Vorlesung „Kryptographie“ – Dietzfelbinger

Ergänzung zu Kapitel 5: Zyklische Gruppen

Für kryptographische Konstruktionen, die durch Begriffe wie „Diskreter Logarithmus“, „Diffie-Hellman-Problem“, „Kryptographie mit elliptischen Kurven“ gekennzeichnet sind, benötigt man als Grundlage das Konzept einer *zyklischen Gruppe* und einige Grundtatsachen darüber. Ein zentrales Beispiel für solche zyklischen Gruppen sind die multiplikativen Gruppen in endlichen Körpern.

Zyklische Gruppen

Beispiele:

(a) Sei $m = 9$. In $\mathbb{Z}_m$ ist 0 das neutrale Element der Addition, und 1 „erzeugt“ die Gruppe in dem Sinn, dass man durch Addieren von 1en alle Gruppenelemente bekommt:

$$1, 1+1 = 2, 1+1+1+ = 3, \ldots, 1+1+1+1+1+1+1+1 = 8, 1+1+1+1+1+1+1+1+1 = 0.$$

Wenn wir noch mehr Einsen addieren, „geht es wieder von vorne los“:

$$1+1+1+1+1+1+1+1+1+1 = 1, 1+1+1+1+1+1+1+1+1+1+1 = 2, \ldots$$

Neben 1 gibt es noch andere Elemente, die die Gruppe erzeugen, zum Beispiel 4:

$$4, 4+4 = 8, 8+4 = 3, 3+4 = 7, 7+4 = 2, 2+4 = 6, 6+4 = 1, 1+4 = 5, 5+4 = 0.$$

Dagegen erzeugt das Element 3 die Gruppe nicht, weil $3 + 3 = 6$ und $3 + 3 + 3 = 0$ gilt.

(b) Wir betrachten die multiplikative Gruppe $\mathbb{Z}_7^*$. Sie hat die Elemente $1, \ldots, 6$. Das Element 3 ist ein erzeugendes Element, weil man alle Elemente durch wiederholte Multiplikation von 3en erhält (modulo 7):

$$3, 3 \cdot 3 = 2, 3 \cdot 3 \cdot 3 = 6, 3 \cdot 3 \cdot 3 \cdot 3 = 6 \cdot 3 = 4, 4 \cdot 3 = 5, 5 \cdot 3 = 1$$

Die 2 ist dagegen kein erzeugendes Element, weil $2 \cdot 2 \cdot 2 = 1$ gilt.

(c) Bei $(\mathbb{Z}, +, 0)$ mit erzeugendem Element 1 ist die Sache etwas anders. Um die 0 zu bekommen, muss man die leere Summe zulassen, und um die negativen Zahlen zu

bekommen, muss man noch das Inverse -1 von 1 nehmen und Summen von (-1)en zulassen. Und: „Im Kreis herum“ geht hier natürlich gar nichts. (Der Unterschied ist, dass $\mathbb{Z}$ unendlich ist, die Gruppen in (a) und (b) aber endlich sind.)

Es sei $(G, \circ, e)$ eine beliebige Gruppe.

Für $a \in G$ definieren wir:

$$\langle a \rangle := \bigcap \{H \mid H \text{ ist Untergruppe von } G \text{ und } a \in H\}$$

Man sieht recht leicht ein, dass $\langle a \rangle$ eine Untergruppe ist und dass jede Untergruppe H mit $a \in H$ auch $\langle a \rangle$ als Teilmenge enthält. Man sagt: $\langle a \rangle$ ist „die kleinste Untergruppe von G, die a enthält“, oder $\langle a \rangle$ ist „die von a erzeugte Untergruppe“.

Beispiele: (a) In der Gruppe $(\mathbb{R}^*, \cdot, 1)$, der multiplikativen Gruppe der reellen Zahlen, bedeutet a^i die gewöhnliche i-te Potenz. (Auch 0^i ist für $i \geq 0$ definiert.) Für $a \in \mathbb{R}^* - \{1, -1\}$ sind die Elemente a^i, $i \in \mathbb{Z}$, alle verschieden, und sie bilden $\langle a \rangle$. (Für $a = 2$ bekommt man $\{\ldots, \frac{1}{16}, \frac{1}{8}, \frac{1}{4}, \frac{1}{2}, 1, 2, 4, 8, 16, \ldots\}$.) Dies ist eine echte Untergruppe von $(\mathbb{R}^*, \cdot, 1)$. Ausnahmen sind $a = 1$ und $a = -1$, weil $\langle 1 \rangle = \{1\}$ und $\langle -1 \rangle = \{1, -1\}$.

(b) In der Gruppe $(\mathbb{Z}, +, 0)$, der additiven Gruppe der ganzen Zahlen, gilt $\langle a \rangle = \{\ldots, -3a, -2a, -a, 0, a, 2a, 3a, \ldots\} = a\mathbb{Z}$, die Menge der Vielfachen von a. Für $a \neq 0$ ist dies eine unendliche Menge. Für $a = 1$ und $a = -1$ ist $\langle a \rangle = \mathbb{Z}$, sonst handelt es sich um echte Untergruppen.

(c) Betrachte die additive Gruppe $(\mathbb{Z}_m, +_m, 0)$ im Ring $\mathbb{Z}_m$. Sei $a \in \mathbb{Z}_m$. Was ist $\langle a \rangle$? Für $m = 30$ ist zum Beispiel $\langle 12 \rangle = \{12, 24, 6, 18, 0\}$. Wie findet man diese Menge allgemein? – Setze $d_a = \mathrm{ggT}(a, m)$. Dann gilt $\langle a \rangle = \{i \cdot d_a \bmod m \mid 0 \leq i < m/d_a\}$, die Menge der Vielfachen von d_a in $\mathbb{Z}_m$. (Man zeigt zunächst, dass $\{i \cdot d_a \bmod m \mid 0 \leq i < m/d_a\}$ eine Untergruppe von $\mathbb{Z}_m$ ist. Das liegt daran, das Addition zweier Vielfacher von d_a modulo m wieder eine solche Zahl liefert, und dass $(m/d_a - i) \cdot d_a$ invers zu $i \cdot d_a$ ist. Dann zeigt man, dass jedes $i \cdot d_a$ als Vielfaches von a modulo m geschrieben werden kann. Das sieht man mit dem Lemma von Bezout ein: Schreibe $d_a = xa + ym$, also $id_a = (ix)a + (iy)m$, also $i \cdot d_a = ((ix) \cdot a) \bmod m$.) Insbesondere gilt $\langle a \rangle = \mathbb{Z}_m$, wenn $a \in \mathbb{Z}_m^*$.

Man kann die Struktur von $\langle a \rangle$ auch ganz leicht „von unten“, durch Aufbau aus a, beschreiben.

Dazu definieren wir Potenzen von a in $(G, \circ, e)$, sowohl positive als auch negative.

$$\begin{aligned} a^0 &:= e; \\ a^i &:= a^{i-1} \circ a, \text{ für } i \geq 1; \\ a^i &:= (a^{-1})^{-i}, \text{ für } i < 0. \end{aligned}$$

Offenbar ist $a^1 = a$, und die Schreibweise a^{-1} ist nicht mehrdeutig.[1]
Anschaulich: $a^i = \underbrace{a \circ \cdots \circ a}_{i\text{-mal}}$, für $i \geq 1$ und $a^i = \underbrace{a^{-1} \circ \cdots \circ a^{-1}}_{(-i)\text{-mal}}$ für $i < 0$.
Man zeigt (ohne Mühe, nur mit etwas Geduld), dass die üblichen Potenzrechenregeln gelten:

$$\begin{aligned} a^i \circ a^j &= a^{i+j}, \text{ für } i, j \in \mathbb{Z}, \\ (a^i)^j &= a^{ij}, \text{ für } i, j \in \mathbb{Z}, \\ (a^i)^{-1} &= a^{-i}, \text{ für } i \in \mathbb{Z}. \end{aligned}$$

Proposition 5.1
$\langle a \rangle = \{a^i \mid i \in \mathbb{Z}\}$.

(Setze $A = \{a^i \mid i \in \mathbb{Z}\}$. Dann ist A eine Untergruppe von G, die a enthält. Andererseits muss jede Untergruppe, die a als Element hat, alle a^i, $i \in \mathbb{Z}$, enthalten.)

Definition 5.2
Eine Gruppe $(G, \circ, e)$ heißt *zyklisch*, wenn es ein $a \in G$ mit $G = \langle a \rangle$ gibt.

Jedes a mit dieser Eigenschaft heißt ein *erzeugendes Element* von G.

Beispiele: (a) $(\mathbb{R}^*, \cdot, 1)$ ist nicht zyklisch.

(b) $(\mathbb{Z}, +, 0)$ ist zyklisch, da $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$ gilt.[2] Die Elemente von $\mathbb{Z} - \{-1, 1\}$ sind keine erzeugenden Elemente.

[1] Wenn die Gruppe *additiv* als $(G, \oplus, 0)$ geschrieben ist, definiert man $0a = 0$, ia für $a \oplus \cdots \oplus a$ mit $i \geq 1$ Summanden, ia für $(-a) \oplus \cdots \oplus (-a)$ mit $-i$ Summanden, für $i \leq -1$. Man spricht von „Vielfachen“ von a, nicht von Potenzen. Die strukturellen Überlegungen hängen natürlich nicht von der Schreibweise ab.

[2] Diese sehr wichtige Gruppe fällt in die Kategorie „zyklisch“, obwohl nirgendwo ein Kreis erkennbar ist.

(c) $(\mathbb{Z}_m, +_m, 0)$ ist zyklisch, da $\mathbb{Z}_m = \langle 1 \rangle$ gilt. Allgemeiner gilt: $\mathbb{Z}_m = \langle a \rangle$ für beliebige $a \in \mathbb{Z}_m^*$. Erzeugende Elemente sind also die a mit $\mathrm{ggT}(a, m) = 1$.

Beispiel: In $\mathbb{Z}_9$ ist 2 ein erzeugendes Element, weil die Vielfachen von 2 die folgenden Elemente sind:

$$2, 4, 6, 8, 10 \equiv_9 1, 1 + 2 = 3, 3 + 2 = 5, 5 + 2 = 7, 7 + 2 = 9 \equiv_9 0.$$

(d) $(\{0,1\}^k, \oplus_k, 0^k)$ ist für $k \geq 2$ nicht zyklisch, da alle Elemente dieser Gruppe $a \oplus_k a = 0^k$ erfüllen.

(e) $(\{0,1\}^k, +_{2^k}, 0^k)$, wobei die Operation $+_{2^k}$ die Addition von Zahlen in Binärdarstellung modulo 2^k bedeutet, ist eine zyklische Gruppe (nach (c)).

Wir halten fest, dass die Beispiele (b) und (c) insofern typisch sind, als jede zyklische Gruppe so aussieht wie eines dieser Beispiele.

Fakt 5.3
(i) Sei $(G, \circ, e)$ eine endliche zyklische Gruppe, mit $m = |G|$ und $G = \langle a \rangle$. Dann ist die Potenzfunktion $p\colon \mathbb{Z}_m \ni i \to a^i \in G$ ein Isomorphismus.
(ii) Sei $(G, \circ, e)$ eine unendliche zyklische Gruppe, mit $G = \langle a \rangle$. Dann ist die Potenzfunktion $p\colon \mathbb{Z} \ni i \to a^i \in G$ ein Isomorphismus.

(Der Beweis geht in etwa folgendermaßen: Man definiert die Potenzfunktion $p_a\colon \mathbb{Z} \ni i \mapsto a^i \in G$. Wenn diese Abbildung injektiv ist, sind wir in Fall (ii). Wenn die Abbildung nicht injektiv ist, dann gibt es Exponenten $i < j$ mit $a^i = a^j$. Daraus folgt $a^{j-i} = a^j \circ a^{-i} = a^j \circ (a^i)^{-1} = e$. Es sei dann $m := \min\{k \geq 1 \mid a^k = e\}$. Dann gilt $m \mid (j - i)$ (sonst wäre $m' = (j - i) \bmod m$ eine Zahl mit $0 < m' < m$ und $a^{m'} = e$). Man erhält $a^i = a^{i \bmod m}$ für alle $i \in \mathbb{Z}$ und $G = \{e, a, a^2, \ldots, a^{m-1}\}$. Dies ist Fall (i). Dies ist der Fall, in dem die wiederholte Multiplikation mit a schließlich „im Kreis herum“ führt.)

In unserer Vorlesung wird es hauptsächlich um *endliche* zyklische Gruppen, also Fall (i), gehen. Man beachte, dass der Isomorphismus zwischen $\mathbb{Z}_m$ und G nicht eindeutig ist, da man jedes beliebige erzeugende Element a von G benutzen kann. (Man sagt, der Isomorphismus ist „nicht kanonisch“.) Weil in $\mathbb{Z}_m$ genau die Zahlen i mit $\mathrm{ggT}(i, m) = 1$ erzeugende Elemente sind, sind in G genau die Elemente a^i, $i \in \mathbb{Z}_m^*$, erzeugende Elemente.

Beispiel: Wir betrachten $\mathbb{Z}_{11}^* = \{1, \ldots, 10\}$ mit Multiplikation modulo 11. Die Potenzen $6^i \bmod 11$ sind, für $i = 0, 1, \ldots, 9$:

i	0	1	2	3	4	5	6	7	8	9
6^i (in $\mathbb{Z}_{11}^*$)	1	6	3	7	9	10	5	8	4	2

Weil diese 10 Potenzen von 6 die Menge $\mathbb{Z}_{11}^*$ ausschöpfen, ist 6 ein erzeugendes Element von $\mathbb{Z}_{11}^*$. Weil 1, 3, 7, 9 zu 10 teilerfremd sind, sind die erzeugenden Elemente von $\mathbb{Z}_{11}^*$ gerade $6^1 = 6$, $6^3 = 7$, $6^7 = 8$ und $6^9 = 2$.

Damit man mit einer zyklischen Gruppe in der Kryptographie etwas anfangen kann, muss sie einige algorithmische Bedingungen erfüllen:

(i) Darstellung der Elemente: Für jedes Element muss es eine Darstellung geben, die der Bearbeitung im Rechner zugänglich ist. (Dies können Wörter über einem endlichen Alphabet sein, Bitstrings, ganze Zahlen, usw.) Es muss einen effizienten Algorithmus geben, der korrekte Darstellungen von fehlerhaften unterscheidet („Syntaxcheck“).

(ii) Effizienz der Operationen: Es muss effiziente Algorithmen geben, die zu gegebenen Elementen a und b das Produkt $a \circ b$ und zu gegebenem a das inverse Element a^{-1} berechnet.

(iii) Es muss effizient möglich sein, ein erzeugendes Element der Gruppe zu finden, oder ein solches Element muss bekannt sein.

(iv) Die Kardinalität m der Gruppe muss effizient berechenbar (oder bekannt) sein.

Wenn Bedingung (ii) gilt, folgt die Effizienz einer weiteren sehr wichtigen Operation, nämlich die der Potenzierung.

Beobachtung 5.4
Wenn $(G, \circ, e)$ eine zyklische Gruppe ist, die (i) und (ii) erfüllt, dann ist die Potenzierungsoperation $(a, i) \mapsto a^i$, für $a \in G$ und $i \in \mathbb{Z}$, effizient ausführbar (nämlich mit $2\lceil \log|i| \rceil$ Gruppenoperationen).

(Falls $i \geq 0$, benutzt man den bekannten Algorithmus für die schnelle Exponentiation aus Kapitel 4. Falls $i < 0$, berechnet man zuerst a^{-1} und benutzt dann schnelle Exponentiation.)

Multiplikative Gruppen in endlichen Körpern

Wir wissen, dass $\mathbb{Z}_p$ ein endlicher Körper ist, für jede Primzahl p. Wir interessieren uns für die multiplikative Gruppe $(\mathbb{Z}_p^*, \cdot_p, 1)$. (Mit $\cdot_p$ ist dabei die Multiplikation modulo p gemeint, natürlich eingeschränkt auf $\mathbb{Z}_p^*$.)

Beispiel: In der Gruppe $\mathbb{Z}_{13}^* = \{1, 2, \ldots, 12\}$ ist 2 ein erzeugendes Element, wie man aus Abb. 1 entnehmen kann, die die Potenzen $2^0, 2^1, \ldots, 2^{11}$ auflistet. Damit ist $\mathbb{Z}_{13}^*$ eine zyklische Gruppe.

i	0	1	2	3	4	5	6	7	8	9	10	11	(12)
2^i	1	2	4	8	3	6	12	11	9	5	10	7	(1)

Abbildung 1: Die Potenzen 2^i mod 13 für $i = 0, 1, \ldots, 12$. Das Element 2 erzeugt die multiplikative Gruppe $\mathbb{Z}_{13}^*$.

In diesem Extra-Abschnitt **(nicht prüfungsrelevant)** wollen wir zeigen, dass für *jeden* endlichen Körper $\mathbb{F}$ die multiplikative Gruppe $\mathbb{F}^*$ zyklisch ist.

Man erinnere sich an die Definition

$$\varphi(m) := |\mathbb{Z}_m^*| = |\{i \mid 0 \leq i < m, \mathrm{ggT}(i, m) = 1\}|$$

der Eulerschen φ-Funktion. Wir nehmen auch von dem Sonderfall $\varphi(1) = 1$ Notiz. Es gilt ja $\mathrm{ggT}(0, 1) = 1$. Da $\mathrm{ggT}(0, m) = m$ für alle m, haben wir $\varphi(m) < m$ für alle $m \geq 2$.

Beispiel: Wir betrachten die Teiler $1, 2, 3, 4, 6, 12$ von $N = 12$ und summieren ihre φ-Werte:

$$\varphi(1) + \varphi(2) + \varphi(3) + \varphi(4) + \varphi(6) + \varphi(12) = 1 + 1 + 2 + 2 + 2 + 4 = 12 = N.$$

Diese Gleichheit ist kein Zufall, wie die folgende (zunächst recht erstaunliche) Feststellung zeigt.

Proposition 5.5
Für beliebige $N \geq 1$ gilt

$$\sum_{d \mid N} \varphi(d) = N.$$

Beweis. Die Idee ist es, die N Brüche

$$\frac{0}{N}, \frac{1}{N}, \frac{2}{N}, \frac{3}{N}, \ldots, \frac{N-1}{N}$$

in gekürzter Form zu betrachten.

Im *Beispiel* $N = 12$ erhalten wir aus

$$\frac{0}{12}, \frac{1}{12}, \frac{2}{12}, \frac{3}{12}, \frac{4}{12}, \frac{5}{12}, \frac{6}{12}, \frac{7}{12}, \frac{8}{12}, \frac{9}{12}, \frac{10}{12}, \frac{11}{12}$$

die gekürzten Versionen

$$\frac{0}{1}, \frac{1}{12}, \frac{1}{6}, \frac{1}{4}, \frac{1}{3}, \frac{5}{12}, \frac{1}{2}, \frac{7}{12}, \frac{2}{3}, \frac{3}{4}, \frac{5}{6}, \frac{11}{12}.$$

Wir gruppieren nach gleichen Nennern:

$$\frac{0}{1}; \qquad \frac{1}{2}; \qquad \frac{1}{3}, \frac{2}{3}; \qquad \frac{1}{4}, \frac{3}{4}; \qquad \frac{1}{6}, \frac{5}{6}; \qquad \frac{1}{12}, \frac{5}{12}, \frac{7}{12}, \frac{11}{12}$$

und beobachten, dass es nach dem Kürzen für jeden Teiler d von $N = 12$ genau $\varphi(d)$ viele Brüche mit Nenner d gibt, nämlich die, deren Zähler i kleiner als d ist und zu d teilerfremd ist. Das gilt offenbar nicht nur für die Teiler von $N = 12$, sondern für beliebige N. Da wir mit N Brüchen begonnen haben, folgt $\sum_{d \mid N} \varphi(d) = N$. □

Wir benötigen den folgenden Spezialfall der allgemeinen Aussage, dass in Körpern ein Polynom vom Grad $k \geq 1$ nicht mehr als k Nullstellen haben kann.

Fakt 5.6
Wenn $\mathbb{F}$ ein (endlicher) Körper ist, dann hat für $k \geq 1$ die Gleichung $X^k = 1$ in $\mathbb{F}$ höchstens k verschiedene Lösungen.

Beweis. (Skizze.) Hier geht es um die Anzahl der Nullstellen des Polynoms $X^k - 1$ mit Grad k. Wenn $a_1, \ldots, a_t$ beliebige t verschiedene Nullstellen sind, dann kann man $X^k - 1 = (X - a_1) \ldots (X - a_t) g(X)$ schreiben, für ein Polynom $g(X) \neq 0$. (Das müsste man natürlich extra beweisen.) Die rechte Seite ist ein Polynom vom Grad $\geq t$, also muss $k \geq t$ sein. □

Nun betrachten wir einen beliebigen endlichen Körper $\mathbb{F}$ mit q Elementen. Die multiplikative Gruppe $(\mathbb{F} - \{0\}, \cdot\,|_{\mathbb{F}-\{0\}}, 1)$ nennen wir $\mathbb{F}^*$. Sie hat $N = q - 1$ Elemente.

Definition 5.7
Für $b \in \mathbb{F}$ definiere $\mathrm{ord}_{\mathbb{F}}(b) := \min\{i \mid b^i = 1\}$, die *Ordnung* von b in $\mathbb{F}$.

Dies ist eine Standarddefinition der Gruppentheorie, die mit Körpern gar nichts zu tun hat. Wie wir oben gesehen haben, ist $\mathrm{ord}_{\mathbb{F}}(b)$ die Kardinalität der zyklischen Gruppe $\langle b\rangle = \{b^i \mid i \in \mathbb{Z}\}$. Eines der ersten Ergebnisse der Gruppentheorie ist, dass in jeder endlichen Gruppe G die Kardinalität einer Untergruppe H von G ein Teiler von $|G|$ ist. In unserem Fall heißt das, dass $|\langle b\rangle| = \mathrm{ord}_{\mathbb{F}}(b)$ ein Teiler von N ist, für jedes $b \in \mathbb{F}^*$.

Wir gruppieren die Elemente von $\mathbb{F}^*$ nach ihrer Ordnung:

$$B_d := \{b \in \mathbb{F}^* \mid \mathrm{ord}_{\mathbb{F}}(b) = d\}, \text{ für } d \mid N.$$

Weil jedes $b \in \mathbb{F}^*$ eine Ordnung hat, gilt

$$\bigcup_{d \mid N} B_d = \mathbb{F}^*, \text{ also } \sum_{d \mid N} |B_d| = N. \tag{1}$$

Beispiel: In Abb. 2 sind die Ordnungen der Elemente $1, 2, \ldots, 12$ in $\mathbb{Z}_{13}^*$ angegeben. (Man probiere einfach aus: $(9^0, 9^1, 9^2, 9^3) = (1, 9, 3, 1)$, usw.) Wir erhalten: $B_1 = \{1\}$, $B_2 = \{12\}$, $B_3 = \{3, 9\}$, $B_4 = \{5, 8\}$, $B_6 = \{4, 10\}$, $B_{12} = \{2, 6, 7, 11\}$. Man kontrolliert nun leicht nach, dass $|B_d| = \varphi(d)$ gilt, für alle Teiler d von $N = 12$.

b	1	2	3	4	5	6	7	8	9	10	11	12
$\mathrm{ord}_{\mathbb{Z}_{13}}(b)$	1	12	3	6	4	12	12	4	3	6	12	2

Abbildung 2: Die Ordnungen der Elemente der multiplikativen Gruppe $\mathbb{Z}_{13}^*$.

Der entscheidende Schritt ist es zu zeigen, dass diese etwas erstaunliche Beobachtung nicht nur im Beispiel, sondern für alle endlichen Körper $\mathbb{F}$ gilt.

Lemma 5.8
Sei $\mathbb{F}$ endlicher Körper. Dann gilt für jeden Teiler d von $N = |\mathbb{F}| - 1$:

$$B_d = \emptyset \text{ oder } |B_d| = \varphi(d).$$

Beweis. Wenn $B_d = \emptyset$ gilt, sind wir fertig. Also können wir $B_d \neq \emptyset$ annehmen. Wir wählen irgendein $b \in B_d$. Aus der Definition von B_d folgt, dass $\langle b\rangle = \{b^0, b^1, b^2, \ldots, b^{d-1}\}$ eine Menge von d Elementen ist, die mit der Operation $\cdot_d$ und neutralem Element 1 eine zyklische Gruppe bildet. Für ein beliebiges Element b^i, $0 \leq i < d$, dieser Menge gilt:

$$(b^i)^d = (b^d)^i = 1^i = 1.$$

Das bedeutet, dass jedes dieser Elemente b^i eine Lösung der Gleichung $X^d = 1$ ist. Nach Fakt 5.6 gibt es in $\mathbb{F}$ höchstens d solche Lösungen. Daraus folgt, dass $\langle b\rangle$ genau die Menge aller Lösungen der Gleichung $X^d = 1$ ist. Weil jedes Element von B_d eine Lösung von $X^d = 1$ ist, folgt weiterhin $B_d \subseteq \langle b\rangle$.

Um $|B_d|$ zu bestimmen, müssen wir also nur die Elemente in $\langle b\rangle$ zählen, die Ordnung d haben. Dies sind genau die erzeugenden Elemente der Gruppe $\langle b\rangle$. Wie wir oben festgestellt haben, ist $(\langle b\rangle, \cdot_d, 1)$ isomorph zu $(\mathbb{Z}_d, +_d, 0)$. Die letztere Gruppe hat genau die Elemente von $\mathbb{Z}_d^*$ als erzeugende Elemente, und das sind $\varphi(d)$ viele. Daraus folgt $|B_d| = \varphi(d)$. □

Um dieses Lemma zu veranschaulichen, betrachten wir für $\mathbb{F} = \mathbb{Z}_{13}$ und $N = 12$ das Element 10 aus B_6. Die ersten sechs Potenzen von 10 modulo 13 sind: $1, 10, 9, 12, 3, 4$. Diese sechs Zahlen erfüllen alle die Gleichung $X^6 = 1$, sind also alle Lösungen dieser Gleichung, weil es in $\mathbb{Z}_{13}$ nicht mehr als sechs solche Lösungen geben kann. Der Beweis folgert nun, dass $B_6 \subseteq \{1, 10, 9, 12, 3, 4\}$ gilt, was man aus Abb. 2 auch direkt abliest. Man sieht auch, dass die Elemente von B_6 die Potenzen 10^1 und 10^5 sind, entsprechend der Tatsache, dass $\mathbb{Z}_6^* = \{1, 5\}$ gilt.

Satz 5.9
Für jeden endlichen Körper $\mathbb{F}$ ist die multiplikative Gruppe $\mathbb{F}^*$ zyklisch.

Beweis. Nach (1) und Prop. 5.5 gilt

$$\sum_{d\,|\,N} |B_d| = N = \sum_{d\,|\,N} \varphi(d).$$

Mit Lemma 5.8 folgt, dass für jeden Teiler d von N die Gleichheit $|B_d| = \varphi(d)$ gelten muss. Das heißt insbesondere, dass $|B_N| = \varphi(N)$ gilt, dass es also in $\mathbb{F}^*$ genau $\varphi(N)$ viele Elemente der Ordnung N gibt. Alle diese Elemente (und nur diese) sind erzeugende Elemente der zyklischen Gruppe $\mathbb{F}^*$. □

In unserem Beispiel sind $2, 6, 7, 11$ die vier erzeugenden Elemente von $\mathbb{Z}_{13}^*$. Dass 2 erzeugendes Element ist, sieht man aus Abb. 1. Wegen $\mathbb{Z}_{12}^* = \{1, 5, 7, 11\}$ sind dann die anderen erzeugenden Elemente $2^5 = 6$, $2^7 = 11$ und $2^{11} = 7$ (in $\mathbb{Z}_{13}$ gerechnet).

Kommentar zum Beweis: Man bemerkt, dass das erzeugende Element *nicht konstruktiv erzeugt* wird, sondern dass „nur“ mit einem Kardinalitätsargument gezeigt wird, dass $|B_N| = \varphi(N)$ gilt, also B_N nicht die leere Menge sein kann. Tatsächlich ist es im

Allgemeinen ein (für die Kryptographie sehr relevantes) nicht triviales Problem, ein erzeugendes Element der multiplikativen Gruppe eines Körpers zu finden.

Wir diskutieren dies noch etwas genauer, und zerlegen das Problem dazu in zwei Teilprobleme. Das erste Teilproblem ist die (effiziente) Erkennung von erzeugenden Elementen. Wenn man hierfür einen Algorithmus hat, kann man noch nach der Dichte von erzeugenden Elementen in $\mathbb{F}^*$ fragen, und ob eine randomisierte Suche erfolgversprechend ist.

Erkennungsalgorithmen

Sei $\mathbb{F}$ ein Körper mit q Elementen. (Wir wissen, dass $q = p^r$ gilt für eine Primzahl p und ein $r \geq 1$.) Sei $N = q - 1 = |\mathbb{F}^*|$.

Lemma 5.10
Ein Element b ist ein erzeugendes Element von $\mathbb{F}^*$ genau dann, wenn $b^{N/s} \neq 1$ für alle Primteiler s von N.

Beweis. „⇒“: Sei $b^{N/s} = 1$ für einen Primteiler s von N. Weil $N/s < N$, ist b kein erzeugendes Element.

„⇐“: Nun nehmen wir an, dass b kein erzeugendes Element ist. Wähle ein kleinstes i mit $1 \leq i < N$ und $b^i = 1$. Die Menge $\langle b \rangle = \{b^0 = 1, b^1 = b, b^2, \ldots, b^{i-1}\}$ ist eine echte Untergruppe von $\mathbb{F}^*$, also ist ihre Kardinalität i ein echter Teiler von N. Sei s ein Primteiler von N/i. Dann gilt $b^{N/s} = (b^i)^{(N/i)/s} = 1$. □

Das Lemma liefert dann einen effizienten Test für „ist b ein erzeugendes Element?“, wenn die Primfaktoren von N bekannt sind. Man kommt also auf das Problem, $N = q - 1$ zu faktorisieren, was im allgemeinen Fall als schwierig gilt.

Ein naheliegender Ausweg ist es, eine Primzahl p und die Faktorisierung von $N = p-1$ gemeinsam herzustellen. Man betrachtet dazu eine (kleine) Zahl $r \geq 2$ und fragt nach einer Primzahl s, so dass $p = rs+1$ ebenfalls Primzahl ist. Dann ist die Primfaktorzerlegung von $N = rs$ bekannt. (Dieser Ansatz wird in einer Übungsaufgabe bearbeitet.)

Dichte der erzeugenden Elemente

Nun wenden wir uns der Frage zu, wie viele erzeugende Elemente es in $\mathbb{F}^*$ gibt. Im Beweis von Satz 5.9 wurde gezeigt, dass dies genau $\varphi(N)$ viele sind. Auf der Seite `https://en.wikipedia.org/wiki/Euler%27s_totient_function#Growth_rate`

findet man die relevante Information:

$$\varphi(N) > \frac{N}{e^\gamma \log\log N + \frac{3}{\log\log N}}, \text{ für } N > 2,$$

wobei $e^\gamma \approx 1.78107$ eine Konstante ist. Also ist $\varphi(N) = \Omega(N/\log\log N)$. Wenn man also ein Element von $\mathbb{F}^*$ zufällig wählt, ist die Wahrscheinlichkeit, ein erzeugendes Element zu erwischen (was man bei bekannter Primzahlzerlegung von N mit dem obigen Kriterium testen kann), mindestens $\Omega(1/\log\log N)$. Bei Misserfolg wiederholt man die zufällige Wahl. Nach erwartet $O(\log\log N)$ Versuchen hat man ein erzeugendes Element gefunden (fehlerfrei, weil der Test fehlerfrei ist).