WEB3CLUBS FOUNDATION LIMITED

Course Instructor: DR. Cyprian Omukhwaya Sakwa
PHONE: +254723584205 Email: cypriansakwa@gmail.com

Foundational Mathematics for Web3 Builders

Lecture 23

June 11, 2024

2 Utilizing difference of squares in factorization

This approach applies the identity $x^2 - y^2 = (x+y)(x-y)$, which states that a difference of squares is equal to a product. To factor a number n, find an integer b such that $n + b^2$ is a perfect square, equivalent to, say a^2.

Then $n + b^2 = a^2 \implies n = a^2 - b^2 \implies n = (a-b)(a+b)$

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

Example 7

Factorize 713.

Solution

We determine an integer b that guarantees that $713 + b^2$ is a perfect square.

$713 + i^2$ where $i = 1, 2, 3, \ldots, 6$

$713 + 1^2 = 714$ not a square

$713 + 2^2 = 717$ not a square

$713 + 3^2 = 722$ not a square

$713 + 4^2 = 729 = 27^2$

Therefore $713 = 27^2 - 4^2 = (27 - 4)(27 + 4) = 23 \cdot 31$

$713 + 4^2 = 27^2$

$713 = 27^2 - 4^2$

$= (27+4)(27-4)$

$= 31 \times 23$

$713 = 31 \times 23$

Example 8

Factor 493.

Solution

We need to determine an integer b that guarantees that $493 + b^2$ is a perfect square. $\sqrt{494}$

$\sqrt{529} = \pm 23$

$493 + 1^2 = 494$ not a square

$493 + 2^2 = 497$ not a square

$493 + 3^2 = 502$ not a square

$493 + 4^2 = 509$ not a square

$493 + 5^2 = 518$ not a square

$493 + 6^2 = 529 = 23^2$

(m, e) $p, q \Rightarrow$ $\phi(m)$ $(p-1)(q-1)$

Therefore $493 = 23^2 - 6^2 = (23-6)(23+6) = 17 \cdot 29$ $e^{-1} = d$

$\therefore 493 + 6^2 = 23^2$

$493 = 23^2 - 6^2 = (23+6)(23-6) = 29 \times 17$

$493 = \underset{p}{29} \times \underset{q}{17}$

N

Example 9

Factor 20711.

Solution

We need to determine an integer b that guarantees that $20711 + b^2$ is a perfect square.

$20711 + 1^2 = 20712$ not a square

$20711 + 2^2 = 20715$ not a square

$20711 + 3^2 = 20720$ not a square

$20711 + 4^2 = 20727$ not a square

$20711 + 5^2 = 20736 = 144^2$

Therefore $20711 = 144^2 - 5^2 = (144 - 5)(144 + 5) = 139 \cdot 149$

$20711 + 5^2 = 144^2$

$20711 = 144^2 - 5^2$

$= (144+5)(144-5) = 149 \times 139$

$20711 = 149 \times 139$

Example 10

Factorize 1189

Solution

We need to determine an integer b that guarantees that $1189 + b^2$ is a perfect square.

$$
\begin{aligned}
1189 + 1^2 &= 1190 && \text{not a square} \\
1189 + 2^2 &= 1193 && \text{not a square} \\
1189 + 3^2 &= 1198 && \text{not a square} \\
11891 + 4^2 &= 1205 && \text{not a square} \\
11891 + 5^2 &= 1214 && \text{not a square} \\
1189 + 6^2 &= 1225 = 35^2
\end{aligned}
$$

Therefore $1189 = 35^2 - 6^2 = (35 - 6)(35 + 6) = 29 \cdot 41$

$1189 + 6^2 = 35^2$

$1189 = 35^2 - 6^2 = (35+6)(35-6) = 41 \times 29$

- It is rare that $n+b^2$ will become a perfect square for a randomly selected value of b if n is large.
- To work around this, it is sufficient to represent a multiple kn of n as a difference of two squares, so that
$$kn = a^2 - b^2 = (a-b)(a+b).$$
- Then, by computing $\gcd(n, a+b)$ and $\gcd(n, a-b)$, the factors may be recovered.

  We provide the following examples to help clarify.

Example 11

Factorize 22881.

Solution

When we list the values of $3n + b^2$, we find;

$3 \cdot 22881 + 1^2 = 68644 = 262^2$

Thus, $3 \cdot 22881 = 262^2 - 1^2 = (262 + 1)(262 - 1) = 263 \cdot 261$.

Compute $\gcd(22881, 263) = 263$ and

$\gcd(22881, 261) = 87$.

Thus the factors of 22881 are 87 and 263 and so $22881 = 87 \cdot 263$.

Example 12

Factorize $n = 3589$.

Solution

$3\cdot 3589+7=104^2$

When we list the values of $3n+b^2$, we find;

$3\cdot 3589+1^2=10768$ not a square

$3\cdot 3589+2^2=10771$ not a square

$3\cdot 3589+3^2=10776$ not a square

$3\cdot 3589+4^2=10783$ not a square

$3\cdot 3589+5^2=10792$ not a square

$3\cdot 3589+6^2=10803$ not a square

$3\cdot 3589+7^2=10816=104^2$

$3\cdot 3589=104^2-7^2=(104+7)(104-7)$

Thus, $3\cdot 3589=104^2-7^2=(104+7)(104-7)=111\cdot 97.$

Compute $\gcd(3589,111)=37$ and $\gcd(3589,97)=97.$

Thus the factors of 3589 are 37 and 97 and so $3589=37\cdot 97.$

Example 13

Factorize $24459.$

Solution

When we list the values of $3n + b^2$, we find;

$3 \cdot 24459 + 8^2 = 271^2$

$$3 \cdot 24459 + 1^2 = \cancel{10768}\ 73378 \quad \text{not a square}$$

$$3 \cdot 24459 = 271^2 - 8^2 = (271+8)(271-8) = 279 \times 263$$

$$3 \cdot 24459 + 2^2 = \cancel{10771}\ 73381 \quad \text{not a square}$$

$$3 \cdot 24459 + 3^2 = \cancel{10776}\ 73386 \quad \text{not a square}$$

$$3 \cdot 24459 + 4^2 = \cancel{10783}\ 73393 \quad \text{not a square}$$

$\gcd(24459, 279) = 93$

$$3 \cdot 24459 + 5^2 = \cancel{10792}\ 73402 \quad \text{not a square}$$

$\gcd(24459, 263) = 263$

$$3 \cdot 24459 + 6^2 = \cancel{10803}\ 73413 \quad \text{not a square}$$

$$3 \cdot 24459 + 7^2 = \cancel{10803}\ 73426 \quad \text{not a square}$$

$$3 \cdot 24459 + 8^2 = 73441 = 271^2$$

$93 = 3 \cdot 31$

Thus, $3 \cdot 24459 = 271^2 - 8^2 = (271 + 8)(271 - 8) = 279 \cdot 263$.

$3 \cdot 31 \cdot 263$

Compute $\gcd(24459, 279) = 93$ and $\gcd(24459, 263) = 263$.

Thus the factors of 24459 are $93 = 3 \cdot 31$ and 263 and so

$24459 = 3 \cdot 31 \cdot 263$.