Journal of Nature, Life and Applied Sciences
Volume (4), Issue (1): 30 Mar 2020
P: 30 - 44

AJSRP
ISSN: 2522-3356

مجلة العلوم الطبيعية والحياتية والتطبيقية
المجلد (4)، العدد (1): 30 مارس 2020م
ص: 30 - 44

Basic points resulting from mixed radius

Mohammad Nour Ibrahem Al Khatieb
Abd Albaset Alkhatib
Faculty of Science || Al-Baath University || Syria
Mohammad Nour Shamma
Faculty of Mechanical and Electrical Engineering || Damascus University || Syria

Abstract: Throughout this research, we present generating the correct points on the Pythagorean circle discussing the different cases of the radius that is defined by the following equation:

$$Z = R_1^n . R_2 . R_3 \;..\; R_k \qquad (1)$$

Where: $R_1, R_2, .., R_k \;\; ; \;\; k \in N$ are different prime pythagorean numbers.

This research is going to create the fundamental points which generate the correct points in the circle. Besides, I am going to calculate the number of the correct points on the circumference of a circle in every different form of the equation (1) via the following:

- Depending on the laws and theoroms resulted from this research.
- Depending on the computer program $(C\#)$ to yield fast and effective results.

We conclude by saying: We should take into account that the aim of this study is to pinpoint the nature and the number of the correct points on the circumference of a Pythagorean circle. As a result, we can exploit these points to decipher the data when they are transferred between users via unsecured nets. The current applied mechanism is to use elliptic curves which are complex and difficult to use if compared to the use of central Pythagorean circles due to its features and characteristics.

Keywords: The fundamental points, The correct points, Pythagorean number, Pythagorean circle, Pythagorean triple (PT), Prime Pythagorean triple(PPT).

النقاط الأساسية الناتجة من أنصاف أقطار مختلطة

محمد نور إبراهيم الخطيب
عبد الباسط الخطيب
كلية العلوم || جامعة البعث || سوريا
محمد نور شمه
كلية الهندسة الميكانيكية والكهربائية || جامعة دمشق || سوريا

الملخص: نقدم في هذا البحث توليد النقاط الصحيحة على الدائرة الفيثاغورية مُناقشين الحالات المختلفة لنصف قطر الدائرة المعرفة بالمعادلة:

$$Z = R_1^n . R_2 . R_3 \;..\; R_k \qquad (1)$$

حيث: $k \in N \;\; ; \;\; R_1, R_2, .., R_k$ أعداد فيثاغورية أولية مختلفة.

سنقوم بإيجاد النقاط الأساسية المولدة للنقاط الصحيحة على الدائرة، كما سنقوم بحساب عدد هذه النقاط على محيط الدائرة في كل حالة من الحالات المختلفة للمعادلة (1) من خلال:

- الاعتماد على القوانين والمبرهنات الناتجة في هذا البحث.
- الاعتماد على برنامج حاسوبي $(C\#)$ من أجل الحصول على نتائج سريعة وفعَّالة.

ونخلص إلى القول: أن الغاية من هذه الدراسة هي معرفة طبيعة وعدد النقاط الصحيحة الواقعة على محيط الدائرة الفيثاغورية من أجل توظيفها في عمليات تشفير البيانات عند نقلها بين المستخدمين عبر شبكات غير آمنة، حيث الآلية المستخدمة حالياً هي استخدام المنحنيات الناقصية التي تتسم بالصعوبة والتعقيد مقارنةً باستخدام الدوائر الفيثاغورية المركزية وذلك لما لها من الميزات والخصائص.

الكلمات المفتاحية: النقاط الأساسية، النقاط الصحيحة، العدد الفيثاغوري، الدائرية الفيثاغورية، الثلاثية الفيثاغورية $(P\ T)$، الثلاثية الفيثاغورية الأولية $(P\ P\ T)$.

مقدمة:

التشفير هو علم يدرس تحويل الرسائل والمعلومات أو البيانات إلى شكل غير مقروء من قبل جميع الأشخاص غير المصرح لهم.

في عام 1985 درست أنواع خاصة من المنحنيات تسمى المنحنيات الناقصية Elliptic Curves وربطت مع التشفير غير المتناظر من قبلVictor Miller،Neal Kobltiz (Al-Riyami, 2004)، وتم بناء أنظمة تشفير يعتمد أمنها على مسألة صعبة الحل تدعى مسألة اللوغاريتم المنفصل ضمن المنحنيات الناقصية (Christof Paar, 2016).

هدفنا من هذا البحث هو دراسة الدوائر الفيثاغورية المركزية عوضاً عن المنحنيات الناقصية وتوليد النقاط الصحيحة الواقعة على محيطها والتعرف على طبيعتها وعددها وربطها مع التشفير وبناء أنظمة تشفير جديدة تتسم بالسهولة وتتمتع بدرجات عالية من الأمان.

كما واهتم الباحثون والعلماء بتوليد الثلاثيات الفيثاغورية بشكل عام والثلاثيات الفيثاغورية الأولية بشكل خاص حيث تم توليد ثلاثيات فيثاغورية (x,y,z) لدى معرفة العدد الأصغر من الثلاثية (x) إذا كان عدداً فردياً أو من مضاعفات العدد (4) (شمة، 2016)، لكن هذا الاهتمام قل كثيراً وكاد يكون معدوماً من أجل توليد ثلاثيات فيثاغورية أولية (x,y,z) عند معرفة العدد z (العدد الأكبر في الثلاثية) وذلك لأنه يتطلب حل معادلة ديوفنتية من الثانية Duofantent Equation وترها معلوم (z)، والضلعين القائمتين (x,y) مجهولتين وهذا أمر صعب جداً (Yan, 2013)، و نقدم في هذا البحث حلاً صحيحاً للمعادلة الديوفنتية من الدرجة الثانية، وذلك بغرض توليد النقاط الصحيحة على الدائرة الفيثاغورية (إيجاد الضلعين القائمتين)

وإيجاد عدد الفيثاغوريات الأولية مناقشين الحالة التي يكون فيها نصف قطر الدائرة الفيثاغورية Z مختلط أي من الشكل:

$$Z = R_1^n \cdot R_2 \cdot R_3 \ \ .. \ \ R_k \qquad (1)$$

حيث $k,n \in \mathbb{N}$; $R_1,R_2,..,R_k$ أعداد فيثاغورية أولية علماً أن k عدد المضاريب الأولية المختلفة و n عدد التكرارت ولبين أنَ عدد الثلاثيات الفيثاغورية الأساسية الأولية هو:

$$N_{PPT} = 2^{k-1}$$

حيث تم مناقشة حالات مختلفة لنصف قطر الدائرة الفيثاغورية وتعاملنا مع دوائر فيثاغورية مركزية $C(O,Z)$ أنصاف أقطارها مضاعفة (الخطيب ش.، 2019)من الشكل:

$$R = R^n$$

حيث R عدد فيثاغوري أولي أصلاً، وكان عدد الفيثاغوريات الأساسية

$$N_{PT} = n$$

حيث n هو درجة الأس(عدد التكرارات) في حين أنَّ عدد الفيثاغوريات الأساسية الأولية N_{PPT} هو الواحد دوماً وذلك $\forall n \in N$.

كما تعاملنا مع دوائر فيثاغورية مركزية $C(O,Z)$ أنصاف أقطارها جداء لأعداد فيثاغورية أولية مختلفة (الخطيب ش.، 2019) من الشكل:

$$Z = R_1 . R_2 . \ .. \ . R_k$$

وكان عدد الفيثاغوريات الأساسية

$$N_{PT} = \frac{3^k - 1}{2}$$

وعدد الفيثاغوريات الأساسية الأولية

$$N_{PPT} = 2^{k-1}$$

حيث k هو عدد المضاريب الأولية المختلفة.

مشكلة البحث:

- تكمن مشكلة البحث في صعوبة حساب النقاط الصحيحة n داخل المجال $\left[\sqrt{R} \ , \ \sqrt{\frac{R}{2}} \right]$ وبالتالي الحصول على القيم $m = \sqrt{R - n^2}$

ومنه الحصول على قيم x, y, z كما يلي:

$$x = 2nm \ , \ y = n^2 - m^2 \ , z = n^2 + m^2$$

وخاصة من أجل القيم R الكبيرة مثل العدد: $R = 923454350$ حيث يولد (388) ثلاثية فيثاغورثية.

- صعوبة التميز بين النقاط الأساسية والأساسية الأولية والعمل على معالجة هذه المشكلة حاسوبياً.
- الصعوبة البالغة عند التعامل مع الدوائر الفيثاغورية التي تملك أنصاف أقطار كبيرة من حيث عدد النقاط الصحيحة المتولدة على هذه الدائرة وكذلك صعوبة تحديد طبيعة نصف القطر فيما إذا كان فيثاغوري أولي أم قابل للتحليل.

مواد البحث وطرائقه:

يعد نوع الدراسة في هذا البحث من حيث الاستعمال جزء من أطروحة دكتوراه تتحدث عن توليد النقاط الأساسية من أنصاف أقطار مختلطة حيث اتبعنا المنهج التحليلي والتركيبي و كانت دراستنا تعتمد على شقين:

الدراسة النظرية:

تم من خلالها عرض مجموعة من التعاريف والمبرهنات الأساسية في نظرية الأعداد والتي تتعلق بالأعداد الأولية وبشكل خاص الفيثاغورية منها بغية التعرف على النقاط الأساسية الضرورية واللازمة للمضي قدماً في البحث، والتعريف بالمعادلات الديوفنتية من الدرجة الثانية(Corvaja, 2016) .

الدراسة العملية:

تم انجاز الدراسة العملية من خلال استخدام البرامج الحاسوبية الحديثة حيث قمنا بكتابة برنامج حاسوبي متكامل باستخدام لغة البرمجة $(C\#)$ وهي من أحدث لغات البرمجة المعول بها حالياً، وكان لهذا البرنامج الأثر الكبير بالحصول على نتائج سريعة وفعالة وخاصةً عند التعامل مع أنصاف أقطار كبيرة.

تعاريف ومبرهنات:

لتكن لدينا الأعداد $x, y, z \in \mathbb{N}$ حيث إنَّ $x<z\ ,\ y<z$ والتي تحقق معادلة فيثاغورث $x^2+y^2=z^2$ ، و لنذكر بالتعاريف والمبرهنات التالية.

تعريف1: العدد الفيثاغوري (Kak, 2010): هو كل عدد طبيعي z يحقق معادلة فيثاغورث

$$\exists\ x, y \in \mathbb{N} \quad ; \quad x^2+y^2=z^2 \Leftrightarrow z=\sqrt{x^2+y^2} \in \mathbb{N}$$

مثال1: الأعداد التالية هي أعداد فيثاغورية

5 , 13 , 17 , 25 , 41 , 61 , 85 , 32577557513, ..

لأنها تكتب بالأشكال التالية:

$$5^2 = 3^2 + 4^2$$
$$17^2 = 8^2 + 15^2$$
$$61^2 = 11^2 + 60^2$$
$$32577557513^2 = 255255^2 + 32577557512^2$$

تعريف2: الثلاثية الفيثاغورية (x, y, z) (Raja Rama Gandhi, 2012): هي ثلاثية من الأعداد الطبيعية وتحقق:

$$x^2+y^2 = z^2 \qquad (2)$$

ويرمز لها اختصاراً PT $(\text{Pythagorian Triple})$.

مثال2: الثلاثية $(3,4,5)$ **هي ثلاثية فيثاغورية، وكذلك الثلاثية** $(9,12,15)$.

تعريف3: الثلاثية الفيثاغورية الأساسية: هي ثلاثية تحقق العلاقة (2) ويكون فيها: $x > y$ أي تقع في الثمن الأول من المستوي XOY .

يرمز لها اختصاراً $B\ P\ T$ (Basic Pythagorian Triple).

تعريف4: الثلاثية الفيثاغورية الأولية (Eckert, 1984): هي ثلاثية من الأعداد الطبيعية تحقق العلاقة (2) وتحقق الشرط:

$$\gcd(x, y, z)=1 \qquad (3)$$

أي أنَّ الأعداد أولية فيما بينها، ويرمز لها $P\,PT$ (prime pythagorian Triple).

تعريف5(Cople, 2006) :

نقول عن العدد Z إنه فيثاغوري أولي إذا وجد عددان طبيعيان x, y يحققان (2) , (1) معاً.

مبرهنة1 (Nar Kiewicz, 2004):

إنَّ جميع الحلول الصحيحة غير الصفرية لمعادلة فيثاغورث $x^2+y^2=z^2$ حيث y عدد زوجي و $\gcd(x, y, z)=1$ تعطى بالعلاقات:

$$x=(r^2-s^2) \quad , \quad y=2rs \quad , \quad z=(r^2+s^2)$$

حيث r, s أعداد صحيحة غير صفرية و$\gcd(s\ , r)=1$، و $r\ ,\ s$ أحدهما فردي والآخر زوجي.

تمهيدية1 (Crandall, 2005):

إذا كان (x, y, z) ثلاثية فيثاغورية أولية فإنَّ x, y أحدهما فردي والآخر زوجي.

تعريف 6: الدائرة الفيثاغورية هي كل دائرة $C(O, Z)$ مركزها O ونصف قطرها العدد الفيثاغوري Z.

تعريف 7:التشفير(U.Maurer, 2009) .

هو فن وعلم يدرس تحويل الرسائل والمعلومات أو البيانات إلى شكل غير مقروء(غير قابل للفهم) من قبل جميع الأشخاص غير المصرح لهم.

مبرهنة2:

الدائرة الفيثاغورية $C(O, R^m)$ تملك على الأقل m نقطة أساسية وبالتالي تملك $N_{P.T}=4(2m+1)$ نقطة صحيحة على محيطها.

الإثبات:

لنثبت ذلك بالاستقراء الرياضي:

من أجل $C(O, R)$ حصلنا على نقطة أساسية (x_0, y_0)، ومن أجل $C(O, R^2)$ حصلنا على النقطتين:

$$(x_1, y_1)=(\ x_0\ R\ ,\ y_0\ R)$$

$$(x_2, y_2)=\left(2n\sqrt{R^2-n^2}\ \ ,\ \left|2n^2-R^2\right|\ \right)$$

نفرض تحقق ذلك من أجل الدوائر $C(O, R^{m-1})$ أي توجد النقاط

$$(x_1, y_1)\ , (x_2, y_2)\ , .. , (x_{m-1}, y_{m-1})$$

من أجل الدائرة $C\left(O,R^m\right)$ لدينا النقاط:

حيث $\left(x_1.R,y_1.R\right),..,\left(x_{m-1}.R,y_{m-1}.R\right),\left(2n\sqrt{R^m-n^2}\ ,\left|2n^2-R^m\right|\right)\ ;n^2<R^m<2n^2$ يتحقق من أجل:

$$\left(x_1.R\right)^2+\left(y_1.R\right)^2=x_1^2.R^2+y_1^2.R^2$$
$$=\left(x_1^2+y_1^2\right)R^2=R^2.R^2=R^4=R^{2m}=\left(R^m\right)^2$$

M

$$\left(x_i.R\right)^2+\left(y_i.R\right)^2=R^{2m}=\left(R^m\right)^2 \qquad ;i=1,2,...,m-1$$

وتبقى لدينا النقطة الأخيرة:

$$\left(2n\sqrt{R^m-n^2}\right)^2+\left(\left|2n^2-R^m\right|\right)^2=4n^2\left(R^m-n^2\right)+4n^4-4R^mn^2+R^{2m}$$
$$=4n^2R^m-4n^4+4n^4-4n^2R^m+R^{2m}$$
$$=R^{2m}=\left(R^m\right)^2$$

ومنه يوجد m نقطة أساسية واقعة على محيط الدائرة، وبما أن كل نقطة لها /8/ نظائر ولدينا أيضاً 4 أقطاب فيصبح العدد الكلي للنقاط الصحيحة على محيط الدائرة: $N_{P.T}=8m+4=4\left(2m+1\right)$

مثال3:

لتكن لدينا الدائرة $C\left(O,5^3\right)$ حيث: $m=3$ و $R=5$.

نعلم أن الدائرة $C\left(O,5\right)$ تملك نقطة أساسية واحدة هي $(4,3)$ ونصف قطرها $R=5$، والدائرة $C\left(O,5^2\right)$ تملك نقطتين أساسيتين هما: $(7\ ,24)\ ,(20\ ,15)$ الدائرة المدروسة هي الدائرة $C\left(O,5^3\right)$ تملك ثلاث نقاط أساسية هي:

النقطة الأولى: $\left(x_1.R\ ,\ y_1.R\right)=\left(20.5\ ,\ 15.5\right)=\left(100\ ,75\right)$

النقطة الثانية: $\left(x_2.R\ ,y_2.R\right)=\left(24.5\ ,\ 7.5\right)=\left(120,35\right)$

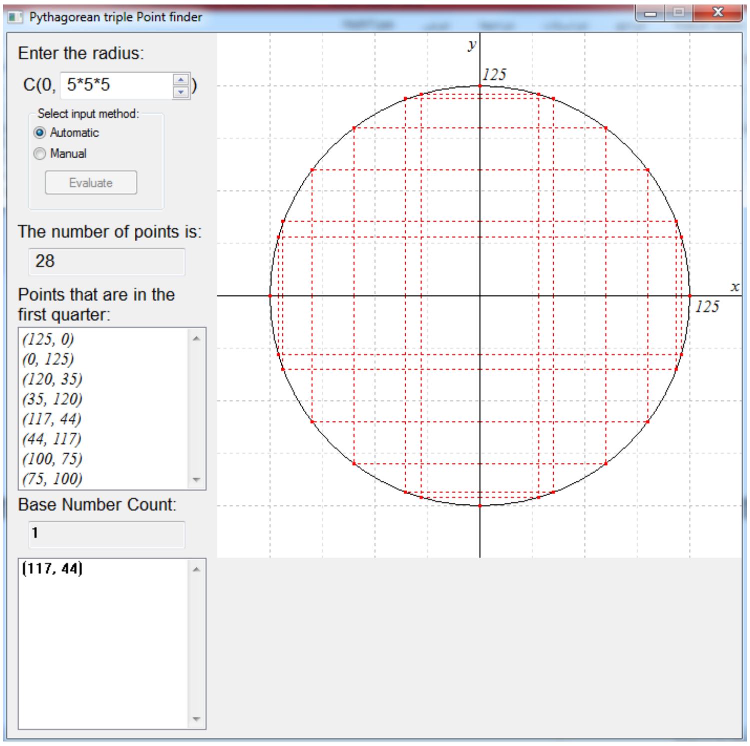
النقطة الثالثة: لإيجادها نختار العدد n على النحو التالي:

$$n\in\left]\sqrt{\frac{R^3}{2}},\sqrt{R^3}\right[=\left]5,59\quad,\quad 11,18\right[\Rightarrow n=11$$

$$\left[\ 2n\sqrt{R^3-n^2},\left|2n^2-R^3\right|\ \right]=\left[\ 2(11)\sqrt{125-121}\ ,\ \left|2(121)-125\right|\ \right]=\left(44,117\right)$$

أصبح لدينا ثلاثة نقاط أساسية واحدة منها فقط أولية، وبالتالي العدد الكلي للنقاط الصحيحة على محيط الدائرة المدروسة هو:

$$N_{P.T}=4\left(2m+1\right)=4\left[2\left(3\right)+1\right]=28\quad;\ m=3$$



الشكل (1) يوضح النقاط الصحيحة والنقاط الأساسية والنقاط الأساسية الأولية على الدائرة الفيثاغورية

نتيجة1:

بفرض $Z = R^m$ فإن عدد النقاط الأساسية الأولية واحد فقط وعدد النقاط الصحيحة هو:

$$N_{PT} = 12 + (m-1)8$$

وهو متوالية حسابية حدها الأول $a = 12$ وأساسها $r = 8$.

مثال 4:

$$Z = R^3 \Rightarrow N = 12 + (m-1).8 = 12 + (2).8 = 28$$
$$Z = R^5 \Rightarrow N = 12 + (m-1).8 = 12 + (4).8 = 44$$
$$Z = R^7 \Rightarrow N = 12 + (m-1).8 = 12 + (6).8 = 60$$

مبرهنة 3:

بفرض $R = R_1.R_2 \,..\, R_K$ حيث $R_i \;;\; i = 1,2,..,K$ أعداد فيثاغورية أولية فإنَّه يوجد 2^{K-1} نقطة أساسية أولية و 4.3^k نقطة صحيحة على محيط الدائرة أي أن:

$$N_{P.P.T} = 2^{K-1}$$
$$N_{P.T} = 4.3^k$$

الإثبات:

بالاستقراء الرياضي ومن الخطوات التالية:

1. من أجل $R = R_1 \Rightarrow K = 1$ توجد ثلاثية واحدة.

2. من أجل $K=2 \Rightarrow R=R_1.R_2$ توجد ثلاثيتان وحيدتان.
3. من أجل $K=3 \Rightarrow R=R_1.R_2.R_3$ يوجد أربع ثلاثيات فيثاغورية.
4. بفرض تحقق الخاصية من أجل $i=k-1$ أي: $R=R_1.R_2.\ ...\ R_{K-1}$

وبالتالي توجد 2^{K-2} ثلاثية فيثاغورية أولية، ولنثبت صحتها من أجل $i=k$.

بما أنَّ $i=k-1$ محقق أي $R=R_1.R_2.\ ...\ R_{k-1}$ عندئذٍ توجد 2^{K-2} ثلاثية أولية أي يوجد

$$R=M_1^2+N_1^2\ ,\quad R=M_2^2+N_2^2\ ,\quad ...\ ,R=M_{k-2}^2+N_{k-2}^2$$

لدينا:

$$\begin{aligned} R &= R_1.R_2.\ ...\ R_k \\ &= \left(n_1^2+m_1^2\right)\left(n_2^2+m_2^2\right)...\left(n_k^2+m_k^2\right) \\ &= \left(N_1^2+M_1^2\right)\left(n_k^2+m_k^2\right) \end{aligned}$$

بما أن $N_1^2+M_1^2$ يولد 2^{k-2} نقطة أساسية وبالتالي:

$$R=\left(N_1^2+M_1^2\right)\left(n_k^2+m_k^2\right)$$

يولد 2^{k-1} نقطة، وهذه النقاط تنتج من:

$$R=\begin{cases}\left(N_1n_K+M_1m_k\right)^2+\left(N_1m_K-M_1n_K\right)^2 \\ \left(N_1m_K+M_1n_K\right)^2+\left(N_1n_K-M_1m_K\right)^2\end{cases} \qquad (4)$$

ومنه يكون عدد الثلاثيات الأساسية الأولية: $N_{P.P.T}=2^{k-1}$.

عدد النقاط الأساسية المتولدة من نصف القطر R والواقعة على محيط الدائرة يساوي:

$$m=\frac{3^k-1}{2}$$

ومنه يكون عدد النقاط الصحيحة:

$$N_{P.T}=4\left[2m+1\right]=4\left[2\left(\frac{3^k-1}{2}\right)+1\right]=4\left[3^k-1+1\right]=4.3^k$$

مثال 5:

بفرض $R=(5)(13)(17)$ لنوجد الـ PPT الأربعة اعتماداً على العلاقة (4).

$$\left.\begin{aligned} R_1 &=5 \to (2,1) \\ R_2 &=13 \to (3,2) \\ R_3 &=17 \to (4,1)\end{aligned}\right\} \Rightarrow \begin{cases} N_1=2\times3+1\times2=6+2=8 & ;M_1=\sqrt{R_1R_2-N_1^2}=1 \\ N_2=2\times2+1\times3=4+3=7 & ;M_2=\sqrt{R_1R_2-N_2^2}=4\end{cases}$$

$$\begin{aligned} N_3 &= N_1m_3+M_1n_3=(8)(1)+(1)(4)=12 \\ N_4 &= N_1n_3+M_1m_3=(8)(4)+(1)(1)=33 \\ N_5 &= N_2n_3+M_2m_3=(7)(4)+(4)(1)=32 \\ N_6 &= N_2m_3+M_2n_3=(7)(1)+(4)(4)=23 \end{aligned}$$

مما سبق يكون:

$$N_3 = 12 \quad \Rightarrow \quad M_3 = \sqrt{1105-144} = 31$$
$$N_4 = 33 \quad \Rightarrow \quad M_4 = \sqrt{1105-1089} = 4$$
$$N_5 = 32 \quad \Rightarrow \quad M_5 = \sqrt{1105-1024} = 9$$
$$N_6 = 23 \quad \Rightarrow \quad M_6 = \sqrt{1105-529} = 24$$

وبالتالي يكون:

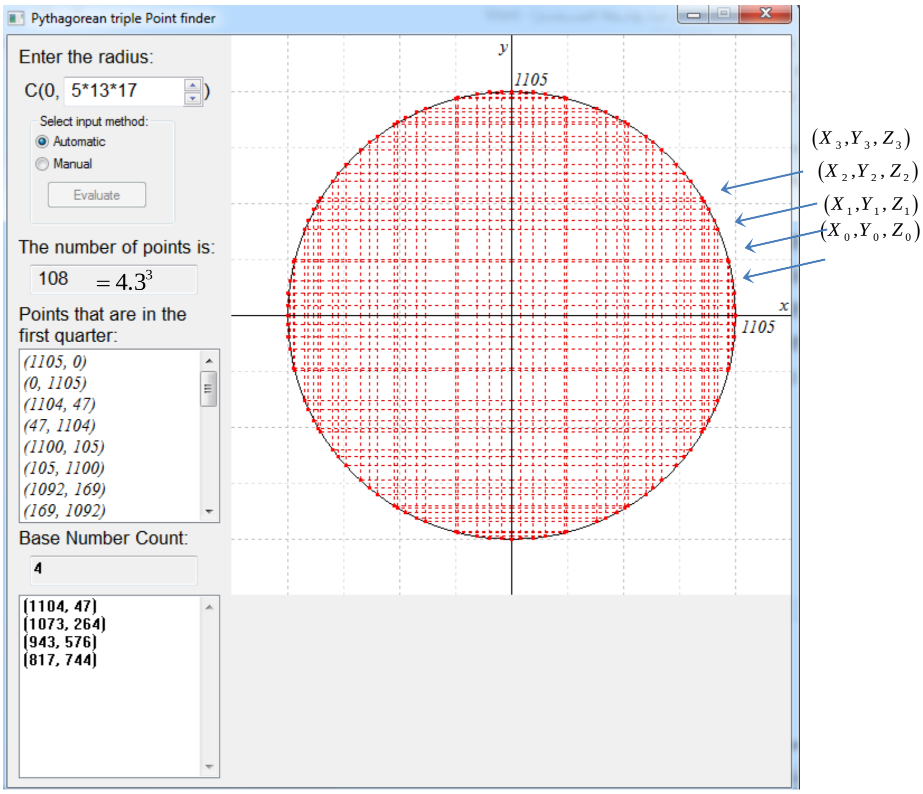
$$\begin{cases} X_1 = 2N_3M_3 = 744 & \Rightarrow \quad Y_1 = 817 \\ X_2 = 2N_4M_4 = 264 & \Rightarrow \quad Y_2 = 1073 \\ X_3 = 2N_4M_4 = 576 & \Rightarrow \quad Y_3 = 943 \\ X_4 = 2N_4M_4 = 1104 & \Rightarrow \quad Y_4 = 47 \end{cases}$$

وبذلك تكون الـ PPT الأربعة هي:

$$\begin{cases} (X_0, Y_0, Z_0) = (1104, 47, 1105) \\ (X_1, Y_1, Z_1) = (1073, 264, 1105) \\ (X_2, Y_2, Z_2) = (943, 576, 1105) \\ (X_3, Y_3, Z_3) = (817, 744, 1105) \end{cases}$$

وعدد النقاط الصحيحة الواقعة على محيط الدائرة:

$$N_{P.T} = 4.3^k = 4.3^3 = 4(27) = 108$$



الشكل (2) يوضِّح النقاط الصحيحة والنقاط الأساسية والنقاط الأساسية الأولية على الدائرة الفيثاغورية

نتيجة 2:

بفرض $Z = R_1 \,.\, R_2 \,..\, R_k$ عندئذ نحصل على ثلاثيات أساسية أولية عددها:

$$N_{PPT} = 2^{k-1}$$

وهذه الثلاثيات تقع في الثمن الأول من الدائرة: $C(O,Z)$، وهذا يعني أن:

- عدد الثلاثيات الأساسية الواقعة في الربع الأول: $N = 2^k$.
- عدد الثلاثيات الأساسية الواقعة في النصف العلوي: $N = 2^{k+1}$.
- عدد الثلاثيات الأساسية الواقعة على محيط الدائرة: $N = 2^{k+2}$

مبرهنة 4:

بفرض $R = R_1^n . R_2 . \,..\, . R_k$ حيث $R_1 \,,\, R_2 \,,\, .. \,,\, R_k$ أعداد فيثاغورثية أولية مختلفة فإن:

$$N_{P.P.T} = 2^{k-1}$$

$$N_{P.T} = 4.3^{k-1}(2n+1)$$

حيث n عدد التكرارات للعنصر R_1، k عدد المضاريب الفيثاغورية المختلفة.

الإثبات:

حسب المبرهنة 2 من أجل $R = R_1^n$ نحصل على عدد الفيثاغوريات الأساسية الأولية الخاصة بالجزء المضاعف من نصف القطر ويساوي:

$$N_{P.P.T} = 1$$

حيث إن $R = R_1^n$ تعامل معاملة R_1 من حيث عدد $P.P.T$ (الثلاثيات الأساسية الأولية).

حسب المبرهنة 3 من أجل $R = R_2 \,.\, R_3 \,.\, .. \,.\, R_k$ يكون عدد الثلاثيات الفيثاغورية الأساسية الأولية الخاصة بهذا الجزء مساوياً:

$$N_{P.P.T} = 2^{k-2}$$

بما أن $R = R_1^n$ هنا تعامل معاملة R_1 من حيث عدد $P.P.T$ عندئذ نصف قطر الدائرة يأخذ الشكل التالي: $R = R_1 . R_2 \,..\, R_k$ وبتطبيق المبرهنة 3 يكون:

$$N_{P.P.T} = 2^{k-1}.$$

ليكن m_1 عدد النقاط الأساسية المتولدة من الجزء المضاعف لنصف القطر عندئذ:

$$m_1 = n.3^{k-1}$$

و m_2 عدد النقاط الأساسية المتولدة من الجزء المختلف لنصف القطر والمساوي:

$$m_2 = \frac{3^{k-1}-1}{2}$$

مما سبق يكون العدد الكلي للنقاط الأساسية المتولدة من نصف القطر R يساوي:

$$m = n.3^{k-1} + \frac{3^{k-1}-1}{2}$$

ومنه يكون عدد النقاط الصحيحة هو:

$$N_{P.T}=4(2m+1)=4\left[2\left(n.3^{k-1}+\frac{3^{k-1}-1}{2}\right)+1\right]=4\left[2n.3^{k-1}+3^{k-1}-1+1\right]$$
$$=4\left[2n.3^{k-1}+3^{k-1}\right]=4.3^{k-1}\left[2n+1\right]$$

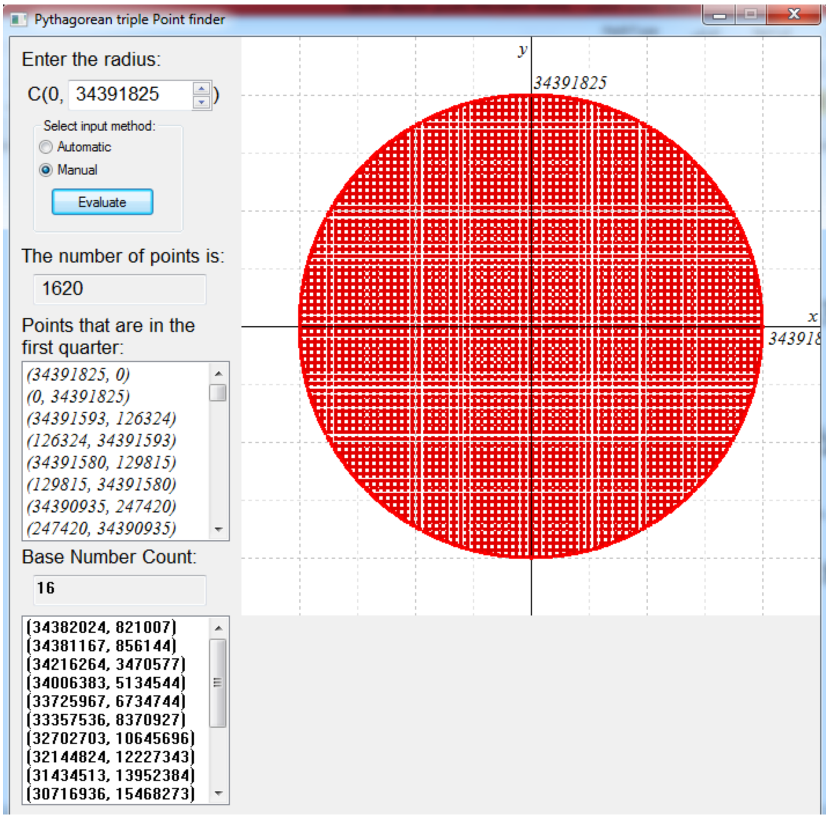
مثال 6: ليكن: $n=2\ ,\ k=5$; $R=5^2\times13\times29\times41\times89=34391825$

عندئذ يكون عدد الثلاثيات الأساسية الأولية:

$$N_{P.P.T}=2^{k-1}=2^{5-1}=2^4=16$$

ويكون عدد النقاط الصحيحة الواقعة على محيط الدائرة يساوي:

$$N_{P.T}=4.3^{k-1}(2n+1)=4\left(3^{5-1}\right)\left[2(2)+1\right]=4(81)(5)=1620$$



الشكل (3) يوضح النقاط الصحيحة والنقاط الأساسية والنقاط الأساسية الأولية على الدائرة الفيثاغورية

نتيجة 3:

بفرض $R=R_1^n.R_2$ حيث R_1,R_2 عددان فيثاغوريان أوليان فإن:

$$N_{P.P.T}=2$$
$$N_{P.T}=4\times3(2n+1)$$

مثال 7: لتكن لدينا الدائرة $C(O\ ,\ R)$ حيث:

$$R=5^2\times13=325\quad,\ n=2,k=2$$

العدد الكلي للثلاثيات الفيثاغورية الأولية:

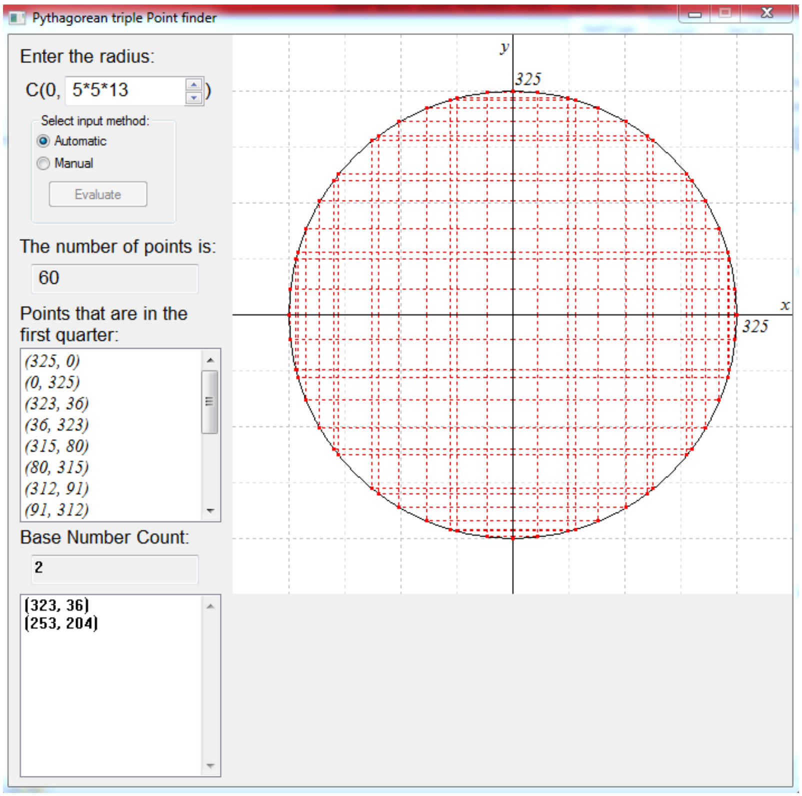
$$N_{P.P.T} = 2^{k-1} = 2^{2-1} = 2$$

والثلاثيات الأولية الناتجة هي:

$$(253 , 204 , 325) \quad , \quad (323 , 36 , 325)$$

عدد النقاط الصحيحة الواقعة على محيط الدائرة:

$$N_{PT} = 4\times 3^{k-1}(2n+1) = 4\times 3^{2-1}\left[2(2)+1\right] = 4\times 3(5) = 60$$



الشكل (4) يوضح النقاط الصحيحة والأساسية والأساسية الأولية على الدائرة الفيثاغورثية

نتيجة4:من أجل $R = R_1^{n_1}.R_2^{n_2} \; .. \; R_m^{n_m}.R_{m+1}.R_{m+2} \; .. \; R_k$

حيث إن: $n_1 , n_2 , \; .. \; , n_m , k \in N$ فإن:

$$N_{P.P.T} = 2^{k-1}$$

$$N_{PT} = 4\times 3^{(k-n)}\left[(2n_1+1).(2n_2+1). \; .. \; .(2n_k+1)\right]$$

مثال8:

من أجل $R = 5^2\times 13^2\times 17^2 = 1221025$

يكون عدد الثلاثيات الفيثاغورية الأساسية الأولية:

$$N_{P.P.T} = 2^{k-1} = 2^{3-1} = 4$$

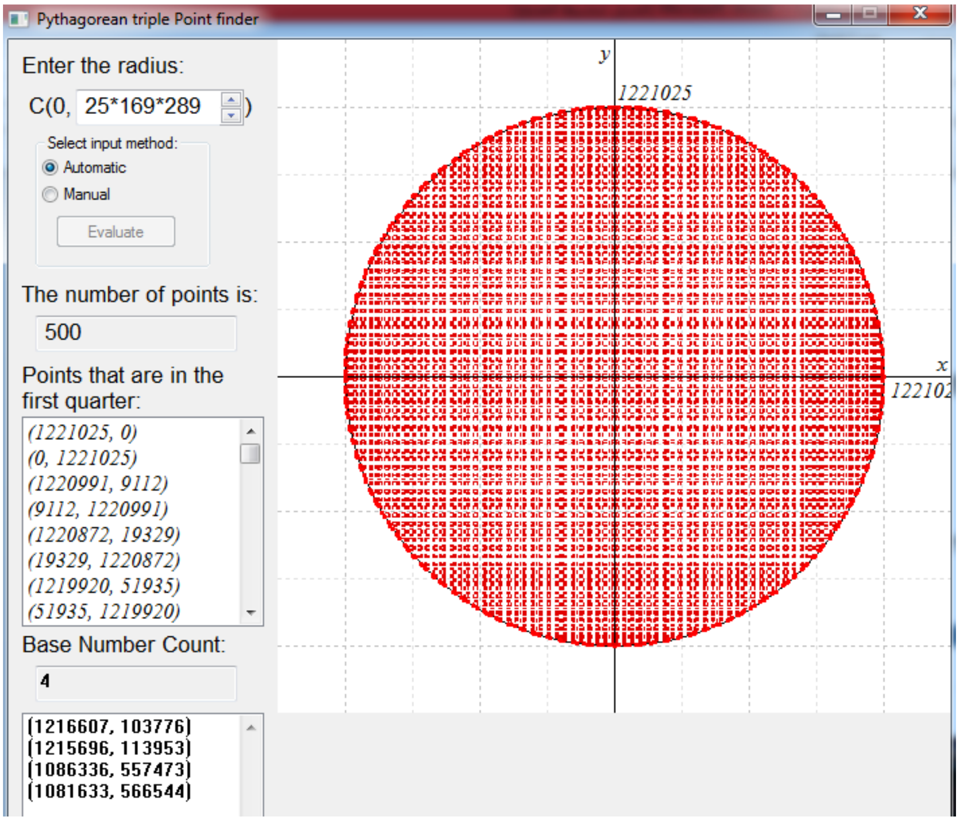
وهذه الثلاثيات هي:

$(1215696, 113953, 1221025)$ ، $(1216607, 103776, 1221025)$

$(1801633, 566544, 1221025)$ ، $(1086336, 557473, 1221025)$

وعدد النقاط الصحيحة الواقعة على محيط الدائرة:

$$N_{PT} = 4\times 3^{(3-3)}\left[(2(2)+1)(2(2)+1)(2(2)+1)\right] = 4\left[(5)(5)(5)\right] = 500$$



الشكل (5) يوضح النقاط الصحيحة والنقاط الأساسية والنقاط الأساسية الأولية على الدائرة الفيثاغورية

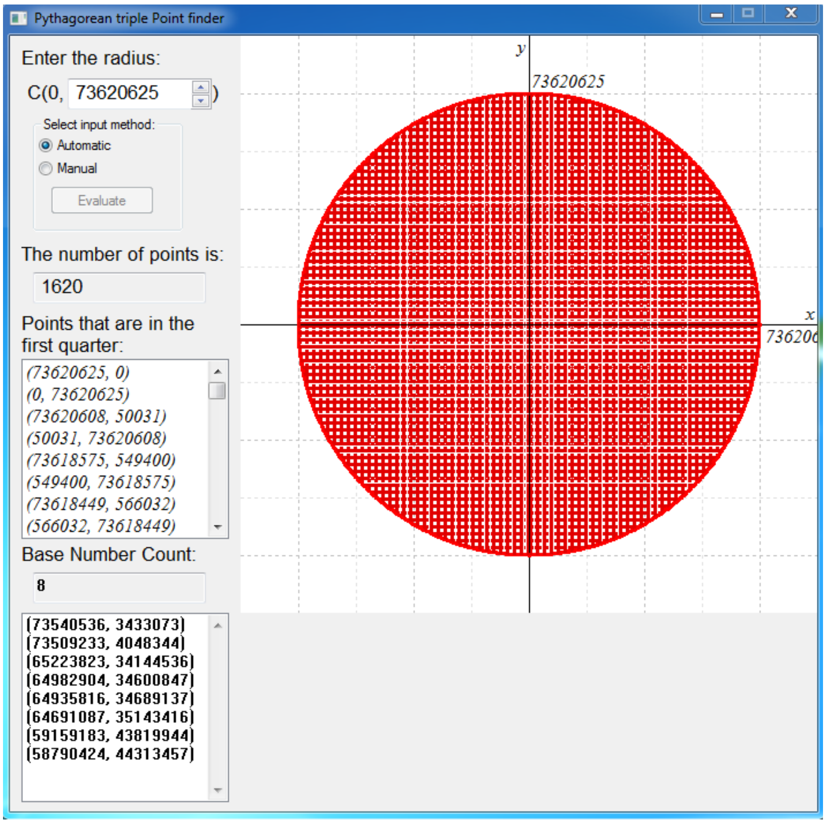
مثال 9:

من أجل: $R = 5^4 \times 13^2 \times 17 \times 41 \times 61 = 73620625$

يكون لدينا:

$$N_{PPT} = 2^{k-1} = 2^{4-2} = 4$$

$$N_{PT} = 4\times 3^{(4-2)}\left[(2(4)+1).(2(2)+1)\right] = 1620$$



الشكل (6) يوضح النقاط الصحيحة والنقاط الأساسية والنقاط الأولية على الدائرة الفيثاغورية

الخلاصة:

قمنا من خلال دراستنا السابقة بالتعامل مع شكل خاص من الدوائر المركزية والغاية من ذلك توظيف المعلومات والنتائج المستنتجة في تطبيقات التشفير وأمن المعلومات والإعتماد على الدوائر الفيثاغورية في التشفير عوضاً عن استخدام المنحنيات الناقصة Elliptic Curves (D.Hankerson, 2004)،والقصد من وراء ذلك التوصل إلى آليات تشفير جديدة تكون أسهل أسرع وأكثر أمناً من سابقاتها، ويبقى الباب مفتوحاً على مصراعيه للتوسع في هذه الأبحاث من خلال التوجه لتعميم هذه الدراسة والتعامل مع الدوائر الفيثاغورية غير المركزية ودراسة الكرات الفيثاغورية المركزية وغير المركزية(Takloo-Bighash, 2018) .

قائمة المراجع

[1] *Cryptography Schemes based on Elliptic Curve Pairings*"(2004)S.S Al-Riyami University of London.

[2] .Springer."*Elliptic Curve Cryotosystems*"(2016)Christof Paar،Jan Pelzl

[3] الكيالي شمة. (2016).*توليد ثلاثيات فيثاغورث أولية من أعداد ذات طبيعة خاصة*.جامعة البعث.

[4] Song Y. Yan) .2013 ".(*Computational Number Theory and Modern Cryptography* ."Wiley.

[5] شمة الخطيب. (2019). *توليد النقاط الصحيحة على الدائرة الفيثاغورثية المولدة بنصف قطر مضاعف*. جامعة البعث.

[6] شمة الخطيب. (2019). *توليد النقاط الصحيحة على الدائرة الفيثاغورثية المولدة بنصف قطر لجداءات مختلفة*. جامعة البعث.

[7].Springer، *Integer Points on Algebraic Varieties*،(2016)،Corvaja،Pietro

[8] Subhash Kak) .20101 " .(*Pythagorean Triples and Cryptographic Coding .* "Oklahoma: Oklahoma State University.

[9] D.Narasimha murty Raja Rama Gandhi) .2012 " .(*Generalization of Pythagorean triples،Quadruple .* " The Bulletin of Society for Mathematical Services and Standarrds.

[10] E.J. Eckert) .1984 " .(*The group of Primitive Pythagorean triangle .* "Math MMagazine.

[11] Coppel،W.A.).2006"،(*Number Theory*،"Springer.

[12] W Nar Kiewicz) .2004 " .(*Elementary and Analytic Theory of Algebraic Numbers .* "springer.

[13] R،Pomerance Crandall) .2005 " .(*Prime Number .* "Springer.

[14] U.Maurer)2009"(*Absraction in Cryptography*". Springer.

[15] A. Menezes،S. Vanstone D.Hankerson) .2004 " .(.*Guide to Elliptic Curve Cryptography .* "Springer.

[16]،Takloo-Bighash،Ramin)2018"،(*A Pythagorean Introduction to Number Theory*،"Springer.