Basic Factoring / Primality Principle

Thm. Let $n \in \mathbb{Z}$. (we wish to factor/test)

If $x, y \in \mathbb{Z}$ satisfy

$$\left.\begin{aligned} x^2 &\equiv y^2 \pmod{n} \\ x &\not\equiv \pm y \pmod{n} \end{aligned}\right\} \star$$

Then $\gcd(x-y, n)$ is a nontrivial factor of n $(\neq 1, n)$

so n is composite.

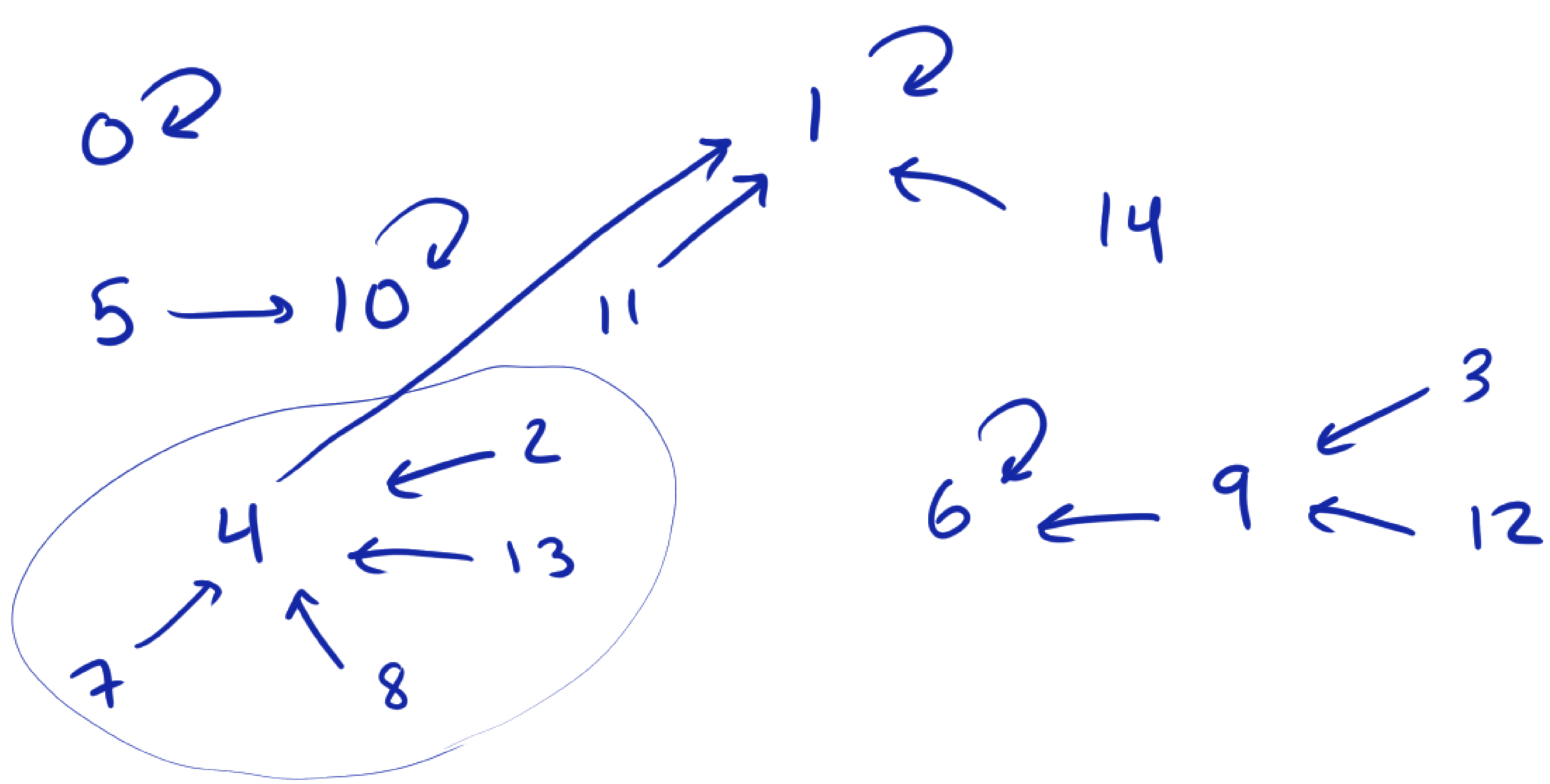
Big Idea: composite $\mathbb{Z}/n\mathbb{Z}$ differs in behavior from prime $\mathbb{Z}/p\mathbb{Z}$.

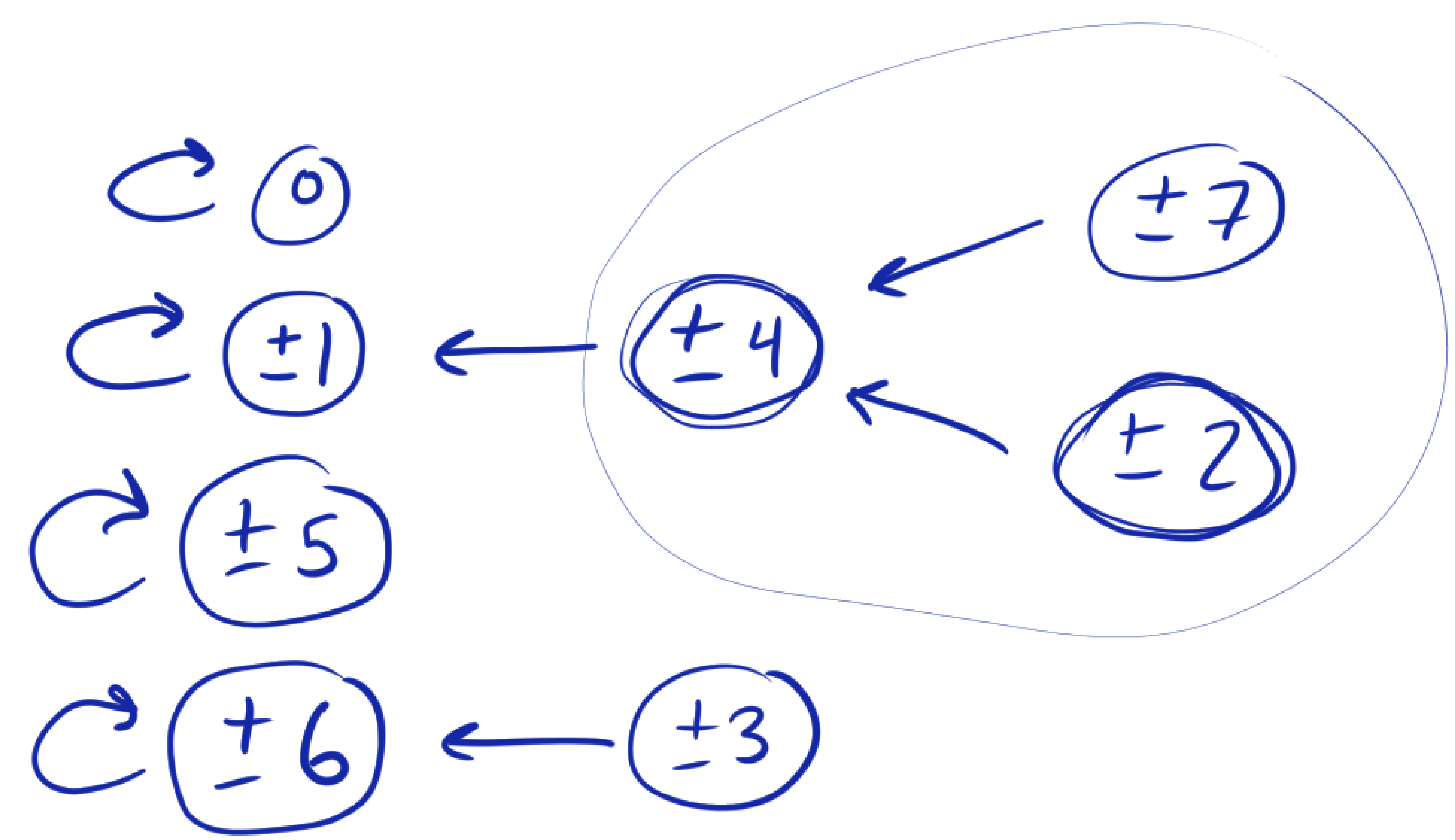
in example, 2 and 8

$2^2 = 4 = 8^2$

$2 \not\equiv \pm 8$

Ex. $n = 15$ Squaring:





Basic Factoring / Primality Principle

Big Idea: composite $\mathbb{Z}/n\mathbb{Z}$ differs in behavior from prime $\mathbb{Z}/p\mathbb{Z}$.

Thm. Let $n \in \mathbb{Z}$. (we wish to factor/test)

If $x, y \in \mathbb{Z}$ satisfy

$$\left.\begin{aligned} x^2 &\equiv y^2 \pmod{n} \\ x &\not\equiv \pm y \pmod{n} \end{aligned}\right\} (*)$$

Then $\gcd(x-y, n)$ is a nontrivial factor of n $(\neq 1, n)$

so n is composite.

$n = 6$

Core idea:
$$n \mid x^2 - y^2 = \underbrace{(x-y)}_{2}\underbrace{(x+y)}_{3}$$

Pf. Let $g = \gcd(x-y, n)$, where $(*)$ holds.

① If $g = n$ then $n \mid x - y$ i.e. $x \equiv y \pmod{n}$ $\rightarrow\leftarrow$.

② Assme $g = 1$.

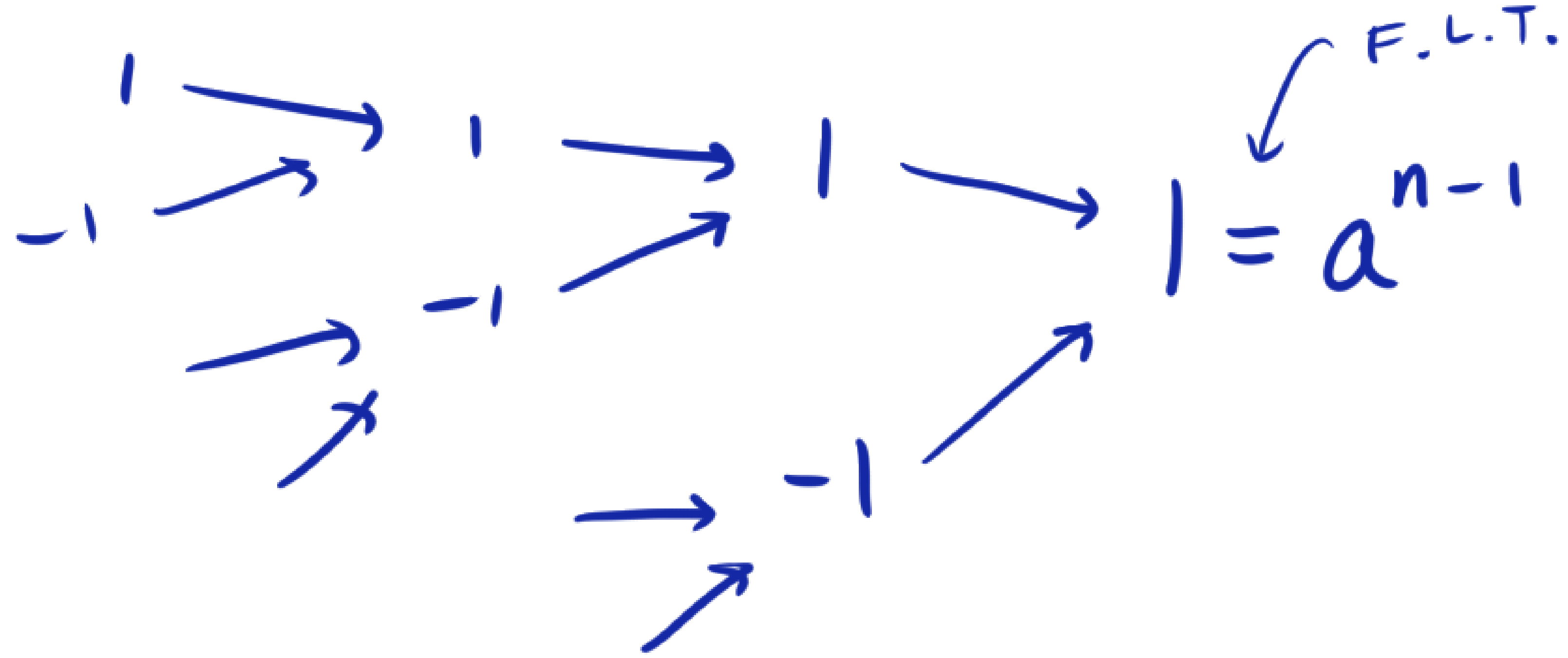
Since $x^2 \equiv y^2 \pmod{n} \Rightarrow n \mid x^2 - y^2 = (x-y)(x+y)$.

Since $g = 1$, $n \mid x + y \Rightarrow x \equiv -y \pmod{n}$. $\rightarrow\leftarrow$ $\square$

Miller-Rabin Primality Test

← F.L.T.
← ppl

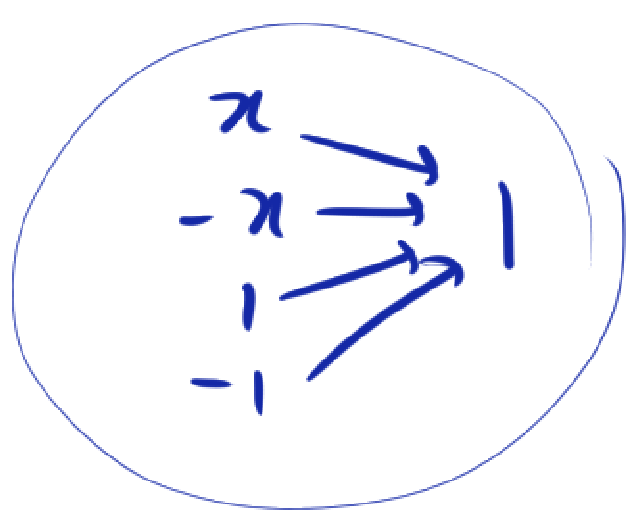
If n is prime the squaring looks like



If n is composite, this could fail 2 ways:

(a) chain never gets to 1 at all! $(a^{n-1} \not\equiv 1)$

(b) we see



for some $x \not\equiv \pm 1$.

Let $1 < a < n$.

Write $n-1 = 2^k m$; m odd.

Consider chain

$$a^m \to a^{2m} \to a^{4m} \to \cdots \to a^{2^k m} = a^{n-1}$$

Miller-Rabin:

Compute the chain, watch for (a) or (b).

If see (a) or (b) ⇒ composite.

otherwise ⇒ probably prime.

M-R Alg. to test n

Write $n-1 \equiv 2^k m$, m odd.

Choose base $1 < a < n$.

(Compute a^{n-1} via
$$a^m \to a^{2m} \to \dots \to a^{2^k m}$$)

① Compute $b_0 :\equiv a^m \pmod n$.

If $b_0 \equiv \pm 1$ then P.P. (Fermat) probable prime.

② Compute $b_1 :\equiv b_0^2 \pmod n$.

If $b_1 \equiv -1$ then P.P. (Fermat)

If $b_1 \equiv 1$ then Composite (Basic Ppl)

$\left(\begin{array}{c} b_0 \not\equiv \pm 1 \\ \text{but} \\ b_0^2 = 1^2 \end{array} \right)$

⋮ Continue, computing b_i

(k-1) Compute $b_{k-1} \equiv b_{k-2}^2 \equiv a^{2^{k-1} m}$

If $b_{k-1} \not\equiv -1 \Rightarrow$ composite (Fermat)

If $b_{k-1} \equiv -1$ then P.P. (Fermat)

Def^n. n is a strong pseudoprime for base a if it passes M-R as P.P. but is composite.

For $X \leq 10^{10}$

455052511	primes
14884	pseudo.pr. base 2
3291	strong pseudop. base 2.

$$\text{Prob(failure)} \approx \frac{1}{10^5}$$

Chinese Remainder Theorem

Thm. Suppose $\gcd(m,n)=1$, and $a,b\in\mathbb{Z}$. The system of equations

$$x \equiv a \pmod m$$
$$x \equiv b \pmod n$$

has a unique solution modulo nm.

(0) Rephrasing: $\mathbb{Z}/nm\mathbb{Z}$ is in bijection w/ $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$

$$\varphi : k \pmod{nm} \longmapsto (k \bmod n,\ k \bmod m).$$

In fact:

$$\mathbb{Z}/nm\mathbb{Z} \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$$
$$(\mathbb{Z}/nm\mathbb{Z})^* \cong (\mathbb{Z}/n\mathbb{Z})^* \times (\mathbb{Z}/m\mathbb{Z})^*$$

Proof 1. (Non-constructive.)

We will show φ is injective.

Since $|\mathbb{Z}/nm\mathbb{Z}| = |\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}|$, then it is bijective.

Suppose
$$x_i \equiv a \pmod m$$
$$x_i \equiv b \pmod n$$
for $i=1,2$.

Then $x_1 \equiv x_2 \pmod m$, so $m \mid (x_1 - x_2)$.

Similarly $n \mid (x_1 - x_2)$.

So $mn \mid (x_1 - x_2)$. $\leftarrow \gcd = 1$

So $x_1 \equiv x_2 \pmod{nm}$. $\blacksquare$