Seminarvortrag aus Reiner Mathematik
Existenz von Primitivwurzeln

Michael Kniely

November 2009

1 Vorbemerkungen

Definition. Sei $n \in \mathbb{N}^+$, $\phi(n) := |\{d \in [0, n-1] \mid ggT(d,n) = 1\}|$. Die Abbildung $\phi : \mathbb{N}^+ \to \mathbb{N}^+$ heißt **Euler'sche Phi-Funktion** und ist für $n \in \mathbb{N}^+$ gleich der Anzahl an Elementen aus $[0, n-1]$, die teilerfremd zu n sind.

Bemerkung. Seien $j \in \mathbb{N}$, $m, n \in \mathbb{N}^+$ und $p \in \mathbb{P}$.

1. $\phi(m) = |(\mathbb{Z}/m\mathbb{Z})^\times|$, $\phi(p) = p-1$ und $\phi(p^j) = (p-1)p^{j-1}$.
2. ϕ ist multiplikativ, das heißt $ggT(m,n) = 1 \Rightarrow \phi(m \cdot n) = \phi(m)\phi(n)$.

Notation. Mit $\pi_m : \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ wird im Folgenden der kanonische Homomorphismus bezeichnet.

Satz. Seien $a \in \mathbb{Z}$, $m \in \mathbb{N}^+$, $p \in \mathbb{P}$.

1. "Euler": $ggT(a,m) = 1 \Rightarrow a^{\phi(m)} \equiv 1 \ (mod\ m)$.
2. "kleiner Fermat": $a^p \equiv a \ (mod\ p)$; $p \nmid a \Rightarrow a^{p-1} \equiv 1 \ (mod\ p)$.

Beweis.

1. Da $ggT(a,m) = 1$ ist, ist $\pi_m(a) \in (\mathbb{Z}/m\mathbb{Z})^\times$ und mittels *Satz von Lagrange* erhält man $ord(\pi_m(a)) \mid |(\mathbb{Z}/m\mathbb{Z})^\times| = \phi(m)$; daraus folgt aber $\pi_m(a)^{\phi(m)} = 1_{(\mathbb{Z}/m\mathbb{Z})^\times}$ und schließlich $\pi_m(a^{\phi(m)}) = \pi_m(a)^{\phi(m)} = 1_{(\mathbb{Z}/m\mathbb{Z})^\times} = \pi_m(1_\mathbb{Z})$, was äquivalent zu $a^{\phi(m)} \equiv 1 \ (mod\ m)$ ist.
2. Mittels Fallunterscheidung erhält man schrittweise:
   - $p \nmid a \Rightarrow ggT(a,p) = 1 \Rightarrow a^{\phi(p)} = a^{p-1} \equiv 1 \ (mod\ p) \Rightarrow a^p \equiv a \ (mod\ p)$
   - $p \mid a \Rightarrow p \mid a^p \Rightarrow p \mid a^p - a \Rightarrow a^p \equiv a \ (mod\ p)$.

Definition. Seien $a \in \mathbb{Z}$ und $m \in \mathbb{N}^+$ mit $ggT(a,m) = 1$. Dann heißt a genau dann eine **Primitivwurzel** modulo m, wenn $\langle \pi_m(a) \rangle = (\mathbb{Z}/m\mathbb{Z})^\times$.

Bemerkung. Definiert man für $a \in \mathbb{Z}$ und $m \in \mathbb{N}^+$ mit $ggT(a,m) = 1$ die **Ordnung** von a modulo m via $ord_m a = min\{k \in \mathbb{N}^+ \mid a^k \equiv 1 \ (mod\ m)\}$, so folgt daraus

1. $ord_m a = ord(\pi_m(a))$ in der Gruppe $(\mathbb{Z}/m\mathbb{Z})^\times$.
2. a ist eine Primitivwurzel modulo $m \Leftrightarrow ord_m a = \phi(m)$.

Beweis.

1. Klar, da $ord(\pi_m(a)) = min\{k \in \mathbb{N}^+ \mid \pi_m(a)^k = 1_{(\mathbb{Z}/m\mathbb{Z})^\times}\}$.
2. $\underline{\Rightarrow:}$ a ist eine Primitivwurzel modulo $m \Rightarrow \phi(m) = |(\mathbb{Z}/m\mathbb{Z})^\times| = |\langle \pi_m(a)\rangle| = ord(\pi_m(a)) = ord_m a$.

   $\underline{\Leftarrow:}$ Aus $|(\mathbb{Z}/m\mathbb{Z})^\times| = \phi(m) = ord_m a = ord(\pi_m(a)) = |\langle \pi_m(a)\rangle|$ und $\langle \pi_m(a)\rangle \subset (\mathbb{Z}/m\mathbb{Z})^\times$ folgt $\langle \pi_m(a)\rangle = (\mathbb{Z}/m\mathbb{Z})^\times$ und damit die Behauptung.

2 Der Satz von Gauß

Lemma. Zu jeder Primzahl p gibt es eine Primitivwurzel a modulo p mit $a^{p-1} \not\equiv 1 \ (mod\ p^2)$.

Beweis. Sei p eine Primzahl, $a_1 \in \mathbb{Z}$ und $a_2 := a_1 + p$. Mithilfe des binomischen Lehrsatzes kann man a_2^p schreiben als

$$a_2^p = (a_1 + p)^p = \sum_{j=0}^{p} \binom{p}{j} a_1^j p^{p-j}.$$

Betrachtet man a_2^p nun modulo p^2, so sieht man, dass p^2 jeden Summanden für $j = 0, ..., p-2$ teilt, da $p^2 \mid p^{p-j} \mid \binom{p}{j} a_1^j p^{p-j}$; für $j = p-1$ ist $\binom{p}{j} a_1^j p^{p-j} = p a_1^{p-1} p$, womit ersichtlich ist, dass auch dieser Term Vielfaches von p^2 ist. Da der letzte Summand $\binom{p}{p} a_1^p p^{p-p} = a_1^p$ ist, erhält man

$$a_2^p \equiv a_1^p \ (mod\ p^2). \tag{1}$$

Aus dem *kleinen Fermat'schen Satz* folgt nun, dass $a_1^p \equiv a_1 \ (mod\ p)$ und $a_2^p \equiv a_2 \ (mod\ p)$ bzw. $a_1^p = a_1 + b_1 p$ und $a_2^p = a_2 + b_2 p$ mit $b_1, b_2 \in \mathbb{Z}$ sind. Man erhält, wenn man diese Beziehungen in (1) einsetzt und $a_2 = a_1 + p$ beachtet

$$a_2 + b_2 p = a_1 + p + b_2 p \equiv a_1 + b_1 p \ (mod\ p^2);$$

dies ist äquivalent zu $b_2 p \equiv b_1 p - p \ (mod\ p^2)$; "kürzt" man das p in dieser Kongruenz, so erhält man

$$b_2 \equiv b_1 - 1 \ (mod\ p).$$

Das heißt nun, dass höchstens eines der beiden $b_i,\ i \in \{1,2\}$ durch p teilbar sein kann; denn sonst wäre $0 \equiv 1\ (mod\ p)$, woraus $p = 1$ folgen würde - ein Widerspruch.

Man wähle nun a_1 als eine Primitivwurzel modulo p, was nach den Erkenntnissen in den vorigen Abschnitten möglich ist; dann gilt $a_2 = a_1 + p \Rightarrow a_2 \equiv a_1\ (mod\ p) \Rightarrow \pi_p(a_2) = \pi_p(a_1)$. Da $(\mathbb{Z}/p\mathbb{Z})^\times = \langle \pi_p(a_1) \rangle = \langle \pi_p(a_2) \rangle$, ist auch a_2 eine Primitivwurzel modulo p.

Sei nun b_2 jenes der beiden b_i von vorhin, das kein Vielfaches von p ist, dann gilt $p \nmid b_2 \Rightarrow p^2 \nmid b_2 p \Rightarrow p^2 \nmid a_2^p - a_2$. Das besagt aber gerade, dass $p^2 \nmid a_2(a_2^{p-1} - 1)$ und insbesondere $p^2 \nmid (a_2^{p-1} - 1)$ gilt. Da die letzte Aussage äquivalent zu

$$a_2^{p-1} \not\equiv 1\ (mod\ p^2)$$

ist, und a_2 eine Primitivwurzel modulo p ist, ist das Lemma bewiesen. □

Der folgende Satz - der *Satz von Gauss* - ist in dieser Form das Gegenstück zum Satz über die notwendige Bedingung für die Existenz von Primitivwurzeln modulo einer natürlichen Zahl; er besagt, dass diese notwendige Bedingung gleichzeitig hinreichend ist.

Satz. Modulo $m \in \mathbb{N}^+$ existieren genau dann Primitivwurzeln, wenn $m \in \{1, 2, 4, p^\alpha, 2p^\alpha \mid p \in \mathbb{P}\backslash\{2\}, \alpha \in \mathbb{N}^+\}$.

Beweis. Wie eben bemerkt, bleibt nur noch zu zeigen, dass es modulo dieser speziellen natürlichen Zahlen tatsächlich Primitivwurzeln gibt.

Für $m = 1$ ist $a = 1$ eine Primitivwurzel, da $(\mathbb{Z}/\mathbb{Z})^\times = \{\overline{0}\}^\times = \{\overline{0}\} = \{\overline{1}\}$; ebenso ist $a = 1$ eine Primitivwurzel modulo $m = 2$, da $(\mathbb{Z}/2\mathbb{Z})^\times = \{\overline{0}, \overline{1}\}^\times = \{\overline{1}\}$, und $a = 3$ eine Primitivwurzel modulo $m = 4$, da $(\mathbb{Z}/4\mathbb{Z})^\times = \{\overline{1}, \overline{3}\} = \langle \overline{3} \rangle$.

Im Folgenden seien p eine ungerade Primzahl und α eine natürliche Zahl. Zunächst wird der Fall $m = p^\alpha$ behandelt und gezeigt, dass es modulo p^α Primitivwurzeln gibt. Zu diesem Zweck wähle man $a \in \mathbb{N}^+$ als eine Primitivwurzel modulo p mit $a^{p-1} \not\equiv 1\ (mod\ p^2)$, das heißt wie im vorangegangenen Lemma. Im nächsten Schritt beweist man mittels vollständiger Induktion die Aussage

$$(\forall\ \alpha \in \mathbb{N}^+, \alpha \geq 2)\ a^{(p-1)p^{\alpha-2}} \not\equiv 1\ (mod\ p^\alpha). \tag{2}$$

In diesem Fall startet der Induktionsbeweis bei $\alpha = 2$ und man hat als Induktionsverankerung $a^{p-1} \not\equiv 1\ (mod\ p^2)$ zu zeigen; diese Aussage erledigt sich aber von selbst, da a ja genauso gewählt wurde, dass es diese Eigenschaft hat. Im folgenden Induktionsschritt setzt man (2) für ein gegebenes $\alpha \geq 2$ als richtig voraus und behält dies im Auge; denn einerseits folgt aus dem *Euler'schen Satz* $a^{\phi(p^{\alpha-1})} \equiv 1\ (mod\ p^{\alpha-1})$ und andererseits $\phi(p^{\alpha-1}) = (p-1)p^{\alpha-2}$ aus den Eigenschaften der *Euler'schen Phi-Funktion*. Zusammen ergibt sich

$$a^{(p-1)p^{\alpha-2}} \equiv 1\ (mod\ p^{\alpha-1})$$

oder äquivalent dazu

$$a^{(p-1)p^{\alpha-2}} = 1 + bp^{\alpha-1}, \tag{3}$$

wobei hier zu beachten ist, dass b zwar ganz ist, aber nach Induktionsannahme kein Vielfaches von p sein kann, da sonst $a^{(p-1)p^{\alpha-2}} = 1 + b'p^{\alpha}$ gelten würde mit $b' \in \mathbb{Z}$, was $a^{(p-1)p^{\alpha-2}} \equiv 1 \ (mod\ p^{\alpha})$ zur Folge hätte - ein Widerspruch zur Induktionsannahme.

Durch Potenzieren von (3) mit p erhält man mittels binomischem Lehrsatz

$$a^{(p-1)p^{\alpha-1}} = (1 + bp^{\alpha-1})^p = \sum_{j=0}^{p} \binom{p}{j} b^j p^{j(\alpha-1)};$$

diese letzte Summe anders angeschrieben ergibt

$$\begin{aligned} \sum_{j=0}^{p} \binom{p}{j} b^j p^{j(\alpha-1)} &= 1 + pbp^{\alpha-1} + \sum_{j=2}^{p} \binom{p}{j} b^j p^{j(\alpha-1)} = \\ &= 1 + bp^{\alpha} + p^{2(\alpha-1)} \sum_{j=2}^{p} \binom{p}{j} b^j p^{(j-2)(\alpha-1)}. \end{aligned}$$

Da $\alpha \geq 2$, ist für $j \geq 3$ jeder Summand Vielfaches von p, da $p \mid p^{(j-2)(\alpha-1)} \mid \binom{p}{j} b^j p^{(j-2)(\alpha-1)}$; beachtet man aber, dass $\binom{p}{2} = \frac{p(p-1)}{2}$ und $p-1$ gerade ist, so sieht man, dass p ein Teiler von $\binom{p}{2}$ ist - was nach einem Resultat aus der Vorlesung "Einführung in die Algebra" ohnehin klar ist (n *ist prim* $\Leftrightarrow$ $(\forall\ m \in \{1, ..., n-1\})\ n \mid \binom{n}{m}$). Insgesamt heißt das also, dass die Summe $\sum_{j=2}^{p} \binom{p}{j} b^j p^{(j-2)(\alpha-1)}$ Vielfaches von p ist; schließlich liefert das

$$1 + bp^{\alpha} + p^{2(\alpha-1)} \sum_{j=2}^{p} \binom{p}{j} b^j p^{(j-2)(\alpha-1)} = 1 + bp^{\alpha} + cp^{2\alpha-1}$$

mit $c \in \mathbb{Z}$ und nochmals zusammengefasst

$$a^{(p-1)p^{\alpha-1}} = 1 + bp^{\alpha} + cp^{2\alpha-1}$$

Da aber $\alpha \geq 2 \Rightarrow 2\alpha - 1 \geq \alpha + 1$, folgt daraus, dass $p^{\alpha+1} \mid cp^{2\alpha-1}$, aber $p^{\alpha+1} \nmid bp^{\alpha}$, da $p \nmid b$ wie bereits weiter oben bemerkt wurde. Das heißt also

$$a^{(p-1)p^{\alpha-1}} \equiv 1 + bp^{\alpha} \not\equiv 1 \ (mod\ p^{\alpha+1}),$$

was genau der Aussage in (2) entspricht mit $\alpha + 1$ anstelle von α. Damit ist der Induktionsbeweis abgeschlossen und die Richtigkeit von (2) gezeigt.

Sei a im Weiteren wie bisher gewählt; dann sind a und p^{α} teilerfremd, denn ein $ggT(a, p^{\alpha}) > 1$ hätte einen gemeinsamen Teiler p zur Folge, womit a ein Vielfaches von p wäre - ein Widerspruch, da a eine Primitivwurzel modulo p ist und somit $ggT(a, p) = 1$ gilt. Also ist es möglich $l := ord_{p^{\alpha}} a$ zu definieren.

Da $ord_{p^\alpha} a \mid n$ für alle $n \in \mathbb{Z}$ mit $a^n \equiv 1 \ (mod\ p^\alpha)$, gilt insbesondere $l \mid \phi(p^\alpha) = (p-1)p^{\alpha-1}$ nach *Euler'schem Satz* und Eigenschaften der *Euler'schen Phi-Funktion*. Allerdings gilt wegen $a^l \equiv 1 \ (mod\ p^\alpha)$ erst recht $a^l \equiv 1 \ (mod\ p)$, da $p \mid p^\alpha \mid a^l - 1$. Wegen $ord_p a = \phi(p) = p-1$ und $ord_p a \mid l$ gilt zusätzlich auch $p-1 \mid l$, zusammen also

$$p-1 \mid l \mid (p-1)p^{\alpha-1};$$

damit kann l nur von der Form $l = (p-1)p^\beta$ mit $\beta \in \{0, ..., \alpha-1\}$ sein. Daher folgt daraus $a^l = a^{(p-1)p^\beta} \equiv 1 \ (mod\ p^\alpha)$; laut (2) ist $\beta \leq \alpha - 2$ aber nicht möglich, da $a^{(p-1)p^\beta} \equiv 1 \ (mod\ p^\alpha)$ mit $\beta \leq \alpha - 2 \Rightarrow p^{\beta+2} \mid p^\alpha \mid a^{(p-1)p^\beta} - 1 \Rightarrow a^{(p-1)p^\beta} \equiv 1 \ (mod\ p^{\beta+2})$, was ein Widerspuch zu (2) mit $\alpha = \beta + 2$ ist.

Damit bleibt nur die Möglichkeit $\beta = \alpha - 1$ übrig, woraus $ord_{p^\alpha} a = l = (p-1)p^{\alpha-1} = \phi(p^\alpha)$ folgt. Dies ist aber nach der Charakterisierung von Primitivwurzeln äquivalent damit, dass a eine Primitivwurzel modulo p^α ist, womit gezeigt ist, dass es modulo p^α mit ungerader Primzahl p und natürlichem α Primitivwurzeln gibt.

Zuletzt muss noch gezeigt werden, dass es auch modulo $2p^\alpha$, mit p und α wie vorhin, Primitivwurzeln gibt. Sei dazu a eine Primitivwurzel modulo p^α; ferner wähle man eine ungerade Primitivwurzel $\hat{a}$ modulo p^α. Solch ein $\hat{a}$ kann man unter den bisherigen Voraussetzungen auch immer finden: Falls a ohnehin ungerade ist, wählt man $\hat{a} := a$, andernfalls $\hat{a} := a + p^\alpha$; $\hat{a}$ ist dann ungerade und Primitivwurzel modulo p^α, da $a \equiv \hat{a} \ (mod\ p^\alpha) \Rightarrow \pi_{p^\alpha}(a) = \pi_{p^\alpha}(\hat{a}) \Rightarrow (\mathbb{Z}/p^\alpha\mathbb{Z})^\times = \langle \pi_{p^\alpha}(a) \rangle = \langle \pi_{p^\alpha}(\hat{a}) \rangle$.

Wegen $ggT(2, p^\alpha) = 1$ folgt aus dem chinesischen Restsatz, dass

$$(\mathbb{Z}/2p^\alpha\mathbb{Z})^\times \cong (\mathbb{Z}/2\mathbb{Z})^\times \times (\mathbb{Z}/p^\alpha\mathbb{Z})^\times \cong (\mathbb{Z}/p^\alpha\mathbb{Z})^\times, \tag{4}$$

wobei die zweite Isomorphie trivial ist, da $(\mathbb{Z}/2\mathbb{Z})^\times = \{\overline{1}\}$. Man wähle nun folgenden Gruppenisomorphismus $f : (\mathbb{Z}/2p^\alpha\mathbb{Z})^\times \to (\mathbb{Z}/p^\alpha\mathbb{Z})^\times$, definiert via $\pi_{2p^\alpha}(x) \to (\pi_2(x), \pi_{p^\alpha}(x)) \to \pi_{p^\alpha}(x)$ für $x \in \mathbb{Z}$, wobei die Abbildungspfeile für die einzelnen Gruppenisomorphismen in (4) stehen. Beachtet man die folgenden Äquivalenzen

$$(\mathbb{Z}/2p^\alpha\mathbb{Z})^\times = \langle \pi_{2p^\alpha}(\hat{a}) \rangle \quad \Longleftrightarrow \tag{5}$$

$$f((\mathbb{Z}/2p^\alpha\mathbb{Z})^\times) = f(\langle \pi_{2p^\alpha}(\hat{a}) \rangle) \iff \tag{6}$$

$$(\mathbb{Z}/p^\alpha\mathbb{Z})^\times = \langle f(\pi_{2p^\alpha}(\hat{a})) \rangle, \tag{7}$$

so sieht man, dass $\hat{a}$ genau dann eine Primitivwurzel modulo $2p^\alpha$ ist, wenn $f(\pi_{2p^\alpha}(\hat{a}))$ die Gruppe $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ erzeugt.

Dazu untersucht man die Wirkung von f auf $\pi_{2p^\alpha}(\hat{a})$:

$$\pi_{2p^\alpha}(\hat{a}) \to (\pi_2(\hat{a}), \pi_{p^\alpha}(\hat{a})) \to \pi_{p^\alpha}(\hat{a}),$$

und erkennt, dass $f(\pi_{2p^\alpha}(\hat{a})) = \pi_{p^\alpha}(\hat{a})$ und Gleichung (7) somit erfüllt ist. Damit sind aber auch (6) und schließlich Aussage (5) wahr, womit gezeigt ist, dass $\hat{a}$ eine Primitivwurzel modulo $2p^\alpha$ ist. □