Number Theory Sum-Up

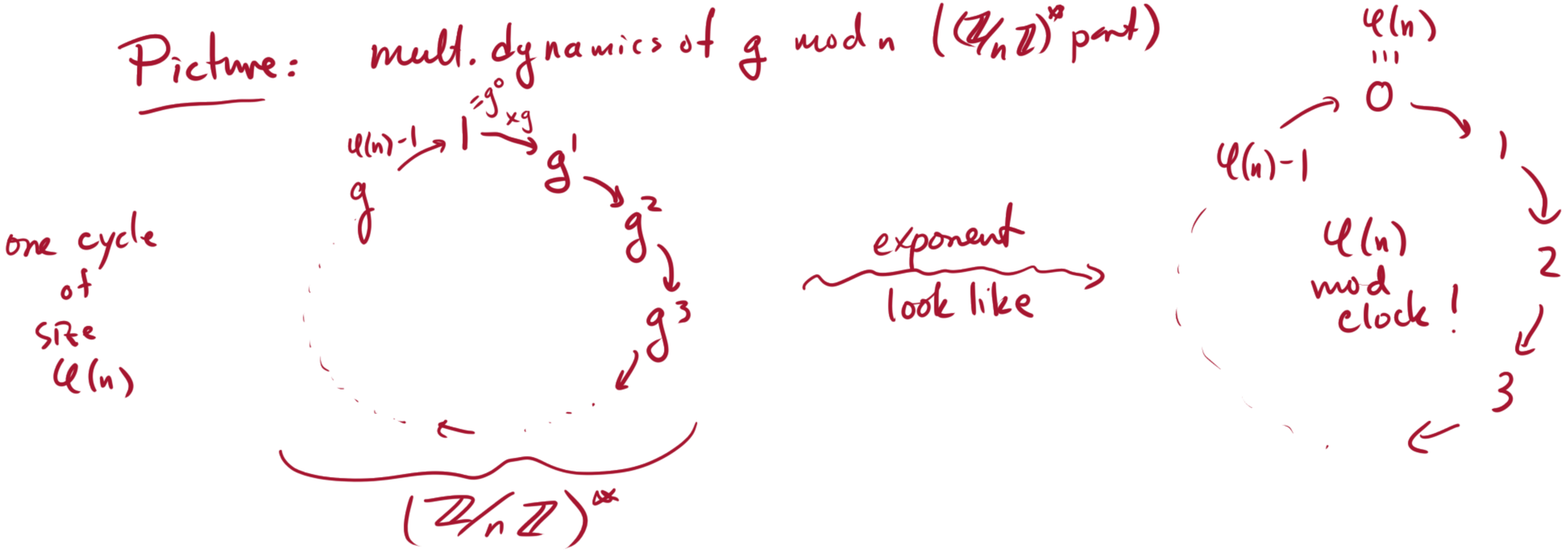
① Let $a \in \mathbb{Z}/n\mathbb{Z}$. Then a is invertible $\iff \gcd(a,n) = 1 \iff$ $x \mapsto ax$ is bijective.

$$(\mathbb{Z}/n\mathbb{Z})^* := \{ a \in \mathbb{Z}/n\mathbb{Z} : a \text{ is invertible} \} \quad \text{"unit group"}$$

$$\varphi(n) := |(\mathbb{Z}/n\mathbb{Z})^*|$$

② A primitive root $g \in (\mathbb{Z}/n\mathbb{Z})^*$ is an element whose powers give all of $(\mathbb{Z}/n\mathbb{Z})^*$.

Picture: mult. dynamics of g mod n ($(\mathbb{Z}/n\mathbb{Z})^*$ part)



③ Key Consequence: the exponents mod n "live" mod $\varphi(n)$.

Theorem. (Euler's Theorem)
Let $a \in \mathbb{Z}/n\mathbb{Z}$ be invertible.
Then $a^{\varphi(n)} \equiv 1 \pmod{n}$.

Theorem (Fermat's Little Theorem).
Let $a \in \mathbb{Z}/p\mathbb{Z}$ be invertible, p prime.
Then $a^{p-1} \equiv 1 \pmod{p}$.

Ex. ① If 111 were prime, then $2^{110} \equiv 2^0 \equiv 1 \pmod{111}$.
But Sage says $2^{110} \not\equiv 1 \pmod{111}$. Therefore 111 is not prime.

② Compute $3^{302} \pmod{101}$ (101 prime.) (so exp. live mod $p-1$).
$\equiv 3^2 \equiv 9 \pmod{101}$. $p-1 = 100$

③ Key Consequence: the exponents mod n "live" mod $\varphi(n)$.

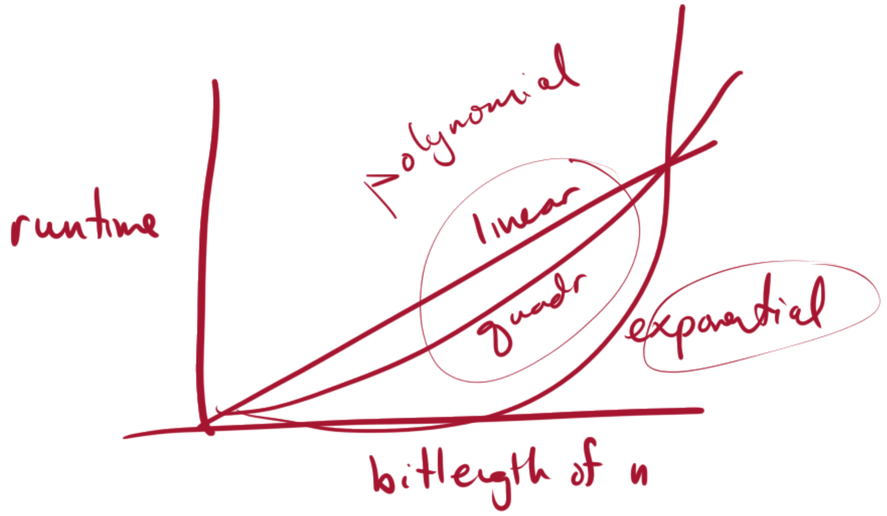
Theorem. (Euler's Theorem)
Let $a \in \mathbb{Z}/n\mathbb{Z}$ be invertible.
Then $a^{\varphi(n)} \equiv 1 \pmod{n}$.

Theorem (Fermat's Little Theorem).
Let $a \in \mathbb{Z}/p\mathbb{Z}$ be invertible, p prime.
Then $a^{p-1} \equiv 1 \pmod{p}$.

Ex. ① If 111 were prime, then $2^{110} \equiv 2^0 \equiv 1 \pmod{111}$.
But Sage says $2^{110} \not\equiv 1 \pmod{111}$. Therefore 111 is not prime.

② Compute $3^{302} \pmod{101}$ (101 prime.) (so exp. live mod $p-1$).
$\equiv 3^2 \equiv 9 \pmod{101}$. $\quad 101-1 = 100$

Sage Demo:



Takeaway

runtime
- polynomial
- exponential

ideally

encrypt/decrypt
(milliseconds)

break/cryptanalyse
(infeasible)

Big-O Notation

Defn. Let $f: [0, \infty) \to \mathbb{R}$

$g: [0, \infty) \to \mathbb{R}^{>0}$.

Then we write

$$f(x) = O(g(x))$$

if $\exists$ { a constant $C > 0$, a constant $x_0 > 0$

st. $|f(x)| \leq C \cdot g(x)$

$\forall \; x > x_0$.

Purpose:
to describe function f as "bounded" by g (simpler)

Big-O Notation

Defn. Let $f: [0, \infty) \to \mathbb{R}$

$g: [0, \infty) \to \mathbb{R}^{>0}$.

Then we write

$$f(x) = O(g(x))$$

if $\exists$ { a constant $C > 0$, a constant $x_0 > 0$

st. $|f(x)| \leq C \cdot g(x)$

$\forall \; x > x_0$.

Purpose:
to describe function f as "bounded" by g (simpler)

Theorem. Computing $b^x \pmod{n}$ by successive squaring, where $x < n$, has runtime $O((\log_2(n))^3)$.

. polynomial!

Pf.