الأربعاء: 2015/4/29

المحاضرة الرابعة عشر

تمرين 21 صفحة 118-

رتب الأعداد $2, 3, 4, \ldots, 21$ في ثنائيات (a,b) بحيث

$$a \cdot b \equiv 1 \pmod{23}$$

الحل:

نظير a بالمقياس 23

$$2 \cdot 12 \equiv 1 \pmod{23}$$
$$3 \cdot 8 \equiv 1 \pmod{23}$$
$$4 \cdot 6 \equiv 1 \pmod{23}$$
$$5 \cdot 14 \equiv 1 \pmod{23}$$
$$7 \cdot 10 \equiv 1 \pmod{23}$$
$$9 \cdot 18 \equiv 1 \pmod{23}$$
$$11 \cdot 21 \equiv 1 \pmod{23}$$
$$13 \cdot 16 \equiv 1 \pmod{23}$$
$$15 \cdot 20 \equiv 1 \pmod{23}$$
$$17 \cdot 19 \equiv 1 \pmod{23}$$

تحقق ويلسون:

$$(23-1)! \equiv -1 \pmod{23}$$
$$22! \equiv -1 \pmod{23}$$

عكس مبرهنة ويلسون - ابن الهيثم:

إذا كان $n \geq 2$ ، وتحقق:

$(n-1)! \equiv -1 \pmod{n}$ فإن n عدداً أولياً

البرهان:

إذا لم تكن n أولياً فله عامل أولي d يقسم n أي:

$d \mid n$ ، $1 < d < n$

$1 < d \leq n-1$ فإن d هو أحد عوامل $(n-1)!$

(1) $d \mid (n-1)!$ و $d \mid n$

و $n \mid (n-1)!+1$

(2) $\Rightarrow d \mid (n-1)!+1$

من (1) و (2) $\Rightarrow d = 1 \Rightarrow n$ أولي.

ملاحظة:

يمكن صياغة مبرهنة ويلسون ابن الهيثم وعكسها معاً على النحو:

n عدد صحيح موجب أولي وأكبر من الواحد $\Longleftrightarrow (n-1)! \equiv -1 \pmod{n}$

تمرين (1) صفحة 114:

أثبت أن $18! \equiv -1 \pmod{437}$

الحل:

$$437 = 19 \times 23$$

حسب ويلسون:

$$22! \equiv -1 \pmod{23}$$

$$18! \equiv -1 \pmod{19} \Rightarrow 19 \mid 18!+1$$

$$22! = 22.21.20.19.18! \equiv (-1)(-2)(-3)(-4)\,18! \pmod{23}$$

$$22! \equiv 18! \pmod{23}$$

$$18! \equiv -1 \pmod{23} \Rightarrow 23 \mid 18!+1$$

و $(19,23) = 1$

$$\Rightarrow (23).(19) = 437 \mid 18!+1$$

ملاحظة:

حيث p عدد أولي. $(p-1)! \equiv -1 \pmod{p}$

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

$$(p, p-1) = 1$$

$$(p-2)! \equiv 1 \pmod{p}$$

$\frac{13}{117}$) أثبت أن باقي قسمة $255!$ على العدد الأولي 257 يساوي 1

الحل:

لنثبت أن: $255! \equiv 1 \pmod{257}$

حسب ويلسون: $(257-1)! \equiv -1 \pmod{257}$

$$256! \equiv -1 \pmod{257}$$

$$\Rightarrow (256)(255)! \equiv -1 \pmod{257}$$

$$256 \equiv -1 \pmod{257}$$

$$255! \equiv 1 \pmod{257}$$

أو

$$(256)(255)! \equiv 256 \pmod{257}$$

يمكن الاختصار حيث $(256, 257) = 1$

$$\Rightarrow 255! \equiv 1 \pmod{257}$$

$\frac{9}{116}$) أوجد باقي قسمة الأعداد 2^{50} و 41^{65} على العدد 7

الحل:

$$41^{65} \equiv k \pmod{7}$$

نريد إيجاد العدد k

حسب فيرما $(41, 7) = 1$

$$\Rightarrow 41^{6} \equiv 1 \pmod{7}$$

$41 \equiv -1 \pmod{7}$; $41^{65} \equiv (41)^{60}(41)^{5} \equiv (-1)^{5} \pmod{7}$

$$41^{65} \equiv -1 \pmod{7}$$

$$41^{65} \equiv 6 \pmod 7 \qquad ; \; k = 6$$

$$2^{50} \equiv k \pmod 7 \; ...$$

$\frac{20}{117}$ أوجد باقي قسمة $2(26!)$ على 29 ؛

الحل:

$$2(26)! \equiv k \pmod{29}$$

$$28! \equiv -1 \pmod{29}$$ حسب ويلسون

أو:

$$27! \equiv 1 \pmod{29}$$

$$28! \equiv (28) \times (27) . 26! \pmod{29}$$

$$28! \equiv (-1)(-2) 26! \equiv 2(26)! \pmod{29}$$

$$2.(26)! \equiv -1 \pmod{29}$$

$$2(26!) \equiv 28 \pmod{29}$$

تتمة حل التمرين السابق:

$$2^6 \equiv 1 \pmod 7$$ حسب فيرما

$$(2^6)^8 \equiv 1^8 \equiv 1 \pmod 7$$

$$2^{48} . 2^2 \equiv 2^2 \equiv 4 \pmod 7$$

$$\Rightarrow 2^{50} \equiv 4 \pmod 7 \qquad ; \; k = 4$$

الفصل الثالث:

- الدوال العددية أو الحسابية وبعض الدوال الخاصة -

تعريف الدالة العددية:
هي الدوال التي منطلقها مجموعة الأعداد الصحيحة الموجبة.

الدالة العددية الضربية:
نقول إن الدالة العددية f دالة ضربية إذا حققت الشرطين.

1) f غير صفرية.

2) $\forall n_1, n_2 \in Z^+$ و $(n_1, n_2) = 1$ فإن

$$f(n_1 \cdot n_2) = f(n_1) \cdot f(n_2)$$

وإذا كان الشرط $(n_1, n_2) \neq 1$ و تحققت الشروط السابقة نسمي دالة ضربية تماماً.

مثال

الدالة المعرفة بـ $f_a(n) = n^a$ ؛ $n \neq 0$ ، $n, a \in Z^{+}$

ضربية تماماً لأن:

1) $n > 0 \Rightarrow f_a(n) \neq 0$

2) $(n_1, n_2) \overset{?}{=} 1 \Rightarrow f_a(n_1 \cdot n_2) = (n_1 \cdot n_2)^a = n_1^a \cdot n_2^a$
$= f_a(n_1) \cdot f_a(n_2)$

وبدون تحقق الشرط $(n_1, n_2) = 1$ محققة.

إذاً الدالة $f_a(n)$ دالة ضربية تماماً.

ملاحظة:

إذا كانت f دالة ضربية فإن $f(1) = 1$

البرهان:

بما أن الدالة f ضربية فإنها غير صفرية أي يوجد عدد n بحيث يكون
$$f(n) \neq 0$$
ولما كان $(n,1)=1$ و
$$f(n) = f(1.n) = f(1).f(n)$$
نختصر $f(n)$ كونها لا يساوي الصفر.
$$\Rightarrow f(1) = 1$$

نتيجة: (1)
يمكن أن نعرف الدالة العددية الضربية بأنها الدالة العددية التي تحقق الشرطين:
1) $f(1) = 1$
2) $\forall n_1, n_2 \in Z^+ ,\ (n_1, n_2) = 1 \Rightarrow f(n_1 . n_2) = f(n_1) . f(n_2)$

نتيجة (2):
إذا كانت f دالة ضربية وكانت العبارة القانونية للعدد n هي:
$n = p_1^{a_1} . p_2^{a_2} \cdots p_r^{a_r}$ فإن:
$$f(n) = f(p_1^{a_1}) . f(p_2^{a_2}) \cdots f(p_r^{a_r})$$
وذلك لأن $p_i^{a_i}$ أولية نسبياً فيما بينها مثنى مثنى.

نتيجة (3):
إذا كانت الدالة f دالة عددية ضربية وكانت الأعداد $n_1, n_2, \ldots, n_r$ أولية نسبياً مثنى مثنى، فإن:
$$f(n_1 . n_2 \cdots n_r) = f(n_1) . f(n_2) \cdots f(n_r)$$

تعريف:
إن العبارة $\sum_{d|n}$ تعني أن المجموع مأخوذ على جميع قواسم العدد n الموجبة.

مثال:

نعين: $\sum_{d|15} f(d)$

$$\sum_{d|15} f(d) = f(1) + f(3) + f(5) + f(15)$$

مبرهنة (1):

إذا كانت f و g دالتين عدديتين فإن:

$$\sum_{\substack{d|m \\ e|n}} f(d).g(e) = \left(\sum_{d|m} f(d)\right).\left(\sum_{e|n} g(e)\right)$$

البرهان:

لنفرض أن $d_1, d_2, \dots, d_s$ هي جميع قواسم العدد m الموجبة.

$e_1, e_2, \dots, e_t$ هي جميع قواسم العدد n الموجبة.

ولكن:

$$\sum_{\substack{d_i|m \\ e_j|n}} f(d_i).g(e_j) = \sum_{i=1}^{s} f(d_i)\, g(e_1) + \sum_{i=1}^{s} f(d_i) g(e_2) + \dots$$

$$+ \sum_{i=1}^{s} f(d_i).g(e_t)$$

$$= \sum_{i=1}^{s} f(d_i)\left[g(e_1) + g(e_2) + \dots + g(e_t) \right]$$

$$= \left(\sum_{i=1}^{s} f(d_i)\right)\left(\sum_{j=1}^{t} g(e_j)\right)$$

$$= \left(\sum_{d|m} f(d)\right)\left(\sum_{e|n} g(e)\right)$$

/ /

تمهيدية (2):
إذا كان n, m عددين صحيحين موجبين وكان $(m,n)=1$ فإن أي قاسم للعدد $n.m$ هو عبارة عن الجداء الوحيد $d_1 d_2$ حيث

$d_1 | n$ ، $d_2 | m$ و $(d_1, d_2) = 1$

مبرهنة:
إذا كانت الدالة العددية f دالة ضربية وإذا عرفت الدالة العددية F على النحو

$$F(n) = \sum_{d|n} f(d)$$

فإن F هي دالة ضربية.

البرهان:

1) $F(1) = \sum_{d|1} f(d) = f(1) = 1$ محقق

2) لنفترض n, m عددين صحيحين موجبين وأن $(n,m)=1$ ولنكتب:

$$F(m.n) = \sum_{d|m.n} f(d) = \sum_{\substack{d_1|m \\ d_2|n}} f(d_1 . d_2)$$

لأن أي قاسم d للجداء $m.n$ يكتب بشكل وحيد كجداء قاسم لـ m لـ d_1 وقاسم لـ n : d_2 حيث $(d_1, d_2) = 1$ ولما كانت f دالة ضربية فإن:

$$F(m.n) = \sum_{\substack{d_1|m \\ d_2|n}} f(d_1). f(d_2)$$

وحسب التمهيدية الأولى فإن:

$$= \Big(\sum_{d_1|m} f(d_1)\Big). \Big(\sum_{d_2|n} f(d_2)\Big)$$

$$= F(m). F(n)$$

إذاً F ضربية.

انتهت المحاضرة...