بسم الله الرحمن الرحيم

وبه نستعين

نظرية أويلر

تمهيد

نظرية أويلر من النظريات المهمة جداً لطلبة الأولمبياد حيث إنها تمكننا من حل أنواع عديدة من الأسئلة المتعلقة بقابلية القسمة. و حقيقةً نظرية أويلر لا فائدة لها بدون معرفة التطابقات في نظرية الأعداد لذلك سأقدم ملخص بسيط لخواص للتطابقات و من أراد المزيد عليه الرجوع إلى المصادر التي سأذكر بعض منها في نهاية هذا المستند – إن شاء الله- .

التطابقات في نظرية الأعداد

تمهيد

إن أول من عرف مفهوم التطابقات هو العالم الألماني (جاوس) حيث قدم لنا طريقة فعالة لتسهيل البراهين و دراسة نظرية الأعداد و يتناول هذا المفهوم – كونه ضمن نظرية الأعداد – دراسة لأنظمة البواقي و قابلية القسمة و التطابقات عموما هو مفهوم واسع سأقتصر - كما ذكرت - في عرض بعض خواصه الأساسية.

تعريف:[1]

- **إذا كان** $n \in \mathbb{N}$ ، $a, b \in \mathbb{Z}$ **فيقال عن** a **أنه يطابق أو يوافق** b **قياس** n ، **و تكتب** $a \equiv b (mod\ n)$ **أو** $a \equiv {}_n b$ **إذا كان** $a - b$ **يقبل القسمة على** n .

لاحظ b باقي قسمة a على n

- **يقال أن** a **قياس** n **يساوي** b ، **و تُكتب** $a(mod\ n) = b$ **إذا كان** $a = nr + b$

(r هو ناتج قسمة $\frac{a}{n}$)

---

[1] الدوسري، أ.د. فالح بن عمران، مقدمة في نظرية الأعداد

أمثلة:

1. $7 \equiv 2 (mod\ 5)$ (لأن ٧-٢=٥ يقبل القسمة على ٥)
2. $-19 \equiv 1(mod\ 4)$ (لأن -١٩-١=-٢٠ تقبل القسمة على ٤)
3. $1 = -19(mod\ 4)$ (لأن ١-(-١٩)= ٢٠ تقبل القسمة على ٤)
4. $31 \not\equiv 5\ (mod\ 12)$ (لأن ٣١-٥=٢٦ لا تقبل القسمة على ١٢)
5. $5(mod\ 3) = 2$ (لأن باقي قسمة ٥ على ٣ هو ٢)
6. $31(mod\ 5) = 1$ (لأن باقي قسمة ٣١ على ٥ هو ١)

خصائص التطابقات:

١. إذا كان $n \in \mathbb{N}$، $a \in \mathbb{Z}$ فإن $a \equiv a\ (mod\ n)$.

٢. إذا كان $n \in \mathbb{N}$، $a, b \in \mathbb{Z}$ وكان $a \equiv b\ (mod\ n)$ فإن $b \equiv a\ (mod\ n)$.

٣. إذا كان $n \in \mathbb{N}$، $a, b, c, d \in \mathbb{Z}$ وكان $a \equiv b\ (mod\ n)$، $c \equiv d\ (mod\ n)$ فإن ١) $a + c \equiv b + d\ (mod\ n)$

٢) $a - c \equiv b - d\ (mod\ n)$

٣) $ac \equiv bd\ (mod\ n)$

٤) $a + e \equiv b + e\ (mod\ n)$ لكل $e \in \mathbb{Z}$.

٥) $ae \equiv be\ (mod\ n)$ لكل $e \in \mathbb{Z}$.

٤. إذا كان $n, m \in \mathbb{N}$، $a, b \in \mathbb{Z}$ $a^m \equiv b^m\ (mod\ n)$.

٥. إذا كان $n, p \in \mathbb{N}$، $a, b \in \mathbb{Z}$، وكان p يقسم n وكان $a \equiv d\ (mod\ n)$ فإن $a \equiv d\ (mod\ p)$

تطبيقات:

١) أوجد باقي قسمة 2^{150} على 7.

الحل

لاحظ أن باقي قسمة 2^3 على 7 هو 1

$2^3 \equiv 1\ (mod\ 7)$ (لماذا أخذنا ٨؟)

$(2^3)^{50} \equiv 1^{50}(mod\ 7)$ (حسب الخاصية ٤)

$2^{150} \equiv 1\ (mod\ 7)$

ومنها يكون الباقي = ١

٢) **أوجد أصغر عدد صحيح موجب** m **بحيث أن** $(79)^2(53)^2 - m$ **يقبل القسمة على** 19 .

الحل

$79 \equiv 3 \pmod{19} \rightarrow A$

$53 \equiv 15 \pmod{19} \rightarrow B$

بضرب $A \cdot B$ **حسب الخاصية ٣/٣ ينتج ...**

$(69)(53) \equiv 45 \pmod{19}$

نربع الطرفين حسب الخاصية ٤ لينتج...

$((69)(53))^2 \equiv 45^2 \pmod{19}$

$(69)^2(53)^2 \equiv 45^2 \pmod{19}$

من خلال تعريف التطابقات فإن $(69)^2(53)^2 - 45^2$ **يقبل القسمة على** 19 **و عليه تكون** $m = 45^2$ **وهو المطلوب.**

لإيجاد باقي القسمة عدد ما a على b بطريقة سهلة باستعمال الآلة الحاسبة نقسم $\frac{a}{b}$ ثم نطرح صحيح العدد الناتج (نأخذ قبل الفاصلة) من العدد الناتج، بعد ذلك نضرب النتيجة في b.

مثال/ أوجد باقي قسمة $\frac{79}{19}$.

١) نقسم باستعمال الحاسبة لينتج لدينا

4.157894737

٢) نطرح 4 من الناتج أي:

4.157894737 - 4=.157894737

٣) نضرب الناتج من (٢) في 19

ليكون الباقي =٣.

و يمكن معرفة باقي القسمة أيضا عن طريق خوارزمية القسمة

تدريبات

١) **بين أن** $\frac{2^{48}-1}{97}$.

٢) **أثبت أن** $a^2 \equiv b^2 (n) \Rightarrow a \equiv b \pmod{n}$.

٣) **أي من العبارات التالية صحيحة (مع ذكر السبب):**

A. $12a \equiv 15 \pmod{35} \Rightarrow 4a \equiv 5 \pmod{7}$

B. $5a \equiv 5b \pmod{7} \Rightarrow a \equiv b \pmod{7}$

C. $3a \equiv b \pmod{4} \Rightarrow 15a \equiv 5b \pmod{20}$

D. $12a \equiv 12b \pmod{15} \Rightarrow a \equiv b \pmod{5}$

٤) **بفرض أن** a **و** b **عددان صحيحان موجبان. بين أنه إذا كان** $4ab - 1$ **يقسم** $(4a^2 - 1)^2$ **فإن** $a = b$

مصادر للبحث:

١- مقدمة في نظرية الأعداد، أ.د فالح بن عمران الدوسري

٢- E. Lines, "A number for your thoughts "Adam Hilger.

٣- Ore: "Number theory and its history".

٤- S. Rose, " a course in number theory" Oxford Science Publication.

نظرية أويلر

بداية سنتعرف على بعض المفاهيم الرياضية المستخدمة:

١- نقول أن العددين a, n عددان أوليان نسبيًا إذا كان العامل المشترك الأكبر لهما هو1.

أمثلة: **(2,1),(17,9),(3,8),(4,3) " كل زوج يمثل عددان أوليان نسبيا"**

٢- φ:أحد رموز المجموعة الخالية و يسمى فاي "*Phi*" و سنستخدمه للدلالة على دالة أويلر.

٣- $\varphi\ (n)$: رمز دالة أويلر و يقرأ "فاي n" و يقصد بها عدد الأعداد الأولية نسبيا مع n و تقع في الفترة بين العدد *1* و العدد n.

أمثلة:

1. $\varphi(6) = 2$ ← أي أن عدد الأعداد الأولية نسبيا مع 6 و التي تقع بين 1و 6 = 2 وهي { ١،٥ }
2. $\varphi(10) = 4$ ← أي أن عدد الأعداد الأولية نسبيا مع 10 و التي تقع بين 1و 10 = 4 وهي { ١،٣،٧،٩ }

و لكن ماذا لو كان العدد n عددا كبيرا (90 مثلا) فكيف يمكن إيجاد عدد الأعداد الأولية نسبيا معه ؟

يمكن ذلك بإتباع الخطوات التالية:

- **تحليل العدد (n) إلى عوامله الأولية .**

أمثلة:

1. $90 = 2 \cdot 3^2 \cdot 5$
2. $400 = 2^4 \cdot 5^2$
3. $15606 = 2 \cdot 3^3 \cdot 17^2$
4. $n = P_1^{a_1} \cdot P_2^{a_2} \cdots P_k^{a_k}$ ← حيث P_1، P_2....P_k أعداد أولية مختلفة، a_1،a_3.... a_3 أعداد صحيحة موجبة.

- **بعد التحليل يمكن بسهولة استخدام القانون التالي:**

$$\varphi(n) = \frac{n}{P_1 \cdot P_2 \cdots P_k}\ (P_1 - 1)(P_2 - 1) \cdots (P_k - 1)$$

لاحظ $\frac{n}{P_1 \cdot P_2 \cdots P_k} \geq 1$

أمثلة (تابع الأمثلة في النقطة الأولى):

1. $\varphi(90) = \frac{90}{2\cdot3\cdot5}\ (2-1)(3-1)(5-1) = 24$
2. $\varphi(400) = \frac{400}{2\cdot5}\ (2-1)(5-1) = 160$
3. $\varphi(15606) = \frac{15606}{2\cdot3\cdot17}\ (2-1)(3-1)(17-1) = 9792$

نص نظرية أويلر:

إذا كان a, n عددان صحيحان موجبان أوليان نسبيا ، إذا سيكون:

$$a^{\varphi^{(n)}} \equiv 1(mod\ n)$$

تطبيقات على نظرية أويلر:

بعد أن تعرفنا على المفاهيم الرياضية فإن تطبيق نظرية أويلر أصبح سهلا.

مثال(أ): **برهن على أن** $17^4 \equiv 1(mod\ 10)$

- **نتأكد من إمكانية تطبيق النظرية:**

١) **نتحقق من أن العددين *17* و*10* مستوفيان لشروط النظرية.**

نلاحظ أن *17* و *10* هما عددان صحيحان موجبان و العامل المشترك الأكبر لهما هو *1*

وعليه فهما محققان للشروط

٢) **نحسب $\varphi(10)$ التي تساوي *4***

- **نطبق النظرية بسهولة.**

$17^{\varphi^{(10)}} \equiv 1(mod\ 10)$

لكن $\varphi^{(10)} = 4$

إذا :

$17^4 \equiv 1(mod\ 10$

مثال(ب): **هل يمكننا إثبات أن $32^4 \equiv 1 (mod\ 10)$ باستخدام نظرية أويلر؟**

لا؛ لإن 32 و 10 ليسا عددان أوليان نسبيًا؛ لأن العامل المشترك الأكبر لهما هو 2 و ليس 1

.

تدريبات

تدريب (١) برهن أن $\varphi(n) = n - 1$ إذا كان n عددا أوليا.

تدريب(٢) برهن أن $\varphi(n) =$ عدد زوجي إذا كان n>2.

تدريب(٣) برهن أن: $\varphi(n) = \frac{}{P_1 \cdot P_2 \cdots P_k} (P_1 - 1)(P_2 - 1) \cdots (P_k - 1)$

تدريب(٤) برهن أن $2^9 \equiv 2\ (mod\ 3)$.

لا تنسونا من صالح الدعاء لي و لوالدي و للجميع