Modular Arithmetic and Residue Classes

Number Theroy
June 6, 2020

If a and b are relatively prime integers, show that ab and $a+b$ are also relatively prime.

$$\gcd(ab, a+b) = d, \quad d \in \mathbb{Z}^+, \quad d \neq 1$$

$$\Rightarrow \quad d \mid ab - b(a+b)$$

$$d \mid ab - ba - b^2 \Rightarrow d \mid b^2$$

$$d \mid ab - a(a+b) \Rightarrow d \mid a^2$$

p - prime, $p \mid d \Rightarrow \begin{matrix} p \mid a^2 \\ p \mid b^2 \end{matrix} \Rightarrow \begin{matrix} p \mid a \\ p \mid b \end{matrix} \Rightarrow \gcd(a,b) \geq 1$

If a and b are relatively prime integers, show that ab and $a+b$ are also relatively prime.

p - prime, $p \mid d$

$\Rightarrow p \mid ab \Rightarrow p \mid a$ or $p \mid b$

Assume that $p \mid a \Rightarrow p \mid a+b$, $p \mid a$ $\Rightarrow p \mid b$

$\Rightarrow \gcd(a,b) \geq p > 1$

Example 1.20. Prove that there are infinitely many primes of the form $4k-1$; that is, congruent to 3 modulo 4.

$S = \{p_1, p_2, \dots, p_k\}$

$P = p_1 p_2 \cdots p_k$,

$4P - 1 \equiv -1 \pmod 4$

$\underbrace{4P-1}_{\text{odd}} = q_1^{\alpha_1} q_2^{\alpha_2} \cdots q_{k_0}^{\alpha_{k_0}}$

$q_i^{\alpha_i} \equiv -1 \pmod 4$

$q_i \equiv \pm 1 \pmod 4$

$\Rightarrow q_i \equiv -1 \pmod 4$

$\exists\, i \in \{1, \dots, k_0\}$

$q_i \equiv -1 \pmod 4$

$\Rightarrow q_i \in S$

ولكن

$P = p_1 \cdots p_k$

$\Rightarrow q_i \mid P,\ q_i \mid 4P-1$

$\Rightarrow q_i \mid 1 \Rightarrow \Leftarrow !!$

[Baltic 2001] Let a be an odd integer. Prove that $a^{2^n}+2^{2^n}$ and $a^{2^m}+2^{2^m}$ are relatively prime for all positive integers n and m with $n \neq m$.

$$\gcd\left(a^{2^n}+2^{2^n},\ a^{2^m}+2^{2^m}\right)=d=1$$

$$\Rightarrow \begin{cases} a^{2^n}+2^{2^n}\equiv 0 \pmod d \\ a^{2^m}+2^{2^m}\equiv 0 \pmod d \end{cases} \Rightarrow \begin{cases} a^{2^n}\equiv -2^{2^n} \pmod d \\ a^{2^m}\equiv -2^{2^m} \pmod d \end{cases} *$$

$$\left(a^{2^n}\right)^2\equiv\left(-2^{2^n}\right)^2 \pmod d \Rightarrow a^{2^{n+1}}\equiv 2^{2^{n+1}} \pmod d$$

$$\Rightarrow \cdots \Rightarrow a^{2^s}\equiv 2^{2^s} \pmod d \quad \forall\ s\in\mathbb{Z}^+,\ s\geq n+1$$

Assume $m>n$

$$a^{2^m}\equiv 2^{2^m} \pmod d \Rightarrow -2^{2^m}\equiv 2^{2^m} \pmod d$$

$d=1 \Leftarrow$ فردي d ولكن $\Rightarrow d \mid 2^{2^m}+2^{2^m}=2\cdot 2^{2^m}=2^{2^n+1}$

Residue Classes

$S = \{a_1, a_2, \ldots, a_k\}$

$T_m = \{ b_i \mid b_i \equiv a_i \pmod{m} \}$

$S = \{4, 7, 10\}$

$T_3 = \{1\}$

$T_4 = \{0, 3, 2\}$

إذا كانت $|T_m| = m$

فإن T_m و S تكونان

مجموعة بواقي

كاملة mod m.

مثال $S = \{3, 5, 11, 7\}$

مجموعة بواقي كاملة

mod 3

$T_5 = \{0, 2, 1\}$

$|T_5| = 3$

Residue Classes

S هي مجموعة بواقي كاملة mod m ، إذا كان

$\forall\, i \in \{1, \ldots, m\}$ $\exists\, s \in S$ such that

$s \equiv i \pmod{m}$

مثال: $S = \{3, 5, 7, 11\}$ مجموعة بواقي كاملة mod 3 .

$\forall\, i \in \{1, 2, 3\}$ $\exists\, j \in S$ such that $j \equiv i \pmod 3$

يوجد $\in S$

$i = 1$, $7 \equiv 1 \pmod 3$

$i = 2$ $5 \equiv 2 \pmod 3$

$i = 3$ $3 \equiv 3 \pmod 3$

(1) $n^2 \equiv 0$ or $1 \pmod 3$;

(2) $n^2 \equiv 0$ or $\pm 1 \pmod 5$;

(3) $n^2 \equiv 0$ or 1 or $4 \pmod 8$;

(4) $n^3 \equiv 0$ or $\pm 1 \pmod 9$;

(5) $n^4 \equiv 0$ or $1 \pmod{16}$;

$\{0^4, 1^4, \ldots, 15^4\} \equiv \{0, 1\}$

$\{0^4, (\pm 1)^4, (\pm 2)^4, \ldots, (\pm 8)^4\} \bmod 16$

(1) $S = \{n^2 \mid n \in \mathbb{Z}\}$

$T_3 = \{0, 1\}$

$T_5 = \{0, 1, -1\}$; $T_5 = \{0, 1, 4\}$

$\{-\frac{m}{2}, \frac{m}{2}\}$

$\{0, m\}$

$|T_m| \leq m$

5, 7

11, 13, 17

1 [Romania 2003] Consider the prime numbers $n_1 < n_2 < \cdots < n_{31}$. Prove that if 30 divides $n_1^4 + n_2^4 + \cdots + n_{31}^4$, then among these numbers one can find three consecutive primes.

$30 \mid \underbrace{n_1^4 + n_2^4 + \cdots + n_{31}^4}$, $n_1, n_2, \longrightarrow n_{31}$ are primes

زوجي

$\Rightarrow n_1 = 2$

$n_2 \overset{?}{=} 3$:

افترض أن $n_2 \neq 3 \Leftarrow n_i^4 \equiv 1 \pmod 8$

$\Rightarrow \sum_{1}^{31} n_i^4 \equiv 31 \equiv 1 \pmod 3 \Rightarrow \Leftarrow !!$

ولكن $30 \mid \sum_{i=1}^{31} n_i^4$

$\Rightarrow n_2 = 3$

[Romania 2003] Consider the prime numbers $n_1 < n_2 < \cdots < n_{31}$. Prove that if 30 divides $n_1^4 + n_2^4 + \cdots + n_{31}^4$, then among these numbers one can find three consecutive primes.

$n_3 \overset{?}{=} 5$:

افترض $n_3 \neq 5$ $\Leftarrow$

$n_i^4 \equiv 1 \pmod 5$

$\Rightarrow \sum_{1}^{31} n_i^4 \equiv 31 \pmod 5 \equiv \underline{1 \pmod 5}$

ولكن $30 \mid \sum_{i=1}^{31} n_i^4 \Leftarrow \underline{5 \mid \sum_{i=1}^{31} n_i^4} \Leftarrow \Rightarrow$!!

$\Rightarrow \boxed{n_3 = 5}$ ✓ $\boxed{2, 3, 5}$ ✓

2 Let m be an even positive integer. Assume that

$$\{a_1, a_2, \ldots, a_m\} \quad \text{and} \quad \{b_1, b_2, \ldots, b_m\}$$

are two complete sets of residue classes modulo m. Prove that

$$\{a_1 + b_1, a_2 + b_2, \ldots, a_m + b_m\}$$

is not a complete set of residue classes.

$$\{a_1, a_2, \ldots, a_m\} \equiv \{1, 2, \ldots, m\} \pmod{m}$$

$$a_1 + a_2 + \cdots + a_m \equiv 1 + 2 + \cdots + m \pmod{m}$$

$$a_1 + \cdots + a_m \equiv \frac{m(m+1)}{2} \pmod{m}$$

$$b_1 + \cdots + b_m \equiv \frac{m(m+1)}{2} \pmod{m}$$

بالمثل

$$(a_1 + b_1) + \cdots + (a_m + b_m) \equiv \frac{m(m+1)}{2} \pmod{m}$$

Let m be an even positive integer. Assume that

$$\{a_1, a_2, \ldots, a_m\} \quad \text{and} \quad \{b_1, b_2, \ldots, b_m\}$$

$\{1, \ldots, m\}$

are two complete sets of residue classes modulo m. Prove that

$$\{a_1 + b_1, a_2 + b_2, \ldots, a_m + b_m\}$$

is not a complete set of residue classes.

$$\underbrace{(a_1 + \cdots + a_m)} + \underbrace{(b_1 + \cdots + b_m)} = \sum_{i=1}^{m} (a_i + b_i)$$

$$\Rightarrow \frac{m(m+1)}{2} + \frac{m(m+1)}{2} \equiv \frac{m(m+1)}{2} \pmod{m}$$

$$\Rightarrow 0 \equiv \frac{m(m+1)}{2} \pmod{m}$$

$$\Rightarrow \rightarrow m \mid \frac{m(m+1)}{2} \Rightarrow \frac{m+1}{2} \in \mathbb{Z} \Rightarrow \Leftarrow !!$$

$/m$

m is even

3 Let a be a positive integer. Determine all the positive integers m such that

$$\{a \cdot 1, a \cdot 2, a \cdot 3, \ldots, a \cdot m\}$$

عدد m

is a set of complete residue classes modulo m.

$\Rightarrow \quad a \cdot i \not\equiv a \cdot j \pmod{m} \quad \forall \; i \neq j$

$i, j \in \{1, \ldots, m\}$

$\Rightarrow \quad m \nmid a_i - a_j \Rightarrow m \nmid a(i-j)$

$0 < |i-j| \leq m-1$

• إذا كان $1 = \gcd(m,a) \Leftarrow$

$m \nmid (i-j)$

$0 < |i-j| \leq m-1 \Rightarrow$ تناقض

• إذا كان $\gcd(m,a) = d$

Let a be a positive integer. Determine all the positive integers m such that

$$\{a \cdot 1, a \cdot 2, a \cdot 3, \ldots, a \cdot m\}$$

is a set of complete residue classes modulo m.

إذا كان $\gcd(m, a) = d$

$m \nmid a(i-j)$

$i = \frac{m}{d} \in \mathbb{Z} \Rightarrow m \nmid a \cdot \left(\frac{m}{d}\right)$

$j = 1 \Rightarrow m \nmid \underbrace{\left(\frac{a}{d}\right)}_{\in \mathbb{Z}} m \Rightarrow\Leftarrow$ تناقض

إذن مجموعة الحل هي الأعداد الأولية نسبياً مع a.

4 Let m be a positive integer. Let a be an integer relatively prime to m, and let b be an integer. Assume that S is a complete set of residue classes modulo m. The set

$$T = aS + b = \{as + b \mid s \in S\}$$

is also a complete set of residue classes modulo m

3 $T_1 = \{as \mid s \in S\}$ مجموعة بواقي كاملة

لأن S مجموعة بواقي كاملة و $\gcd(a,m)=1$

$T_1 = \{a\cdot 1, a\cdot 2, \dots, a\cdot m\}$

$T = \{t+b \mid t \in T_1\} \Rightarrow T = \{1+b, 2+b, \dots, m+b\}$

لأن T_1 مجموعة بواقي كاملة

$r \quad r+1 \quad \dots, m-1, 0, \dots, r-1$

* بما أن $|T| = m$ و لا يوجد عنصران متطابقان $\equiv \pmod m$ $\Leftarrow$ T مجموعة بواقي كاملة

$i+b \equiv j+b \pmod m \Leftrightarrow i \equiv j \pmod m$

5 Let m be a positive integer. Let a be an integer relatively prime to m, and let b be an integer. There exist integers x such that $ax \equiv b \pmod{m}$, and all these integers form exactly one residue class modulo m.

$b_r = b \pmod{m}$

$S = \{ax \mid x \in \{1, \dots, m\}\} = \{a1, a2, \dots, am\}$

جميع البواقي الممكنة

$\downarrow \pmod{m}$

$\Rightarrow$ S مجموعة بواقي كاملة $\equiv \{0, 1, 2, \dots, b_r, \dots, m\}$

$\Rightarrow \exists\, x$ such that $ax \equiv b_r \equiv b \pmod{m}$

بما أن $|S| = m$ ، فإنه يوجد عنصر وحيد x يحقق أن $ax \equiv b \pmod{m}$

في $\{1, \dots, m\}$

أو $\{0, \dots, m-1\}$

inverse of a (mod

النظير الضربي لـ a ، a' ، $\bmod m$ يحقق

$$a\,a' \equiv 1 \pmod m$$

متى يوجد النظير الضربي ؟

① لو كان $\gcd(a,m)=d$ $\Leftarrow$ $d \mid aa'-1$ $\Leftarrow$ $d \mid 1$

$d=1$

② لو كان $\gcd(a,m)=1$ ، من مسألة ⑦ نعتبر $b=1$

يوجد x وحيد $\bmod m$ يحقق $ax \equiv 1 \pmod m$ $\Leftarrow$ نأخذ $x=a'$

inverse of a (mod

$a\,a' \equiv 1 \pmod m$, $\underline{a' \equiv b'} \pmod m$

$b\,b' \equiv 1 \pmod m$

$\overset{?}{\Longrightarrow} \quad a \equiv b \pmod m$

• نعم ، لأن a هو نظير a' و b هو نظير b'

ولكن $a' \equiv b'$ ويوجد لدينا نظير وحيد $\Leftarrow a \equiv b \pmod m$

• أو

$ar \equiv br \pmod m \Rightarrow a \equiv b \pmod m$

[Wilson's Theorem] For any prime p, $(p-1)! \equiv -1 \pmod{p}$.

1.2. -- $(p-1) \equiv -1 \pmod{p}$

- $p=2 \Rightarrow 1 \equiv -1 \pmod{2}$ ✓
- $p=3 \Rightarrow 2 \equiv -1 \pmod{3}$
- $p \geq 5$

$\forall\ s \in \{1, \dots, p-1\}\ \exists\ s'$ such that $ss' \equiv 1 \pmod{p}$

لأن $\gcd(s,p)=1$.

① لكل s يوجد s' وحيد.

② $s \equiv s'$ فقط عندما $s=1$ أو $s=p-1$ (لأن $s^2 \equiv 1 [p] \Rightarrow s \equiv \pm 1 [p]$)

[Wilson's Theorem] For any prime p, $(p-1)! \equiv -1 \pmod{p}$.

إذن بالنسبة لـ $\{2, 3, \ldots, p-2\}$ لكل عدد يوجد

نظير ضربي وحيد مختلف عن العدد نفسه

$$2 \cdot 3 \cdot \ldots (p-2) = \underbrace{(x)^{=1}(x)^{=1} \ldots (x)^{=1}}_{\text{زوج } \frac{p-3}{2}} \equiv 1 \pmod{p}$$

$$\Rightarrow (p-1)! \equiv (2 \cdot 3 \cdot \ldots (p-2))(p-1) \equiv 1(p-1) \equiv -1 \pmod{p}$$

بالنسبة لـ $p \geq 5$.

Bézout's identity

$\forall\ a, b \in \mathbb{Z} \quad \exists\ x, y \in \mathbb{Z}$ such that

$$ax + by = \gcd(a, b)$$

الإثبات:

$d = \gcd(a, b)$

$a = d\,a'$, $b = d\,b'$, $\gcd(a', b') = 1$

$\Rightarrow \quad ax + by = d \iff a'x + b'y = 1$

$\iff \quad a'x = (-y)\,b' + 1 \quad \exists\, y \in \mathbb{Z} \iff a'x \equiv 1 \pmod{b'}$

ولكن بما أن $\gcd(a', b') = 1$ ، فإنه يوجد نظير ضربي لـ a'

$\exists\, x \in \mathbb{Z}$ such that $a'x \equiv 1 \pmod{b'}$ $\Leftarrow$ $(\bmod\ b')$

7 Let m be a positive integer, and let a and b be integers relatively prime to m. If x and y are integers such that

$$a^x \equiv b^x \pmod{m} \quad \text{and} \quad a^y \equiv b^y \pmod{m},$$

then

$$a^{\gcd(x,y)} \equiv b^{\gcd(x,y)} \pmod{m}.$$

$a^x \equiv b^x \pmod{m} \Rightarrow a^{xu} \equiv b^{xu} \pmod{m}$ ①

$a^y \equiv b^y \pmod{m} \Rightarrow a^{yv} \equiv b^{yv} \pmod{m}$ ②

بضرب ① في ②

$\Rightarrow a^{xu+yv} \equiv b^{xu+yv} \pmod{m}$

هل يمكن كتابة $\gcd(x,y)$ على الصيغة $xu+yv$؟

حيث أن u و v أعداد صحيحة موجبة

Let m be a positive integer, and let a and b be integers relatively prime to m. If x and y are integers such that

$$a^x \equiv b^x \pmod{m} \quad \text{and} \quad a^y \equiv b^y \pmod{m},$$

then

$$a^{\gcd(x,y)} \equiv b^{\gcd(x,y)} \pmod{m}.$$

$$a^{-yv} \equiv b^{-yv} \pmod{m} \Rightarrow a^{xu-yv} \equiv b^{xu-yv} \pmod{m}$$

$$a^{xu} \equiv b^{xu} \pmod{m}$$

$$\Rightarrow a^{xu+yv} \equiv b^{xu+yv} \pmod{m}$$

لكل الأعداد الصحيحة u, v ، ومن بيزوه يوجد u, v يحققان

أن $xu+yv = \gcd(x,y)$

* يمكن حل هذه المسألة باستخدام أويلر

Fermat's little theorem. Let p be a prime number.

(a) Show that if k is an integer with $0 < k < p$, then $\binom{p}{k}$ is divisible by p.

(b) Show that if $a \in \mathbb{Z}$, then $(a+1)^p \equiv a^p + 1 \pmod{p}$.

(c) Show that if $a \in \mathbb{Z}$, then $a^p \equiv a \pmod{p}$.

(d) Show that if a is an integer not divisible by p, then $a^{p-1} \equiv 1 \pmod{p}$.