Kleiner Fermat $\quad a^{p-1} \equiv 1 \pmod p \quad$ für $p \nmid a$

a^{p-1} lässt Rest 1 in $\mathbb{Z}/p\mathbb{Z}$

$$\underbrace{\overline{a}^{\,p-1}}_{\substack{\shortparallel \\ \underbrace{\overline{a}\cdot\overline{a}\cdot\ldots\cdot\overline{a}}_{p-1 \text{ mal}}}} = \overline{a^{p-1}} = \overline{1} \quad \text{in } \mathbb{Z}/p\mathbb{Z}$$

Wie rechnet man a^b in $\mathbb{Z}/n\mathbb{Z}$ aus?

Wähle a' so, dass $a' \equiv a \mod n$ und $0 \le a' < n$ $\quad$ evtl. noch besser: $-\frac{n}{2} \le a' \le \frac{n}{2}$

$\overline{a^b} = \overline{(a')^b}$ in $\mathbb{Z}/n\mathbb{Z}$

O.E. $\quad 0 \le a < n$.

Rechne a^2 aus und davon den Rest modulo n

$$a^b = a^2 \cdot a^2 \cdot \ldots \cdot a^2 \,\vdots\, \cdot a \,\vdots$$

$$\overline{a^b} = \overline{a^2} \cdot \overline{a^2} \cdot \ldots \cdot \overline{a^2} \,\vdots\, \cdot \overline{a} \,\vdots$$

$(\qquad)$ $\qquad$ paarweise zusammenfassen

Bsp: $\quad n = 12, \quad a = \overset{29}{28}, \quad b = 5 \qquad \overset{29^5}{28^5} \mod 12 = ?$

$$\overline{28^5} = \overline{4^5} = \overline{4^2} \cdot \overline{4^2} \cdot \overline{4} = \underbrace{\overline{4}\cdot\overline{4}}\cdot\overline{4} = \overline{4}^2 = \overline{4}$$

$$\overset{\shortparallel}{\overline{16}}$$

$$\overline{29^5} = \overline{5^5} = \overline{5^2} \cdot \overline{5}^2 \cdot \overline{5} = \overline{1}\cdot\overline{1}\cdot\overline{5} = \overline{5}$$

mit Fermat bzw Euler :

$p = 7$ Rechnen in $\mathbb{Z}/7\mathbb{Z}$

$$\overline{7003^{6004}} = \overline{3^{6004}} = \overline{3^{6\cdot 1000+4}} = (\overline{3^6})^{1000} \cdot \overline{3}^4 = \overline{3}^4 = (\overline{3^2})^2 = \overline{2}^2 = \overline{4}$$

$\overline{3^6} = \overline{1}$ kleiner Fermat, $\overline{3^2} = \overline{9}$

$n = 12$, rechne in $\mathbb{Z}/12\mathbb{Z}$, $\varphi(12) = 4$

$$\overline{7^{6004}} = \overline{7^{4\cdot 1501}} = \overline{1}^{1501} = \overline{1}$$

Noch ohne Beweis : $n = p_1^{k_1} \cdot \ldots \cdot p_m^{k_m}$ Primfaktorzerlegung

p_i paarweise verschiedene Primzahlen

$k_i \geq 1$

Dann $\varphi(n) = (p_1 - 1)\cdot p_1^{k_1 - 1} \cdot \ldots \cdot (p_m - 1)\cdot p_m^{k_m - 1}$

Bsp $n = 12 = 2^2 \cdot 3$

$\varphi(12) = (2-1)\cdot 2^1 \cdot (3-1)\cdot 3^0 = 4$

$n = 2^4 \cdot 3^3 \cdot 5 \cdot 7^3$, $\varphi(n) = 1 \cdot 2^3 \cdot 2 \cdot 3^2 \cdot 4 \cdot 6 \cdot 7^2$

Weitere Anwendungen des Satzes von Fermat bzw. Euler

(1) Primzahltests:

Problem: Gegeben $n \in \mathbb{N}$, ist n Primzahl?

„naive" Vorgehensweise: teste für alle Zahlen k von 2 bis $\lfloor\sqrt{n}\rfloor$, ob sie n teilen.

dauert zu lange, aber gibt stets korrekte Antwort!

Fermat-Test: teste für ausgewählte Zahlen $a < n$, ob $a^{n-1} \equiv 1 \mod n$

Falls nein, so ist n keine Primzahl!

Falls ja, so ist keine Aussage möglich.

Probleme:
- man kann bei Antwort „ja" nicht gut quantifizieren, mit welcher Wahrscheinlichkeit n eine Primzahl ist
- es gibt sogenannte Carmichael-Zahlen, das sind Zahlen n, die keine Primzahlen sind, für die aber stets $a^{n-1} \equiv 1 \mod n$ für $0 < a < n$ gilt.

Es gibt unendlich viele Carmichael-Zahlen.

Die tatsächlich benutzten Primzahltests sind probabilistisch und benutzen den kleinen Satz von Fermat als Ingredienz.

② **RSA-Kryptografie** (das mathematische Prinzip dahinter)
(Rivest, Shamir, Adleman)

$$\underset{\text{Sender}}{A} \xrightarrow{\text{Information}} \underset{\text{Empfänger}}{B}$$

↑
Lauscher

a) Man wählt zwei große, „unbekannte" Primzahlen p und q (in der Praxis mit probabilistischen Tests)
↓
Sollen nicht in veröffentlichten Listen auftauchen oder von besonderer Form sein
(z.B. kein Mersenne-Primzahlen, d.h. von der Form $2^n - 1$)

b) Rechne $n = p \cdot q$ aus, und $\varphi(n) = (p-1)\cdot(q-1)$ ⟶

Welche Zahlen x mit $0 < x \le p \cdot q$ sind nicht teilerfremd zu $p \cdot q$?

$1\cdot q,\ 2\cdot q,\ 3\cdot q,\ \ldots\ldots,\ (p-1)\cdot q$: $p-1$
$1\cdot p,\ 2\cdot p,\ 3\cdot p,\ \ldots\ldots,\ (q-1)\cdot p$: $q-1$
$p\cdot q$: 1

Wieviele Zahlen x mit $0 < x \le p\cdot q$ sind teilerfremd zu $p \cdot q$?

$$p\cdot q - (p-1) - (q-1) - 1$$
$$= p\cdot q - p + 1 - q + 1 - 1$$
$$= p\cdot q - p - q + 1$$
$$= (p-1)(q-1)$$

Bem: Wer nur n kennt und nicht die Primfaktorzerlegung von n, kann (nach heutigem Wissensstand) $\varphi(n)$ nicht schnell ausrechnen.

c) Wähle ein „zufälliges" e, das teilerfremd zu $\varphi(n)$ ist
z.B. nicht zu klein, nicht zu nahe bei $\varphi(n)$, nichts, was einfache Rückschlüsse auf $\varphi(n)$ zuließe

Öffentlicher Schlüssel: n, e

Geheimer Schlüssel: $p, q, \varphi(n)$

Alphabet ist $\mathbb{Z}_n$ (bzw. $\mathbb{Z}/n\mathbb{Z}$)

(Text muss geschickt in $\mathbb{Z}_n$ kodiert werden)

Ein Nachricht $A = (a_1, \dots, a_k) \in \mathbb{Z}_n^k$ wird kodiert als

$$\underbrace{A^e := (a_1^e, \dots\dots, a_k^e)}_{\substack{\text{in } \mathbb{Z}_n \text{ ausgerechnet} \\ \cong \\ \mathbb{Z}/n\mathbb{Z}}}$$

<u>Entschlüsselung</u>: Man rechnet ein Inverses d von e in $\underset{\substack{\cong? \\ (\mathbb{Z}/\varphi(n)\mathbb{Z})^*}}{\mathbb{Z}_{\varphi(n)}^*}$ aus, d.h. $e \cdot d \equiv 1 \mod \varphi(n)$

existiert, da $ggT(e, \varphi(n)) = 1$, und ist mit erkl. Algorithmus schnell berechenbar

Dann berechnet man $(A^e)^d := ((a_1^e)^d, \dots, (a_k^e)^d)$

<u>Behauptung</u>: $(a_i^e)^d = a_i$ in $\mathbb{Z}_n$

falls $ggT(a, n) = 1$, so $a^{\varphi(n)} \equiv 1 \mod n$

<u>Beweis</u>: $\boxed{\text{1. Fall}}$ a_i ist teilerfremd zu n

$$(a_i^e)^d = a_i^{\varphi(n) \cdot \ell + 1} = (a_i^{\varphi(n)})^\ell \cdot a_i \overset{\text{Euler}}{=} 1^\ell \cdot a_i = a_i$$

$\boxed{\text{2. Fall}}$ a_i ist nicht teilerfremd zu n

$\boxed{2a}$ $a_i = 0$, dann $(a_i^e)^d = 0^{e \cdot d} = 0$ ✓

$\boxed{2b}$ a_i ist Vielfaches von p, aber nicht von q

$\boxed{2c}$ a_i ist Vielfaches von q, aber nicht von p

$\boxed{\text{2. Fall, b}}$ (2c ist völlig symmetrisch dazu)

$a_i = k \cdot p$, $\quad k, q$ teilerfremd

Dann $p \mid a_i^{e\cdot d} - a_i$

Andererseits: $\varphi(q) = q-1 \mid \varphi(n) = (p-1)(q-1)$

also $\varphi(q)$ teilt $\varphi(n)$ teilt $e\cdot d - 1$, da $e \cdot d \equiv 1 \mod \varphi(n)$

somit $e\cdot d \equiv 1 \mod \varphi(q)$

Satz von Euler: $a_i^{e\cdot d} \equiv a_i \mod q$, denn $a_i^{e\cdot d} = \underbrace{a_i^{\varphi(q)}}_{=1}{}^{\cdot k' + 1}$ $= 1$ da a_i teilerfremd zu q

Also $q \mid a_i^{e\cdot d} - a_i$

Da p, q teilerfremd, folgt $p \cdot q \mid a_i^{ed} - a_i$, d.h. $a_i^{ed} \equiv a_i \mod \overset{n}{p \cdot q}$

(Anmerkung: Die spezielle Gestalt von n als Produkt von 2 versch. Primzahlen geht hier ein!)