The Fermat-Kraitcheik Factorization Method

Krittapas Ngammuengman 6305146

November 28, 2023

Outline

Introduction

Example 1

Find the prime factorization of 2013.

Because $44 < \sqrt{2013} < 45$, it is enough to examine the primes $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43$.
We have

$$
\begin{aligned}
2013 &= 7 \times 289 \\
&= 7 \times 17 \times 17.
\end{aligned}
$$

Introduction

Example 1

Find the prime factorization of 2013.

Because $44 < \sqrt{2013} < 45$, it is enough to examine the primes $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43$.
We have

$$\begin{aligned} 2013 &= 7 \times 289 \\ &= 7 \times 17 \times 17. \end{aligned}$$

Fermat Factorization

Theorem 1 (Fermat Factorization)

If n is an odd positive integer, then there is a one-to-one correspondence between factorizations of n into two positive integers and differences of two squares that equal n. That is,

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

Proof I

Suppose that n be an odd positive integer with $n = ab$, whenever $a \geq b \geq 1$. Notice that

$$\begin{aligned} n &= ab \\ &= \left(\frac{a+b}{2} + \frac{a-b}{2}\right)\left(\frac{a+b}{2} - \frac{a-b}{2}\right) \\ &= \left(\frac{a+b}{2}\right)^2 - \left(\frac{a-b}{2}\right)^2 \end{aligned}$$

We set $s = \left(\frac{a+b}{2}\right)$ and $t = \left(\frac{a-b}{2}\right)$ are both integers because a and b are both odd.

Proof II

Conversely, assume that $n = s^2 - t^2$ where $s, t \in \mathbb{N}$.
Then it is clearly that n can be factored as

$$n = s^2 - t^2 = (s - t)(s + t).$$

Then we choose $a = s + t$ and $b = s - t$.
Moreover, because n is odd integer, then a and b are themselves odd. $\square$

The Algorithm

To search for possible x and y satisfying the equation

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

1. We write $s^2 - n = t^2$.
2. Determining the smallest integer $k^2 \geq n$.
3. We search for a square among the sequence of integers

$$k^2 - n,\ (k+1)^2 - n,\ (k+2)^2 - n,\ \ldots$$

Remark

It may be necessary to check as many as $\frac{(n+1)}{2} - \lfloor \sqrt{n} \rfloor$ integers to determine whether they are perfect squares.

Example

Example 2

Using the Fermat factorization method, factor the 2013.

We find that $44 < \sqrt{2013} < 45$, then it suffices to consider values of $k^2 - 2013$ for those k that satisfy the inequality $45 \le k < \dfrac{(2013+1)}{2} = 1007$. The calculations begin as follows:

$$45^2 - 2013 = 2025 - 2013 = 12$$
$$46^2 - 2013 = 2116 - 2013 = 103$$
$$47^2 - 2013 = 2209 - 2013 = 196 = 14^2$$

And then $2013 = 47^2 - 14^2 = (47+14)(47-14) = 61 \times 33$.

Example

Example 2

Using the Fermat factorization method, factor the 2013.

We find that $44 < \sqrt{2013} < 45$, then it suffices to consider values of $k^2 - 2013$ for those k that satisfy the inequality $45 \leq k < \dfrac{(2013+1)}{2} = 1007$. The calculations begin as follows:

$$
\begin{aligned}
45^2 - 2013 &= 2025 - 2013 = 12 \\
46^2 - 2013 &= 2116 - 2013 = 103 \\
47^2 - 2013 &= 2209 - 2013 = 196 = 14^2
\end{aligned}
$$

And then $2013 = 47^2 - 14^2 = (47+14)(47-14) = 61 \times 33$.

Example

Figure: Fermat's Factorization in spreadsheets

References

David M. Burton.
Elementary Number Theory.
McGraw-Hill Higher Education, 7th edition, 2010.

Kenneth H. Rosen.
Elementary Number Theory and Its Applications.
Pearson, 6th edition, 2011.