The Fermat - Kraitchik Factorization Method

Given integer $n > 1$

Trial method Find a factor of n by dividing by all primes $\leq \sqrt{n}$

Ex. $n = 9 \quad \sqrt{n} = 3$

$P = 3 \quad P \leq \sqrt{3}$

if $2 \nmid 9, 3 \nmid 9 \Rightarrow n$ is not a prime.

if n is divisible by atleast one prime from $2, \cdots \sqrt{n}$ then n is not a prime o.w. n is prime.

First real improvement over the classical method of attempting to find a factor of n by dividing by all primes not exceeding $\sqrt{n}$, Fermat's described a technique of this for factoring large numbers.

Factoring of an odd integer n is equivalent to obtaining integral solutions x and y of the equation

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

If $n = x^2 - y^2$ (diff of two squares) then

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

Conversely, $n = ab \quad , \quad a \geq b \geq 1$

then $n = \left(\frac{a+b}{2}\right)^2 - \left(\frac{a-b}{2}\right)^2$ { $\because$ product of two odd integers is an odd integer }

$\because n$ is odd $\Rightarrow$ $a, b \rightarrow$ odd

$a = 2n+1 \quad b = 2n+1$

$\therefore \frac{a+b}{2}, \frac{a-b}{2}$ will be non negative integer

To find posible x and y satisfying $n = x^2 - y^2$;

we start $x^2 - n = y^2$

find smallest k s.t. $k^2 \geq n \Rightarrow (k^2 - n^2 \geq 0)$ $y^2 \geq 0$

then we look successively at the numbers

$k^2 - n$; $(k+1)^2 - n$, $(k+2)^2 - n$, $(k+3)^2 - n$, ...

untill a value of $m \geq \sqrt{n}$ is found

s.t. $m^2 - n \rightarrow$ a square

0, 1, 4, 9, 6, 5,

If an integer is a perfect square then its last two digits are

00	21	41	64	89
01	24	44	69	96
04	25	49	76	
09	29	56	81	
16	36	61	84	

Example: $n = 119143$

$345^2 < 119143 < 346^2$

$n < k^2$

→ $346^2 - 119143 = 119716 - 119143 = 573$ ✗ not a perfect square

→ $347^2 - 119143 = 120409 - 119143 = 1266?$ ✗

→ $348^2 - 119143 = 121104 - 119143 = 1961?$ ✗

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

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

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

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

$\therefore 352^2 - n = 69^2$

$\therefore \boxed{n = 352^2 - 69^2}$

47
47 | 1961
16
369
329

6
6 | 4761
36
1161
1149
12

$n = 23449$ Use fermat's method and find the factors;

the smallest square exceeding n is 154^2 so that the sequence

$$(153)^2 < 23449 < (154)^2$$

$$\therefore \quad n < k^2$$

$$k = 154$$

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

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

$$k^2 - n = y^2$$

$$k^2 - n = (154)^2 - 23449$$

$$= 23716 - 23449 = 267$$

$$(155)^2 - 23449 = 24025 - 23449 = 576 = 24^2$$

$$\therefore \quad 23449 = (155)^2 - (24)^2$$