بسم الله الرحمن الرحيم

جامعة السودان للعلوم والتكنولوجيا

كلية التربية

قسم العلوم - شعبة الرياضيات

بحث تكميلي لنيل درجة بكالريوس الشرف في التربية رياضيات

بعنوان : نظرية الأعداد وبعض تطبيقاتها

Numbers Theory and some its Applications

إعداد الطلاب :

- آمنة جبريل بوش محمد
- حواء حسين عيسى يعقوب
- نعيمة آدم محمد دهب
- نادية محمد الفزاري
- هاجر معتصم عبدالدائم محمد

إشراف الدكتور :

عبدالقادر البشرى الضي

2018 م سبتمبر

بسم الله الرحمن الرحيم

الآيـة

قال تعالى: ﴿يَا أَيُّهَا الَّذِينَ آمَنُوا إِذَا قِيلَ لَكُمْ تَفَسَّحُوا فِي الْمَجَالِسِ فَافْسَحُوا يَفْسَحِ اللَّهُ لَكُمْ وَإِذَا قِيلَ انشُزُوا فَانشُزُوا يَرْفَعِ اللَّهُ الَّذِينَ آمَنُوا مِنكُمْ وَالَّذِينَ أُوتُوا الْعِلْمَ دَرَجَاتٍ وَاللَّهُ بِمَا تَعْمَلُونَ خَبِيرٌ (١١)﴾

صدق الله العظيم

المجادلة : الآية (11)

الإهداء

لا خيل عندي أهديها ولا مال..فليسعد النطق إن لم يسعد الحال

إلهي لا يطيب الليل إلا بشكرك..ولا يطيب النهار إلا بطاعتك..

ولا تطيب اللحظات إلا بذكرك ..ولا تطيب الآخرة إلا بعفوك..

ولا تطيب الجنة إلا برؤيتك..

الله جلّ جلاله

إلى من بلغ الرسالة وأدّى الأمانة ..ونصح الأمة ..إلى نبي الرحمة..إلى نور العالمين ..سيدنا

محمد صلّى الله عليه وسلم

إلى ملاكي في الحياة ..إلى معنى الحب وإلى معنى الحنان والتفاني..إلى بسمة الحياة ..إلى سر الوجود..إلى من كان دعائها سر نجاحي ..وحنانها بلسم جراحي ..إلى أغلى الحبايب ..إلى من بها أكبر وعليها أعتمد..إلى شمعة متقدة تنير ظلمة حياتي ..إلى من بوجودها أكتسب قوة ومحبة لا حدود لها ..إلى من عرفت معها معنى الحياة ..

أمي الحبيبة

إلى من كلله الله بالهيبة والوقار .. إلى من علمني العطاء بدون إنتظار ..إلى من أحمل اسمه بكل إفتخار ..أرجو من الله أن يمد في عمرك لترى ثماراً قد حان قطافها بعد طول إنتظار ..وستبقى كلماتك نجوم أهتدي بها اليوم وفي الغد وإلى الأبد..

والدي العزيز

إلى إخوتي ورفاق دربي في هذه الحياه ..أنتم بها كل شي..وبدونكم لا شي..معكم أكون أنا ..وبدونكمأكون لا شيء..في نهايةٍ لمشوار أريد أن اشكركم لمواقفكم النبيلة إلى تطلعاتكم لنجاحي بنظرات من الأمل..

إخوتي وزملائي الأعزاء

شكر وعرفان

لابد لنا ونحن نخطو خطواتنا الأخيرة في حياتنا الجامعية من وقفة تعود إلى أيام قضيناها في رحاب الجامعة مع أساتذتنا الكرام الذين قدموا لنا الكثير باذلين بذلك جهودا كبيرة في بناء جيل الغد لتبعث الأمة من جديد

وقبل أن نمضي نقدم اسمى ايات الشكر والإمتنان والتقدير والمحبة ..إلى الذين حملوأقدس رسالة في الحياة ..إلى الذين مهدوا لنا طريق العلم والمعرفة ..إلى جميع أساتذتنا الأفاضل..

بجامعة السودان للعلوم والتكنولوجيا

والشكر كل الشكر

لمن لم يبخل لنا بوقته الثمين ... ولا بعلمه الرائع

لمن كان لنا أخاً قبل أن يكون أباً ... وكان أباً قبل أن يكون معلماً

وكان معلماً قبل أن يكون قدوة

الدكتور : عبدالقادر البشرى الضي .

Abstract

The research includes four chapters dealing with the first chapter discussed the research plan .In the second chapter ,we learned about the theory of numbers , integers numbers ,their properties ,the base of the order ,the mathematical extrapolation ,the division ,the common denominator ,and the primary numbers . In three chapter, we identified the correspondence and its properties, the sediment systems, the oiler function ,the linear matches ,finally in the fourth chapter we discussed numerical functions and coding and obtained some results through the research topics ,as well as some recommendations and the references through which the research was written .

المستخلص

يتضمن البحث أربعة فصول تتناول الفصل الأول مناقشة الخطة البحثية. في الفصل الثاني ،يتحدث عن نظرية الأعداد ، أعداد الأعداد الصحيحة ، خواصها ، وقاعدة الترتيب الحسن ، الاستقراء الرياضي ، قابليةالقسمة ، القاسم المشترك الاعظموالأعداد الأولية .كذلك في الفصل الثالث ،تعرفنا على تطابق وخواصه وانظمة الرواسب ودالة اويلر والتطابقات الخطية وبعض التطابقات الخاصة والتطابق الجبري ، وأخيرا في الفصل الرابع تناولنا الدوال العددية والتشفير وتحصلنا على بعض النتائج من خلال موضوعات البحث ، وكذلك بعض التوصيات و المراجع التي تم من خلالها كتابة البحث.

الفهرست

الفصل الاول

(1-1)المقدمة:

العدد لغة العلم ، وأفضل وسيلة للتعبير عنه هي الرموز، والأرقام هي أشكال تكتب بها رموز الأعداد ، والحساب أونظرية الأعداد هيعلم العدد ، جانبه النظري يعالج الأرقام والأعداد ، مراتبها والنسب التي بينها وتكرارها على نسق معين ، وأنواعها وكيفية بنائها ودراسة خواصها والعلاقات بينها ،وجانبه العملي يتناول الحسبان ، معرفة المطلوب بالعمليات الأربعة ، وتكثر الحاجة إلى الحسبانبإستخراج المطلوب من صلة بعض الأشياء ببعض، ولولا الحسبان لعجز الإنسان عن تسجيل أحداث الزمن، ولما وجدت التقاويم والنقود ، ومما جاء عن سراقة أن :الحساب علم قديم فوائده جمه منها ما في الميقات من أوقات الصلاة ، وحساب الأعوام والشهور والأيام وحركات الشمس في البروج والكواكب وحلول القمر في المنازل المقدرة له ومعرفة الساعات وغير ذلك ، ومنها في علم الفقه في حساب الزكاة وما يحسبه المكلف في الصيام وأعمال الحج وقسمة الغنائم والإجارة وغير ذلك مما يحتاج إليه غالب الناس ، ومنها في علم الفرائض من التأجيل والتصحيح وقسمة التركات بل أن الله تعالى قال بحق نفسه : (وهو أسرع الحاسبين) ، لذلك كان لابد لنا من الإهتمام بنظرية الأعداد لأنها تهتم بدراسة خواص وعلاقات الأعداد الصحيحة وتوسعاتها الجبرية والتحليلية ومن هذا الأساس بحثنا في نظرية الأعداد وبعض تطبيقاتها المختلفة إذا كان في مجال الأعداد الصحيحة أو في الجوانب الأخرى كالتشفير مثلا ، وبعض الدوال التي تهتم بتطبيقات الأعداد الصحيحة كقواسم الأعداد الصحيحة عددها ومجموعها وغيرها من الموضوعات ذات الصلة .

(1- 2) مشكلةالبحث :

لاتوجد بحوث أو دراسات كثيرة في مجال نظرية الأعداد وكذلك لأهمية نظرية الأعداد بصورة عامة وعلاقتها ببعض مجالات العلوم الأخرى ، وأيضا لها بعض التطبيقات المهمة في مجال التشفيرالذي يعتبر من الموضوعات المهمة في الحياة .

(1- 3) أهمية البحث :

يبين البحث نظرية الأعداد بطريقة مبسطة تساعد في تكوين خلفية علمية راسخة، وحل التطابقات بأنواعها،وتوضح التطبيقات التي تؤكد بأن نظرية الأعداد لها أهمية كبرى في الحياة العامة ،وتستخدم نظرية الأعداد في التشفير .

(1-4) أهداف البحث:

(1) توضيح المفاهيم الأساسية لنظرية الأعداد.
(2) إكتساب القدرة على تطبيق نظرية الأعداد في الحياة العملية.
(3) حل المقادير الجبرية بواسطة التطابق .
(4) إستخدام نظرية الأعداد في بعض نماذج التشفير.
(5) إيجاد العلاقة بين نظرية الأعداد وتطبيقاتها .

(1 – 5) منهج البحث :

يستخدم في البحث المنهج الوصفي التحليلي .

(1-6) مصطلحات البحث :

القاسم المشترك الأعظم :

ليكن a , b عددين صحيحين ليس كلاهما صفرا نقول ان dهو القاسم المشترك الاعظم للعددين a, b

إذا كان القاسم المشترك الأعظم يقسم العددين الصحيحين .

التطابق :

ليكن $a , b \epsilon Z$ و $n \epsilon Z^+$ نقول أن a يطابق b قياس n ونرمز لذلك بالرمز $a \equiv b(mod\ n)$ إذا كان

$n/(a-b)$ وإذا كان $n \nmid (a-b)$ فاننا نقول أن a لا تطابق b قياس n ونكتب $a \not\equiv b(mod\ n)$

دالة أويلر :

إذا كان n عدد صحيح موجب فإننا نعرف دالة أويلر بأنها عدد العناصر التي يحتويها أي نظام رواسب مختزل قياس n ونرمز لها بالرمز $\varphi(n)$.

التشفير :

التشفير هو عبارة عن سلسلة من التقنيات المستخدمة لتحويل المعلومات إلى تنسيق أخر بديل من الممكن إرجاعها فيما بعد إلى صورتها الأصلية . ويقصد بهذا التنسيق البديل بمصطلح نص الشفرة ويتم إنشاؤه عادة من خلال إستخدام خوارزمية الشفرة ومفتاح الشفرة , وتمثل خوارزمية الشفرة بواسطة معادلة رياضية تنطبق على المعلومات المراد تشفيرها .

(1-2)المفـاهيم الأساسـية:

(1-1-2)نظرية الأعداد:

تعريف:

هي دراسة الرياضيات المتعلقة بالأعداد الصحيحة وخواصها .

(2-1-2) الأعداد الصحيحة :

تعريف :

هي مجموعة الأعداد الصحيحة الموجبة ومجموعة الأعداد الصحيحة السالبة والصفر ويرمز لها بالرمز Zحيث :

$$Z = \{0, \pm1, \pm2, \pm3, \dots\} \text{ أو } Z = \{\dots, -2, -1, 0, 1, 2, \dots\}$$

(3-1-2)خواص الأعداد الصحيحة :

يمكن بناء الأعداد الصحيحة $Z = \{0, \pm1, \pm2, \pm3, \dots\}$ من مجموعة الأعداد الطبيعية $N = \{1,2,3,4, \dots\}$ ثم نستنتج منها خواصا اخرى أساسية :

إذا كان $a, b, c \in Z$ فإن :

1) $a + b = b + a , a \cdot b = b \cdot a$

أي أن جمع وضرب الأعداد الصحيحة إبدالي

2) $(a + b) + c = a + (b + c) , (a \cdot b) \cdot c = a \cdot (b \cdot c)$

أي أن جمع وضرب الأعداد الصحيحة تجميعي

3) $a + 0 = 0 + a = a , a \cdot 1 = 1 \cdot a = a$

4) $\forall a \in Z \; \exists -a \in Z \text{ st} : a + (-a) = (-a) + a = 0$

5) $(a + b)\cdot c = a\cdot c + b\cdot c \ , \quad a\cdot(b + c) = a\cdot b + a\cdot c$

أي أن الضرب توزيعي على الجمع .

6) إذا كان : $a + b = a + c$ فإن: $b = c$

7) لكل $a , b \in N$ نجد ان $a + b \in N \ , \quad a\cdot b \in N$

مبرهنة (1) :

إذا كان : $a , b \in Z$ فإن :

أ- $a\cdot 0 = 0\cdot a = 0$

ب-$(-a)\cdot b = a\cdot(-b) = -(ab)$

ج- $-(-a) = a$

د- $(-a)(-b) = ab$

البرهان:

وبما أن:$0 = (0 + 0)$ إذن $a(0 + 0) = a.0$ وعليه فإن $a.0 + a.0 = a.0$

لكن $a\cdot 0 = a\cdot 0 + 0$ اذن : $a\cdot 0 + a\cdot 0 = a\cdot 0 + 0$ وعلية فإن $a.0 = 0$ حسب الخاصية (6) لكن $a\cdot 0 = 0\cdot a$حسب الخاصية(1) اذا $a\cdot 0 = 0\cdot a = 0$

ب) بما أن $(-a)\cdot b = (-a)\cdot b + 0$ حسب الخاصية (3) وبما أن $ab + 0 = -((ab))$حسب الخاصية (4) إذا باستخدام الخواص (2) و (3) و (5) نجد أن :

$(-a)\cdot b = ($

$[(-a) + a]b$

وبنفس الطريقة يمكن أن نبرهن على أن : $a(-b) = -(ab)$ إذا :

ج) بما أن : $0 + (-a) = -(-a)$ و $-(-a) + (a) = 0$إذاً :

$-(-a) = -($

د) $(-a)(-b) = -[-(a(-b)] = -(-(ab)) = ab$

وذلك حسب (ب)،(ج)

تعريف:

اذا كان : $Z^+ = \{1,2,3, \dots\} = N - \{0\} = N^*$ وكان : $a, b \in Z$ فيقال عن:

أ) a أنها أصغر من b أو أن bأكبر من a ونكتب $a < b$ إذا كان :$b - a \in N^*$

ب) a أنهاأصغر من أو تساوي b أو ان b أكبر من أو تساوي a ونكتب $a \leq b$إذا كان $b - a \in N$

مبرهنة (2) :

أ) إذا كان : $a, b, c \in Z$ وكان : $b < c$ و $a < b$ فإن : $a < c$.

ب) إذا كان : $a, b, c \in Z$ وكان $a < b$ و $c > 0$ فإن $ac < bc$.

ج) إذا كان : $a, b \in Z$ فواحدة فقط من هذه العبارات صحيحة : إما $a < b$ او $a = b$.

البرهان:

أ) بما أن $b - a \in N^* \Leftrightarrow a < b$ و $b < c \Leftrightarrow c - b \in N^*$إذا

$(c - b) + (b - a) \in N^*$ وعليه فان : $c - a \in N^*$ ومنه ينتج أن : $a < c$

ب) بما أن : $a < b \Leftrightarrow b - a \in N^*$ وبما أن : $c \in N^*$ إذن :

$(b - a)c = bc - ac \in N^*$ وعليه فإن : $ac < bc$.

ج) نفرض أن : $a < b$ و $a = b$ إذا : $b < b$ وهذا تناقض وإذا كان : $a > b$ و$a = b$ فإن : $b > b$وهذا تناقض أيضا .أما إذا كان :

$a < b$ و $a > b$ فإن : $a < a$ حسب (أ) وهذا تناقض أيضا : إذن واحدة فقط من العبارات أعلاه صحيحة

تعريف:

إذا كان : $a \in Z$ فيقالعن |a|أنها القيمة المطلقة للعدد a إذا كان :

$$|a| = \begin{cases} a & \forall\, a \geq 0 \\ -a & \forall\, a < 0 \end{cases}$$

مبرهنة(3)

إذا كان $a, b \in Z$ فإن

أ) $|a| \geq 0$

ب) $|a| = 0 \Leftrightarrow a = 0$

ج) $-|a| \leq a \leq |a|$

د) $|-a| = |a|$

ه) $|ab| = |a|\,|b|$

و) $|a| \leq b \Leftrightarrow -b \leq a \leq b$

ز) $|a+b| \leq |a| + |b|$

ح) $|a-b| \geq |a| - |b|$

البرهان :

أ) إذا كان :$a \geq 0$ فإن : $|a| = a \geq 0$ و إذا كان : $a < 0$ فإن : $|a| = -a > 0$ إذن $|a| \geq 0$: .

ج) نفرض أن : $a \geq 0$ اذن $|a| = a$ وعليه فإن : $|a| \geq 0$ ومنه ينتج أن : $-|a| \leq 0$ اذن :

$-|a| \leq 0 \leq a = |a|$ وعليه فإن : $-|a| \leq a \leq |a|$

أما إذا كان : $a < 0$ فإن : $-a < 0$ وعليه فإن : $|a| = -a > 0$ ومنه ينتج أن :

$-|a| < 0$ إذن : $-|a| = a < 0 < -a = |a|$ وعليه فإن : $-|a| \leq a \leq |a|$

ه) إذا كان : $a, b \geq 0$ فإن : $ab \geq 0$ وعليه فإن : $|a| = a\,,\ |b| = b$ ومنه ينتج أن :

$|ab| = ab = |a||b|$ وإذا كان: $a \geq 0\,, b < 0$ فإن : $ab < 0$ وعليه فإن :

$|a| = a\,, |b| = -b$ إذن : $|ab| = a(-b) = |a||b|$ وإذا كان : $a < 0\,, b \geq 0$

فإن : $ab < 0$ و $|b| = b$ و $|a| = -a$ وعليه فإن : $|ab| = -(ab) = (-a)b = |a||b|$

وإذا كان :$a, b < 0$ فإن : $|b| = -b$ و $|a| = -a$ وعليه فإن : $|ab| = ab$ ومنه يبتج أن :

$$|ab| = |a||b|$$

ز) بما أن :$-|a| \leq a \leq |a|$ and $-|b| \leq b \leq |b|$ حسب (ج) إذن :

$-(|a| + |b|) \leq a + b \leq |a| + |b|$ وحيث أن : $a, b \in Z$ إذا إما :

$a + b \geq 0$ أو $a + b < 0$ فاذا كان $a + b \geq 0$ فإن $|a + b| = a + b$

وعليه فإن $|a + b| \leq |a| + |b|$ أما إذا كان $a + b < 0$

فإن $|a + b| = -(a + b)$ لكن $a + b \leq -(|a| + |b|)$ إذن

وعليه فإن $|a + b| \leq |a| + |b|$ $-(a + b) \geq |a| + |b|$

(2-2) علاقة الترتيب الجزئي:

تعريف:

يقال عن علاقة $\preccurlyeq$ على مجموعة غير خالية A انها علاقة ترتيب جزئي اذا كانت :

أ) $\preccurlyeq$ علاقة منعكسة (Reflexive) على A أي أن : $a \preccurlyeq a$ لكل $a \in A$

ب) $\preccurlyeq$ علاقة متعدية (Transitive) على A أي أنه اذا كان : $b \preccurlyeq c$ و $a \preccurlyeq b$ فان: $a \preccurlyeq c$.

ج) $\preccurlyeq$ علاقة متخالفة او تخالفية (Ant symmetric) على A أي أنه اذا كان : $a \preccurlyeq b$ و $b \preccurlyeq a$ فان : $a = b$.

ويقالعن $(A, \preccurlyeq)$ انها مجموعة مرتبة ترتيبا جزئيا (Partially ordered set) اذا كانت: $A \neq \emptyset$ و $\preccurlyeq$ علاقة ترتيب جزئي على A .

مثال (1):

أ) اذا كان : $A \in \{N, Z, Q, R\}$ وكان : $a \leq b \Leftrightarrow a \preccurlyeq b$ فان : $(A, \preccurlyeq)$ مجموعة مرتبة تريبا جزئيا .

ب) اذا كان : $X \neq \emptyset$ فان : $(p(x), \subseteq)$)مجموعة مرتبة ترتيبا جزئيا لان : $p(x) \neq \emptyset$ و $\subseteq$علاقة ترتيب جزئي على $p(x)$

ج) اذا كانت : $A = \{1,2,3,4\}$

$\preccurlyeq = \{(1,1$

فان $\preccurlyeq$علاقة ترتيب جزئي على A

د) اذا كانت :$\preccurlyeq$معرفه على N^* كالاتي : $a \preccurlyeq b \iff b \mid a$ فان :$\preccurlyeq$ علاقة ترتيب جزئي على N^* وعليه فإن $(N^*, \preccurlyeq)$ مجموعة مرتبة جزئيا .

تعريف:

إذا كانت $(A, \preccurlyeq)$ مجموعة مرتبة جزئيا فيقال عن $a \in A$ أنه عنصر أول أو أصغر عنصر للمجموعهA ونكتب $l(A) = a$ اذا كان : $a \preccurlyeq x$ لكل: $x \in A$

مثال (2) :

ا) $(N, \leq)$مجموعه مرتبة جزئيا . $l(N) = 0$

ب) اذا كانت : $X \neq \emptyset$ فان : $(p(x), \subseteq)$ مجموعه مرتبة جزئيا

$l(p(x)) = \emptyset$ الان: $\emptyset \subseteq A$ لكل $A \in P(x)$.

ج) إذا كانت $A = \{ x \in R \mid 0 < x < 1 \}$ فان : $(A, \leq)$مجموعة مرتبة جزئيا ولكنها لا تملك عنصر أول .

د) إذا كانت : $A = \{2,4,6\}$ وكانت $\preccurlyeq$معرفة على Aكالأتي :$a \preccurlyeq b \iff a \mid b$, $a, b \in A$

أذن : $(A, \leq)$مجموعة مرتبةٍ ترتيباً جزئيٍّ . و $l(A) = 2$

(3-2) قاعدة الترتيب الحسن (Well – Ordering Principle):

إذا كان S مجموعة غير خالية من الأعداد الصحيحة السالبة فانه يوجد عنصر أصغر في Sأي يوجد عنصر

$s_0 \in S$ بحيث : $s_0 < S$ ولكل $s \in S$ ويكون s_0 وحيد .

تعريف :

يقال عن مجموعة مرتبة جزئيا $(A, \preccurlyeq)$ أنها مجموعة مرتبة ترتيبا حسنا , إذا كانت كل مجموعة جزئية من A غير خالية تحوي عنصراً أولاً .

مثال (3) :

ا) إذا كانت : $A = \{1,2,3,4\}$ فان : $(A, \leq)$ مجموعة مرتبة حسناً لان : $(A, \leq)$ مجموعة مرتبة جزئياً وكل مجموعة جزئية من A تحوي عنصر أول .

ب) اذا كانت : $A = [0,1]$ فان : A مجموعه ليست مرتبه ترتيباً حسناً لأن : $B =]0,1] \subset$ A لاتحوي عنصر أول .

ج) $(Z, \leq)$ مجموعة ليست مرتبة ترتيباً حسناً , لان : $\{\ldots, -3, -2, -1\}$ مجموعة جزئية منها لا تحوي على عنصر أول (عنصر أصغر)

مبرهنة (4) :

أ) لايوجد عدد صحيح بين الصفر والواحد.

ب) الواحد أصغر عدد موجب .

ج) اذا كان : $n \in Z$ فلا يوجد $m \in Z$ بحيث أن : $n < m < n + 1$.

البرهان :

أ) نفرض وجود : $x \in N$ بحيث ان : $0 < x < 1$ اذا :

$S = \{m \in N \mid 0 < m < 1\} \neq \emptyset$ لكن : N مرتبة حسناً

$\emptyset \neq S \subseteq N$ اذا : S تمتلك عنصر أول (أصغر) وليكن n إذاً : $0 < n < 1$ وعليه فإن :

$0 < n^2 < n < 1$ وهذا يعنيأن : $n^2 \in S$ و $n^2 < n$ وهذا يناقض كون أن : n عنصر أول في S

إذا : $S = \emptyset$.

ب) بما ان : $S = \{m \in N \mid 0 < m < 1\} = \emptyset$ حسب (أ) , إذاً الواحد هو أصغر عدد صحيح موجب

ج) نفرض أن : $m \in Z$ بحيث ان : $n < m < n + 1$ إذاً : $0 < (m - n) < 1$ وهذا يناقض (أ) . إذاً لا يوجد $m \in Z$ بحيث ان : $n < m < n + 1$.

(4-2) مبدأ الاستقراء الرياضيThe principle of mathematical induction:

كما هو معلوم يتم مبدأ الاستقراء الرياضي وفق خطوات :

لنفرض ان : $p(n)$ عبارة ما حيث : $n \in Z^+$ ولنفرض ان q عدد صحيح موجب معطى لاثبات ان $p(n)$

عبارة صحيحة $\forall n \geq q$ يكفي ان نثبت ما يلي :

1) $p(n)$عبارة صحيحة .

2)إذا كان:$m \geq q$ وكانت $p(m)$ صحيحة فان $p(m+1)$ عبارة صحيحة

مبرهنة (5):

العبارات الاتية متكافئة :

أ) قاعدة الأستقراء الرياضي:إذا كانت B مجموعة جزئية من N^* وكان : $1 \in B$ و$\Longrightarrow$ $n \in B$) $n + 1 \in B$) فان : $B = N^*$.

ب) القاعدة العامة للاستقراء الرياضي :

اذا كانت : B مجموعة جزئية من N^* وكان : $1 \in B$ و $n \in B$ عندما : $n \in B$ لكل n > m فان $B = N^*$.

ج) لكل مجموعة جزئية غير خالية من N^* عنصر اول (اصغر) .

البرهان :

سنثبت أن (أ) $\Longleftarrow$ (ب) $\Leftarrow$ (ج) $\Leftarrow$ (أ) :

أ) $\Leftarrow$ (ب) لتكن : $B \subseteq N$ بحيث أن $1 \in B$ و$n \in B$ عندما $n \in B$ لكل : n > m ولنفرض أن :

$E = \{ x \in N \mid y \in B \; \forall y \leq x \}$ إذن : $E \subseteq B$ وعليه يتم إثبات المطلوب وهو أن : $E = N^*$

ولإثبات ذلك لاحظ أن : $1 \in E$ لأن : $1 \in B$ وإذا كان : $n \in E$ فإن: $y \in B$ لكل $y \leq n$

إذا: $(n + 1) \in B$

وعليه فإن : $y \in B$ لكل : $y \leq n + 1$ و هذا يعني أن : $n + 1 \in E$ اذا $E = N^*$ حسب (أ)

(ب) ⇐ (ج) لتكن : B مجموعة جزئية من N^* و B لا تمتلك عنصر أول .اذاً :

$1 \notin B$ وعليه فإن : $1 \in N^* - B$ إذا كانت : $m \in N^* - B$ لكل $m < n$ فإن :

$n \in N^* - B$ لأنه إذا كان العكس فإن :n هي العنصر الأول للمجموعة B وهذا يناقض الفرض .

واذاً :$B = \emptyset$ حسب (ب) . ومنه ينتج أن : $B = N^* - N^*$

اذاً : لكل مجموعة جزئية غير خالية من N^*عنصر أول.

ج)⇐ (أ) لتكن Bمجموعة جزئية من N^*بحيث ان :$1 \in B$و$(n \in B \Longrightarrow n + 1 \in B)$

ولتكن: $B` = N^* - B$

إذا كانت : $B` \neq \emptyset$ فإن : B`تمتلك عنصر أول وليكن : m ,اذاً $m \neq 1$ لأن :$1 \in B$

وعليه فإن : $m > 1$ لكن :$m - 1 < m$ اذاً : $(m - 1) \notin B'$ وعليه فإن : $(m - 1) \in$ B وبالتالي

فإن : $m = (m - 1) + 1 \in B$ إذا :$m \notin B`$ وهذا تناقض .اذاً : $B` = \emptyset$ وعليه فان $B = N^*$:

ملاحظة :

لإثبات صحة العبارة P(n)لجميع قيم : $n \in N^*$يكفي أن نبرهن على أن :P(1) عبارة صحيحة ونثبت أن صحة العبارة P(m) يؤدي الى صحة العبارة P(m + 1) لأنه إذا كانت :

$$S = \{n \in N^* : p(n) \text{ عبارة صحيحة}\}$$

فإن :$1 \in S$ كما أنه إذا كانت :$m \in S$ فإن :$m + 1 \in S$ وعليه فإن : $S = N^*$

مثال(4) :

أثبت أن:

$$\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}$$

الإثبات :

1)نفرض أن :$p(n) = \sum_{i=1}^{n} i^2 = \frac{(n+1)(2n+1)}{6}$

إذن عندما :$n = 1$ نجد أن الطرف الأيمن يساوي :

$1 = \frac{(1)(2)(3)}{6}$والطرف الايسريساوي : $1 = 1^2$أيضا وعليه فإن : $p(1)$ عبارة صحيحة .

2) $p(m)$عبارة صحيحة . فنجد أن :

$$p(m) = \sum_{i=1}^{m} i^2 = \frac{m(m+1)(2m+1)}{6}$$

3) ولإثبات صحة العبارة $p(m+1)$ نجد أن:

$p(m+1)$

وعليه فإن :

$$\sum_{i=1}^{m-1} i^2 = \frac{(m+1)[m(2m+1)+6(m+1)]}{6} = \frac{(m+1)(2m^2+7m+6)}{6}$$

$$= \frac{(m+1)(m+2)(2m+3)}{6}$$

$$= \frac{(m+1)[(m+1)+1][2(m+1)+1]}{6}$$

إذن $p(m+1)$ عبارة صحيحة وعليه فإن $p(n)$ عبارة صحيحة لجميع قيم n الصحيحة الموجبة

مثال (5) :

أثبت أن : $a + (a+r) + (a+2r) + \cdots + [a + (n-1)r] = \frac{n}{2}[2a + (n-1)r]$

لاحظ أن الطرف الأيسر يمثل متتابعة عددية حدها الأول a وأساسها r وعدد حدودها n

الإثبات :

لتكن : $P(n): a + (a+r) + (a+2r) + \cdots + [a + (n-1)r] = \frac{n}{2}[2a + (n-1)r]$

فإذا كان : $n = 1$ فإن : $R.H.S = a$ و $L.H.S = a$ وعليه فإن : $P(1)$ صحيحة .

لنفرض أن : $P(m)$ صحيحة . إذن :

$$a + (a+r) + (a+2r) + \cdots + [a + (m-1)r] = \frac{m}{2}[2a + (m-1)r]$$

وعليه فإن :

$$a + (a +$$

$$= \frac{m}{2}[2a + (m-1)r] + (a + mr)$$

$$a + (a + r) + (a + 2r) + \cdots + (a + mr)$$

$$= (m + 1)a + \frac{[m(m-1) + 2m] \cdot r}{2}$$

$$= (m + 1)a + \frac{m(m+1)r}{2} = \frac{m+1}{2}(2a + mr)$$

وعليه فإن : $P(m + 1)$صحيحة إذا $P(n)$ صحيحة لكل $n \in N^*$

مثال(6):

إذا كان : $ab = ba$ فإن : $(a + b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k}b^k$ لكل $n \in N^*$حيث

$\binom{n}{k} = \frac{n!}{k!(n-k)!}$يسمى هذا القانون " مبرهنة ذي الحدين ".

الإثبات :

لتكن :

إذا كانت $n = 1$ فإن

$$R.H.S = \sum_{k=0}^{1} \binom{1}{k} a^{1-k}b^k = \binom{1}{0}a + \binom{1}{1}b = a + b \ , \qquad L.H.S = a + b$$

وعليه فإن $p(1)$ صحيحة

والأن نفرض أن $p(m)$إذن:$(a + b)^m = \sum_{k=0}^{m} \binom{m}{k} a^{m-k}b^k$وعليه فإن :

$$(a+b)^{m+1} = \sum_{k=0}^{m} \binom{m}{k} a^{m-k}b^{k}(a+b)$$

$$=\left[\binom{m}{0}a^{m} + \binom{m}{1}a^{m-1}b + \binom{m}{2}a^{m-2}b^{2} + \cdots + \binom{m}{m}b^{m}\right](a+b)$$

$$=\binom{m}{0}a^{m+1} + \left[\binom{m}{0} + \binom{m}{1}\right]a^{m}b + \cdots + \left[\binom{m}{i} + \binom{m}{i-1}\right]a^{m+1-i}b^{i} + \cdots + \binom{m}{m}b^{m+1}$$

لكن $\binom{m}{k} + \binom{m}{k-1} = \binom{m+1}{k}$ اذن

$$(a+b)^{m+1} = \binom{m+1}{0}a^{m+1} + \cdots + \binom{m+1}{i}a^{m+1-i}b^{i} + \ldots + \binom{m+1}{m+1}b^{m+1}$$

$$= \sum_{k=0}^{m+1} \binom{m+1}{k} a^{(m+1)-k}b^{k}$$

إذن $P(m+1)$صحيحة وعليه فإن $P(n)$صحيحة لكل $n \in N^{*}$

(5-2) قابلية القسمة(Divisibility) :

تعريف:

يكون العدد الصحيح a حيث$a \neq 0$قاسماً للعدد الصحيح b ونكتب $a \mid b$ إذا وفقط إذا وجد عدد صحيح c يحقق المساواة $b = ca$ كما نقول أن : aعامل من عوامل b أو bقابل للقسمة علىa أو أن bمن مضاعفات aواذا كان : aلايقسم bنكتب :$a \nmid b$. وعلى سبيل المثال :

$3 \mid 15$ $\quad 4 \nmid 10$ $\quad 7 \mid 28$

$3 \mid 15$ لان : $15 = 5 \times 3$ و $7 \mid 28$ لان : $28 = 4 \times 7$

(6-5-2) الخواص الاساسية لقابلية القسمة :

لتكن $a , b, c \in Z$

(1) $1 \mid a$

(2) إذا كان $a \mid b$ فإن : $a \mid bc$.

(3) إذا كان : $a \mid b$ و $b \mid c$ فإن : $a \mid c$.

(4) $a \mid 0$

(5) إذا كان : $a \mid b$ فإن :$|a| \mid |b|$.

(6) إذا كان : $a \mid b$ و $b \mid a$ فان : $a = \pm b$.

(7) إذا كان $a \mid b$ و $a \mid c$ فإن : $a \mid (bx + cy)$ لجميع الأعداد الصحيحة x , y .

(8) إذا كان :$a > 0$ و $b > 0$ وكان : $a \mid b$فإن : $a \leq b$

البرهان :

(1) $a = 1 \cdot a \implies 1 \mid a$

(2) لنفرض ان : $a \mid b$ لاحظ ان : $a \mid a$ من (1) نستنتج ان : $a \mid (ax + by)$ لجميع قيم x, y ونضع $x = 0$ و $y = c$نحصل على $a \mid bc$.

(3) بمان ان : $a \mid b$ و $b \mid c$فإنه يوجد عددان صحيحان s, t بحيث يكون : $b = as$ و $c = bt$ وعليه فإن : $c = ast$ ومنه نجد أن : $a \mid c$.

(4) $0 = a \cdot 0 \implies a \mid 0$

(5) بما أن $a \mid b$ فإن $b = ac$ حيث $c \in Z$ بأخذ القيمة المطلقة للطرفين نحصل علي:

$$|b| = |a||c| \text{ ومنه } |a| \mid |b|$$

(6) بما أن : $a \mid b$ و $b \mid a$فإن : $|a| \mid |b|$ وكذلك : $|b| \mid |a|$وبإستخدام (5) نجد أن :$|a| \leq |b|$ و $|b| \leq |a|$ وهذا يعني أن : $|a| = |b|$ وبالتالي فإن$a = \pm b$.

(7) لما كان $a \mid b$ و $a \mid c$فإنه يوجد عددان صحيحان s, tبحيث أن : $b = as$ و $c = at$ وعليه فان :

$$b x + c y = asx + aty = a (sx + ty)$$

ومنه نجد ان : $a \mid (bx + cy)$.

(8) لما كان : $a \mid b$ فان : $b = ac$ حيث : $c \in Z$ وبما ان : $a > 0$ و $b > 0$ فان :

$c > 0$ ومنه نجد أن $c \geq 1$: لأن c عدد صحيح موجب . وبالتالي فان :

$$b = ac \geq a .$$

(7-2) خوارزمية القسمة:

مبرهنة(6):

ليكن : a , b عددان صحيحان $b > 0$ عند ذلك يوجد عددان صحيحان وحيدان r , q بحيث يتحق التالي :

$b = q a + r$ حيث : $0 \leq r \leq a$

البرهان :

اولاً لنبرهن وجود العددين r, q إعتبر المجموعة $S = \{|x \geq 0 : x = b - ta , t \in Z\}$ هذه المجموعة غير خالية لأن :

$b - ta \geq 0$ إذا وفقط اذا كان $t \leq \frac{b}{a}$

من مبدأ الترتيب الحسن يوجد عنصر أصغر في S وليكن r لتكن قيمة t المقابلة للعدد r هي q أذن نحصل على $r = b - qa$ اي ان $b = qa + r$ لاحظ ان $r \geq o$ بقي ان نبين $r < a$ لنفرض ان $r \geq a$ إذن

$r - a \in S$ وهذا يجعل $0 \leq r - a = b - qa - a = b - (q + 1)a$ ولكن $r - a < r$ مما يناقض كون أن r عنصر أصغر في S إذن $r < a$.

لنبرهن الأن على وحدانية العددين r, q:

ولنفرض ان $b = qa + r$ حيث $0 \leq r < a$ وان $b = \grave{q}a + r`$

حيث $0 \leq r` < a$ وبطرح المعادلتين أعلاه نحصل على $r` - r = (q - q`)a$ وبجمع المتباينتين التاليتين

$0 \leq r` < a , \ -a < -r \leq 0$ والقسمة على العدد a نحصل على $-1 < \frac{\grave{r}-r}{a} < 1$

وبما ان $q - q` = \frac{r` - r}{a}$ فإننا نستنتج ان $q - q` = 0$ أي ان $q = q`$ وكذلك $r = r`$ وفي هذه المبرهنة يسمى العدد q بخارج القسمة b على a والعدد r بباقي القسمة .

مثال (7):

لنبرهن ان أي عدد صحيح فردي يمكن كتابته على الصورة $4k + 3$ او $4k + 3$ حيث $k \in Z$

باخذ $a = 4$ وبإستخدام خوارزمية القسمة نستطيع كتابة اي عدد صحيح b على الصورة $4k +$ r حيث $r = 0,1,2,3$ ومنه نجد أن أي عدد فردى يكتب على الصورة $4k + 1$ او $4k + 3$ لان $4k + 2$ و $4k$ عددان زوجيان .

(8-2) تمثيل الأعداد الصحيحة :

المبرهنة التالية تطبيق لخوارزمية القسمة

مبرهنة (7) :

إذا كان k عددا صحيحا أكبر من الواحد فإننا نستطيع كتابةأي عدد صحيح موجب N بطريقة وحيدة على الصورة

$N = a_m k^m + a_{m-1} k^{m-1} + \cdots + a_2 k^2 + a_1 k + a_0$ علما بان : المعاملات a_t تاخذ قيما صحيحة بين العددين 0 و $k - 1$ و $a_m \neq 0$

البرهان:

باستخدام خوارزمية القسمة نستطيع ايجاد عددين صحيحين q_1 و a_0 يحققان العلاقة :

$$N = q_1 k + a_0 \quad \text{حيث} \quad 0 \leq a_0 < k$$

اذا كان : $q_1 \geq k$ فاننا نستخدم خوارزمية القسمة مرة اخرى لنحصل على عددين صحيحين a_1 و q_2 يحققان العلاقة : $q_1 = q_2 k + a_1 , \; 0 \leq a_1 < k$

وبالتعويض عن قيمة q_1 في المعادلة الأولى نحصل على

$$N = (q_2 k + a_1)k + a_0 = q_2k^2 + a_1 k + a_0$$

وبالطريقة نفسها نحصل على في المرحلة m على q_m و a_{m-1} بحيث يكون

$q_{m-1} = q_m k + a_{m-1}$, $0 \le a_{m-1} < k$ وبما ان : $q_1 > q_2 > \cdots > 0$ متتالية متناقصة نحصل على المرحلة التي يكون فيها $q_m < k$ عندئذ نتوقف ونجعل على $a_m = q_m$ وبذلك نحصل على المساواة :

$$N = a_m k^m + a_{m-1}k^{m-1} + \cdots + a_2k^2 + a_1k + a_0$$

وللبرهان على وحدانية التمثيل نفرض ان:

$$N = a_m k^m + a_{m-1}k^{m-1} + \cdots + a_2k^2 + a_1k + a_0$$

$$= b_n k^n + b_{n-1}k^{n-1} + .. + a_1k + b_0$$

لنفرض ان: $m \ge n$ وبإضافة معاملات صفرية في التمثيل الثاني يمكن ان نفرض ان : $m = n$ وبالطرح نحصل على :

$$(a_m - b_m)k^m + (a_{m-1} - b_{m-1})k^{m-1} + \cdots + (a_1 - b_1)k + (a_0 - b_0) = 0 \rightarrow (1)$$

وبفرض ان التمثيلين مختلفين فهذا يعني ان احد المعاملات اعلاه لا يساوي الصفر .

ليكن $a_i - b_i$ أول معامل غير صفري في العلاقة السابقة (1) وبحذف الحدود التي معاملاتها أصفار ونقل الحد $(a_i - b_i)k^i$ الى الطرف الأيمن في العلاقة (1) نحصل على المساواة :

$$(a_m - b_m)k^m + (a_{m-1} - b_{m-1})k^{m-1} + \cdots + (a_{i+1} - b_{i+1})k^{i+1} = -(a_i - b_i)k^i$$

وبالقسمة على k^i وباخذ k عامل مشترك من الطرف الأيسر :

$$k\left[(a_m - b_m)k^{m-i-1} + (a_{m-1} - b_{m-1})k^{m-i-2} + \cdots + (a_{i+1} - b_{i+1})\right] = -(a_i - b_i) \rightarrow (2)$$

ومن العلاقة (2) نحصل على $k \mid -(a_i - b_i)$ اي ان : $k \mid |a_i - b_i|$ ومنه نجد ان :

$|a_i - b_i| \geq k$ ولكن: $0 \leq a_i \leq k-1$ و $0 \leq b_i \leq k-1$ ومنه نجد

$|a_i - b_i| \leq k-1$ وهذا تناقض وبالتالي فلابد أن يكون التمثيلان متساويان .

مثال (8) :

أكتب العدد 37 للأساس $k = 2$

الحل :

$37 = 2(18) + 1 \qquad q_1 = 18 > k$

$18 = 2(9) + 0 \qquad q_2 = 9 > k$

$9 = 2(4) + 1 \qquad q_3 = 4 > k$

$4 = 2(2) + 0 \qquad q_4 = 2 \geq k$

$2 = 2(1) + 0 \qquad q_5 = 1 < k$

نضع $q_5 = a_5$ نحصل على التمثيل

$$37 = 1(2^5) + 0(2^4) + 0(2^3) + 1(2^2) + 0(2^1) + 1(2^0) = (100101)$$

مثال (9) :

أكتب العدد 61469 للأساس $k = 16$

الحل :

$61469 = 16(3841) + 13 \qquad q_1 = 3841 > K$

$3841 = 16(240) + 1 \qquad q_2 = 240 > K$

$240 = 16(15) + 0 \qquad q_3 = 15 < K$

نضع $q_3 = a_3$ فنحصل على التمثيل :

$$61469 = 15 \times (16^3) + 0 \times (16^2) + 1 \times (16^1) + 13 \times (16^0)$$

$$= F \times (16^3) + 0 \times (16^2) + 1 \times (16^1) + D \times 16^0$$

$$= (F01D)_{16}$$

حيث انه في النظام الستة عشري تدل الحروف A, B, C, D, E على الاعداد :

$10, 11, 12, 13, 14, 15$ على الترتيب .

(9-2) القاسم المشترك الأعظم :(Greatest Common Divisor):

تعريف:

ليكن a, b عددين صحيحين ليس كلاهما صفرا نقول ان d هو القاسم المشترك الاعظم للعددين

a, b ونرمز لذلك بالرمز $d = (a, b)$ إذا وفقط اذا كان :

1) $d > 0$
2) $d \mid b \wedge d \mid a$
3) اذا كان : $c \mid a \wedge c \mid b c > 0$ فان : $c \leq d$

مثلا :

$$(5, 15) = 5 \quad , \quad (6, 9) = 3 \quad , \quad (-3, -9) = 3 \quad , \quad (27, 41) = 1$$

مبرهنة (8) :

إذا كان : a, b عددين صحيحين ليس كلاهما صفراً فإنه يوجد عددان : x_0, y_0 بحيث

$(a, b) = a x_0 + b y_0$ وهذه العباره تسمى تركيبا خطياً من a, b .

البرهان :

نعرف المجموعة التالية $S = \{ax + by : ax + by > 0, x, y \in Z\}$ بما ان : a, b ليس كلاهما صفراً فلنفرض أن : $a \neq 0$ إذا كان : $a > 0$ فان : $a \in S$ لأن

$$a = a \times 1 + b \times 0$$

اما اذا كان : $a < 0$, $-a > 0$فان $-a = a \times (-1) + b \times (0)$

اي ان : $-a \in S$ ومنه نستطيع أن نستنتج أن S غير خالية حسب مبدأ الترتيب الحسن يوجد عنصر أصغر موجب d ومن تعريف S يوجد عددان صحيحان x_0, y_0 بحيث ان

ندعي أن: $d = (a, b)$ $d = a x_0 + b y_0$

إذا كان $d \mid a$ فهذا هو المطلوب ولكن قد يكون $d \nmid a$ من خوارزمية القسمة يوجد عددان وحيدان r, q بحيث:

$0 < r < d$, $a = dq + r$ لان

$$r = a - dq = a - (a x_0 + b y_0)q = a(1 - x_0 q) + b(-y_0 q)$$

أي أن $r \in S$ ولكن $r < d$ وهذا تناقض اذا لا بد من ان $d \mid a$ وبالطريقة نفسها نبرهن علي أن $d \mid b$ واخيرا اذا كان $c \mid a$ و $c \mid b$ واستنادا للخواص نعلم أن:

$c \mid (a x_0 + b y_0)$ أي أن : $c \mid d$ وإستنادا الى الخواص نجدأن : $c \leq d$ وبالتالي فإن d هو القاسم المشترك الأعظم

(10-2) خوارزمية إقليدس (Euclidean Algorithm):

ليكن $0 < a \geq b$ عددين صحيحين من خوارزمية القسمة

$$\begin{aligned}
b &= aq_1 + r_1 && , && 0 < r_1 < a \\
a &= r_1 q_2 + r_2 && , && 0 < r_2 < r_1 \\
r_1 &= r_2 q_3 + r_3 && , && 0 < r_3 < r_2 \\
&\vdots && && \vdots \\
r_{n-2} &= r_{n-1} q_n + r_n && , && 0 < r_n < r_{n-1} \\
r_{n-1} &= r_n q_{n+1} + 0 && , && r_{n+1} = 0
\end{aligned}$$

عندئذ $(a, b) = r_n$ حيث أن r_n هي القاسم المشترك الأعظم .

البرهان :

من الخوارزمية الموصوفة بالنص نلاحظ ان

$$a > r_1 > r_2 > r_3 > \cdots > r_n > r_{n+1}$$

ولما كانت الاعداد r_i صحيحة فلا بد من وجود n بحيث $r_{n+1} = 0$

$$\Longrightarrow (b, a) = (a_1, r_1) = (r_1 , r_2) = \cdots = (r_n , r_{n+1}) = (r_n, 0) = r_n$$

ملاحظة :

علاوة على إيجاد القاسم المشترك الأعظم للعددين a, b فإن خوارزمية إقليدس تستخدم أيضا لإيجاد x, y المرتبطين بالمساواة $(a, b) = ax + by$ ويتم ذلك كما يلي :

بما ان $d = r_n$ فان

$$d = r_{n-2} - q_n r_{n-1}$$
$$= r_{n-2} - q_n(r_{n-3} - q_{n-1} r_{n-2})$$
$$= r_{n-2}(1 + q_n q_{n-1}) - r_{n-3} q_n$$

وبالتعويض عن r_{n-2} بالقيمة $r_{n-4} - q_{n-2} r_{n-3}$ بالاستمرار الخطوات على المنوالنفسه نحصل في النهاية على x, y بحيث يكون :

$$d = ax + by$$

مثال (10) :

اوجد القاسم المشترك الاعظم (a, b) اذا كان :

$$a = 42 \ , \quad b = 30 \qquad (1)$$
$$a = 90 \ , \quad b = 52 \qquad (2)$$

الحل : (1) من خوارزمية اقليدس :

$$a = bq + r$$

$$42 = 30(1) + 12$$

$$30 = 12(2) + 6$$

$$12 = 6(2) + 0$$

$$(42,30) = 6$$

$$a = 90 \qquad b = 52 \qquad (1)$$

$$90 = 52(1) + 38$$

$$52 = 38(1) + 14$$

$$38 = 14(2) + 10$$

$$14 = 10(1) + 4$$

$$10 = 4(2) + 2$$

$$4 = 2(2) + 0$$

$$d = 2 \implies (90,52) = 2$$

مثال(11) :

اوجد القاسم المشترك الاعظم (a, b) اذا كان : $a = 264 \ , \ b = 42$

ثم اوجد x, y التي تجعل $d = ax + by$

الحل :

من خوارزمية اقليدس :

$$a = bq + r$$

$$264 = 42(6) + 12$$

$$42 = 12(3) + 6$$

$$12 = 6(2) + 0$$

$$d = 6$$

ومن الخطوة قبل الاخيرة

$$6 = 42 - 12(3)$$

$$= 42 - \big(264 - 42(6)\big)(3)$$

$$= 42 - (264(3) + 42(18)$$

$$= 42(19) - 264(3)$$

$$= 42(19) + 264(-3)$$

مثال (12) :

أجد القاسم المشترك الاعظم ل:(6755,1587645) ثم جد x, y التي تجعل

$$d = ax + by$$

الحل:

من خوارزمية اقليدس : $a = bq + r$

$$1587645 = 235(6755) + 220$$

$$6755 = 30(220) + 155$$

$$220 = 1(155) + 65$$

$$155 = 2(65) + 25$$

$$65 = 2(25) + 15$$

$$25 = 1(15) + 10$$

$$15 = 1(10) + 5$$

$$10 = 2(5) + 0$$

وعليه فان $(6755,1587645) = 2$

من الخطوة قبل الاخيرة اعلاه وبالمرور علي خطوات الخوارزمية عكسيا نجد :

$$5 = 15 - 1(10)$$
$$= 15 - 1(25 - 1(15))$$
$$= -25 + 2(15)$$
$$= -25 + 2(65 - 2(25))$$
$$= 2(65) - 5(155 - 2(65))$$
$$= 2(65) - 5(155)$$
$$= -5(155) + 12(65)$$
$$= -5(155) + 12(220 - 1(155))$$
$$= 12(220) - 17(6755) - 30(220)$$
$$= -17(6755) + 522(220)$$
$$= -17(6755) + 522(1587645) - 235(6755)$$
$$= 6755(-122687) + 1587645(522)$$

ومنه نجد ان $y = 522$ و $x = -122687$

(11-2) الأعداد الأوليةنسبياً :

تعريف :

ليكن a, b عددين صحيحين غير صفرين يقال ان العددين a, b اوليان نسبياً اذا كان القاسم المشترك الاعظم لهما يساوي الواحد اي ان:

تعريف :

لتكن $a_1, a_2, a_3, \dots, a_n$اعداد صحيحة ليست جميعها اصفار نقول ان d هو القاسم المشترك الاعظم للاعداد :$a_1, a_2, a_3, \dots, a_n$ ونرمز لها بالرمز $d = (a_1, a_2, a_3, \dots, a_n)$ إذا وفقط إذا كان :

$d > 0$ (1)

(2) $d \mid a_i$ لكل $1 \le i \le n$

(3) اذا كان $c \mid a$ لكل $1 \le i \le n$ وكان $c > 0$ فان $c \le d$

مبرهنة(9) :

لتكن $a_1, a_2, a_3, \dots, a_n$ اعداد صحيحة ليست جميعها اصفار فان

$(a_1, a$

البرهان:

سنبرهن على أن القواسم المشتركة لمجموعة الأعداد $A = (a_1, a_2, a_3, \dots, a_n)$

هي القواسم المشتركة لمجموعة الاعداد $B=\{a_1, a_2, \dots, a_{n-2}, (a_{n-1}, a_n)\}$

نفسها .

ليكن b قاسما مشتركا لمجموعة الاعداد A اذن: $b \mid a_1, b \mid a_2, \dots, b \mid a_{n-2}$

ولكون $b \mid a_{n-1}$ و $b \mid a_n$ فان $b \mid (a_{n-1}, a_n)$ وبالتالي فإنه القاسم المشترك لمجموعة الأعداد B .

ومن ناحية أخرى اذا كان c قاسمًا مشتركًا لمجموعة الأعداد B فإن :

ولكون $c \mid a_1 , c \mid a_2 , \cdots, c \mid a_{n-2}$ فان $c \mid (a_{n-1}, a_n)$ أي أن $c \mid a_{n-1}, c \mid a_n$ قاسم مشترك لمجموعة الأعداد A .

بما ان c مجموعة القواسم المشتركة للمجموعتين A , B متساوية ومنتهية فبأخذ العنصر الأكبر في هذه المجموعة نستنتج أن :

$(a_1,$

مثال (13) :

جد (256 , 112,72)

الحل : $(256, 112,72) = (256, (112, 72)) = (256, 8) = 8$

تعريف:

توصف الاعداد $a_1, a_2, a_3, \dots, a_n$ بانها اولية تبادلياً اذا كان :

$a_1, a_2, a_3, \dots, a_n = 1$ وتوصف بانها اوليه نسبيا مثنى مثنى

اذا كان : $(a_i, a_j) = 1$ لكل : $1 \leq i \neq j \leq n$

مثال (14) :

الأعداد $15, 21, 35$ أولية تبادلياً لأن :

$$(15, 21, 35) = (15, (21, 35)) = (15, 7) = 1$$

ولكنها ليست اعداد اولية نسبيا مثنى مثنى لان :

$$(21, 35) = 7 \quad , \quad (15, 35) = 5 \quad , \quad (15, 21) = 3$$

(12-2) المضاعف المشترك الاصغر :

تعريف :

لتكن : $a_1, a_2, a_3, \dots a_n$ جميعها لا يساوي الصفر نقول أن : m هو المضاعف المشترك الأصغر

للأعداد $a_1, a_2, a_3, \dots a_n$

ونكتب $m = a_1, a_2, a_3, \dots a_n$

إذا وفقط اذا كان

(1) $m > 0$

(2) $a_i \mid m, \ \forall i, 1 \leq i \leq n$

(3) اذا كان $c > 0$ و $a_i \mid c$ لكل $1 \leq i \leq n_i$

فان $m \leq c$

ملاحظة :

بما ان مجموعة مضاعفات الاعداد $a_1 , a_2 , a_3 , \dots a_n$ هي مجموعة جزئية غير خالية من الاعداد الصحيحة الموجبة فان مبدأ الترتيب الحسن يضمن لنا وجود عدد اصغر وحيد في هذه المجموعة وهذا العدد هو المضاعف المشترك الاصغر .

مثال(15) :

$$[5.15] = 15 \quad [6.15] = 30 \quad [9.8] = 72$$

المبرهنة التالية هي طريقة لحساب المضاعف المشترك الاصغر لعددين اذا علم القاسم المشتركالاعظم لهما :

مبرهنة(10) :

اذا كان $a, b > 0$ فان $[a, b](a, b) = ab$

البرهان :

بافتراض ان $d = (a, b)$ وان $m = \frac{ab}{d}$ فانه يوجد عددان s, r بحيث ان $a = dr , b = ds$

وبالتالي فان $m = as = rb$ اذا كان $b \mid c$ و $a \mid c$ فانه يوجد عددان t , u بحيث يكون

$c = au = bt$ وبما ان $d = (a, b)$ فانه يوجد عددان x, y بحيث ان $d = ax + by$

وعليه فان : $\frac{c}{m} = \frac{cd}{ab} = \frac{c(ax+by)}{ab} = \frac{c}{b}x + \frac{c}{a}y = tx + uy$

ومنه نجد ان $m \mid c$ اي ان $m \leq c$ ونكون برهنا علي ان $m = [a, b]$

ملاحظة :

الصيغة الواردة في المبرهنة (10)غير صالحة لاكثر من عددين بمعنى اخر ان

$abc \neq [a,b,c](a,b,c)$كما هو مبين في المثال التالي :

مثال (16) :

$$[6,10,15] = 30$$

$$(6,10,15) = 1$$

(13-2) الأعداد الأولية :

تعريف:نقول أن العدد الصحيح P عدد اولي اذا كان $P > 1$وكان لا يقبل القسمة الا على نفسه والعدد 1. يسمى العدد الصحيح الموجب غير الأولي الذي لا يساوي 1 عدداً مؤلفاً إذن فالعدد المؤلف nيمكن كتابته كما يلي $m = ab$ حيث أن $1 < a < n$. $1 < b < n$

مبرهنة (11) :

أي عدد صحيح $n > 1$ هو إما أولي أو حاصل ضرب عدد منتهي من الأعداد الأولية .

البرهان :

تبرهن بواسطة المبدأ الثاني للاستقراء الرياضي

الخطوة الأساسية **:** العدد 2 عدد اولي

خطوة الاستقراء :

لنفرض ان اي عدد m بحيث ان $2 \leq m \leq k$ هو حاصل ضرب عدد منتهي من الاعداد الاولية سنبرهن على ان $k + 1$هو حاصل ضرب عدد منتهي من الاعداد الاولية

اذا كان $k + 1$ عدد اولي فهو يعني بمنطوق المبرهنة انه اذا كان $k + 1$ عددا مؤلفا فان

$k + 1 = ab$ حيث ان $2 \leq a , b \leq k$ باستخدام فرضية الاستقراء نستطيع كتابة كل من a, b كحاصل ضرب عدد منتهي من الاعداد الاولية وبالتالي فاننا نستطيع كتابة $k + 1$ كحاصل ضرب عدد منتهي من الاعداد الاولية .

نتيجة(1):

لكل عدد صحيح $n > 1$ يكون له قاسم أولي .

البرهان:

إذا كان n عدد اولي فالعبارة صحيحة لان $n \mid n$ اما اذا كان n عددا مؤلفا فاننا نحصل على القاسم الاولي باستخدام مبرهنة (11) .

نتيجة(2) :

اذا كان n عددا مؤلفا فانه يوجد قاسماً اولياً P للعدد n بحيث أن $P \leq \sqrt{n}$

البرهان :

بما ان n عددا مؤلفا فان $n = ab$ و $1 < a \leq b < n$ اذن $m = ab \geq a^2$ ومنه نجد ان $a < \sqrt{n}$.

وباستخدام نتيجة (1) يوجد عدد اولي P بحيث $P \mid a$ ومنه نجد أن $P \mid n$ و $P \leq a$ وبالتالي فإن

$$P \leq \sqrt{n}$$

(14-2) مرشحة اراتواستينس :The Sieve of Eratosthenes :

وهي قاعدة لايجاد الاعداد الاولية والفكرة هي :

اننا نريد ايجاد جميع الاعداد الاولية التي تقل عن 100 نكتب جميع الاعداد بين 2 و 100 وبما ان العدد 2 هو عدد اولي فاننا نضع دائرة حوله ونشطب جميع الاعداد الزوجية الاخرى لانها من

مضاعفات العدد 2 . العدد التالي في الاقائمة هو العدد 3 يتم شطبه ووضع دائرة حوله ثم نقوم بشطب كل ثالث عدد بعد ذلك لانها من مضاعفات العدد 3 بعد نهاية الخطوة ستكون القائمة كالآتي :

②. ③ , 4,5,6,7,8,9,~~10~~,11,12,13,~~14~~,15,~~16~~,17,~~18~~,19,20,~~21~~,22……

وبذلك يكون اصغر عدد في القائمة الذي لم توضع حوله دائرة او لم يتم شطبه هو عدد اولي

مما سبق يمكن الاستنتاج انه من المحتمل عند خطوة معينه من خطوات مرشحة اراتوستينس ان الاعداد الكبيرة ستشطب وهذا يعني ان عدد الاعداد الاولية منته.

ان مثل هذا الاستنتاج خاطئ وقد قدم اكثر من برهان لوجود عدد غير منته من الاعداد الاولية وكان اول هذه البراهين هو الذي قدمه اقليدس في الجزء **IX**من كتابه المشهور العناصر (Elements) وسنقدم برهانا مشابه لبرهان اقليدس .

مبرهنة (12) :

يوجد عدد منته من الاعداد الاولية

البرهان :

لنضع $a_n = n! + 1$ حيث أن $n \geq 1$ باستخدام نتيجة (1) للمبرهنة (11) نجد أن Q_n له على الاقل عامل اولي واحد وليكن q_n اذا كان $q_n \leq n$ فان $q_n \mid n!$ ومنه نجد ان

$q_n \mid (Q_n - n!)$ اي ان $q_n \mid 1$ وهذا مستحيل اي ان $q_n > n$ اذن نكون قد برهنا على انه يوجد لكل عدد صحيح موجب nعدد اولي اكبر من n وبالتالي يكون عدد الاعداد الاولية غير منته .

(15-2) المبرهنة الأساسية في الحساب :

اي عدد صحيح $n > 1$ يمكن كتابته بشكل وحيد (باستثناء الترتيب) كحاصل ضرب عدد منته من الاعداد الاولية .

البرهان :

لقد برهنا سابقا في مبرهنة (11) علي ان اي عدد صحيح $n > 1$ يمكن كتابته كحاصل ضرب عدد منته من الاعداد الاولية ولإتمام البرهان نحتاج الي ان نثبت ان n يكتب بشكل وحيد ونستخدم لذلك المبدأ الثاني للاستقراء الرياضي على n

الخطوة الاساسية:

اذا كان $n = 2$ فمن الواضح ان العبارة الصحيحة

خطوة الاستقراء :

لنفرض ان العبارة الصحيحة لجميع الاعداد الصحيحة التي هي اكبر من 1 واقل من n اذا كان n عددا اوليا فالقضية صحيحة . لنفرض اذا ان n عدد مؤلف واننا نستطيع كتابة العدد n كحاصل ضرب عدد منته من الاعداد الاولية بطريقتين مختلفتين اي ان :

$$n = p_1\, p_2 \dots \dots p_t$$

$$= q_1\, q_2 \dots \dots q_s$$

بما ان q_s . ... $q_1\, q_2$ | P_1 فانه يوجد عدد i بحيث $1 < i \leq s$ بحيث ان : $p_1 \mid q_1$ ولكن بامكاننا ان نعيد ترتيب الاعداد q_s. ... $q_1\ q_2$ بحيث يكون : $p_1 \mid q_1$ وبما ان : p_1 و q_1 عددان اوليان فان : $p_1 = q_1$ وبالتالي فان : $1 < \frac{n}{p_1} < n$ و $\frac{n}{p_1} = p_2 p_3 \cdots p_t = q_2 q_3 \cdots q_s$

فباستخدام فرضية الاستقراء الرياضي نستنتج ان الطريقتين السابقتين للكتابة $\frac{n}{p_1}$ متطابقتان باستثناء ترتيب العوامل

وعليه فان : $S = t$ وان طريقتي تحليل العدد n الى عوامل اولية متطابقتان , وبهذا يتم برهان المبرهنة .

مثال (19):

برهن على ان العدد $\log_{10} 2$ عدد غير نسبي

الحل:

اذا كان $\log_{10} 2$ فان : $\log_{10} 2 = \frac{a}{b}$ بحيث $a , b \in Z$ و $b \neq 0$ ومنه نجد ان :

$10^a = 2^b$ اي ان : $2^a \cdot 5^a = 2^b$ وهذا يناقض الوحدانية في المبرهنة الاساسية للحساب .

مثال (20) :

برهن على ان العدد $\sqrt[3]{10}$ غير نسبي

الحل :

بما ان :$10 = 2 \times 5$ فانه باستخدام المبرهنة الاساسية في الحساب لا يمكن ان يكون مكعبا لعدد صحيح وعليه

فان :$\sqrt[3]{10}$ عدد غير صحيح وبالتالي فانه غير نسبي .

(1-3) التــطــابــق :

قد كان واضحا من الفصل السابق ان قابلية القسمة تمثل احد المفاهيم الاساسية في نظرية الاعداد .في هذا الفصل سنستمر في دراسة قابلية القسمة ولكن من وجهة نظر مختلفة نوعا ما فان التطابق هو تعبير اخر لقابلية القسمة ولكن اكثر تطورا حيث انه باستخدمنا للتطابق نستطيع التوصل للبراهين بصورة اسهل. التطابق يؤدي الي مساواة وهنالك تشابه كبير بين خواصه وخواص المساواة وبذلك نستطيع ان نركز هذه الخواص بصورة اسهل .

تعريف:

ليكن $a , b \in Z$ و $n \in Z^+$ نقول أن a يطابق b قياس n ونرمز لذلك بالرمز $a \equiv b(\text{mod } n)$ إذا كان

$n \mid (a - b)$ وإذا كان $n \nmid (a - b)$ فاننا نقول أن a لا تطابق b قياس n ونكتب $a \not\equiv b(\text{mod } n)$

مبرهنة (1) :

اذا كان $a , b \in Z$ فان $a \equiv b(\text{mod } n)$ اذا وفقط اذا وجد عدد صحيح k بحيث ان $a = b + kn$

البرهان:

اذا كان $a \equiv b(\text{mod } n)$ فان $n \mid (a - b)$ بالتالي يوجد عدد صحيح k حيث ان $a - b = kn$ اي ان

$$a = b + kn$$

وبالعكس اذا فرضنا وجود عدد صحيح k

حيث ان $a = b + kn$ فان $a - b = kn$

ومنه نجد ان $n \mid (a - b)$ اي ان $a \equiv b(\text{mod } n)$

مثال(1):

$5 = 1(3) + 2$ لأن $5 (\mod 3) = 2$

و $2 (\mod 3) = 2$

لأن $2 = 0(3) + 2$

و $3 (\mod 3) = 0$ لأن $3 = 1(3) + 0$

مبرهنة (2) :

بعض خواص التطابق مقياس n:

اذا كان $a, b, c \in Z$ وكان $n \epsilon Z^+$ فان

(1) $a \equiv a (\mod n)$

(2) اذا كان $a \equiv b (\mod n)$ فان $b \equiv a (\mod n)$

(3) اذا كان $a \equiv b (\mod n)$ وكان $b \equiv c (\mod n)$ فان $a \equiv c (\mod n)$

البرهان:

(1) بما ان $n \mid (a - a) = 0$ فان $a \equiv a (\mod n)$

(2) بما ان $a \equiv b (\mod n)$ فاننا نستطيع ايجاد عدد صحيح k بحيث ان $a - b = kn$ اي ان

$b - a = (-k)n$ ومنه نجد أن : $b \equiv a (\mod n)$

(3) بما ان $a \equiv b (\mod n)$ وان $b \equiv c (\mod n)$ فانه يوجد عددان صحيحان j, k بحيث ان

$kn = a - b$ وان $jn = b - c$ وبناءا على ذلك نجد ان

$a - c = (a - b) + (b - c) = kn + jn = (k + j)n$ اي ان $n \mid (a -$

ومنه نجد ان $a \equiv c (\mod n)$ c)

مبرهنة(3) :

اذا كانت : a, b, c, d اعداد صحيحة وكان : n عددا صحيحا موجبا بحيث ان $a \equiv b(\text{mod } n)$ وان $c \equiv b(\text{mod } n)$ فان :

$$a + c \equiv b + d \ (\text{mod } n) \quad (1)$$
$$a - c \equiv b - d \ (\text{mod } n) \quad (2)$$
$$ac \equiv bd \ (\text{mod } n) \quad (3)$$

البرهان :

بما ان $a \equiv b(\text{mod } n)$ وان : $c \equiv b(\text{mod } n)$ فانه يوجد عددان صحيحان k, j بحيث ان

$$kn = a - b \text{ وان } jn = c - d$$

$$(a + c) - (b + d) = (a - b) + (c - d) = kn + nj$$
$$= (k + j)n \quad (1)$$

ومنه نجد ان :

$$(a + c) \equiv b + d(\text{mod } n) \text{ : اي ان } a + c = (b + d) + (k + j)n$$
$$(a - c) - (b - d) = (a - b) - (c - d) = kn - nj$$
$$= (k + j)n \quad (2)$$

ومنه نجد ان :

$$(a - c) \equiv b - \text{ : اي ان } a - c = (b - d) + (k - j)n$$
$$d(\text{mod } n)$$
$$ac - bd - ac = ba + bc - bd = c(a - b) + b(c - d)$$
$$= (ck + bj)n \quad (3)$$

ومنه نجد ان :

$ac \equiv bd(\mathrm{mod}\ n)$ اي ان $ac = bd + (ck + bj)n$

مبرهنة (4) :

إذا كان :$a \equiv b(\mathrm{mod}\ n)$ وكان $m \mid n$ فإن : $a \equiv b(\mathrm{mod}\ m)$

البرهان :

بما أن $a \equiv b(\mathrm{mod}\ n)$ فإن :$n \mid (a - b)$ بما أن $m \mid n$ فإن $m \mid (a - b)$ وبالتالي فإن:

تعريف:

ليكن a^* عددا صحيحا نقول ان العدد a^*هو النظير الضربي للعدد a قياس n اذا كان $aa^* \equiv 1(\mathrm{mod}\ n)$

ونعني بالنظير الضربي للعدد الصحيح هو مقلوب العدد

$$a.\frac{1}{a} = 1$$

مثال (2) :

لاحظ ان و$2(1) \equiv 2(\mathrm{mod}\ 4)$ و$2(0) \equiv 0(\mathrm{mod}\ 4)$

و$2(2) = 2(\mathrm{mod}\ 4)$

و$2(2) \equiv 0(\mathrm{mod}\ 4)$

اذن العدد 2 ليس له نظير ضربي قياس 4

مثال (3) : اثبت ان

$$f_5 = 2^{32} + 1 \equiv 0(\mathrm{mod}\ 641)$$

الحل:

$$2^4 \equiv 16(\text{mod } 641)$$

$$2^8 \equiv 256(\text{mod } 641)$$

$$2^{16} \equiv 154(\text{mod } 641)$$

$$2^{32} \equiv 640(\text{mod } 641)$$

اذن $f_5 = 2^{32} + 1 \equiv 0(\text{mod } 641)$

(2-3) انظمة الرواسب:Residue systems

ليكن nعدد صحيح موجب إن علاقة التطابق قياسnهي علاقة تكافؤ على مجموعة الأعداد الصحيحة وعليه فانها تجزئ المجموعة Z إلي nمن المجموعات المختلفة والتي يسمى كل منها فصل تطابق قياس n وكل مجموعة من هذه المجموعات تحوي الاعداد المتطابقة المختلفة قياس nفعلى سبيل المثال أن فصول التطابق المختلفة قياس 3

$$[0] = \{\dots, -9, -6, -3, 0, 3, 6, 9, \dots\}$$

$$[1] = \{\dots, -8, -5, 1, 4, 7, 10, \dots\}$$

$$[2] = \{\dots, -7, -4, -1, 2, 5, 8, 11, \dots\}$$

مبرهنة (5) :

اي عدد صحيح يجب ان يكون مطابقا لعدد واحد فقط من بين الاعداد $0,1,2,3, \dots, n-1$ قياس n

البرهان:

لنفرض أن x عدد صحيح بإستخدام خوارزمية القسمة نستطيع كتابة العدد x على الصورة

$x = qn + r$ و

$0 \leq r \leq n-1$ومن تعريف التطابق نجد ان$x \equiv r(\text{mod } n)$وإذا فرضنا ايضا ان

$x \equiv \grave{r} \pmod n$ حيث ان $0 \le \grave{r} \le n-1$ فان $x = \grave{q}\, n + \grave{r}$ و $\grave{q} \in Z$ اي ان

$x = \grave{q}\, n + \grave{r} = qn + r$ وبستخدام الوحدانية في خوارزمية القسمة نجد ان $r = \grave{r}$

(3-3)مجموعة الباقي (الرواسب) التامة:(complete residue system)

تعريف:

نقول ان الاعداد $r_1 , r_2, \cdots , r_n$ تمثل نظام رواسب تام قياس n اذا كان لكل عدد صحيح يطابق عدد واحد فقط من الاعداد $r_1 , r_2 \cdots r_n$ قياس n

مثال (3) :

اثبت ان المجموعة $\{0, \pm 1 , \pm 2\}$ تمثل نظام رواسب تام قياس 5

الحل:

لاحظ ان $4 \equiv -1 \pmod 5$ و $3 \equiv -2 \pmod 5$ و $0 \equiv 0 \pmod 5$ و $1 \equiv 1 \pmod 5$ و

مبرهنة (6) :

اي nمن الأعداد الصحيحة المتتالية تمثل نظام رواسب تام قياسn

البرهان :

لتكن $b, b+1, b+2 \cdots , b+n-1$ أعداد متتالية عددهاnولنفرض ان

$b + j \equiv b + k \pmod n, \quad k \ne j$ ومنه نجد ان $j \equiv k \pmod n$ وهذا تناقض لأن

$0,1,2,3, \cdots n-1$ نظام رواسب تام .

(4-3) نظام الرواسب المختزل قياس n: (Reduced Residue System):

تعريف:

ليكن $S = \{r_1, r_2, \cdots, r_n\}$ نظام رواسب تام قياس nنقول ان المجموعة الجزئية

$T = \{a \in S : (a, n) = 1\}$ نظام رواسب مختزل قياس n

مثال (4) : اذا كان $n = 12$ واخذنا $\{0,1,2 \cdots ,11\}$كنظام رواسب تام قياس 12 فان $\{1,5,7,11\}$ تكون نظام رواسب مختزل قياس 12 واذا اخذنا المجموعة $\{0, \pm1, \pm2, \pm3, \pm4, \pm5,6\}$ كنظام رواسب تام قياس 12 فعند اذن يكون $[\pm1, \pm5]$ نظام رواسب مختزل قياس 12.

(5-3) دالة اويلر :

تعريف:

إذا كان n عدد صحيح موجب فإننا نعرف دالة أويلر بأنها عدد العناصر التي يحتويها أي نظام رواسب مختزل قياس nونرمز لها بالرمز $\varphi(n)$.

اي ان :

من تعريف نظام الرواسب المختزل قياس n نجد ان عناصره هي الاعداد الأولية نسبيا مع n والتي هي اقل من n او تساويه ومن ثم فانه يكون واضحا لدينا ان$\varphi(n)$ هو عدد الاعداد الاولية نسبيا مع n التي هي اقل من n او تساويه .

مثال (5) :

إذا كان : $n = 2$

فإنَ: $\varphi(n) = \varphi(2) = 1$

مثال (6) :

اذا كان : $n = 5$

فان : $\varphi(n) = \varphi(5) = 4$ اي ان :

اذا كان : $n = p$ حيث p عدد اولي فان :

$$\varphi(n) = \varphi(p) = p - 1$$

واذا كان : $(a.b) = 1$ فان : $\varphi(a.b) = \varphi(a)\,\varphi(b)$ حيث φ في هذه الحالة تسمى دالة ضربية .

مثال (7) :

1) $\varphi(6) = \varphi(2.3) = \varphi(2)\varphi(3) = 1 \times 2 = 2$

2) $\varphi(12) = \varphi(3.4) = \varphi(3)\varphi(4) = 2 \times 2 = 4$

(6-3) التطابقات الخطية :linear congruence :

لتكن n عدد صحيح موجب اكبر من الواحد و a, b عددين صحيحين فان :

يسمى تطابق خطي مقياس n حيث x متغير . مثلا :

حل التطابق الخطي :

اي عدد صحيح x_0 يحقق التطابق $ax \equiv b(\text{mod } n)$ يسمى حل التطابق الخطي اي ان x_0 حل للتطابق الخطي (1) اذا وفقط اذا كان $ax_0 \equiv b(\text{mod } n)$ واذا كان x_0 حل التطابق فان $x_0 + kn$ حل ايضا لكل $k \in Z$ ويكتب الحل كما يلي :

مبرهنة (7) :

اذا كان : $d = (a, n)$ فان للتطابق الخطي $ax = b(\text{mod } n)$ حلا اذا وفقط اذا كان $d \mid b$ واذا كان $d \mid b$ وكان x_0 حلا للتطابق فان جميع الحلول غير المتطابقة هي : $x = x_0 + \frac{kn}{d}$ و $0 \leq k \leq d - 1$

البرهان :

لقد لاحظنا ان التطابق $ax \equiv b(\text{mod } n)$ يكافئ المعادله الديوفنتية الخطية $ax - ny = b$ وبالتالي فان للمعادلة $ax \equiv b(\text{mod } n)$ حلا اذا وفقط اذا كان $d \mid b$ فان جميع الحلول تكتب على الصورة :

$X = x_0 + \frac{n}{d}k \quad y = y_0 + \frac{a}{d}k$ حيث $k \in Z$ لناخذ من بين جميع الاعداد الصحيحة التي تحقق المعادلة الاولى الاعداد التي قيم k عنها $0,1,2,3, \dots, d-1$ وهذه القيم هي :

$$x_0, x_0 + \frac{n}{d}, x_0 + \frac{2n}{d}, \dots, x_0 + \frac{(d-1)n}{d}$$

سنبرهن الأن على أن جميع هذه الأعداد غير متطابقة قياس n هو أي حل اخر يجب أن يكون مطابقا مع أحد هذه الأعداد قياس n لنفرض أنه :

$x_0 + \frac{n}{d}k_1 \equiv x_0 + \frac{n}{d}k_2 (\text{mod } n)$ حيث ان $0 \leq k_1 < k_2 \leq d - 1$ ومنه نجد ان :

$\frac{n}{d}k_1 \equiv \frac{n}{d}k_2 (\text{mod } n)$ وبما ان : $(\frac{n}{d}, n) = \frac{n}{d}$ نجد ان : $k_1 \equiv k_2 (\text{mod } d)$ اي ان $d \mid k_2 - k_1$

وهذا مستحيل لأن $0 \leq k_2 - k_1 < d$ لنفرض الأن أن $x_0 + \frac{n}{d}k$ حلا للتطابق . وبإستخدام خوارزمية القسمة نستطيع كتابة k علي الصورة : $k = qd + r \quad 0 \leq r \leq d - 1$ و وعليه فان

$$x_0 + \frac{n}{d}k = x_0 + \frac{n}{d}(qd + r) = x_0 + nq + \frac{n}{d}r = x_0 + \frac{n}{d}r \ (\text{mod } n)$$

(7-3) انظمة التطابقات الخطية بمتغير واحد : System of Linear Congruence In One Variable

لنفرض انه لدينا التطابقين التاليين $6x \equiv 4(\mod 8)$ و $3x \equiv 2(\mod 5)$

اذا وجدنا قيمة x فاننا نسميه حلا لنظام التطابقات ونجد ان $x = 2 + 4k$ و $k = 0,1$ هي جميع الحلول غير المتطابقة قياس 8 بالنسبة للتطابق الاول . اما التطابق الثاني فله حل واحد فقط قياس 5 وهو $x = 4$ولحل النظام يجب ان نجد عدد x بحيث يكون $x \equiv 2(\mod 4) \rightarrow (1)$ و$x \equiv 4(\mod 5) \rightarrow (2)$من (1) نجد ان $x = 2 + 4k_1$ حيث $k_1 \epsilon Z$ وبالتعويض في (2) نجد ان $2 + 4k_1 \equiv 4(\mod 5)$ اي ان

$4k_1 \equiv 2(\mod 5)$ وبحل التطابق الاخير نجد ان $k_1 \equiv 3(\mod 5)$ وعليه فان $k_1 = 3 + 5k_2$ حيث ان $k_2 \epsilon Z$ وبالتعويض عن قيمة k_1 في المعادلة $x = 2 + 4k_1$ نجد ان $x = 14 + 20k_2$وبالتالي فان $x = 14(\mod 20)$ يحقق التطابقين معا .

تمهيدية:ليكن نظام التطابقات التالي:

$$a_1x \equiv c_1(\mod m_1)$$

$$a_2x \equiv c_2(\mod m_2)$$

$$\vdots \qquad \vdots$$

$$a_kx \equiv c_k(\mod m_k)$$

ليكن $d_1 = (m_i)$ و $1 \leq i \leq k$و وليكن :x_1 حلا للتطابق $a_ix \equiv i(\mod m_i)$ و $1 \leq i \leq k$ عندئذ حلا للنظام (1) اذا وفقط اذا كان x حلا للنظام $x \equiv x_1(\mod \frac{m_1}{d_1})$

$$x \equiv x_2(\mod \frac{m_2}{d_2})$$

$$\vdots$$

$$x \equiv x_k (\mathrm{mod}\ \frac{m_k}{d_k})$$

مثال (8) :

لقد وجدنا ان : $x \equiv 14 (\mathrm{mod}\ 20)$ حلا للنظام $6x \equiv 4 (\mathrm{mod}\ 8)$ و $3x \equiv 2 (\mathrm{mod}\ 5)$ وبما ان

$(6,8) = 2$ و $(3,5) = 1$ وان $x_1 \equiv 2 (\mathrm{mod}\ 4)$ و $x_2 \equiv 4 (\mathrm{mod}\ 5)$

حلا للتطابقين على الترتيب وباستخدام تمهيديه نجد انه يجب ان يكون هنالك حلا للنظام :

$$x \equiv 2 (\mathrm{mod}\ 4)$$

$$x \equiv 4 (\mathrm{mod}\ 5)$$

من الواضح انه اذا كانت احدى التطابقات في نظام ما غير قابلة للحل فان النظام غير قابل للحل ولكن العكس ليس صحيح, كما يوضح المثال التالي :

مثال (9):

ليكن لدينا النظام

$$6x \equiv 4 (\mathrm{mod}\ 8)$$

$$9x \equiv 3 (\mathrm{mod}\ 12)$$

بما ان : $4 \mid 2 = (6,8)$ و $3 \mid 3 = (9,12)$ فانه يوجد حل لكل تطابق من التطابقين وباستخدام طريقة الحل $x \equiv 2 (\mathrm{mod}\ 4)$ حل للتطابق الاول وان : $x \equiv 3 (\mathrm{mod}\ 4)$ حل للتطابق الثاني وباستخدام التمهيدية فانه يكون للنظام (2) حلا للنظام اذا وفقط اذا كان النظام :

$$x \equiv 2 (\mathrm{mod}\ 4)$$

$$x \equiv 3 (\mathrm{mod}\ 4) \rightarrow (3)$$

حل ولكن من الواضح انه ليس حل للنظام (3) وعليه فانه لايوجد حل للنظام (2)

(8-3) مبرهنة الباقي الصينية : The Chinese remainder theorem

هذه المبرهنة تستخدم لايجاد حل مشترك وحيد معيار n .

اذا كانت الاعداد $m_1 , m_2, m_3 \dots , m_k$ اعداد اولية نسبيا مثنى مثنى فانه يوجد للنظام

$$x \equiv c_1 (\mathrm{mod} m_1)$$

$$x \equiv c_2 (\mathrm{mod} m_2)$$

$$\vdots \qquad \vdots$$

$$x \equiv c_k (\mathrm{mod}\, m_k)$$

حل وحيد قياس العدد $M = m_1 m_2 m_3 \dots . m_k$

البرهان:

لايجاد حل للنظام نفرض ان $M_1 = \frac{M}{m_1} = m_1 . m_2 . m_3 \dots . m_k$ و $r = 1,2,3, \dots , k$ بما ان $(m_s, m_r) = 1$ عندما $r \neq s$ نجد ان $(m_s, m_n) = 1$ ومنه نجد ان العدد M_1 نظير ضربي قياس m_r وليكن y_r وهذا يعني ان $m_r y_r \equiv 1 (\mathrm{mod} m_r)$ لنبرهن الان على ان العدد x حيث ان $x = c_1 M_1 Y_1 + c_2 M_2 Y_2 + \cdots + c_k M_k Y_k$هو حلا للنظام وللبرهنة علي ذلك يجب ان نثبت $x \equiv c_r (\mathrm{mod}\, m_r)$ لكل r حيث ان $1 \leq r \leq k$ بما ان $m_r \mid M_s$ عندما $r \neq s$فان $M_s \equiv 0 (\mathrm{mod} m_r)$ ومنه $x \equiv c_r M_r Y_r \equiv c_r (\mathrm{mod} m_r)$ ولبرهان الوحدانية نفرض ان x_1, x_0 حلان للنظام ومن تعريف الحل نجد ان $x_0 \equiv x_1 \equiv c_r (\mathrm{mod} m_r)$ لكل r حيث $1 \leq r \leq r$ ومنه نجد ان$m_r \mid (x_0 - x_1)$و

$N \mid (x_0 - x_1)$ اي ان $x_0 \equiv x_1 (\mathrm{mod} M)$

مثال (10) :

اوجد حل التطابقات الاتية :

$$x \equiv 2 \pmod 3$$

$$x \equiv 2 \pmod 4$$

$$x \equiv 3 \pmod 5$$

الحل :

	m_i	a_i	M_i	y_i
	3	2	20	2
	4	2	15	3
	5	3	12	3

لايجاد y_i نعوض في $M_i y_i \equiv 1 \pmod{m_i}$

$$20y_1 \equiv 1 \pmod 3 \quad \Longrightarrow \; y_1 = 2$$

$$15y_2 \equiv 1 \pmod 4 \quad \Longrightarrow \; y_2 = 3$$

$$12y_3 \equiv 1 \pmod 5 \quad \Longrightarrow \; y_3 = 3$$

$$Z = \sum_{i=1}^{3} a_i M_i y_i$$

$$= 2 \times 20 \times 2 + 2 \times 15 \times 3 + 3 \times 12 \times 3 \left(\mathrm{mod}(3 \times 4 \times 5)\right)$$

$$= 80 + 90 + 180 (\text{mod } 60)$$

$$Z \equiv 278 \ (\text{mod } 60)$$

$$Z \equiv 38 (\text{mod } 60)$$

$$Z = 38$$

مثال(11) :

استخدم مبرهنة الباقي الصينية لحل التطابق $19x \equiv 1 (\text{mod } 140)$

الحل:

التطابق يكافئ النظام

$$19x \equiv 1 (\text{mod } 4)$$

$$19x \equiv 1 (\text{mod } 5)$$

$$19x \equiv 1 (\text{mod } 7)$$

وهذا بدوره يكافئ النظام

$$x \equiv 3 (\text{mod } 4)$$

$$x \equiv 4 (\text{mod } 5)$$

$$x \equiv 3 (\text{mod } 7)$$

ومنه نجد ان $M_1 = 35 . M_2 = 28 . M_3 = 20$ بحل المعادلة $35y_1 \equiv 1 (\text{mod } 4)$ نجد ان $y_1 = -1$ ومن المعادلة $28y_2 \equiv 1 (\text{mod } 5)$ نجد $y_2 = 2$ ومن المعادلة $20y_3 \equiv 1 (\text{mod } 7)$ نجد ان $y_3 = -1$ مما سبق نجد ان $x \equiv (35)(-1)(3) + (28)(2)(4) + (20)(-1)(3) = 59 (\text{mod } 140)$

(3-9) بعض التطابقات الخاصة:special congruencies

مبرهنة اويلر(8) :

اذا كان n عددا صحيحا موجبا وكان $(a,n) = 1$ فان $a^{\varphi(n)} \equiv 1(\text{mod}n)$ حيث ان $\varphi(n)$ ترمز لدالة اويلر

البرهان:

لنفرض ان الاعداد $r_1, r_2 \dots, r_{\varphi(n)}$ نظام رواسب مختزل قياس n بما ان a فباستخدام المبرهنة نجد ان $ar_1 . ar_2 \dots . ar_{\varphi(n)}$ نظام رواسب مختزل قياس n ونجد ان كل r_i يجب ان يطابق عدد وحيد ar_j قياس n وعليه فان $(ar_1).(ar_2) \dots . (ar_{\varphi(n)}) \equiv r_1 . r_2 \dots . r_{\varphi(n)}(\text{mod}n)$ اي ان $r_1 . r_2 \dots . r_{\varphi(n)}(\text{mod}n)$ وبما ان $a^{\varphi(n)} r_1 r_2 \dots . r_{\varphi(n)} \equiv r_1 r_2 \dots . r_{\varphi(n)}. n = 1$ فان $a^{\varphi(n)} \equiv 1(\text{mod}n)$.

مثال (12) :

1) $2^{12} \equiv 1(\text{mod } 21)$
2) $2^{36} \equiv 1(\text{mod } 21)$
3) $5 \times 2^{40} \equiv 1(\text{mod } 21)$

اوجد باقي قسمة 5×2^{40} علي 21

الحل :

بما ان n=21 و a=2 نوجد $\varphi(21)$

$\varphi($

نجد ان :

$$(1)2^{\varphi(21)} \equiv 1(\text{mod } 21)$$

$$2^{12} \equiv 1(\text{mod } 21)$$

$$(2)2^{36} \equiv 1(\text{mod } 21)$$

$$2^{12^3} \equiv 1 \pmod{21}$$

$$1^3 \equiv 1 \pmod{21} = 1 \equiv 1 \pmod{21}$$

$$(3)\quad 5 \times 2^{40} \equiv 1 \pmod{21}$$

$$5 \times 2^{40} = 2^4 = 5 \times 1 \times 2^4$$
$$= 5 \times 16 = 80$$

اذن باقي قسمة 5×2^{40} على 21 هو 17

اذن $5 \times 2^{40} \equiv 17 \pmod{21}$

مبرهنة فيرما الصغرى (9) :

اذا كانP عدد اولي حيث ان $a \nmid P$فان $a^{p-1} \equiv 1 \pmod{P}$

البرهان :

بمان ان $a \nmid P$ فان $(a.P) = 1$ وان $\varphi(p) = p - 1$وباستخدام مبرهنة اويلر نجد ان $a^{p-1} \equiv 1 \pmod{P}$

مثال (13) :

جد باقي قسمة العدد 5^{38} على العدد 11

الحل :

باستخدام مبرهنة فيرما الصغرى نجد ان : $5^{10} \equiv 1 \pmod{11}$

ومنه نجد ان : $5^{38} \equiv (5^{10^3})(5^{2^4}) \equiv (1)(3^4) \equiv 81 \equiv 4 \pmod{11}$ إذن باقي القسمة هو العدد 4.

مبرهنة ويلسن (10) :

اذا كان Pعدد اولي فان $(p-1)! \equiv -1(\mathrm{mod}P)$

البرهان :

اذا كان $P = 2$ فان $(p-1)! \equiv 1 \equiv -1(\mathrm{mod}\ 2)$ لنفرض ان $p > 2$ وبما ان $(a,p) =$ 1لكل a بحيث $1 \leq a \leq p-1$ فانه يوجد نظير ضربي a^*للعدد قياس P بحيث ان $1 \leq a^* \leq p-1$ نجد ان

$a \equiv \pm 1(\mathrm{mod}P)$ اذا وفقط اذا كان $a^2 \equiv 1(\mathrm{mod}P)$ اذن نستطيع ان سنتنتج ان الاعداد التي تقل عن P و تساويه نظيرها الضربي قياس P هي $P-1$ و 1 وعليه يكون باستطاعتنا تكوين $\frac{p-3}{2}$ زوجا من الاعداد بين $P-2$ و 2 بحيث يكون حاصل ضرب كل زوج يطابق 1 قياس P ومنه نجد ان

$(P-2)(P-3) \ldots\ldots (3)(2) \equiv 1(\mathrm{mod}\ P)$ ومنه نجد ان

$(1)(2)(3) \ldots$

اي ان $(P-1)! \equiv -1(\mathrm{mod}\ P)$ من الملاحظ ان عكس مبرهنة ويلسن صحيح .

مبرهنة عكس مبرهنة ويلسن (11) :

اذا كان $n \epsilon Z^+$حيث ان $(n-1)! \equiv 1(\mathrm{mod}n)$فان nعدد اولي

البرهان :

لنفرض ان nعدد مؤلف وعليه غان $a > 1$و $b < n\ ,\ n-ab$ بما ان

فان $a \mid (n-1)!$ وبما ان $(n-1)! \equiv -1(\mathrm{mod}\ n)$فان $n \mid (n-1)! + 1$ ومنه نجد ان:

$a \mid (n-1)! + 1$ وبالتالي فاننا نستنتج ان $a \mid 1$ وهذا مستحيل .

مثال (14) :

بما ان $p = 17 \equiv 1(\mathrm{mod}\ 4)$ فان للتطابق $x^2 = -1(\mathrm{mod}\ 17)$ حلا . احد الحلول هو

$\left(\frac{17-1}{2}\right)! = 8!$ ولكن $8! \equiv 13(\mathrm{mod}\ 17)$ اذن $x = 13$ هو احد الحلول و

$x = -13 \equiv 4(\mathrm{mod}\ 17)$ هو حل اخر .

(3-10)التطابق الجبري:

تطابق كثيرة الحدود**:**

لتكن :(1) $\rightarrow$ $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in Z[x]$

كثيرة حدود على حلقة الاعداد الصحيحة Z حيث $a_0 , a_1, \ldots, a_n \in Z$, $n \geq 0$ فان f كثيرة حدود من الدرجة nأي : $n = degreeof$ أو $n = degf$

تعريف:

a_r

حيث $a_0 , a_1 \ldots . , a_n \in Z$ و $n \geq 0$ و $m > 1$ و x (متغير) يسمى تطابق جبري مقياس m .

اذا كان $m \nmid a_n$ فان التطابق (1) يسمى تطابق من الدرجة n او $f(x)$ كثيرة حدود من الدرجة n معيار m

اذا كان p عدد أولي نقول ان f كثيرة حدود على الحقل Z_p أو $F \in Z_p[x]$.

ويمكن كتابة التطابق (2) $\rightarrow$ $f(x) \equiv 0(\mathrm{mod} m)$ واذا كان $n = 1$ فان التطابق (1) او (2) يكون تطابق خطي : $f(x) \equiv a_1 x + a_0 \equiv 0\ (\mathrm{mod} m)$ ويقال ان العدد $x_0 \in Z$ حلا للتطابق (1) او (2) اذا كان :

$f(x_0) \equiv 0(\mathrm{mod} m)$ يسمى x_0 جذر او صفر التطابق (1) .

مثال (15) :

أوجد حل التطابقات الجبرية الاتية :

1) $x^2 - 1 \equiv 0(\mathrm{mod}\ 3)$

2) $x^3 - 2x \equiv 0(9\mathrm{mod}\ 8)$

3) $x^5 - x \equiv 0(\mathrm{mod}\ 5)$

الحل :

1) $x^2 - 1 \equiv 0(\mathrm{mod}\ 3)$

بالتجربة بعناصر $C\ S\ R$ وهي $2\ ,\ 1\ ,\ 0$ او $0, \pm 1$

$$0 - 1 \not\equiv 0(\mathrm{mod}\ 3)$$

$$1 - 1 \equiv 0\ (\mathrm{mod}\ 3)$$

$$4 - 1 \equiv 0\ (\mathrm{mod}\ 3)$$

$$x_0 = 1\ ,2$$

بالتجربة بعناصر $C\ S\ R$ وهي $0\ ,1\ ,2,3,4,5,6,7$

اذن الحلول هي : $x_0 = 0\ ,4$

$3) x^5 - x \equiv 0\ (\mathrm{mod}\ 5)$

$$CSR = 0\ , \pm 1\ , \pm 2$$

$$x_0 = 0\ ,1, -1, -2$$

تعريف :

لتكن $f\ , g \in Z[x]$ حيث $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$

$g(x) = b_n x^n + b_{n-1}x^{n-1} + \cdots + b_0$ كثيرتا حدود على حلقة الأعداد الصحيحة Z نقول ان f تطابق مقياس m ونكتب :$f(x) \equiv g(x)(\mathrm{mod}m)$

اذا كان : $a_i \equiv b_i (\mathrm{mod} m)$ لكل $i = 1 . 2 . 3 \ldots . n$

مثال (16) :

اذا كان :

$$f(x) = x^3 + 2x + 1, g(x) = x^3 + 6x + 5$$

بين ان :$f(x) \equiv g(x) (\mathrm{mod}\ 4)$

الحل :

$$m = 4 \quad \deg f = 3 = n$$

$$a_n = 1 \quad , \ a_1 = 2 \ , \quad a_0 = 1$$

$$b_n = 1 \ , \quad b_1 = 6 \ , b_0 = 5$$

نجد ان :

$$1 \equiv 1(\mathrm{mod}\ 4)$$

$$2 \equiv 6(\mathrm{mod}\ 40$$

$$1 \equiv 5(\mathrm{mod}\ 4) \therefore f(x) \equiv g(x)(\mathrm{mod}\ 4)$$

(1-4) الدوال العددية

الدالة f التي مجالها مجموعة الأعداد الصحيحة الموجبة ومجالها الصاحب مجموعة الحقيقية أو المركبة تسمي دالة عددية .

تعريف :

يقال أن $f \neq 0$ أنها دالة عددية ضربية إذا كان :$f(m n) = f(m)f(n)$ حيث $(m , n) = 1$

أمثلة :

1) دالة أويلر φ دالة ضربية .

2) الدالة $f(n) = 1$ دالة ضربية لأن إذا كان $(m , n) = 1$ فإن $f(m\, n) = 1$

$$f(m\, n) = f(m)f(n) = 1 \cdot 1 = 1$$

تعريف :

تسمى الدالة f دالة عددية ضربية تماما إذا كانت $f(m\, n) = f(m) \cdot f(n) \ , \forall\, m, n \in R$ بدون شرط $(m, n) = 1$.

مثال(1):

$$\varphi(2 \cdot 6) = \varphi(12) = \varphi(3 \cdot 4)$$

$$= \varphi(3)\emptyset(4) = 2 \cdot 2 = 4$$

تعريف :

لتكن n عدد صحيح موجب نرمز لعدد قواسم n الموجبة بالرمز $\tau(n)$ ولمجموع قواسم العدد n الموجبة بالرمز $\delta(n)$

مثال(2) :

إذا كان $n = 3$ اوجد : $\delta(n)$ و $\tau(n)$

الحل :

$$\tau(3) = 2 \ , \delta(3) = 1 + 3 = 4$$

نظرية (1) :

1) إذا كان p عدد اولي فإن: $\tau(p) = 2$

2) إذا كان p عدد اولي و $\alpha \geq 1$ فإن $\tau(p^{\alpha}) = \alpha + 1$

3) اذا كان $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_r^{\alpha_n}$ فان :

البرهان :

1) قواسم العدد الاولي p هي : 1 و p اذن عددها $\tau(p) = 2 \Leftarrow$

2) قواسم العدد p^{α} هي $1, p, p^2, \cdots, p^{\alpha}$: عددها $\alpha + 1$ إذن

3 τ) دالة ضربية و $(p_i^{\alpha i}, p_j^{\alpha j}) = 1$

$\Longrightarrow \tau(n)$

مثال (3) :

اوجد $\tau(n)$ إذا كان :

1) $n = 21$
2) $n = (2^3)$
3) $n = 20$
4) $n = (2^5 \cdot 3^2 \cdot 7)$

الحل :

1) $\tau(21) = \tau(3 \cdot 7) = \tau(3)\tau(7) = 2 \cdot 2 = 4$
2) $\tau(2^3) = 3 + 1 = 4$
3) $\tau(20) = (5 \cdot 2^2) = 2 \cdot (2 + 1) = 6$

4) $\tau(2^5 \cdot 3^2 \cdot 7) = \tau(2^5)\tau(3^2)\tau(7) = (5+1)(2+1)\cdot 2 = 6 \cdot 3 \cdot 2 =$ 36

نظرية (2) :

1) إذا كان p عدد أولي فإن : $\delta(p) = p + 1$

2) إذا كان p عدد أولي فإن :$\alpha \geq 1$ فإن : $(p^{\alpha}) = \frac{p^{\alpha+1}}{p-1}$

3) إذا كان $n = p_1^{\alpha_1}, p_2^{\alpha_2} \cdots, p_r^{\alpha_r}$فإن: $\delta(n) = \Pi_{i=1}^{r} \frac{p^{\alpha_{i+1}}}{p_i - 1}$

البرهان :

1) قواسم العدد p هي :p, 1

إذن مجموع القواسم $\delta(p) = p + 1$

2) قواسم العدد p^{α} هي : $1, p, p^2, \cdots, p^{\alpha}$ فإن:

$\delta($

3) $\delta(n) = \delta\left(p_1^{\alpha_1}, p_2^{\alpha_2}, \cdots p_r^{\alpha_r}\right) = \delta\left(p_1^{\alpha_1}\right)\delta\left(p_2^{\alpha_2}\right)\cdots\delta\left(p_r^{\alpha_r}\right)$

$$= \frac{p_2^{\alpha_2+1} - 1}{p_2 - 1} \cdots \frac{p_r^{\alpha_r+1} - 1}{p_r - 1} = \Pi_{i=1}^{r} \frac{p_i^{\alpha_i+1} - 1}{p_i - 1} \overset{2}{\Rightarrow} \frac{p_1^{\alpha_1+1} - 1}{p - 1}$$

مثال(4) :

أوجد $\delta(n)$ إذا كان :

1) $n = 6$

2) $n = 15$

3) $n = 60$

الحل :

1) $\delta(n) = \delta(6) = \delta(2 \cdot 3) = 3 \cdot 4 = 12$

2) $\delta(15) = \delta(3 \cdot 5) = (3 + 1)(5 + 1) = 4 \cdot 6 = 24$

3) $\delta(60) = \delta(2^2 \cdot 3 \cdot 5) = \frac{2^{2+1}-1}{2-1} \cdot 4 \cdot 6$

$= 7 \cdot 4 \cdot 6 = 168$

(2-4) التشـــــفير :

تعريف :

التشفير هو عبارة عن سلسلة من التقنيات المستخدمة لتحويل المعلومات إلى تنسيق أخر بديل من الممكن إرجاعها فيما بعد إلى صورتها الأصلية . ويقصد بهذا التنسيق البديل بمصطلح نص الشفرة ويتم إنشاؤه عادة من خلال إستخدام خوارزمية الشفرة ومفتاح الشفرة , وتمثل خورزمية الشفرة بواسطة معادلة رياضية تنطبق على المعلومات المراد تشفيرها .

مفتاح الشفرة هو عبارة عن متغير إضافي يتم إدراجه داخل الخوارزمية لضمان أن نص الشفرة غير مقتبس بإستخدام نفس العملية الحسابية في كل مرة تقوم فيها الخوارزمية بمعالجة المعلومات .

(1-2-4) بعض انواع الشفرات :

أ. شفرة هيل Hill Cipher :

تعتبر شفرة هيل هي اول شفرة نتعامل فيها مع ثلاث حروف في نفس الوقت . وهي تعتمد في عملها على الجبر الخطي ونظرية الاعداد ولكي نستطيع التشفير بها يجب ان يكون جدول الحروف قريب لديك :

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

علينا اولا اختيار المفتاح مثلا كان مكون من 9 احرف سوف نكون مصفوفة 3*3 أي ثلاثة صفوف وثلاثة أعمدة

فمثلا لدي جملة التشفير التالية :

GYBNQKURP بعد إعطاء كل حرف قيمته نقوم بوضعه داخل مصفوفة 3*3 ويكون شكل المصفوفة كالأتي : $\begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix}$

وليكن النص الأصلي هو : A C T وفي حال كان أكبر منذلك يتم التقسيم الى بلوكات وكل واحد يتكون من ثلاث حروف نقوم بوضع النص الأصلي داخل مصفوفة $1 * 3$:

$$\begin{bmatrix} 0 \\ 2 \\ 19 \end{bmatrix}$$

والأن نقوم بضرب المصفوفتين ونأخذ ناتج باقي القسمة mod 26 :

$$\begin{bmatrix} 0 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix} \begin{bmatrix} 0 \\ 2 \\ 19 \end{bmatrix} = \begin{bmatrix} 27 \\ 222 \\ 319 \end{bmatrix} = \begin{bmatrix} 15 \\ 14 \\ 7 \end{bmatrix} \bmod 26$$

اذن الناتج من هذا النص بعد تحويل الأرقام الى حروف هو:

النص المشفر هو P O H

ولفك الشفرة كل ما علينا هو إيجاد معكوس المصفوفة ونقوم بضربه في النص المشفر مع أخذ باقي القسمة على 26

$$\begin{bmatrix} 8 & 5 & 10 \\ 21 & 8 & 21 \\ 21 & 15 & 8 \end{bmatrix} \begin{bmatrix} 15 \\ 14 \\ 7 \end{bmatrix} = \begin{bmatrix} 260 \\ 574 \\ 539 \end{bmatrix} = \begin{bmatrix} 0 \\ 2 \\ 19 \end{bmatrix} \bmod 26$$

وبشكل عام إذا كان لدينا شفرة من نوع هيل فإنه سوف يكون لدينا مصفوفة من النوع $n * n$

الصورة التالية توضح كيفية التشفير وفك الشفرة :

مثال (5) :

على Hill Cipher – 2وهذا يعني أن المصفوفة مكونة من 2*2 تحتوي على حروف اللغة 26 ولكي نستخرج معكوس المصفوفة الصحيح عند الفك يجب أن يكون محدد هذه المصفوفة أولي مع العدد 26 أي أن القاسم المشترك الأكبر لمحددة المصفوفة و 26 يساوي واحد

$$\text{Key : a } 2 \times 2 \text{ matrixofelementsfrom} Z_{26}$$

$$\det \begin{bmatrix} a & b \\ c & d \end{bmatrix} = (ad - bc) \text{isrelativleyprimeto 26}$$

Encrytion :

يكون التشفير عن طريق ضرب المصفوفة مع أول حرفين من النص الأصلي مع أخذ ناتج باقي القسمة على 26

$$\begin{bmatrix} c_1 \\ c_2 \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} p_1 \\ p_2 \end{bmatrix} \text{mod 26}$$

Thatis :

$$c_1 = (a \cdot p_1 + b \cdot p_2) \text{mod 26}$$

$$c_2 = (c \cdot p_1 + d \cdot p_2) \text{mod 26}$$

فك التشفير يتم عن طريق ضرب معكوس المصفوفة مع أول حرفين من النص المشفر وأخذ الناتج في عملية باقي القسمة على 26

$$\begin{bmatrix} p_1 \\ p_2 \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}^{-1} \begin{bmatrix} c_1 \\ c_2 \end{bmatrix} \text{ (mod 26)}$$

إيجاد معكوس المصفوفة 2×2 :

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}^{-1} = d^{-1} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$$

Determinant of a matrix A:

$$\text{if } A(a_{ij}) \text{is } 2 \times 2 . \text{ then det A} = a_{11} a_{22} - a_{12} a_{21}$$

والأن لإيجاد معكوس d يجب ان يتوفر لدينا معكوس ما بحيث حاصل ضرب هذا المعكوس مع d مع أخذ ناتج باقي القسمة على 26 ليكون الباقي واحد .

$$d * d' = 1 \text{ (mod 26)}$$

الجدول التالي يبين معكوس الأعداد الأولية من 3 الى 25 :

a	3	5	7	9	11	15	17	19	21	23	25
a	9	21	15	3	19	7	23	11	5	17	25

مثال(6):

للتشفير وفك التشفير:

تم إختيار المصفوفة والتأكد من أن لها معكوس $A = \begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix}$

$$\det A = 9 \times 7 - 4 \times 5 = 43 \equiv 17 (\mathrm{mod}\ 26)$$

ثم إيجاد المعكوس: $17^{-1} \mod 26 = 23$

$$A^{-1} = 23 \begin{bmatrix} 7 & -4 \\ -5 & 9 \end{bmatrix} \equiv \begin{bmatrix} 5 & 12 \\ 15 & 25 \end{bmatrix} \mathrm{mod}\ 26$$

هنا تم تشفير الحرفين f o والناتج 5 14 . x t → "f o"

$$\begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix} \begin{bmatrix} 5 \\ 14 \end{bmatrix} \equiv \begin{bmatrix} 23 \\ 19 \end{bmatrix}$$

قم بضرب الناتج مع معكوس المصفوفة وسوف يخرج الناتج الأصلي

23 19 → "x t "

بعض الخوارزميات :

إيجاد القاسم المشترك الأعظم : (G C D)

تم كتابة أكثر من طريقة لتطبيق هذه الخوارزمية ومنها الطريقة العادية

```
int classcal_ GCD (int x . int y ){
        int small i
        if ( x < y)
        small i = x ;
        else
        small i = y ;
while (x% small ! = 0 ‖ y% small ! = 0)
```

```
small – – ;
return small ; }
```

حل أخر بواسطة خوارزمية إقليدس :

تم كتابة ثلاثة تطبيقات (implementation) لها الأول والثاني متشابهان والثالث تم فيه إستخدام مفهوم النداء الذاتي :

```
int Euclid_ GCD (int x . int y) {
int tmp = 0 ;
while (x > 0)
if ( x < y ){
tmp = x ;
x = y ;
y = tmp ;
}
x = x – y }
return y ;
}
```

الحل بواسطة النداء الذاتي :

```
int Euclid _GCD_ Recursion (int x . int y )
{
if (y = = 0)
return x ;
eles
```

```
return Euclid _GCD_ (y. x%);
}
```

إختبار أولية العدد بإستخدام Trial Division :

```
pool  i = prime (int  n){
for (int i = 2 ; 1 < = sqrt (n); i + +)
if( n% i = = 0)
return flas ;
it's prime  number
return  true ;
}
```

ب . شفرة Affine Cipher :

التشفير بطريقة Affine Cipher " التشفير المختلط " سميت بهذا الإسم لأنها تخلط بين نوعين من التشفير الأول هو شفرة قيصر والثاني شفرة الضرب.

ففي شفرة قيصر يكون التشفير كالأتي :

(وهنا key تعتبر الإزاحة)

وفي شفرة الضرب يكون التشفير كالأتي :

والأن في شفرة Affine جمعت بين الطريقتين حيث يتم الجمع والضرب

ولكن هنالك شرط وهو ان تكون m . n أوليان وفي حالة لم ينفذ الشرط فإنه يمكن فك الشفرة ولكن لفك الشفرة يجب أن نوجد معكوس m وفي حال كانت GCD(m . n) = 1 فإنه يمكن ايجاد المعكوس .

ولفك التشفير نتبع $p = m^{\circ} * (c - key \pmod n)$.

مثال (7) :

نريد تشفير العبارة W A R L O S T والمفتاح يساوي 10 ومعامل الضرب m يساوي 7 .

قبل ان نبدأ في التشفير يجب ان نتاكد من ان هنالك معكوس ل m وحتى يمكن فك الشفرة ناخذ المشترك الاعظم ل m . n و $n = 26$. $GCD(7.26) = 1$ اذا نتاكد ان هنالك معكوس ل m .

نضع جدول الحروف حتى يساعدنا في معرفة موقع الحرف :

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

الأن بعد تحويل النص الأصلي الى أرقام يكون بهذا الشكل : 19 18 14 11 17 0 22

الأن نبدأ تطبيق القانون : $C = m * p + key \pmod{26}$

$$c_1 = 7 * 22 + 10 \pmod{26} = 8$$

$$c_2 = 7 * 0 + 10 \pmod{26} = 10$$

$$c_3 = 7 * 17 + 10 \pmod{26} = 25$$

$$c_4 = 7 * 11 + 10 \pmod{26} = 9$$

$$c_5 = 7 * 14 + 10 \pmod{26} = 4$$

$$c_6 = 7 * 18 + 10 \pmod{26} = 6$$

$$c_7 = 7 * 19 + 10 \pmod{26} = 13$$

وتكون النتيجة بعد التشفير هي : 13 6 4 9 25 10 8 ونقوم بتحويلها إلى حروف ليصبح لدينا النص :

I K Z J E G N .

ولفك التشفير يجب أن نعرف ماهو معكوس m حتى نستطيع التطبيق في القانون التالي :

$$p = m^{\circ} * (c - key) \pmod{26}.$$

نوجد المعكوس عن طريق خوارزمية إقليدس وندخل العددين 7 و26 في الخوارزمية لينتج لدينا المعكوس 15 . ونطبق في القانون $p_1 = 15 * (8 - 10) \bmod 26 = 22$

$$p_2 = 15 * (10 - 10) \bmod 26 = 0$$

$$p_3 = 15 * (25 - 10) \bmod 26 = 17$$

$$p_4 = 15 * (9 - 10) \bmod 26 = 11$$

$$p_5 = 15 * (4 - 10) \bmod 26 = 14$$

$$p_6 = 15 * (6 - 10) \bmod 26 = 18$$

$$p_7 = 15 * (13 - 10) \bmod 26 = 19$$

إذن النص الأصلي هو 19 18 14 11 17 0 22 وبعد تحويله إلى حروف يصبح W A R L O S T وهو المطلوب .

النتـــائج :

(1) تعرفنا على أن خوارزمية إقليدس يمكن إستخدامها في إيجاد القاسم المشترك الأعظم لأي عددين صحيحين .
(2) استنتجنا أن علاقة التطابق علاقة تكافؤ .
(3)توصلنا على أنه توجد بعض التطابقات لايوجد لها حل في حالة $(n \nmid ax - b)$ بالتجربة في مجموعة الباقي التامة قياس n.
(4) وجدنا أنه يمكن إستخدام دالة أويلر لتبسيط حل التطابق في حالةالمقياسn كبير .
(5) تمكنا من إستخدام مفهومي القاسم المشترك الأعظم والتطابق في التشفير .

التوصيـــات :

(1)الإهتمام بعمل بحوث ودراسات في نظرية الأعداد .
(2) توفير مصادر ومراجع مختلفة في نظرية الاعداد .
(3)التوسع في دراسة التطابق وتطبيقاته .
(4) كتابة بحوث في نظرية الأعداد وعلاقتها بالتشفير .

المراجــع :

1) مدخل إلى نظرية الأعداد - ترجمة : د. رمضان محمد جهيمة , د. إبراهيم رياض
2) مقدمة في نظرية الأعداد - د . فوزي أحمد الذكير , د. معروف عبدالرحمن سمحان , جامعة الملك سعود – المملكة العربية السعودية .7 / 1 /1414 ه الموافق : 27 /6/ 1993 م.
3) مقدمة في نظرية الأعداد :أ.د. فالح بن عمران بن محمد الدوسري , جامعة أم القرى – مكة المكرمة – الطبعة الأولى : 1428 ه – الموافق : 2007 م .
4) نظم تأمين الشبكات : مرجع شامل لنظم تأمين الشبكات - ACTIV – DEFENSE , الناشر الأجنبي : سايبكس كرس برنتون , كامسرون هانت, الطبعة الأولى – 2003 م , الطبعة الأجنبية – 2001م.
5) مقدمة في التشفير بالطرق الكلاسيكية - د. وجدي عصام عبدالرحيم .