الثلاثاء: 2015/4/29

المحاضرة الثالثة عشر:

مبرهنة فيرما الصغرى:

إذا كان p عدداً أولياً و $p \nmid a$ فإن $a^{p-1} \equiv 1 \pmod p$

البرهان:

لنأخذ المجموعة A_1 وهي مضاعفات العدد a ;

$$A_1 = \{1.a, 2.a, \dots, (p-1)a\}$$

لنرى فيما إذا كانت هذه الأعداد متطابقة فيما بينها بالمقاس p

إن مضاعف a التي تنتمي إلى A_1 غير متطابقة بالمقاس p

لإثبات ذلك نفرض أنها متطابقة ولكن:

$$sa \equiv ta \pmod p \quad ; \quad 0 < s < t \leq p-1$$

حسب الخواص

$$p \nmid a \Rightarrow s \equiv t \pmod p$$

وهذا مستحيل كون s,t غير متطابقة بالمقاس p

وعناصر المجموعة A_1 هي أولية نسبياً مع p

نجد أن كل عنصر من A_1 يطابق عنصر واحد من A بالمقاس p حيث:

$$A = \{1, 2, \dots, p-1\}$$

وهي مجموعة بواقي تامة أيضاً.

نجد أن جداء عناصر المجموعة A_1 يطابق جداء عناصر المجموعة A بالمقاس p الأمر الذي يعطي:

$$1.a \cdot 2a \cdot 3.a \dots (p-1)a \equiv 1.2.3 \dots (p-1) \pmod p$$

$$(p-1)!\, a^{p-1} \equiv (p-1)! \pmod p$$

p أولي مع الأعداد 1, 2, ..., p-1
فإنه أولي مع (p-1)!
حسب الخواص يمكننا الاختصار على (p-1)!
وبالتالي نصل على الصيغة:

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

نتيجة:
إذا كان $p \nmid a$ ، p أولي فإن: $a^p \equiv a \pmod{p}$

إذا كان $p \mid a$ $a^p \equiv 0 \equiv a \pmod{p}$

تمرين:
أثبت أن $5^{38} \equiv 4 \pmod{11}$

الحل:
لدينا $p = 11$ أولي و $38 = 10(3) + 2(4)$

$$\Rightarrow 5^{38} = (5^{10})^3 (5^2)^4$$

ولدينا حسب مبرهنة:
$5^{10} \equiv 1 \pmod{11}$ ولدينا $5^2 \equiv 25 \equiv 3 \pmod{11}$

$$\Rightarrow 5^{38} \equiv (1)^3 (3)^4 \pmod{11}$$
$$\equiv 81 \pmod{11} \equiv 4 \pmod{11}$$

نتيجة:
إذا كان p ، q عددين أوليين مختلفين وكان $(a, p.q) = 1$
وكان:

$a^p \equiv a \pmod q$ ، $a^q \equiv a \pmod p$

فإن:

$$a^{p.q} \equiv a \pmod{p.q}$$

الإثبات:

$$(a^p)^q \equiv a^p \pmod p$$

حسب نيرما $\Rightarrow a^{pq} \equiv a^p \equiv a \pmod p$

$$\Rightarrow p \mid a^{pq} - a$$

كذلك:

$$(a^q)^p \equiv a^q \pmod q$$

$$(a^q)^p \equiv a \pmod q \Rightarrow q \mid a^{pq} - a$$

$$(p,q) = 1 \Rightarrow p.q \mid a^{p.q} - a$$

$$\Rightarrow a^{pq} \equiv a \pmod{p.q}$$

مثال:

أثبت أن: $2^{340} \equiv 1 \pmod{341}$

الحل:

$$2^{341} \equiv 2 \pmod{341}$$

نضع (2)

$$341 = 11 \times 31$$

$$2^{10} \equiv 1 \pmod{11}$$

حسب نيرما

$$2^{31} \equiv (2^{10})^3 \cdot 2 \equiv 2 \pmod{11}$$

$$\Rightarrow \boxed{2^{31} \equiv 2 \pmod{11}}$$

نجد أن:

$$2^{5} \equiv 1 \pmod{31}$$

$$2^{10} \equiv 1^{2} \equiv 1 \pmod{31} \Rightarrow \boxed{2^{11} \equiv 2 \pmod{31}}$$

حسب النتيجة السابقة:

$$2^{11 \times 31} \equiv 2 \pmod{11 \times 31}$$

$$\Rightarrow 2^{340} \equiv 1 \pmod{341}$$

ملاحظة:

نلاحظ من النتيجة السابقة أن مبرهنة فيرما محققة من أجل العدد 341 غير الأولي مما يدل على أن عكس مبرهنة فيرما غير صحيح.

تعريف:

تسمى الأعداد الصحيحة غير الأولية n التي تحقق العلاقة $2^{n} \equiv 2 \pmod{n}$ أشباه الأوليات.

- حقق أثبت أنه يوجد عدد غير منته من أصغر هذه الأعداد هو العدد 341 و يليه العدد 561 .....

مبرهنة ويلسون - ابن الهيثم:

إذا كان p عدداً أولياً فإن:

$$(p-1)! \equiv -1 \pmod{p}$$

أو:

$$p \mid (p-1)! + 1$$

الإثبات:

إذا كان $p=2$ ← $2 \mid 1+1=2$ محققة.

إذا كان $p=3$ ← $3 \mid 2+1=3$ محققة.

لنثبت صحة العلاقة من أجل $p>3$ ، لكل العدد a هو أحد عناصر المجموعة:

$$A=\{2,3,\dots,p-2\}$$

بما أن $a \in A$ فإن $(a,p)=1$ ، أي أنه لكل عنصر a نظير ضربي واحد بالمقاس p وهو ينتمي إلى المجموعة

$$\{0,1,2,\dots,p-1\}$$

وحيث العلاقة:

$$a.a^{*} \equiv 1 \pmod p$$

ولكن من الواضح أنه $a^{*} \neq 0 \pmod p$

كذلك نجد أنه: $a^{*} \not\equiv \mp 1 \pmod p$ لو كان ذلك لوجدنا

$a^{*} \equiv \mp 1 \pmod p$ وأن $a \equiv \mp 1 \pmod p$ ، $a \in A$

وهذا غير محقق

$$a^{*} \not\equiv 1 \pmod p, \quad a^{*} \not\equiv -1 = p-1 \pmod p$$

أي أن:

$$a^{*} \in A$$

وجدنا أن a, a^{*} من A

لو كان $a \equiv a^{*} \pmod p$ لوجدنا:

$$a^2 \equiv 1 \pmod p$$

$$a^2-1 \equiv (a-1)(a+1) \equiv 0 \pmod p$$

$$\Rightarrow \begin{cases} a-1 \equiv 0 \pmod p \Rightarrow a \equiv 1 \pmod p \\ a+1 \equiv 0 \pmod p \Rightarrow a \equiv -1 \pmod p \end{cases}$$

وهذا غير محقق أي أن:

$a^* \neq a \pmod p$

أي أن a^* هو أحد عناصر A ويختلف عن a، مثلاً في حالة

عدد عناصر المجموعة A هي $p-3$ وهو عدد زوجي

حيث أن a في A

a, a^* التي تحقق $\frac{p-3}{2}$ زوج من الأعداد

$$a\,a^* \equiv 1 \pmod p$$

$$1.2.3.4 \dots (p-2) \equiv 1 \pmod p$$

بضرب الطرفين بـ $(p-1)$

$$1.2.3.4 \dots (p-2)(p-1) \equiv (p-1) \pmod p$$

$$(p-1)! \equiv p-1 \equiv -1 \pmod p$$

وهو المطلوب

وانتهت المحاضرة ...