Factorization

Fermat's Factorization method is based on the representation of an odd integer as the difference of two squares.
For an integer **n**, we want **a** and **b** such as:

$$n = a^2 - b2 = (a+b)(a-b)$$

where (a+b) and (a-b) are
the factors of the number n.

Example:

Fermat's factoring

$n = t^2 - s^2$

$(t+s)(t-s)$

$n = t^2 - s^2$

$s^2 = t^2 - n$.

$t = [\sqrt{n}] + 1$. if $t^2 - n$ is a perfect square

Ex: 809009

$n = 809009$

$t = [\sqrt{n}] + 1$

$t = [\sqrt{809009}] + 1$

$t = [899.44] + 1$

$t = [900.44]$. $= 900$

$s^2 = t^2 - n$.

$t^2 = (900)^2 \Rightarrow 810000$

$t^2 - n = 810000 - 809009$

$s^2 \Rightarrow 991$

$s = \sqrt{991} = 31.48$ - not a perfect square.

next tak $t = [\sqrt{n}] + 2$

$t = [900.44] + 2$

$= 902$.

$s^2 = t^2 - n$

$t^2 = (902)^2 \Rightarrow 813604$

$t^2 - n = 813604 - 809009$

$s^2 = 4595 \Rightarrow$ not a perfect square.

$t = [\sqrt{n}] + 3 \Rightarrow 6400 = (80)^2 =$ perfect square

$n = (t+s)(t-s)$

$= (903+80)(903-80)$

$n = 983 * 823$

$\therefore$ factorization.

2. Input: n = 6557
Output: [79,83]
Explanation:
For the above value,
the first try for a is ceil value
of square root of 6557, which is 81.

Then,
$b^2 = 81^2 - 6557 = 4$,
as it is a perfect square.
So, b = 2

So, the factors of 6557 are:
(a - b) = 81 -2 = 79 &
(a + b) = 81 + 2 = 83.