Quadratic Sieve

How it works

Quadratic Seive is an algorithm for factoring numbers based on the fact that n is composite and that you can find an x, y that satisfy these equations:

$$x^2 \equiv y^2 \pmod{n}$$

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

Once these can be satisfied you are able to easily factor n.

This is because once you have x, y you can compute:

$$\gcd(n, x + y)$$

$$\gcd(n, x - y)$$

which gives factors of n.

Example

12 divides $10^2 - 4^2 = (10 + 4)(10 - 4)$ but it doesn't divide either of the factors $10 + 4 = 14$ and $10 - 4 = 6$. But from these we can calculate:

$$\gcd(12, 14) = 2$$

$$\gcd(12, 6) = 6$$

Which are factors of 12!