Für $m \in \{0, \dots, n-1\}$ schreiben wir m für $[m]_n$

Def: Sei $p \in \mathbb{P}$ und $a \in (\mathbb{Z}/p\mathbb{Z})^\times$

Die Ordnung von a modulo p (bezeichnet $\mathrm{ord}_p(a)$ oder $\mathrm{ord}(a)$) ist die kleinste Zahl $n \in \mathbb{N}^+$ mit $a^n = 1$ (d.h. $a^n \equiv 1 \bmod p$)

a heisst eine primitive Wurzel modulo p wenn $\mathrm{ord}(a) = p-1$.

Bemerkung: Wegen dem kleinen Fermatschen Satz ist $a^{p-1} = 1$
also ist $p-1$ die maximale Ordnung.

Lemma 4.7: Sei $a \in (\mathbb{Z}/p\mathbb{Z})^\times$ und $n \in \mathbb{N}$

$$a^n = 1 \iff \mathrm{ord}_p(a) \mid n$$

insbesondere gilt $\mathrm{ord}(a) \mid p-1$

Beweis: Aufgabe

Gibt es primitive Wurzeln?

Lemma 4.8: Sei $d \in \mathbb{N}^+$ mit $d \mid p-1$ und sei $r(d)$ die Anzahl der primen Restklassen modulo p der Ordnung d.
Dann ist $r(d) = 0$ oder $\phi(d)$

Beweis (-Skizze): Wenn $r(d) \neq 0$, sei a eine prime Restklasse der Ordnung d modulo p.

Dann ist a eine Nullstelle von $X^d - 1$ modulo p, und $a^2, a^3, \ldots, a^d$ alle auch, und alle verschieden.

Aber $X^d - 1$ hat nur höchstens d Nullstellen $\rightarrow$ müsste bewiesen werden!

also sind $a, a^2, \ldots, a^d$ die einziger Nullstellen

Wenn $(i,d) > 1$, dann ist

$$(a^i)^{\frac{d}{(i,d)}} = (a^d)^{\frac{i}{(i,d)}} = 1$$

also $\operatorname{ord}(a^i) \leq \frac{d}{(i,d)} < d$

Wenn $(i,d) = 1$ und $(a^i)^j = a^{ij} = 1$, dann gilt $d \mid ij$ (L. 4.7)

$$\Rightarrow d \mid j \quad (i,d) = 1$$

$$\Rightarrow d \leq j$$

also gilt $\operatorname{ord}(a^i) = d \Leftrightarrow (i,d) = 1$ □

Wir brauchen auch

Lemma 4.9: $\forall n \in \mathbb{N}^+$ ist $\sum_{d \mid n} \phi(d) = n$

Beweis: Übungsaufgabe

Satz 4.10 (Gauß): Sei $d \in \mathbb{N}^+$ ein Teiler von $p-1$

Dann ist $r(d) = \phi(d)$

Insbesondere gibt es genau $\phi(p-1)$ verschiedene primitive Wurzeln modulo p.

Beweis: Es gelt

$$\sum_{d \mid p-1} r(d) = p-1$$

wegen Lemma 4.7 kann d nur dann eine Ordnung einer Restklasse sein, wenn $d \mid p-1$

$$\Rightarrow p-1 = \sum_{d \mid p-1} r(d) \leq \sum_{d \mid p-1} \phi(d) \qquad (L\,4.8)$$

$$= p-1 \qquad (L\,4.9)$$

Weil Gleichheit gilt, ist $r(d) = \phi(d) \quad \forall\, d \mid p-1$ □

Beobachtung: Sei a eine primitive Wurzel modulo p.

Dann ist $\{a, a^2, \ldots, a^{p-1}\} = \{1, 2, \ldots, p-1\}$ (modulo p)

(in einer anderen Reihenfolge)

Eine Anwendung von primitiven Wurzeln

Diffie - Hellman Schlüsselaustausch

(oder Diffie - Hellman - Merkle)

Ein kryptographisches Verfahren, mit dem zwei Benutzer einen gemeinsamen Geheimschlüssel generieren können, auch wenn jede verschickte Nachricht öffentlich lesbar ist.

Grundidee: Farben mischen (trennen ist schwer)

öffentliche Farbe: gelb

Alice	Bob
Geheimfarbe: Rot 	Geheimfarbe: Blau 
Mischen: Orange: 	Grau: 
(öffentlich) verschicken: Grün: 	Orange: 
mit Geheimfarbe mischen: Braun: 	Braun: 

Dritte Person sieht nur gelb, grün und orange, kann Braun nicht richtig herzeugen (wird immer zu gelblich sein.

1. Zwei Benutzer A und B wählen eine (große) Primzahl p,
und eine primitive Wurzel g
p und g sind öffentlich

2. A wählt einen Exponenten a
B wählt einen Exponenten b
a und b bleiben geheim.

3. A verschickt $g^a \bmod p$
B verschickt $g^b \bmod p$

4. A rechnet $(g^b)^a = g^{ab} \bmod p$
B rechnet $(g^a)^b = g^{ab} \bmod p$

$g^{ab} \bmod p$ ist der gemeinsame Geheimschlüssel

5. Um eine Nachricht n zu verschlüsseln, rechne man $n \cdot g^{ab} \bmod p$

6. A rechnet $(g^b)^{p-1-a} = (g^{p-1})^b g^{-ab} = g^{-ab} \bmod p$
B rechnet $(g^a)^{p-1-b} = (g^{p-1})^a g^{-ab} = g^{-ab} \bmod p$

g^{-ab} bleibt geheim

7. Um eine verschlüsselte Nachricht n zu entschlüsseln,
rechne man $n g^{-ab} \bmod p$.

Ist das sicher?

Die Sicherheit des Verfahrens basiert darauf, dass das Diffie-Hellman Problem schwer ist.

d.h. gegeben g, g^a und $g^b \mod p$
berechne $g^{ab} \mod p$.

Mathematiker glauben, dass dieses Problem schwer ist, aber das ist nicht bewiesen.

Es ist höchstens so schwer wie das diskrete-Logarithmen-Problem
d.h. gegeben g und $g^a \mod p$, berechne a.

Der Schwierigkeitsgrad dieses Problems ist auch nicht bekannt.

Primzahltests

Wir haben gesehen: $p \in \mathbb{P}, (a,p)=1 \Rightarrow a^{p-1} \equiv 1 \mod p$.

Äquivalent ist: $\exists\, a \in \mathbb{Z}, (a,n)=1$ sodass $a^{n-1} \not\equiv 1 \mod n \Rightarrow n \notin \mathbb{P}$

Kann man das als Primzahltest hernehmen.

Def: Eine Zahl $n>1$ heisst eine <u>Carmichaelzahl</u> wenn

(i) $n \notin \mathbb{P}$

(ii) $a^{n-1} \equiv 1 \mod n \quad \forall a \in \mathbb{Z}$ mit $(a,n)=1$.

Lemma 4.11 (Carmichael 1912): Es gibt Carmichaelzahlen.

Beweis: Übungsaufgabe

Satz 4.12 (Korselt 1899): Eine Zahl n mit Primfaktorzerlegung $n = q_1 \cdots q_k$ ist eine Carmichaelzahl genau dann wenn

(i) $k \geq 2$

(ii) n ist quadratfrei (d.h. $q_i \neq q_j$ für $i \neq j$)

(iii) $q_i - 1 \mid n-1 \quad \forall\, 1 \leq i \leq k$

Beweis: Nächstes Mal.

Satz 4.13 (Alford, Granville, Pomerance 1993):

Es gibt unendlich viele Carmichaelzahlen

(asymptotisch $\geq n^{2/7}$ unterhalb n)