Stichworte: $\mathrm{ord}(G)$, UG, Satz von Lagrange, $k \cdot a$ in $(G,+)$ und a^k in $(G,\cdot)$, $\langle a\rangle = \{k \cdot a;\ k \in \mathbb{Z}\}$ in $(G,+)$, $\langle a\rangle = \{a^k;\ k \in \mathbb{Z}\}$ in $(G,\cdot)$, $\mathrm{ord}(a) = \#\langle a\rangle$, $a^{\mathrm{ord}(G)} = 1$ in $(G,\cdot)$ ⇝ Euler-Fermat, kleiner Fermat, schnelles Potenzieren, Lösen quadratischer Kongruenzen, faires Münzwurf-Knobeln am Telefon

---

1.1.3 Gruppen

Die Gruppen $(\mathbb{Z}_m, +, 0)$ und $(\mathbb{Z}_m^*, \cdot, 1)$ sind endliche abelsche Gruppen. Wir untersuchen ein paar ihrer allgemeinen Eigenschaften und führen dabei ein paar Grundbegriffe ein.

1.) **Def.:** Die Ordnung einer endlichen Gruppe G ist die Anzahl ihrer Elemente, Kurz: $\mathrm{ord}(G) := \#G$.

2.) **Def.:** Eine Teilmenge H einer Gruppe G mit Verknüpfung $*$ heißt Untergruppe, falls auch $(H, *)$ eine Gruppe ist. Kurz: UG.

3.) **Satz von Lagrange:** Ist $(G, *)$ eine endliche Gruppe, so ist die Ordnung einer Untergruppe H stets ein Teiler von $\mathrm{ord}(G)$.

Bew.: Die Linksnebenklassen $a*H := \{a*h;\ h \in H\}$ für $a \in G$ sind paarweise disjunkt, d.h. stets gilt $a*H = b*H$ oder $a*H \cap b*H = \emptyset$.
(Denn: ist $c \in a*H \cap b*H$, ist $c = a*g = b*h$ für $g, h \in H$, also $a = b*(h*g^{-1})$, somit $a*H = \{a*m;\ m \in H\} = \{b*h*g^{-1}*m;\ m \in H\} = \{b*m;\ m \in H\} = b*H$.)
Also ist G die disjunkte Vereinigung endlich vieler Linksnebenklassen $a_1*H, \ldots, a_r*H$.
Da $\#(a*H) = \#H$ für alle $a \in G$ gilt, folgt mit $\mathrm{ord}(G) = r \cdot \mathrm{ord}(H)$ die Beh. □

4.) **Def.:** Sei $(G, +)$ eine abelsche Gruppe und $a \in G$. Für $k \in \mathbb{Z}$ definieren wir $ka := a + \ldots + a$ (k-mal), falls $k > 0$, $k \cdot 0 := 0$ und $k \cdot a := -(-k)a$ falls $k < 0$.
Dann ist $\langle a\rangle := \{ka;\ k \in \mathbb{Z}\}$ eine UG von G. [Klar!]
Wir nennen $\langle a\rangle$ die von a erzeugte UG bzw. Erzeugnis von a und a einen Erzeuger. Ist $\langle a\rangle$ endliche UG, heißt ihre Ordnung die Ordnung von a, Kurz: $\mathrm{ord}(a) := \#\langle a\rangle$.
Eine Gruppe G mit Erzeuger a, d.h. $G = \langle a\rangle$, heißt zyklisch.

Schreibt man die Gruppe multiplikativ mit Verknüpfung "$\cdot$" ("mal"), so setzt man $a^k := \overbrace{a \cdots a}^{k\text{-mal}}$ falls $k>0$, $a^0 := 1$, $a^k := (a^{(-k)})^{-1}$ falls $k<0$, und $\langle a \rangle := \{a^k ; k \in \mathbb{Z}\}$. Ansonsten ist bis auf Schreibweise die Begrifflichkeit und Theorie zu "Erzeugern" und "Ordnungen" dieselbe.

Nach dem Satz von Lagrange gilt für jede endl. Gruppe G und $a \in G$ stets $\underline{\operatorname{ord}(a) \mid \operatorname{ord}(G)}$.

5.) Bsp.: $\mathbb{Z}/m\mathbb{Z} = \{0, 1, \dots, m-1\}$ ist "die" zyklische Gruppe G mit $\operatorname{ord}(G) = m$. Ist $m = p$ prim, können außer $\{0\}$ und $\mathbb{Z}/p\mathbb{Z}$ keine weiteren UG ex.

6.) Lemma: Sei $(G,+)$ Gruppe, $a \in G$. Es ist $\operatorname{ord}(a)$ die kleinste natürliche Zahl m mit $ma = 0$. Es gilt: $ka = 0 \Leftrightarrow \operatorname{ord}(a) \mid k$.
(Bei multiplikativer Schreibweise: $\operatorname{ord}(a) = \min\{m \in \mathbb{N} ; a^m = 1\}$ und $a^k = 1 \Leftrightarrow \operatorname{ord}(a) \mid k$.)
Bew.: Erster Teil klar, zweiter Teil: "$\Rightarrow$": Falls $k \in \mathbb{N}$ mit $ka = 0$ ist, nehme Division von k durch $\operatorname{ord}(a)$ vor: $k = q \cdot \operatorname{ord}(a) + r$ mit $0 \le r < \operatorname{ord}(a)$. Wegen $0 = ka = q \cdot \underbrace{\operatorname{ord}(a) \cdot a}_{=0} + ra$ folgt $ra = 0$, wegen der Minimalität von $\operatorname{ord}(a)$ also $r = 0$, also $\operatorname{ord}(a) \mid k$.
"$\Leftarrow$": Für $k = m \cdot \operatorname{ord}(a)$ folgt $ka = m \cdot (\underbrace{\operatorname{ord}(a) \cdot a}_{=0}) = 0$. □

7.) Folgerung: $\operatorname{ord}(G) \cdot a = 0$ bzw. multiplikativ: $a^{\operatorname{ord}(G)} = 1$ (da $\operatorname{ord}(a) \mid \operatorname{ord}(G)$ nach Lemma 6.)

8.) Folgerung: Da $\operatorname{ord}((\mathbb{Z}/m\mathbb{Z})^*) = \varphi(m)$, ist $a^{\varphi(m)} \equiv 1 \bmod m$, falls $\underline{\operatorname{ggT}(a,m) = 1}$.
Für p prim: $a^{p-1} \equiv 1 \bmod p$ für $p \nmid a$.
(Korollar aus 7.) "Kleiner Satz von Fermat"

9.) Bem.: Die Kongruenz $a^{\varphi(m)} \equiv 1 \bmod m$, falls $\operatorname{ggT}(a,m) = 1$, heißt auch "Satz von Euler-Fermat". Als Ordnung eines $a \in \mathbb{Z}_m^*$ (Notation: $\operatorname{ord}_m(a)$) kommt also nur ein Teiler von $\varphi(m)$ in Frage.

10.) Bsp.: Haben $\varphi(15) = \varphi(3 \cdot 5) = \varphi(3) \cdot \varphi(5) = 2 \cdot 4 = 8$. Die möglichen Ordnungen von Zahlen a mod 15, wo $\operatorname{ggT}(a,15) = 1$ ist, sind also 1, 2, 4, 8.
Wegen $4^2 = 16 \equiv 1 \ (15)$ ist z.B. $\operatorname{ord}_{15}(4) = 2$. Bei anderen Zahlen muss man u.U. Potenzen mit größeren Exponenten ausrechnen, um die Ordnung zu bestimmen.

Generell stellt sich in Anwendungen die Frage, wie man leicht und schnell (modulare) Potenzen $a^k \bmod m$ mit großem k berechnen kann.
Der Satz von Euler-Fermat erlaubt bereits eine Reduktion von k mod $\varphi(m)$:
Ist $k = q \cdot \varphi(m) + r$ mit $0 \le r < \varphi(m)$, folgt $a^k = a^{\varphi(m)\cdot q + r} = (a^{\varphi(m)})^q \cdot a^r \equiv 1^q \cdot a^r = a^r \bmod m$. Ist aber auch $\varphi(m)$ bzw. r groß, hilft man sich mit folgender Methode des schnellen Potenzierens weiter:

11.) Geg. sei eine Gruppe $(G, \cdot)$, zu berechnen ist für $r \in \mathbb{N}$, $a \in G$ die Potenz $a^r := \underbrace{a \cdots a}_{r\text{-mal}}$ in der Gruppe G.

1. Schritt: Mit höchstens $d := \lfloor \frac{\log r}{\log 2} \rfloor$ vielen Verknüpfungen in G berechne durch sukzessives Quadrieren: a^2, $a^{2^2} = a^4 = (a^2)\cdot(a^2)$, $a^{2^3} = (a^{2^2})\cdot(a^{2^2})$, $a^{2^4} = (a^{2^3})\cdot(a^{2^3})$, …, a^{2^d}

2. Schritt: Schreiben r als Binärzahl: $r = \sum_{i=0}^{d} c_i 2^i$ mit $c_i \in \{0,1\}$.

3. Schritt: Berechnen $a^r = a^{c_0} \cdot a^{2c_1} \cdot a^{2^2 c_2} \cdots a^{2^d c_d} = (a^{c_0}) \cdot (a^2)^{c_1} \cdot (a^{2^2})^{c_2} \cdots (a^{2^d})^{c_d}$
mit maximal d weiteren Verknüpfungen in G.

Somit reichen höchstens $2d = O(\log r)$ viele Anwendungen der Gruppenverknüpfung "$\cdot$".
Bei additiver Schreibweise einer Gruppe $(G, +)$ geht das Verfahren zur Berechnung von $r \cdot a$ analog. Man nennt es dann auch das "dual-and-add"-Verfahren.

12.) Bsp.: $5^{12} = 5^{2^2+2^3} = 5^{2^2} \cdot 5^{2^3}$, modulo 11 rechnen wir: $5^2 \equiv 3\ (11)$, $5^{2^2} \equiv 3^2 \equiv -2\ (11)$, $5^{2^3} \equiv (-2)^2 \equiv 4\ (11)$,
also $5^{12} \equiv (-2)\cdot 4 \equiv 3\ (11)$; geht schneller als $5^{12} = 244140625$ von Hand durch 11 zu teilen bzw. das $\cdot$ auszurechnen… ($\not\equiv 5^{2^3} = 5^{(2^3)} = 5^8 \not\equiv (5^2)^3 = 5^{2\cdot 3} = 5^6$)

Eine Anwendung des Kleinen Fermats

13.) Im Fall $p \equiv 3\ (4)$ prim können wir Lösungen quadratischer Kongruenzen mod p bestimmen: Sei $p = 4k+3$ prim und a mit $p \nmid a$ ein quadratischer Rest mod p, d.h. es ex. ein $b \in \mathbb{Z}$ mit $a \equiv b^2\ (p)$, und wir möchten $\pm b$ mod p ausrechnen können. Nach dem Kleinen Fermat folgt $b^{4k+2} = b^{p-1} \equiv 1\ (p)$.
Es folgt: $(a^{k+1})^2 \equiv (b^2)^{2(k+1)} = b^{(4k+2)+2} \equiv 1 \cdot b^2 \equiv a\ (p)$,
d.h. die Lösungen von $b^2 \equiv a\ (p)$ sind $b = \pm a^{k+1}\ (p)$.
Da $a^{k+1} \not\equiv -a^{k+1}\ (p) \Leftrightarrow 2a^{k+1} \not\equiv 0\ (p)$, gibt es genau 2 Lösungen mod p, die wir etwa im Restsystem $\{0, 1, \dots, p-1\}$ angeben können und mit $\pm a^{k+1}$ mod p berechnen können, z.B. mit dem schnellen Potenzieren.

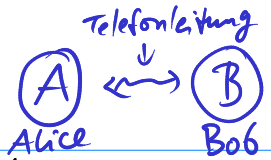
14.) Sei nun n eine zus.gesetzte Zahl, etwa $n = p \cdot q$ mit $p \equiv q \equiv 3 \,(4)$ prim, etwa $p = 4k+3$, $q = 4\ell+3$ mit $k, \ell \in \mathbb{N}_0$, und sei $p \neq q$.
Sei a mod n ein quadratischer Rest mod n, d.h. es existiere ein $b \in \mathbb{Z}$ mit $a \equiv b^2 \,(n)$.
Gesucht seien die Lösungen der Kongruenz $a \equiv x^2 \,(n)$.
Nach dem CRS gilt: $x^2 \equiv a \,(n) \iff x^2 \equiv a \,(p)$ und $x^2 \equiv a \,(q)$, und die jeweiligen Lösungen $\pm a^{k+1}$ mod p und $\pm a^{\ell+1}$ mod q kann man zusammensetzen zu (maximal) vier Lösungen mod n. Es sind genau 4 Lösungen, die explizit wie folgt bestimmt werden können:
Sind $r, s \in \mathbb{Z}$ geg. mit $rp + sq = 1$, d.h. die Bézout-Elemente von p und q, und ist $\pm b$ Lsg. von $x^2 \equiv a \,(p)$ [2 Mögl.]
$\pm c$ Lsg. von $x^2 \equiv a \,(q)$ [2 Mögl.],
so liefert die CRS-Formel (Inv. von q mod p, Inv. von p mod q)

$$x = \pm b\, s\, q \pm c\, r\, p$$

genau vier Lösungen von $x^2 \equiv a \,(p \cdot q)$. Diese müssen paarweise inkongruent mod pq sein, da wir laut CRS den Ringiso $\mathbb{Z}_{pq} \cong \mathbb{Z}_p \times \mathbb{Z}_q$ haben und die 4 versch. Lösungspaare (b, c), $(-b, c)$, $(b, -c)$, $(-b, -c)$ deswegen genau 4 Restklassen in $\mathbb{Z}_{pq}$ entsprechen.

15.) Bsp.: Betr. $p = 11$, $q = 19$, d.h. $k = 2$, $\ell = 4$. Wähle $a = 47$.
Die Lösungen von $x^2 \equiv 47 \equiv 3 \,(11)$ sind $\pm 3^3 \,(11) \equiv \pm 5 \,(11)$,
die Lösungen von $x^2 \equiv 47 \equiv 9 \,(19)$ sind $\pm 3 \,(19)$.
Bézout-El. bestimmen (hier Probieren): Inv. von $19 \equiv 8$ mod 11 ist 7, Inv. von 11 mod 19 ist 7.
$\rightsquigarrow s = r = 7$ und $x \equiv \mp 5 \cdot 7 \cdot 19 \mp 3 \cdot 7 \cdot 11 \;(11 \cdot 19)$
ergibt $x \in \{\pm 16, \pm 60\}$. Probe: $16^2 \equiv 47 \,(11 \cdot 19)$ ✓, $60^2 \equiv 47 \,(11 \cdot 19)$ ✓

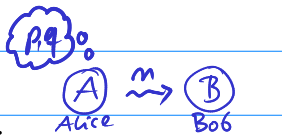
Man beachte, dass wir hier benötigen, dass a ein quadratischer Rest mod 11 und mod 19 sein muss. Würde man a zufällig wählen, wäre das nicht unbedingt der Fall; dann ist $x^2 \equiv a \,(n)$ ohnehin unlösbar, falls a kein quadratischer Rest mod $11 \cdot 19$ ist.
Wir besprechen nun eine Anwendung.



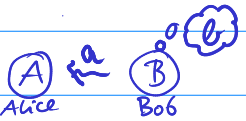
16.) Problem des fairen Münzwurfknobelns am Telefon:
Zwei Spieler, Alice (A) und Bob (B) möchten etwas ausknobeln (z.B. wer beim Fernschach beginnen soll und dann einen Vorteil hat, etc.), allerdings sprechen sie sich am Telefon oder mailen sich, und können sich daher nicht sehen. (A) wirft eine Münze, und (B) denkt vorher "Kopf" oder "Zahl", verrät das aber nicht. (*) (A) teilt (B) das Ergebnis mit, und (B) verkündet, wer gewonnen hat: (A), wenn ihr Münzwurfergebnis mit der Wahl von (B) übereinstimmt, ansonsten gewinnt (B).
Sei (B)s geheime Wahl "Zahl".
Teilt (A) mit, dass sie "Zahl" geworfen hat, akzeptieren (A) und (B) den Spielausgang, weil dann (A) gewinnt und (B) ihr dies verkündet. Falls (A) jedoch mitteilt, dass sie "Kopf" geworfen hat, teilt (B) mit, dass (A) verloren habe, was (A) natürlich nicht akzeptieren würde.
↝ Problem: Wie kann bei Ergebnis "Kopf" Spieler (B) ihre Mitspielerin (A) überzeugen, dass er vor dem Münzwurf die Wahl "Zahl" getroffen hat?
Unsere Antwort: Wenn (B) dann eine Zahl $n=pq$ faktorisieren könnte, deren Primteiler p,q ansonsten nur (A) kennt!

(*): (Wäre (B) live dabei, würde er "Kopf" oder "Zahl" sagen und das Ergebnis sehen. Am Telefon gilt: Würde (A) seine Wahl vorher kennen, so würde (B) ihr mitgeteiltes Münzwurfergebnis u.U. anzweifeln.)

17.) Das Verfahren funktioniert wie folgt:

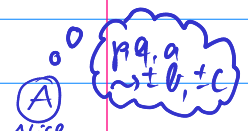


Schritt (1.) (A) wählt Primzahlen $p,q \equiv 3 (4)$, $p \neq q$, berechnet $n=p \cdot q$ und schickt n an (B)



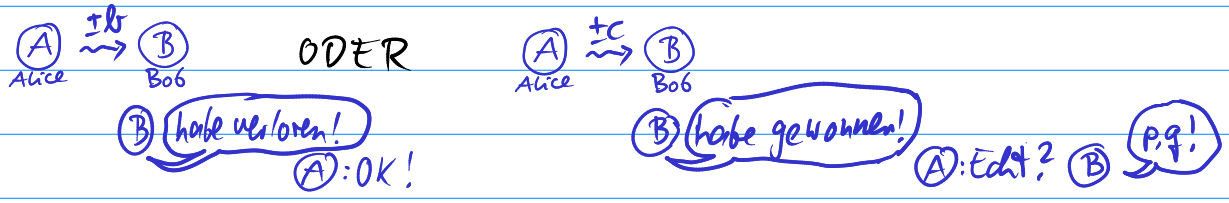
Schritt (2.) (B) wählt $1 \leq b \leq n-1$ zufällig und behält b geheim, er berechnet $a \equiv b^2 (n)$, und schickt a an (A)

Schritt (3.) (A) berechnet die 4 Lösungen von $x^2 \equiv a (n)$ mit der Berechnungsmethode aus 14.), die 4 Lösungen seien $\pm b, \pm c \in \mathbb{Z}$, (mit b von (B)), die Lösungen $\pm c$ sind andere, die (B) nicht kennt.



Soweit die Vorbereitung; dann der eigentliche Münzwurf:

Schritt (4.) Ⓐ wählt eine der 4 Lösungen zufällig aus (etwa durch Münzwurf!), d.h. entweder $\pm b$ oder $\pm c$, und schickt Ⓑ das Ergebnis. Ⓐ kann nicht wissen, dass Ⓑ die Zahl b gewählt hat. Die Vereinbarung ist nun: Schickt Ⓐ eine der Zahlen $\pm b$, gewinnt Ⓐ,
schickt Ⓐ eine der Zahlen $\pm c$, gewinnt Ⓑ, und das verkündet Ⓑ.



Schritt (5.) Es erfolgt die Verifikation, dass Ⓐ wirklich verloren hat im 2. Fall, dann muss sich Ⓐ davon überzeugen, dass Ⓑ vorher wirklich $\pm b$ gewählt hat: Er kann Ⓐ die Lösungen $\pm b$ einfach mitteilen, da Ⓐ auch diese berechnet hat. Alternativ kann Ⓑ ihr sogar die Primfaktoren von n nennen:

Er berechnet $b+c \bmod n$ und

$d = ggT(b+c, n)$ mit dem euklidischen Algo.

Dann ist $d=p$ oder $d=q$. ⌜Denn aus $b^2 \equiv a \equiv c^2 \ (pq)$ folgt:
$pq \mid (b-c)(b+c) = b^2 - c^2$, und da $b \not\equiv c \ (p)$, $b \not\equiv c \ (q)$ folgt $q \mid b+c$ oder $p \mid b+c$,
und $d \neq n$, weil sonst $b \equiv -c \bmod n$ wäre ↯.⌟

Also kann Ⓑ, weil er c kennt, die von Ⓐ gewählten Primfaktoren bestimmen und Ⓐ mitteilen und auf diese Art Ⓐ überzeugen.

Das konnte Ⓑ nur, weil er vorher auch wirklich die nicht von Ⓐ genannte Lösung $\pm b$ hatte.

Damit ist das Spiel fair.

P.S.: In der praktischen Umsetzung wird noch ein Verfahren zur Erzeugung großer, möglichst zufälliger Primzahlen p, q gebraucht. Man kennt in der Praxis schnelle Tests (den Miller-Rabin-Test), um zu entscheiden, ob eine große Zahl n (mit ev. hunderten von Stellen in Dezimaldarstellung) zusammengesetzt ist oder (sehr wahrscheinlich) prim. Daher erzeugt man solange Zufallszahlen in der gewünschten Größe, bis der Primzahltest "anschlägt".