الثلاثاء: 2015/4/14

المحاضرة الخامسة (عملي):

- تمارين صفحة 116 -

(1/116) أعط مثالاً يبين أنه إذا كان $a^2 \equiv b^2 \pmod n$ فليس من الضروري أن يكون $a \equiv b \pmod n$

الحل:

نأخذ $a=5 \quad , \quad b=3, \quad n=16$

$5^2 \equiv 3^2 \pmod{16} \Rightarrow 5 \not\equiv 3 \pmod{16}$

نأخذ $a=3, \quad b=2, \quad n=5$

$3^2 \equiv 2^2 \pmod 5 \Rightarrow 3 \not\equiv 2 \pmod 5$

نأخذ $a=9, \quad b=6 \quad , \quad n=5$

$9^2 \equiv 6^2 \pmod 5 \Rightarrow 9 \not\equiv 6 \pmod 5$

(2/116) أعط مثالاً يبين أنه إذا كان $a^k \equiv b^k \pmod n$ ، فليس من $k \equiv j \pmod n$ الضروري أن يكون

$a^j \equiv b^j \pmod n$

الحل:

نأخذ: $n=3 \; , a=2, \quad b=1, \quad k=2, \; j=5$

مثلاً: $\left.\begin{matrix} 2 \equiv 5 \pmod 3 \\ 2^2 \equiv 1^2 \pmod 3 \end{matrix}\right\} \Rightarrow 2^5 \not\equiv 1^5 \pmod 3$

نأخذ مثال آخر:

$n=5 \; , \quad a=3, \quad b=2 \; , \quad k=6 \; , \quad j=1$

$$729 = 3^6 \equiv 2^6 \pmod 5$$

$$6 \equiv 1 \pmod 5 \Rightarrow \quad \dot{3} \neq \dot{2} \pmod 5$$

(3/116) أثبت أنه إذا كان $(a,n)=1$ فإن الأعداد:
$c, c+a, c+2a, \dots, c+(n-1)a$ تؤلف مجموعة بواقي تامة بالمقاس n
مهما كان $c \in Z$

الحل:

1. نلاحظ أن عدد العناصر يساوي n
2. لنثبت أن العناصر كلٌ غير متطابقة بالمقاس n
لنفرض أنه يوجد عنصران متطابقان بالمقاس n

$$c+at_1 \equiv c+at_2 \pmod n \quad ; \quad 0 \leq t_1 < t_2 \leq n-1$$

لدينا: $c \equiv c \pmod n$ حسب خاصة.

$$c+at_1 - c \equiv c+at_2 - c \pmod n$$

$$at_1 \equiv at_2 \pmod n$$

وبما أن $(a,n)=1$ حسب خاصة:

$$t_1 \equiv t_2 \pmod n$$

وهذا غير ممكن لأن $t_1 \not\equiv t_2 \pmod n$

إذن عدد عناصر المجموعة n عنصراً وهي غير متطابقة بالمقاس n أي تؤلف مجموعة بواقي مختلفة.

4/116) أثبت بطريقة الإستقراء أنه إذا كان a عدداً صحيحاً مردياً فإن

$$a^{2^n} \equiv 1 \pmod{2^{n+2}} \quad ; \quad n \geq 1$$

الحل:

1- خطوة البداية: نثبت أن الصحة من أجل $n = 1$

$$n=1 \Rightarrow a^2 \equiv 1 \pmod{2^3} \quad ; \quad 2^3 = 8$$ محققة

بما أن a فردي فإن مربعه من مضاعفات العدد 8

$$n=2 \Rightarrow a^4 \equiv 1 \pmod{16}$$ محققة

2- خطوة الاستقراء:

نفرض أن العلاقة محققة من أجل $n = k \geq 1$ ونثبت صحتها من أجل $n = k+1$

$$a^{2^k} \equiv 1 \pmod{2^{k+2}}$$

$$a^{2^k} \equiv 1 + M \cdot 2^{k+2}$$

$$\left(a^{2^k}\right)^2 = a^{2^k \cdot 2} = a^{2^{k+1}} = \left(1 + M \cdot 2^{k+2}\right)^2$$ نربع الطرفين

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

$$a^{2^{k+1}} = 1 + M \cdot 2^{(k+1)+2} + M^2 \cdot 2^{2k+4}$$

$$\Rightarrow a^{2^{k+1}} \equiv 1 \pmod{2^{(k+1)+2}}$$

وبالتالي العلاقة محققة من أجل $n = k+1$ وهو صحيح من أجل $n \geq 1$

حيث القوى

$$k+3 < 2k+4$$

$2^{k+3} \mid 2^{2k+4}$

الحد الأخير يطابق الصفر بالمقاس 2^{k+3}

مبرهنة فيرما الصغرى:

إذا كان p عدداً أولياً و $p \nmid a$ فإن:

$$a^{p-1} \equiv 1 \pmod{p}$$

مثال:

نأخذ $p = 3$; $(a, 3) = 1$

$$\Rightarrow a^2 \equiv 1 \pmod{3}$$

$p = 5$, $(a, 5) = 1$

$$\Rightarrow a^4 \equiv 1 \pmod{5}$$

(5/116) إذا كان n عدداً صحيحاً فردياً لا يقبل القسمة على 3 فبرهن أن:

$$72 \mid 5n^6 + 3n^4 - 3n^2 - 5$$

الحل:

لدينا: $72 = 8 \times 9$ و n عدد فردي صحيح

$$n^2 \equiv 1 \pmod{8}$$

$$\left.\begin{aligned} n^4 &\equiv n^2 \pmod{8} \\ 3n^4 &\equiv 3n^2 \pmod{8} \end{aligned}\right\} \Rightarrow 8 \mid 3n^4 - 3n^2$$

$$n^2 \equiv 1 \pmod{8} \Rightarrow n^6 \equiv 1 \pmod{8} \Rightarrow 5n^2 \equiv 5 \pmod{8}$$

$$8 \mid 5n^6 - 5 \Rightarrow 8 \mid 5n^6 - 5 + 3n^4 - 3n^2$$

حسب فيرما:

$(n,3)=1 \Rightarrow n^2 \equiv 1 \pmod 3$

حسب الخاصة (10) (مبرهنة)

$$(n^2)^{3^1} \equiv 1 \pmod{3^{1+1}}$$
$$n^6 \equiv 1 \pmod 9$$
$$\Rightarrow 5n^6 \equiv 5 \pmod 9 \Rightarrow 9 \mid 5n^6 - 5$$

$n^2 \equiv 1 \pmod 3 \Rightarrow n^2 = 1 + M.3$
$\Rightarrow 3n^2 = 3 + M.9$
$\Rightarrow 3n^2 \equiv 3 \pmod 9$
$\Rightarrow 3n^4 \equiv 3n^2 \pmod 9$
$\Rightarrow 9 \mid 3n^4 - 3n^2$
$\Rightarrow 9 \mid 5n^6 - 5 + 3n^4 - 3n^2$

بما أن $(8,9)=1$

$\Rightarrow 9 \times 8 = 72 \mid 5n^6 - 5 + 3n^4 - 3n^2$

انتهت المحاضرة ...