7.3 Euler's Generalization of Fermat's Theorem

Note Title 10/24/2005

1. Use Euler's Theorem to establish the following:

(a) For any integer a, $a^{37} \equiv a \mod (1729)$

Pf: $1729 = 7 \cdot 13 \cdot 19$, $\phi(7) = 6$, $\phi(13) = 12$, $\phi(19) = 18$

$\therefore a^{18} \equiv 1 \pmod{19} \Rightarrow a^{36} \equiv 1 \pmod{19}$

$a^{12} \equiv 1 \pmod{13} \Rightarrow a^{36} \equiv 1 \pmod{13}$

$a^{6} \equiv 1 \pmod{7} \Rightarrow a^{36} \equiv 1 \pmod{7}$

$\therefore a^{36} \equiv 1 \pmod{7 \cdot 13 \cdot 19}$ [prob. #13, Sec. 4.2]

$\therefore a^{37} \equiv a \pmod{1729}$

(b) For any integer a, $a^{13} \equiv a \pmod{2730}$

Pf: $2730 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 13$ $\phi(2) = 1$, $\phi(3) = 2$, $\phi(5) = 4$, $\phi(7) = 6$, $\phi(13) = 12$

$\therefore a \equiv 1 \pmod{2} \Rightarrow a^{12} \equiv 1 \pmod{2}$

$a^{2} \equiv 1 \pmod{3} \Rightarrow a^{12} \equiv 1 \pmod{3}$

$a^{4} \equiv 1 \pmod{5} \Rightarrow a^{12} \equiv 1 \pmod{5}$

$a^6 \equiv 1 \pmod{7} \Rightarrow a^{12} \equiv 1 \pmod{7}$

$a^{12} \equiv 1 \pmod{13}$

$\therefore a^{12} \equiv 1 \pmod{2\cdot 3\cdot 5\cdot 7\cdot 13}$ [prob. #13, Sec. 4.2]

$\therefore a^{13} \equiv a \pmod{2730}$

(c) For any odd integer a, $a^{33} \equiv a \pmod{4080}$

Pf: $4080 = 15\cdot 16\cdot 17 = 15\cdot 2\cdot 4\cdot 2\cdot 17$

$\gcd(a, 2\cdot 15) = 1$ since a is odd

$\therefore a^{\phi(30)} \equiv 1 \pmod{30}$

$\phi(30) = 8 \Rightarrow a^8 \equiv 1 \pmod{30}$

$\Rightarrow a^{32} \equiv 1 \pmod{30}$

$\gcd(a, 2\cdot 17) = 1$ since a is odd

$\therefore a^{\phi(34)} \equiv 1 \pmod{34}$

$\phi(34) = (2-1)(17-1) = 16$

$\therefore a^{16} \equiv 1 \pmod{34} \Rightarrow a^{32} \equiv 1 \pmod{34}$

$\gcd(a, 16) = 1$ since a is odd

$\therefore a^{\phi(16)} \equiv 1 \pmod{16}$.

$\phi(16) = 8$, $\therefore a^8 \equiv 1 \pmod{16}$

$\therefore a^{32} \equiv 1 \pmod{16}$

$\operatorname{lcm}(30, 34, 16) = 4080$

$\therefore a^{32} \equiv 1 \pmod{4080}$ [prob. #13, Sec. 4.2]

$\therefore a^{33} \equiv a \pmod{4080}$

2. Use Euler's Theorem to confirm that, for any integer $n \geq 0$, $51 \mid 10^{32n+9} - 7$

Pf: $51 = 17 \cdot 3$. $\therefore \phi(51) = 16 \cdot 2 = 32$

$\gcd(10, 51) = 1$, $\therefore 10^{\phi(51)} = 10^{32} \equiv 1 \pmod{51}$

$\therefore 10^{32n} \equiv 1 \pmod{51}$ [1]

Is $10^9 \stackrel{?}{\equiv} 7 \pmod{51}$

$$10 \equiv 7 \pmod{3}$$
$$10 \equiv 1 \pmod{3} \Rightarrow 10^8 \equiv 1 \pmod{3}$$
$$\therefore 10^9 = 10^8 \cdot 10 \equiv 7 \cdot 1 \pmod{3}, \text{ or}$$
$$10^9 \equiv 7 \pmod{3} \quad [2]$$

$$-10 \equiv 7 \pmod{17}$$
$$\therefore (-10)^2 \equiv 7^2 = 49 \equiv -2 \pmod{17}$$
$$\therefore (-10)^8 = 10^8 \equiv (-2)^4 = 16 \equiv -1 \pmod{17}$$
$$\therefore 10^9 \equiv -10 \equiv 7 \pmod{17} \quad [3]$$

$$[2] \,\&\, [3] \Rightarrow 10^9 \equiv 7 \pmod{51} \quad [4]$$

$$[1] \,\&\, [4] \Rightarrow 10^{32n} \cdot 10^9 \equiv 1 \cdot 7 \pmod{51}, \text{ or}$$

$$10^{32n+9} \equiv 7 \pmod{51}$$

$$\therefore 51 \mid 10^{32n+9} - 7$$

3. Prove $2^{15} - 2^3$ divides $a^{15} - a^3$ for any integer a.

Pf: $a^{15} - a^3 = a^3(a^{12} - 1) = a^3(a^6+1)(a^6-1)$
$$= a^3(a^6+1)(a^3+1)(a^3-1)$$
$$= a^3(a^6+1)(a^3+1)(a^2+a+1)(a-1)$$

$$2^{15} - 2^3 = 2^3(2^{12}-1) = 2^3(2^6+1)(2^6-1)$$

$= 2^3(2^6+1)(2^3+1)(2^3-1)$
$= 2^3(2^6+1)(2^3+1)(2^2+2+1)(2-1)$
$= 8(65)(9)(7)$
$= 8\cdot 5\cdot 13\cdot 9\cdot 7 = 2^3\cdot 3^2\cdot 5\cdot 7\cdot 13$

Could go through each factor and show it divides $a^3(a^6+1)(a^3+1)(a^2+a+1)(a-1)$.

However, easier to use Euler's Theorem.

$\phi(8)=4, \ \phi(5)=4, \ \phi(13)=12, \ \phi(9)=6, \ \phi(7)=6$

(a) $\therefore$ If $\gcd(a, 2^{15}-2^3)=1$, then

$\gcd(a,8)=1 \quad \gcd(a,13)=1 \quad \gcd(a,7)=1$
$\gcd(a,5)=1 \quad \gcd(a,9)=1$

$\therefore a^4 \equiv 1 \pmod 8 \quad a^{12}\equiv 1 \pmod{13} \quad a^6 \equiv 1 \pmod 7$
$a^4 \equiv 1 \pmod 5 \quad a^6 \equiv 1 \pmod 9$

Make all $a^{12}\equiv 1$ so that

$a^{12} \equiv 1 \pmod{8\cdot 5\cdot 13\cdot 9\cdot 7}$

$\therefore a^{15} \equiv a^3 \pmod{2^{15}-2^3}$

(b) If $\gcd(a, 2^{15}-2^3) \neq 1$, then

$a = K(2^{15}-2^3)$, some K, and

$\therefore a^{15}-a^3 = (a^{14}-a^2)a = (a^{14}-a^2)K(2^{15}-2^3)$

$\therefore a^{15} \equiv a^3 \pmod{2^{15}-2^3}$

$\therefore$ (a) + (b) $\Rightarrow$ for all a, $a^{15} \equiv a^3 \pmod{2^{15}-2^3}$

4. Show that if $\gcd(a,n) = \gcd(a-1, n) = 1$, then

$1 + a + a^2 + \dots + a^{\phi(n)-1} \equiv 0 \pmod n$

Pf: By Euler, $\gcd(a,n) = 1 \Rightarrow a^{\phi(n)} \equiv 1 \pmod n$

$\therefore a^{\phi(n)} - 1 \equiv 0 \pmod n$

But $a^{\phi(n)} - 1 = (a-1)(a^{\phi(n)-1} + \dots + a^2 + a + 1)$

$\therefore (a-1)(a^{\phi(n)-1} + \dots + a^2 + a + 1) \equiv 0 \pmod n$

Since $\gcd(a-1, n) = 1$, can cancel $(a-1)$,

$\therefore (a^{\phi(n)-1} + \dots + a^2 + a + 1) \equiv 0 \pmod n$

5. If m and n are relatively prime positive integers, prove $m^{\phi(n)} + n^{\phi(m)} \equiv 1 \pmod{mn}$

Pf: Since $\gcd(m,n)=1$, Then

$$m^{\phi(n)} \equiv 1 \pmod{n} \quad \text{and} \quad n^{\phi(m)} \equiv 1 \pmod{m}$$

But $n^{\phi(m)} \equiv 0 \pmod{n}$ and $m^{\phi(n)} \equiv 0 \pmod{m}$

$$\therefore m^{\phi(n)} + n^{\phi(m)} \equiv 1 + 0 = 1 \pmod{n}$$

$$n^{\phi(m)} + m^{\phi(n)} \equiv 1 + 0 = 1 \pmod{m}$$

By prob. #13, Sec. 4-2, $m^{\phi(n)} + n^{\phi(m)} \equiv 1 \pmod{mn}$

6. Fill in any missing details in The following proof to Euler's Theorem

Let p be a prime divisor of n and $\gcd(a,p)=1$

Note: if n is prime, choose $p=n$, and There are $p-1$ choices for a.

By Fermat's Theorem, $a^{p-1} \equiv 1 \pmod{p}$, so that

$a^{p-1} = 1 + tp$ for some t Def. $a \equiv b \pmod p$

$\therefore a^{p(p-1)} = (1+tp)^p = 1 + \binom{p}{1}(tp) + \dots + (tp)^p \equiv 1 \pmod{p^2}$

Expansion by Binomial Th. Also, $p \mid \binom{p}{1} = \frac{p!}{(p-1)!} = p$

So each term in $\binom{p}{1}(tp) + \dots + (tp)^p$ contains p^2

By induction $a^{p^{k-1}(p-1)} \equiv 1 \pmod{p^k}$, $k = 1, 2, \dots$

For $k=1$: $a^{p^{1-1}(p-1)} = a^{p-1} \equiv 1 \pmod p$, by Fermat

For $k \Rightarrow k+1$: Assume $a^{p^{k-1}(p-1)} \equiv 1 \pmod{p^k}$

$\therefore a^{p^{k-1}(p-1)} = 1 + qp^k$, some q.

Note $p^{(k+1)-1}(p-1) = p^k(p-1) = p[p^{k-1}(p-1)]$

$\therefore a^{p^{(k+1)-1}(p-1)} = \left(a^{p^{k-1}(p-1)}\right)^p = (1+qp^k)^p$

$= 1 + \binom{p}{1}(qp^k) + \dots + (qp^k)^p$

Since $p \mid \binom{p}{1}$, then $p^{k+1} \mid \binom{p}{1}(qp^k) + \dots + (qp^k)^p$

$\therefore a^{p^{(k+1)-1}(p-1)} = 1 + q'p^{k+1}$ completing induction

Raise both sides of this congruence to the $\phi(n)/p^{k-1}(p-1)$ power to get $a^{\phi(n)} \equiv 1 \pmod{p^k}$

Since p is a prime divisor of n, let k be the power of p in the prime factorization of n. $\therefore$ By Th. 7.3, $\phi(n)$ contains as a factor $p^k - p^{k-1} = p^{k-1}(p-1)$, and so $p^{k-1}(p-1)$ divides $\phi(n)$

Thus, $a^{\phi(n)} \equiv 1 \pmod{n}$

If $n = p_1^{k_1} \cdots p_r^{k_r}$, then by above, $a^{\phi(n)} \equiv 1 \pmod{p_i^{k_i}}$

Since $\gcd(p_i, p_j) = 1$ for $i \neq j$, $1 \leq i, j \leq r$,

Then by prob. #13, Sec. 4.2, $a^{\phi(n)} \equiv 1 \pmod{p_1^{k_1} \cdots p_r^{k_r}}$

or, $a^{\phi(n)} \equiv 1 \pmod{n}$

Note: These are the exact same steps shown on p. 137. Prob. #6 was probably in earlier edition whereas proof on p. 137 was not, and #6 was accidently left in.

7. Find the units digit of 3^{100} by Euler's Theorem.

$\gcd(10,3)=1$. By Euler's Th., $3^{\phi(10)} \equiv 1 \pmod{10}$
$\phi(10) = 4$. $\therefore 3^4 \equiv 1 \pmod{10}$. $\therefore (3^4)^{25} \equiv 1 \pmod{10}$
$\therefore 3^{100} \equiv 1 \pmod{10}$. $\therefore$ Units digit of 3^{100} is 1.

8. (a). If $\gcd(a,n)=1$, show the linear congruence $ax \equiv b \pmod{n}$ has the solution $x \equiv b\,a^{\phi(n)-1} \pmod{n}$.

Pf: If $x \equiv b\,a^{\phi(n)-1} \pmod{n}$, then

$$ax = a\left(b\,a^{\phi(n)-1}\right) = b\,a^{\phi(n)}.$$

But $a^{\phi(n)} \equiv 1 \pmod{n}$ by Euler's Th. since $\gcd(a,n)=1$.

$$\therefore ax = b\,a^{\phi(n)} \equiv b \cdot 1 = b \pmod{n}$$

(b) Use (a) to solve the linear congruences
$3x \equiv 5 \pmod{26}$, $13x \equiv 2 \pmod{40}$, $10x \equiv 21 \pmod{49}$

$3x \equiv 5 \pmod{26}$ $\quad$ $\gcd(3,26)=1$, $\phi(26)=12$

$$\therefore x \equiv 5 \cdot 3^{\phi(26)-1} \pmod{26}, \text{ or}$$

$x \equiv 5 \cdot 3^{11} \pmod{26}$

To simplify, $3^4 = 81 = 3 \cdot 26 \equiv 3 \pmod{26}$

$\therefore 3^8 \equiv 9 \pmod{26}$

$3^3 = 27 \equiv 1 \pmod{26}$

$\therefore 3^{11} \equiv 9 \pmod{26}$

$\therefore \underline{x} = 5 \cdot 3^{11} \equiv 45 \equiv 19 \pmod{26}$

$13x \equiv 2 \pmod{40}$ $\quad \gcd(13, 40) = 1$

$\phi(40) = (2^3 - 2^2)(5-1) = 16$

$\therefore x \equiv 2 \cdot 13^{15} \pmod{40}$

To simplify, $13^2 = 169 \equiv 9 \pmod{40}$

$\therefore 13^4 \equiv 81 \equiv 1 \pmod{40}$

$\therefore 13^{12} \equiv 1 \pmod{40}$, $13^{14} \equiv 9 \pmod{40}$

$9 \cdot 13 = 117 \equiv -3 \pmod{40}$

$\therefore 13^{15} \equiv -3 \pmod{40}$

$\therefore \underline{x} \equiv 2 \cdot 13^{15} \equiv -6 \equiv 34 \pmod{40}$

$10x \equiv 21 \pmod{49}$ $\quad \gcd(10, 49) = 1$

$\phi(49) = 7^2 - 7 = 42$

$\therefore x \equiv 21 \cdot 10^{41} \pmod{49}$

To simplify, $10^2 \equiv 2 \pmod{49}$

$2^{10} = 1024 \equiv 44 \equiv -5 \pmod{49}$

$\therefore 10^{20} \equiv 2^{10} \equiv -5 \pmod{49}$

$\therefore 10^{40} \equiv 25 \pmod{49}$, $10^{41} \equiv 250 \equiv 5 \pmod{49}$
$\therefore x \equiv 21 \cdot 5 = 105 = 98 + 7 \equiv 7 \pmod{49}$
$\therefore x \equiv 7 \pmod{49}$

9. Use Euler's Th. to evaluate $2^{100000} \pmod{77}$

$\gcd(2, 77) = 1$. $\therefore 2^{\phi(77)} \equiv 1 \pmod{77}$
$\phi(77) = 6 \cdot 10 = 60$. $\therefore 2^{60} \equiv 1 \pmod{77}$

$\therefore 2^{60000} \equiv 1 \pmod{77}$, $(2^{60})^{300} = 2^{18000} \equiv 1 \pmod{77}$
$\therefore 2^{36000} \equiv 1 \pmod{77}$
$\therefore 2^{96000} \equiv 1 \pmod{77}$, $2^{1800} \equiv 1 \pmod{77}$
$2^{3600} \equiv 1 \pmod{77}$
$\therefore 2^{99600} \equiv 1 \pmod{77}$, $2^{180} \equiv 1 \pmod{77}$
$\therefore 2^{360} \equiv 1 \pmod{77}$
$\therefore 2^{99960} \equiv 1 \pmod{77}$

But $2^{10} = 1024$, $13 \cdot 77 = 1001$, $\therefore 2^{10} \equiv 23 \pmod{77}$
$\therefore 2^{40} \equiv 23^4 \pmod{77}$

$\therefore 2^{100000} \equiv 23^4 \pmod{77}$

$23^2 = 529 = 6 \cdot 77 + 67$. $\therefore 23^2 \equiv -10 \pmod{77}$
$\therefore 23^4 \equiv 100 \equiv 23 \pmod{77}$

$\therefore 2^{100000} \equiv 23 \pmod{77}$

10. For any integer a, show that a and a^{4n+1} have the same last digit.

Pf: Need to show $a \equiv a^{4n+1} \pmod{10}$ for all a.
Assume $n > 0$.

(1) If $\gcd(a, 10) = 1$, then $a^{\phi(10)} \equiv 1 \pmod{10}$
But $\phi(10) = 4$. $\therefore a^4 \equiv 1 \pmod{10}$,
$\therefore a^{4n} \equiv 1 \pmod{10}$, $a^{4n+1} \equiv a \pmod{10}$

(2) Suppose $\gcd(a, 10) = 10$, then $a = 10x$,
and $\therefore a \equiv 0 \pmod{10}$, $a^{4n+1} = (10x)^{4n+1}$
$= 10^{4n+1} x^{4n+1}$. $\therefore a^{4n+1} \equiv 0 \pmod{10}$, so
$a \equiv a^{4n+1} \pmod{10}$

(3) Suppose $\gcd(a, 10) = 5$

Lemma: For $n \geq 1$, $5^n \equiv 5 \pmod{10}$
By induction, clearly true for $n = 1$.
Suppose $5^k \equiv 5 \pmod{10}$
$\therefore 5^{k+1} \equiv 25 = 20 + 5 \equiv 5 \pmod{10}$.
$\therefore k \Rightarrow k+1$ true, $\therefore$ true for all n.

Let $a = 5^x p_1^{k_1} \cdots p_r^{k_r}$, $p_i \neq 2$, $x \geq 1$

$$\therefore p_1^{k_1} \cdots p_r^{k_r} = 2s+1, \text{ some } s \geq 1$$

$$\therefore a = 5^x(2s+1) = 5^x \cdot 2s + 5^x$$
$$= 10(5^{x-1} \cdot s) + 5^x$$

$$\therefore a \equiv 5^x \pmod{10} = 5 \pmod{10}$$

$$a^{4n+1} = (5^x)^{4n+1} (p_1^{k_1} \cdots p_r^{k_r})^{4n+1}$$

$$= 5^{4xn+x} \cdot p_1^{k_1'} \cdots p_r^{k_r'}$$

But $p_1^{k_1'} \cdots p_r^{k_r'} = 2r+1$, some $r \geq 1$

$$\therefore a^{4n+1} = 5^{4xn+x} \cdot (2r+1)$$

$$= 5^x \cdot 10 \cdot 5^{4xn-1} + 5^{4xn+x}$$

$$\therefore a^{4n+1} \equiv 5^{4xn+x} \equiv 5 \pmod{10}$$

$$\therefore a \equiv 5 \equiv a^{4n+1} \pmod{10}$$

(4) Suppose $\gcd(a, 10) = 2$

Let $a = 2^x p_1^{k_1} \cdots p_r^{k_r}$, $p_i \neq 5$, $x \geq 1$

Let $p_1^{k_1} \cdots p_r^{k_1} = 5q + r$, $0 < r < 5$

$\therefore a = 2^x(5q+r) = 2^{x-1} \cdot 10 \cdot q + 2^x \cdot r$

$\therefore a \equiv 2^x \cdot r \pmod{10}, \quad r = 1, 2, 3, 4$

Lemma: $2^{4n+1} \equiv 2 \pmod{10}, \ n \geq 0$

Pf: Clearly true for $n = 0$

For $n = 1$, $2^5 = 32 \equiv 2 \pmod{10}$

Assume true for k.

$\therefore 2^{4k+1} \equiv 2 \pmod{10}, \ k \geq 0$

$\therefore 2^{4(k+1)+1} = 2^{4k} \cdot 2^5$

But $2^5 = 32 \equiv 2 \pmod{10}$

$\therefore 2^{4k} \cdot 2^5 \equiv 2^{4k} \cdot 2 \pmod{10}$

But $2^{4k} \cdot 2 = 2^{4k+1} \equiv 2 \pmod{10}$

$\therefore 2^{4(k+1)+1} \equiv 2 \pmod{10}$.

$\therefore k \Rightarrow k+1$, $\therefore$ true for all n.

$r = 1$: $a \equiv 2^x \pmod{10}$

$\therefore a^{4n+1} \equiv (2^x)^{4n+1} \pmod{10}$

But $(2^x)^{4n+1} = \left(2^{4n+1}\right)^x \equiv 2^x \pmod{10}$

by Lemma above.

$\therefore a^{4n+1} \equiv 2^x \equiv a \pmod{10}$

$r=2$: $a \equiv 2^x \cdot 2 \pmod{10}$

This is is same as case $r=1$.

$r=3$: $a \equiv 2^x \cdot 3 \pmod{10}$

$\therefore a^{4n+1} \equiv (2^x \cdot 3)^{4n+1} \pmod{10}$

$= (2^{4n+1})^x \cdot 3^{4n+1}$

$= 2^x \cdot 3^{4n+1} \pmod{10}$

by Lemma above.

Lemma: $3^{4n+1} \equiv 3 \pmod{10}$, $n \geq 0$

Pf: Clearly true for $n=0$

Assume true for $K \geq 1$

$\therefore 3^{4(K+1)+1} = 3^{4K+5} = 3^{4K+1} \cdot 3^4$

$3^4 = 81 = 80 + 1$

$\therefore 3^{4K+1} \cdot 3^4 = (3^{4K+1}) \cdot 80 + 3^{4K+1} \pmod{10}$

$\equiv 3^{4K+1} \pmod{10}$

$\equiv 3 \pmod{10}$

$\therefore 3^{4n+1} \equiv 3 \pmod{10}$ for all n

$\therefore a^{4n+1} = 2^x \cdot 3^{4n+1} \equiv 2^x \cdot 3 \pmod{10}$

$\therefore\ a^{4n+1} \equiv 2^x \cdot 3 \equiv a \pmod{10}$

$r=4$: $a \equiv 2^x \cdot 4 \pmod{10}$

$2^x \cdot 4 = 2^{x+2}$, $\therefore\ a \equiv 2^{x+2} \pmod{10}$,
which is the same as the case $r=1$.

$\therefore$ If $a = 2^x p_1^{k_1} \cdots p_r^{k_r}$, $p_i \neq 5$, $x \geq 1$

Then $a \equiv a^{4n+1} \pmod{10}$

$=$

(1), (2), (3), and (4) $\Rightarrow a \equiv a^{4n+1} \pmod{10}$ for all a.

11. For any prime p, establish each of the assertions below:

(a) $\tau(p!) = 2\tau((p-1)!)$

Pf: Let $p! = p_1^{k_1} \cdots p_r^{k_r} \cdot p = 1 \cdot 2 \cdot \cdots (p-1) \cdot p$

$\therefore\ (p-1)! = p_1^{k_1} \cdots p_r^{k_r}$

Since $\gcd(p, p_1^{k_1} \cdots p_r^{k_r}) = 1$,

$\tau(p!) = \tau(p \cdot p_1^{k_1} \cdots p_r^{k_r}) = \tau(p) \cdot \tau(p_1^{k_1} \cdots p_r^{k_r})$

$= \tau(p) \cdot \tau((p-1)!)$

$$= 2 \cdot \tau((p-1)!), \text{ since } \tau(p) = 2$$

(b) $\sigma(p!) = (p+1)\,\sigma((p-1)!)$

As in (a), $p! = p_1^{k_1} \cdots p_r^{k_r} \cdot p = (p-1)! \cdot p$

$$\therefore \sigma(p!) = \sigma((p-1)!) \cdot \sigma(p)$$

$$= \sigma((p-1)!) \cdot (p+1), \text{ as } \sigma(p) = p+1$$

(c) $\phi(p!) = (p-1)\,\phi((p-1)!)$

As in (a), $p! = p_1^{k_1} \cdots p_r^{k_r} \cdot p = (p-1)! \cdot p$

$$\therefore \phi(p!) = \phi((p-1)!) \cdot \phi(p)$$

$$= \phi((p-1)!) \cdot (p-1), \text{ as } \phi(p) = p-1$$

12. Given $n \geq 1$, a set of $\phi(n)$ integers relatively prime to n is called a reduced set of residues modulo n (i.e., a subset of a complete set of residues modulo n, whose members are relatively prime to n).

Verify the following:

(a) The integers $-31, -16, -8, 13, 25, 80$ form a reduced set of residues modulo 9.

The complete set of residues mod 9 =
$\{0, 1, 2, 3, 4, 5, 6, 7, 8\}$

The relatively prime members are $\{1, 2, 4, 5, 7, 8\}$, and all members are incongruent mod 9 since they are a subset of the complete set.

$\therefore$ Suffices to show each integer in question is congruent to one and only one of $\{1, 2, 4, 5, 7, 8\}$.

The Division Algorithm will do this.

$$-31 = -4 \cdot 9 + 5 \qquad 13 = 1 \cdot 9 + 4$$
$$-16 = -2 \cdot 9 + 2 \qquad 25 = 2 \cdot 9 + 7$$
$$-8 = -1 \cdot 9 + 1 \qquad 80 = 8 \cdot 9 + 8$$

$\therefore \{-31, -16, -8, 13, 25, 80\}$ forms a reduced set.

(b) $3, 3^2, 3^3, 3^4, 3^5, 3^6$ form a reduced set of residues mod 14

As in (a), the reduced set of residues mod 14 is: $\{1, 3, 5, 9, 11, 13\}$

$3 \equiv 3 \pmod{14}$

$3^2 \equiv 9 \pmod{14}$

$3^3 = 27 \equiv 13 \pmod{14}$

$3^4 = 81 = 5 \cdot 14 + 11 \equiv 11 \pmod{14}$

$3^5 = 3^4 \cdot 3 \equiv 11 \cdot 3 = 33 \equiv 5 \pmod{14}$

$3^6 = 3^4 \cdot 3^2 \equiv 11 \cdot 9 = 99 = 7 \cdot 14 + 1 \equiv 1 \pmod{14}$

$\therefore \{3, 3^2, 3^3, 3^4, 3^5, 3^6\}$ is congruent mod 14 to one and only one of $\{1, 3, 5, 9, 11, 13\}$ and is $\therefore$ a reduced set of residues mod 14.

(c) The integers $2, 2^2, 2^3, \ldots, 2^{18}$ form a reduced set of residues mod 27.

$27 = 3^3$, $\therefore \phi(n) = 3^3 - 3^2 = 18.$

Clearly, $\gcd(2^n, 3^3) = 1$, for $n \geq 1$.

Since $\phi(27) = 18$, and there are 18 numbers: $2^1, 2^2, \dots, 2^{18}$, only have to show the numbers are incongruent to each other mod 27.

Since $\gcd(2, 3^3) = 1$, By Euler's Th.,

$2^{\phi(27)} \equiv 1 \pmod{27}$, or $2^{18} \equiv 1 \pmod{27}$

Also, $2 \not\equiv 1 \pmod{27}$.

$\therefore 2^{17} \not\equiv 1 \pmod{27}$, for if $2^{17} \equiv 1 \pmod{27}$, then $2^{18} = 2^{17} \cdot 2 \equiv 1 \cdot 2 = 2 \pmod{27}$, and so $1 \equiv 2 \pmod{27}$, clearly false.

This can be done for $2^{16}, 2^{15}, \dots, 2^1$
That is, $2^x \not\equiv 1 \pmod{27}$ for $x = 1, 2, \dots, 17$

$\therefore 2^n \not\equiv 2^m \pmod{27}$, $n \neq m$, $0 < n, m \leq 18$

For if $2^n \equiv 2^m \pmod{27}$, $n \neq m$, $0 < n, m \leq 18$, then (assuming for ease $n > m$) $2^{n-m} \equiv 1 \pmod{27}$, contradicting

The above: $2^x \not\equiv 1 \pmod{27}$, $0<x<18$

$\therefore \{2^1, \dots, 2^{18}\}$ are incongruent mod 27,

There are $\phi(27) = 18$ such members,

and $\therefore$ They form a reduced set of residues mod 27.

13. If p is an odd prime, show that the integers

$$-\frac{p-1}{2}, \dots, -2, -1, 1, 2, \dots \frac{p-1}{2}$$

form a reduced set of residues mod p.

Pf: $\phi(p) = p-1$, and There are $p-1$ elements in The above set, and They are all integers since $p \geq 3$ so That $p-1$ is even.

As all of $1, 2, \dots, \frac{p-1}{2} < p$, Then They are all incongruent to each other, mod p

Similarly, $-\frac{p-1}{2}, \dots, -2, -1$ are all incongruent mod p. For if $a, b \in \{-\frac{p-1}{2}, \ldots, -2, -1\}$

and $a \equiv b \pmod p$, then $-a \equiv -b \pmod p$, contradicting the incongruity of $\{1, 2, \ldots, \frac{p-1}{2}\}$!

$\therefore$ Need only need to show if $a \in \{1, 2, \ldots, \frac{p-1}{2}\}$

and $b \in \{-\frac{p-1}{2}, \ldots, -2, -1\}$, then $a \not\equiv b \pmod p$

Suppose $a \equiv b \pmod p$. Then $a \equiv b + p \pmod p$

But $b + p$ is of the form:

$$p - \frac{p-1}{2}, \ldots, p-2, p-1, \quad \text{or}$$

$$\frac{2p-p+1}{2}, \ldots, p-2, p-1, \quad \text{or}$$

$$\frac{p+1}{2}, \ldots p-2, p-1$$

$\therefore b + p > a$, and $b + p < p$

$\therefore b + p \not\equiv a \pmod p$, a contradiction.

$\therefore$ All $p-1$ elements of $\{-\frac{p-1}{2}, \ldots, -2, -1, 1, 2, \ldots, \frac{p-1}{2}\}$ are incongruent mod p to each other and so form a reduced set of residues.