An Application of Pythagorean Circles in Cryptography and Some Ideas for Future Non Classical Systems

Mehmet Merkepci[1], Maretta Sarkis[2]

Department of Computer Engineering, Gaziantep University, Gaziantep, Turkey
Abu Dhabi University, Abu Dhabi, United Arab Emirates
Emails: mehmet.merkepci@gmail.com; Sarkismaretta1990@gmail.com

Abstract

In this work, we present a direct application for Pythagorean circles in the theory of cryptography by using integer points on these circles, as well as we describe some numerical systems to generalize classical well-known crypto-algorithms and systems. Also, we illustrate many examples to clarify the validity of our work.

Keywords: Plain text; Encryption; Decryption; Key point.

1.Introduction

The theory of cryptography studies the possibility of sending and transforming messages and information in a non-readable way for some people.

As a rich field in computer science, there are many intersections between cryptography and pure mathematics, where primes, gcds, and elliptic curves were used widely [3-6].

In this work, we use Pythagorean circles to build an encryption system depends on choosing points from a circle with integer points and integer radius R.

Also, we suggest some possible ways to generalize RSA algorithm by using dual\neutrosophic/split-complex numbers.

Main discussion.

Definition: A triple(x, y, z) is called Pythagorean if and only if $x^2 + y^2 = z^2$with $x, y, z \in N$ and $x < y, y < z$.
For example: (6,8,10) is a Pythagorean.
Remark : z is called a Pythagorean number. We denote it by pyth-number.
Definition: a pyth-number z is called prime if there exists x, y such that $x^2 + y^2 = z^2$ with $gcd(x, y, z) = 1$.
Definition: a pyth- circle is a circle $c(o, z)$ with center o and z as radius, where z is a pyth-number.
Definition 2.4 : Let $M_1(x_1, y_1), M_2(x_2, y_2) \in \bar{C}(o, R)$, then:
$M_1 + M_2 = (x_1 + x_2, y_1 + y_2)$.
$M_1 - M_2 = (x_1 - x_2, y_1 - y_2)$.
$M_1.M_2 = (x_1.x_2, y_1.y_2)$.
$\frac{M_1}{M_2} = \left(\frac{x_1.x_2 + y_1.y_2}{{x_2}^2 + {y_2}^2}, \frac{-x_1.y_2 - x_2.y_1}{{x_2}^2 + {y_2}^2}\right)$
Remark:

1). $M(x, y) \in \bar{C}(o, R)$ if and only if $\sqrt{x^2 + x^2} \leq R$.

Doi: https://doi.org/10.54216/GJMSA.020205
Received: March 18, 2022 Accepted: September 16, 2022

2). If $M(x,y) \notin C(o,R); x,y < R$, Then $M(R-x,R-y) \in C(o,R)$.

Remark:

The key point is a point $M(x,y) \in C(R)$such that $gcd(\|M\|,R) = 1$.

Theorem:

Let $M_1(x_1,y_1), M_2(x_2,y_2)$ are key points of $\bar{C}(o,R)$, then $M_3(x_3,y_3) = M_1.M_2$is a key point.

Proof.

We have $gcd(\|M_1.M_2\|,R) = gcd(\|M_1\|,R).gcd(\|M_2\|,R) = 1$.

So that, the proof holds.

Remark:

Suppose that we have two sides A and B.

A makes a choice $A(x_1,y_1)$, $gcd(|A|,R) = 1$, and B makes a choice choice$B(x_2,y_2)$, $gcd(|B|,R) = 1$.

The two sides A and B have an agreement that $I(x,y)$ is a key.

A does the operation $A.I$ and sends it to B, then B does $A.I.B$ and sends to A. This provides a key $K(a,b) = A.I.B$ which is invertible with respect to multiplication.

The algorithm of encryption:

After choosing a key K, the both sides agread about a point$C(x_1,y_1) \in C(R)$.

A chooses the main text $X(x_0,y_0)$ and uses the formula $Y = (KX + C)$(1) and R sends it to B.

B decrypts the text by the formula $X = K^{-1}[Y - C]$ (2).

Example:

Consider the text $X = (33,35)$, with$C(O,65)$ and $K(5,3)$, $C(5,7)$.

$Y = (KX + C)$ mod $R = (0,21)$ mod 65.

$X = K^{-1}[Y - C]$mod $R = (25,63)[(0,21) - (5,7)]$mod $65 = (33,35)$mod 65.

Example : consider the circle $C(O,65)$, the text is $X = (3,5)$, the key is $K(4,5)$ with $C(4,3)$.

$Y = (KX + C)$ mod$65 = (64,40)$ mod 65.

$K^{-1} = (35,11)$mod 65,

$X = K^{-1}[Y - C]$mod $65 = (35,11)[(64,40) - (4,3)]$mod $65 = (3,5)$mod $65 = (3,5)$.

Example:

Consider $C(O,325)$, $X = (4,2)$, $K = (3,7)$, $C(5,6)$.

$Y = (KX + C)$ mod$325 = (3,40)$ mod 325.

$K^{-1} = (241,196)$mod325.

$X = K^{-1}[Y - C]$mod $325 = (-7146,7802)$mod $325 = (4,2)$mod $325 = (3,54,2)$.

Towards Non classical crypto-systems:

In the literature, we find many algorithms for mathematical cryptology such as RSA algorithm, cryptography with groups, and cryptography with Elliptic curves [3].

In the following, we suggest some novel methods to increase the complexity of codes. These methods depend on some novel mathematical algebraic systems.

Doi: https://doi.org/10.54216/GJMSA.020205

Received: March 18, 2022 Accepted: September 16, 2022

Definition:

Let $a, b \in R$, then $R(I) = \{a + bI, I^2 = I\}$ is called the neutrosophic real number field.

Definition:

Let $a, b \in R$, then $R(I_1, I_2) = \{a + bI_1 + cI_2, {I_1}^2 = I_1, {I_2}^2 = I_2, I_1.I_2 = I_2.I_1 = I_1\}$ is called the refined neutrosophic real number field.

In [1], the foundations of neutrosophic number theory were presented such as Euler's function, congruencies, and Diophantine equations.

Also, in [2], the foundations of refined neutrosophic number theory were studied and handled.

From this point of view, we make our first suggestion.

Suggestion 1:

We recommend researchers and computer scientists to define and study if neutrosophic integers or neutrosophic refined integers can help with building a neutrosophic or refined neutrosophic version of RSA algorithm, were congruencies and exponents maybe very useful.

Another point is to compute the complexity of the suggested system and to compare it with classical RSA.

Definition : Let $a, b \in R$, the set $D = \{a + bJ, J^2 = 0\}$ is called the ring of dual numbers.

The set $S = \{a + bJ, J^2 = 1\}$ is called the ring of split- complex numbers.

Suggestion 2:

We recommend authors to study if dual/split-complex integers are useful in generalizing RSA algorithm.

Suggestion 3:

We recommend authors to define and study the algebraic properties of the following concepts:

1). The neutrosophic elliptic curve.

2). The refined neutrosophic elliptic curve.

3). The dual/split-complex elliptic curve.

Then, the following open question comes to light:

Can be use the previous kinds of elliptic curves to generalize the classical cryptography by elliptic curves.

Conclusion

In this paper, we have presented some applications of Pythagorean circles in cryptology. Also, we have suggested many possible future ideas to generalize the classical well-known crypto-systems depending on split-complex, dual or neutrosophic numbers. In the future, we aim that our suggestion may lead researchers to achieve more and more in this rich field of knowledge.

References

[1] Abobala, M., Partial Foundation of Neutrosophic Number Theory, Neutrosophic Sets and Systems, Vol. 39 , 2021.
[2] Ibrahim, M., and Abobala, M., "An Introduction To Refined Neutrosophic Number Theory", Neutrosophic sets and systems, Vol. 45, 2021.
[3] History of Cryptography ,"AN ESAY TO UNDERSTAND HISTORY OF CRYPTOGEAPHY " , Thawet, 2013 .
[4] H.S.A.Rose,Course in number theory .Oxford Sciences publication .(Clarendon),1988.
[5] Cryptography Schemes based on Elliptic Curve Pairings "(2004) S . S Al-Riyami University of London .
[6].Springer."Elliptic Curve Cryptosystems" (2016) Christof Paar,Jan Pelzl.

Doi: https://doi.org/10.54216/GJMSA.020205

Received: March 18, 2022 Accepted: September 16, 2022