

تقرير حلقة بحث في مادة الرياضيات بعنوان :

التطابقات



تقديم الطلاب :سليم جليط

الصف: العاشر

تاريخ : 2016\2015 .م

اشراف: أ.رشا عثمان

**المقدمة** :

الأعداد هي لغة العلم وأفضل وسيلة للتعبير عنه فهي الرموز والأرقام هي أشكال تكتب بها رموز الرياضيات والحساب (نظرية الأعداد). علم العدد جانبه النظري يعالج الأرقام والأعداد أي مراتبها والنسب التي بينها وتكرارها على نسق معين , أنواعها وكيفية بنائها ودراسة خواصها والعلاقات التي بينها , وجانبه العملي يتناول بالحسبان, أي معرفة المطلوب بالعمليات الأربعة وتكثر الحاجة إلى الحسبان باستخراج المطلوب من صلة بعض الأشياء ببعض ولولا الحسبان لعجز الإنسان عن نسج ما يدور من أحداث الزمن ولما وجدت التقاويم والنقود كما قال جاوس : "الرياضيات ملكة العلوم , والحساب ملك الرياضيات" ولذلك أقدم هذا البحث العلمي الذي يجيب عن عدة تساؤلات.

**إشكالية البحث:**

 ما هو التطابق وما خواصه ؟

وما النظريات التي تعتمد عليه ؟

وبما يمكن أن نستخدم التطابق؟

الفصل الأول :

 التطابقات Congruences

التطابق هو تعبير آخر لمفهوم قابلية الهندسة قدّم من قبل العالم الألماني يوهان كارل فريدريش غاوس $Johann Carl Friedrich Gauss$ بطريقة جعلته أداة فعالة لتسهيل البراهين ووسيلة أخرى لدراسة نظرية الأعداد

تعريف 1-1

يقال عنa أنه يطابق أو يوافق bقياس(modulo) nونكتب$a ≡b(mod n)$

أوbn Ξ*a*

إذا كان n ϵ N\*  , a,b ϵ Z و إذا كان a ­b يقبل القسمة على n

أماإذا كان a لا يطابق b قياسn, فيعبر عن ذلك بالشكل$a ≅b(mod n)$

مثال(1) :

)أ) $ 37≡1 \left(mod 2\right)$لان 37 ­ 1 = 36 و يقبل القسمة على 2

(ب) $31≅2 (mod 2)$, لان 2931 ­ 2 = ولا يقبل القسمة على 2

مبرهنة 1-1 :

 التطابق قياس n علاقة تكافؤ على Z . أيأن :

(أ). $a ≡a(mod n)$, لكل a ϵ Z

(ب). إذا كان a,b ϵ Z , وكان $a ≡b(mod n)$ , فان $b ≡a(mod n)$

(ج). إذا كان a,b,c ϵz , وكان $b≡c\left(mod n\right),a ≡b(mod n)$فان

$$a ≡c(mod n)$$

البرهان :

1. بما أن$a ­ a=0$ لكل $a\in Z$وبما أنn\0 لكل 0≠ n اذاً

$a≡ a$ لكل $a\in Z$

1. بما أن$a ≡b(mod n)$ اذاً n\a-b , وعليه يوجد $r\in Z$بحيث أنa-b = nr وعليه , فان b-a = n(-r) , -r ϵ z وبالتالي فان

و $b≡c\left(mod n\right)$

(ج) بما أن$a ≡b(mod n)$ و $b≡c\left(mod n\right)$ اذاً يوجد r,sϵ Z بحيث أنa-b = nr , b-c = ns , ومنها نجد أنa-c = n(r+s) لكن r,sϵ Zاذاً
$$a ≡c(mod n)$$

مبرهنة 1-2 :

إذا كان a,b,c,d ϵZ وكان n ϵN\* , و $a ≡ b (mod n)$ و

$c ≡ d (mod n)$ فان :

1. $ a \mp c≡b \mp d (mod n)$
2. $ac≡bd (mod n)$

البرهان :

بما أن :

1. $a ≡ b (mod n) \rightarrow ∃x ϵ Z : a = b + nx $
2. $c ≡ d (mod n) \rightarrow ∃y ϵ Z : c = d + ny $

اذاً بجمع المعادلتين (1) و (2) ينتج أن$a+c= b+d+n(x+y) $ لكن $x + y ϵ Z$اذاً$a+c≡b+d \left(mod n\right)$

 وبطرح المعادلتين ينتج أن$a-c=b-d+n (x-y) $ لكن $x-y ϵ Z$اذاً$a-c≡b-d \left(mod n\right)$

وبضرب المعادلتين ينتج أن$ac=bd+n(by+xd+nxy)$ لكن

$by+xd+nxy ϵ Z$*اذاً*$ac ≡bd (mod n)$

*مبرهنة 1-3 :*

*إذا كان* $a≡b (mod n)$ *فإن*

1. $a+e ≡b+e \left(mod n\right)$ *لكل* $e ϵ Z$
2. $ae ≡be \left(mod n\right)$ *لكل* $e ϵ Z$

*البرهان :*

*بما أن*$a ≡b (mod n)$ *, و* $e ≡e (mod n)$ *لكل*$ e ϵ Z$*اذاً حسب*

*مبرهنة 1-2*$a+e ≡b+e \left(mod n\right)$ *لكل* $e ϵ Z$

*و* $ae ≡be \left(mod n\right)$ *لكل* $e ϵ Z$

*ملاحظة :*

*إذا كان* $ac≡bc (mod n)$ فليس بالضرورة أن يكون

$a ≡b (mod n)$ كما يوضح ذلك المثال الآتي : $28 ≡24 (mod 2)$ بينما $7 ≅6 (mod 2)$

إذا كان $a ≡b (mod n)$ , وكان *m ϵ N\*فإن*b m (mod )*a m ≡*

*مثال (2) :*

أثبت أن : $12233×455679+87653^{3}$ يقبل القسمة على $4$

نعلم أن العدد يقبل القسمة على $4$ اذا كانت مرتبة الآحاد والعشرات تقبل القسمة على $4$ اذا $12233≡33≡1 (mod 4)$ وبذات الطريقة نجد

 ,$455679≡79≡3(mod 4)87653≡53≡1(mod 4)$ وبالتالي نجد أن $87653^{3}≡1^{3}≡1(mod 4)$ ومما سبق نجد ان

***الفصل الثاني:***

*التطابقات الخطية ومبرهنة الباقي الصينية*

*تعريف 2-1 :*

*يقال عن علاقة تطابق أنها علاقة تطابق خطي بمتغير واحد إذا كان*

$$ax ≡b (mod n)$$

*ويقال عن* $x\_{1} ϵ Z$ *انه حل للتطابق اذا كان* $ax\_{1} ≡b (mod n)$ *ويقال عن* $x\_{1},x\_{2} ϵ Z$ *أنهما متطابقان (congruent solutions) إذا كان*$x\_{1} ≡ x\_{2} (mod n) $ *واذا كان غير ذلك فيقال عن الحلان انهما غير متطابقان (incongruent solutions)*

*مثال (1) :*

1. *اذا كان* $3x ≡1 (mod 4)$*فإن 3,7 حلان متطابقان لذلك التطابق لأن* $3×3 ≡1 (mod 4)$ *و* $3×7 ≡1 (mod 4)$ *و* $7 ≡3 (mod 4)$
2. *إذا كان* $2x ≡6 (mod 8)$ *فإن 3,7 حلان غير متطابقان لذلك التطابق لأن* $2×3 ≡6 (mod 8)$ *و* $2×7 ≡6 (mod 8)$ *بينما* $7 ≅3 (mod 8)$

 *ملاحظة :*

*اذا كان (a,n) = 1 فإن للتطابق الخطي* $ax ≡b (mod n)$ *حل وحيد قياس* $n$

*تعريف 2-2 :*

*يقال عن* $b\in Z$ *أنه معكوس أو نظير ضربي للعدد* $a\in Z$ *قياس* $n$ *إذا كان* $ab ≡1 (mod n)$

*مثال (2) :*

$2×3 ≡1 (mod 5)$*اذاً* $2$ *معكوس ضربي للعدد* $ 3$*قياس* $5$

*نتيجة (1) :*

*يكون للعدد* $a\in Z$ *معكوساً ضربياً قياس* $n$ *اذا وفقط اذا كان* $\left(a,n\right)=1$

*البرهان :*

*نفرض* $b\in Z$ *هو المعكوس الضربي للعدد* $a$ *قياس* $n$ *اذاً* $ab≡1 (mod n)$ *وعليه فإن*$ n\ ab-1 $وبالتال $ab-1=nr $ومنه $ab+n\left(-r\right)=1$ وبالتالي $\left(a,n\right)=1$

مبرهنة 2-1 : ليكن $d=(a,n)$

$$ax ≡b (mod n)$$

1. اذا يوجد للتطابق الخطي حل اذا كان $d\ b $
2. *اذا كان* $d\b$ *فإن للتطابق الخطي* $d$ *من الحلول غير المتطابقة قياس* $n$

*البرهان :*

1. نفرض ان $x$ حل للتطابق الخطي اذاً $n\ax-b$ لكن $d\n$ *و* $d\a$ *اذاً* $d\b$
2. نفرض ان $\frac{a}{d}=c,\frac{n}{d}=m,\frac{b}{d}=e$ *اذاً*

$$ ax≡b\left(mod n\right)⇒ cx≡e\left(mod m\right), \left(c,m\right)=1$$

*وعليه يوجد حل وحيد* $x≡x\_{0}(mod m)$ *للتطابق الخطي*

$cx≡e(mod m)$ *لكن* $0≡mr(mod m)$ *لكل* $r\in Z$ *اذاً*

$x≡x\_{0}+mr(mod m)$لكن ليس كل الأعداد صحيحة على الشكل $x\_{0}+mr$ متطابقة قياس $n$ اذا الاعداد غير المتطابقة قياس $n$ *تمثل الحلول غير المتطابقة للتطابق الخطي* $ax≡b\left(mod n\right)$ *فإذا كان*

$$x\_{0}+rm≡x0+sm\left(mod m\right)⇒rm≡sm(mod n)$$

$⇒r≡s(mod d)$*وعليه اذا كان* $r\in D=\{0,1,……,d-1\}$ *فإن* $\left(m,d\right)=1$*و*$R=\{mr+x\_{0}|r\in D\}$*نظام بواقي تام قياس* $d$ *وعليه يوجد* $d$ *من الحلول غير المتطابقة وهي* $x\_{0},\{x\_{0}+m\},\{x\_{0}+2m\}…..\{x\_{0}+\left(d-1\right)m\}$ *ولكن* $m=\frac{n}{d}$ *اذا مجموعة الحلول غير المتطابقة هي* $x\_{0, }x\_{0}+\frac{n}{d} , x\_{0}+ \frac{2n}{d}…….x\_{0}+\frac{\left(d-1\right)n}{d}$

*مثال :*

*اوجد الحلول غير المتطابقة للتطابق الخطي* $32x ≡8 (mod 42)$

*الحل:*

*بما ان* $\left(32,84\right)=2$ *و* $2\8$ *اذا يوجد حلان غير متطابقان للتطابق الخطي السابق*

$32x≡8\left(mod 42\right)⇒ 16x ≡4 (mod 21)$*و حيث أن* $\left(16,21\right)=1$*اذا يوجد حل للتطابق والآن نضرب الطرفين بالنظير الضربي للعدد* $16x ≡4\left(16\right)^{-1} (mod 21)$ *لكن* $16^{-1}=4 \in Z\_{21}$*اذاً*

$x\_{0} ≡16 (mod 21)$ وبما أن مجموعة الحلول تنتمي الى

$R=\{ x\_{0}+21r\}$ نجد أن $x=16,37$

*مبرهنة 2-2 :*

*إذا كان* $a\_{1},a\_{2},n,r\in Z$ *و* $n,r>0$ *فيوجد حل لنظام التطابق*

1. $X≡a\_{1} (mod n) $
2. $X≡a\_{2} (mod r)$

*اذا كان* $\left(n,r\right)\(a\_{2}-a\_{1})$

*البرهان :*

*بما ان* $X≡a\_{1} (mod n) $ *اذا يوجد* $s\in Z$ *بحيث ان* $X= a\_{1}+ns$

*وبالتعويض في B ينتج ان* $a\_{1}+ns≡a\_{2} (mod r)$ *ومنها نجد ان*

$$ns≡ a\_{2}-a\_{1} (mod r)$$

*اذا يوجد حل للتطابق اذا كان* $\left(n,r\right)\(a\_{2}-a\_{1})$

*ويمكن ان تستخدم هذه المبرهنة لأكثر من تطابقين خطيين*

*مثال : حل النظام التالي*

1. $X≡1 (mod 2)$
2. $X ≡2 (mod 3)$
3. $X≡4 (mod 7)$

*الحل :*

*من التطابق*$a$ *نجد ان* $X=1+2r (d$ *حيث* $r\in Z$ *وبتعويض* $d$ *في* $b$ *نجد ان* $1+2r≡2\left(mod 3\right)$ وبالتالي $2r ≡1 (mod 3)$ ومنه $r ≡2 \left(mod 3\right)⇐r=2+3t (e$ وبتعويض $e$*في* $d$ *نجد ان* $X=5+6t (f$ *حيث* $t\in Z$ *وبتعويض* $f$ *في* $c$ *نجد ان*

$5+6t ≡4 (mod 7)⇐6t ≡6(mod 7)t≡1 mod 7⇐$ *وبالتالي* $t=1+7n (g$ *حيث* $n\in Z$ *والان بتعويض* $g$ *في* $f$ *نجد ان* $X=11+42n$ *ومنه* $X≡11(mod 42)$

***الفصل الثالث:***

 *البواقي التربيعية*

*تعريف 3-1 :*

*اذا كان* $ n \in Z^{+}$ *فيقال عن عدد* $a \in Z$ *أنه باقي تربيعي قياس n , اذا كان (a,n)=1 ويوجد*$ x \in Z$ *بحيث*$x^{2}≡a (mod n)$

اما اذا كان (a,n)=1 ولا يوجد $x \in Z$ بحيث ان $x^{2}≡a (mod n)$ فيقال عن a انه باقي غير تربيعي قياس n

إذا كان a باقياً تربيعياً قياس n فيعبر عن ذلك بالشكل aRn أما إذا كان a باقياً غير تربيعي قياس n فيعبر عنه بالشكل aNn

مثال(1) :

اذا كان n=5 , فان$2^{2}≡4 \left(mod 5\right)$, $1^{2}≡1 \left(mod 5\right)$ و (1,5)=(4,5)=1 اذاً aR5 لكل$ a \in \{1,4\}$ و aN5 لكل$ a \in \{2,3\}$

نلاحظ ان $\left|\left\{a\in Z\_{5}^{\*}:aR\_{5}\right\}\right|=\left|\left\{ a\in Z\_{5}^{\*}:aN\_{5}\right\}\right|=\frac{5-1}{2}=2$

مثال(2) :

اذا كان n=9 , فان (1,9)=(2,9)=(4,9)=(5,9)=(7,9)=(8,9)=1 و

$2^{2}≡4 \left(mod 9\right)$ , $1^{2}≡1 \left(mod 9\right)$ , $4^{2}≡7 \left(mod 9\right)$ إذاً

aR9 لكل $a \in \{1,4,7\}$ اما aN9 فلكل $a \in \{2,5,8\}$

نلاحظ ان $\left|\left\{a\in Z\_{9}^{\*}:aR\_{9}\right\}\right|=\left|\left\{ a\in Z\_{9}^{\*}:aN\_{9}\right\}\right|=\frac{3(3-1)}{2}=3$

وبصورة عامة اذا كان $n= \prod\_{i=1 }^{r}p\_{i}^{e\_{i}}$ عدداً فردياً صحيحاً

فإن $\frac{ɸ(n)}{2^{r}}$ = $\left|\left\{a\in Z\_{n}^{\*}:aR\_{n}\right\}\right|$

واذا كان p عدداً أولياً فردياً , (a,p)=1 فإن

1. $a^{\frac{p-1}{2}}≡1 \left(mod n\right) \leftrightarrow aR\_{p}$
2. $a^{\frac{p-1}{2}}≡-1 \left(mod n\right) \leftrightarrow aN\_{p}$

تعريف 3-2 :

اذا كان p عدداً أولياً فردياً وكان (a,p)=1 فيعرف رمز لجندر (a/p) كالآتي

$$(a\p) \left\{\begin{array}{c}1 aR\_{p}كان اذا\\-1 aN\_{p}كان اذا\\0 a≡0 \left(mod p\right)كان اذا\end{array}\right.$$

مثال(3) :

إذا كان p=7 فإن (1/7)=(2/7)=(4/7)=1, لأن كلاً من 1,2,4 باقي تربيعي قياس7 اما (3/7)=(5/7)=(6/7)=-1 , لأن كلاً من 3,5,6 باقي غير تربيعي قياس 7

بعض الخواص لرمز لجندر

اذا كان p عدداً أولياً فردياً وكان $ a,b \in Z$, (a,p)=(b,p)=1فإن :

1. $\left(a/p\right)≡ a^{\frac{p-1}{2}} (mod p)$
2. اذا كان $a ≡b (mod p)$ , فإن (a/p)=(b/p)
3. (a2/p) = 1
4. (ab/p)=(a/p)(b/p)
5. (1/p)=1 , (-1/p) = $(-1)^{\frac{p-1}{2}}$
6. (ab2/p) = (a/p)

مثال (4) :

أثبت ان للتطابق $x^{2}≡-38(mod 17)$ حل

الحل :

بما ان $17$ عدد اولي اذاً $\left(-1/p\right)=(-1)^{\frac{17-1}{2}}=1 $ *حسب الخاصة (ج) اذاً*

$\left(-38/17\right)=\left(-1/17\right)\left(38/17\right)=(38/17)$*لكن* $38≡4mod17$ *وبالتالي* $\left(38/17\right) = (4/17)$ *حسب الخاصة (ب) لكن*

$\left(4/17\right)=(2^{2}/17)=1$ *حسب الخاصة (ت) اذاً* $\left(38/17\right)=1$ *ومنه* $38R\_{17}$ *وبالتالي فإن للتطابق* $x^{2}≡-38(mod 17)$ *حل*

نتيجة : اذا كان p عدداً أولياً فردياً , فإن

 $(-1/p) = \left\{\begin{array}{c} 1p≡1(mod 4) \\-1 p≡3(mod 4)\end{array}\right.$

البرهان :

إذا كان p=4m+1 فإن $\frac{p-1}{2}=2m$ عدد زوجي ولكن

(-1/p) =$(-1)^{\frac{p-1}{2}}=(-1)^{2m}=1 $ أما ا*ذا كان p=4m+3 فإن* $\frac{p-1}{2}=2m+1$ *عدد فردي وبالتالي*(-1/p) =$(-1)^{\frac{p-1}{2}}=(-1)^{2m+1}=-1$

الخاتمة :

وبختام هذا البحث نكون قد تعرفنا:

1. على التطابقات ودرسنا خواصها وميزاتها كافة
2. على التطابقات الخطية
3. كيفية حل التطابقات الخطية
4. مبرهنة البواقي الصينية والبواقي التربيعية اللتان تعتمدان على فكرة التطابقات بشكل اساسي ودرسنا حالاتها كافة

والآن وبعد دراسة هذا البحث سيصبح القارئ قادر على حل مسائل من نوع:

1. ايجاد باقي قسمة عدد على عدد آخر إثب
2. ات قابلية قسمة عدد على عدد آخر
3. تحديد خانة الآحاد والعشرات لعدد ما
4. ايجاد حل للتطابقات الخطية
5. اختبار وجود او عدم وجود حل لتطابق ما
6. ايجاد حل لنظام تطابقات ما

المصادر والمراجع:

* رشدي راشد : "تاريخ الرياضيات العربية بين الجبر والحساب". مركز دراسات الوحدة العربية بيروت 1989م
* رشدي راشد : التحليل الديوفنطيسي ونظرية الاعداد : موسوعة تاريخ العلوم العربية الجزء الثاني , مركز دراسات الوحدة العربية بيروت 1997م
* فالح بن عمران الدوسري : مقدمة في البنى الجبرية , الطبعة الثانية , توزيع : الدار السعودية للنشر والتوزيع .

D.M.Burton,"Elementary Number Theory" Allyn and Bacon Co. (1980)

O. Ore: "Number Theory and its History" , Dover publications (1980)

H. S. Rose : "A Course in Number Theory" Oxford Science publications (1988)