Fermat Factorization

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

then $a = x - y$ and $b = x + y$.

Or $\underline{\underline{n = ab}}$

Conversely, let $n = ab$, with $a \geq b \geq 1$.

Then, $n = \left(\frac{a+b}{2}\right)^2 - \left(\frac{a-b}{2}\right)^2$.

Let n be $\underline{\underline{\text{odd}}}$ integer.

$\Rightarrow$ $\underline{a \text{ and } b}$ are $\underline{\text{odd}}$.

$\Rightarrow$ $\frac{a+b}{2}$ and $\frac{a-b}{2}$ are non-negative integers.

$\therefore$ Searching for factors a and b of n is same as searching for x & y such that $n = x^2 - y^2$.

Or $x^2 - n = y^2$.

Let k be the smallest integer such that $k^2 \geq n$.

Consider the sequence,

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

.....

Searching through the sequence until a number $m \geq \sqrt{n}$ such that $m^2 - n$ is a square.

i.e., $m^2 - n = y^2$

Now taking $x = m$ and y, we get $n = (x+y)(x-y)$

$= a \cdot b$

The process of searching must terminate as,

$$\left(\frac{n+1}{2}\right)^2 - n = \left(\frac{n-1}{2}\right)^2$$

Ex:- $n = 2279$

$\sqrt{n} = 47.73\ldots$

$k = 48 \Rightarrow 48^2 - n = 25 = 5^2$

$\therefore n = (48-5)(48+5)$

$= \underline{43 \times 53}$

Ex:- $n = 10541$

$\sqrt{n} = 102.66\ldots$

$k = 103 \Rightarrow k^2 - n = 68 \neq y^2$

$104 \Rightarrow = 275 \neq y^2$

$105 \Rightarrow = 484 = 22^2$

$\therefore x - y = 105 - 22 = 83$

$x + y = 105 + 22 = 127$

$\therefore \underline{10541 = 83 \times 127}$

Ex:- $n = 340663$.

$\sqrt{n} = 583.66$.

$k = 584 \Rightarrow k^2 - n = 393$

⋮

$k = 592 \Rightarrow k^2 - n = 9801 = 99^2$

$x - y = 493$ (not a prime)

$x + y = 691$ (prime)

$\sqrt{493} = 22.2\ldots$

$k = 23 \Rightarrow k^2 - 493 = 36 = 6^2$

$\therefore 493 = (23-6)(23+6)$

$= 17 \times 29$

$\therefore n = 340663 = 17 \times 29 \times 691$

HW

① Factor 200819

② Factor 809009

Generalized Fermat Factorization:-

We find x and y such that

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

$\Rightarrow x^2 - y^2 = kn \Rightarrow (x-y)(x+y) = kn$

Let $d = gcd(x-y, n)$

or $d = gcd(x+y, n)$.

$n \mid (x-y)(x+y)$

$\Rightarrow pq \mid (x-y)(x+y)$ (if $n = pq$)

If $p \mid x-y$ and $q \mid (x-y)$

$\Rightarrow pq \mid (x-y)$

$\Rightarrow x \equiv y \pmod{n}$

Similarly, if $p \mid x+y$ & $q \mid x+y$

$\Rightarrow x \equiv -y \pmod{n}$

In this case, we get $d = \gcd(x-y, n)$ is a trivial one.

∴ we want $x^2 \equiv y^2 \pmod{n}$

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

We choose a small k, and set $t = \lfloor \sqrt{kn} \rfloor + 1$, $\lfloor \sqrt{kn} \rfloor + 2$, etc. till we obtain

$t^2 - kn = s^2$ (a square)

$\Rightarrow (t+s)(t-s) = kn$

If $t \not\equiv \pm s \pmod{n}$, we

Find gcd $(t+3, n) = d$, a nontrivial divisor of n.

Ex :- $n = 141467$.

$t = 377, 378, \ldots\ldots$

$\Rightarrow$ Fermat factorization.

Let $t = \lceil \sqrt{3n} \rceil + 1 = 652$

$\Rightarrow 652^2 - 3n \neq s^2$

$\vdots$

$\Rightarrow 655^2 - 3 \cdot n = 68^2$

$\Rightarrow \gcd(655 - 68, 141467)$

$= 587$

$\Rightarrow n = 241 \times 587$

Ex:- $n = 68987$

$t = \lceil \sqrt{3n} \rceil + 1 = 455$

Ans: $n = 149 \times 463$

$n = 29895581$

$t = \lfloor \sqrt{3n} \rfloor + 2 = 9472$

$\Rightarrow n = 3217 \times 9293$

HW

19572079

17018759