8.1 The Order of an Integer Modulo n

Note Title 1/18/2006

1. Find the order of the integers 2, 3, and 5:

(a) modulo 17

$\phi(17) = 16$, $\therefore$ divisors are 1, 2, 4, 8, 16

$2^2 \equiv 4$, $2^4 \equiv 16$, $2^8 \equiv 1 \pmod{17}$,
$3^2 \equiv 9$, $3^4 \equiv 13$, $3^8 \equiv 16$, $3^{16} \equiv 1 \pmod{17}$
$5^2 \equiv 8$, $5^4 \equiv 13$, $5^8 \equiv 16$, $5^{16} \equiv 1 \pmod{17}$

$\therefore$ ord(2) = 8 mod 17
ord(3) = 16 mod 17
ord(5) = 16 mod 17

(b) modulo 19

$\phi(19) = 18$, $\therefore$ divisors are 1, 2, 3, 6, 9, 18

$2^2 \equiv 4$, $2^3 \equiv 8$, $2^6 \equiv 7$, $2^9 \equiv 18$, $2^{18} \equiv 1$. $\therefore$ Ord(2) = 18
$3^2 \equiv 9$, $3^3 \equiv 8$, $3^6 \equiv 7$, $3^9 \equiv 18$, $3^{18} \equiv 1$, $\therefore$ Ord(3) = 18
$5^2 \equiv 6$, $5^3 \equiv 11$, $5^6 \equiv 7$, $5^9 \equiv 1$, $\therefore$ Ord(5) = 9

(c) modulo 23

$\phi(23) = 22$, $\therefore$ divisors are 1, 2, 11, 22

$2^2 \equiv 4$, $2^{11} \equiv 1$, $\therefore \text{Ord}(2) = 11$
$3^2 \equiv 9$, $3^{11} \equiv 1$, $\therefore \text{Ord}(3) = 11$
$5^2 \equiv 2$, $5^{11} \equiv 22$, $5^{22} \equiv 1$, $\therefore \text{Ord}(5) = 22$

2. Establish each of the statements below:
(a) If a has order hk modulo n, then a^h has order k modulo n.

Pf: $a^{hk} \equiv 1 \pmod{n} \Rightarrow (a^h)^k \equiv 1 \pmod{n}$
Suppose $(a^h)^r \equiv 1 \pmod{n}$, $0 < r < k$
$\therefore 0 < hr < hk$. Then a would not have order hk since $hr < hk$ and $a^{hr} \equiv 1$.

(b) If a has order $2k$ modulo the odd prime p, then $a^k \equiv -1 \pmod{p}$.

Pf: $a^{2k} \equiv 1 \pmod{p}$. If $p = 2$, a odd, then a has order $\phi(2) = 1 \neq 2k$. $\therefore$ Assume p odd.

$$\therefore (a^k)^2 - 1 \equiv 0 \pmod{p}$$

$$\therefore (a^k - 1)(a^k + 1) \equiv 0 \pmod{p}$$

$$\therefore p \mid (a^k - 1)(a^k + 1)$$

If $p \mid (a^k - 1)$, then $a^k \equiv 1 \pmod{p}$, so a would not have order $2k$.

$\therefore p \nmid a^k - 1$, so $p \mid (a^k+1)$ (by Th. 3.1)

$\therefore a^k + 1 \equiv 0 \pmod{p} \Rightarrow a^k \equiv -1 \pmod{p}$.

(c) If a has order $n-1$ modulo n, then n is prime.

Pf: $a^{n-1} \equiv 1 \pmod{n}$ and $a^{\phi(n)} \equiv 1 \pmod{n}$
If $\phi(n) < n-1$, then it would contradict $n-1$ as the order of a.
$\therefore \phi(n) = n-1$.
If n were composite, it would have a divisor d, $1 < d < n$. n is also a divisor of n, so $\phi(n) \le n-2$. But $\phi(n) = n-1$, so n is not composite,
$\therefore n$ is prime.

3. Prove $\phi(2^n - 1)$ is a multiple of n, all $n > 1$.

Pf: Since $(2^n - 1) \equiv 0 \pmod{2^n - 1}$, then $2^n \equiv 1 \pmod{2^n-1}$

Let k be order of 2 mod $2^n - 1$.
$\therefore 2^k \equiv 1 \pmod{2^n - 1}$, or $2^k - 1 = a(2^n - 1)$, $a > 0$
But $2^k > 1$ for $k \ge 1$, and $2^k - 1 < 2^n - 1$ for

$k < n$. $\therefore$ $2^k - 1 = a(2^n - 1)$ only if $k = n$, $a = 1$.

$\therefore$ Order of 2 mod $2^n - 1$ is n.

Note that $\gcd(2, 2^n - 1) = 1$, since $2^n - 1$ is odd. $\therefore$ By Euler's Th.,
$2^{\phi(2^n - 1)} \equiv 1 \pmod{2^n - 1}$.
$\therefore$ By Th. 8.1, $n \mid \phi(2^n - 1)$

4. Assume order of a mod n is h, and
order of b mod n is k.
Show the order of ab mod n divides hk.
In particular, if $\gcd(h, k) = 1$, then ab has order hk.

Pf: (1) We know $a^h \equiv 1 \pmod n$
$b^k \equiv 1 \pmod n$

$\therefore$ $a^{hk} \equiv 1^k \equiv 1 \pmod n$
$b^{kh} \equiv 1^h \equiv 1 \pmod n$

$\therefore$ $(ab)^{hk} = a^{hk} b^{hk} \equiv 1 \pmod n$

$\therefore$ By Th. 8.1, order of ab divides hk.

(2) Suppose $\gcd(h, k) = 1$

Let $h = p_1^{h_1} p_2^{h_2} \cdots p_r^{h_r}$, $k = q_1^{k_1} \cdots q_s^{k_s}$, where

$q_i \neq p_i$ since $\gcd(h, k) = 1$.

Let w = order of ab. From (1), $w \mid hk$, so
$w = p_1^{l_1} p_2^{l_2} \cdots p_r^{l_r} q_1^{m_1} q_2^{m_2} \cdots q_s^{m_s}$,

where $0 \le l_i \le h_i$, $0 \le m_i \le k_i$

Let $w = h_x k_y$, where $h_x = p_1^{l_1} \cdots p_r^{l_r}$

$k_y = q_1^{m_1} \cdots q_s^{m_s}$

$\therefore h_x \mid h$, $k_y \mid k$

$\therefore$ let $h = h' h_x$, $k = k' k_y$

$\therefore (ab)^{h_x k_y} = a^{h_x k_y} b^{h_x k_y} \equiv 1 \pmod n$

$\therefore \left(a^{h_x k_y} b^{h_x k_y}\right)^{h'} \equiv 1 \pmod n$ [1]

but $\left(a^{h_x k_y} b^{h_x k_y}\right)^{h'} = a^{h' h_x k_y} b^{h' h_x k_y}$

$= (a^h)^{k_y} (b^h)^{k_y} \equiv (b^h)^{k_y} \pmod n$ [2]

since $a^h \equiv 1 \pmod n$

$\therefore$ [1] and [2] imply $(b^h)^{k_y} \equiv 1 \pmod{n}$

Since order of b is k, then by Th. 8.1,

$k \mid h k_y$. Since $\gcd(h,k)=1$, then $k \mid k_y$

$\therefore k_y \mid k$ and $k \mid k_y \Rightarrow k_y = k$.

Similarly, $h_x = h$.

$\therefore w = hk$, so $\gcd(h,k)=1 \Rightarrow$ order $ab = hk$

5. Given that a has order 3 mod p, where p is an odd prime, show $a+1$ must have order 6 mod p.

Pf: $a^3 \equiv 1 \pmod{p}$

$\therefore p \mid (a^3-1) \Rightarrow p \mid (a-1)(a^2+a+1)$

If $p \mid (a-1)$, then $a \equiv 1 \pmod{p}$, which contradicts order $a = 3$. $\therefore p \nmid (a-1)$

$\therefore p \mid (a^2+a+1) \Rightarrow a^2+a+1 \equiv 0 \pmod{p}$ [1]

$\therefore a^2+2a+1 \equiv a \pmod{p}$, or

$(a+1)^2 \equiv a \pmod{p}$. ($\therefore$ order $a+1 \neq 2$)

$(a+1)^3 \equiv a(a+1) = a^2 + a \equiv -1$ from [1]

$\therefore$ order $a+1 \neq 3$

$(a+1)^4 = [(a+1)^2]^2 \equiv a^2$ $\therefore$ order $a+1 \neq 4$

$(a+1)^5 = (a+1)^3(a+1)^2 \equiv a(-1) = -a$.

$\therefore$ order $a+1 \neq 5$

$(a+1)^6 = [(a+1)^3]^2 \equiv (-1)^2 = 1 \pmod{p}$.

Also, $a+1 \not\equiv 1$. If true, then $a \equiv 0 \Rightarrow a^3 \equiv 0$ contradicting order of a is 3.

Also, $a \not\equiv 1$, since if true, a would have order 1.

$\therefore$ Order $(a+1)$ mod p is 6.

6. Verify the following assertions:

(a) The odd prime divisors of the integer n^2+1 are of the form $4k+1$.

Pf: When n is even, n^2+1 is odd. The prime factorization of n^2+1 will thus contain odd primes.

$\therefore$ consider p as any odd prime divisor of n^2+1.

Assume $\gcd(n,p)=1$, for if $n=kp$, $n^2=k^2p^2$, so $p \mid n^2$. This with $p \mid n^2+1 \Rightarrow p \mid 1$.

$\therefore p \mid n^2+1$, so $n^2+1 \equiv 0 \pmod{p}$, or

$n^2 \equiv -1 \pmod{p}$, $\therefore n^4 \equiv 1 \pmod{p}$

Let r be order of n mod p. $\therefore$ By Th. 8.1, $r \mid 4$, $\therefore r = 1, 2,$ or 4.

If order n was 1, then $n \equiv 1 \pmod{p}$, so $n^2 \equiv 1$, $n^2+1 \equiv 2$, but $n^2+1 \equiv 0$, so $2 \equiv 0 \pmod{p}$, contradicting p an odd prime.

Similarly, order of n can't be 2 since $n^2 \equiv 1$, again yielding $2 \equiv 0$.

$\therefore$ order of n mod p is 4.

$\therefore$ By Th. 8.1, $\phi(p)$ is a multiple of 4.

$\therefore 4k = \phi(p) = p-1 \Rightarrow \underline{p = 4k+1}$

(6) The odd prime divisors of n^4+1 are of the form $8k+1$.

Pf: Assume $p \mid n^4+1$. $\therefore n^4 \equiv -1 \pmod{p}$

$\therefore n^8 \equiv 1 \pmod{p}$

Assume $\gcd(n,p)=1$, for if $n=kp$, then $n^4 = k^4 p^4$, so $p \mid n^4$. This with $p \mid n^4+1 \Rightarrow p \mid 1$, so assume $\gcd(n,p)=1$

Let r be order of $n \bmod p$.

$\therefore r \mid 8$ by Th. 8.1.

$\therefore r = 1, 2, 4$, or 8

Order of n can't be 1, for $n \equiv 1 \Rightarrow n^4 \equiv 1$.
Order of n can't be 2. If true, then $n^2 \equiv 1$, $n^4 \equiv 1$, but $n^4 \equiv -1$.
Order of n can't be 4 since $n^4 \equiv -1$.

$\therefore$ Order of $n \bmod p$ must be 8.

$\therefore 8 \mid \phi(p) \Rightarrow 8 \mid p-1 \Rightarrow 8k = p-1$,

or $\underline{p = 8k+1}$, some k.

(c) The odd prime divisors of the integer n^2+n+1 that are different from 3 are of the form $6k+1$.

Pf: Observe that for n odd or even, n^2+n+1 is always odd. $\therefore$ restrict divisors to primes >2. For $n=1$, $n^2+n+1=3$, so not of form $6k+1$. $\therefore$ Consider $p>3$.

Assume p prime >3, and

$n^2+n+1 \equiv 0 \pmod{p}$

Note that $2 \mid p-1$, since p is odd.

Also, $(n-1)(n^2+n+1) \equiv 0 \pmod{p}$,

and $(n-1)(n^2+n+1) = n^3-1$.

$\therefore n^3 \equiv 1 \pmod{p}$

Now, $n \not\equiv 1 \pmod{p}$ for that would restrict n.

Also, $n^2 \not\equiv 1 \pmod{p}$, for if $n^2 \equiv 1$, then $n^2+n+1 \equiv n+2$. But

$n^2+n+1 \equiv 0$, so $n+2 \equiv 0$, so $n \equiv -2$,
also impossible for all n.

$\therefore$ order of n mod p is 3 [1]

But $\gcd(n,p)=1$. For if $n=kp$, some k,
Then $n^2 = k^2p^2$. $\therefore n^2+n = k^2p^2 + kp = (k^2p+k)p$
$\therefore p \mid (n^2+n)$. Since $p \mid (n^2+n+1)$, this
implies $p \mid 1$, a contradiction.

$\therefore n^{\phi(p)} \equiv 1 \pmod{p}$, and with [1]

$3 \mid \phi(p) \Rightarrow 3 \mid p-1$

Since $2 \mid p-1$, $\therefore 2\cdot 3 \mid p-1$, or $6 \mid p-1$.

$\therefore 6k = p-1$, or $\underline{p = 6k+1}$, some k.

7. Establish that there are infinitely many primes of the form $4k+1$, $6k+1$, and $8k+1$!

Pf: (a) $4k+1$

Assume finitely many primes of form $4k+1$,
$p_1, p_2, \dots, p_r$.

Consider The integer $(2p_1p_2\cdots p_r)^2+1$.
This integer is odd, and so its prime factorization will contain odd primes.
Let q be such a prime.
By prob. 6(a), q is of The form $4K+1$ and so q must be among $p_1, \ldots, p_r$.

$\therefore q \mid (2p_1\cdots p_r)^2$ and $q \mid (2p_1\cdots p_r)^2+1$

$\therefore q \mid 1$, a contradiction.

$\therefore$ Assumption of finitely many primes of form $4K+1$ is false.

(b) $6K+1$

Assume finitely many primes of form $6K+1$, $p_1, p_2, \ldots, p_r$. Note That all p_i are Thus odd.

Consider The integer $(3p_1p_2\cdots p_r)^2+(3p_1p_2\cdots p_r)+1$

This is an odd integer since $3p_1\cdots p_r$ is odd
It must have a prime divisor other Than 3, for if $3^s = (3p_1\cdots p_r)^2+(3p_1\cdots p_r)+1$, some s, Then $3 \mid 1$, a contradiction.
$\therefore$ Let q be such an odd divisor of $(3p_1\cdots p_r)^2+(3p_1\cdots p_r)+1$

By prob. 6(c), q must be of form $6k+1$, and so must be among $p_1, \dots, p_r$.

$\therefore\ q \mid (3p_1 \cdots p_r)^2 + (3p_1 \cdots p_r)$, and so

$q \mid 1$, a contradiction.

$\therefore$ Main assumption false, so infinitely many primes of form $6k+1$.

(c) $8k+1$

Assume finitely many primes of form $8k+1$, $p_1, \dots, p_r$. $\therefore$ All p_i are odd.

Consider $(2p_1 \cdots p_r)^4 + 1$, an odd integer

Let q be a prime divisor of $(2p_1 \cdots p_r)^4 + 1$.

$\therefore\ q$ is odd since $(2p_1 \cdots p_r)^4 + 1$ is odd, and

by prob. 6(b), q is of form $8k+1$.

$\therefore\ q$ must be one of $p_1, \dots, p_r$.

$\therefore\ q \mid (2p_1 \cdots p_r)^4 \Rightarrow q \mid 1$.

$\therefore$ Assumption false, so there are infinitely many primes of form $8k+1$.

8. (a) Prove that if p and q are odd primes and $q \mid a^p - 1$, then either $q \mid a-1$ or else $q = 2kp+1$, some k.

Pf: First note $\gcd(a,q)=1$. For if not, then let $d = \gcd(a,q)$, $d>1$.
$\therefore d \mid q$ and $q \mid a^p - 1 \Rightarrow d \mid a^p - 1$. Since also $d \mid a$, then $d \mid 1$, a contradiction.
$\therefore \gcd(a,q) = 1$

Since $q \mid a^p - 1$, then $a^p \equiv 1 \pmod{q}$

Let r be order of a mod q.
$\therefore$ By Th. 8.1, $r \mid p$. Since p is prime, $r = 1$ or p.

If $r=1$, then $a \equiv 1 \pmod{q} \Rightarrow \underline{q \mid (a-1)}$

If $r = p$, then since $a^{\phi(q)} \equiv 1 \pmod{q}$, then by Th. 8.1, $p \mid \phi(q)$
But $\phi(q) = q-1$

$\therefore p \mid q-1 \Rightarrow$ There is some k' s.t.

$pk' = q-1$. But q odd $\Rightarrow q-1$ even.

Since p is odd, k' must be even, so $k' = 2k$ some k.

$\therefore p(2k) = q-1$, $\underline{q = 2pk+1}$, some k.

(b) Use part (a) to show that if p is an odd prime, then the prime divisors of $2^p - 1$ are of the form $2kp+1$.

Pf: 2^p is even, so $2^p - 1$ is odd, so it contains an odd prime divisor. Let it be q.

$\therefore q \mid 2^p - 1$. From (a) above, letting

$a = 2$, since $q \nmid (2-1)$, then

$q = 2kp + 1$, some k.

(c) Find the smallest prime divisors of $2^{17}-1$ and $2^{29}-1$.

$2^{17}-1$: By (b), prime divisors are of form

$$2(17)K+1 = 34K+1$$

Primes of form $34K+1$:
103, 137, 239, 307, 409, 433, 613, 647, ...

However, $2^{17}-1$ happens to be prime.

$2^{29}-1$: By (b), prime divisors are of form

$$2(29)K+1 = 58K+1$$

$\therefore$ Primes of form $58K+1$ are:
59, 233, ...

$$2^{29} \stackrel{?}{\equiv} 1 \pmod{59}$$

$$2^{6} = 64 \equiv 5 \pmod{59}$$
$$2^{24} \equiv 5^{4} = 625 \equiv 35 \pmod{59}$$
$$2^{5} \equiv 32 \pmod{59}$$
$$\therefore 2^{29} = 2^{24} \cdot 2^{5} \equiv 35 \cdot 32 \equiv 58 \pmod{59}$$

$2^{29} \overset{?}{\equiv} 1 \pmod{233}$

$2^4 \equiv 16 \pmod{233}$

$2^8 \equiv 256 \equiv 23$

$2^{16} \equiv 23^2 = 529 \equiv 63 \pmod{233}$

$2^{24} \equiv 23 \cdot 63 = 1449 \equiv 51 \pmod{233}$

$\therefore 2^{29} \equiv 2^{24} \cdot 2^5 \equiv 51 \cdot 32 = 1632 \equiv 1 \pmod{233}$

$\therefore 2^{29} \equiv 1 \pmod{233}$

$\therefore$ 233 smallest prime divisor of $2^{29}-1$

9. Prove there are infinitely many primes of the form $2kp+1$, where p is an odd prime.

Pf: Assume finitely many primes of form $2kp+1$. Call them $q_1, q_2, \ldots, q_r$

Let $a = 2q_1q_2\cdots q_r$, and consider the integer $(2q_1q_2\cdots q_r)^p - 1 = a^p - 1$

Plan: Use 8(a) to show an odd prime divisor q of a^p-1 must be one of q_i, and so must divide a, and so will divide 1.

$$a^p - 1 = (a-1)(a^{p-1} + a^{p-2} + \ldots + 1)$$

$$= (a-1)(a^{p-1} + a^{p-2} + \ldots + a^{p-p})$$

$\therefore a^{p-1} + a^{p-2} + \ldots + 1$ has p terms

If a is even, $a^{p-1} + a^{p-2} + \cdots + 1$ is odd
If a is odd, since p is odd,
$a^{p-1} + \cdots + a^2 + a$ is even ($p-1$ terms),
so $a^{p-1} + \cdots + 1$ is odd.

$\therefore a^{p-1} + a^{p-2} + \cdots + 1$ is always odd, and so must have an odd prime divisor. Call it q.

$\therefore q \mid a^{p-1} + a^{p-2} + \cdots + 1$, or

$$a^{p-1} + a^{p-2} + \ldots + 1 \equiv 0 \pmod{q} \quad [1]$$

$\therefore q \mid a^p - 1$ since $a^p - 1 = (a-1)(a^{p-1} + \ldots + 1)$

$\therefore$ By 8(a), either $q \mid (a-1)$ or $q = 2kp + 1$.

Suppose $q \mid (a-1)$. $\therefore a \equiv 1 \pmod{q}$

$\therefore a^2 \equiv 1, a^3 \equiv 1$, etc.

$\therefore a^{p-1} + a^{p-2} + \dots + 1 \equiv p \pmod{q}$ [2]

since there are p terms in $a^{p-1} + a^{p-2} + \dots + 1$.

$\therefore$ [1] and [2] $\Rightarrow p \equiv 0 \pmod{q}$

$\therefore p = q$ since both are prime.

$\therefore a \equiv 1 \pmod{p}$ since $a \equiv 1 \pmod{q}$ by assumption

But $a = 2q_1 q_2 \cdots q_r$

$= 2(2k_1 p + 1)(2k_2 p + 1) + \cdots (2k_r p + 1)$

Since $2k_i p + 1 \equiv 1 \pmod{p}$, then $a \equiv 2 \pmod{p}$

$\therefore a \equiv 1 \pmod{p}$ and $a \equiv 2 \pmod{p}$

$\therefore$ assumption that $q \mid (a-1)$ is false.

$\therefore q = 2kp+1$ by 8(a), so

q must be one of $q_1, q_2, \dots, q_r$

since they are finite.

$\therefore q \mid (2q_1q_2\cdots q_r)$ and since

$q \mid a^p - 1$, then $q \mid (2q_1q_2\cdots q_r)^p - 1$,

so $q \mid 1$, an impossibility.

$\therefore$ Assumption that primes of form $2kp+1$ is finite is false.

10. (a) Verify 2 is a primitive root of 19 but not of 17.

$\phi(19) = 18 \qquad 2^6 = 64 \equiv 7 \pmod{19}$

$7^2 = 49 \equiv 11 \pmod{19}$

$7^3 \equiv 77 = 4 \cdot 19 + 1 \equiv 1 \pmod{19}$

$\therefore 2^{18} = (2^6)^3 \equiv 7^3 \equiv 1 \pmod{19}$

$\therefore 2^{18} = 2^{\phi(19)} \equiv 1 \pmod{19}$

Suppose order of 2 mod 19 $= r$, $r < 18$

$\therefore r \mid 18$, so $r \in \{1, 2, 3, 6, 9\}$

$r \neq 1$, since $2^1 \not\equiv 1 \pmod{19}$
$r \neq 2$, since $2^2 = 4 \not\equiv 1 \pmod{19}$
$r \neq 3$, since $2^3 = 8 \not\equiv 1 \pmod{19}$
$r \neq 6$, since $2^6 = 64 \equiv 7 \not\equiv 1 \pmod{19}$
$r \neq 9$, since $2^9 = 2^3 \cdot 2^6 \equiv 8 \cdot 7 = 56 \equiv 18 \pmod{19}$

$\therefore 18 = \phi(19)$ is the smallest integer r
for which $2^r \equiv 1 \pmod{19}$
$\therefore 2$ is a primitive root of 19

For 17, $\phi(17) = 16$ Let r be order of 2

$\therefore r \in \{1, 2, 4, 8, 16\}$

Clearly $r \neq 1, 2, 4$

$2^8 = 256 = 15(17) + 1 \equiv 1 \pmod{17}$

$\therefore 2^8 \equiv 1 \pmod{17}$, so order of

2 mod 17 is 8, not 16.

$\therefore 2$ not a primitive root of 17.

(6) Show 15 has no primitive root by calculating orders of 2, 4, 7, 8, 11, 13, and 14 mod 15.

The integers relatively prime to 15: 1, 2, 4, 7, 8, 11, 13, 14
$\therefore \phi(15) = 8$.

Divisors of 8: 1, 2, 4, 8

1: $1^1 = 1 \equiv 1 \pmod{15}$ $1 < 8 \Rightarrow 1$ not a primitive root
2: $2^4 = 16 \equiv 1 \pmod{15}$ $4 < 8 \Rightarrow 2$ not a prim. root
4: $4^2 = 16 \equiv 1 \pmod{15}$ $2 < 8 \Rightarrow 4$ not a prim. root
7: $7^2 = 49 \equiv 4$
$\therefore 7^4 \equiv 16 \equiv 1 \pmod{15}$ $4 < 8 \Rightarrow 7$ not a prim. root
8: $8^2 = 64 \equiv 4 \pmod{15}$
$8^4 \equiv 16 \equiv 1 \pmod{15}$ $4 < 8 \Rightarrow 8$ not a prim. root
11: $11^2 = 121 \equiv 1 \pmod{15}$ $2 < 8 \Rightarrow 11$ not a prim. root
13: $13^2 = 169 \equiv 4 \pmod{15}$
$13^4 \equiv 16 \equiv 1 \pmod{15}$ $4 < 8 \Rightarrow 13$ not a prim. root
14: $14^2 = 196 \equiv 1 \pmod{15}$ $2 < 8 \Rightarrow 14$ not a prim. root

11. Let r be a primitive root of the integer n. Prove that r^k is a primitive root of n if and only if $\gcd(k, \phi(n)) = 1$.

Pf: Since r has order $\phi(n)$ mod n, by

Th. 8.3, r^k has order $\phi(n)/\gcd(k,\phi(n))$

(a) $\therefore$ If $\gcd(k,\phi(n))=1$, then r^k has order $\phi(n)$

$\therefore r^k$ is a primitive root of n

(b) Suppose r^k is a primitive root of n.

$\therefore r^k$ has order $\phi(n)$. From above,

$$\phi(n) = \phi(n)/\gcd(k,\phi(n))$$

$\therefore \gcd(k,\phi(n))=1$

12. (a) Find two primitive roots of 10.

$10=2\cdot 5$. $\therefore \phi(10) = (2^1-2^0)\cdot(5^1-5^0) = 4$

These relatively prime numbers are 1, 3, 7, 9

If 10 has a primitive root, then it has exactly $\phi(\phi(10)) = \phi(4) = 2$ of them.

$\therefore 3$: $3^4 = 81 \equiv 1 \pmod{10}$

and $3^1 \equiv 3 \pmod{10}$, $3^2 \equiv 9 \pmod{10}$, $3^3 \equiv 7 \pmod{10}$

7: $7^2 \equiv 9 \pmod{10}$. $\therefore 7^4 \equiv 81 \equiv 1 \pmod{10}$
$7^1 \equiv 7$, $7^2 = 49 \equiv 9$, $7^3 \equiv 63 \equiv 3 \pmod{10}$

$\therefore$ 3, 7 are primitive roots of 10.

Note $9^2 = 81 \equiv 1 \pmod{10}$, $\therefore$ 9 not a prim. root, since $2 < 4$. ($9^4 \equiv 1 \pmod{10}$).

(b) Use the information that 3 is a primitive root of 17 to obtain the eight primitive roots of 17.

Note $\phi(\phi(17)) = \phi(16) = 2^4 - 2^3 = 8$

By Th. 8.3, since 3 has order $\phi(17) = 16$ mod 17, then 3^r has order $16/\gcd(r, 16)$

$\therefore$ When $\gcd(r, 16) = 1$, 3^r will have order 16, and so be a prim. root of 17.

$\therefore$ For $\gcd(r, 16) \Rightarrow r = 1, 3, 5, 7, 9, 11, 13, 15$

$\therefore 3^3 \equiv 27 \equiv \underline{10} \pmod{17}$

$3^5 \equiv 10 \cdot 3^2 \equiv \underline{5} \pmod{17}$

$3^7 \equiv 3^5 \cdot 3^2 \equiv 5 \cdot 9 \equiv 45 \equiv \underline{11} \pmod{17}$

$3^9 \equiv 3^7 \cdot 3^2 \equiv 11 \cdot 9 \equiv 85 + 14 \equiv \underline{14} \pmod{17}$

$3^{11} \equiv 3^9 \cdot 3^2 \equiv 14 \cdot 9 \equiv 126 \equiv 119 + 7 \equiv \underline{7} \pmod{17}$

$3^{13} \equiv 3^{11} \cdot 3^2 \equiv 7 \cdot 9 \equiv 63 = 51 + 12 \equiv \underline{12} \pmod{17}$

$3^{15} \equiv 3^{13} \cdot 3^2 \equiv 12 \cdot 9 = 108 \equiv 102 + 6 \equiv \underline{6} \pmod{17}$

$\therefore$ Primitive roots of 17 are: $\underline{3, 5, 6, 7, 10, 11, 12, 14}$

13.(a). Prove That if p and $q > 3$ are both odd primes and $q \mid R_p$, Then $q = 2kp + 1$ for some integer k.

Pf: $R_p = \dfrac{10^p - 1}{9}$. $\therefore$ If $q \mid R_p$, Then for some r, $qr = \dfrac{10^p - 1}{9}$, or $q(9r) = 10^p - 1$.

By prob. 8a, $q \mid 10 - 1$ or $q = 2kp + 1$, some k.

Since $q > 3$, Then $q \nmid (10-1)$ since $10-1 = 3^2$

$\therefore q = 2kp + 1$, some k.

(b). Find The smallest prime divisors of The repunits $R_5 = 11111$ and $R_7 = 1111111$.

R_5: First test 3 : $R_5 = 3 \cdot 3700 + 11$.

$\therefore 3 \nmid R_5$.

By (a) if $q > 3$, Then $q = 2k(5) + 1$

$\therefore q = 10k + 1$

$\therefore$ Test 11, 31, 41, 71, 101, ...

By trial, $11 \nmid R_5$, $31 \nmid R_5$, but $41 \mid R_5$.

$\therefore$ Smallest prime divisor of R_5 is $\underline{41}$

R_7 : First test 3 : $R_7 = 3 \cdot 370000 + 1111$

$1111 = 3 \cdot 370 + 1$

$\therefore 3 \nmid R_7$

By (a), if $q > 3$, Then $q = 2k(7) + 1$

$\therefore q = 14k + 1$

$\therefore q = 29, 43, 71, 113, 127, 197, 211, 239, \ldots$

By trial, $\underline{239} \mid R_7$ is the smallest

14. (a) Let $p > 5$ be prime. If R_n is the smallest repunit for which $p \mid R_n$, establish that $n \mid p-1$. For example, R_8 is the smallest repunit divisible by 73, and $8 \mid 72$.

Pf: $p \mid R_n \Rightarrow$ There is some k s.t.

$$pk = \frac{10^n - 1}{9}$$

$$\therefore p(9k) = 10^n - 1, \text{ or } 10^n \equiv 1 \pmod{p}$$

Suppose $\exists\, m < n$ s.t. $10^m \equiv 1 \pmod{p}$

Then $10^m - 1 = kp$, some k.

But for $m \geq 1$, $9 \mid 10^m - 1$

$\therefore 9 \mid kp$, so $9 \mid k$ since p is prime, $p > 5$.

$\therefore$ let $9k' = k$.

$$\therefore \frac{10^m - 1}{9} = \frac{kp}{9} = k'p$$

$\therefore p \mid R_m$, contradicting that R_n is the smallest repunit divisible by p.

$\therefore$ order of 10 mod p is n.

Since $\gcd(10, p) = 1$, $10^{\phi(p)} \equiv 1 \pmod{p}$, or $10^{p-1} \equiv 1 \pmod{p}$.

By Th. 8.1 and [1], $\underline{n \mid p-1}$

(b) Find the smallest R_n divisible by 13.

By (a), if $13 \mid R_n$, then $n \mid 12$

$\therefore$ Consider $n = 1, 2, 3, 4, 6$

$13 \nmid R_1$ since $13 \nmid 1$

$13 \nmid R_2$ since $13 \nmid 11$

$13 \nmid R_3$ since $13 \nmid 111$

$13 \nmid R_4$ since $13 \nmid 1111$

$13 \mid R_6$ since $13 \cdot 8547 = 111{,}111$