Vorlesung Einführung in die Zahlentheorie

EZ 9: Primitivwurzeln

Stichworte: Primitivwurzel, Satz von Euler über PWn, Konstruktion und Anzahl von PWn, binomische Kongruenzen, diskreter Logarithmus bzw. Index

---

9.1. Einleitung:

Wir nennen einen Erzeuger der multiplikativen Restklassengruppe $(\mathbb{Z}/m)^*$ eine Primitivwurzel. Nach dem Satz von Euler über Primitivwurzeln gibt es diese genau dann, wenn $m \in \{1, 2, 4\}$ oder $m = p^k$ oder $m = p^{2k}$ für ein $p \in \mathbb{P}, p \neq 2$, und $k \in \mathbb{N}$ ist.
Dieser Satz erfordert zum Beweis einen gewissen Tiefgang.

9.2. Def.: Für $m \in \mathbb{N}$ heißt ein $a \in \mathbb{Z}$ mit $(a, m) = 1$ eine Primitivwurzel modulo m (Kurz: PW mod m), falls $\{a^l;\ 1 \leq l \leq \varphi(m)\}$ ein reduziertes RS mod m bildet,
d.h. falls $\operatorname{ord}_m(a) = \varphi(m)$ ist,
bzw. falls $\underline{a}$ ein erzeugendes Element der Gruppe $(\mathbb{Z}/m)^*$ ist,
d.h. $\{\underline{a}^l;\ 1 \leq l \leq \varphi(m)\} = (\mathbb{Z}/m)^*$.

Eine PW bzw. erzeugendes El. einer Gruppe heißt auch einfach Erzeuger.

9.3. Bsp.: • $a = 2$ ist PW mod 5, da $\{\underline{2}, \underline{2}^2, \underline{2}^3, \underline{2}^4\} = \{\underline{2}, \underline{4}, \underline{3}, \underline{1}\} = (\mathbb{Z}/5)^*$.
• Mod 12 ex. keine PW, da $\varphi(12) = \varphi(3)\varphi(2^2) = 2 \cdot (2^2 - 2) = 4$, $\underline{1}^2 = (\underline{-1})^2 = \underline{1}$, $\underline{5}^2 = (\underline{-5})^2 = \underline{1}$.

Ziel des Kapitels ist der Beweis des folgenden Satzes.

9.4. Satz von Euler über Primitivwurzeln: Für $m \in \mathbb{N}$ existiert genau dann eine PW mod m, wenn $m \in \{1, 2, 4\} \cup \{p^k;\ p \in \mathbb{P} \setminus \{2\}, k \in \mathbb{N}\} \cup \{2p^k;\ p \in \mathbb{P} \setminus \{2\}, k \in \mathbb{N}\}$.

Bem.: Der Fall $m = p$ wurde von Gauß bewiesen; gelegentlich wird 9.4. auch "Satz von Gauß" genannt.

Bew.: 1. Schritt: PWn für $m = p \in \mathbb{P} \setminus \{2\}$.

1.) Seien $d_1, \dots, d_k$ alle modulo p auftretenden Ordnungen und $d = [d_1, \dots, d_k]$.
Es wird sich herausstellen, dass $d = \varphi(p) = p - 1$ ist und selbst als Ordnung angenommen wird, was der Behauptung entspricht.

2.) Da alle d_j Teiler von $\varphi(p) = p - 1$ sind (ganz 7.15(4)), gilt $d \mid (p-1)$, insb. $d \leq p - 1$.

3.) Für jedes $a \in (\mathbb{Z}/p)^*$ ist $a^d \equiv 1 \ (p)$, da $\operatorname{ord}_p(a)$ die Zahl d teilt.
Die Kongruenz $x^d - 1 \equiv 0 \ (p)$ hat $p-1$ Lösungen mod p,
nämlich alle $x \in \mathbb{Z}$ mit $p \nmid x$.
Nach dem Satz von Lagrange 8.6 muss $d \geq p-1$ sein.
Mit 2.) folgt $d = p-1$. Wegen $p > 2$ ist damit auch $d > 1$.

4.) Sei $d = p_1^{b_1} \cdots p_\ell^{b_\ell}$ die PFZ von d.
Sind $d_j = p_1^{b_{1,j}} \cdots p_\ell^{b_{\ell,j}}$ für alle $1 \leq j \leq k$ die PFZen der auftretenden Ordnungen (einige Exponenten können 0 sein), so gilt $b_h = \max\{b_{h,j};\ 1 \leq j \leq k\}$ für $1 \leq h \leq \ell$ nach Kor. 2.22.
Also gibt es ein $c_1 \in \mathbb{Z}$ und ein $d_1' \in \mathbb{N}$ mit $(c_1, p) = 1$ und
$\operatorname{ord}_p(c_1) = p_1^{b_1} \cdot d_1'$, und $p_1 \nmid d_1'$.
[Man nehme z.B. ein $c_1 \in \mathbb{Z}$, $(c_1, p) = 1$, mit $\operatorname{ord}_p(c_1) = d_\mu$,
wobei $\mu \leq k$ so gewählt ist, dass $p_1^{b_1}$ ein Teiler von d_μ ist.]
Nach Lemma 7.15(5) existiert ein a_1 $(= c_1^{d_1'})$ mit $\operatorname{ord}_p(a_1) = p_1^{b_1}$.
Analog erhält man $a_2, \ldots, a_\ell$.
Da die $p_j^{b_j}$ mit $j \leq \ell$ paarweise teilerfremd sind,
ergibt Lemma 7.15(6), dass $\operatorname{ord}_p(a_1 \cdots a_\ell) = p_1^{b_1} \cdots p_\ell^{b_\ell} = d$.
Mit 3.) hat man $\operatorname{ord}_p(a_1 \cdots a_\ell) = p-1$, die Beh.

2. Schritt: PWn für $n = p^k$ bzw. $2p^k$, $p \neq 2$ prim und $k \in \mathbb{N}$.

1.) Es sei g eine PW mod p $(\neq 2)$ laut 1. Schritt.
Es werden die Zahlen $c_\ell := (g + p\ell)^{p-1}$ mit $\ell \in \mathbb{N}_0$, $\ell \leq p-1$, betrachtet.
Es gibt ein $b_0 \in \mathbb{Z}$ mit $c_0 = g^{p-1} = 1 + pb_0$.
Für alle $\ell \leq p-1$ gibt es ein $y_\ell \in \mathbb{Z}$ mit
$$c_\ell = (g+p\ell)^{p-1} = g^{p-1} + (p-1)g^{p-2}p\ell + p^2 y_\ell$$
$$= 1 + p \cdot (b_0 - \ell g^{p-2} + p \cdot (y_\ell + g^{p-2}\ell))$$
$$= 1 + pb_\ell$$
mit $b_\ell := b_0 - \ell g^{p-2} + p \cdot (y_\ell + g^{p-2}\ell)$ für alle $\ell \leq p-1$.
Wegen $(g, p) = 1$ durchlaufen mit ℓ auch die b_ℓ ein volles RS mod p.
Insbesondere gibt es ein $\nu \in \{0, \ldots, p-1\}$ mit $p \nmid b_\nu$, welches im folgenden benutzt wird.

2.) Sei $k \in \mathbb{N}$ und $d := \operatorname{ord}_{p^k}(g+pv)$. Dann gilt $(g+pv)^d \equiv 1 \ (p)$, deshalb ist $p-1$ Teiler von d, da mit g auch $g+pv$ eine PW mod p ist.

3.) Nach Lemma 7.15(3) gilt $d \mid \varphi(p^k) = p^{k-1}(p-1)$, also gibt es wegen 2.) ein $n \leq k$ mit $d = p^{n-1}(p-1)$.

4.) Aus $(g+pv)^{p-1} = 1 + b_v p$ folgt schrittweise die Existenz von zu p teilerfremden $b_{v,j} \in \mathbb{Z}$ mit $j \in \mathbb{N}$ so, dass

$$(g+pv)^{p^1(p-1)} = 1 + p^2 \cdot b_{v,1},$$
$$(g+pv)^{p^2(p-1)} = 1 + p^3 \cdot b_{v,2}, \ \ldots$$

gelten, indem die vorangehende Gleichung mit p potenziert wird.

Denn wegen $p>2$ gilt für alle $j \in \mathbb{N}$, dass

$$(1 + p^{j+1} b_{v,j})^p = \sum_{k=0}^{p} \binom{p}{k} \cdot (p^{j+1} \cdot b_{v,j})^k = 1 + p^{j+2} \cdot (b_{v,j} + p y_{v,j})$$

$p \neq 2$, s. Bem. zu 4.) $\rightarrow$ für ein $y_{v,j} \in \mathbb{Z}$ ist. Mit $b_{v,0} := b_v$ setzt man für alle $j \in \mathbb{N}_0$, also $b_{v,j+1} := b_{v,j} + p \cdot y_{v,j}$, was für $(b_{v,j}, p) = 1$ auch wieder teilerfremd zu p ist. ⌟

Aus der Kongruenz $(g+pv)^d = (g+pv)^{p^{n-1}(p-1)} \equiv 1 \ (p^k)$ wird daher $1 + p^n b_{v,n-1} \equiv 1 \ (p^k)$.

Wegen 3.) ist also $n = k$ und $g+pv$ eine PW mod p^k.

Bem.: Man beachte, dass $p \neq 2$ bei "$y_{v,j} \in \mathbb{Z}$" verwendet wird:

Für $p=2$ ist $(1 + b_{v,j} \cdot 2^{j+1})^2 = 1 + 2 \cdot 2^{j+1} b_{v,j} + (2^{j+1} b_{v,j})^2 = 1 + 2^{j+2} \cdot (b_{v,j} + b_{v,j}^2 \cdot 2^j)$

mit geradem $b_{v,j} + b_{v,j}^2$ für $j=0$ und ungeradem $b_{v,j} \in \mathbb{Z}$. (gerade für $j=0$)

(Dieser problematische Fall tritt auf, wenn im letzten Summanden $\binom{p}{p} \cdot b_{v,j}^p \cdot p^{p(j+1)}$ der Exponent $p(j+1)$ mit $j+2$ übereinstimmt.

Haben $p(j+1) = j+2 \iff j(p-1) = p-2 \iff j = -\frac{p-2}{p-1}$, was nur für $j=0$, $p=2$ möglich ist.)

5.) Ist h PW mod p^k, so ist die ungerade unter den Zahlen h und $h+p^k$ eine PW mod $2p^k$.

Denn nach Satz 7.13(2) ist $\varphi(2p^k) = \varphi(p^k)$. Falls ein ungerades $x \in \mathbb{Z}$ die Kongruenz $x^j \equiv 1 \ (p^k)$ mit $j \in \mathbb{N}$ erfüllt, dann auch mod $2p^k$ und umgekehrt. Für ungerade x ist also $\operatorname{ord}_{p^k}(x) = \operatorname{ord}_{2p^k}(x)$. ⌟

3. Schritt: $m = 2^k$ besitzt PWn nur für $k=1$ und $k=2$.

Klar: • 1 ist PW mod 2, da $1 \equiv 1\ (2)$ ist. • 3 ist PW mod 4, da $3 \equiv 3\ (4)$, $3^2 \equiv 1\ (4)$ ist.

Es ist $\varphi(2^k) = 2^{k-1}$ nach Satz 7.13(3).

Ein ungerades $a \in \mathbb{Z}$ hat jedoch mod 2^k höchstens die Ordnung 2^{k-2}, falls $k \geq 3$ ist.

⌜Denn man sieht induktiv die Existenz von $a_j \in \mathbb{Z}$ für alle $j \in \mathbb{N}$ mit

$$a^{2^1} = 1 + 8a_1,\quad a^{2^2} = 1 + 16 a_2, \dots, a^{2^{j-2}} = 1 + 2^j a_{j-2} \equiv 1\ (2^j).$$

Zu a_1: Es gibt ein $b \in \mathbb{Z}$ mit $a = 2b+1$. Dann ist $a^2 = 4b^2 + 4b + 1 = 4(b^2+b)+1$, und z^2+z ist für alle $z \in \mathbb{Z}$ gerade.⌟

Bem.: Für $k \geq 3$ bilden die 2^{k-1} Zahlen $\pm 5^0, \pm 5^1, \dots, \pm 5^{2^{k-2}-1}$ ein reduziertes RS mod 2^k.

⌜Man benutzt dabei $5^{2^{j-3}} \equiv 1 + 2^{j-1}\ (2^j)$ für alle $j \in \mathbb{N}$, $j \geq 3$, was $\operatorname{ord}_{2^k}(5) = 2^{k-2}$ zeigt

⌜⌜VI: $j=3$: $5 \equiv 1+4\ (2^3)$ ✓, $j \to j+1$: $5^{2^{j-2}} = (5^{2^{j-3}})^2 \overset{\text{Vor.}}{\equiv} (1+2^{j-1})^2 = 1 + 2^j + 2^{2j-2} \equiv 1 + 2^j\ (2^{j+1})$, ⌞ $2j-2 \geq j+1$

Die Zahlen mit "+" sind $\equiv 1\ (4)$, die mit "−" sind $\equiv -1\ (4)$, also sind alle p.W. inkongruent mod 2^k.⌟⌟

4. Schritt: Ausschließen der weiteren $m \in \mathbb{N}$.

Sei $1 < m = q_1^{\alpha_1} \cdots q_\mu^{\alpha_\mu}$ die PFZ und $c \in \mathbb{Z}$, $(c, m) = 1$.

Für jedes $j \leq \mu$ gilt $c^{\varphi(q_j^{\alpha_j})} \equiv 1\ (q_j^{\alpha_j})$ laut Eulerscher Kongruenz.

Ist $f := [\varphi(q_1^{\alpha_1}), \dots, \varphi(q_\mu^{\alpha_\mu})]$, so folgt $c^f \equiv 1\ (q_j^{\alpha_j})$ für alle $j \leq \mu$,

also ist $c^f \equiv 1\ (m)$, vgl. 6.3(6). Wegen $f \mid \varphi(m)$ ex. PWn mod m also nur,

wenn $\varphi(q_1^{\alpha_1}) \cdots \varphi(q_\mu^{\alpha_\mu}) = \varphi(m) = f = [\varphi(q_1^{\alpha_1}), \dots, \varphi(q_\mu^{\alpha_\mu})]$ ist.

Falls m mindestens zwei ungerade Primteiler besitzt,

ist $f \leq \frac{\varphi(m)}{2}$. Im Fall $m = 2^{\alpha_1} \cdot q_2^{\alpha_2}$ mit $\alpha_1 \geq 2$ und $q_2 > 2$ gilt dies ebenfalls.

Also bleiben wegen dem 3. Schritt nur die im Satz genannten m.

□

9.5. **Bem.:** • Die Konstruktion von PWn mod $p \in \mathbb{P}$ erfolgt wie im 1. Schritt 4) angegeben, sofern die PFZ von $\varphi(p) = p-1$ vorliegt.

• Hat man eine PW mod $p \in \mathbb{P}$ gefunden, kann man wie im 2. Schritt beschrieben zu PWn mod p^k und mod $2p^k$, $k \in \mathbb{N}$, aufsteigen. Genaueres sagt Satz 9.9.

• Eine bislang unbewiesene Vermutung von Artin besagt, dass 2 für unendlich viele $p \in \mathbb{P}$ eine PW mod p ist.

Falls zu $m \in \mathbb{N}$ eine PW $g \in \mathbb{Z}$ ex., bilden die Zahlen g^j mit $j \leq \varphi(m)$ ein reduziertes RS mod m. Weitere PWn sind dann auch Potenzen von g:

9.6 Satz: Sei $m \in \mathbb{N}$, $g \in \mathbb{Z}$ eine PW mod m. Dann gilt: g^ℓ PW mod $m \iff (\ell, \varphi(m)) = 1$.

Bew.: Da $(g,m)=1$, gilt $\operatorname{ord}_m(g^\ell) = \frac{\operatorname{ord}_m(g)}{(\operatorname{ord}_m(g),\ell)} = \frac{\varphi(m)}{(\varphi(m),\ell)}$ nach Lemma 7.16, also folgt: g^ℓ PW mod $m \iff \varphi(m) = \operatorname{ord}_m(g^\ell) \iff (\varphi(m),\ell) = 1$. □

9.7 Kor.: Somit gibt es zu den in Satz 9.4 (von Euler über PWn) genannten Moduln m genau $\varphi(\varphi(m))$ verschiedene PWn mod m.

9.8 Bem.:
- Die Struktur der abelschen Gruppe $((\mathbb{Z}/m)^*, \cdot)$ kann vollständig beschrieben werden.
- Ist $1 < m = q_1^{\alpha_1} \cdots q_n^{\alpha_n}$ die PFZ von m, dann zeigt der CRS, dass
$$(\mathbb{Z}/m)^* \cong (\mathbb{Z}/q_1^{\alpha_1})^* \times \ldots \times (\mathbb{Z}/q_n^{\alpha_n})^*.$$
- Für $q_j > 2$ ist $((\mathbb{Z}/q_j^{\alpha_j})^*, \cdot)$ isomorph zur zyklischen Gruppe $(\mathbb{Z}/\varphi(q_j^{\alpha_j}), +)$.
- Für $q=2$ und $k \geq 3$ ist nach der Bem. im 3. Schritt des Beweises von 9.4 hingegen $(\mathbb{Z}/2^k)^* \cong \underbrace{\mathbb{Z}/2}_{\text{bzgl. } \cdot} \times \underbrace{\mathbb{Z}/2^{k-2}}_{\text{bzgl. } +}$.

9.9 Satz (Auffinden von PWn mod p^k): Sei $p \in \mathbb{P} \setminus \{2\}$, g_0 eine PW mod p und $k \in \mathbb{N}$. Dann gilt:
Ist $g_0^{p-1} \not\equiv 1 \ (p^2)$, so ist $g = g_0$ eine PW mod p^k,
ist $g_0^{p-1} \equiv 1 \ (p^2)$, so ist $g = g_0 + p$ eine PW mod p^k.

Bew.: 1.) Ist $g^{p-1} \not\equiv 1 \ (p^2)$, so ist auch g eine PW mod p^k:
Laut kleinem Fermat ist $g^{p-1} = 1 + cp$, wo $p \nmid c$ nach Vor.
Für $a := g \bmod p^2$ gilt dann $\operatorname{ord}_{p^2}(a^{p-1}) = p^{k-1}$ (da $p \neq 2$, vgl. 2. Schritt 4.) in 9.4).
Sei $\ell := \operatorname{ord}_{p^2}(a)$. Dann ist $g^\ell \equiv 1 \ (p^2)$, also $g^\ell \equiv 1 \ (p)$, so dass $p-1 = \varphi(p)/\ell$.
Damit ist $p^{k-1} = \operatorname{ord}_{p^2}(a^{p-1}) \overset{7.16}{=} \frac{\ell}{(\ell, p-1)} = \frac{\ell}{p-1}$, also $\ell = (p-1)p^{k-1} = \varphi(p^k)$, es folgt die Beh.
2.) Sei g_0 eine beliebige PW mod p. Ist $g_0^{p-1} \not\equiv 1 \ (p^2)$, so fertig nach 1.)
Sei also $g_0^{p-1} \equiv 1 \ (p^2)$, betrachte $g := g_0 + p$. Es ist $g^{p-1} = (g_0+p)^{p-1} \equiv g_0^{p-1} + (p-1)g_0^{p-2}p \ (p^2)$,
also $g^{p-1} \equiv 1 - g_0^{p-2}p \ (p^2)$, und $g^{p-1} \not\equiv 1 \ (p^2)$, nach 1.) ist also g PW mod p^k.

□

9.10. Anwendung: Binomische Kongruenzen: Für $p>2$ prim können Kongruenzen der Form

$$\circledast \quad x^k \equiv a \ (p)$$ behandelt werden.

Falls $a \equiv 0 \ (p)$, ist die einzige Lösung $x \equiv 0 \ (p)$. Andernfalls erhalten wir folgendes Ergebnis.

9.11. Satz: Sei $p>2$ prim, $p \nmid a$, $k \in \mathbb{N}$. Dann hat die Kongruenz $x^k \equiv a \ (p)$ entweder keine oder $(k, p-1)$ viele Lösungen mod p, und die Anzahl der reduzierten a mod p, für die die Kongruenz lösbar ist, ist $\frac{p-1}{(k,p-1)}$.

Bew.: Sei $a \not\equiv 0 \ (p)$. Dann sei g eine PW mod p (laut Satz 9.4 von Euler/Gauß).

Demnach ex. ein $c \in \mathbb{N}$ mit $g^c \equiv a \ (p)$.

Für eine Lösung x muss $p \nmid x$ sein, definiere y durch $g^y \equiv x \ (p)$.

Die Kongruenz $\circledast$ lautet dann $g^{ky} \equiv g^c \ (p)$,

es folgt $ky \equiv c \ (p-1)$.

Damit wurde die polynomielle Kongruenz $\circledast$ auf eine lineare zurückgeführt, welche genau für $(k, p-1) \mid c$ lösbar ist. In diesem Fall liegt y in einer Restklasse mod $\frac{p-1}{(k,p-1)}$, also gibt es $(k, p-1)$ viele Lösungsrestklassen mod $p-1$. □

Der Satz 9.11 motiviert die Definition des diskreten Logarithmus.

9.12. Def.: Sei $m \in \mathbb{N}$ und $a \in \mathbb{Z}$, $(a,m)=1$, sei g eine PW mod m (also m laut Satz 9.4). Die eindeutig bestimmte Restklasse ℓ mod $\varphi(m)$ so, dass $g^\ell \equiv a \ (m)$ gilt, heißt diskreter Logarithmus von a mod m bzgl. der PW g,

Kurz: $\operatorname{dlog}_g(a) = \ell :\Leftrightarrow g^\ell \equiv a \ (m)$. (Anderer Begriff: Index von a,

Notation: $\ell = \operatorname{ind}_g(a)$.

9.13. Bsp.: Gesucht ist eine PW mod 11 und Tabelle für den diskreten Logarithmus.

Wir prüfen erst 2. Die Teiler von $11-1=10$ sind $1, 2, 5, 10$, und

$2^1 = 2 \not\equiv 1 \ (11)$, $2^2 = 4 \not\equiv 1 \ (11)$, $2^5 = 32 \equiv 10 \not\equiv 1 \ (11)$, also ist 2 PW mod 11.

Die Potenzen von 2 mod 11 sind

y	1	2	3	4	5	6	7	8	9	10
$x \equiv 2^y$	2	4	8	5	10	9	7	3	6	1

Die Logarithmustabelle ist also

x	1	2	3	4	5	6	7	8	9	10
$y = \operatorname{dlog}_2(x)$	10	1	8	2	4	9	7	3	6	5

9.14. Bsp.: Wir nutzen 9.13, um die folgenden Kongruenzen zu lösen.

1.) $x^3 \equiv 6\ (11)$. Mit $x \equiv 2^y\ (11)$ ist $x^3 \equiv 2^{3y}$, laut Tabelle ist $6 \equiv 2^9\ (11)$. Zu lösen ist also $3y \equiv 9\ (10) \Leftrightarrow y \equiv 3\ (10)$. Damit ist $x \equiv 2^3 = 8\ (11)$ Lösung.

2.) $x^5 \equiv 9\ (11)$. Mit $x \equiv 2^y\ (11)$ ist $5y \equiv 6\ (10)$ zu lösen, was wegen $(5,10) = 5 \nmid 6$ unlösbar ist.

3.) $x^{65} \equiv 10\ (11)$. Mit $x \equiv 2^y\ (11)$ ist $65y \equiv 5\ (10)$ zu lösen, d.h. $13y \equiv 1\ (2)$, was die einzige Lösung $y \equiv 1\ (2)$ hat, und somit gibt es 5 Lösungen mod 10, nämlich $y \equiv 1, 3, 5, 7$ oder 9 mod 10. Die ursprüngliche Kongruenz hat also die 5 Lösungen $x \equiv 2, 8, 10, 7, 6\ (11)$.