Fermat's and Euler's Theorems

Wednesday, 9 March 2022 14:06

Clarification:

For finite rings with unity,

Integral Domains = Division Rings = Fields

$= \mathbb{F}_q$ (finite field of q elements)
$q = p^n$

Theorem: Let R be a ring with unity 1. $R^\times = \{\text{units}\}$. Then $(R^\times, \cdot)$ is a group

Proof: (0) $R^\times$ is closed under $\cdot$

$a, b \in R^\times$, i.e., $ac = 1$, $bd = 1$ for $c, d \in R^\times$

$(ab)(dc) = a(bd)c = ac = 1$

So $ab \in R^\times$

(1) $\cdot$ is associative follows from the axiom of R

(2) $1 \in R^\times$ b/c $1 \cdot 1 = 1$

(3) $a \in R^\times \Rightarrow ab = 1,\ b \in R^\times$

$\Rightarrow b = a^{-1} \in R^\times$. $\square$

Goal: Use the group structure of $\mathbb{Z}_n^\times$ to do "basic" arithmetics.

$\mathbb{Z}_p^\times = \{1, \dots, p-1\}$

Thm (Fermat's Little Theorem): If $a \in \mathbb{Z}$ is not a multiple of p, then $a^{p-1} \equiv 1 \pmod{p}$.

Proof: If $a \not\equiv 0 \pmod{p}$, then $a \in \mathbb{Z}_p^\times$. So the order k of a divides $|\mathbb{Z}_p^\times| = p-1$.

$$a^{p-1} = (a^k)^{\frac{p-1}{k}} = 1^{\frac{p-1}{k}} = 1 \text{ in } \mathbb{Z}_p^\times$$

$$a^{p-1} \equiv 1 \pmod{p} \qquad \square$$

Corollary: For any $a \in \mathbb{Z}$,

$$a^p \equiv a \pmod{p}.$$

Proof: If $a \not\equiv 0 \pmod{p}$, then FLT

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

If $a \equiv 0 \pmod{p}$, then

$$a^p \equiv 0 \equiv a \pmod{p}. \qquad \square$$

Example: Find $5^{102} \pmod{13}$

(RSA system)

By FLT, $5^{12} \equiv 1 \pmod{13}$.

$$5^{102} \equiv 5^{12 \times 8 + 6} \equiv (5^{12})^8 \cdot 5^6$$

$$\equiv 1^8 \cdot 5^6 \equiv (5^2)^3$$

$\equiv (25)^3 \equiv (-1)^3$
$\equiv -1 \equiv 12 \pmod{13}.$

How about $\mathbb{Z}_n^\times$? $a \in \mathbb{Z}_n$ is a unit $\Leftrightarrow$ $\gcd(a,n) = 1$.

Pick any $A \in \mathbb{Z}$ s.t. $A \equiv a \pmod{n}$

$\gcd(a,n) := \gcd(A,n)$.

Suppose we chose another $A' \in \mathbb{Z}$ s.t. $A' \equiv a \pmod{n}$. $A' = A + nr$

$$\gcd(A',n) = \gcd(A+nr, n) = \gcd(A,n).$$

Def: $\varphi(n) := |\mathbb{Z}_n^\times|$

$= \#\{1 \leq a \leq n : \gcd(a,n) = 1\}$.

(Euler phi / totient function)

Examples: $\varphi(5) = |\{1,2,3,4\}| = 4$

$\varphi(6) = |\{1,5\}| = 2$

$\varphi(10) = |\{1,3,7,9\}| = 4$

Thm (Euler): If $\gcd(a,n)=1$, then $a^{\varphi(n)} \equiv 1 \pmod{n}$.

Proof: Since $\gcd(a,n)=1$, $a \in \mathbb{Z}_n^\times$, and the order k of a in $(\mathbb{Z}_n^\times, \cdot)$ divides $|\mathbb{Z}_n^\times|$ by Lagrange thm.

$$a^{\varphi(n)} = (a^k)^{\frac{\varphi(n)}{k}} = 1^{\frac{\varphi(n)}{k}} = 1 \text{ in } \mathbb{Z}_n$$

$$a^{\varphi(n)} \equiv 1 \pmod{n} \qquad \square$$

Example: $5^{102} \pmod{12}$

$\varphi(12) = |\{1, 5, 7, 11\}| = 4$

By Euler thm, $5^4 \equiv 1 \pmod{12}$

$$5^{102} \equiv 5^{4\times 25+2} \equiv (5^4)^{25} \cdot 5^2$$
$$\equiv 1^{25} \cdot 5^2 \equiv 1 \pmod{12}.$$

Example: Show that $n^{33} - n$ is always divisible by 15.

If $\gcd(n, 15) = 1$, then

$$n^{\varphi(15)} \equiv 1 \pmod{15}$$

$\varphi(15) = |\{1, 2, 4, 7, 8, 11, 13, 14\}| = 8$

$$n^{33} - n \equiv (n^{8\cdot 4}) \cdot n - n$$
$$\equiv (1)^4 \cdot n - n \equiv n - n \equiv 0 \pmod{15}.$$

If $\gcd(n,15)=3$, then n is divisible by 3

$n^{33}-n \equiv 0 \pmod 3$

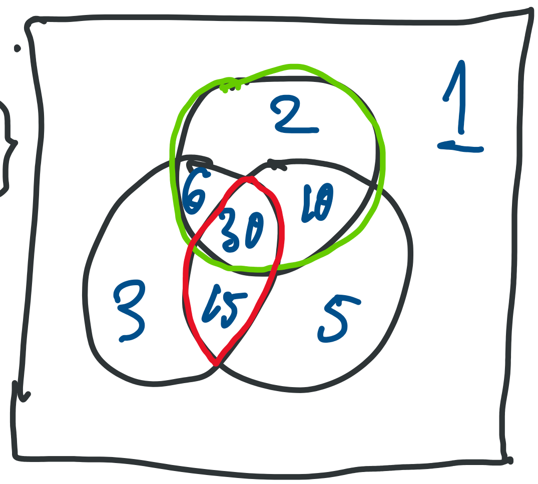
By FLT, $n^4 \equiv 1 \pmod 5$

$n^{33}-n = (n^4)^8 \cdot n - n \equiv n-n \equiv 0 \pmod 5$

Similarly for $\gcd(n,15)=5$ or 15. □

Find $\varphi(1200)$

$1200 = 2^4 \cdot 3 \cdot 5^2$



$\#\{1 \le a \le 1200, \gcd(a,1200)=1\}$

$= 1200$

$- \{1 \le a \le 1200 : a \text{ is a multiple of } 2\}$

$- \{\text{'' '' } 3\} - \{\text{'' } 5\} + \{\text{'' } 6\}$

$+ \{\text{'' } 10\} + \{\text{'' } 15\} - \{\text{'' } 30\}$

$$= 1200 - \frac{1200}{2} - \frac{1200}{3} - \frac{1200}{5} + \frac{1200}{2\times 3} + \frac{1200}{2\times 5} + \frac{1200}{3\times 5} - \frac{1200}{2\times 3\times 5}$$

$$= 1200\left(1 - \frac{1}{2} - \frac{1}{3} - \frac{1}{5} + \frac{1}{2\times 3} + \frac{1}{2\times 5} + \frac{1}{3\times 5} - \frac{1}{2\times 3\times 5}\right)$$

$$= 1200\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right)$$

$$= 1200 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{4}{5} = 320$$

If $n = p_1^{a_1} \cdots p_k^{a_k}$, then

$$\varphi(n) = n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_k}\right).$$