<u>SCHEMA FÜR EINEN RANDOMISIERTEN PRIMZAHLTEST</u>

Eingabe: $n \in \mathbb{N}$

Ausgabe: $\textsc{Prime}$ oder $\textsc{Composite}$, so daß

n prim $\Longrightarrow$ Antwort *immer* $\textsc{Prime}$

n zusammengesetzt $\Longrightarrow$ Antwort mit W'keit $\geq 1 - 2^{-100}$ $\textsc{Composite}$

Wiederhole 100 mal:

Wähle eine Zahl $a \in \{2, 3, \ldots, n-1\}$ zufällig,

teste ob a "*bezeugt*", daß n <u>keine</u> Primzahl ist.

Falls mind. ein solcher Zeuge gefunden wurde, antworte $\textsc{Composite}$, andernfalls antworte $\textsc{Prime}$.

Wdh. Diskrete Strukturen I

- $\langle G, \circ, e \rangle$ heißt **Gruppe**, falls gilt

  — $\circ$ ist eine Abbildung $G \times G \to G$
  — $\circ$ ist assoziativ, d.h.

$$(a \circ b) \circ c = a \circ (b \circ c) \qquad \forall a, b, c \in G$$

  — e ist ein (linksseitiges) Einselement, d.h.

$$e \circ a = a \qquad \forall a \in G$$

  — zu jedem Element a von G existiert in Inverses, d.h.

$$\forall a \in G \ \exists a^{-1} \in G \ \text{ mit } \ a \circ a^{-1} = e$$

  Beispiele:

  $\mathbb{Z}_n := \{0, 1, 2, \ldots, n-1\}$
  ist Gruppe bzgl. Addition modulo n

  $\mathbb{Z}_n^* := \{x \in \mathbb{Z}_n \setminus \{0\} \mid \text{ ggT}(x, n) = 1\}$
  ist Gruppe bzgl. Multiplikation modulo n

- $H \subseteq$ heißt **Untergruppe**, falls gilt H bzgl. $\circ$ abgeschlossen ist.

  Es gilt: H Untergruppe von $G \implies |H|$ teilt $|G|$.

- Eine Gruppe $\langle G, \circ, e \rangle$ heißt **zyklisch**, wenn es ein $b \in G$ gibt mit

$$G = \{b, b^2, \ldots, b^{|G|}\},$$

  wobei $b^k := \underbrace{b \circ \ldots \circ b}_{k \text{ mal}}$

Wdh. Diskrete Strukturen I

- **Erweiterter Euklidischer Algorithmus**

  Bestimmt zu gegebenen $n, m \in \mathbb{N}$ Zahlen $x, y \in \mathbb{Z}$
  mit $mx + ny = \text{ ggT}(m, n)$.
  Laufzeit: polynomiell in $\log(n + m)$

- **Chinesischer Restsatz**

  Für alle $m, n \in \mathbb{N}$ mit $\text{ggT}(m, n) = 1$ gilt:
  Zu jedem Paar $a \in \mathbb{Z}_m$ und $b \in \mathbb{Z}_n$ existiert ein eindeutig bestimmtes $t \in \mathbb{Z}_{mn}$ mit

  $$\begin{aligned} t &\equiv a \mod m \quad \text{und} \\ t &\equiv b \mod n. \end{aligned}$$

- **Satz von Fermat**

  Für alle $n \in \mathbb{N}$ gilt:

  $$n \text{ Primzahl} \iff a^{n-1} \equiv 1 \mod n \quad \forall a \in \mathbb{Z}_n \setminus \{0\}.$$

- p Primzahl $\Longrightarrow$ $\mathbb{Z}_p^*$ zyklisch

$\textsc{PrimalityTest}(n)$

Choose an integer $a \in \{2, \ldots, n-1\}$ uniformly at random;
if $\gcd(a, n) \neq 1$ or $n \geq 4$ is even **then**
  return $\textsc{Composite}$
else if $a^{n-1} \not\equiv 1 \mod n$ **then**
  return $\textsc{Composite}$
else
  for all $d \geq 1$ s.t. $2^d \mid n-1$ **do**
    if $1 < \gcd(a^{(n-1)/2^d} - 1, n) < n$ **then**
      return $\textsc{Composite}$
else
  return $\textsc{Prime}$.