BOHR

ISSN (online) 2583-2026

BOHR International Journal of Smart Computing and Information Technology
2022, Vol. 3, No. 1, pp. 1–8
https://doi.org/10.54646/bijscit.011
www.bohrpub.com

Large Semi Primes Factorization with Its Implications to RSA Cryptosystems

Richard Omollo and Arnold Okoth

Department of Computer Science and Software Engineering, School of Informatics and Innovative Systems, Jaramogi Oginga Odinga University of Science and Technology, Box 210-40601, Bondo-Kenya
E-mail: richard.otieno@gmail.com; arnolaeustein9790@gmail.com

Abstract. RSA's strong cryptosystem works on the principle that there are no trivial solutions to integer factorization. Furthermore, factorization of very large semi primes cannot be done in polynomial time when it comes to the processing power of classical computers. In this paper, we present the analysis of Fermat's Last Theorem and Arnold's Theorem. Also highlighted include new techniques such as Arnold's Digitized Summation Technique (A.D.S.T.) and a top-to-bottom, bottom-to-top approach search for the prime factors. These drastically reduce the time taken to factorize large semi primes as for the case in RSA Cryptosystem.

Keywords: Arnold's theorem, Fermat Last Theorem, RSA Cryptosystem, semi primes, factorization limit, Fermat method, RSA numbers.

INTRODUCTION

In the year 1978, Ronald Rivest, Adi Shamir and Leonard Adleman released one of the first public-key cryptosystem [1] known as RSA Cryptosystem. It has been over 40 years down the line and it still one of the strongest cryptosystems in the world. It takes one of the greatest problems in Number Theory (integer factorization) to be one of the most suitable solutions to computer security. There are still no trivial solutions to the factorization of semi primes. The RSA Cryptosystem works on the basis of multiplying two relatively large prime numbers k and l of at least 50 digits each [2, 3]. The semi prime (y) obtained can be as big as 100 to 600 digits (500 to 2048 bits). Attempts have been made to crack these RSA numbers with modern factorization methods such as the Elliptic Curve Method, Quadratic Field Sieve and the Number Field Sieve [8]. Still, the factorization of these large semi primes might take several months even for a supercomputer. It takes an estimated 2000 years' work for a 2.2 GHz Opteron computer to factorize a 232 digit RSA number [4].

Recently, there have been advancements in the field of quantum cryptography which might lead to the possibility of factorizing these large semi primes in just a few days if not hours [6]. The Shor Algorithm is one of the most commonly used algorithms in quantum computing developed by Peter Shor. Though quantum cryptography seems promising, they are still not yet widely applicable [7]. This might remain the case for the next few years to come. In comparison, classical computers still cannot factorize very large semi primes in polynomial time [22, 23]. At least not until there are significant technical developments in the processing power of the classical computers or a breakthrough is found for integer factorization. If a trivial solution is found for integer factorization then the RSA Cryptosystem would be rendered useless [5].

We are going to analyze a version of Fermat's Last Theorem and Arnold's Theorem for right angled triangles. From the Fermat's Last Theorem, we obtain the shortened Diophantine equation

$$x^2 = z^2 = y$$

This equation can be further expanded to $(x+z)(x-z) = y$. From the first part of the equation you get the equations $x+z = k$ and $x-z = l$ where the value of y is the semi prime; k and l are the two prime factors for y.

$$x, y, z, k, l, \in N$$

That equation is used to form the Fermat's method for factorization [9–13]. We also look at Arnold's Theorem which is rived from the Pythagorean equation $a^2 + b^2 = c^2$ which can be written as $a^2 = c^2 - b^2$ [21]. This can be expanded to the equation $a^2 = (c+b)(c-b)$. So if $c - b = 1$ it will leave us with the equation $a^2 = b + c$.

Therefore, the two equations which form Arnold's Theorem for right angled triangles are $a^2 = b + c$ and $c - b = 1$. They are very critical in setting up a factorization limit which will in turn create a different angle for finding the prime factors.

The technique employed after getting the factorization limit is referred to as the top-to-bottom, bottom-to-top approach. It involves several independent operations which will be running simultaneously from two points A to B, B being the factorization limit. There are two operations; one will run from point A heading towards point B and the other running from point B heading towards point A. there will also be two other operations starting from the central point O. One will run from point O towards point A and the other will run from point O towards point B. Therefore, if the prime difference between the two prime factors is too big, too small of too centralized you will find it in just a matter of seconds. This was a problem with Fermat method for factorization [15–20].

Techniques such as Arnold's Digitized Summation Technique (A.D.S.T.) helps identify hidden properties of large semi primes used in RSA Cryptography. It simply involves adding the digits of a number until one is left with only one single digit [14]. Since RSA numbers have hundreds of digits, A.D.S.T. is going to bring them down to just one digit. That is combined with the operation, which will always give you a multiple of 4. These techniques are solely meant to drastically reduce the time taken to factorize large semi primes. This aligns with the objective of the paper which is to be able to factorize and factorize RSA numbers in polynomial time using the processing power of the average classical computer.

RESEARCH METHODOLOGY

Here, we give the definitions of some terms which are helpful as the research methodology.

Definition 1. Arnold's Digitized Summation Technique (A.D.S.T.): This refers to the subsequent addition of the digits of a number until you are left with only one single digit.

Definition 2. Digitized number form (D.N.F.): This refers to the digit you obtain after applying A.D.S.T. to a number.

Definition 3. Semi primes: These refer to composite numbers which only have two prime factors.

Definition 4. Prime difference: This refers to the difference between the two prime factors of the semi prime.

Definition 5. Factorization limit: This refers to the point where you have the largest possible prime difference between the two prime factors of the semi prime.

RESULTS AND DISCUSSIONS

Here, we give the results of the study and further discussion. We start with the analysis of a version of Fermat Last Theorem which involves squares and then Arnold's Theorem on right angled triangles.

Theorem 6. If y is a semi prime in $x^2 - z^2 = \mathrm{y}$ which can be expanded to $(x+z)\ (x-z) = y$, then $(x+z) = k$ and $(x-z) = l$ where k and l are the two prime factors of the semi prime y such that $k > l$.

Proof

We have seen that $k \times l = y$ from the statement above. Also $k - l = d$, where (d) is the prime difference and (y) is the semi prime. From the Gold Bach Conjecture we observe that when you add two prime numbers you will eventually have an even number. This is true for prime numbers greater than 2. From that we get that $k + l = 2x$.

The above equation means that x is half the value of the two prime numbers k and l. It can also be written as $k = 2x - l$. We now replace k from the two equations $k \times l = y$ and $k + l = 2x$. The equation $k \times l = y$ will be $(2x - l)l = y$ which is $2xl - l^2 = \mathrm{y}$ and $k + l = 2x$ will be $2x - l + l = 2x$. The equation $2xl - l^2 = y$ can be rewritten as the quadratic equation;

$$l^2 - 2\mathrm{xl} + \mathrm{y} = 0$$

This will give us the two equations $l = x - \sqrt{x^2 - y}$ and $k = x + \sqrt{x^2 - y}$. So let us say that $\sqrt{x^2 - y} = z$. We get that $l = x - z$ and $k = x + z$. Therefore, the equation $k \times l = y$ is written as $(x+z)(x-z) = y$. This equation can be written as

$$x^2 - z^2 = \mathrm{y}$$

We have seen that $x + z = k$ and $x - z = l$. From the two equations we get that z can be expressed as $z = k - x$ and $z = x - l$. Combining the two equations we get $k - x = x - l$ and $k + l = 2x$. Dividing both sides by 2, one gets that $x = \frac{k+l}{2}$. Replacing the x in the equation $z = k - z$ we get $z = k + \frac{k+l}{2}$. This can be factored into the equation $z = \frac{k-l}{2}$.

Replacing the x and z in the equation $x^2 - z^2 = \mathrm{y}$ with $x = \frac{k+l}{2}$ and $z = \frac{k-l}{2}$.

We get

$$\left(\frac{k+l}{2}\right)^2 - \left(\frac{k-l}{2}\right)^2 = \mathrm{y}$$

The equation $(\frac{k+l}{2})^2$ is expanded to

$$\frac{\mathrm{k}^2 + 2kl + l^2}{4}$$

And the equation $(\frac{k-l}{2})^2$ is expanded to

$$\frac{\mathrm{k}^2 - 2kl + l^2}{4}$$

Therefore,

$$\left(\frac{k+l}{2}\right)^2 - \left(\frac{k-l}{2}\right)^2 = y$$

becomes

$$\frac{k^2+2kl+l^2}{4}-\frac{k^2-2kl+l^2}{4}=y$$

Solving the equation, we get,

$$\begin{aligned}&\frac{k^2+2kl+l^2}{4}-\frac{k^2-2kl+l^2}{4}\\&=\frac{k^2+2kl+l^2-k^2+2kl-l^2}{4}=\frac{4kl}{4}=kl\end{aligned}$$

Hence;

$$y=kl$$

We have observed that z can be expressed as the equation $z=\frac{k-l}{2}$ and $k-l=d$. So by replacing $k-l$ with d in the first equation, we get that $z=\frac{d}{2}$. This can also be written as

$$d=2z$$

also since $(x+z)(x-z)=y$ and $d=(x+z)-(x-z)$. This gives us $d=x+z-x=z$ which can be solved back to $d=2z$. The value of d and z are directly proportional, so if the prime difference is big then the z is also be big. Also, we know that $x>z$, so during computation it takes a longer time to find the value of x if d is very large. This is because using the Fermat method for factorizing semi primes; we first start by the searching for the value of x.

From the equations above we can tell that just by having the semi prime and the prime difference we obtain the two other prime numbers k and l. This is majorly due to the fact that $d=2z$.

Problem. Given the semi prime 55, one finds the two prime numbers given that the prime difference is 6?

Solution. Since $z=\frac{d}{2}$

$$z=\frac{6}{2}=3$$

We also know that $x^2-z^2=\mathrm{y}$ and we have the value for z and y. After replacing these values, we get the equation $x^2-3^2=55$ which is $x^2=55+9=64$. Therefore, x will be 8. We also saw that $x+z=k$ and $x-z=l$ where k and l are the two prime numbers.

So $8+3=k$ and $8-3=l$

The two prime numbers will be $k=11$ and $l=5$.

$$k,l,x,y,z,d\in N$$

Theorem 7. Arnold's Theorem for right angled triangle states that $a^2=\mathrm{b}+\mathrm{c}$. If a is the smallest side of a right-angled triangle where $a\neq b$ and $a<b$ then $c-b=1$

Proof

The Pythagorean equation $a^2+b^2=c^2$ can also be written as $a^2=c^2-b^2$. This can be expanded to the equation $a^2=(c+b)(c-b)$. So if $c-b=1$ it leaves us with the equation $a^2=\mathrm{b}+\mathrm{c}$.

Therefore, the two equations which form Arnold's Theorem for right angled triangles are

$$a^2=\mathrm{b}+\mathrm{c}$$

and

$$c-b=1$$

Using the two equations we can formulate the simultaneous equation

$$\begin{gathered}c+b=a^2\text{ (Equation i)}\\c-b=1\text{ (Equation ii)}\end{gathered}$$

So when a right angled triangle satisfies both equation and we are only given the value of a, we can easily obtain the two other sides. This is possible through the simultaneous equation above. This brings us back to the equation $x^2-z^2=\mathrm{y}$ in Theorem 6. In this case, we replace a^2 with y. So when you are only given the semi prime y, one solves it using the simultaneous equation

$$\begin{gathered}x+z=y\text{ (Equation i)}\\x-z=1\text{ (Equation ii)}\end{gathered}$$

Problem. Given the semi prime 55 can you obtain the two prime numbers k and l. (Note that this time we are not given the prime difference.)

Solution

$$\begin{gathered}x+z=55\text{ (Equation i)}\\x-z=1\text{ (Equation ii)}\end{gathered}$$

This will give you $z=27$. To get the value of x we substitute z from (equation i) with 27. This will give us $x+27=55$ $x=28$. Therefore, the equation $x^2-z^2=\mathrm{y}$ will be $28^2-27^2=55$.

To find the two prime numbers we used the two equations $x+z=k$ and $x-z=l$ where k and l are the two prime numbers. In this case we notice something very interesting with our values for k and l

$$\begin{gathered}28+27=k\\28-27=l\end{gathered}$$

Therefore, k and l will be 55 and 1. This means that using Arnold's Theorem of right-angled triangles; it treats the semi prime as an actual prime number. So how is this important to us? The Fermat method for factorization searches for the prime difference of a semi prime y from 1 till an undefined value. Using Arnold's Theorem, we set a limit to the largest prime difference a semi prime can have. By treating a semi prime as a prime number, it means that the prime difference will be the largest since it is

$k-1$. That is, we are only subtracting one from the largest prime number k. When we subtract any value larger than 1 then the prime difference have a much smaller value. The largest possible prime difference is what is referred to as the factorization limit. So during the search for the prime difference through the search of z, we run two operations simultaneously. One starts from where the prime difference is smallest as it runs towards the largest possible value for the prime difference. This is actually what happens with the Fermat method for factorization. The other operation runs from the largest possible value for the prime difference as it heads down towards the smallest value. When we say that it searches through the prime difference, what we mean is that we modify the search for z since the prime difference is directly proportional to z. The search uses the equation $x^2 - z^2 = \text{y}$ and we saw that $d = 2z$.

RSA Cryptosystem

RSA Cryptosystem relies on the fact that finding the prime difference of two large prime numbers of at least 50 digits each cannot actually be done in polynomial time using a single 2.2 GHz Opteron computer. However, adding this new property into the equation it increases our chances of finding the prime difference even if it is too big. Furthermore, if the prime difference is too big or too small, we find it very fast using the two operations which runs simultaneously. So the most ideal prime difference for RSA numbers are not be too large or too small. It should be centralized. However, since we have the highest and lowest point where the values of the prime difference are, we can actually modify the computer operations to also accommodate the prime difference being centralized. This is demonstrated on Figure 1 where point A is where the prime difference is smallest, point O is where the prime difference is centralized and point B is where the prime difference is largest. Actually, we run a total of 4 operations simultaneously to find the prime difference much faster. The first operation starts at point A heading towards point O. The second operation starts at point O heading towards point A. The third operation also starts at point O but this time heading towards point B. The final operation starts at point B heading towards point O. This is what is referred to as the top-to-bottom, bottom-to-top approach.

Note that this is just the primary application of that concept. One can actually split point A to point O twice and point O to point B also twice such that we have a total of 8 operations running simultaneously. One can have as many operations running simultaneously depending on the size of the semi prime. For semi primes up to about 50 digits, having four operations running simultaneously is enough. But when the semi prime is about 600 digits as the case with RSA numbers, we can even have 32 operations running simultaneously. This however depends on the processing power of the computer. The operations are not exactly tied to be done on one computer. One can also assign as many computers as he/she wish to run some of the operations. This depends on the availability and practicality of using many computers in the first place. There are other properties of semi primes that we will see ahead that also help in reducing the number of tests the operations entail.

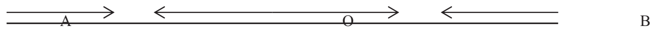


Figure 1. Top-to-bottom, bottom-to-top approach for finding the prime difference.

Going back to the equation $x^2 - z^2 = \text{y}$, we realize that the expression $x - z$ does not have to be 1 as stated in Arnold's Theorem for right angled triangles. We can try it with other integers 1, 2, 3, 4... and subject it to the simultaneous equation. If we let $x - z = 2$ we get that the equation $x^2 - z^2 = \text{y}$ is expanded to $(x+z)(x-z) = y$. So if $x - z = 2$ the two equations will be

$$2x + 2z = y \text{ (Equation i)}$$
$$x - z = 2 \text{ (Equation ii)}$$

Solving for the semi prime 55 we will get

$$2x + 2z = 55 \text{ (Equation i)}$$
$$x - z = 2 \text{ (Equation ii)}$$

We multiply equation Eqn. (ii) by 2 and add the two equations which give us $x = 14.75$. Substituting the x in equation ii we get that $z = 14.75 - 2$. Therefore, $x = 14.75$ and $z = 12.75$.

From the Table 1 above we observe that only when $x - z$ is 1, 5 and 11 is when the values of x, y and z are whole numbers. That is $x, y, z \in Z$. We also observe that the integers of $x - z$ are the same when $x - z = l$ and $x + z = k$ which in our case is 5 and 11. But for $x - z = 11$ the 3 in z is negative. The real value for $x - z$ is actually 6 but in our case, it gives us different values for x and z. However, when we use 6 as the prime difference in Fermat's Last Theorem equation $x^2 - z^2 = y$ we obtained the values for x and z to be 8 and 3 respectively. Furthermore, one

Table 1. The values of $x - z$ from 1 to 11 for the semi prime 55.

$x-z$	$x^2 - z^2 =$	y
1	$28^2 - 27^2 =$	55
2	$14.75^2 - 12.75^2 =$	55
3	$10.66667^2 - 7.66667^2 =$	55
4	$8.875^2 - 4.875^2 =$	55
5	$8^2 - 3^2 =$	55
6	$7.58333^2 - 1.58333^2 =$	55
7	$7.42857^2 - 0.42857^2 =$	55
8	$7.4375^2 - (-0.5625)^2 =$	55
9	$7.55556^2 - (-1.44444)^2 =$	55
10	$7.75^2 - (-2.55)^2 =$	55
11	$8^2 - (-3)^2 =$	55

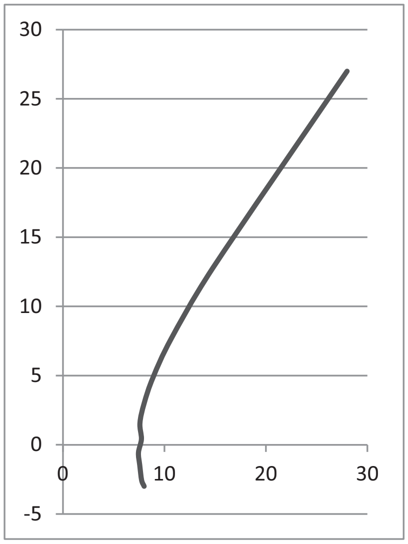


Figure 2. The graph shows the plotted values for the different values of $x - z$ in $x^2 - z^2 = 55$.

also notice that for $(x - z) > 6$ which is the actual prime difference between the two prime numbers the value of z are less than one. That is $z < 1$.

The y-axis represents x^2 while the x-axis represents z^2. The use of such curves is used in another complex method of factorizing numbers known as the *Elliptic Curve Method* which is not discussed in depth in this paper.

Arnold's Digitized Summation Technique (A.D.S.T.)

We are now going to bring in Arnold's Digitized Summation Technique which simply involves adding the digits of a number until one is left with only one digit. When one adds the digit of a number like 1234 one gets $1 + 2 + 3 + 4 = 10$, which one keeps adding till he is left with only one digit, so if one gets 10 one adds $1 + 0 = 1$. The process of adding is what is referred to as A.D.S.T. The resultant digit 1 becomes the Digitized Number Form (D.N.F.) of the number 1234. Since RSA Cryptosystem is based on using very large numbers even up to 600 digits, we are going to utilize A.D.S.T to look at some properties of such numbers which would otherwise be hard to observe. The Python code below is supposed to sum down a 1000 digits number into a single digit in just a few seconds.

Considering that we are only given the semi prime (y), we first need to find the digitized number form through A.D.S.T. In other words, we need to add the digits of that semi prime until we are left with only one single digit. Since the semi primes in the case of RSA numbers have over 100 digits, the Python code above is of great help since it can find the D.N.F. of a-thousand-digit semi prime in just a second. If the Digitized Number Form (D.N.F.) is 2, 5 or 8, it means that the semi prime is of the form $6n - 1$. If it is 1, 4 or 7, it means that the semi prime is of the form $6n + 1$.

Table 2. D.N.F. of the values of x and z when the D.N.F. of the semi primes are 2, 5 and 8.

x^2	$-$	z^2	$=$	y
9	$-$	7	$=$	2
9	$-$	4	$=$	5
9	$-$	1	$=$	8

Table 3. D.N.F. of the values of x and z when the D.N.F. of the semi primes are 1, 4 and 7.

x^2	$-$	z^2	$=$	y
1	$-$	9	$=$	1
4	$-$	9	$=$	4
7	$-$	9	$=$	7

A semi prime cannot have a D.N.F. of 3, 6 or 9. This is because such numbers are all multiples of 3. This holds true if the semi prime is an odd number, which is true for almost all cases apart from when another prime number is multiplied by 2 which is also a prime number.

Examples

$55 = 5 + 5 = 10$, $10 = 1 + 0 = 1$ D.N.F. of 55 is 1 and is of the form $(6n + 1)$

$65 = 6 + 5 = 11$, $11 = 1 + 1 = 2$ D.N.F. of 65 is 2 and is of the form $(6n - 1)$

$99 = 9 + 9 = 18$, $18 = 1 + 8 = 9$ D.N.F. of 99 is 9 and it will be a multiple of 3

For even numbers, if a number has a D.N.F. of 1, 4 or 7, then it is of the form $3n + 1$ where n is an odd number. If a number has a D.N.F. of 2, 5 or 8, then it is of the form $3n - 1$. If it has a D.N.F. of 3, 6 or 9 it still remains to be a multiple of 3. So how does A.D.S.T. come in to the actual equation used in the factorization process?

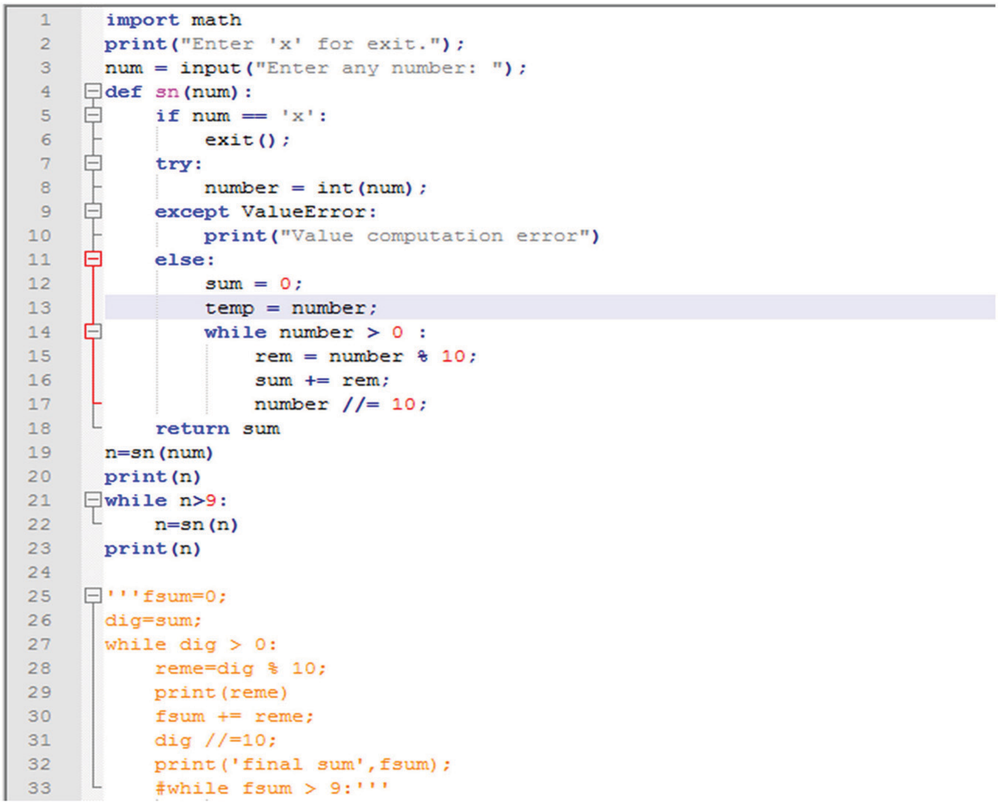
Arnold's Digitized Summation Technique and the $x^2 - z^2 = y$ Equation

When we look at the D.N.F. of numbers forming the equation $x^2 - z^2 = y$, we notice something very interesting. Below, we have highlighted two tables which form the basic identities for semi primes having either a D.N.F. of 1, 4 and 7 or 2, 5 and 8.

From Table 2 we notice that all the values of x^2 have a D.N.F. of 9 and from Table 3, we notice that all the values of z^2 have a D.N.F. of 9. This means that those values are actually multiples of 9. This property is seen with the multiples of 9 shown below.

Example

$9 = 9$ D.N.F. is 9
$18 = 1 + 8 = 9$ D.N.F. is 9
$27 = 2 + 7 = 9$ D.N.F. is 9
$36 = 3 + 6 = 9$ D.N.F. is 9
$45 = 4 + 5 = 9$ D.N.F. is 9
$54 = 5 + 4 = 9$ D.N.F. is 9



```
import math
print("Enter 'x' for exit.");
num = input("Enter any number: ");
def sn(num):
    if num == 'x':
        exit();
    try:
        number = int(num);
    except ValueError:
        print("Value computation error")
    else:
        sum = 0;
        temp = number;
        while number > 0 :
            rem = number % 10;
            sum += rem;
            number //= 10;
    return sum
n=sn(num)
print(n)
while n>9:
    n=sn(n)
print(n)

'''fsum=0;
dig=sum;
while dig > 0:
    reme=dig % 10;
    print(reme)
    fsum += reme;
    dig //=10;
    print('final sum',fsum);
    #while fsum > 9:'''
```

Figure 3. Python code showing how you can obtain the A.D.S.T. of a number.

Table 4. Real values of x, y and z when the D.N.F. of the semi primes are 2, 5 and 8.

x^2	$-$	z^2	$=$	y
81	$-$	16	$=$	65
81	$-$	4	$=$	77
36	$-$	1	$=$	35

Table 5. D.N.F. of x, y and z for the values in Table 4.

x^2	$-$	z^2	$=$	y
9	$-$	7	$=$	2
9	$-$	4	$=$	5
9	$-$	1	$=$	8

$63 = 6 + 3 = 9$ D.N.F. is 9
$72 = 7 + 2 = 9$ D.N.F. is 9
$81 = 8 + 1 = 9$ D.N.F. is 9
$90 = 9 + 0 = 9$ D.N.F. is 9

Examples of real values of $x^2 - z^2 = $ y and their D.N.F. are shown on the tables below. The values of Table 4 and 6 are obtained from Fermat Last Theorem as shown in Theorem 6.

Now we are look at examples of real values $x^2 - z^2 = $ y and their D.N.F. This time the values of Tables 8 and 10 are obtained from Arnold's Theorem for right angled triangles as shown in Theorem 7.

Table 6. Real values of x, y and z when the D.N.F. of the semi primes are 1, 4 and 7.

x^2	$-$	z^2	$=$	y
64	$-$	9	$=$	55
256	$-$	9	$=$	247
196	$-$	81	$=$	115

Table 7. D.N.F. of x, y and z for the values in Table 6.

x^2	$-$	z^2	$=$	y
1	$-$	9	$=$	1
4	$-$	9	$=$	4
7	$-$	9	$=$	7

Table 8. Real values of x, y and z when the D.N.F. of the semi primes are 2, 5 and 8.

x^2	$-$	z^2	$=$	y
1089	$-$	1024	$=$	65
1521	$-$	1444	$=$	77
324	$-$	289	$=$	35

It is important to note that the values for the semi prime y are the same for Tables 4 and 8. The same is seen with Tables 6 and 10 which have the same values for y. But as we saw earlier, the two theorems give different values for x and z. However, the D.N.F. identity actually remains the same when we use either of the two theorems.

Table 9. D.N.F. of x, y and z for the values in Table 8.

x^2	$-$	z^2	$=$	y
9	$-$	7	$=$	2
9	$-$	4	$=$	5
9	$-$	1	$=$	8

Table 10. Real values of x, y and z when the D.N.F. of the semi primes are 1, 4 and 7.

x^2	$-$	z^2	$=$	y
784	$-$	729	$=$	55
15376	$-$	15129	$=$	247
3364	$-$	3249	$=$	115

Table 11. D.N.F. of x, y and z for the values in Table 10.

x^2	$-$	z^2	$=$	y
1	$-$	9	$=$	1
4	$-$	9	$=$	4
7	$-$	9	$=$	7

From Tables 4, 6, 8 and 10 we also notice that if x^2 or z^2 is an even number in $x^2 - z^2 =$ y (Fermat's Last Theorem) then it also be an even number in $x^2 - z^2 =$ y (Arnold's Theorem)

Arnold's Digitized Summation Technique and the $y \pm 1$ Operation

Here we look at the final step in an attempt to factorize large semi primes in polynomial time. We have a total of 4 scenarios for the $y \pm 1$ operation.

i. If y + 1 is divisible by 4 and y has a D.N.F. of 2, 5 or 8, then x^2 is divisible by 36.
ii. If y − 1 is divisible by 4 and y has a D.N.F. of 2, 5 or 8, then z^2 is divisible by 4.
iii. If y + 1 is divisible by 4 and y has a D.N.F. of 1, 4 or 7, then x^2 is divisible by 4.
iv. If y − 1 is divisible by 4 and y has a D.N.F. of 1, 4 or 7, then z^2 is divisible by 36.

We obtained these properties of the semi primes while trying to find the trivial solution for integer factorization. Eventually, we did not get any trivial solution after the analysis of several semi primes and composite numbers in general. However, by studying the sequence of semi primes containing the same D.N.F., we were able to come up with the four definite scenarios shown above. They are incorporated into the programs which were running simultaneously in search for the value of x^2 and z^2. They are able to drastically reduce the time taken to factor large semi primes once combined with the top-to-bottom, bottom-to-top approach. We are still carrying out further research in search for a trivial solution for integer factorization.

CONCLUSION

We can be able to conclude that it is technically possible to factorize relatively large semi primes in polynomial time using the processing power of the average classical computer. Using techniques such as Arnold's Digitized Summation Technique (A.D.S.T.) and the top-to-bottom, bottom-to-top approach, the time taken to factorize large semi primes will be drastically reduced. This, we find that has greater implications on RSA which is about large prime numbers. Our paper provides an insight into reviewing RSA and excites further research interests in co-primes and primes, as a breakthrough to improving cryptographic chances in computer and network security in regards to data.

CONFLICTS OF INTEREST

Authors declares no conflict of interest.

REFERENCES

[1] Nigel Smart, "Cryptography: An Introduction", 3rd Edition, McGraw-Hill College, 2004; pp. 433.

[2] Jonathan Katz and Yehuda Lindell, "Introduction to Modern Cryptography", CRC Press, Boca Raton London New York Washington, DC 2007; pp. 248.

[3] Luis Finotti, "A Gentle Introduction to Number Theory and Cryptography", Lecture Notes, 2009; pp. 60. Website: https://www.math.utk.edu/~finotti/papers/grad.pdf [Accessed: April 2022].

[4] Boaz Barak, "An Intensive Introduction to Cryptography", Lecture Notes, 2018; pp. 366. Website: https://files.boazbarak.org/crypto/lnotes_book.pdf [Accessed: April 2022].

[5] Bruce Schneier, "Applied Cryptography: Protocols, Algorithms, and Source Code in C", John Wiley & Sons, 1996; pp. 784.

[6] Matthew Hayward, "Quantum Computing and Shor's Algorithm", Lecture Notes, 2015; pp. 59. Website: https://pdfs.semanticscholar.org/8072/dc7247460849b18abbb463429a09cfb2e3e6.pdf [Accessed: April 2022].

[7] Duplij Steven A and Shapoval I Iillia, "Quantum Computations: Fundamentals and Algorithms", Problems of Atomic Science and Technology (PAST) – 2007, pp. 230–235.

[8] Minakshi Bhatt, Anjali Aneja and Sonam Tripathi, "Classical Cryptography v/s Quantum Cryptography: A Comparative Study", International Journal of Electronics and Computer Science Engineering, Vol. 1 No. 1, ISSN 2277-1956, pp. 121–129.

[9] Mohamed Barakat, Christian Eder and Timo Hanke, "An Introduction to Cryptography", Lecture Notes, 2018; pp. 145. Website: https://www.mathematik.uni-kl.de/~ederc/download/Cryptography.pdf [Accessed: April 2020].

[10] Richard Crandall and Carl Pomerance, "Prime Numbers: A Computational Perspective", 2nd Edition, Springer-Verlag New York, 2005; pp. 597.

[11] Borevich Z. I and Shafarevich I. R, "Number Theory", Academic Press, 1996; pp. 435.

[12] Gareth J Janacek and Mark Lemmon Close, "Mathematics for Computer Scientists", Ventus Publishing Aps, ISBN: 978-87-7681-426-7, 2011; pp. 153.

[13] William Stallings, "Cryptography and Network Security: Principles and Practice", 5th Edition, Prentice Hall, 2011; pp. 900.

[14] Okoth A and Okelo B. "Arnold's Digitized Summation Technique and the Generalized Notion of the Collatz Conjecture", International Journal of Modern Computation, Information and Communication Technology, 2019; 2(5–6), pp. 36–42. ISSN: 2581-5954.

[15] William Stein, “Elementary Number Theory: Primes, Congruence and Secrets”, Lecture Notes, 2017, pp. 172. Website: https://wstein.org/ent/ent.pdf. [Accessed: April 2022].

[16] Eric Lehman, F Thomson Leighton and Albert R Meyer, “Mathematics for Computer Science”, 2017; pp. 988, Website: https://courses.csail.mit.edu/6.042/spring17/mcs.pdf. [Accessed: April 2022].

[17] Ares Saul and Castro Mario, “Hidden Structures in the Randomness of Prime Number Sequence?” 2005, Website: https://arxiv.org/abs/cond-mat/0310148. [Accessed: April 2022].

[18] Terence Tao, “Structure and Randomness in the Prime Numbers” 2007. Website: https://www.math.ucla.edu/~tao/preprints/Slides/primes.pdf [Accessed: April 2022].

[19] Emmer Michele, “Mathematics and Culture III”, Springer-Verlag Berlin Heidelberg, 2012, pp. 208.

[20] Seidikassyn Baibekov and Serik Altynbek, “Development of New Methods for Generating Prime Numbers”, Natural Science, Scientific Research Publishing, Vol. 7, pp. 416–423, 2015.

[21] Janet Heine Barnett, “Generating Pythagorean Triples: A Gnomonic Exploration” 2017. Website: https://digitalcommons.ursinus.edu/cgi/viewcontent.cgi?article=1008&context=triumphs_number [Accessed: April 2022].

[22] Keith Devlin, “The Millennium Problems: The Seven Greatest Unsolved Mathematical Puzzles of our Time”, Basic Books, 2002. ISBN: 978-87-7681-426-7, pp. 288.

[23] Samuel Budd, “The Distribution of Prime Numbers and its Applications”, Project Report, 2015; Website: https://www.lakeheadu.ca/sites/default/files/uploads/77/images/Budd%20Samuel.pdf [Accessed: April 2022].