

Aufgabe 42

Beh.: Genau dann wenn $n = 2, n = 4, n = p^e$ oder $n = 2 \cdot p^e$, mit p ungerade und prim und $e \in \mathbb{N}$, existiert eine primitive Restklasse $\pmod n$.

Bew.: Zunächst zeigen wir, dass in den oben genannten Fällen primitive Restklassen existieren.

- Für $n = 2$ und $n = 4$ gilt dies offensichtlich mit [1] bzw. [3].

- Nun für p^e

Wir beweisen aus $[r]_{p^e}$ ist primitive Restklasse $\pmod{p^e}$ folgt für einen geeignet gewählten Repräsentanten r' von $[r]_{p^e}$ gilt $[r']_{p^{e+1}}$ ist primitive Restklasse $\pmod{p^{e+1}}$.

IV: Sei $[r]_p$ primitive Restklasse $\pmod p$. Wähle r' , so dass gilt $r'^{p-1} \not\equiv 1 \pmod{p^2}$ (1).

Für r' gilt dann $[r']_{p^2}$ ist primitive Restklasse $\pmod{p^2}$, denn als Ordnung kommen nur Teiler von $\Phi(p^2)$, also $\Phi(p^2)$ selbst, p und Teiler von $p-1$ in Frage. Teiler von $p-1$ entfallen offensichtlich. p ebenso, da $r'^p \equiv r' \not\equiv 1 \pmod p$ gilt. Es bleibt also nur $\Phi(p^2)$.

IA: Für $r'^{p^{e-2} \cdot (p-1)} \not\equiv 1 \pmod{p^e}$ gilt $[r']_{p^e}$ ist primitive Restklasse $\pmod{p^e}$.

IS: $r'^{p^{e-2} \cdot (p-1)} \equiv r'^{\Phi(p^{e-1})} \equiv 1 \pmod{p^{e-1}}$ also $r'^{p^{e-2} \cdot (p-1)} = 1 + bp^{e-1}$ mit $b \in \mathbb{Z}$. Potenzieren mit p liefert $r'^{p^{e-1} \cdot (p-1)} \equiv (1 + bp^{e-1})^p \stackrel{(4)}{\equiv} 1 + bp^e \pmod{p^{e+1}}$, wegen $p \nmid b$ (siehe IA) gilt: $r'^{p^{e-1} \cdot (p-1)} \not\equiv 1 \pmod{p^{e+1}}$. Es bleibt zu zeigen, dass die Restklasse primitiv ist.

Die Ordnung m der Restklasse $\pmod{p^e}$ ($e \geq 2$) muss ein Teiler von $\Phi(p^e) = p^{e-1} \cdot (p-1)$ sein, ausserdem folgt $(p-1) \mid m$ (da gilt $r'^m \equiv 1 \pmod{p^k} \Rightarrow r'^m \equiv 1 \pmod p$). Somit $m = p^t \cdot (p-1)$ mit $0 \leq t \leq e-1$. Wäre $t < e-1$ würde folgen: $r'^{p^{e-2} \cdot (p-1)} \equiv 1 \pmod{p^e}$ was aber dem oben gezeigten widerspricht. Also $t = e-1$ mithin $m = \Phi(p^e)$.

- $2 \cdot p^e$:

Sei r ein Vertreter einer primitiven Restklasse $\pmod{p^e}$. Dann kann r wegen $r \equiv r + p^e \pmod{p^e}$ als ungerade vorausgesetzt werden. Es gilt also $p^e \mid r^m - 1 \Leftrightarrow 2p^e \mid r^m - 1$. Wäre also $2p^e \mid r^m - 1$ mit $m < \Phi(2p^e) = \Phi(p^e)$ erfüllt, so wäre $[r]$ keine primitive Restklasse $\pmod{p^e}$ somit muss $[r]$ dann auch primitive Restklasse $\pmod{2p^e}$ sein.

Nun die Nichtexistenz von primitiven Restklassen in anderen Fällen :

- Zunächst für ein beliebig Potenzen von 2, 2^m mit $m \geq 3$.

Wir beweisen durch vollständige Induktion: $a^{2^{e-2}} \equiv 1 \pmod{2^e}$ für $e \geq 3$, dies führt zum Widerspruch mit der Aussage [a] sei primitive Restklasse $\pmod{2^e}$, da $2^{e-2} < 2^{e-1} = \Phi(2^e)$

IA: Für $e = 3$ gibt es keine Restklasse $\pmod m$, da $\Phi(8) = 4$ und für jede primitive Restklasse $[a] \pmod 8$ gilt $[a]^2 = [1]$.

IV: Für $e \geq 3$ gilt $a^{2^{e-2}} \equiv 1 \pmod{2^e}$.

IS: Gilt $a^{2^{e-2}} \equiv 1 \pmod{2^e}$, dann $a^{2^{e-2}} = 1 + b \cdot 2^e$ mit $b \in \mathbb{Z} \xrightarrow{(*)} a^{2^{e-1}} = 1 + 2b2^e + (b \cdot 2^e)^2 = 1 + (b + b^2 2^{e-1})2^{e+1} \Rightarrow a^{2^{e-1}} \equiv 1 \pmod{2^{e+1}}$.

(*) durch quadrieren.

- Nun für beliebige zusammengesetzte Zahlen $p = u \cdot v$ und $ggT(u, v) = 1$ (2) sowie $u, v > 2$. Da $\Phi(u)$ und $\Phi(v)$ beide gerade sind (3) gilt $ggT(\Phi(u), \Phi(v)) = d \geq 2$. Daher
 $h = \text{kgV}(\Phi(u), \Phi(v)) = \frac{\Phi(u) \cdot \Phi(v)}{d} = \frac{\Phi(uv)}{d} \leq \frac{\Phi(uv)}{2}$
 Wenn $[a]$ primitive Restklasse \pmod{p} ist, dann gilt $ggT(a, u) = 1$ und $ggT(a, v) = 1$ also $a^h \equiv a^{\frac{\Phi(uv)}{d}} \equiv a^{\Phi(u) \frac{\Phi(v)}{d}} \equiv 1^{\frac{\Phi(v)}{d}} \equiv 1 \pmod{p}$ (Analog für v).
 Somit $u|a^h - 1$ und $v|a^h - 1$, da $ggT(u, v) = 1$ gilt dann $p|a^h - 1$, da $h < \Phi(uv)$ ist $[a]$ keine primitive Restklasse \pmod{p} .

Hilfssätze:

1. r' kann immer so gewählt werden, falls gilt $r^{p-1} \equiv 1 \pmod{p^2}$ so wähle $r' = r + p$, dann gilt $r'^{p-1} \equiv (r+p)^{p-1} \equiv r^{p-1} + (p-1)r^{p-2}p \equiv 1 - pr^{p-2} \pmod{p^2}$
2. Jede zusammengesetzte Zahl > 4 lässt sich auf diese Weise schreiben. Man faktorisiert dazu zunächst p und teilt die Primfaktoren disjunkt auf u und v auf.
3. Für jede Zahl $u > 2$ gilt:
 $\Phi(u) = 2 \cdot n \quad n \in \mathbb{N}$
 - (a) u ist prim: da $\Phi(u) = u - 1$ und $u > 2$ gilt u ungerade, daher $u - 1$ gerade.
 - (b) u nicht prim: dann mit $u = \prod_1^\infty p_i^{\alpha_i}$ kanonische Primfaktorzerlegung.
 $\Phi(u) = \prod_1^\infty \Phi(p_i^{\alpha_i}) = \prod_1^\infty p_i^{\alpha_i - 1} \cdot (p_i - 1)$
 $p_i^{\alpha_i - 1} \in \begin{cases} \{2n | n \in \mathbb{N}\} & \text{wenn } p \text{ gerade und } \alpha_i - 1 > 0 \\ \{2n + 1 | n \in \mathbb{N}\} & \text{sonst} \end{cases}$
 $p - 1 \in \begin{cases} \{2n | n \in \mathbb{N}\} & \text{wenn } p \text{ ungerade} \\ \{2n + 1 | n \in \mathbb{N}\} & \text{sonst} \end{cases}$
 somit sind alle Faktoren von $\Phi(u)$ gerade also ist $\Phi(u)$ gerade.

4.

$$\begin{aligned}
(1 + bp^{e-1})^p &= \sum_{k=0}^p \binom{p}{k} 1^{p-k} (bp^{e-1})^k \\
&= 1 \\
&+ \binom{p}{1} (bp^{e-1}) \\
&+ \binom{p}{2} (bp^{e-1})^2 \\
&+ \dots \\
&+ \binom{p}{p-1} (bp^{e-1})^{p-1} + \\
&+ (bp^{e-1})^p \\
&\stackrel{(*)}{=} 1 \\
&+ pbp^{e-1} + n_1p(bp^{e-1})^2 \\
&+ n_2p(bp^{e-1})^3 + \dots \\
&+ p(bp^{e-1})^{p-1} + (bp^{e-1})^p \\
&= 1 + bp^e + n_1b^2p^{2e-1} \\
&+ \dots + b^{p-1}p^{(e-1)(p-1)+1} \\
&+ bp^{pe-p} \\
&\stackrel{(*^2)}{\Rightarrow} (1 + bp^{e-1})^p \equiv 1 + bp^e \pmod{p^{e+1}}
\end{aligned}$$

$$(*)p \mid \binom{p}{k} \text{ für } 1 \leq k \leq p-1$$

$$(*^2) \text{ für } e > 1$$

Anmerkungen:

1. Zu den Begrifflichkeiten :

Eine Restklasse $[a]$ heisst primitiv, wenn sie die maximale Ordnung $\Phi(m)$ hat. In diesem Fall besteht sie aus allen Potenzen von $[a]$ mit $[a]^{\Phi(m)} = [1]$. Eine veraltete Bezeichnung für eine ganze Zahl x mit der Eigenschaft $\text{ord}_m[x] = \Phi(m)$ ist primitive Kongruenzwurzel mod m

(frei nach 'Einführung in die Zahlentheorie' von Peter Bundschuh, Springer Verlag, Berlin, September 2002)