WiSe'21/'22, hhu
K. Halupczok

Vorlesung Einführung in die Zahlentheorie

EZ7: Modulare Potenzen

Stichworte: Potenzrechnung mod m, schnelles Potenzieren, Satz von Euler(-Fermat)/Eulerkongruenz, Kleiner Satz von Fermat/Fermatkongruenz, Eulersche φ-Funktion, Ordnung

---

7.1. Einleitung: In $\mathbb{Z}/m$ kann es nur endlich viele Potenzen $\underline{a}^j$ von $\underline{a} \in \mathbb{Z}/m$ geben, wenn $j \in \mathbb{Z}$, und auch nur endlich viele "modulare" Quadrate, Kuben, ... n-te Potenzen. Dies führt zur Euler-(Fermat)kongruenz und zum Ordnungsbegriff. Modulare Potenzen können darüberhinaus durch "schnelles Potenzieren" effektiv und schnell ausgerechnet werden.

7.2. Vereinbarung: Sei $m \in \mathbb{N}$ ein fester Modul, betrachte $\mathbb{Z}/m\mathbb{Z}$.

7.3. Def.: Sei $\underline{a} \in \mathbb{Z}/m\mathbb{Z}$, $n \in \mathbb{N}$. Dann heißt $\underline{a}^n := \underbrace{\underline{a} \cdots \underline{a}}_{n \text{ mal}} = \underline{a^n}$ die n-te Potenz von $\underline{a}$ (in $\mathbb{Z}/m\mathbb{Z}$). Die 2-ten Potenzen heißen Quadrate (in $\mathbb{Z}/m\mathbb{Z}$). Jeder Repräsentant von $\underline{a}^n$ heißt n-ter Potenzrest (von a mod m), jeder Repräsentant von $\underline{a}^2$ heißt quadratischer Rest (von a mod m).
Setzen auch $\underline{a}^0 := \underline{1}$ und $\underline{a}^{-n} := (\underline{a}^{-1})^n$, falls $a \in (\mathbb{Z}/m\mathbb{Z})^*$, d.h. $(a,m)=1$, so dass das Inverse $\underline{a}^{-1}$ von $\underline{a}$ existiert.

7.4. Lemma (modulare Potenzgesetze): Für alle $\underline{a}, \underline{b} \in \mathbb{Z}/m\mathbb{Z}$, $k, l \in \mathbb{N}_0$ gilt:
(1) $\underline{a}^k \cdot \underline{a}^l = \underline{a}^{k+l}$, (2) $(\underline{a}^k)^l = \underline{a}^{k \cdot l}$, (3) $(\underline{a} \cdot \underline{b})^k = \underline{a}^k \cdot \underline{b}^k$.
Sind $\underline{a}, \underline{b} \in (\mathbb{Z}/m\mathbb{Z})^*$, gelten die Gesetze auch mit $k, l \in \mathbb{Z}$.

Bew.: Klar, die Potenzgesetze in $\mathbb{Z}$ übertragen sich mod m. □

7.5. Bem.: Auch andere Rechenregeln übertragen sich, z.B. die binomischen Formeln
$(\underline{a} \pm \underline{b})^2 = \underline{a}^2 \pm 2\underline{a}\underline{b} + \underline{b}^2$, $\underline{a}^2 - \underline{b}^2 = (\underline{a} - \underline{b})(\underline{a} + \underline{b})$, $(\underline{a} + \underline{b})^n = \sum_{k=0}^{n} \binom{n}{k} \underline{a}^k \underline{b}^{n-k}$,
und z.B. $(-1) \cdot (-1) = +1$, denn $(-1 + m\cdot\mathbb{Z}) \cdot (-1 + m\mathbb{Z}) = (-1)^2 + m\mathbb{Z} = 1 + m\mathbb{Z}$.

7.6. Bem.: Modulare Potenzen können besonders effizient berechnet werden.
1. Bsp.: Was ist $\underline{g}^8$ in $\mathbb{Z}/100\mathbb{Z}$? Man muss nicht erst umständlich $g^8 = 43\,046\,721$ ausrechnen, um auf $\underline{g}^8 = \underline{21}$ zu schließen. Wegen $\underline{g}^8 = \underline{g}^{2^3} = \underline{g}^{2\cdot 2\cdot 2} = (((\underline{g})^2)^2)^2$ reicht dreimaliges Quadrieren: $\underline{g}^2 = \underline{81} = \underline{-19}$, dann $(\underline{81})^2 = (\underline{-19})^2 = \underline{361} = \underline{61}$, dann $(\underline{61})^2 = \underline{3721} = \underline{21}$. Mehrfaches Quadrieren klappt für $\underline{a}^k$, wenn $k = 2^l$ eine 2er-Potenz ist (dann also mit l-fachem Quadrieren).

2. Bsp.: Ist d in a^d keine 2er-Potenz, schreibt man d als Summe von Zweierpotenzen (d.h. $d = \sum_{i=0}^{e} b_i 2^i$ mit $b_i \in \{0,1\}$ im Dualsystem zur Basis $g=2$, vgl. 6.27), und rechnet trotzdem effizient, hier mod $m=100$, wie folgt:

- $7^{17} = 7^{1+2^4} = 7^1 \cdot 7^{2^4} = 7 \cdot 1 = 7$, denn $7^2 = 49$, $49^2 = 2401 = 1$.
  Ja, $7^{17} = 232\,630\,513\,987\,207$ hat die beiden Endziffern 07. ✓
- $3^{10} = 3^{2+8} = 3^2 \cdot 3^{2^3} = 9 \cdot 61 = 549 = 49$, denn $3^2 = 9$, $9^2 = 81$, $81^2 = 61$ (s. 1. Bsp.).
- $1011^{100} = 11^{4+32+64} = 11^4 \cdot 11^{2^5} \cdot 11^{2^6} = 41 \cdot 21 \cdot 41 = 21 \cdot 41^2 = 21 \cdot 81 = 1$,
  denn $11^2 = 121 = 21$, $11^4 = 21^2 = 441 = 41$, $11^8 = 41^2 = 1681 = 81$, $11^{16} = 81^2 = 61$,
  $11^{32} = 61^2 = 21$, $11^{64} = 21^2 = 41$.

Die Reduktion mod m nach jeder Multiplikation hält die Repräsentanten stets klein.

7.7. Satz (schnelles Potenzieren): Sei $m \in \mathbb{N}$, $a \in \mathbb{Z}$. Für alle $d \in \mathbb{N}$ ist die Berechnung der modularen Potenz a^d mod m mit höchstens $2 \cdot \log_2(d)$ vielen Multiplikationen in $\mathbb{Z}/m\mathbb{Z}$ möglich.

Bew.: 1. Schritt: Mit höchstens $k := \lfloor \log_2(d) \rfloor$ vielen Multiplikationen (mit Reduktion mod m) berechnet man durch sukzessives Quadrieren

$a^2 = a \cdot a$ (m), $a^{2^2} = a^2 \cdot a^2$ (m), $a^{2^3} = a^{2^2} \cdot a^{2^2}$ (m), ..., $a^{2^k} = a^{2^{k-1}} \cdot a^{2^{k-1}}$ (m).

2. Schritt: Schreiben d zur Basis $g=2$ als $d = \sum_{i=0}^{k} b_i 2^i$ mit $b_i \in \{0,1\}$ für alle $i \le k$.

3. Schritt: Berechne mit maximal (nochmals) k vielen Multiplikationen mod m:

$$a^d = a^{b_0} \cdot a^{2b_1} \cdot a^{2^2 b_2} \cdots a^{2^k b_k} = a^{b_0} \cdot (a^2)^{b_1} \cdot (a^{2^2})^{b_2} \cdots (a^{2^k})^{b_k}$$

Der Rechenaufwand beträgt also maximal $2k \le 2 \cdot \log_2(d)$ viele Multiplikationen. □

7.8. Bem.:
- Anstelle in $\mathbb{Z}/m\mathbb{Z}$ kann in jeder (multiplikativ geschriebenen) Gruppe $(G, \cdot)$ dieses effiziente Berechnungsverfahren für Potenzen genutzt werden. Es heißt auch "Square-and-multiply-Verfahren".
- Schreibt man eine Gruppe $(G,+)$ additiv, geht das Verfahren analog, um Vielfache $d \cdot a := a + \ldots + a$ (d mal) in G effizient berechnen zu können. Es ist dann auch als "Dual-and-add-Verfahren" bekannt.
- Ist d groß, aber verhältnismäßig klein im Vgl. zu m, ist schnelles Potenzieren sehr geeignet. Andernfalls helfen die folgenden Sätze weiter, die daher rühren, dass $\mathbb{Z}/m\mathbb{Z}$ ja endlich ist und sich die Potenzen $a, a^2, a^3, \ldots$ darin wiederholen müssen.

Wir erinnern, dass $\varphi(m) = \#(\mathbb{Z}/m\mathbb{Z})^* = \#\{a \in \{1,\dots,m\};\ (a,m)=1\}$ die Eulersche φ-Fkt. ist. Der folgende Satz von Euler besagt, dass die Folge der Potenzen $a, a^2, a^3, a^4, \dots$ (spätestens) nach $\varphi(m)$ Schritten periodisch wird.

7.9. **Satz** (von Euler (-Fermat)): Für alle $m \in \mathbb{N}$ und $a \in \mathbb{Z}$ mit $(a,m)=1$ gilt $\boxed{a^{\varphi(m)} \equiv 1 \ (m)}$.
auch: Euler-Kongruenz

Bew.: Seien $\{x_1,\dots,x_{\varphi(m)}\}$, $\{y_1,\dots,y_{\varphi(m)}\}$ zwei reduzierte RSe mod m. Nach eventueller Umbenennung gilt $x_j \equiv y_j \ (m)$ für alle $j \le \varphi(m)$, durch Multiplikation folgt $x_1 \cdots x_{\varphi(m)} \equiv y_1 \cdots y_{\varphi(m)} \ (m)$. ⊛ Sei $P := x_1 \cdots x_{\varphi(m)}$. Nach 6.13 kann für $\{y_1,\dots,y_{\varphi(m)}\}$ das red. RS $\{ax_1,\dots,ax_{\varphi(m)}\}$ genommen werden, da $(a,m)=1$. Aus ⊛ wird dann $P \equiv a^{\varphi(m)} \cdot P \ (m)$, und wegen $(P,m)=1$ folgt $1 \equiv a^{\varphi(m)} \ (m)$. □

7.10 **Kor.** (Fermat-Kongruenz, Kleiner Fermatscher Satz): Für $p \in \mathbb{P}$, $a \in \mathbb{Z}$, $p \nmid a$, gilt $a^{p-1} \equiv 1 \ (p)$.

Bew.: Nach 7.9 mit $m=p$, da $\varphi(p) = p-1$ (p prim)
(denn $\#\{a \le p;\ (a,p)=1\} = \#\{1,2,\dots,p-1\} = p-1$). □

7.11. **Bem.:** • Wird in 7.10 nicht $p \nmid a$ vorausgesetzt, wird die Fermat-Kongruenz angegeben als
$a^p \equiv a \ (p)$ für alle $a \in \mathbb{Z}$. [Klar für $p \mid a$, für $p \nmid a$ ist $a \equiv 0$ und die Kongruenz auch klar.]

• Die Euler-Kongruenz ist ein Spezialfall des gruppentheoretischen Satzes (vgl. Algebra A2.18):
Ist $(G,\cdot)$ eine Gruppe, $\#G = n \in \mathbb{N}$, und ist $e \in G$ das neutrale Element in G, so gilt $g^n = e$ für alle $g \in G$. (Hier: Haben $\#(\mathbb{Z}/m\mathbb{Z})^* = \varphi(m)$.)

7.12. **Bem.:** Aufgrund des Satzes von der Euler-(Fermat-) Kongruenz kann in einer modularen Potenz der Exponent stets mod $\varphi(m)$ reduziert werden: $a^{q\varphi(m)+d} = (\underbrace{a^{\varphi(m)}}_{\equiv 1})^q \cdot a^d = a^d$

Bsp.: $m=10$, $\varphi(10)=4$ (da $(\mathbb{Z}/10\mathbb{Z})^* = \{1,3,7,9\}$),
dann ist $3^{21} = 3^{5\cdot 4+1} = (3^4)^5 \cdot 3^1 = 3$ bzw. $3^{21} \equiv 3 \ (10)$.
Zuletzt kann a^d noch mit schnellem Potenzieren berechnet werden.

Somit ist auch die Berechnung von $\varphi(m)$ eine Aufgabe, die am besten vorab erledigt werden sollte. Dabei hilft Satz 7.13.

Die Eulerfunktion φ hat die folgenden Grundeigenschaften.

7.13. Satz: Seien $m,n \in \mathbb{N}$, $(m,n)=1$, $\{x_{1,1},\dots,x_{\varphi(m)}\}$ ein red. RS mod m,
$\{y_{1,1},\dots,y_{\varphi(n)}\}$ ein red. RS mod n.

Seien $p \in \mathbb{P}$, $e_1,\dots,e_r \in \mathbb{N}$, $p_1,\dots,p_r \in \mathbb{P}$ mit $p_1 < p_2 < \dots < p_r$.

Dann: (1) $\{x_j n + y_i m \in \mathbb{Z};\ j \le \varphi(m),\ i \le \varphi(n)\}$
ist ein red. RS mod mn.

(2) $\varphi(mn) = \varphi(m)\varphi(n)$ (d.h. die Fkt. φ ist multiplikativ; dabei muss $(m,n)=1$ vorausgesetzt sein!)

(3) $\varphi(p^a) = p^a - p^{a-1} = p^{a-1}(p-1)$
und $\varphi\left(\prod_{j=1}^{r} p_j^{e_j}\right) = \prod_{j=1}^{r} p_j^{e_j-1}(p_j-1)$.

Beweis (1)&(2):
- Die $\varphi(m)\cdot\varphi(n)$ vielen angegebenen Zahlen sind zu mn teilerfremd.
Hat mn mit $z_{j,i} := x_j n + y_i m$ einen Primteiler p gemeinsam, dann gilt OE $p \mid n$, also $p \mid z_{j,i} - x_j m = y_i m$. Wegen $(y_i, n)=1$ und 1.16(2)(Gauß) folgt $p \mid m$, also $p \mid (m,n)=1$ ↯.
- Die $z_{j,i}$ sind paarweise inkongruent.
Seien $x_j n + y_i m \equiv x_{j'} n + y_{i'} m \mod mn$, wobei $1 \le j,j' \le \varphi(m)$, $1 \le i,i' \le \varphi(n)$.
Dann folgt $m \mid \left((x_j - x_{j'})n + (y_i - y_{i'})m\right)$, also $m \mid (x_j - x_{j'})n$.
Mit $(m,n)=1$ und 1.16(2)(Gauß) ergibt sich $m \mid (x_j - x_{j'})$
bzw. $x_j \equiv x_{j'} \mod m$, das heißt aber $j=j'$. Ebenso folgt $i=i'$.
- Außerdem ist jedes $z \in \mathbb{Z}$ mit $(z, mn)=1$ zu einem der $z_{j,i}$ mod mn kongruent.
Dann nach 3.2 (Bézout) ex. $x',y' \in \mathbb{Z}$ mit $z = x'm + y'm$. Hier muss $(x',m)=(y',n)=1$ sein, da ansonsten $(z, mn) > 1$ wäre.
Es gibt also $j', i' \in \mathbb{Z}$ mit $x' \equiv x_{j'} (m)$, $y' \equiv y_{i'} (n)$,
also $z \equiv (x_{j'} n + y_{i'} m)$ (mn). Dies zeigt (1), (2).

Alternativer Beweis zu (2) mit CRS: Laut CRS ist $\mathbb{Z}/m \times \mathbb{Z}/n \cong \mathbb{Z}/mn$,
also $(\mathbb{Z}/m \times \mathbb{Z}/n)^* = (\mathbb{Z}/m)^* \times (\mathbb{Z}/n)^* \cong (\mathbb{Z}/mn)^*$, und Kardinalitätenvergleich.

(3): Haben $\varphi(p^a) = \#\{a \le p^a;\ p \nmid a\} = \#\{a \le p^a\} - \#\{a \le p^a;\ p \mid a\} = p^a - p^{a-1}$.
Die letzte Formel folgt aus (2) und dem Vorigen. □

Wie das Beispiel $m=9$, $\varphi(9)=9-3=6$, $4^2=\underline{17}$, $4^3=4\cdot 7=\underline{28}=\underline{1}$ zeigt, muss $\varphi(m)$ nicht notwendig die kleinste Periode für die Potenzen eines a mod m sein.

Wir gelangen zum Begriff der Ordnung einer Restklasse $\underline{a}$.

7.14. **Def. (Ordnung):** Sei $m\in\mathbb{N}$, $a\in\mathbb{Z}$ mit $(a,m)=1$.

Dann heißt $\operatorname{ord}_m(a) := \min\{d\in\mathbb{N} \mid a^d\equiv 1\ (m)\}$ die Ordnung von a mod m.

Bem.:
- Nach der Eulerkongruenz gibt es ein solches $d\le\varphi(m)$. Somit ist stets $\operatorname{ord}_m(a)\le\varphi(m)$.
- Der Ordnungsbegriff entspricht dem der Ordnung des Elements $a+m\mathbb{Z}$ in der Gruppe $(\mathbb{Z}/m)^*,\cdot)$.
- Man beachte, dass $\operatorname{ord}_m(a)$ nur für $(a,m)=1$ definiert ist.

7.15. **Lemma (zu Ordnungen):** Seien $m\in\mathbb{N}$, $a\in\mathbb{Z}$, $(a,m)=1$. Dann gilt:

(1) Für alle $j,k\in\mathbb{N}_0$, $j<k\le\operatorname{ord}_m(a)$ gilt $a^j\not\equiv a^k\ (m)$.
(Die Zahlen $a^0, a^1, \dots, a^{\operatorname{ord}_m(a)-1}$ sind paarweise inkongruent mod m.)

(2) Für alle $j,k\in\mathbb{N}_0$ gilt: $a^l\equiv a^k\ (m) \Leftrightarrow l\equiv k\ (\operatorname{ord}_m(a))$.

(3) Insb. gilt für alle $l\in\mathbb{N}_0$: $a^l\equiv 1\ (m) \Leftrightarrow \operatorname{ord}_m(a)\mid l$.

(4) $\operatorname{ord}_m(a)\mid\varphi(m)$.

(5) Sind $n,d\in\mathbb{N}$, $\operatorname{ord}_m(a)=nd$, so folgt $\operatorname{ord}_m(a^n)=d$.

(6) Seien $a_1,a_2\in\mathbb{Z}$ mit $(a_1a_2,m)=1$. Sei $d_1:=\operatorname{ord}_m(a_1)$, $d_2:=\operatorname{ord}_m(a_2)$.
Ist $(d_1,d_2)=1$, so folgt $\operatorname{ord}_m(a_1a_2)=d_1d_2$.

Bew.: Zu (1): Für alle $j,k\in\mathbb{N}$, $j<k\le\operatorname{ord}_m(a)$ und $a^j\equiv a^k\ (m)$ folgt wegen $(a,m)=1$ und Folgerung 6.3 (5), dass $a^{k-j}\equiv 1\ (m)$. Dies ist (wegen $k-j<\operatorname{ord}_m(a)$) ein Widerspruch zur Minimalität von $\operatorname{ord}_m(a)$.

Zu (2): Seien $k,l\in\mathbb{N}_0$. Nach Satz 1.7 (Div. mit Rest) ex. $q,q\in\mathbb{Z}$, $r,s\in\mathbb{N}$, mit $r,s<\operatorname{ord}_m(a)$ und $k=q\operatorname{ord}_m(a)+r$, $l=q\operatorname{ord}_m(a)+s$.

Nach Folgerung 6.3 (3) folgt $a^k=(a^{\operatorname{ord}_m(a)})^q\cdot a^r\equiv 1^q\cdot a^r\equiv a^r\ (m)$

und $a^l=(a^{\operatorname{ord}_m(a)})^q\cdot a^s\equiv 1^q\cdot a^s\equiv a^s\ (m)$.

- Falls $a^k\equiv a^l\ (m)$, folgt $a^r\equiv a^k\equiv a^l\equiv a^s\ (m)$, und mit (1) ergibt sich $r=s$. Aus $a^k\equiv a^l\ (m)$ folgt also $l\equiv k\ (\operatorname{ord}_m(a))$.

• Ist umgekehrt $\ell \equiv k \ (\mathrm{ord}_m(a))$, so ist $r = s$,
und es folgt $a^\ell \equiv a^r \equiv a^s \equiv a^k \ (m)$.

Zu (3): Klar mit $k=0$ in (2).

Zu (4): Nach der Eulerkongruenz ist $a^{\varphi(m)} \equiv 1 \equiv a^0 \ (m)$, mit (3) folgt $\mathrm{ord}_m(a) \mid \varphi(m)$.

Zu (5): Seien $m, d \in \mathbb{N}$, $\mathrm{ord}_m(a) = md$. Sei $t := \mathrm{ord}_m(a^n)$.
Dann gilt $a^{nt} = (a^n)^t \equiv 1 \equiv a^0 \ (m)$.
Mit (3) und $\mathrm{ord}_m(a) = md$ folgt $nt \equiv 0 \ (md)$,
bzw. die Existenz eines $k \in \mathbb{Z}$ mit $nt = mdk$, also ist $t = dk$.
Insbesondere ist $k > 0$, da $t, d > 0$.
Andererseits ist $(a^n)^d = a^{nd} = a^{\mathrm{ord}_m(a)} \equiv 1 \equiv (a^n)^0 \ (m)$,
und mit (2) und $t = \mathrm{ord}_m(a^n)$ folgt $t \mid d$.
Also ist d ein Vielfaches von $t = dk$, was nur mit $k = 1$ möglich ist.
Das heißt aber $d = t = \mathrm{ord}_m(a^n)$.

Zu (6): Sei $e := \mathrm{ord}_m(a_1 a_2)$. Potenziert man die Kongruenz $(a_1 a_2)^e \equiv 1 \ (m)$
mit d_1, so ergibt sich $a_1^{ed_1} \cdot a_2^{ed_1} \equiv 1 \ (m)$.
Wegen $a_1^{ed_1} = (a_1^{d_1})^e \equiv 1^e = 1 \ (m)$ wird daraus $a_2^{ed_1} \equiv 1 \ (m)$.
Nach (2) folgt $d_2 \mid e d_1$, und mit 1.16(2)(Gauß), da $(d_1, d_2) = 1$,
folgt $d_2 \mid e$.
Analog ergibt sich $d_1 \mid e$, und erneut wegen $(d_1, d_2) = 1$ folgt $d_1 d_2 \mid e$.
Aus (2) und $(a_1 a_2)^{d_1 d_2} = (a_1^{d_1})^{d_2} \cdot (a_2^{d_2})^{d_1} \equiv 1^{d_2} \cdot 1^{d_1} = 1 = (a_1 a_2)^0 \ (m)$
folgt umgekehrt $e \mid d_1 d_2$, woraus sich $e = d_1 d_2$ ergibt. □

Als nützliche Verallgemeinerung von 7.15(5) erhalten wir folgendes Lemma.

7.16 **Lemma (Ordnung von Potenzen):** Sei $m \in \mathbb{N}$, $a \in \mathbb{Z}$, $(a, m) = 1$, $j \in \mathbb{Z}$.
Dann gilt $\mathrm{ord}_m(a^j) = \dfrac{\mathrm{ord}_m(a)}{(\mathrm{ord}_m(a), j)}$.

Bew.: Sei $k := \mathrm{ord}_m(a)$, $d := (k, j)$. • Dann ist $(a^j)^{\frac{k}{d}} = (a^{\frac{kj}{d}}) \equiv 1^{\frac{j}{d}} \equiv 1 \ (m)$,
also $\mathrm{ord}_m(a^j) \mid \frac{k}{d}$ nach 7.15(3).

• Und umgekehrt: $1 = (a^j)^{\mathrm{ord}_m(a^j)} \Rightarrow k \,\mathrm{ord}_m(a) \mid j \,\mathrm{ord}_m(a^j) \Rightarrow \frac{k}{d} \mid \frac{j}{d} \mathrm{ord}_m(a^j)$.
Weil $(\frac{k}{d}, \frac{j}{d}) = 1$, folgt mit 1.16(2)(Gauß), dass $\frac{k}{d} \mid \mathrm{ord}_m(a^j)$. □