Factoring.

Remind: Basic Ppl.

If $\left\{ \begin{array}{l} x^2 \equiv y^2 \pmod n \\ x \not\equiv \pm y \pmod n \end{array} \right\}$ then $\gcd(x-y, n)$ is a nontrivial factor of n.

$n = (x+y)(x-y) = x^2 - y^2$

Warmup: Fermat Factoring.

Idea: Look for $x^2 - n = y^2$ OR $n + y^2 = x^2$) then $x^2 \equiv y^2 \pmod n$

Algorithm: Compute $n+1^2$, $n+2^2$, $n+3^2$, ... and check if result is a square. (x^2)

($y=1$, $y=2$, y^2)

If $n = \underset{\text{primes}}{pq}$, it takes $\frac{|p-q|}{2}$ steps $\left\{ \begin{array}{l} p = x+y \\ q = x-y \end{array} \right\}$ difference $2y = |p-q| \Rightarrow y = \frac{|p-q|}{2}$

Lesson: In RSA, $n = pq$ is bad if $|p-q|$ is small.

Fix: Choose p, q not to close.

Quadratic Sieve (to factor n)

⓪ Pick a factor base of primes $< B$. (some, not all) $p_1, \dots, p_k$

① Collect facts:

$$x_j^2 \equiv \prod_i p_{i,j}^{a_{i,j}} \pmod{n}$$

② Combine facts to get an equivalence of squares:

e.g.

$$x^2 \equiv 2^4 \cdot 3 \cdot 5$$
$$y^2 \equiv 3 \cdot 5 \cdot 7$$
$$z^2 \equiv 7 \cdot 11^2$$

$$\Rightarrow \underbrace{(x \cdot y \cdot z)}_{X}^2 \equiv 2^4 \cdot 3^2 \cdot 5^2 \cdot 7^2 \cdot 11^2 \pmod{n}$$
$$\equiv \underbrace{(2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11)}_{Y}^2$$

$$X^2 \equiv Y^2 \pmod{n}$$

(0, 1, 1, 0, 0)
(0, 1, 1, 1, 0)
(0, 0, 0, 1, 0)
―――――――――
(0, 0, 0, 0, 0)

③ Check if it is a basic ppl example (take $\gcd(X-Y, n)$).

Note: Step ② is linear algebra

$$\prod p_i^{a_i} \longleftrightarrow v = (a_1, a_2, \dots, a_k) \in (\mathbb{Z}/2\mathbb{Z})^k$$

want: $\sum v_j = \vec{0}$

Hard Part is ① ⟶ Sieve.

Sieving.

Want: $x^2 \equiv \prod p_i^{e_i} \pmod n$

i.e. $x^2 = \prod p_i^{e_i} + kn$

try $k = 1$

$x^2 - n \Rightarrow$ try to factor as $\prod p_i^{e_i}$.

Factor Base:

$p_1, \dots, p_k \le B$

Def^n
An integer is B-smooth if it factorization is supported on prime $\le B$.

Start with a list of numbers: k^2-n, $(k+1)^2-n$, $(k+2)^2-n$, ... (form of x^2-n)

Want to find B-smooth #s in the list.

Naive solution: "B-factor" each #.
↳ means write as $\prod p_i^{e_i} \cdot m$ ← other stuff

Solution: Sieving.

Observation: $p \mid x^2 - n \iff x^2 \equiv n \pmod p \iff x \equiv \alpha, \beta \pmod p$
(if any solutions)

Can generalize to Number Field Sieve — fastest known method of factorization.

Runtime is <u>subexponential</u> (but not polynomial). $\approx O(e^{\sqrt[3]{n}})$