

Fermat's Factorization method.

If a number 'n' can be expressed as $x^2 - y^2$ then its factors are $(x+y)(x-y)$

$$\text{i.e. } (x+y)(x-y) = n \text{ if } n = x^2 - y^2$$

Consequently if 'a' & 'b' are factors of a number 'n' such that $n = ab$

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

Example: Use Fermat's factorization method to factorize $n = 119143$

$$\text{Solution } 345^2 < 119143 < 346^2$$

$$\text{W.K.T } x^2 - y^2 = n$$

$$\therefore x^2 - n = y^2, \quad x, y \text{ are integers}$$

$$x \geq 346^2 \therefore y^2 \text{ is +ve}$$

$$\therefore 346^2 - 119143 = 119716 - 119143 = 573$$

$$347^2 - 119143 = 120409 - 119143 = 1266$$

$$348^2 - 119143 = 121104 - 119143 = 1961$$

$$349^2 - 119143 = 121801 - 119143 = 2658$$

~~34~~

$$350^2 - 119143 = 122500 - 119143 = 3357$$

$$351^2 - 119143 = 123201 - 119143 = 4058$$

$$352^2 - 119143 = 123904 - 119143 = 4761 = 69^2$$

which satisfies x, y are integers

$$\therefore x = 352, y = 69$$

$$\therefore n = (352 + 69)(352 - 69) = (421)(283)$$