Fermat’s Little Theorem and Euler’s Theorem

7 June, 2020

From last lecture:

Corollary 1.21. Let m be a positive integer, and let a, b, and c be integers with $c \neq 0$. If $ac \equiv bc \pmod{m}$, then

$$a \equiv b \left(\bmod \frac{m}{\gcd(c, m)} \right).$$

$m \mid ac - bc$

$\Rightarrow m \mid (a-b)c$

$\Rightarrow \frac{m}{\gcd(m,c)} \mid a-b$

* **Corollary 1.23.** 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

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

$xu + yv = \gcd(x,y)$

$x, y \geq \gcd(x,y) \Rightarrow$

u, v أحدهما سالب.

نفرض أن

$v' = -v \ , \ v' \geq 0 \Leftarrow v \leq 0 \ , \ u \geq 0$

$\Rightarrow \boxed{xu - yv' = \gcd(x, y)} \leftarrow$ الهدف

$a^{xu} \equiv b^{xu} \pmod m \ , \ a^{yv'} \equiv b^{yv'} \pmod m$

$\Rightarrow a^{xu} \, b^{yv'} \equiv b^{xu} \cdot a^{yv'} \pmod m$

$\gcd(a, m) = \gcd(b, m)$

$xu > yv'$,

$\Rightarrow a^{yv'} \left(a^{xu - yv'} \right) b^{yv'} \equiv b^{yv'} \left(b^{xu - yv'} \right) \cdot a^{yv'} \pmod m$

$\Rightarrow a^{\boxed{xu - yv'}} \equiv b^{xu - yv'} \pmod m$ ← موجب

* لماذا $a^{\gcd(x,y)} \equiv b^{\gcd(x,y)} \pmod m$ صحيحة ؟

بدأنا بـ a^x, b^x, a^y, b^y $\xRightarrow{\text{تقليص للأس}}$ $a^{\gcd(x,y)} \equiv b^{\gcd(x,y)}$

* لو كان الـ $\gcd(x,y)$ معروف :

• مثال $\gcd(x,y)=1 \Rightarrow a \equiv b \pmod m$

• $\gcd(x,y)=2,3,p$ ... ...

* لو كانت $m \geq a^{\gcd(x,y)}$

$$m \mid \underline{\underline{a^{\gcd(x,y)} - b^{\gcd(x,y)}}}$$

$$a^{\gcd(x,y)} - b^{\gcd(x,y)} = 0 \Rightarrow a=b$$

Summary of last lecture:

* مجموعة البواقي الكاملة -

* إذا كانت S مجموعة بواقي كاملة و $|S| = m$.

$$\Longrightarrow \quad \sum_{i=1}^{m} s_i \equiv \sum_{i=0}^{m-1} i \pmod{m}$$

$$\prod_{i=1}^{m} s_i \equiv m! \pmod{m} \quad , \quad \prod_{\substack{i=1 \\ i \neq k_0}}^{m} s_i \equiv (m-1)! \pmod{m}$$

$(s_{k_0} \equiv 0)$

* النظير الضربي $\Leftarrow$ نظرية ويلسون .

1 **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 $a^{p-1} \equiv 1 \pmod{p}$.

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

$$\Rightarrow \quad 1^p \equiv 1 \pmod{p}$$

$a := 1$

$$2^p \equiv 1+1 \equiv 2 \pmod{p}$$

$a := 2$

$$\Rightarrow \quad 3^p \equiv (2)^p + 1 \equiv 2+1 \pmod{p}$$
$$\equiv 3 \pmod{p}$$

بالاستقراء الرياضي

$a \in \{1, \dots, k\}$ لكل $a^p \equiv a \pmod{p}$

$$(k+1)^p \equiv k^p + 1 \equiv k+1 \pmod{p}$$

2 **Another look at Fermat's little theorem.** Let p be a prime number, and a an integer not divisible by p.

(a) Show that $\{a, 2a, 3a, \ldots, (p-1)a\} \equiv \{1, 2, 3, \ldots, p-1\} \pmod{p}$.

(b) Show that $a \cdot 2a \cdot 3a \cdot \cdots \cdot (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdot \cdots \cdot (p-1) \pmod{p}$.

(c) Conclude that $a^{p-1} \equiv 1 \pmod{p}$.

(c) $a^{p-1} \cdot (p-1)! \equiv (p-1)! \pmod{p}$

$p \nmid (p-1)!$

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

3 **Euler's totient function.** We use $\phi(n)$ to denote the number of elements in $\{1, 2, \ldots, n\}$ that are relatively prime to n. That is, $\phi(n) = |\mathbb{Z}_n^*|$.

(a) Compute $\phi(7)$ and $\phi(24)$.

(b) Compute $\phi(p^n)$, where p is a prime and n is a positive integer.

(c) Show that if m and n are relatively prime integers, then $\phi(mn) = \phi(m)\phi(n)$.

(d) Find a formula for computing $\phi(n)$ in terms of the prime factorization of n.

a) $\phi(7) = 6$

$\phi(24) = 8$ $\quad (1, 5, 7, 11, 13, 17, 19, 23)$

b) $\phi(p^n) =$ عدد الأرقام الأولية نسبياً مع p^n

= عدد الأرقام الأولية نسبياً مع p = عدد الأرقام التي لا تقبل القسمة على p

$$|\{s \mid p \mid s, s \le p^n\}| = \frac{p^n}{p} = p^{n-1} \Rightarrow \{s \mid p \nmid s, s \le p^n\} = p^n - p^{n-}$$

عدد اولي نسبياً مع a $\varphi(b)$

a

$1+0$	$2+0$	3	k	j	a	
$1+a$	$2+a$	$3+a$	$a+k$	$j+a$	$2a$	
$1+2a$	$2+2a$	$3+2a$	$2a+k$		$3a$	b
$1+(b-1)a$	$2+(b-1)a$			$j+(b-1)a$	ba	

$\varphi(b)$

$\gcd(a,b)=1$

مجموعة جزئية كاملة mod b

عدد الأعداد الأولية نسبياً مع ab $= \phi(ab)$

$k, \quad \gcd(a,k)>1 \Rightarrow \gcd(ab,k)>1$

$\gcd(ab, at+k)>1$

① يوجد $\varphi(a)$ عمود عناصره أولية نسبياً مع a.

② كل عمود يملك مجموعة بواقي كاملة $\bmod b$، لأن الأعداد على الصيغة $k+ai$ حيث أن k ثابت و $i \in \{1, \dots, b\}$ و $\gcd(a,b)=1$

← في مجموعة البواقي الكاملة $(\bmod\ b)$، يوجد $\boxed{\varphi(b)}$ عدد أولي نسبياً مع b.

$$\varphi(ab) = \underline{\varphi(b)} \cdot \underline{\varphi(a)}$$

عدد الأعداد الأولية نسبياً مع b في كل عمود أزرق

عدد الأعمدة التي عناصرها أولية نسبياً مع a

d) $\varphi(n)$, $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$

(part c)

$$\varphi(n) = \varphi(\underbrace{p_1^{\alpha_1}}_{m} \underbrace{\cdots p_k^{\alpha_k}}_{n}) = \varphi(p_1^{\alpha_1})\,\varphi(\underbrace{p_2^{\alpha_2}}_{m} \underbrace{\cdots p_k^{\alpha_k}}_{n})$$

$$= \varphi(p_1^{\alpha_1})\,\varphi(p_2^{\alpha_2})\,\varphi(p_3^{\alpha_3} \cdots p_k^{\alpha_k})$$

$$= \varphi(p_1^{\alpha_1}) \cdots \varphi(p_k^{\alpha_k})$$

$$= \prod_{i=1}^{k} (p_i^{\alpha_i} - p_i^{\alpha_i - 1}) = \prod_{i=1}^{k} p_i^{\alpha_i - 1}(p_i - 1) \ *$$

part b

$$= \prod_{i=1}^{k} \underline{\underline{p_i^{\alpha_i}}} \left(1 - \frac{1}{p_i}\right) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_k}\right)$$

طريقة أخرى لحساب $\varphi(n)$.

$n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$

$\rightarrow T_i = \{d : d \leq n \text{ and } p_i \mid d\} \quad \forall\, i \in \{1, \dots, k\}$

$|T_i| = \frac{n}{p_i}$

العناصر الغير أولية نسبياً

$$\varphi(n) = \underline{\underline{n -}}\ |T_1 \cup T_2 \cup \cdots \cup T_k|$$

$$|T_1 \cup \cdots T_k| = \sum |T_i| - \sum |T_i \cap T_j| + \sum |T_i \cap T_j \cap T_k| \cdots$$

$$= (-1)^{k-2} \sum |T_{i_1} \cap \cdots \cap T_{i_{k-1}}| + (-1)^{k-1} |T_1 \cap \cdots \cap T_k|$$

$|T_{i_1} \cap T_{i_2} \cap \cdots \cap T_{i_m}|$ = عدد الأعداد التي تقبل القسمة على $p_{i_1}, p_{i_2}, \ldots, p_{i_m}$

= عدد الأعداد التي تقبل القسمة على $p_{i_1} p_{i_2} \ldots p_{i_m}$

$$= \frac{n}{p_{i_1} \cdots p_{i_m}}$$

$$\Rightarrow \varphi(n) = n - \sum \frac{n}{p_i} + \sum \frac{n}{p_i p_j} - \sum \frac{n}{p_{i_1} p_{i_2} p_{i_3}}$$

$$+ \cdots + (-1)^k \frac{n}{p_1 \cdots p_k} = n\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_n}\right)$$

Euler's Theorem Let a and m be relatively prime integers.

(a) Let $\mathbb{Z}_n^* = \{r_1, r_2, \ldots, r_{\phi(n)}\}$ be the set of positive integers less than n and relatively prime to n. Show that

$$\{r_1, r_2, \ldots, r_{\phi(n)}\} \equiv \{ar_1, ar_2, \ldots, ar_{\phi(n)}\} \pmod{n}.$$

where $\gcd(a, n) = 1$

(b) Show that $a^{\phi(m)} \equiv 1 \pmod{m}$.

A set S of integers is also called a **reduced complete set of residue classes** modulo m if for each i with $0 \leq i \leq n-1$ and $\gcd(i, m) = 1$, there is an element $s \in S$ such that $i \equiv s \pmod{m}$. It is clear that a reduced complete set of residue classes modulo m consists of $\varphi(m)$ elements.

For a given positive integer m, let $\{a_1, a_2, \ldots, a_{\varphi(m)}\}$ be a reduced complete set of residue classes modulo m. By the existence and uniqueness of inverses, it is not difficult to see that the set of their inverses, denoted by

$$\{a_1^{-1}, a_2^{-1}, \ldots, a_{\varphi(m)}^{-1}\} \quad \text{or} \quad \left\{\frac{1}{a_1}, \frac{1}{a_2}, \ldots, \frac{1}{a_{\varphi(m)}}\right\},$$

is also a reduced complete set of residue classes modulo m.

Consider the sequence $a_1, a_2, \ldots$ defined by

$$a_n = 2^n + 3^n + 6^n - 1$$

Find an infinite nonconstant arithmetic progression of positive integers such that each term is not a sum of two perfect cubes.

What is the smallest positive integer t such that there exist integers $x_1, x_2, \ldots, x_t$ with

$$x_1^3 + x_2^3 + \ldots + x_t^3 = 2002^{2002} ?$$

Theorem [Gauss] For any positive integer n,

$$\sum_{d|n} \varphi(d) = n.$$