Fermat's Thm

If $gcd(a,p)=1$ and $p \in Prime$ $a^{p-1} \equiv 1 \pmod{p}$.

Euler ϕ function

$\phi(n) = \#$ ints in set $\{1, 2, \ldots, n\}$ relatively prime with n.

$$\phi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1) = p^k\left(1-\frac{1}{p}\right), \ p \in Prime$$

$$\phi(p_1^{k_1} p_2^{k_2} \cdots p_m^{k_m}) = \phi(p_1^{k_1})\phi(p_2^{k_2}) \cdots \phi(p_m^{k_m})$$

Euler's Thm

If $gcd(a,n)=1$, $a, n \in \mathbb{Z}^+$, $a^{\phi(n)} \equiv 1 \bmod n$

* A generalization of Fermat's Thm. Fermat's theorem __IS__ euler's thm when $n \in Prime$.

Reduced Residue System mod n a set of $\phi(n)$ values $a_1, a_2, \ldots a_{\phi(n)}$ s.t. for each value a_i, $gcd(a_i, n) = 1$ and for all $i \neq j$ $a_i \not\equiv a_j \pmod{n}$

$$n = 15, \ \phi(15) = \phi(3^1)\phi(5^1) = (3-1)(5-1) = 8$$

$$S = \{1, 2, 4, 7, 8, 11, 13, 14\}$$

If S is a reduced residue system mod n, and we create a new set S' by multiplying each item in S by a s.t. $gcd(a,n)=1$, S' will also be a reduced residue system mod n.

Pick $a=4$, $S' = \{4, 8, 16, 28, 32, 44, 52, 56\}$ 10/21/19 2

4 8, 1, 13, 2, 14, 7, 11

(1) no value in S' shares a common factor with n

(2) all values in S' are inequivalent mod n.

→ all terms of the form aa_i where $\gcd(a,n)=1$ and $\gcd(a_i,n)=1$.

Proof by Contradiction.

Assume the opposite that $aa_i \equiv aa_j \pmod{n}$ $i \neq j$. ($a_i \not\equiv a_j \bmod n$)

$$aa_i \equiv aa_j \pmod{n}$$

$$aa_i - aa_j \equiv 0 \pmod{n}$$

$$a(a_i - a_j) \equiv 0 \pmod{n}$$

$$\Longrightarrow n \mid a(a_i - a_j)$$

for all ints n, if $\gcd(n,a)=1$ and $n \mid ab$, then $n \mid b$.

Since $\gcd(n,a)=1$, it follows that $n \mid (a_i - a_j)$.

But this contradicts ~~so~~ our assumption that $a_i \not\equiv a_j \pmod{n}$.

Euler's Thm Pf

Let S be a reduced residue sys mod n. Create S' by multiplying each term in S by a where gcd(a,n) = 1. S' is also a reduced residue sys mod n. Thus, the product of all values in S is equivalent to the product of all values is S'.

Let $S = \{a_1, a_2, \ldots, a_{\phi(n)}\}$

So $S' = \{aa_1, aa_2, \ldots, aa_{\phi(n)}\}$

$$\prod_{i=1}^{\phi(n)} aa_i \equiv \prod_{i=1}^{\phi(n)} a_i \pmod n$$

$$\prod_{i=1}^{\phi(n)} aa_i - \prod_{i=1}^{\phi(n)} a_i \equiv 0 \pmod n$$

$$a^{\phi(n)} \prod_{i=1}^{\phi(n)} a_i - \prod_{i=1}^{\phi(n)} a_i \equiv 0 \pmod n$$

$$\left(\prod_{i=1}^{\phi(n)} a_i\right)\left(a^{\phi(n)} - 1\right) \equiv 0 \pmod n$$

$$\Rightarrow n \,\Big|\, \left(\left(\prod_{i=1}^{\phi(n)} a_i\right)\left(a^{\phi(n)} - 1\right)\right),$$

for all i, $\gcd(n, a_i) = 1$, $\gcd(n, \prod_{i=1}^{\phi(n)} a_i) = 1$.

Thus $n \mid (a^{\phi(n)} - 1) \to a^{\phi(n)} - 1 \equiv 0 \mod n \to \boxed{a^{\phi(n)} \equiv 1 \pmod n}$

10/19/21 (4)

How I can test Euler's Thm?

$n = 91$

What is the remainder when 30^{145} is divided by 91?

$\gcd(91,30) = 1$, $\phi(91) = \phi(7\cdot 13) = \phi(7)\phi(13)$
$= 6\cdot 12 = 72$

$30^{72} \equiv 1 \mod 91$ via Euler's.

$$30^{145} \equiv 30^{144}\cdot 30 \pmod{91}$$
$$\equiv (30^{72})^2 \cdot 30^1 \pmod{91}$$
$$\equiv 1^2 \cdot 30^1 \pmod{91}$$
$$\equiv \boxed{30 \pmod{91}}$$

$3^3 \equiv 12 \mod 15$

$3^4 \equiv 3^3\cdot 3 \equiv 12\cdot 3 \equiv 6 \mod 15$

$n = 15$

consider $2^i \mod 15$

ord(2 mod 15) is 4, min exp raise 2 to to get 1 mod 15 is 4

	0	1	2	3	4	5				ord(a mod n)	$\phi(n)$
2	1	2	4	8	1	2	4	8	...		
3	1	3	9	12	6	3	.....				
4	1	4	1	...							
7	1	7	4	13	1						
8	1	8	4	2	1						
11	1	11	1								
13	1	13	4	7	1						
14	1	14	1								
0	1	1									