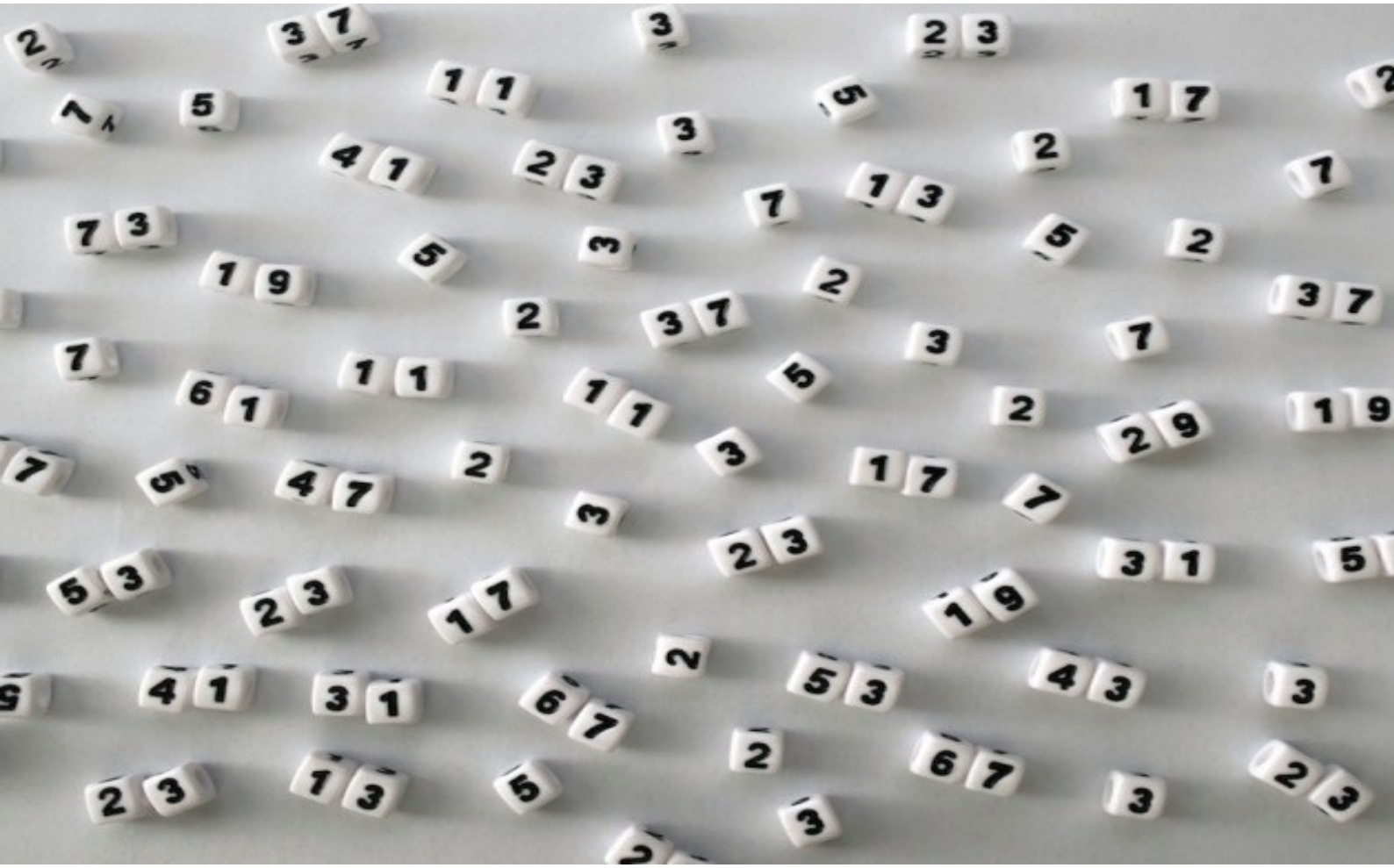
الجمهورية العربية السورية
هيئة التميز والإبداع
المركز الوطني للمتميزين

حلقة بحث علمية في مادة الرياضيات بعنوان:

تقريبات في الأعداد الأولية

إعداد الطالب: حسن دعبول
إشراف المدرسة: ندى علي



المقدمة:

يعرف العدد الأولي بكل عدد أكبر قطعا من الواحد ويقبل القسمة على نفسه وعلى العدد واحد فقط. لقد شغلت عدة قضايا في الأعداد الأولية علماء الرياضيات منذ العام 300ق.م وحتى الآن ما زال البحث جارٍ لإيجاد حل لهذه القضايا.

خضعت الأعداد الأولية لبحوث عديدة، حيث أثبتت العديد من المبرهنات أن الأعداد الأولية غير منتهية كمبرهنة إقليدس ومبرهنة أويلر التحليلي كما استطاع العالم yitang zhang في عام 2013 أن يثبت أن الأعداد الأولية غير نهائية لكنه أكد في دراسته أنها تصبح أكثر ندرةً كلما تقدما في اكتشاف أعداد أولية أكبر حيث وصل الفرق بين أكبر عددين أوليين مكتشفين حتى الآن إلى 70 مليون عدد، كما يوجد العديد من الحدسيات الغير مثبتة حتى الآن والتي تؤدي إلى تنظيم مبسط للأعداد الأولية والتقليل من عشوائيتها. كما قدم العلماء الرياضيون عدة دراسات أخرى حول الأعداد الأولية من بينها مبرهنتي أويلر وفيرما، كما بذل العلماء جهدا كبيرا لإيجاد طرق لاستنتاج وإيجاد أعداد أولية كبيرة جدا ومن القواعد التي استخدمت هي قواعد ميرسين وقواعد فيرما وقد تم إيجاد تطبيقات كثيرة على هاتين القاعدتين.

الإشكالية:

ما هي أهم الدراسات التي تعرضت لها الأعداد الأولية وما أهميتها وهل هناك قدرة أو طريقة معينة تمكننا من إيجاد أعداد أولية كبيرة؟

الباب الأول: مقدمة في دراسة الأعداد الأولية

تعريف 1-1 [1]

(أ) يقال عن $P \in N^*$ أنه عدد أولي (Prime Number) ، إذا كان $p > 1$ ولا يقبل القسمة إلا على P و 1 .

(ب) يقال عن $1 < a \in Z$ ، أنه عدد مؤلف (Composite number) ، إذا كان a عدداً غير أولي .

مثال (١) :

(أ) 2,3,5,7,11,13,17,19,23 أعداد أوليه بينما 6 عدد مؤلف لأن 6 يقبل القسمة على 2 .

(ب) $5! + 2$ عدد مؤلف ، لأن $5! + 2$ يقبل القسمة على 2 . لاحظ أن $5!+2 = 2(61)$.

(ج) $5! + 3$ عدد مؤلف ، لأنه يقبل القسمة على 3 ، كما أن $5!+3 = 3(41)$ ، $1 < 3 < (5!+3)$ ، $1 < 41 < (5!+3)$.

إذا كان $n > 2$ ، فإن n عدد مؤلف إذاً وإذا فقط وجد $a,b \in Z$ ، بحيث أن $n = ab$ ، $1 < a < n$ ، $1 < b < n$

" يسمى كل من a,b عامل من عوامل n "

البرهان :

إذا كان $n = ab$ ، $1 < a < n$ ، $1 < b < n$ ، فمن الواضح أن n عدد مؤلف . ولإثبات العكس نفرض أن n عدد مؤلف . إذاً يوجد $1 \neq a \neq n$ و $a \backslash n$ وعليه يوجد $b \in Z$ بحيث أن $n = ab$ ، لكن $n,a \in Z^+$. إذاً $b \in Z^+$ ، وعليه فإن $1 \leq a$ ، $1 \leq b$. لكن $a \backslash n$ و $b \backslash n$. إذاً $a \leq n$ و $b \leq n$. لكن $a \neq 1$ ، $a \neq n$. إذاً $1 < a < n$. وإذا كان $b = 1$ ، فإن $n = a$ وهذا غير ممكن . إذاً $b \neq 1$. وإذا كان $b = n$ ، فإن $a = 1$ وهذا غير ممكن . إذاً $1 < b < n$.

□

مبرهنة 1-2 [1]

كل الأعداد الأولية فردية ما عدا العدد 2 ، وكل منها على الشكل $4m+1$ أو $4m-1$ حيث $m \in Z^+$ ، لأن أي عدد صحيح يمكن كتابته بالشكل

$$m \in Z \ ، \ 4m \ , \ 4m+1 \ , \ 4m+2 \ , \ 4m+3$$

لكن $4m$ ليس أولياً ، كما أن $2 \backslash 4m+2$ ، وعليه فإن $4m+2$ عدد أولي عندما $m=0$ و 2 عدد أولي زوجي . إذاً أي عدد أولي فردي على الشكل $4m+1$ ، $4m+3$. لكن $S=\{4m+3 \mid m \in n\}=\{4m-1 \mid m \in n^*\}$

إذاً كل عدد أولي فردي على الشكل $4m-1$ أو $4m+1$ ، $m \in n^*$

ولأهمية الأعداد الأولية وضع العلماء تخمينات (Conjectures) كثيرة عليها منها :

(أ) يوجد عدد لا نهائي من الأعداد الأولية على الشكل n^2+1 ، $n \in n^*$ وهذا الحدس أو التخمين لم يثبت بعد . لاحظ أن $2=1^2+1$ ، $5=2^2+1$ ، $17=4^2+1$ ، $37=6^2+1$ ، $197=(14)^2+1$.

(ب) حدس جولدباخ (١٦٩٠-١٧٦٤م) عام ١٧٤٢م :

يمكن التعبير عن أي عدد صحيح زوجي أكبر من 2 كمجموع عددين أوليين .

لاحظ أن $4=2+2$ ، $6=3+3$ ، $8=3+5$ ، $1=3+7$ ، $12=5+7$ ، $14=7+7$ ، $16=5+11$.

وإذا كان حدس جولدباخ صحيحاً ، فإن ذلك يعني أنه يمكن العبير عن أي عدد فردي أكبر في 5 كمجموع ثلاثة أعداد فردية ، لأن إذا كان $n>5$ عدداً فردياً فإن $n-3$ عدد زوجي أكبر من 2 وعليه فإن $n-3=p+q$ ، حيث p,q عددين أوليين وبالتالي فإن $n=p+q+3$.

(ت) يوجد عدد لا نهائي من الأعداد الأولية على الشكل P,P+2، حيث P عدد أولي.
تسمى الأعداد التي تكون على هذا الشكل "الأعداد الأولية التوأمية (Twin prims)
مثل 3,5 ، 11,13 ، 17,19.

(ث) تخمين أو حدس العالم الفرنسي لاجرانج (1736-1813) عام 1775م: إذا كان n عددا صحيحا فرديا أكبر من 5، فإن $n=p_1+2p_2$، حيث p_1،p_2 عددين أوليين.

والآن إلى التعريف التالي:

تعريف

الترتيب الطبيعي للأعداد الأولية هو $p_1=2, p_2=3, p_5=11, p_n, ...$ ويسمى p_n العدد الأولي النوني في الترتيب الطبيعي.

ويمكننا الآن أن نبرهن ما يلي:

مبرهنة 1-3 [1]

$$p_n \le 2^{2^{m-1}} \text{ لكل } n \in n^* .$$

البرهان : (باالأستقراء على n)

إذا كان $n=1$ ، فإن $p_1=2$ وعليه فإن العلاقة صحيحة عندما $n=1$.

والآن لنفرض أن العلاقة أعلاه صحيحة عندما $n=m$ ، إذاً $p_m \le 2^{2^{m-1}}$.

ولإثبات صحة العلاقة عندما $n=m+1$. لاحظ أن

$$p_{m+1} \le p_1 p_2 \cdots p_m + 1 \le 2 \cdot 2^2 \cdots 2^{2^{m-1}} + 1$$

لكن $2 \cdot 2^2 \cdots 2^{2^{m-1}} = 2^{1+2+\cdots 2^{m-1}}$ ، $1+2+\cdots+2^{m-1} = 2^m - 1$. إذاً

$p_{m+1} \le 2^{2^m-1}+1$. لكن $1 \le 2^{2^m-1}$ لكل $m \in N$. إذاً

$p_{m+1} \le 2^{2^m-1}+2^{2^m-1} = 2 \cdot 2^{2^m-1} = 2^{2^m}$ ، وعليه فإن العلاقة أعلاه صحيحة عندما $n=m+1$. إذاً $p_n \le 2^{2^{n-1}}$ لكل $m \in N^*$

نتيجة :

إذا كان $n \geq 1$ عدداً صحيحاً ، فيوجد على الأقل $n+1$ من الأعداد الأولية كل منها أقل من 2^{2^n} .

البرهان :

بما أن كلاً من $p_1, p_2, \cdots, p_{n+1}$ أقل من 2^{2n} حسب مبرهنة (٢-٢-٢) .
إذاً يوجد على الأقل $(n+1)$ من الأعداد الأولية كل منها أقل من 2^{2n} .

مبرهنة 4-1 [2]

(أ) إذا كان $a,b \in Z$ ، p عدداً أولياً كان $p \backslash ab$ فإما $p \backslash a$ أو $p \backslash b$.

(ب) إذا كان $a_1, \cdots, a_n \in Z$ و p عدداً أولياً وكان $p \backslash a_1 a_2 \cdots a_n$ فإن $p \backslash a_i$ لبعض قيم $1 \leq i \leq n$.

البرهان :

(أ) نفرض أن $p \backslash ab$ ، $p \backslash b$. إذاً $(b,p)=1$ ، وعليه فإن $p \backslash a$ حسب مبرهنة (٢-١-٩ب) .

(ب) (بالأستقراء الرياضي على n) .

فإذا كان $n=1$ فإن $p \backslash a_1$ بالفرض ، وعليه فإن النتيجة صحيحة في هذه الحالة . والآن لنفرض أن النتيجة صحيحة عندما $n=m$. ولكي نثبت صحة النتيجة عندما $n=m+1$. لاحظ أنه إذا كان $p \backslash (a_1 a_2 \cdots a_{m+1})$ فإن $p \backslash a_1 (a_2 \cdots a_{m+1})$ وعليه إما $p \backslash a_1$ أو $p \backslash (a_2 \cdots a_{m+1})$ حسب (أ) فإذا كان $p \backslash a_1$ فقد أنتهى البرهان ، أما إذا كان $p \nmid a_1$ ، فإن $p \backslash a_2 \cdots a_{m+1}$ ، وعليه يوجد $2 \leq i \leq m+1$ بحيث أن $p \backslash a_i$ حسب فرضية الأستقراء الرياضي . إذاً النتيجة صحيحة عندما $n=m+1$. وعليه فإنها صحيحة لجميع قيم $n \in N^*$.

مبرهنة 5-1 [2]

(أ) كل عدد صحيح أكبر من الواحد يقبل القسمة على عدد أولي .

(ب) مجموعة الأعداد الأولية لا نهائية .

البرهان :

(أ) نفرض أن

$S=\{n\in Z^{+} \mid$ n أكبر من الواحد ولا يقبل القسمة على عدد أولي $\}\neq\phi$.

إذاً S تحوي عنصر أول (أصغر) وليكن m . إذاً m أكبر من الواحد ولا يقبل القسمة على عدد أولي فإذا كان m عدداً أولياً فإن $m\backslash m$ وهذا خلاف الفرض، أما إذا كان m غير أولي ، فإن $r\backslash m$ ، $1\neq r\neq m$ ، وعليه فإن $r<m$ ، ومنه ينتج أن $r\notin S$ ، وبالتالي فإن r يقبل القسمة على عدد أولي وليكن p ، وعليه فإن $p\backslash m$ وهذا خلاف الفرض أيضاً . إذاً $S=\varnothing$.

(ب) نفرض أن مجموعة الأعداد الأولية مجموعة منتهية وأن عنصرها هي $p_1,p_2,\cdots,p_n$. وليكن $n=1+(p_1\ldots p_n)$. إذاً $n>1$ ، وعليه فإن n يقبل القسمة على عدد أولي مثل p (حسب أ) . فإذا كان $p=p_i$ لبعض قيم $1\leq i\leq n$ ، فإن $p\backslash n$ و $p\backslash(p_1p_2\cdots p_n)$ ، وعليه فإن $p\backslash 1$، ومنه ينتج أن $p=1$ وهذا يناقض كون p عدداً أولياً . إذاً $p\neq p_i$ لكل $i=1,2,\cdots,n$ ، وعليه فإن مجموعة الأعداد الأولية مجموعة لا نهائية .

□

نتيجة (١) :

لكل عدد مؤلف n قاسم أولي p بحيث أن $p\leq\sqrt{n}$.

البرهان :

بما أن n عدد مؤلف . إذاً $n=ab$ ، $1<a\leq b$ ، وعليه فإن $a^2\leq n$ ، وبالتالي فإن $a\leq\sqrt{n}$. وبتطبيق مبرهنة (٢-٢-٤أ) يمكننا إيجاد عدد أولي p بحيث أن $p\backslash a$. لكن $a\backslash n$. إذاً $p\backslash n$ و $p\leq a$ ، وعليه فإن $p\leq\sqrt{n}$.

الباب الثاني: مبرهنتي اويلر وفيرما

يعرف الصينيون قبل حوالي 2000 سنة بأن (2^p-2) يقبل القسمة على p لأي عدد أولي p، وقد عمم فيرما تلك الحقيقة بدون إثبات عام 1640م إلى ما يسمى مبرهنة فيرما الصغرى "Fermat's Little Theorem" والتي تنص على أنه إذا كان a عددا صحيحا لا يقبل القسمة على p، فإن $(a^{p-1}-1)$ يقبل القسمة على p.

وقد حصل الألماني ليبنز (1646-1716) على نفس النتيجة وأثبتها بالإستقراء الرياضي سنة 1683م ولم ينشر البرهان. أما أول إثبات منشور لتلك المبرهنة فقد كان لأويلر سنة 1736م ثم عمم أويلر تلك المبرهنة سنة 1760م.

وسنقوم الآن بدراسة هاتين المبرهنتين وبعض تطبيقاتهما.

مبرهنة 2-1 [2]

إذا كان n عدداً صحيحاً موجباً وكان $a \in Z$ ، $(a,n)=1$ فإن $a^{\phi(n)} \equiv 1 \pmod n$.

البرهان :

ليكن $R=\{r_1,\cdots,r_{\phi(n)}\}$ نظام بواقي مختزل قياس n . إذاً $aR=\{ar_1,\cdots,ar_{\phi(n)}\}$ نظام بواقي مختزل قياس n حسب مبرهنة (٣-٣-٥) ، كما أن $|R|=|aR|=\phi(n)$. وعليه فإن كل عنصر من عناصر aR يطابق عنصراً وحيداً من عناصر R ، وبالتالي فإن

$$\prod_{i=1}^{\phi(n)}(a\,r_i) \equiv \prod_{i=1}^{\phi(n)} r_i \pmod n$$ ، وعليه فإن

$$a^{\phi(n)} \cdot \prod_{i=1}^{\phi(n)} r_i \equiv \prod_{i=1}^{\phi(n)} r_i \pmod n$$. لكن

$$a^{\phi(n)} \cdot \prod_{i=1}^{\phi(n)} r_i \equiv \prod_{i=1}^{\phi(n)} r_i \pmod n$$. لكن

$(r_i,n)=1$ لكل $1 \le i \le \phi(n)$. إذاً $(\prod_{i=1}^{\phi(n)} r_i,n)=1$ حسب مبرهنة (٢-١-٩أ) ، وعليه فإن $a^{\phi(n)} \equiv 1 \pmod n$ حسب نتيجة مبرهنة (٣-١-٤) .

فيرما الصغرى:

مبرهنة 2-2 [2]

إذا كان p عددا أوليا وكان $a \in Z$ و a و b أوليان فيما بينهما، فإن $a^p \equiv 1 (mod p)$.

الإثبات: بما أن a و b عددان أوليان فيما بينهما، إذا العامل المشترك الأكبر لهما هو 1 وعليه فإن $a^{f(p)} \equiv 1 (mod\ p)$ حسب مبرهنة أويلر، لكن

$$f(p) = |\{ m \in Z \mid 1 \le m \le p : (m,p) = 1 \}| = |\{ 1,2,3,\ldots,p-1 \}| = p-1$$

إذا $a^{p-1} \equiv 1 (mod\ p)$

المبرهنة 2-3 [3]

إذا كان p عددا أوليا فإن $a^{p-1} \equiv 1\ (mod\ p)$

الإثبات: سنناقش في الإثبات حالتين:

الحالة الأولى: a و p عددان غير أوليان فيما بينهما و p يقسم a بدون باقي فإن $a \equiv 0\ (mod\ p)$ وعليه فإن $a^p \equiv 0\ (mod\ p)$ وبالتالي فإن $a^p \equiv a$.

الحالة الثانية: a و p عددان أوليان فيما بينهما، فحسب مبرهنة فيرما يصبح لدينا $a^{p-1} \equiv 1\ (mod\ p)$ ومن ذلك نجد أن $a^p \equiv a\ (mod\ p)$.

مثال: لنحاول إثبات العلاقة التالية $a^{37} \equiv a\ (mod\ 1729)$

$1729 = 7 * 13 * 19$ إذاً إذا كان $(a,7) = (a,13) = (a,19) = 1$ فإن $a^6 \equiv 1\ (mod\ 7)$, $a^{12} \equiv 1\ (mod\ 13)$, $a^{18} \equiv 1\ (mod\ 19)$ حسب مبرهنة فيرما، وعليه فإن $a^6 * a^{12} * a^{18} = a^{1729}$ وهذا يعني $a^{36} \equiv a\ (mod\ 1729)$ إذا $a^{37} \equiv 1\ (mod\ 1729)$.

المبرهنة 2-4 [3]

إذا كان $(a,n) = 1$ فإن $a^{f(n)-1} \equiv 1\ (mod\ n)$ معكوس ضربي للعدد a قياس n.

الإثبات: بما أن $(a,n) = 1$ إذا $a^{f(n)} \equiv 1\ (mod\ n)$ وعليه فإن $a * a^{f(n)-1} \equiv 1\ (mod\ n)$ ومنها نجد أن $a^{f(n)-1}$ معكوس ضربي للعدد a قياس n.

المبرهنة 2-5 [3]

إذا كان $(a,n)=1$ فإن الحل الوحيد للتطابق $ax \equiv b (mod\ n)$ هو $x \equiv a^{\phi(n)-1}\ b (mod\ n)$

البرهان :

بما أن $(a,n)=1$. إذاً الحل الوحيد للتطابق الخطي $ax \equiv b \pmod n$ هو $x \equiv a^{-1} b \pmod n$ حسب مبرهنة (٣-٤-١) . لكن $a^{-1} = a^{\phi(n)-1}$ حسب نتيجة (٣) . إذاً الحل الوحيد هو $x \equiv a^{\phi(n)-1} \cdot b \pmod n$.

مبرهنة2،6

[1]

إذا كان $(a,n)=(a-1\,,\,n)=1$ ، فإن

$$1 + a + a^2 + \cdots + a^{\phi(n)-1} \equiv 0 \pmod n \,.$$

البرهان :

بما أن $(a,n)=1$. إذاً $a^{\phi(n)} \equiv 1 \pmod n$ حسب مبرهنة أويلر . لكن $a^{\phi(n)} - 1 = (a-1)(a^{\phi(n)-1} + \cdots + a^2 + a + 1)$ و $a^{\phi(n)} - 1 \equiv 0 \pmod n$ إذاً $(a-1)(a^{\phi(n)-1} + \cdots + a^2 + a + 1) \equiv 0 \pmod n$. لكن $(a-1\,,\,n)=1$ إذاً $(a^{\phi(n)-1} + \cdots + a^2 + a + 1) \equiv 0 \pmod n$ حسب نتيجة مبرهنة (٣-١-٤) .

□

ملاحظة :

عكس مبرهنة فيرما ليس صحيحاً . أي أنه إذا كان $(a,p)=1$ $a^{p-1} \equiv 1 \pmod p$ فقد لا يكون p عدداً أولياً كما يوضح ذلك المثال الآتي : $5^3 \equiv 1 \pmod 4$ و $(5,4)=1$ بينما 4 ليس أولياً .

الباب الثالث: أعداد خاصة

سوف ندرس أعداد مرسين وأعداد فيرما

إحدى طرق إيجاد الأعداد الأولية الكبيرة هي دراسة الأعداد على الشكل a^m+1 and a^m-1

ومن المثبت أنه إذا كان a^m-1 عددا أوليا فإن m عدد أولي و a=2 أما إذا كان a+1

ومن هنا نجد التعريف التالي: $2^n=m$ عدد زوجي و عدد a أولي فإن

يقال عن عدد F_n أنه عدد فيرما ، إذا كان $F_n = 2^{2^n} + 1$ ، $n \in N$.
وإذا كان F_n عدداً أولياً ، فيسمى F_n عدد فيرما الأولي .

مثال (١) :

$F_0 = 3$ ، $F_1 = 5$ ، $F_2 = 17$ ، $F_3 = 257$ ، $F_4 = 2^{16} + 1 = 65537$

وهي أعداد أولية ، وعلى الرغم من أن فيرما لم يحسب إلا تلك الأعداد فقد أعتقد أن F_n عدد أولي لكل $n \in N$ ، لكن أويلر أثبت عدم صحة ذلك بإثباته بأن $F_5 = 2^{32} + 1$ يقبل القسمة على 641 . ونعلم اليوم وبإستخدام برنامج " Maple " بأن F_n عدد مؤلف لكل $5 \le n \le 30$ ، وعندما $n = 36,38,39,55,63,73,382447$.

ولم يُكْتشف لحد الآن أي عدد فيرماتي أولي غير F_n ، $0 \le n \le 4$ ولذلك يعتقد العلماء عدم وجود أعداد فيرما أولية غير تلك الأعداد .

وتبرز أهمية أعداد فيرما الأولية بعد إثبات جاوس سنة ١٧٩٦م بأنه يمكن أن نرسم بالمسطرة والفرجال مضلعاً منتظماً عدد أضلاعه p إذاً وإذا فقط كان p عدد فيرما أولي .

$$\prod_{i=0}^{n-1} F_i = F_n - 2$$ لكل $n \in Z^+$.

البرهان : " بالإستقراء على n "

إذا كان $n = 1$ ، فإن $L.H.S. = F_1 = 3$ ، $R.H.S. = F_1 - 2 = 5 - 2 = 3$ ،
وعليه فإن الطرفين متساويان وبالتالي فإن العلاقة صحيحة عندما $n = 1$
والآن لنفرض أن العلاقة صحيحة عندما $n = m$. إذاً

$$\prod_{i=0}^{m-1} F_i = F_m - 2$$

مبرهنة 3-

$\underline{1}$ (4) $\underline{2}$

[2] مقدمة في نظرية الأعداد، أ.د فالح بن عمران بن محمد الدوسري، جامعة أم القرى-مكة1 المكرمة، الطبعة الأولى.

فـــردي ، لأن أعـــداد فيرمـــا أعـــداد فرديـــة ، إذاً $(p,2)=1$ ، وعليـــه فـــإن $2^{p-1}\equiv 1\,(\mathrm{mod}\ p)$ حسب مبرهنة فيرما ، وبالتالي فإن $2^{n+1}\backslash(p-1)$ حسب مبرهنة (٥-١-٣) ، ومنها نجد أن $p\equiv 1\ \mathrm{mod}(2^{n+1})$

□

مثال (٣) :

أثبت أن $F_4=2^{16}+1=65537$ عدد أولي .

الإثبات :

نفرض أن $p\backslash F_4$. إذاً $p=m\cdot 2^5+1$ حسب نتيجة مبرهنة (٥-١-٣) . وعليه فإن $p=3\cdot 2^5+1=97$ أو $p=8(2^5)+1=257$. لكن $97\nmid F_4$ و $p=257>\sqrt{F_4}\simeq 256\cdot 0019$. إذاً F_4 عـــدد أولـــي حـــسب نتيجـــة (٢) مبرهنة (٢-٢-٤) .

□

مثال (٤) :

أثبت أن $F_5=2^{2^5}+1$ عدد مؤلف .

الإثبات :

إذا كان $p\backslash F_5$ ، فإن $p=m\cdot 2^6+1$ حسب نتيجة مبرهنـــة (٥-١-٣) ، وعليـــه فـــإن $p=4(64)+1=257$ أو $p=10(64)+1=641$. لكـــن $F_5=4294967297$ لا يقبل القسمة على 257 و $p=641<\sqrt{F_5}=65537$ كما أن $F_5=641\times 6700417$. إذاً F_5 عدد مؤلف .

والآن إلى تعريف ودراسة خواص أعداد مرسين .

$\mathrm{ord}_7(6)=2$ لأن $6^2\equiv 1\,(\mathrm{mod}\ 7)$.

إذا كان p عـــدداً أوليـــاً ، $a\in Z$ ، $(a,p)=1$ ، $\mathrm{ord}_p(a)=n$ ، وكـــان $a^m\equiv 1\,(\mathrm{mod}\ p)$ ، فإن $n\backslash m$.

البرهان :

نفرض أن $d=(m,n)$. إذاً يوجد $r,s\in Z$ بحيث $d=mr+ns$ حـــسب مبرهنة (٢-١-٥) . لكن $a^n\equiv a^m\equiv 1(\mathrm{mod}\,p)$. إذاً $a^{mr}\equiv a^{nr}\equiv 1(\mathrm{mod}\,p)$ وعليه فإن $a^d\equiv a^{mr+ns}\equiv 1(\mathrm{mod}\ p)$. لكن n أصغر عدد صـــحيح موجـــب بحيث أن $a^n\equiv 1(\mathrm{mod}\ p)$. إذاً $n\le d$. لكن $d\backslash n$ يعنـــي أن $d\le n$. إذاً $n=d$. لكن $d\backslash m$ ، إذاً $n\backslash m$.

$$p \in \left\{ \begin{array}{l} 2,3,5,7,17,19,31,61,89,107,127,521,607,1279,2203 \\ 2281,3217,4253,4423,9689,9941,11213,19937,21701 \\ 23209,44497,86243,110503,132049,216091,756839 \\ 859433,1257787,1398269,2976221,3021377,6972593 \\ 13466917,25964951 \end{array} \right\}$$

تعريف

يقال عن عدد صحيح موجب M_n أنه عدد مرسين (Mersenne number) نسبة للفرنسي مرسين (١٥٨٨-١٦٤٨م) ، إذا كان $M_n = 2^n - 1$ ، $n \geq 2$.
وإذا كان M_n عدداً أولياً فيسمى M_n عدد مرسين الأولي .

لاحظ أنه إذا كان M_n عدداً أولياً ، فإن n عدد أولي حسب مبرهنة (٢-٢-٦)، كما أن هذا النوع من الأعداد معروف لأقليدس (٣٥٠ق.م) ونيقوماخوس (١٠٠ق.م) وثابت بن قرة (٨٢٦-٩٠١م) وغيره من الرياضيين العرب والمسلمين .

مثال (٥) :

$M_2 = 3$ ، $M_3 = 7$ ، $M_5 = 31$ ، $M_7 = 127$ أعداد أولية ، بينما $M_4 = 15$ ، $M_4 = 2047$ ليست أعداد أولية .

ونعرف حالياً وبإستخدام الحاسب الآلي أربعين عدد مرسين أولي M_p عندما

الخاتمة والنتائج:

*- بعد إنهاء هذا البحث نجد أن الأعداد الأولية تعتبر من أوسع مجالات الدراسة في الرياضيات حيث تم تقديم العديد من الدراسات الهامة في مجال الأعداد الأولية من بينها مبرهنتي أويلر وفيرما وأوجد العلماء طريقة لإيجاد الأعداد الأولية الكبيرة وهو ما يسمى بقاعدة مرسين وقاعدة فيرما أيضا ودرسنا كيفية استخدام هذه القواعد لاستنتاج الأعداد الأولية وما هي أهم تطبيقاتهما إلا أن هناك العديد من القضايا في الأعداد الأولية لم تحل بعد كقضية العشوائية في الأعداد الأولية التي عجز العلماء عن حلها منذ العام 300 قبل الميلاد، حيث وضع العلماء عدة حدسيات غير مبرهنة حتى الآن لإيجاد تنظيم جيد للأعداد الأولية وكما أنه ومن المؤكد أن الوصول إلى إثبات إحدى الحدسيات سيؤدي إلى تنظيم جزء من عشوائية الأعداد الأولية.

*- يوجد علاقة وثيقة بين الأعداد الأولية والأعداد المؤلفة "الغير أولية" حيث يمكننا استنتاج عدد كبير من الأعداد الأولية من الأعداد المؤلفة عبر عدة قواعد درسناها في البحث.

المراجع العلمية:

1- مقدمة في نظرية الأعداد، أ.د فالح بن عمران بن محمد الدوسري، جامعة أم القرى-مكة المكرمة، الطبعة الأولى.

2- .نظرية الأعداد، د.دعد الحسين و د.محمد بشير قابيل، منشورات جامعة دمشق

3- Elementary number theory ،David Burton ،University of new Hampshire.

4- شرح نظرية الأعداد، د.أحمد حسان العضين، منشورات جامعة تشرين

5- www.plus.maths.org

الفهرس:

العنوان	الصفحة
المقدمة	2
الإشكالية	2
الباب الأول: مقدمة في دراسة الأعداد الأولية	3
الباب الثاني: مبرهنتي أويلر وفيرما	8
الباب الثالث: أعداد أولية خاصة	11
الخاتمة والنتائج	15
المراجع العلمية	16
الفهرس	16