كلية العلوم

القسم : الرياضيات

السنة : الرابعة

المادة : نظرية الاعداد

المحاضرة : اسئلة مذاكرة /نظري/

{{ مكتبة A to Z }}

Facebook Group : مكتبة A to Z

يمكنكم طلب المحاضرات برسالة نصية (SMS) أو عبر (What's app-Telegram) على الرقم 0931497960

نموذج A

1) أثبت أن العدد $4 \times (18! + 1)$ يقبل القسمة على العدد 23 دون باقي.

2) أثبت أن $p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}$ حيث p و q عددان أوليان فرديان مختلفان.

3) أوجد أصغر عدد صحيح موجب تماماً باقي قسمته على 8 يساوي 7 وباقي قسمته على 9 يساوي 2 وباقي قسمته على 25 يساوي 7.

4) أثبت أن $m = 561$ هو عدد كاريكل، ماذا ستتج؟

نموذج B

1) أثبت أن العدد $(43 \times 651 + 24)$ يقبل القسمة على العدد 67 دون باقي.

2) أثبت أن $Fn = 2^{2^n} + 1$ حيث $Fn \equiv 5 \pmod{12}$ حيث $n \geq 1$.

3) أوجد أصغر عدد صحيح موجب تماماً باقي قسمته على 8 يساوي 2 وباقي قسمته على 11 يساوي 6 وباقي قسمته على 9 يساوي 1.

4) أثبت أن $m = 341$ عدد سيدو أولي للأساس 2، ماذا ستتج؟

نموذج A

الحل 1 لنثبت أن: $23 \mid 4 \times (18! + 1)$

أي لنثبت أن: $4 \times (18! + 1) \equiv 0 \pmod{23}$

23 عدد أولي ـ حسب ويلسون: $(23-1)! \equiv -1 \pmod{23}$

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

$22 \times 21 \times 20 \times 19 \times 18! \equiv -1 \pmod{23}$

$(-1) \times (-2) \times (-3) \times (-4) \times 18! \equiv -1 \pmod{23}$

$24 \times 18! \equiv -1 \pmod{23}$

$(+1) \times 18! \equiv -1 \pmod{23} \rightarrow 18! \equiv -1 \pmod{23}$

$18! + 1 \equiv 0 \pmod{23}$

$4 \times (18! + 1) \equiv 0 \pmod{23}$ ← نضرب طرفي التطابق بـ 4

ومنه $23 \mid 4 \times (18! + 1)$

2 بما أن p و q عددان أوليان فرديان مختلفان فإن: $\gcd(p,q) = 1$

مسبقاً: $p^{q-1} \equiv 1 \pmod{q}$ ..... (1)

$q^{p-1} \equiv 1 \pmod{p}$ ..... (2)

ونعلم أن: $p^{q-1} \equiv 0 \pmod{p}$ ..... (3)

$q^{p-1} \equiv 0 \pmod{q}$ ..... (4)

بجمع (1) مع (4) ..... $* \quad p^{q-1} + q^{p-1} \equiv 1 \pmod{q}$

بجمع (2) مع (3) ..... $** \quad p^{q-1} + q^{p-1} \equiv 1 \pmod{p}$

من * و ** وكون $\gcd(p,q) = 1$ فإن:

$p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}$

TEL:0931497960 - Facebook Group: A to Z مكتبة

3

$x \equiv 7 \pmod 8 \Rightarrow b_1 = 7 \;,\; m_1 = 8$

$x \equiv 2 \pmod 9 \Rightarrow b_2 = 2 \;,\; m_2 = 9$

$x \equiv 7 \pmod{25} \Rightarrow b_3 = 7 \;,\; m_3 = 25$

بما أن $\gcd(m_i, m_j) = 1 \quad \forall\, 1 \le i, j \le 3 \;;\; i \ne j$

فإنه يوجد للجملة حل مشترك وحيد بالنسبة للمقاس

$m = m_1 m_2 m_3 = 8 \times 9 \times 25 = 1800$

وذلك حسب مسألة اللغز الصيني فإن هذا الحل هو:

$x^* = b_1 m'_1 N_1 + b_2 m'_2 N_2 + b_3 m'_3 N_3$

$m'_1 = \frac{m}{m_1} = 225 \;,\; m'_2 = \frac{m}{m_2} = 200 \;,\; m'_3 = \frac{m}{m_3} = 72$

N_1 : هو المعكوس الضربي لـ m'_1 بالنسبة للمقاس m_1 :

$\phi(m_1) = \phi(8) = 8\left(1 - \frac{1}{2}\right) = 4$

$(m'_1)^{\phi(m_1)-1} = (225)^{4-1} = (225)^3 \equiv 1^3 \pmod 8 \equiv 1 \pmod 8$

بالتالي $N_1 = 1$

N_2 : هو المعكوس الضربي لـ m'_2 بالنسبة للمقاس m_2 :

$\phi(m_2) = \phi(9) = 9\left(1 - \frac{1}{3}\right) = 6$

$(m'_2)^{\phi(m_2)-1} = (200)^{6-1} = (200)^5 \equiv 2^5 \pmod 9 \equiv 5 \pmod 9$

بالتالي $N_2 = 5$

N_3 : هو المعكوس الضربي لـ m'_3 بالنسبة للمقاس m_3 :

$\phi(m_3) = \phi(25) = 25\left(1 - \frac{1}{5}\right) = 20$

$(m'_3)^{\phi(m_3)-1} = (72)^{20-1} = (72)^{19} \equiv (22)^{19} \pmod{25}$

$\equiv 22^1 \cdot (22)^{18} \pmod{25} \equiv 22 \times 14 \pmod{25}$

$\equiv 8 \pmod{25}$ بالتالي $N_3 = 8$

TEL:0931497960 - Facebook Group: A to Z مكتبة

$x^* = 7 \times 225 \times 1 + 2 \times 200 \times 5 + 7 \times 72 \times 8 = 7607$

$x^* \equiv 407 \pmod{1800}$ فالعدد 11 المطلوب 407

4) حتى يكون $m = 561$ هو عدد كارميكل يجب تحقق أنه:

من أجل كل عدد صحيح a يحقق: $gcd(a, m) = 1$

يتحقق: $a^{m-1} \equiv 1 \pmod{m}$

أي لنثبت: $a^{560} \equiv 1 \pmod{561}$

لدينا $561 = 3 \times 11 \times 17$ ومن أجل:

$gcd(a, 561) = 1$ فإن:

$gcd(a, 3) = gcd(a, 11) = gcd(a, 17) = 1$

$gcd(a, 3) = 1$ ونرما $a^{3-1} = a^2 \equiv 1 \pmod{3}$

$(a^2)^{280} \equiv 1^{280} \pmod{3}$

$a^{560} \equiv 1 \pmod{3}$ ... (1)

$gcd(a, 11) = 1$ ونرما $a^{11-1} = a^{10} \equiv 1 \pmod{11}$

$(a^{10})^{56} \equiv 1^{56} \pmod{11}$

$a^{560} \equiv 1 \pmod{11}$ ... (2)

$gcd(a, 17) = 1$ ونرما $a^{17-1} = a^{16} \equiv 1 \pmod{17}$

$(a^{16})^{35} \equiv 1^{35} \pmod{17}$

$a^{560} \equiv 1 \pmod{17}$ ... (3)

من (1) و (2) و (3) وكون $gcd(3, 11, 17) = 1$ نجد:

$a^{560} \equiv 1 \pmod{3 \times 11 \times 17}$

$a^{560} \equiv 1 \pmod{561}$ $m = 561$ هو عدد كارميكل.

نستنتج أن عكس مبرهنة نيرما غير صحيح.

نموذج B

الحل 1) لنثبت أن : $67 / (43 \times 651 + 24)$

أي لنثبت أن : $(43 \times 651 + 24) \equiv 0 \pmod{67}$

67 عدد أولي ← مبرهنة ويلسون : $(67-1)! \equiv -1 \pmod{67}$

$66! \equiv -1 \pmod{67}$

$66 \times 651 \equiv -1 \pmod{67}$

$(-1) \times 651 \equiv -1 \pmod{67} \Rightarrow 651 \equiv 1 \pmod{67}$

نضرب طرفي التطابق بـ 43 $\Rightarrow 43 \times 651 \equiv 43 \pmod{67}$

نجمع 24 للطرفين $\Rightarrow 43 \times 651 + 24 \equiv 43 + 24 \pmod{67}$

$43 \times 651 + 24 \equiv 67 \pmod{67} \equiv 0 \pmod{67}$

ومنه $67 / (43 \times 651 + 24)$

2) $F_n = 2^{2^n} + 1$, لنثبت $\forall n \geq 1 \quad F_n \equiv 5 \pmod{12}$

$12 = 3 \times 4$

$F_n = 2^{2^n} + 1 \equiv (-1)^{2^n} + 1 \pmod{3} \equiv 2 \pmod{3}$

$F_n \equiv 5 \pmod{3} \quad \ldots (1)$

$F_n \equiv 1 \pmod{4} \Rightarrow F_n \equiv 5 \pmod{4} \quad \ldots (2)$

من (1) و (2) وكون $\gcd(3,4) = 1$ نجد :

$F_n \equiv 5 \pmod{3 \times 4} \Rightarrow F_n \equiv 5 \pmod{12}$

ويصح الإثبات بالاستقراء الرياضي .

3) $x \equiv 2 \pmod{8} \Rightarrow b_1 = 2 , m_1 = 8$

$x \equiv 6 \pmod{11} \Rightarrow b_2 = 6 , m_2 = 11$

$x \equiv 1 \pmod{9} \Rightarrow b_3 = 1 , m_3 = 9$

بما أن $gcd(m_i, m_j) = 1$ $\forall i, j \in \{1,2,3\}$ و $i \neq j$

فإنه يوجد للجملة حل مشترك وحيد بالنسبة للمقاس

$m = m_1 m_2 m_3 = 8 \times 11 \times 9 = 792$

وذلك حسب مسألة اللغز الصيني فإن هذا الحل هو :

$x^* = b_1 m'_1 N_1 + b_2 m'_2 N_2 + b_3 m'_3 N_3$

$m'_1 = \frac{m}{m_1} = 99$ ، $m'_2 = \frac{m}{m_2} = 72$ ، $m'_3 = \frac{m}{m_3} = 88$

N_1 : هو المعكوس الضربي لـ m'_1 بالنسبة للمقاس m_1 :

$\phi(m_1) = \phi(8) = 8(1 - \frac{1}{2}) = 4$

$(m'_1)^{\phi(m_1)-1} = (99)^{4-1} = (99)^3 \equiv 3 \pmod 8 \Rightarrow N_1 = 3$

N_2 : هو المعكوس الضربي لـ m'_2 بالنسبة للمقاس m_2 :

$\phi(m_2) = \phi(11) = 11 - 1 = 10$

$(m'_2)^{\phi(m_2)-1} = (72)^{10-1} = (72)^9 \equiv 6^9 \pmod{11} \equiv 2 \pmod{11}$

$\Rightarrow N_2 = 2$

N_3 : هو المعكوس الضربي لـ m'_3 بالنسبة للمقاس m_3 :

$\phi(m_3) = \phi(9) = 9(1 - \frac{1}{3}) = 6$

$(m'_3)^{\phi(m_3)-1} = (88)^{6-1} = (88)^5 \equiv 4 \pmod 9 \Rightarrow N_3 = 4$

$x^* = 2 \times 99 \times 3 + 6 \times 72 \times 2 + 1 \times 88 \times 4 = 1810$

فالعدد المطلوب 226 $x^* \equiv 226 \pmod{792}$

4 متى يكون $m = 341$ عدد سودوكي للأساس 2 حيث

تحقق : $2^{m-1} \equiv 1 \pmod m$

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

TEL:0931497960 - Facebook Group: A to Z مكتبة

لدينا $341 = 11 \times 31$

وبما أن $\gcd(2, 341) = 1$ فإن:

$\gcd(2, 11) = \gcd(2, 31) = 1$

$\gcd(2, 11) = 1 \xrightarrow{\text{فيرما}} 2^{11-1} = 2^{10} \equiv 1 \pmod{11}$

$(2^{10})^{34} \equiv 1^{34} \pmod{11} \Rightarrow 2^{340} \equiv 1 \pmod{11}$ ... (1)

$\gcd(2, 31) = 1 \xrightarrow{\text{فيرما}} 2^{31-1} = 2^{30} \equiv 1 \pmod{31}$

$(2^{30})^{11} \cdot 2^{10} \equiv 2^{330} \cdot 2^{10} \pmod{31}$

$\equiv 1^{11} \cdot 1 \pmod{31} \Rightarrow 2^{340} \equiv 1 \pmod{31}$ ... (2)

من (1) و (2) وكون $\gcd(11, 31) = 1$ نجد:

$2^{340} \equiv 1 \pmod{11 \times 31}$

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

و $m = 341$ عدد سشبه أولي للأساس 2.

نستنتج أن عكس مبرهنة فيرما غير صحيح.

TEL:0931497960 - Facebook Group: A to Z مكتبة