كلية العلوم

القسم : **الرياضيات**

السنة : **الرابعة**

مكتبة A to Z للخدمات الجامعية

المادة : نظرية الاعداد

المحاضرة : الثالثة /نظري/

{{ A to Z مكتبة }}

Facebook Group : A to Z مكتبة

السؤال الأول: كم هو عدد الأعداد الأولية:

شغلت هذه المسألة عقول علماء الرياضيات منذ القدم وقد وضعت براهين كثيرة تثبت أنّ عدد الأعداد الأولية غير منتهٍ ومن أقدم هذه البراهين وأبسطها البرهان الذي وضعه اقليدس

مبرهنة اقليدس: يوجد عدد غير منتهٍ من الأعداد الأولية.

الاثبات:

لتكن S مجموعة كل الأعداد الأولية نفرض جدلاً أنّه يوجد عدد غير منتهٍ من الأعداد الأولية $|S| = n \; ; n \in \mathbb{Z}^+$

$S = \{p_1, p_2, \ldots, p_n\}$ و $p_1 < p_2 < \ldots < p_n$

لنأخذ $N = p_1 p_2 \ldots p_n + 1$ بما أنّ $N > 1$ فهو يملك عامل أولي p حيث $N \notin S$

$p | n$ عندئذٍ يوجد i بحيث $p = p_i$ فنلاحظ:

$p | p_1 p_2 \ldots p_n$ & $p | N$ بالتالي: $p | (N - p_1 p_2 \ldots p_n) \Rightarrow p | 1$

وهذا مرفوض بالتالي الفرض الجدلي خاطئ بالتالي هنالك عدد غير منتهٍ من الأعداد الاولية.

السؤال الثاني: هل هنالك صيغة تعطي جميع الأعداد الأولية:

1- الأعداد ذات الصيغة $N_k = p_1 p_2 \ldots p_k + 1 \; ; k \in \mathbb{Z}^+$

اعتقد اقليدس بأنّها تعطي أعداد أولية

$N_1 = p_1 + 1 = 2 + 1 = 3$ (عدد أولي)

$N_2 = p_1 \cdot p_2 + 1 = 2\times 3 + 1 = 7$ (عدد أولي)

$N_3 = 31$ (عدد أولي)

$N_4 = 211$ & $N_5 = 2311$

$N_6 = 2\times3\times5\times7\times11\times13 + 1$ ولكن لسوء الحظ

$N_6 = 59 \times 506 \Rightarrow$ N_6 ليس عدد أولي

2- وضع فيرما (1601 - 1665)

الصيغة $F_n = 2^{2^n} + 1$ وظنّ أنها تعطي أعداد أولية من أجل جميع قيم n

$n = 0, 1, 2, \ldots$ ولكن فيما بعد تبيّن أنّ اعتقاد فيرما ليس صحيح حيث

أثبت أولر أنّ F_5 عدد مؤلف يقبل القسمة على 641

الاثبات:

$F_5 = 2^{2^5} + 1 = 2^{32} + 1 = (2^7)^4 \cdot 2^4 + 1$

نضع $a = 2^7$ & $b = 5$

$641 = 1 + ab = 1 + 2^7 \cdot 5$

$16 = 1 + ab - b^4 \Rightarrow F_5 = (2^7)^4 \cdot 2^4 + 1$

$a^4(1 + ab - b^4) + 1$

$= a^4 + a^5 b - a^4 b^4 + 1$

$= a^4(1 + ab) - (a^4 b^4 - 1)$

$= a^4(ab+1) - (a^2b^2 - 1)(a^2b^2+1)$

$= a^4(ab+1) - (ab-1)(ab+1)(a^2b^2+1)$

$= (1+ab)\left[a^4 - (ab-1)(a^2b^2+1)\right]$

$= (1+ab) \cdot t \quad ; \quad t = a^4 - (ab-1)(a^2b^2+1)$

$\Rightarrow (1+ab) \mid F_5 \Rightarrow 641 \mid F_5$

بالتالي F_5 عدد ليس أولي

• سوف نقدّم بعض النتائج المتعلّقة بأعداد فيرما:

مبرهنة: ليكن لدينا $f_n = 2^{2^n}+1$ حيث $n \in \mathbb{N}$

1. $F_0 \cdot F_1 \cdot \ldots \cdot F_{m-1} = F_m - 2 \quad \forall m \geq 1$

2. $gcd(F_n , F_m) = 1$ حيث $n \neq m$ أو بطريقة أخرى أثبت أنّ أعداد فيرما أولية فيما بينها مثنى مثنى؟

الاثبات:

[1] بطريقة الاستقراء الرياضي:

• نثبت صحة العلاقة من أجل $m=1$:

$$\left.\begin{array}{l} P_1 = f_0 = 2^{2^0}+1 = 3 \\ P_2 = f_1 - 2 = 2^{2^1}-2+1 = 3 \end{array}\right\} \Rightarrow P_1 = P_2$$

العلاقة محققة من أجل $m=1$

• نفرض صحة العلاقة من أجل $m=k$:

$$F_0 \cdot F_1 \cdot \ldots \cdot F_{k-1} = F_k - 2$$

• نثبت صحة العلاقة من أجل $m=k+1$ أي لنثبت أنّ:

$$f_0 \cdot f_1 \cdot \ldots \cdot f_k = f_{k+1} - 2$$

لدينا: $P_1 = f_0 \cdot f_1 \cdot \ldots \cdot f_k = f_0 \cdot f_1 \cdot \ldots \cdot F_{k-1} \cdot f_k =$

$$(f_k - 2) \cdot f_k = (2^{2^k}-1)(2^{2^k}+1) = (2^{2^k})^2 - 1 =$$

$$2^{2^{k+1}} - 1 = 2^{2^{k+1}}+1-1-1 = 2^{2^{k+1}}+1-2 = F_{k+1}-2 = P_2$$

بالتالي نلاحظ مما سبق أنّ العلاقة محققة من أجل $n=k+1$

ومنه العلاقة محققة $\forall n \in \mathbb{N}$.

[2] الاثبات:

باعتبار $n \neq m$ فرضاً بالتالي أحد العددين وليكن m أكبر من n

$(m > n)$ وليكن $d = gcd(f_n , f_m)$ لنثبت أنّ $d=1$

$$\Rightarrow d \mid f_m \ \& \ d \mid f_n$$

لدينا $f_0 . f_1 . \dots . f_{m-1} = f_m - 2$

$f_0 . f_1 . \dots . f_n . \dots . f_{m-1} = f_m - 2$

$$\left.\begin{array}{l} d \mid f_n \Rightarrow d \mid (f_m - 2) \\ \& \ d \mid f_m \end{array}\right\} \Rightarrow d \mid (f_m - (f_m - 2)) \Rightarrow d \mid 2$$

نلاحظ أنّ $d \neq 2$ لأنّ أعداد فيرما أعداد فردية بالتالي $d = 1$

وبالتالي $\gcd(f_n , f_m) = 1$

ملاحظة: $\forall n,m \in \mathbb{N}$ $n \neq m$ و $\gcd(f_n , f_m) = 1$

بالتالي يوجد عدد لانهائي من أعداد فيرما المختلفة f_k

f_k

أولي — مؤلف

بالتالي هناك عدد لانهائي من الأعداد الأولية — (يملك عامل أولي)

- التحليل إلى عوامل أولية بطريقة فيرما:

أوجد فيرما طريقة لتحليل العدد الصحيح إلى عوامله الأولية حيث تتعامل فقط مع الأعداد الفردية لأنّه إذا كان n عدد زوجياً فيمكن ببساطة أن يكتب $n = 2^i . m$ حيث m عدد فردي عندئذٍ يمكن تحليل العدد n إلى عوامله الأولية بطريقة فيرما

- تعتمد طريقة فيرما على الحقيقة التالية:

مبرهنة تمهيدية: ليكن n عدداً صحيحاً موجباً فردياً عندئذٍ n تُكتب كحاصل ضرب عددين صحيحين موجبين a و b إذا وفقط إذا أمكن كتابة n كفرق لمربعي عددين صحيحين.

البرهان:

$\Leftarrow$ $a,b \in \mathbb{Z}^+$ و $n = ab$ ، $\frac{a+b}{2} \in \mathbb{Z}$, $\frac{a-b}{2} \in \mathbb{Z}$

لأنّ n فردي

$$n = \left(\frac{a+b}{2}\right)^2 - \left(\frac{a-b}{2}\right)^2 = x^2 - y^2 \quad ; \quad \begin{cases} x = \frac{a+b}{2} \\ y = \frac{a-b}{2} \end{cases}$$

$(\Rightarrow)$ $$n = x^2 - y^2 = (x-y)(x+y) \Rightarrow n = ab$$

وهو المطلوب.

• طريقة فيرما في تحليل العدد الفردي:

إنّ طريقة فيرما في تحليل عدد فردي n إلى جداء عاملين تعتمد على كتابة n بالشكل $n = x^2 - y^2$ أي $x^2 - n = y^2$

وتتلخص بالخطوات التالية:

1. نوجد أصغر عدد صحيح موجب k بحيث $k \geq \sqrt{n}$.
2. نحسب بالتالي: $k^2 - n \,,\, (k+1)^2 - n \,,\, (k+2)^2 - n , \dots$

فنلاحظ قيمة m $(m \geq \sqrt{n})$ تجعل $(m^2 - n)$ مربعاً كاملاً.

$$m^2 - n = d^2 \Rightarrow n = m^2 - d^2 = (m-d)(m+d)$$

3. إنّ خطوات العمل من دون شك منتهية لأنّه لابدّ أن نصل إلى الخطوة الأخيرة $\left(\frac{n+1}{2}\right)^2 - n = \left(\frac{n-1}{2}\right)^2$

وعندها $n = n.1$ مما يدل على أنّ n عدد أولي

وذلك إذا لم نحصل على (m^2-n) مربعاً صحيحاً في خطوة سابقة.

مثال (1): حلل العدد $n = 23449$ إلى جداء عاملين بطريقة فيرما:

$\sqrt{n} = \sqrt{23449} = 153.1306632$ $\qquad k = 154$

$k^2 - n = (154)^2 - 23449 = 267$

$(k+1)^2 - n = (155)^2 - (23449) = 576$

$\sqrt{576} = (24)^2$ و مربع كامل

$n = (155)^2 - (24)^2 = (155+24)(155-24)$

$n = (179)(131)$ جداء أعداد أولية

مثال (2): حلّل العدد $n = 315$ إلى عوامله الأولية:

$k = \sqrt{315} = 17.748 \Rightarrow k = 18$

$k^2 - n = (18)^2 - n = 9 = 3^2$

$\Rightarrow n = (18-3)(18+3) = 15 \times 21 = 3 \times 5 \times 3 \times 7$

$n = 3^2 \times 5 \times 7$ جداء أعداد أولية

مثال 3: أثبت أنّ $n = 43$ عدد أولي باستخدام طريقة فيرما

الحل:

$\sqrt{43} = 6.557 \Rightarrow k = 7$

$k^2 - n = (7)^2 - 43 = 6$

$(k+1)^2 - n = (8)^2 - 43 = 21$

$(k+2)^2 - n = 38$

$(k+3)^2 - 43 = 57$

$(k+15)^2 - 43 = (22)^2 - 43 = 441 = (21)^2$

$\Rightarrow n = 43 = (22)^2 - (21)^2 = (22-21).(22+21)$

$= 1 \times 43$ جداء أولي

التّطابقات: قدّم الرياضي الألماني غاوس (1777 – 1855) مفهوم التطابق بالنسبة لمقاس عدد صحيح موجب m. يعدّ التطابق أداة قوية في برهان الكثير من المسائل المتعلقة بقابليّة القسمة وبواسطته نستطيع أن نحل وبسهولة الكثير من المسائل الرياضية.

التعريف: ليكن $a, b \in \mathbb{Z}$ و $m \in \mathbb{Z}^+$ يُقال إنّ العدد a يطابق العدد b بالمقاس n ونكتب $a \equiv b \pmod{n}$ أو $a \underset{m}{\equiv} b$

إذا كان $m \mid (a-b)$.

ملاحظة: إذا كان $m \nmid (a-b)$ فإننا نقول بأن a لا يطابق العدد b بالمقاس m ونكتب $a \not\equiv b \pmod{n}$

مثال 1: $111 \equiv 1 \pmod{5}$

مثال 2: $-30 \equiv 3 \pmod{11}$

مثال 3: $10 \equiv -11 \pmod{21}$

$10 \not\equiv 2 \pmod{7}$

مبرهنة: إذا كان $a, b \in \mathbb{Z}$ و $m \in \mathbb{Z}^+$ فإن $a \equiv b \pmod{n}$

$\Longleftrightarrow$ يوجد عدد صحيح q بحيث أن $a = b + q.m$.

البرهان:

لزوم الشرط $\Rightarrow$ لدينا $a \equiv b \pmod{m} \Rightarrow m \mid (a-b)$

$\exists q \in \mathbb{Z} \; ; a-b = q.m \Longrightarrow a = b + q.m$

كفاية الشرط $\Longrightarrow$ $a = b + q.m \; ; q \in \mathbb{Z}$

$a - b = q.m$

$\Rightarrow m \mid (a-b)$

$\Rightarrow a \equiv b \pmod{m}$

انتهت المحاضرة