3rd International Conference on
Research in Applied Science
06-08 November 2020
Munich, Germany

A New Method for Factorizing Semi-Primes Using Simple Polynomials

Anthony Overmars[1] and Sitalakshmi Venkatraman [2,]

[1] School of Engineering, Construction & Design, Melbourne Polytechnic, Victoria, Australia

[2]School of Engineering, Construction & Design, Melbourne Polytechnic, Victoria, Australia

Abstract.

This paper presents a new method to factorize semi-primes using simple polynomials.We consider a semi-prime, whose factors are both congruent as represented by:According to Fermat's Christmas Theorem, a sum of two squares can be found for each prime and two sums of two squares for the semi-prime . Using this property, we propose a new method to find the first of these sums of two squares and once this is known, the Brahmagupta identity is used to find the second sum of two squares. Subsequently, a modified Euler factorization is applied to recover the two prime constructs of the semi-prime. The correctness of our new factorisation method is established with mathematical proofs.

Keywords: semi-prime factorization, Brahmagupta identity, Euler's factorisation, encryption key

1. Introduction

Integer factorization into prime factors has been a challenge mathematically, and large number factorization is computationally very difficult. This property of semi-prime facrorization has interesting applications in cryptosystems for secure digital communications. Since factorization of large semi-primes used for Rivest–Shamir–Adleman (RSA) encryption keys results in breaking the corresponding cryptosystem, recent research attention dwells in developing new factorization methods. Hence, in this paper we propose a new semi-prime factorization method using simple polynomials. The existing methods found in literature are very much different from our original approach presented here.

A triangular number counts the number of points contained by an equilateral triangle. The sequence of triangular numbers, On-Line Encyclopaedia of Integer Sequences (OEIS) sequence A000217 (Sloane, 2015). Any two consecutive triangular numbers form a perfect square, OEIS sequence A000290 (Sloane, 2010).

A000217 0,1,3,6,10,15,21,28,36,45,55,66,78, 91,105,120,136,153,171,...

A000290 0,1,4,9,16,25,36,49,64,81,100,121,144,169,196,225,256,289,324,…

A prime congruent to 1 mod 4 has a representation as two squares according to Fermat's Christmas Theorem (Zagier, 1990). These two squares are an integer apart. In consideration of the two squares having opposite parity, the integer separating these two squares is odd (Overmars et al., 2019). This reduces the search by half.

A semi-prime whose construct is of two such primes, for each the sum of two squares, produces a sum of four squares. It Is long proven mathematically that this sum of four squares relates to the two sums of two squares that represents the semi-prime (Fibonacci, 1225). Euler showed how these two sums of two squares could recover the two prime constructs of the semi-prime, thereby providing its factorization (McKee, 1996). The semi-prime representation of these two sums of two squares are also separated by constant.

This paper develops a method to find this constant. The significance of this constant, is that this is a rational representation of the sum of the two squares of one of the original prime constructs. The connection to Euler's factorization can be used to validate this rational representation, thereby providing a direct method to the factorization of the semi-prime. The appropriate proofs are provided.

Comparisons with earlier works are made and the similarities with Euler's method and existing works are noted (Hermite, 1972; Brillhart, 1972; Williams, 1884). We believe our simple semi-prime factorization method would open new research and application in the areas of crypto synthesis and cryptanalysis.

2. Proposed Semi-Prime Factorization Method with Mathematical Proofs

In this section, we propose a new method to factorise a semi-prime, $N = p_1 p_2$, whose factors p_1 and p_2 are both congruent to modulo 4, i.e. $p_1, p_2 \equiv 1 \, mod \, 4$. Thi is according to Fermat's Christmas Theorem, where a sum of two squares can be found for each prime and two sums of two squares for the semi-prime N. We provide the mathematical definitions, properties, and our derivations along with proofs as follows.

Let us first consider triangle numbers which are given by

$$T_n = \frac{n(n+1)}{2} \tag{1}$$

The sum of two consecutive numbers is a square

$$S_n = T_{n-1} + T_n \tag{2}$$

A prime congruent to $1 \, mod \, 4$ has a representation as two squares according to Fermat's Christmas Theorem. Similarly, the semi-prime N, also has a sum of two squares representation. These two squares are an integer j, apart. Let such a square representation be

$$S_{n+j} = T_{n+j-1} + T_{n+j} \tag{3}$$

$$N = S_n + S_{n+j} \tag{4}$$

$$N = T_{n-1} + T_n + T_{n+j-1} + T_{n+j} \tag{5}$$

Using equation (1) we have,

$$T_{n-1} = \frac{(n-1)n}{2}, T_n = \frac{n(n+1)}{2}, T_{n+j-1} = \frac{(n+j-1)(n+j)}{2}, T_{n+j} = \frac{(n+j)(n+j+1)}{2}$$

$$N = \frac{(n-1)n}{2} + \frac{n(n+1)}{2} + \frac{(n+j-1)(n+j)}{2} + \frac{(n+j)(n+j+1)}{2}$$

$$N = n^2 + (n+j)^2 = n_1^2 + n_2^2 \tag{6}$$

$$N = 2n^2 + 2jn + j^2 \tag{7}$$

Solutions for n are given by

$$n_{1,2} = \frac{-j \pm \sqrt{2N - j^2}}{2} \tag{8}$$

The parity of these two squares for both the primes and the semi-prime, is odd-even. As such these two squares are an odd integer j, apart. We consider the absolute values because they are squared.

Solutions exist for $j = n_2 - n_1$

Proof:

It is sufficient to prove $2N - j^2$ is a perfect square when $j = n_2 - n_1$

From equation (8), $2N - j^2$ is a perfect square

$$N = n_1^2 + n_2^2, j = n_2 - n_1 \implies 2N - j^2 = 2(n_1^2 + n_2^2) - (n_2 - n_1)^2$$

$$2N - j^2 = n_1^2 + 2n_1n_2 + n_2^2 = (n_1 + n_2)^2 \ \square \tag{9}$$

For $j = n_2 - n_1$, $n_{1,2} = \frac{-j \pm \sqrt{2N - j^2}}{2} \implies \frac{-(n_2 - n_1) \pm (n_1 + n_2)}{2} = \frac{2n_1}{2}, \frac{2n_2}{2} = n_1, n_2 \ \square$

Let j always be odd $j = 2m - 1, m \in \mathbb{N}$, as per previous work (Overmars & Venkatraman, 2019), equation (7) becomes

$$N = 2n^2 + 2jn + j^2 \implies N = 2n^2 + 2n(2m-1) + (2m-1)^2 \tag{10}$$

And solutions for n from equation (8) are given by

$$n_{1,2} = \frac{-(2m-1) \pm \sqrt{2N-(2m-1)^2}}{2} \tag{11}$$

Example: For $\boldsymbol{N = 533 = 7^2 + 22^2}$

$$m_1 = 8, j_1 = 15, \sqrt{2(533) - 15^2} = 29, \; n_{1,2} = \frac{-15 \pm 29}{2}, \qquad n_{1,2} = (7,22),$$

$$N = 7^2 + 22^2$$

$$m_2 = 11, j_2 = 21, \sqrt{2(533) - 21^2} = 25, \; n_{3,4} = \frac{-21 \pm 25}{2}, \; n_{3,4} = (2,23), \; N = 2^2 + 23^2$$

From Overmars & Venkatraman (2019),

$$\Delta o = 23 - 7 = 16, \Delta e = 22 - 2 = 20, g = \gcd(\Delta o, \Delta e) = \gcd(20,16) = 4$$

$$p_1 = \left(\frac{\Delta o}{g}\right)^2 + \left(\frac{\Delta e}{g}\right)^2 = \left(\frac{16}{4}\right)^2 + \left(\frac{20}{4}\right)^2 = 41, \qquad p_2 = \frac{N}{p_1} = \frac{533}{41} = 13$$

As N becomes large, finding $(m_1 \wedge m_2)$ becomes more difficult. Finding either $(m_1 \vee m_2)$ is still computationally feasible. Once $(m_1 \vee m_2)$ becomes known a method for finding the other sum of two squares based upon the known sum of two squares is now provided.

$$p_1 = x_1^2 + x_2^2, p_2 = x_3^2 + x_4^2, N = p_1 p_2 = (x_1 x_3)^2 + (x_1 x_4)^2 + (x_2 x_3)^2 + (x_2 x_4)^2$$

From Brahmagupta [5] $N = (x_2 x_4 \pm x_1 x_3)^2 + (x_2 x_3 \mp x_1 x_4)^2 = a^2 + b^2 = c^2 + d^2$

$$a^2 + b^2 = c^2 + d^2 \Rightarrow b^2 - d^2 = c^2 - a^2 = (b+d)(b-d) = (c+a)(c-a)$$

$$b + d = (c + a)\left[\frac{c-a}{b-d}\right] \Rightarrow \left[\frac{b+d}{c+a}\right] = \left[\frac{c-a}{b-d}\right]$$

$$k_1 = \frac{b+d}{c+a} = \frac{c-a}{b-d}, \qquad k_2 = \frac{c+a}{d-b} = \frac{b+d}{c-a} \tag{12}$$

$$kd = -c + a + kb \tag{13}$$

$$d = kc + ka - b \Rightarrow \quad kd = k^2 c + k^2 a - kb \tag{14}$$

(14) - (13) $\Rightarrow 0 = c + k^2 c + k^2 a - 2kb - a = a(k^2 - 1) - 2kb + (k^2 + 1)c$

$$c = -a\left[\frac{k^2-1}{k^2+1}\right] + b\left[\frac{2k}{k^2+1}\right] \tag{15}$$

(13) + (14) $\Rightarrow 2kd = -c + a + k^2 c + k^2 a = a(k^2 + 1) + (k^2 - 1)c \Rightarrow \; d = \frac{a(k^2+1)+(k^2-1)c}{2k}$

From equation (15), substituting for c we get:

$$d = a\left[\frac{2k}{k^2+1}\right] + b\left[\frac{k^2-1}{k^2+1}\right] \quad (16)$$

$$\begin{bmatrix} c \\ d \end{bmatrix} = \frac{1}{k^2+1}\begin{bmatrix} k & 1 \\ -1 & k \end{bmatrix}^2 \begin{bmatrix} -a \\ b \end{bmatrix} \quad (17)$$

3. Conclusion and Future Work

In this paper, we began with the properties of two triangle numbers that form a square (Sierpinski, 2011). Two such squares can be used to describe a prime number congruent to $1 \, mod \, 4$ as per Fermat's Christmas Theorem. This was extended further in consideration of the odd/even parity of the two squares. The two squares are an odd integer apart. Equation (10) gives a polynomial whose integer solutions are given by equation (11). In earlier work] we showed that for a semi-prime whose construction was from two primes congruent to $1 \, mod \, 4$, two sums of two squares exists (Overmars & Venkatraman, 2019; Overmars & Venkatraman, 2020). An example calculation was given which was extended to show that a relationship exists beyond that of previous work. Equation (17) describes a variable k, which combines the four squares (from the two sums of two squares) in two ways. Each combination represents the sums of two squares of the prime factors of the semi-prime. The rational representations of k_1, k_2 are, as shown, the sum of squares of the factors p_1, p_2 of the semi-prime. The factors of a semi-prime can be found by using solutions to a quadratic modulus equation, which were then applied to the Euclidean algorithm to find a rational representation of the sum of squares. These two sums of two squares is then represented as two ratios, each of which are the sums of the two squares of the factors of the semi-prime. Expressions for 3 different polynomials and their connections to each other have been given. A method for solving one of these using modular forms has also been given. Once a solution can be found all of the other polynomial solutions can be found leading to the factorization of the semi-prime.

The representation of k as a rational in this paper is none the less interesting. If an efficient method to find the solutions to the quadratic modulus can be found as per (Williams, 1994), the method presented in this paper will quickly extract the two prime factors of the semi-prime. Future work entails extending k such that, if only one sum of two squares for the semi-prime is known, a method for finding the second sum of two squares can be provided.

Acknowledgment

This paper is part of the ongoing research output from Melbourne Polytechnic's Research and Seed Grant Project. The authors thank the anonymous reviewers for their invaluable feedback.

References

[1] Sloane N. (2015), "Triangular Numbers". *The On-line Encyclopedia of Integer Sequences.* Extracted from https://oeis.org/A000217 26/05/2020

[2] Sloane N. (2010), "The Squares". *The On-line Encyclopedia of Integer Sequences*. Extracted from https://oeis.org/A000290 26/05/2020

[3] Zagier D. (1990), "A One-Sentence Proof That Every Prime p ≡ 1 (mod 4) Is a Sum of Two Squares", *The American Mathematical Monthly, Mathematical Association of America*, vol. 97, 2, 144.

[4] Overmars A., Ntogramatzidis L. and Venkatraman S. (2019), "A new approach to generate all Pythagorean triples". *AIMS Mathematics*, 2019, vol. 4, 2, pp. 242-253. Doi: 10.3934/math.2019.2.242

[5] Fibonacci, L.P. (1225), *The Book of Squares (Liber Quadratorum)* An annotated translation into modern English by L. E. Sigler (1987) Orlando, FL: Academic Press.

[6] McKee J. (1996), "Turning Euler's Factoring Method into a Factoring Algorithm". *Bulletin of the London Mathematical Society*. vol. 4, 28, pp. 351–355. doi: 10.1112/blms/28.4.351

[7] Hermite C. (1848), "Note au sujet de l'article precedent," *Math. Pures Appl.*, v. 1848, p.15; also: "Note sur un theorem relatif aux nombres entieres," Oevres. vol. 1, 264.

[8] Brillhart J. (1972) "Note on representing a prime as a sum squares", *Math. Comp*. vol. 26, 192, pp. 1011-1013.

[9] Williams K. (1994) "Some refinements of an algorithm of Brillhart", *Number theory* (Halifax, NS, 1994) *CMS Conf. Proc.*, vol. 15, Amer. Math. Soc., Providence, RI, 1995, pp. 409–416.

[10] Overmars A., Venkatraman S. (2019) "A Fast Factorisation of Semi-Primes Using Sum of Squares" *Math. Comput. Appl.* 2019, 24, 62; doi: 10.3390/mca24020062

[11] Overmars, A. and Venkatraman, S. (2020) "Mathematical Attack of RSA by Extending the Sum of Squares of Primes to Factorize a Semi-Prime". *Math. Comput. Appl.*, vol. *25,* 63, pp. 1-15.

[11] Sierpinski W. (2011) *Pythagorean Triangles* Dover Publications. ISBN-13:9780486432486.

[12] Williams K. (1994) "On Finding the Solutions of $n = au^2 + buv + cv^2$ in Integers u and v" *Utilitas Mathematica*, vol. 46, pp. 3-19.