# Square Roots & Factoring / Primality

Sps $x^2 \equiv y^2 \pmod n$ but $x \not\equiv \pm y \pmod n$

"interesting square roots"

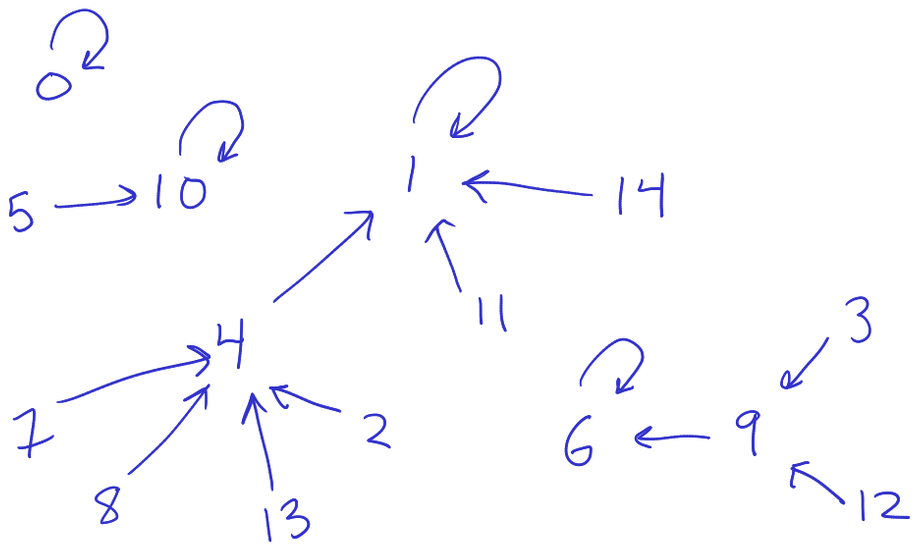
Then $0 \equiv x^2 - y^2 \equiv (x-y)(x+y) \pmod n$

$\not\equiv 0 \quad \not\equiv 0$

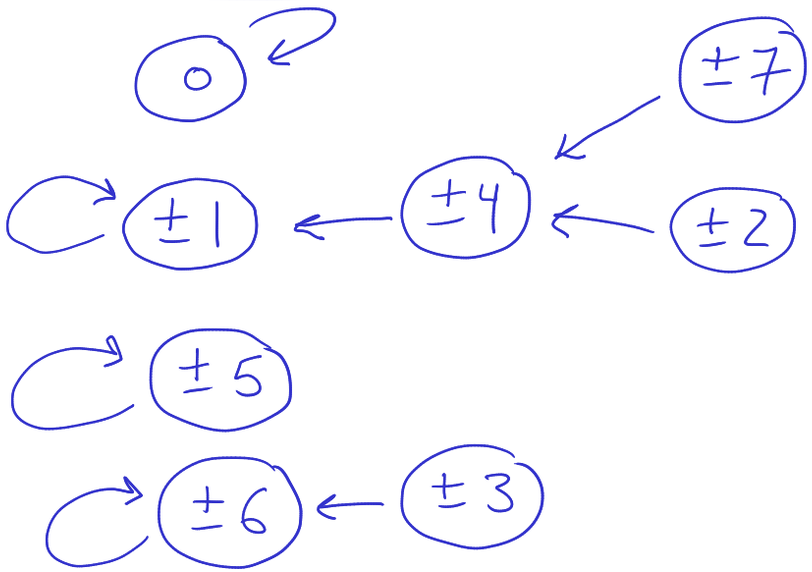
So $x+y$ and $x-y$ both contain a proper factor of $n$ (not 1 or $n$)

eg. $n = 15$

Squaring




Another way to draw




$x^2 \equiv y^2$

$8^2 \equiv 2^2 \pmod{15}$

but $8 \not\equiv \pm 2 \ (15)$

$x - y = 6$

$x + y = 10$

$\gcd(6, 15) = 3$

$\gcd(10, 15) = 5$

$\Rightarrow$ found factors of 15!

So.

finding interesting square roots mod $n$

i.e. $x^2 \equiv y^2 \pmod{n}$

$x \not\equiv \pm y \pmod{n}$

$\Longrightarrow$

factoring $n$ by taking $\gcd(x+y, n)$ or $\gcd(x-y, n)$

eg. $n = 295927$

notice $544^2 \equiv 3^2 \pmod{n}$ ???

$\gcd(n, 544-3) = 541$

in fact, $n = 541 \cdot 547$.

# Miller-Rabin Primality Test

Let $1 < a < n$ (pick randomly)

Write $n-1 = 2^k m$, $m$ odd

Consider chain:

$$a^m \longrightarrow a^{2m} \longrightarrow a^{4m} \longrightarrow \cdots \longrightarrow a^{2^k m} = a^{n-1} \boxed{\overset{?}{\equiv} 1}$$

Fermat Primality Test

What do we learn?

If $n$ is composite, there are 2 ways to notice:

ⓐ chain never gets to 1 at all (fails Fermat test)

ⓑ we see $x \longrightarrow 1$ in chain, $x \not\equiv \pm 1 \pmod n$

then we have interesting square roots ie. $\left(\begin{array}{c} x^2 \equiv 1^2 \equiv 1 \\ x \not\equiv \pm 1 \end{array}\right)$

Test: If we see ⓐ or ⓑ then composite.

If not, probably prime.

Ex. $n = 252601$

$n-1 = 252600 = 2^3 \cdot \overbrace{31575}^{\text{odd}}$

$a = 85132$ (pick randomly)

Chain:

$a^{31575} \xrightarrow{\text{sq}} a^{2 \cdot 31575} \xrightarrow{\text{sq}} a^{2^2 \cdot 31575} \xrightarrow{\text{sq}} a^{n-1}$

$191102 \qquad 184829 \longrightarrow 1 \qquad 1$

(b)

Composite!

---

Fermat Factoring If $n = x^2 - y^2$ then $x^2 \equiv y^2 \pmod{n}$

Try $n + 1^2 \stackrel{?}{=} \square$

$n + 2^2 \stackrel{?}{=} \square$

$n + 3^2 \stackrel{?}{=} \square$

Recall example $n = 295927$

$$295927 + 1 \neq \square$$
$$\| \quad + 2^2 \neq \square$$
$$\| \quad + 3^2 = 544^2$$

$$n = 544^2 - 3^2$$
$$= (544+3)(544-3)$$
$$= 547 \cdot 541$$

Observation: If $n = pq$ with $p$ & $q$ similar in size, then this factoring method may work well.

Moral: Don't choose $p$ near $q$ in RSA.

# Quadratic Sieve

① Factor base of small primes: $2, 3, 5, \ldots, p_k < B$

② Look for relations:

Let $k \sim \sqrt{n}$

Try to factor in factor base:

$k^2 - n$, $(k+1)^2 - n$, $(k+2)^2 - n$, etc.

Example. $n = 2201$ $k = 47$

$47^2 - n = 2^3$

$48^2 - n$ = doesn't factor in fac. base

$49^2 - n = 2^3 \cdot 5^2$

$47^2 \equiv 2^3 \pmod{n}$

$(3, 0)$ in fac. base $2, 5$

$49^2 \equiv 2^3 \cdot 5^2 \pmod{n}$

$(3, 2)$

$$\Rightarrow \quad 47^2 \cdot 49^2 \equiv 2^6 \cdot 5^2 \pmod{n}$$

$$(47 \cdot 49)^2 \equiv (2^3 \cdot 5)^2 \pmod{n}$$

$$\gcd(47 \cdot 49 - 2^3 \cdot 5, n) = 31$$



$$\begin{array}{r} (3,0) \\ +(3,2) \\ \hline (6,2) \end{array}$$ all even

---

## Quadratic Sieve

1) Choose factor base $p_1, p_2, \ldots p_m < B$
2) Let $k = \lceil \sqrt{n} \rceil$
3) Try to factor (in factor base) $k^2 - n$, $(k+1)^2 - n$, $(k+2)^2 - n$, ... etc.
4) Interpret factorizations as exponent vectors
   $ find a linear combination that has all even entries
   $\Rightarrow x^2 \equiv y^2 \pmod{n}$
5) If $x \not\equiv \pm y$, take $\gcd(x \pm y, n)$ $\longrightarrow$ get a proper factor of $n$.