Global Journals LaTeX JournalKaleidoscope™
Artificial Intelligence formulated this projection for compatibility purposes from the original article published at Global Journals. However, this technology is currently in beta. *Therefore, kindly ignore odd layouts, missed formulae, text, tables, or figures.*

CrossRef DOI of original article:

Scan to know paper details and author's profile

Received: 1 January 1970 Accepted: 1 January 1970 Published: 1 January 1970

Abstract

This paper explores the use of a system of equations to factor semiprime numbers. Semiprime numbers are a special type of composite number that are the product of two prime numbers. Factoring semiprime numbers is important in cryptography and number theory. In this study, we present a method that applies a system of polynomial equations to factor semiprime number M.Where M can be any semiprime number. In fact, we build a family of systems where each system compose from three polynomial equations with three variables. The results of this study show that a solution for one system results with a complete factorization for a semiprime number. It may be possible to apply well known algorithms, such as Gröbner method [1], to solve one of those systems for a particular semiprime number M. semiprime, factorization, system of equations.

Index terms—

1 I. INTRODUCTION

2 Yonatan Zilpa

Let s 1 , s 2 , and S be any integers such that S = s 1 s 2 , then (s 2 -s 1) 2 + 4S is a perfect square. Indeed (s 2 -s 1) 2 + 4S = (s 2 + s 1) 2 .

Let M be a semiprime number and let p, q be its prime factors, where q > p. Let d = q -p and let n and x be any integers, such that n divides M -x, thenM -x n -n 2 + 4(M -x) = M -x n + n (1.1) is a positive integer. Thus, if M -x n -n 2 -4x is a non-negative perfect square, then M -x n -n 2 -4x = d 2 . (1.2) Equation (1.2) implies that M -x n -n = 4x + d 2 .

Hence, x must contain a factor t such thatx t -t = d.

The number x must be of the form: where j is an integer. Let k be a positive integer less than p, then substituting(d + j)jx with k(d + k) in equation (1.2) yields M -(d + k)k n -n 2 -4(d + k)k = d 2 (1.3)

Solving equation (1.3) for d we get the following two solutions d 0 = M -k 2 +2kn-n 2 k-n = M -(k-n) 2 k-n d 1 = M -k 2 -2kn-n 2 k+n = M -(M -(d+k)k n -n 2 -4k(d + k) = d 2 M -(d+(k+1))(k+1) n+1 -(n + 1) 2 -4(k + 1)(d + (k + 1)) = d 2 M -(d+(k+2))(k+2) n+2 -(n + 2) 2 -4(k + 2)(d + (k + 2)) = d 2**(1.6)**

System (1.6) has three equations with three variables n, k, d, however this system is dependent. We may overcome this problem by trying other functions. Let t : Z ? Z be any function, replace n with t(n) and k with u in equation (1.3). Equality (1.5) implies that u -t(n) = p (or t(n) -u = p) and k -n = p (or n -k = p), which gives us a system of equationsu -t(n) = p k -n = p from which we deduce u -k -t(n) + n = 0 or equivalently u = k + t(n) -n.

We get the following equality:? ? M -d + k + t(n) -n k + t(n) -n t(n) -t(n) ? ? 2 + -4 k + t(n) -n d + k + t(n) -n = d 2 (1.7)

Based on equation (1.7) we can deduce a new system of three equations with three variables k, n and, d. We may find three functions t 1 , t 2 , t 3 : Z ? Z and replace t(n) with t 3 (n) to get the third equation, t(n) with t 2 (n) to get the second equation, and finally t(n) with t 1 (n) to get the first equation. The key here is to select the functions t 1 , t 2 , and t 3 in such a way that our system has a unique solution, where |n -k| ? = 1. When moving d 2 to the left side of equality (1.7) and multiplying it with t 2 (n), the left side of this equality

becomes:?(t, n, k, d) := M -d + k + t(n) -n k + t(n) -n -t 2 (n) 2 -4t 2 (n) k + t(n) -n d + k + t(n) -n -t 2 (n)d 2

(2.1) If t is a polynomial function in R with integral coefficients, then ? can be viewed as a polynomial function from R 3 to R. In this case we also denote the function ?(t, n, k, d) with ? t (x, y, z). We thus get a system of polynomial equations:? t1 (x, y, z) = 0 ? t2 (x, y, z) = 0 ? t3 (x, y, z) = 0 (2.2)

The problem with d 0 is that the variant of system (1.7) is infinite, any integer n, k such that |n -k| = 1 satisfying this system. However, applying solution d 1 in equality (1.4) and requiring that n, k be positive integers implies that k + n = p.

(3.1)

Replacing n with t(n) and k with u in equation (1.3) we get the following systemu + t(n) = p k + n = p**(3.2)**

from which we deduce u + t(n) -k -n = 0 or equivalently u = n + k -t(n). Now we can replace k with n + k -t(n) and n with t(n) and d with d 1 in equation(1.3) to get ? ? M -d+ n+k-t(n) n+k-t(n) t(n) -t(n) ? ? 2 -4 n + k -t(n) d + n + k -t(n) = d 2 (3.3)

Since t(n) relies on the second equality of (1.4) and since t(n) differs from n, the first solution in (1.4) won't solve equality **??**3.3). Hence, by replacing t(n) with polynomial t 1 (n) with positive coefficients we get two independent polynomials.

3 Let us denote

t (n, k, d) := M -(d+n+k-t(n))(n+k-t(n)) t(n) -t(n) 2 -4 d + (n + k -t(n)) n + k -t(n)) -d 2 then equality (3.3) becomes t (n, k, d) = 0. **(3.4)**

If we set t(n) = n, then equation (3.4) is equivalent to (1.3). However, if polynomial t(n) differs from n, then solution d 0 is lost. Hence, for any polynomial t 2 (n) with positive integers that differs from n, polynomials n and t2(n) are independent.

We can repeatedly use the result u = n + k -t(n), obtained from system (3.2), to get the following system of three polynomial equations with three variables:? ? ? ? ? t1 (n, k, d) = 0 ? t2 (n, k, d) = t1 (t 2 (n), n + k -t(n), d) = 0 t1 (t 3 (n), n + k -t(n), d) + ? t2 (t 3 (n), n + k -t(n), d) = 0. (3.5)

If polynomials t 1 , t 2 , and t 3 differ in pairs and having non-negative integers and if none of these polynomial is zero, then none of the polynomial in system (3.5) depends on the other.

The RSA cryptosystem [4] as well as all public key cryptography implementations rely on the complexity of semiprime factorization. Mathematical attacks based on known relations, such as Pythagorean primes [3] or the use of a polynomial of third degree order [6] have been recently proposed for potential methods for factoring semiprimes numbers. When it comes to factoring large semiprime numbers, well known existing algorithms may consume too much memory and running time. Other algorithms, such as the firefly algorithm [5], may address some of these issues [2].

In this article, we attempt to attack the problem of semiprime factorization by using relationships between M and two different numbers, that are less than M . Using only quadratic relationships, we have constructed a wide variety of systems of three polynomial equations with three variables. A solution of one of one system may lead to a complete factorization of the semiprime number M .

I would like to express my sincere gratitude to Professor Shai Haran, who provided invaluable feedback on the manuscript. His insightful comments and suggestions greatly improved the clarity and rigor of the research findings. I am grateful for his time and expertise, which helped me to refine my research questions and the methodology used to address them. Without his guidance, this paper would not have been possible. ? ?

Figure 1:

(1.4)

k+n) 2

k+n

Since d is a positive integer. The first equality of equation (1.4) implies that

|k -n| = 1 or

|n -k| = p (1.5)

Figure 2:

.1 ACKNOWLEDGEMENTS REFERENCES

.2 London Journal of Research in Computer Science and Technology

[Ronald L Rivest et al. ()] 'A method for obtain-ing digital signatures and public-key cryptosystems'. Adi Ronald L Rivest , Leonard Shamir , Adleman . *Communications of the ACM* 1978. 21 (2) p. .

[Mishra and Chaturvedi ()] 'A multithreaded bound varying chaotic firefly algorithm for prime factorization'. Mohit Mishra , Utkarsh Chaturvedi . *2014 IEEE International Advance Computing Conference (IACC)*, 2014. IEEE. p. .

[Zilpa ()] 'About efficient algorithm for factoring semiprime number'. Zilpa . *J Theor Comput Sci Open Access* 2021. 7 p. 53.

[Buchberger ()] *Ein algorithmus zum auffinden der basiselemente des restklassenrings nach einem nulldimensionalen polynomideal*, Bruno Buchberger . 1965. Austria. Universitat Innsbruck (Ph. D. Thesis)

[Yang and He ()] 'Firefly algorithm: recent advances and ap-plications'. Xin-She Yang , Xingshi He . *International journal of swarm intelligence* 2013. 1 (1) p. .

[Overmars and Venkatraman ()] 'New semi-prime factor-ization and application in large rsa key attacks'. Anthony Overmars , Sitalakshmi Venkatraman . *Journal of Cybersecurity and Privacy* 2021. 1 (4) p. .