Problems on Chinese Remainder Theorem

14 June, 2020

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

$$x \equiv a \pmod{m}$$
$$x \equiv b \pmod{n}$$

(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

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

هل x وحيد
$\mod(mn)$ ؟

إذا وجد x'
يحقق:

$x \equiv x' \equiv a\ [m]$
$x \equiv x' \equiv b\ [n]$

$\Rightarrow x \equiv x'\ [mn]$
$\Rightarrow$ ابلي وحيد

a)

$x \equiv a\ [m]$

$x \equiv b\ [n]$

$gcd(m,n) = 1$

let $x = um + a \quad u \in \mathbb{Z}$

$\rightarrow um + a \equiv b\ [n]$

$\rightarrow um \equiv b - a\ [n] \quad gcd(m,n)=1 \Rightarrow \exists\ m'$ s.t $mm' \equiv 1\ [n]\ \ m' \in \mathbb{Z}$

$\rightarrow u(mm') \equiv m'(b-a)\ [n]$

$u \equiv m'(b-a)\ [n]$

$\Rightarrow u = vn + m'(b-a) \quad v \in \mathbb{Z}$

$\Rightarrow x = u(vn + m'(b-a)) + a \in \mathbb{Z}$ and satisfys both properties

حل إياد

$um = c\ [n]$
$gcd(m,n) = 1$

$u = ?\ [n]$

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

$$x \equiv a \pmod{m}$$
$$x \equiv b \pmod{n}$$

(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

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

b) $x \equiv a_i [m_i]$ $i = 1, 2, \ldots, k$, $\gcd(m_i, m_j) = 1$ for $i = 1, 2, \ldots, k$

if we take $x \equiv a_1 [m_1]$, $x \equiv a_2 [m_2]$ $\exists$ x that satisfys this condition, if we input the value of x that satisfys s in $x \equiv a_3 [m_3]$, and we will get an x that satisfys, and so on until we reach $x \equiv a_k [m_k]$ which will satisfy all the previous conditions.

$$\begin{cases} x \equiv a_1 [m_1] \\ x \equiv a_2 [m_2] \end{cases}$$

$$\Rightarrow \begin{cases} x \equiv c_2 [m_1 m_2] \\ x \equiv a_3 [m_3] \end{cases}$$

$$\Rightarrow \begin{cases} x \equiv c_3 [m_1 m_2 m_3] \\ x \equiv a_4 [m_4] \end{cases}$$

$$\begin{cases} x \equiv c_{k-1} [m_1 \cdots m_{k-1}] \\ x \equiv a_k [m_k] \end{cases}$$

(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.*

حل

$\underbrace{\{1, \ldots, 1001\}}_{96}, \underbrace{\{1002, \ldots, 2002\}}_{96}, \ldots \underbrace{\{9010, \ldots, \boxed{10010}\}}_{96}$

(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.

n : psafe if $|n - pk| > 2 \quad \forall\, k \in \mathbb{Z}$

العدد يكون p-safe إذا كان لا يطابق $\Rightarrow 0, \pm 1, \pm 2 \pmod p$

x is 7-safe if $x \equiv 3, 4 \pmod 7 \rightarrow 2$ عدد

" 11-safe if $x \equiv 3, 4, \ldots, 8 \pmod{11} \rightarrow 6$ عدد

" 13-safe if $x \equiv 3, 4, \ldots, 10 \pmod{13} \rightarrow 8$ عدد

$7 \cdot 11 \cdot 13 = 1001$

يوجد $2 \times 6 \times 8 = 96$ باقي ممكن لـ $x \pmod{1001}$

(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.

في كل من المجموعات التالية يوجد 96 قيمة لـ n

تكون 7-safe, 11-safe, 13-safe

$\{1, 2, \ldots, 1001\} \rightarrow 96$

$\{1002, \ldots, 2002\} \rightarrow 96 \Rightarrow$

$\vdots$

$\{9010, \ldots, 10010\} \rightarrow 96$

960 عدد صالح

من 1 الى 10010

ولكن في المجموعة

$\{10001, \ldots, 10010\}$ يوجد عدد صالحان (10006, 10007).

$\Leftarrow$ عدد الأعداد الصالحة من 1 إلى 10000 هو $960 - 2 = 958$

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

- if $p \mid c \Rightarrow x = p$
- if $\gcd(p, c) = 1$:

* قوة CRT هي قدرتنا على تجميع عدد .
مثلاً

$$\begin{cases} x \equiv i \pmod{p-1} \\ x \equiv j \pmod p, \quad \underline{j \neq 0} \end{cases}$$

الأس ← دورية $\mod (p-1)$

الأساس ← دورية $\mod (p)$

$$x^x \equiv j^x \pmod p \Rightarrow x^x \equiv j^{(p-1)k+i} \equiv \underbrace{j^i}_{\equiv c} \pmod p$$

$x = (p-1)k + i$

$$\begin{cases} x \equiv 1 \pmod{p-1} \\ x \equiv c \pmod p \end{cases} \Rightarrow$$ يوجد حل من CRT

نختار $j = c, \ i = 1$
أو مثلاً:

$$x = p(p-c) + c$$

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

حل
إياد

متغيرين

$x^x \equiv c\ [p]$

let $x = y + (p-1)k$ s.t $y \in \mathbb{Z}^+$, $k \in \mathbb{Z}$

x^x

$\equiv (y+(p-1)k)^{y+(p-1)k} \equiv (y-k)^y \cdot \underbrace{(y-k)^{p-1}}_{\equiv 1}{}^k \equiv \boxed{(y-k)^y} \equiv c\ [p]$

$y + (p-1)k \equiv y - k\ [p]$

غير قيمة k

The set

$\{y^y, (y-1)^y, (y-2)^y, \dots, (y-(p-1))^y\} \equiv \{0, 1, 2, \dots, p-1\}\ [p]$

أثبتنا مسبقاً

if $\gcd(y, p-1) = 1$.

one of the elements of the set $\equiv c\ [p]$ because it's a complete residue class.

$\Rightarrow$ if $\gcd(y, p-1) = 1$

$\Rightarrow x^x \equiv (y-k)^y \equiv c\ [p]$ for some k $(p-1 \geq k \geq 0)$

(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 $a = b$.*

$$a^n + n \mid b^n + n \quad \forall\, n \in \mathbb{N}$$

$$\Rightarrow \quad a^n + n \mid b^n - a^n \quad \forall\, n \in \mathbb{N}$$

نريد إثبات أن $b^n - a^n$ يساوي صفر أو $b^c - a^c$ يساوي صفر حيث أن c عدد ثابت.

بشكل عام:

* أحد طرق إثبات أن مقدار ثابت يساوي 0 هو إثبات أنه يقبل القسمة على عدد لانهائي من الأعداد / أو إثبات أنه يقبل القسمة على عدد أكبر منه.

(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 $a = b$.*

نريد إيجاد عدد أولي p حيث أن

$$\begin{cases} p \mid a^n + n \\ n \equiv c \pmod{p-1} \end{cases} \Rightarrow$$ (للنزول من الأس n إلى c)

نختار $c = 1$،

$$\begin{cases} p \mid a^n + n \\ n \equiv 1 \pmod{p-1} \end{cases} \iff \boxed{\begin{cases} n \equiv -a \pmod{p} \\ n \equiv 1 \pmod{p-1} \end{cases}} \; *$$

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

[من CRT يوجد n محقق * لكل p عدد أولي.

(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 $a = b$.*

الحل الرسمي :

لكل p عدد أولي نعرف n_p عدد صحيح موجب حيث أن

$$① \begin{cases} n_p \equiv -a \pmod{p} \\ n_p \equiv 1 \pmod{p-1} \end{cases}$$

واضح أن n_p موجودة من CRT لأن $\gcd(p, p-1) = 1$.

$$a^{n_p} \equiv a^1 \pmod{p} \Rightarrow a^{n_p} + n_p \equiv a + n_p \equiv a + (-a) \pmod{p}$$

$$\Rightarrow p \mid a^{n_p} + n_p \quad ②$$

بما أن $p \mid a^{n_p} + n_p$ فإن $p \mid b^{n_p} + n_p$ من شرط السؤال

(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 $a = b$.*

إذن

$$p \mid a^{np} - b^{np}$$

$$\Rightarrow \quad a^{np} \equiv b^{np} \pmod{p} \quad (3)$$

ولكن $np \equiv 1 \pmod{p-1}$ من (1) ، إذن

$$a^{np} \equiv a \pmod{p}$$
$$b^{np} \equiv b \pmod{p}$$

$$\overset{(3)}{\Longrightarrow} \quad a \equiv b \pmod{p}$$

إذن لكل عدد أولي p يوجد n_p يجعل $p \mid b-a$

بالتالي $b-a$ تقبل القسمة على عدد لانهائي من الأعداد الأولية $\Leftarrow b-a=0 \Leftarrow b=a$

(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.*]*

Example 2.4.2 (Korea 1999). *Find all positive integers* n *such that* $2^n - 1$ *is a multiple of 3 and* $(2^n - 1)/3$ *is a divisor of* $4m^2 + 1$ *for some integer* m.