Number Theory Sum-Up

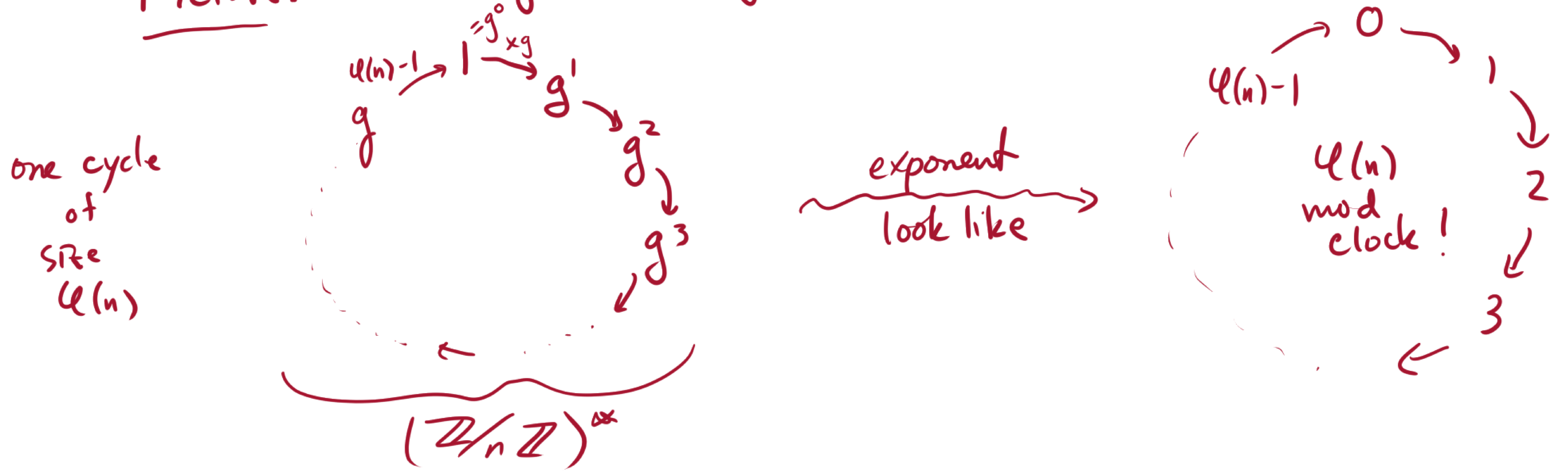
① Let $a \in \mathbb{Z}/n\mathbb{Z}$. Then a is invertible $\iff \gcd(a,n) = 1 \iff$ $x \mapsto ax$ is bijective.

$$(\mathbb{Z}/n\mathbb{Z})^* := \{ a \in \mathbb{Z}/n\mathbb{Z} : a \text{ is invertible} \}$$ "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 $\boxed{\varphi(n) = n \prod_{p \mid n} \left(1 - \frac{1}{p}\right)}$.

$$\varphi(10) = 10\left(1-\frac{1}{2}\right)\left(1-\frac{1}{5}\right)$$
$$= 10\left(\frac{1}{2}\right)\left(\frac{4}{5}\right) = 4.$$

1 $\boxed{\varphi(p) = p\left(1-\frac{1}{p}\right) = p-1}$

$$\varphi(p^2) = p^2\left(1-\frac{1}{p}\right) = p(p-1)$$
$$\varphi(p^k) = p^{k-1}(p-1)$$

$$\varphi(45) = \varphi(5)\varphi(9) = (5-1)\cdot 3\cdot(3-1)$$
$$= 4\cdot 3\cdot 2 = 24.$$

$45 = 5 \cdot \underbrace{3\cdot 3}$

$$\varphi(10) = \varphi(2)\varphi(5)$$
$$= (2-1)(5-1)$$
$$= 1\cdot 4 = 4$$

$$\varphi(45) = 45\left(1-\frac{1}{5}\right)\left(1-\frac{1}{3}\right)$$
$$= 45\left(\frac{4}{5}\right)\left(\frac{2}{3}\right)$$
$$= 24$$

2 **Thm.** Let $m, n \in \mathbb{Z}$, coprime. Then $\varphi(mn) = \varphi(m)\varphi(n)$.

When is it ok to cancel?

$$\left[\begin{array}{c} a \text{ is invertible} \\ \Updownarrow \\ \gcd(a,n)=1 \\ \Updownarrow \\ x \longmapsto ax \text{ is bijective} \end{array} \right] \iff \left(\begin{array}{c} ax \equiv ay \pmod{n} \\ \Downarrow \times a^{-1} \\ x \equiv y \pmod{n} \end{array} \right)$$

Theorem. Computing $b^x \pmod{n}$ by successive squaring takes $O(\log_2(x))$ modular multiplications.

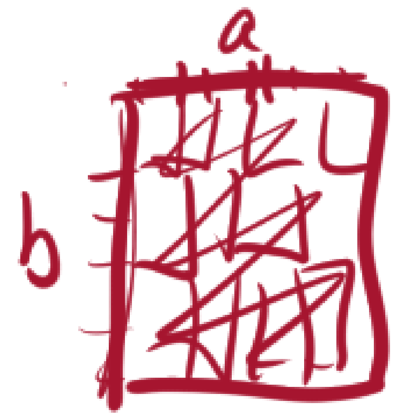
Pf. There are $\leq \log_2(x)+1$ bits in the binary expansion of x.

So there are at most

$$\begin{cases} \log_2(x) & \text{squarings} \\ \log_2(x) & \text{multiplications} \end{cases}$$

So $\leq 2\log_2(x)$ total multiplications.

This is $O(\log_2(x))$. $\boxtimes$

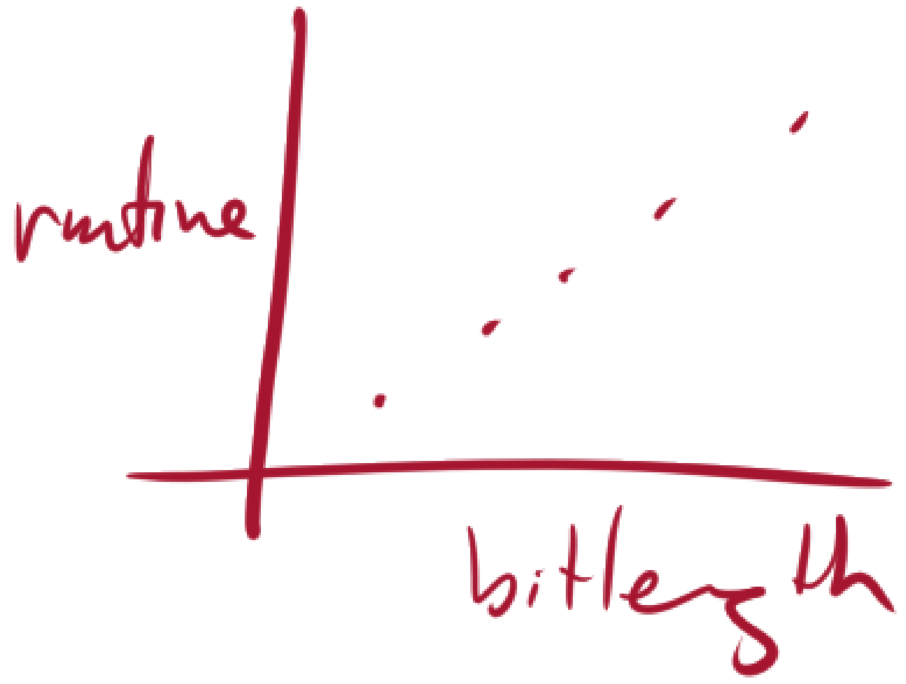


Comments:

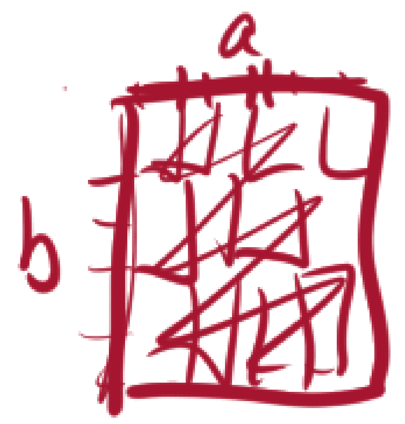
① Modular exponentiation is linear in bitlength of the exponent.

② A modular multiplication takes $O((\log(n))^2)$ bit operations.
(constant from the perspective of $x \to \infty$)

③ Sage data:



linear.



Theorem. Computing $b^x \pmod{n}$ by successive squaring takes $O(\log_2(x))$ modular multiplications.

Pf. There are $\leq \log_2(x) + 1$ bits in the binary expansion of x.

So there are at most

$$\begin{cases} \log_2(x) & \text{squarings} \\ \log_2(x) & \text{multiplications} \end{cases}$$

So $\leq 2\log_2(x)$ total multiplications.

This is $O(\log_2(x))$. $\boxtimes$

Comments:

① Modular exponentiation is linear in bitlength of the exponent.

② A modular multiplication takes $O((\log(n))^2)$ bit operations.
(constant from the perspective of $x \to \infty$)

③ Sage data:

linear.

Theorem. Computing the modular inverse (via Gauss) of $a \pmod{n}$ involves $O(\log(n))$ instances of division algorithm and $O(\log(n))$ final multiplications.

Pf. The size of "a" decreases by at least $\frac{1}{2}$ each time.

So # loops $\leq \log_2(a)$. $\boxtimes$

Tips & Tricks for Big-Oh

① $O(\log_a(x)) = O(\log_b(x))$ for any bases a, b.

Why? $\log_a(n) = \frac{\log_e(n)}{\log_e(a)}$ } multiply by a constant

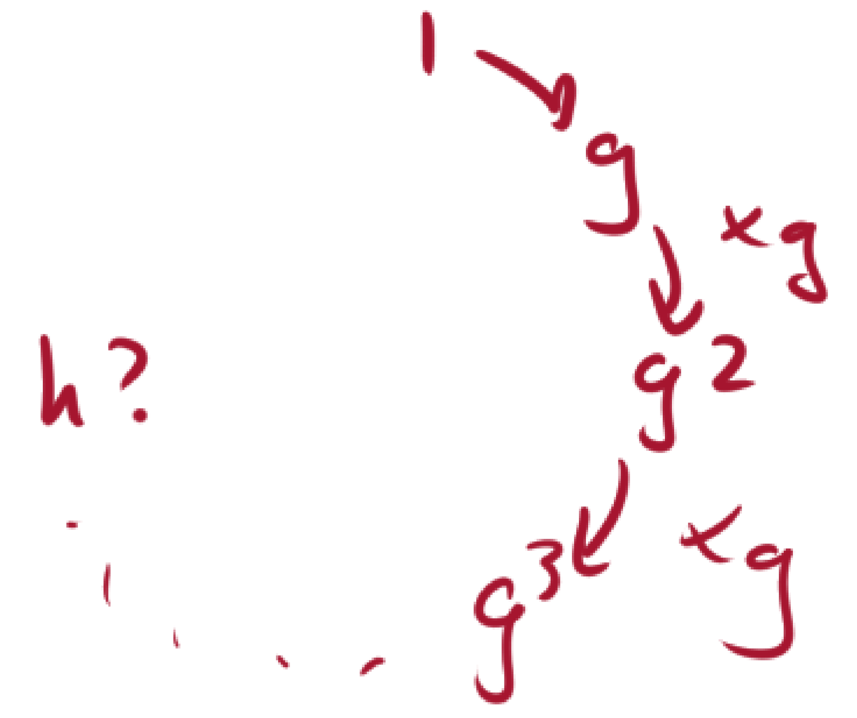
So we often leave off the base in big-Oh.

② $x^a = O(x^b)$ for $b \geq a$.

So, e.g.

$x^3 + 2x^2 + x + 1000 = O(x^3)$

$h = g^x \pmod{n}$



Thm. Discrete logarithm via exhaustive search involves $O(n)$ modular multiplications

Pf. Start at g.
Multiply by g at most $n-2$ times,
each time checking if the result is h. $\boxtimes$

This is *exponential* runtime in $\log(n)$
since $n = \exp(\log(n))$

Current Record:

795-bit prime	DLP
768	2016
596	2014
530	2007
431-bit	2005

Moral:

computing $h = g^x$ polynomial time   ← do in milliseconds

$\wedge$

finding x exponential time   ← not feasible.

Birthday Attack for Discrete Log

$$\boxed{\text{Solve} \quad g^x \equiv h \pmod p}$$

① Make a list of g^k for random k

② " h^ℓ " " " ℓ

Watch for a collision:

$$g^k \equiv h^\ell \pmod p$$

$$\Rightarrow g^k \equiv g^{x\ell} \pmod p$$

$$\Rightarrow k \equiv x\ell \pmod{p-1}$$

$\Rightarrow$ solve for x
(invert ℓ)

Problem: maybe ℓ is not invertible!

Better:

① List g^k random k

② List $h \cdot g^{-\ell}$ random ℓ

A collision:

$$g^k \equiv h \cdot g^{-\ell} \pmod p$$

$$\Rightarrow g^k \equiv g^{x-\ell} \pmod p$$

$$\Rightarrow \boxed{k \equiv x - \ell} \pmod{p-1}$$