Chinese Remainder Theorem and Problems on Order of an Element

13 June, 2020

Let q be fixed prime number. Show that there exists infinitely many primes of the form $qm + 1$

Hint: We previously proved that $\frac{(p^p-1)}{p-1}$ prime deviosrs are of the form $pk + 1$. Try to do a similar thing on $\frac{(A^p-1)}{A-1}$.

نفرض أن عدد الأعداد الأولية على الصيغة $qm+1$ محدود والأعداد

هي $q_1, q_2, \ldots, q_n$.

نفرض أن p قاسم أولي لـ $\frac{A^q-1}{A-1}$

$$\Rightarrow \begin{cases} A^q \equiv 1 \pmod{p} \quad (1) \Rightarrow \operatorname{ord}_p A \mid q \Rightarrow \operatorname{ord}_p A = 1, q \\ p \mid A^{q-1} + A^{q-2} + \cdots + 1 \quad (2) \end{cases}$$

Let q be fixed prime number. Show that there exists infinitely many primes of the form $qm + 1$

Hint: We previously proved that $\frac{(p^p-1)}{p-1}$ prime deviosrs are of the form $pk + 1$. Try to do a similar thing on $\frac{(A^p-1)}{A-1}$.

- If $\text{ord}_p A = 1 \Rightarrow \underline{A \equiv 1 \pmod p}$ *

بالتعويض في : 2

$p \mid 1^{q-1} + 1^{q-2} + \cdots + 1 \Rightarrow p \mid q \Rightarrow p = q \overset{*}{\Rightarrow} q \mid A-1$

(لتفادي هذه الحالة نريد $q \nmid A-1$ ، لذا نختار A مضاعف لـ q)

- If $\text{ord}_p A = q \Rightarrow q \mid p-1$

Let q be fixed prime number. Show that there exists infinitely many primes of the form $qm + 1$

Hint: We previously proved that $\frac{(p^p-1)}{p-1}$ prime deviosrs are of the form $pk + 1$. Try to do a similar thing on $\frac{(A^p-1)}{A-1}$.

$p \mid A^q - 1 \Rightarrow \gcd(A, p) = 1$

(نريد التناقض بإثبات أن p مختلف عن $q_1, \ldots, q_k$، لذا نجعل A مضاعف لكل من $q_1, \ldots, q_k$

$\Leftarrow$ p مختلفة عن $q_1 \ldots q_k$

p على الصيغة $qm+1$

$\Leftarrow$ تناقض

Let q be fixed prime number. Show that there exists infinitely many primes of the form $qm + 1$

Hint: We previously proved that $\frac{(p^p-1)}{p-1}$ prime deviosrs are of the form $pk + 1$. Try to do a similar thing on $\frac{(A^p-1)}{A-1}$.

الحل بعد إعادة كتابته:

نفرض أن عدد الأعداد الأولية على الصيغة $qm+1$ محدود، والأعداد هي $q_1, q_2, \ldots, q_k$.

$$A = q q_1 q_2 \cdots q_k$$

ليكن P قاسم أولي للمقدار $\frac{A^q-1}{A-1}$.

① P مختلف عن $q_1, q_1, \ldots, q_k$

$$P \mid A^q - 1 \Rightarrow \begin{cases} \gcd(P, A) = 1 \longrightarrow q_1, q_1, \ldots, q_k \\ \operatorname{ord}_P(A) \mid q \longrightarrow \operatorname{ord}_P(A) = 1, q \end{cases}$$

Let q be fixed prime number. Show that there exists infinitely many primes of the form $qm + 1$

Hint: We previously proved that $\frac{(p^p-1)}{p-1}$ prime deviosrs are of the form $pk + 1$. Try to do a similar thing on $\frac{(A^p-1)}{A-1}$.

Case 1: $\mathrm{ord}_p(A)=1$

$\Rightarrow A \equiv 1 \pmod{p}$

ولكن

$p \mid A^{q-1}+A^{q-2}+\cdots+A+1$

$\Rightarrow p \mid 1^{q-1}+\cdots+1^1+1 \Rightarrow p \mid q \Rightarrow p=q$ تناقض مع ①

Case 2: $\mathrm{ord}_p(A)=q$

$q \mid p-1 \Rightarrow p=qm+1$

ولكن p مختلفة عن $q_1, q_2, \ldots, q_k$ من ①

$\Rightarrow$ تناقض

إذن عدد الأعداد الأولية على الصيغة $qm+1$ غير محدود.

Calculate $ord_{3^n}(2)$ *for any* $n \in \mathbb{N}$.

Hint: $ord_{3^n}(2) = \varphi(3^n)$

لتكن $ord_{3^n}(2) = s$: $3^n \mid 2^s - 1$

$\Rightarrow 2^s \equiv 1 \pmod 3 \Rightarrow 2 \mid s$ (mod 3)

$s \mid \varphi(3^n) \Rightarrow s \mid 2 \cdot 3^{n-1}$.

$\Rightarrow s = 2 \cdot 3^{\alpha}$, $\alpha \leq n-1$

نريد إثبات أن $s = 2 \cdot 3^{n-1} \Leftrightarrow s \nmid 2 \cdot 3^{n-2}$

$3^n \nmid 2^{2 \cdot 3^{n-2}} - 1 \Leftrightarrow 2^{2 \cdot 3^{n-2}} \not\equiv 1 \pmod{3^n}$

$\Leftrightarrow 3^n \nmid 4^{3^{n-2}} - 1 = (4^{3^{n-3}})^3 - 1 = (4^{3^{n-3}} - 1)(4^{2 \cdot 3^{n-3}} + 4^{3^{n-3}} + 1)$

$\not\equiv 0 \pmod{3^{n-1}}$

Calculate $ord_{3^n}(2)$ *for any* $n \in \mathbb{N}$.

Hint: $ord_{3^n}(2) = \varphi(3^n)$

$$4^{2\cdot 3^{n-3}} + 4^{3^{n-3}} + 1 \equiv \left(64^{3^{n-4}}\right)^2 + 64^{3^{n-4}} + 1 \equiv 1+1+1 \pmod{9}$$

$n \geq 4$ لأنه

$$4,\ 4^3 \equiv 64 \equiv 1 \pmod{9}$$

$$\Rightarrow 3 \,\|\, \left(4^{2\cdot 3^{n-3}} + 4^{3^{n-3}} + 1\right) \Rightarrow 3^n \nmid 4^{3^{n-2}} - 1$$

بالاستقراء $\leftarrow 3^{n-1} \nmid 4^{3^{n-3}} - 1$

$(n-1) \to (n)$

$$\Rightarrow s \nmid 2\cdot 3^{n-2} \Rightarrow \begin{cases} 2 \mid s \\ s \mid 2\cdot 3^{n-1} \\ s \nmid 2\cdot 3^{n-2} \end{cases} \Rightarrow s = 2\cdot 3^{n-1}$$

Calculate $ord_{3^n}(2)$ *for any* $n \in \mathbb{N}$.

Hint: $ord_{3^n}(2) = \varphi(3^n)$

(طريقة أفضل للكتابة)

$$\begin{cases} 3^{n-1} \nmid 4^{3^{n-3}} - 1 \\ 3^{n-2} \mid 4^{3^{n-3}} - 1 \end{cases} \iff 3^{n-2} \,\|\, 4^{3^{n-3}} - 1$$

فرضية الاستقراء

$$\Rightarrow \quad 3^{n-1} \,\|\, 4^{3^{n-2}} - 1$$

نريد إثبات أن

$$(4^{3^{n-3}} - 1)(\quad + \quad + \quad)$$

3^1

من الاستقراء 3^{n-2}

Find all pairs of prime numbers (p,q) *such that*

① $\dfrac{(2p^2-1)^q+1}{p+q}$ *and* ② $\dfrac{(2q^2-1)^p+1}{p+q}$ *are integers*

Hint: $2p^2-1 \equiv 2q^2-1 \pmod{p+q}$.

نلاحظ أن $2p^2-1 \equiv 2q^2-1 \pmod{p+q}$ ، بالتالي سنعتمد على $2p^2-1$

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

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

ليكن $s = \mathrm{ord}_{p+q}(2p^2-1)$. نلاحظ $\gcd(2p^2-1, p+q)=1$

$\Rightarrow$ $s \mid 2q$ ، $s \mid 2p$ ، $s \nmid p$ ، $s \nmid q$ ← (لأن $p+q>4$ ، $p+q \neq 2$)

Find all pairs of prime numbers (p,q) *such that*

$$\frac{(2p^2-1)^q+1}{p+q} \text{ and } \frac{(2q^2-1)^p+1}{p+q} \text{ are integers}$$

Hint: $2p^2-1 \equiv 2q^2-1 \pmod{p+q}$.

$\Rightarrow \quad s \mid 2\gcd(p,q)$

<u>Case 1</u>: $p \neq q$, WLOG $p > q$.

$\Rightarrow \quad s \mid 2, \quad s \nmid p, \; s \nmid q$

$\Rightarrow \quad s \neq 1 \Rightarrow s = 2 \Rightarrow p, q$ are odd primes

من تعريف الاعداد :

$$\Rightarrow \begin{cases} (2p^2-1)^2 \equiv 1 \pmod{p+q} \; * \\ (2p^2-1)^q \equiv -1 \pmod{p+q}, \quad q = 2k+1 \end{cases}$$

$$\Rightarrow \left((2p^2-1)^2\right)^k (2p^2-1) \equiv -1 \pmod{p+q}$$

$$\overset{*}{\Rightarrow} (1)^k (2p^2-1) \equiv -1 \pmod{p+q}$$

$$\Rightarrow 2p^2-1 \equiv -1 \pmod{p+q}$$

Find all pairs of prime numbers (p,q) *such that*

$$\frac{(2p^2-1)^q+1}{p+q} \text{ and } \frac{(2q^2-1)^p+1}{p+q} \text{ are integers}$$

Hint: $2p^2-1 \equiv 2q^2-1 \pmod{p+q}$.

$\Rightarrow \quad 2p^2-1 \equiv -1 \pmod{p+q}$

$\Rightarrow \quad 2p^2 \equiv 0 \pmod{p+q}$

$\Rightarrow \quad p+q \mid 2p^2 \quad \Rightarrow \quad \frac{p+q}{2} \mid p^2$

$p+q$ is even

$\Rightarrow \quad \frac{p+q}{2} = \underbrace{1}_{\text{مستحيل}}, \underbrace{p}_{p=q \text{ مستحيل}}, p^2$

$\Rightarrow \quad \frac{p+q}{2} = p^2$

$\Rightarrow \quad p+q = 2p^2$

$\Rightarrow \quad q = p(2p-1)$

$\Rightarrow \quad q \not\equiv p \pmod 3$

لكن $p>q$ تناقض أو لأن $p(2p-1)$ عدد مؤلف

Find all pairs of prime numbers (p,q) *such that*

$$\frac{(2p^2-1)^q+1}{p+q} \text{ and } \frac{(2q^2-1)^p+1}{p+q} \text{ are integers}$$

Hint: $2p^2-1 \equiv 2q^2-1 \pmod{p+q}$.

Case 2: $p=q$:

$2p \mid (2p^2-1)^p+1$ العبارتين تكافئ

$\Leftrightarrow 2p \mid (-1)^p+1$

if $p>2$:

$2 \mid (2p^2-1)^p+1$

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

$\Rightarrow (p,p)$

if $p=2$: $\Rightarrow 4 \mid (-1)^2+1 = 2 \Rightarrow \times$

* مجموعة الحل (k,k)، حيث أن k عدد أولي فردي

Let k, n be positive integers greater than 1. Prove that if there exists natural number a such that $k|2^a + 1, n|2^a - 1$ then there is no natural number b satisfying $k|2^b - 1, n|2^b + 1$.

Hint: look at the summary of last lecture

$$\begin{cases} 2^a \equiv -1 \pmod{k} \\ 2^b \equiv 1 \pmod{k} \end{cases}, \quad \begin{cases} 2^a \equiv 1 \pmod{n} \\ 2^b \equiv -1 \pmod{n} \end{cases}, \quad \begin{cases} 2^{2a} \equiv 1 \pmod{k} \\ 2^{2b} \equiv 1 \pmod{n} \end{cases}$$

$\mathrm{ord}_k(2) = s_k$, $\mathrm{ord}_n(2) = s_n$

$s_k \mid b$, $s_n \mid a$

$s_k \mid 2a$, $s_n \mid 2b$

$k, n > 2 \Rightarrow 1 \not\equiv -1 \pmod{k}, \pmod{n}$

$s_k \nmid a$ $\quad s_n \nmid b$

Let k, n be positive integers greater than 1. Prove that if there exists natural number a such that $k|2^a+1$, $n|2^a-1$ then there is no natural number b satisfying $k|2^b-1$, $n|2^b+1$.

Hint: look at the summary of last lecture

في summary المحاضرة الماضية اثبتنا أن

$$\Rightarrow \begin{cases} sk \mid 2a \\ sk \nmid a \end{cases} \Rightarrow v_2(2a) = v_2(sk)$$

$$\Rightarrow v_2(sk) = v_2(a) + 1 \quad (1)$$

وبالمثل

$$sk \mid b$$

$$\Rightarrow v_2(sk) \leq v_2(b) \quad (2)$$

من (1) و (2):

$$v_2(a) + 1 \leq v_2(b) \quad *$$

Let k, n be positive integers greater than 1. Prove that if there exists natural number a such that $k|2^a+1$, $n|2^a-1$ then there is no natural number b satisfying $k|2^b-1$, $n|2^b+1$.

Hint: look at the summary of last lecture

بتطبيق المثل على S_n :

$S_n \nmid b$

$S_n \mid 2b$ $\Rightarrow$ $v_2(S_n) = v_2(b)+1$

$S_n \mid a$ $\Rightarrow$ $v_2(S_n) \leq v_2(a)$

$\Rightarrow$ $v_2(b)+1 \leq v_2(a)$ $**$

بجمع $*$ و $**$ $\Rightarrow$ $v_2(a)+v_2(b)+2 \leq v_2(a)+v_2(b)$ تناقض

وبالتالي

When $3|p-2$ show that $a^3 \equiv b^3 (\bmod p)$ if and only if $a \equiv b \ (\bmod p)$ where p is a prime number.

حل غلا :

$$a^{p-1} \equiv b^{p-1} \quad [p]$$

Assume that $p \nmid a \Rightarrow p \nmid b$

$$a(a^{p-2}) \equiv b(b^{p-2}) \quad [p]$$

$$(a^3)^k \equiv (b^3)^k$$

$$\underline{a \equiv b} \quad [p]$$

if $p|a \Rightarrow p|a^3 \Rightarrow p|b^3 \Rightarrow p \Rightarrow p|a \Leftrightarrow p|b$ $\quad a \equiv b \ (\bmod p)$

When $3|p-2$ *show that* $a^3 \equiv b^3 (mod\ p)$ *if and only if* $a \equiv b\ (mod\ p)$.

حل إياد

$3|p-2$

$a^3 \equiv b^3\ [p] \iff a \equiv b\ [p]$

if $a^3 \equiv b^3\ [p]$

$\Rightarrow (a^3)^{\frac{p-2+3}{3}} \equiv (b^3)^{\frac{p-2+3}{3}}\ [p]$, $3|p-2 \Rightarrow 3 \mid p-2+3 = \underline{p+1}$

$3|p+1$

$(a^3)^{\frac{p+1}{3}} \equiv (b^3)^{\frac{p+1}{3}}\ [p]$

$a^{p+1} \equiv b^{p+1}\ [p]$

$a^p \cdot a \equiv b^p \cdot b\ [p]$

باستخدام فيرما

$a^2 \equiv b^2\ [p]$

$a \equiv \pm b\ [p]$

if $a \equiv b\ [p]$ we are done

if $a \equiv -b\ [p]$

$\Rightarrow a^3 \equiv -b^3\ [p]$

$\Rightarrow 2b^3 \equiv 0\ [p]$, $2a^3 \equiv 0\ [p] \Rightarrow p \mid 2a^3, 2b^3$ p odd , if $p=2$ $a \equiv b \equiv -b\ (mod\ 2)$

$p \mid a^3, p \mid b^3 \Rightarrow p \mid a, b \Rightarrow a \equiv b \equiv 0\ [p]$

if $a \equiv b\ [p] \Rightarrow (a)^3 \equiv (b)^3\ [p] \Rightarrow a^3 \equiv b^3\ [p]$ ∎

When $3|p-2$ *show that* $a^3 \equiv b^3 \pmod{n}$ *if and only if* $a \equiv b \pmod{n}$.

- If $p|a \Rightarrow \text{---} \Rightarrow p|b$

  $\Rightarrow a \equiv b \pmod{p}$

- If $\gcd(a,p) = \gcd(b,p) = 1$

$\Rightarrow (ab^{-1})^3 \equiv b^3(b^{-1})^3 \equiv 1 \pmod{p}$

$c = ab^{-1} \Rightarrow c^3 \equiv 1 \pmod{p} \Rightarrow \mathrm{ord}_p(c) \mid 3$

أو

$\| \ \mathrm{ord}_p(c) \mid \gcd(3, p-1)$

$\gcd(k, p-1) = 1$

<u>Case 1</u> $\mathrm{ord}_p(c) = 3$:

$\Rightarrow 3 \mid p-1 \Rightarrow\Leftarrow !!$

<u>Case 2</u> $\mathrm{ord}_p(c) = 1$:

$\Rightarrow x \equiv 1 \pmod{p} \Rightarrow ab^{-1} \equiv 1 \pmod{p} \Rightarrow a \equiv b \pmod{p}$

تعميم: إذا كان k عدد صحيح موجب و $\gcd(p-1, k) = 1$ فإن

$\| \ a^k \equiv b^k \pmod{p} \Leftrightarrow a \equiv b \pmod{p}$

When $3|p-2$ *show that* $a^3 \equiv b^3 (mod\ n)$ *if and only if* $a \equiv b\ (mod\ n)$.

إذن المسألة تقتضي أن

$\{0^3, 1^3, 2^3, \ldots, (p-1)^3\}$

مجموعة بواقي كاملة، عندما $3|p-2$.

التعميم يقتضي أن

$\{0^k, 1^k, 2^k, \ldots, (p-1)^k\}$

مجموعة بواقي كاملة عندما $gcd(p-1, k)=1$.

(Balkan MO 1999). *Let $p > 2$ be a prime number such that $3|(p-2)$. Let*

$$S = \{y^2 - x^3 - 1 | 0 \le x, y \le p-1 \cap x, y \in \mathbb{Z}\}$$

Prove that there are at most p elements of S divisible by p.

نريد عدد (x,y) التي تحقق $y^2-x^3-1 \equiv 0 \pmod p$.

$$y^2-x^3-1 \equiv 0 \pmod p$$

$$\Leftrightarrow \quad x^3 \equiv y^2-1 \pmod p$$

مجموعة بواقي كاملة لأن $3|p-2$

$$\Rightarrow \quad x^3 \equiv \{0^3, 1^3, 2^3, \ldots, (p-1)^3\} \equiv \{0, 1, \ldots, p-1\}$$

(Balkan MO 1999). *Let $p > 2$ be a prime number such that $3|(p-2)$. Let*

$$S = \{y^2 - x^3 - 1 | 0 \le x, y \le p-1 \cap x, y \in \mathbb{Z}\}$$

Prove that there are at most p elements of S divisible by p.

لكل قيمة لـ y ⇐ توجد قيمة وحيدة لـ y^2-1 وتوجد قيمة وحيدة لـ x تجعل $x^3 \equiv y^2-1 \pmod p$.

⇐ يوجد p قيمة ممكنة لـ y ⇐ يوجد على الأكثر p زوج (x,y) يحقق أن $x^3 \equiv y^2-1 \pmod p$.

Chinese Remainder Theorem

Chinese remainder theorem

(a) If m and n are relatively prime integers greater than one, and a and b are arbitrary integers, then show that there exists an integer x such that

$$\begin{aligned} x &\equiv a \pmod{m} \\ x &\equiv b \pmod{n} \end{aligned}$$

(b) If $m_1, m_2, \ldots, m_k$ are pairwise relatively prime integers greater than one, and $a_1, a_2, \ldots, a_k$ are arbitrary integers, then show that there exists an integer x such that

$$x \equiv a_i \pmod{m_i}, \quad i = 1, 2, \ldots, k.$$

(AIME II 2012). For a positive integer p, define the positive integer n to be p-safe if n differs in absolute value by more than 2 from all multiples of p. For example, the set of 10-safe numbers is 3, 4, 5, 6, 7, 13, 14, 15, 16, 17, 23, ... Find the number of positive integers less than or equal to 10, 000 which are simultaneously 7-safe, 11-safe, and 13-safe.

Exam Problems

Problem 1. Suppose that each of the positive integers a, b, c, d is divisible by $ad - bc$. Find all possible values of $ad - bc$.

$$\underline{ad-bc} \mid a, b, c, d$$

$$\Rightarrow ad-bc \mid \gcd(a, b, c, d)$$

$$\gcd(a, b, c, d) = k, \qquad a = ka' \quad d' = kd'$$

$$\Rightarrow k^2(a'd' - b'c') \mid k \Rightarrow k^2 \mid k \Rightarrow k = 1$$

$$\Rightarrow (a'd' - b'c') \mid 1 \Rightarrow a'd' - b'c' = 1$$

$$\Rightarrow ad - bc = 1$$

Problem 2. Find all positive integers n and d with $d \mid n$ such that $n^2 + d^2$ is divisible by $nd + 1$.

$n = kd$

$\Rightarrow \quad kd^2+1 \mid k^2d^2 + d^2$

$\Rightarrow \quad \underline{kd^2+1} \mid (k^2+1)\,\underline{d^2}$

ولكن $\gcd(kd^2+1, d^2) = 1$

$\Rightarrow \quad kd^2+1 \mid k^2+1$

$kd^2+1 \mid k^2+1-kd^2-1$

$kd^2+1 \mid k^2-kd^2$

$\underline{kd^2+1} \mid \underline{k}(k-d^2)$

ولكن $1 = \gcd(kd^2+1, k)$

$\Rightarrow kd^2+1 \mid k-d^2$

أو

$k^2 \equiv -1 \pmod{kd^2+1}$

$k.(-k) \equiv 1 \pmod{kd^2+1}$ *

$kd^2 \equiv -1 \pmod{kd^2+1}$

$k(-d^2) \equiv 1 \pmod{kd^2+1}$ **

$k^{-1} \equiv -k$ * و $k \equiv -d^2$ **

إذن بما أن النظير الضربي وحيد فإن

$kd^2+1 \mid k-d^2 \Leftarrow -k \equiv -d^2 \pmod{kd^2+1}$

Problem 2. Find all positive integers n and d with $d \mid n$ such that $n^2 + d^2$ is divisible by $nd + 1$.

بكل الطريقتين

$$kd^2+1 \mid k-d^2$$

ولكن

$$|k-d^2| < kd^2+1$$

لأن

$$kd^2+1 > \max(k, d^2) > |k-d^2|$$

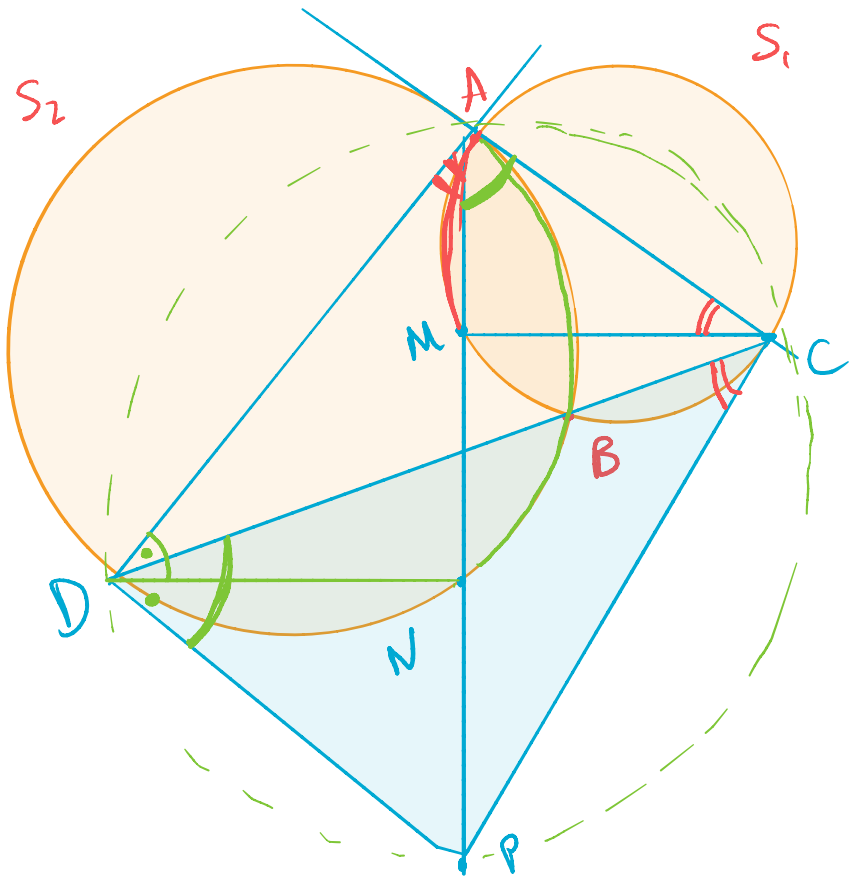
$$\Rightarrow \quad k-d^2=0 \Rightarrow k=d^2 \Rightarrow n=d^3$$

بالتحقق من الحل

$$d \mid n \Leftrightarrow d \mid d^3 \checkmark$$

$$nd+1 \mid n^2+d^2 \Leftrightarrow d^4+1 \mid d^6+d^2 = d^2(d^4+1) \checkmark$$

Problem 3. Two circles S_1 and S_2 intersect at points A and B. The tangent at A to S_1 meets S_2 at C and the tangent at A to S_2 meets S_1 at D. A line through A to interior of angle CAD meets S_1 at M, S_2 at N and meets the circumcircle of triangle ACD at P. prove that $AM = NP$.



• $\angle MCA = \angle MAD$
من التماس

• $\angle MAD = \angle PAD$
$= \angle PCD$
للرباعي الدائري

$\Rightarrow \angle PCD = \angle MCA$

بالمثل

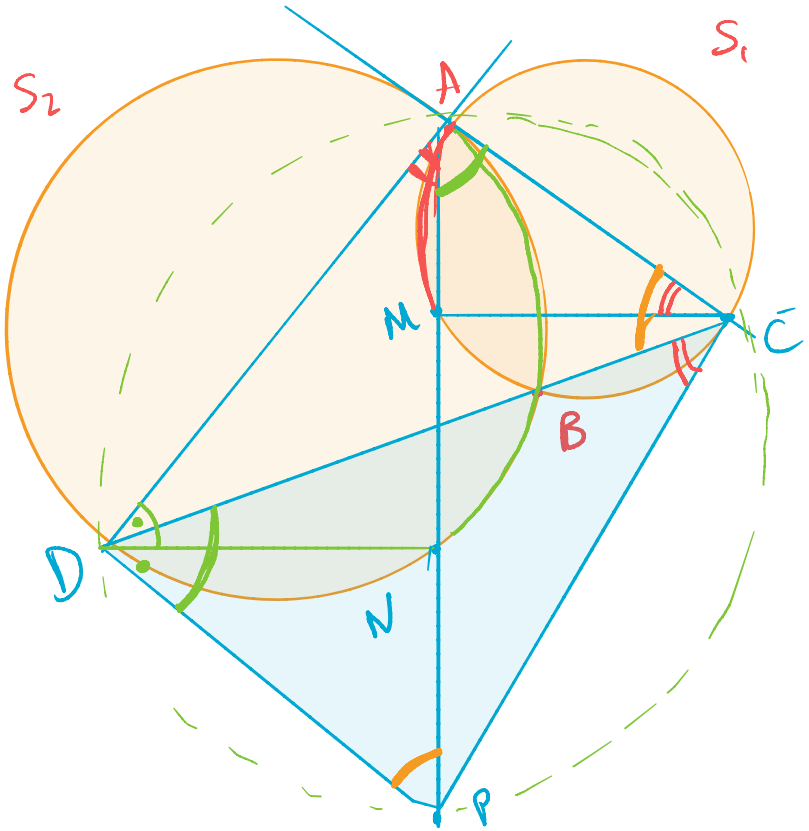
$\angle NDA = \angle NAC$
من التماس

$\angle NAC = \angle PAC$
$= \angle PDC$ للرباعي الدائري

$\Rightarrow \angle NDA = \angle PDC$

$\Rightarrow \angle PDN = \angle CDA$

Problem 3. Two circles S_1 and S_2 intersect at points A and B. The tangent at A to S_1 meets S_2 at C and the tangent at A to S_2 meets S_1 at D. A line through A to interior of angle CAD meets S_1 at M, S_2 at N and meets the circumcircle of triangle ACD at P. prove that $AM = NP$.



نلاحظ أن :

$\triangle CMA \sim \triangle CPD$

$\Rightarrow \boxed{\dfrac{AM}{DP} = \dfrac{CA}{CD}} \Rightarrow AM = \dfrac{DP.CA}{CD}$ *

بالمثل

$\angle ACD = \angle APD$

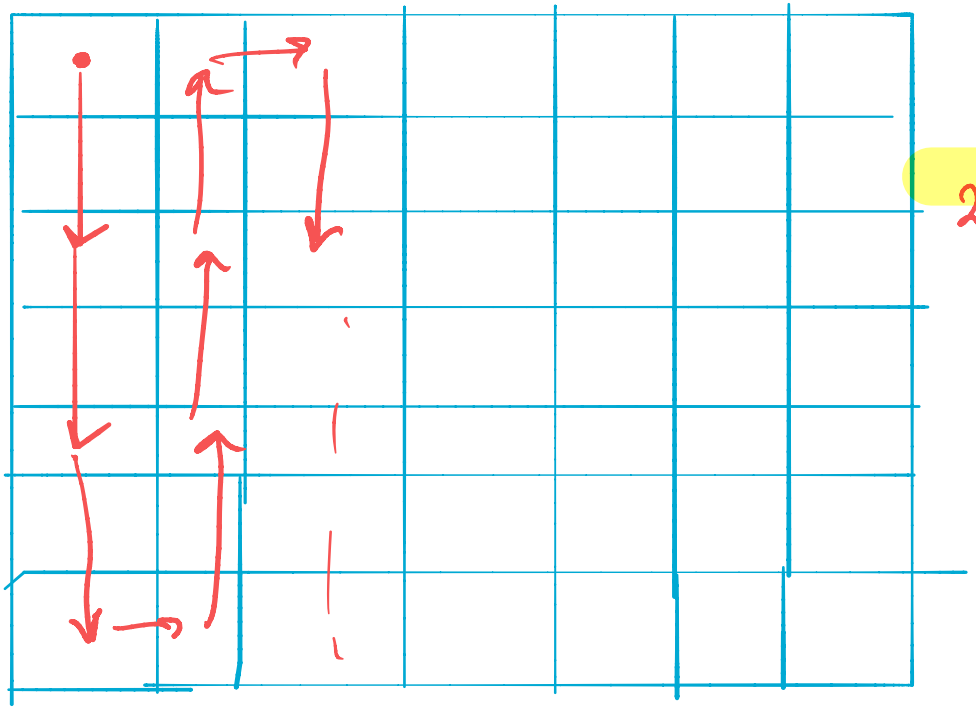
$\triangle DCA \sim \triangle DPN$

$\Rightarrow \boxed{\dfrac{PN}{CA} = \dfrac{DP}{DC}} \Rightarrow PN = \dfrac{DP.CA}{CP}$ **

من * و ** ينتج

$AM = PN$

Problem 4. Let n be a positive integer. A spider travels on a $(2n+1) \times (2n+1)$ board. In every move, it can travel two squares vertically (up or down), two squares diagonally or one square horizontally (left or right). Find the minimum number of moves the spider needs to pass through every single square. For each move, the spider is considered to have visited the starting square, the ending square and the square between the starting and ending square when the spider moves two squares. The starting point can be arbitrarily chosen.



في كل عمود n خطوة

في الانتقال بين الأعمدة $2n$ خطوة.

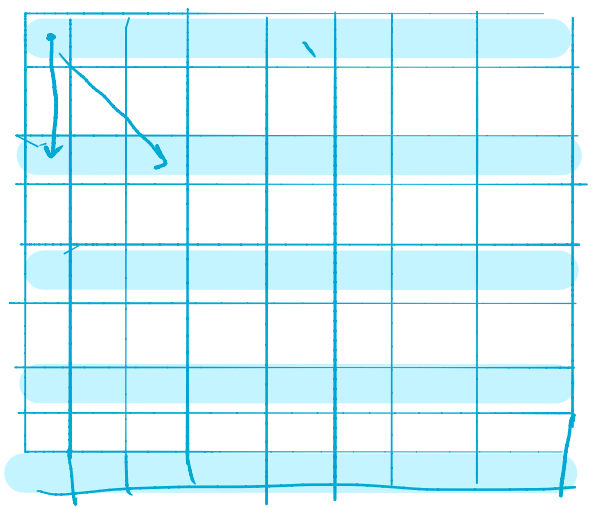
إذن عدد الخطوات الكلي

$$n(2n+1) + 2n$$
$$= n(2n+3)$$

نريد إثبات أن هذا هو أقل عدد ممكن من الخطوات

Problem 4. Let n be a positive integer. A spider travels on a $(2n+1) \times (2n+1)$ board. In every move, it can travel two squares vertically (up or down), two squares diagonally or one square horizontally (left or right). Find the minimum number of moves the spider needs to pass through every single square. For each move, the spider is considered to have visited the starting square, the ending square and the square between the starting and ending square when the spider moves two squares. The starting point can be arbitrarily chosen.

إثبات أنه نحتاج $2n$ خطوة على الأقل من نوع



بما أن الفرق بين عدد الخلايا الزرقاء والبيضاء هو $2n+1$ نحتاج $2n$ خطوة من النوع الأخير.

عدد الخلايا الزرقاء:

$(n+1)(2n+1)$

عدد الخلايا البيضاء $n(2n+1)$

$\Rightarrow$ 1 blue 1 white تغطي

$\Rightarrow$ 1 blue 1 white تغطي

$\Rightarrow$ 1 black أو 1 white

More Problems ☺

(AoPS). *Show that for $c \in \mathbb{Z}$ and a prime p, the congruence $x^x \equiv c \pmod{p}$ has a solution.*

(ISL 2005 N6). *Let a, b be positive integers such that $b^n + n$ is a multiple of $a^n + n$ for all positive integers n. Prove that $a = b$.*

(USAMO 1991). *Show that, for any fixed integer* $n \geq 1$, *the sequence*

$$2,\ 2^2,\ 2^{2^2},\ 2^{2^{2^2}}, \ldots \pmod{n}$$

is eventually constant.

[The tower of exponents is defined by $a_1 = 2,\ a_{i+1} = 2^{a_i}$. *Also* $a_i \pmod{n}$ *means the remainder which results from dividing* a_i *by* n.*]*