Liften von Lösungen modulo 2

Übung:

- An welcher Stelle im vorigen Beweis benötigen wir $p \neq 2$?
- Geben Sie ein Gegenbeispiel für voriges Lemma für $p = 2, r = 3$.
- Modifizieren Sie den Beweis, um das folgende Lemma zu zeigen.

Lemma Liften mod 2

Sei $x \in \mathbb{Z}$ mit $x \equiv 1 \bmod 4$. Für $r \geq 2$ gilt

$$x \equiv 1 \bmod 2^{r-1} \Leftrightarrow x^2 \equiv 1 \bmod 2^r$$

U_{p^r} ist zyklisch für $p \geq 3$

Satz

Für $p \in \mathbb{P} \setminus \{2\}$ und $r \in \mathbb{N}$ ist U_{p^r} zyklisch, d.h. $U_{p^r} \cong \mathbb{Z}/\varphi(p^r)\mathbb{Z}$.

Beweis:

- Wir wissen bereits, dass U_p zyklisch ist. Sei g ein Generator.
- Behauptung: U_{p^r} wird von g oder von $g' := g + p$ generiert.
- Wir müssen zeigen, dass $g^{\frac{\varphi(p^r)}{q}} \not\equiv 1 \bmod p^r$ (oder analog für g') für alle Primteiler q von $\varphi(p^r) = p^{r-1}(p-1)$.
- **Fall 1** $q \mid p-1$: Offenbar gilt $g \equiv g' \bmod p$.
- Da g ein Generator von U_p ist, folgt $g'^{\frac{p-1}{q}} \equiv g^{\frac{p-1}{q}} \not\equiv 1 \bmod p$.
- $(p-1)$-malige Anwendung des Lift-Lemmas (Folie 103) liefert

$$g^{\frac{p^{r-1}(p-1)}{q}} \not\equiv 1 \bmod p^r. \text{ (bzw. für } g')$$

U_{p^r} ist zyklisch für $p \geq 3$

Beweis: (Fortsetzung)

- **Fall 2** $q = p$. Wir müssen zeigen, dass entweder
$$g^{p^{r-2}(p-1)} \not\equiv 1 \bmod p^r \text{ oder } g'^{p^{r-2}(p-1)} \not\equiv 1 \bmod p^r$$
- $(r-2)$-malige Anwendung unseres Lemmas liefert
$$g^{(p-1)} \not\equiv 1 \bmod p^2 \text{ oder } g'^{(p-1)} \not\equiv 1 \bmod p^2.$$
- Annahme: $g^{(p-1)} \equiv 1 \bmod p^2$ und $(g+p)^{(p-1)} \equiv 1 \bmod p^2$
- Es folgt
$$1 \equiv (g+p)^{p-1} \equiv g^{p-1} + (p-1)g^{p-2}p \equiv 1 + (p-1)g^{p-2}p \bmod p^2.$$
- Damit ist $-g^{p-2}p \equiv 0 \bmod p^2$ bzw. $g^{p-2} \equiv 0 \bmod p$.
(Widerspruch: $(U_p, \cdot)$ ist abgeschlossen und $0 \notin U_p$.)

Test auf Primitivwurzel für U_{p^r}

Korollar

Sei g ein Generator von U_p, $p \in \mathbb{P}$. Für $r > 1$ ist ein Generator von U_{p^r}

$$\begin{cases} g & \text{falls } g^{p-1} \not\equiv 1 \bmod p^2 \\ g+p & \text{sonst} \end{cases}.$$

Beweis: Folgt direkt aus dem Beweis zuvor.

Bsp:

- 2 ist Generator von U_5 wegen $2^{\frac{5-1}{2}} = 4 \not\equiv 1 \bmod 5$.
- Wegen $2^4 = 16 \not\equiv 1 \bmod 25$ ist 2 auch Generator für U_{p^r} mit $r \geq 2$.

Die Potenzen von 2

Der folgende Satz zeigt, dass U_{2^r} für $r \geq 3$ nicht zyklisch ist.

Satz

Für $r \geq 3$ gilt $U_{2^r} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{r-2}\mathbb{Z}$.

Beweis:

- Wir zeigen, dass die folgende Abbildung ein Isomorphismus ist:
$$\Psi : \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{r-2}\mathbb{Z} \to U_{2^r} \text{ mit } (\bar{i}, \bar{j}) \mapsto \overline{(-1)}^i \bar{5}^j.$$
- Da $\bar{j} = j + 2^{r-2}\mathbb{Z}$, benötigen wir $\operatorname{ord}(\bar{5}) = 2^{r-2}$, damit wir im Exponenten mod 2^{r-2} rechnen können. (Wohldefiniertheit von Ψ)
- Wir zeigen zunächst, dass $5^{2^{r-2}} \equiv 1 \bmod 2^r$.
- $(r-2)$-malige Anwendung des Lift-Lemmas mod 2 liefert
$$5^{2^{r-2}} \equiv 1 \bmod 2^r \Leftrightarrow 5 \equiv 1 \bmod 2^2.$$
- Damit gilt $\operatorname{ord}(\bar{5}) | 2^{r-2}$. Falls $\operatorname{ord}(\bar{5}) \nmid 2^{r-3}$ folgt $\operatorname{ord}(\bar{5}) = 2^{r-2}$.
- Es gilt $5^{2^{r-3}} \not\equiv 1 \bmod 2^r \Leftrightarrow 5 \not\equiv 1 \bmod 2^3$.

Die Potenzen von 2

Beweis: (Fortsetzung)

- Bleibt zu zeigen, dass Ψ bijektiv ist. Da Urbild- und Bildmenge Kardinalität 2^{r-1} besitzen, genügt es, Injektivität zu zeigen.
- Es gilt $\Psi((\bar{i},\bar{j}) - (\bar{i}',\bar{j}')) = \Psi(\bar{i},\bar{j}) \cdot \Psi(\bar{i}',\bar{j}')^{-1}$.
- D.h. für $\Psi(\bar{i},\bar{j}) = \Psi(\bar{i}',\bar{j}') \Rightarrow (\bar{i},\bar{j}) = (\bar{i},\bar{j}')$ müssen wir zeigen, dass
$$\Psi(\bar{i},\bar{j}) = \bar{1} \Rightarrow (\bar{i},\bar{j}) = (\bar{0},\bar{0}).$$
- Sei $\Psi(\bar{i},\bar{j}) = (-1)^i 5^j \equiv 1 \bmod 2^r$ für $r \geq 3$.
- Insbesondere gilt $(-1)^i \equiv 1 \bmod 4$. D.h. $i = 0 \bmod 2$ bzw. $\bar{i} = \bar{0}$.
- Damit gilt $\Psi(\bar{0},\bar{j}) = 5^j \equiv 1 \bmod 2^r$.
- Wegen $\operatorname{ord}(\bar{5}) = 2^{r-2}$ folgt $j \equiv 0 \bmod 2^{r-2}$ bzw. $\bar{j} = 0$.

Klassifikation der zyklischen U_p

Satz Klassifikation der zyklischen U_p

Für $n \in \mathbb{N}$ ist die Einheitengruppe U_n zyklisch gdw

$$n = 2, 4, n = p^r \text{ oder } n = 2p^r \text{ für } p \in \mathbb{P} \setminus \{2\} \text{ und } r \in \mathbb{N}.$$

Beweis:

- Es gilt $U_2 = \{\bar{1}\}$ und $U_4 = \{\bar{1}, \bar{3}\}$ mit Generatoren $\bar{1}$ bzw. $\bar{3}$.
- Dass U_{p^r} zyklisch ist, wurde auf Folie 106 gezeigt.
- Ferner gilt nach CRT (Lemma auf Folie 68)
$$U_{2p^r} \cong U_2 \times U_{p^r} \cong U_{p^r}.$$
- Damit ist auch U_{2p^r} zyklisch.
- Alle anderen n schreiben wir als
$$n = a \cdot b \text{ für teilerfremde } a, b \text{ mit } 2 < a, b < n.$$
- Nach CRT (Lemma auf Folie 68) gilt $U_n \cong U_a \times U_b$.
- D.h. U_n ist isomorph zu einem Produkt nicht-trivialer Gruppen.

k-te Wurzeln in U_n

- Sei U_n zyklisch mit Primitivwurzel g.
- Wir haben bereits den folgenden Isomorphismus studiert:
$$\exp_g : (\mathbb{Z}/\varphi(N), +) \to (U_n, \cdot) \text{ mit } \bar{i} \mapsto \bar{g}^i.$$
- Damit gilt $\exp_g(x + y) = \exp_g(x) \cdot \exp_g(y)$.
- Die Umkehrfunktion ist der Diskrete Logarithmus
$$\log_g : (U_n, \cdot) \to (\mathbb{Z}/\varphi(N), +) \text{ mit } \bar{g}^i \mapsto \bar{i}.$$
- Damit ist $\log_g(xy) = \log_g(x) + \log_g(y)$ und $\log_g(x^k) = k \log(x)$.

Ziel: Finde alle Lösungen $x \in U_n$ von $x^k \equiv a \bmod n$.

- Anwendung von $\log_g$ liefert $k \log_g x \equiv \log_g a \bmod \phi(n)$.
- Wir können nun diese lineare Gleichung nach $\log_g x$ auflösen.
- Wenn wir $\log_g a$ berechnen, erhalten wir alle Lösungen für $\log_g x$.
- Anwenden von exp auf diese Lösungen liefert alle Lösungen für x.

Bsp. Berechnen einer 3-ten Wurzel in U_7

Bsp: Berechne alle Lösungen von $x^3 \equiv 6 \bmod 7$

- Wir wissen bereits, dass $\bar{3}$ eine Primitivwurzel von U_7 ist.
- Anwendung von $\log_3$ liefert $3 \cdot \log_3 x \equiv \log_3 6 \bmod 6$.
- Wir bestimmen $\log_3 \bar{6} = \bar{3}$ mittels folgender Wertetabelle

i	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\exp_3(i)$	$\bar{1}$	$\bar{3}$	$\bar{2}$	$\bar{6}$	$\bar{4}$	$\bar{5}$

- Wegen $\mathrm{ggT}(3,6) = 3$ erhalten wir die Lösungen
$$\log x \equiv 3^{-1} \cdot \tfrac{3}{3} \equiv 1 \bmod 2.$$
- In U_7 erfüllen diese Kongruenz die Restklassen $\bar{1}$, $\bar{3}$ und $\bar{5}$.
- Durch Anwendung von $\exp_3$ erhalten wir alle 3 Lösungen
$$\exp_3(\bar{1}) = \bar{3}, \exp_3(\bar{3}) = \bar{6} \text{ und } \exp_3(\bar{5}) = \bar{5}.$$
- Wir testen $3^3 \equiv 6^3 \equiv 5^3 \equiv 6 \bmod 7$.

Anmerkung: In U_n kostet das Berechnen der Wertetabelle Zeit $\Omega(n)$.

Übung: Zeigen Sie:
$f_k : U_n \to U_n, \bar{x} \mapsto \bar{x}^k$ ist für $\mathrm{ggT}(k, \varphi(n)) = 1$ ein Isomorphismus.
Geben Sie einen Alg. zum Berechnen von f_k^{-1} in Zeit $\mathcal{O}(\log^3 n)$.

Baby-Step Giant-Step Algorithmus

Ziel: Berechnen von $\log_g a$ in U_n in Zeit und Platz $\mathcal{O}(\sqrt{n}\log n)$.

Idee: Baby-Step Giant-Step Algorithmus

- Sei $x \equiv \log_g a \bmod \varphi(n)$ mit $0 \leq x < \varphi(n)$, d.h. $g^x \equiv a \bmod n$.
- Setze $A := \lceil \sqrt{n} \rceil$.
- Schreibe $x = x_1 A + x_0$ mit $x_0, x_1 < A \leq \lceil \sqrt{n} \rceil$.
- Es gilt die Identität $(g^A)^{x_1} \equiv a \cdot g^{-x_0} \bmod n$.
- Erstelle zwei Listen mit Kandidaten für $(g^A)^{x_1}$ bzw. $a \cdot g^{-x_0}$.
- Zwei gleiche Listenelemente liefern (x_0, x_1) und damit x.