_{j=1}^{p-1} (-j) \equiv 0 \ (p)$, also $1 + (p-1)! \equiv 0 \ (p)$. □

Laut Satz 8.4, der auf dem CRS beruht, können polynomielle Kongruenzen auf den speziellen Fall $f(x) \equiv 0 \ (p^k)$ mit $p \in \mathbb{P}$, $k \in \mathbb{N}$, zurückgeführt werden. Denn die Lösungen zu einem Modul $m = p_1^{k_1} \cdot \ldots \cdot p_r^{k_r}$ können aus denen modulo $p_1^{k_1}, \ldots, p_r^{k_r}$ dann zu denen modulo m "chinesisch" zusammengesetzt werden. Im Weiteren wird gezeigt, dass es im Prinzip sogar ausreicht, nur Primzahlmoduln statt Primpotenzmoduln zu betrachten, indem man zu höheren Potenzen "aufsteigen" kann. Befriedigende Aussagen, was Lösbarkeit, Lösungsanzahl und die Gestalt der Lösungen angeht, sind jedoch nur im Fall linearer oder quadratischer Kongruenzen möglich. Die quadratischen Kongruenzen behandeln wir einleitend ab Kapitel EZ 10.

Der folgende Satz zeigt, wie von den Lösungen mod p^k zu denen mod p^{k+1} aufgestiegen werden kann. Es ist klar, dass aus $f(x) \equiv 0 \ (p^{k+1})$ die schwächere Bedingung $f(x) \equiv 0 \ (p^k)$ folgt. Eine Restklasse $x_0 + p^k\mathbb{Z}$ modulo p^k zerfällt in p viele Restklassen modulo p^{k+1}, nämlich $(x_0 + b p^k) + p^{k+1}\mathbb{Z}$ mit $b \in \mathbb{N}_0$, $b < p$. Ist also $x_0 + p^k\mathbb{Z}$ eine Lösungsrestklasse mod p^k, so prüft man, welche der Restklassen $(x_0 + b p^k) + p^{k+1}\mathbb{Z}$ Lösungen modulo p^{k+1} sind, und kann so von allen Lösungen mod p^k auf die mod p^{k+1} schließen.

8.8. **Aufstiegssatz / Hensel's Lemma (elementare Version für Kongruenzen):**
Sei $f \in \mathbb{Z}[X]$, $k \in \mathbb{N}$, $p \in \mathbb{P}$, $x_0 \in \mathbb{Z}$ mit $f(x_0) \equiv 0 \ (p^k)$.
Sei $g := g(x_0, k) := \#\{ b \in \mathbb{N}_0 ; \ b < p, \ f(x_0 + b p^k) \equiv 0 \ (p^{k+1}) \}$,
d.h. g ist die Anzahl der Lösungen mod p^{k+1}, die aus x_0 entstehen.
Sei f' die formale Ableitung von f.
Dann gilt
(1) $g = 1$, falls $f'(x_0) \not\equiv 0 \ (p)$
(2) $g = p$, falls $f'(x_0) \equiv 0 \ (p)$ und $f(x_0) \equiv 0 \ (p^{k+1})$,
(3) $g = 0$, falls $f'(x_0) \equiv 0 \ (p)$ und $f(x_0) \not\equiv 0 \ (p^{k+1})$.

Bew.: • Die Taylor-Entwicklung von f um x_0 zeigt die Existenz eines $c \in \mathbb{Z}$, so dass für alle $b \in \mathbb{N}_0$, $b < p$ gilt: $f(x_0 + b p^k) = f(x_0) + b p^k \cdot f'(x_0) + c p^{k+1}$,
d.h. $f(x_0 + b p^k) \equiv f(x_0) + b p^k f'(x_0) \ (p^{k+1})$.

Hierbei wurde benutzt, dass die Faktoren $\frac{f^{(\nu)}(x_0)}{\nu!}$ im Taylorschen Satz für alle $\nu \in \mathbb{N}_0$ ganzzahlig sind. Somit ist $x_0 + b p^k$ genau dann eine Lösung modulo p^{k+1}, wenn $0 \equiv f(x_0) + b p^k f'(x_0) \quad (p^{k+1})$,

d.h. $\circledast$ $f(x_0) p^{-k} + b f'(x_0) \equiv 0 \quad (p)$ ist.

1. Fall: $f'(x_0) \not\equiv 0 \ (p)$. Dann ist $(p, f'(x_0)) = 1$, so dass aus Satz 8.3 genau ein $b \in \mathbb{N}_0$, $b < p$ existiert mit $\circledast$, nämlich $b \equiv -f(x_0) p^{-k} \cdot (f'(x_0))^{-1} \ (p)$. ($(f'(x_0))^{-1}$: Inverses von $f'(x_0)$ mod p)

Damit folgt (1).

2. Fall: $f'(x_0) \equiv 0 \ (p)$ und $f(x_0) \equiv 0 \ (p^{k+1})$.

Dann wird $\circledast$ von allen $b \in \mathbb{N}_0$, $b < p$, erfüllt, es ergibt sich (2).

3. Fall: $f'(x_0) \equiv 0 \ (p)$ und $f(x_0) \not\equiv 0 \ (p^{k+1})$.

Dann gilt zwar $p \mid f'(x_0)$, aber wegen $p \nmid f(x_0) p^{-k}$ wird $\circledast$ von keinem $b \in \mathbb{Z}$ gelöst. Dann gilt (3). □

8.9. Bsp.: Sei $p := 3$, $f(x) := x^4 + 7x + 4$. Durch Einsetzen sieht man

$f(0) = 4 \not\equiv 0 \ (3)$, $f(1) = 1 + 7 + 4 = 12 \equiv 0 \ (3)$

und $f(2) = 16 + 14 + 4 = 34 \not\equiv 1 \ (3)$.

Sei also $x_0 := 1$. Wegen $f'(x_0) = 4 \cdot 1^3 + 7 = 11 \equiv 2 \ (3)$ tritt der 1. Fall ein.

$\circledast$ wird zu $\frac{12}{3} + 11 b \equiv 0 \ (3) \iff 4 + 2b \equiv 0 \ (3) \iff b \equiv 1 \ (3)$.

4 (3²) / 0 (3)

Somit ist $x_0 + 1 \cdot 3 = 4$ die einzige Lösung modulo 9.

8.10. Bsp.: Sei $p := 5$, $f(x) := x^3 - 2x + 1$. Haben $x_0 := 1$, $x_1 := 2$ als einzige Lösungen von $f(x) \equiv 0 \ (p)$.

Wegen $f'(2) = 3 \cdot 2^2 - 2 \equiv 0 \ (5)$ und $f(2) = 2^3 - 2 \cdot 2 + 1 = 5 \not\equiv 0 \ (5^2)$

erzeugt x_1 keine Lösung mod $5^2 = 25$. Da $f'(1) = 1^3 - 2 = -1 \not\equiv 0 \ (5)$,

ist $0 \cdot 5^{-1} - 1 \cdot b \equiv 0 \ (5)$ zu lösen. Es folgt $b = 0$, was die einzige Lösung

$y_0 + b \cdot 5 \equiv 1 \ (25)$ erzeugt.

1 (5²) / ⋮ / 1 (5)

8.11. Bsp.: Sei $p := 7$, $f(x) := x^2 - 2$. Haben: $x_0 := 3$, $x_1 := 4$ als Lösungen von $x^2 \equiv 2 \ (7)$.

Wegen $f'(x) = 2x \not\equiv 0 \ (7)$ liegt der 1. Fall vor, man steigt zu genau einer Lösung auf

mod 7^2, 7^3, ... Z.B. mod 7^2 erzeugt $x_0 = 3$ die Lösung $x_0 + b \cdot p = 3 + b \cdot 7$

mit $b \equiv -\frac{f(x_0)}{p} \cdot (f'(x_0))^{-1} = -\frac{7}{7} \cdot (-1)^{-1} = 1$, also $3 + 7 = 10 \bmod 7^2$

! / ⋮ / ⋮ (7²)

39 / 10

4 / 3 (7)