

## 1.1 Mathematical Induction

Note Title

4/21/2004

1. a.  $1+2+3+\dots+n = \frac{n(n+1)}{2}$  for all  $n \geq 1$ .

$$1 = \frac{1 \cdot (1+1)}{2} = 1$$

Suppose  $1+2+\dots+k = \frac{k(k+1)}{2}$

Then  $1+2+\dots+k+(k+1) = \frac{k(k+1)}{2} + (k+1)$

$$\begin{aligned} &= \frac{k(k+1)}{2} + \frac{2(k+1)}{2} \\ &= \frac{(k+1)(k+2)}{2} \end{aligned}$$

So,  $k \Rightarrow k+1$

6.  $1+3+5+\dots+(2n-1) = n^2$  for all  $n \geq 1$ .

$$1 = 1$$

Suppose  $1+3+\dots+(2k-1) = k^2$

Then  $1+3+\dots+(2k-1)+(2k+1) = k^2 + 2k+1$

$$= (k+1)^2$$

So,  $k \Rightarrow k+1$

$$C. 1 \cdot 2 + 2 \cdot 3 + 3 \cdot 4 + \dots + n(n+1) = \frac{n(n+1)(n+2)}{3}, \text{ all } n \geq 1$$

$$K=1 : 1 \cdot 2 = \frac{(1+1)(1+2)}{3} = \frac{1 \cdot 2 \cdot 3}{3} = 2$$

Suppose statement is true K. Then,

$$\begin{aligned} 1 \cdot 2 + \dots + k(k+1) + (k+1)(k+2) &= \frac{k(k+1)(k+2)}{3} + (k+1)(k+2) \\ &= \frac{k(k+1)(k+2)}{3} + \frac{3(k+1)(k+2)}{3} \\ &= \frac{(k+1)[k(k+2) + 3k + 6]}{3} = \frac{(k+1)[k^2 + 5k + 6]}{3} \\ &= \frac{(k+1)[(k+2)(k+3)]}{3} \quad \text{So, } K \Rightarrow k+1 \end{aligned}$$

$$d. 1^2 + 3^2 + 5^2 + \dots + (2n-1)^2 = \frac{n(2n-1)(2n+1)}{3}, \text{ all } n \geq 1$$

$$K=1 : 1^2 = \frac{(2 \cdot 1 - 1)(2 \cdot 1 + 1)}{3} = \frac{1 \cdot 1 \cdot 3}{3} = 1$$

$K \Rightarrow K+1 :$

$$1^2 + 3^2 + \dots + (2k-1)^2 + (2k+1)^2 =$$

$$\begin{aligned}
& \frac{k(2k-1)(2k+1)}{3} + (2k+1)^2 \\
&= \frac{k(2k-1)(2k+1)}{3} + \frac{3(2k+1)^2}{3} \\
&= \frac{(2k+1)[k(2k-1) + 3(2k+1)]}{3} \\
&= \frac{(2k+1)[2k^2 - k + 6k + 3]}{3} \\
&= \frac{(2k+1)[2k^2 + 5k + 3]}{3} = \frac{(2k+1)(2k+3)(k+1)}{3} \\
&= \frac{(k+1)(2k+1)(2k+3)}{3}. \text{ So true for } k+1.
\end{aligned}$$

e.  $1^3 + 2^3 + 3^3 + \dots + n^3 = \left[ \frac{n(n+1)}{2} \right]^2$ , a/l  $n \geq 1$

$$k=1: 1^3 = \left[ \frac{1 \cdot 2}{2} \right]^2 = 1^2 = 1$$

$$K \Rightarrow K+1: 1^3 + 2^3 + \dots + k^3 + (k+1)^3$$

$$\begin{aligned}
 &= \left[ \frac{k(k+1)}{2} \right]^2 + (k+1)^3 \\
 &= \frac{k^2(k+1)^2}{4} + \frac{4(k+1)^2(k+1)}{4} \\
 &= \frac{(k+1)^2 [k^2 + 4k + 4]}{4} = \frac{(k+1)^2 (k+2)^2}{4} \\
 &= \left[ \frac{(k+1)(k+2)}{2} \right]^2 \quad \text{So, true for } k+1
 \end{aligned}$$

2. If  $r \neq 1$ , Then  $a + ar + \dots + ar^n = \frac{a(r^{n+1} - 1)}{r-1}$ ,  $n \geq 1$

$$\text{For } k=1: a + ar^1 = a(1+r) = \frac{a(r^2 - 1)}{r-1} = a(r+1)$$

$K \Rightarrow K+1$ :

$$a + ar + \dots + ar^n + ar^{n+1} = \frac{a(r^{n+1} - 1)}{r-1} + ar^{n+1}$$

$$= \frac{a(r^{n+1} - 1)}{r-1} + \frac{ar^{n+1}(r-1)}{r-1}$$

$$= \frac{ar^{n+1} - a + ar^{n+2} - ar^{n+1}}{r-1}$$

$$= \frac{ar^{n+2} - a}{r-1} = \frac{a(r^{n+2} - 1)}{r-1}$$

So, true for  $K+1$

$$3, a^n - 1 = (a-1)(a^{n-1} + a^{n-2} + \dots + a + 1), \text{ for } n \geq 1$$

$$\text{For } K=1 : a^1 - 1 = a - 1 = (a-1)(a^0) = a - 1$$

$$\begin{aligned} K \Rightarrow K+1 : a^{K+1} - 1 &= a^{K+1} - a^K - a + a^K + a - 1 \\ &= a^{K+1} - a + a^K - 1 - a^K + a \\ &= a(a^K - 1) + a^K - 1 - a(a^{K-1} - 1) \\ &= (a+1)(a^K - 1) - a(a^{K-1} - 1) \end{aligned}$$

Use 2nd principle of finite induction for  $K, K-1$

$$= (a+1) [(a-1)(a^{K-1} + a^{K-2} + \dots + a + 1)]$$

$$- a [(a-1)(a^{K-2} + a^{K-3} + \dots + a + 1)]$$

$$= (a-1) \left[ a(a^{K-1} + a^{K-2} + \dots + a + 1) + (a^{K-1} + a^{K-2} + \dots + a + 1) - a(a^{K-2} + a^{K-3} + \dots + a + 1) \right]$$

Combine  
these two

$$= (a-1) \left[ a(a^{k-1} + a^{k-2} + \dots + a+1) + (a^{k-1} + a^{k-2} + \dots + a+1) - (a^{k-1} + a^{k-2} + \dots + a^2 + a) \right]$$

$$= (a-1) \left[ (a^k + a^{k-1} + \dots + a^2 + a) + 1 \right]$$

and so, works for  $k+1$

4. Cube of any integer can be written as the difference of two squares.

Proof:  $n^3 = (1^3 + 2^3 + \dots + n^3) - (1^3 + 2^3 + \dots + (n-1)^3)$ , all  $n$

$$\text{From 1(e), } 1^3 + 2^3 + \dots + n^3 = \left[ \frac{n(n+1)}{2} \right]^2, n \geq 1$$

$$\text{So, } n^3 = \left[ \frac{n(n+1)}{2} \right]^2 - \left[ \frac{(n-1)n}{2} \right]^2$$

If  $n$  is even, Then  $\frac{n}{2}$  is an integer.

If  $n$  is odd, Then  $n+1$  and  $n-1$  are even,  
so  $\frac{n+1}{2}$  and  $\frac{n-1}{2}$  are integers.

$\therefore n^3$  is the difference between squares.

5. (a). For  $n=4$ ,  $n!+1 = 25 = 5^2$   
 $n=5$ ,  $n!+1 = 121 = 11^2$   
 $n=7$ ,  $n!+1 = 5041 = 71^2$

(b). False

$$(3 \cdot 2)! = 720 \neq 3! \cdot 2! = 6 \cdot 2 = 12$$

$$(2+3)! = 120 \neq 2! + 3! = 2 + 6$$

6. a.  $n! > n^2$  for  $n \geq 4$

Proof:  $4! = 24 > 16 = 4^2$

Suppose  $k! > k^2$ , for  $k \geq 4$

$$(k+1)! = (k+1) \cdot k! > (k+1) \cdot k^2$$

$$= k^3 + k^2$$

Since  $k \geq 4$ , then  $k \geq 2$ , so  $k^2 > 2k$ .

Since  $k \geq 1$ , then  $k^3 > 2k$ , so  $k^3 \geq 2k+1$

$$\text{So, } k^3 + k^2 \geq k^2 + 2k + 1 = (k+1)^2$$

$$\text{So } (k+1)! > k^3 + k^2 \geq (k+1)^2$$

$$\text{So } (k+1)! > (k+1)^2$$

$$\text{So, } k \Rightarrow k+1$$

$$6.6. n! > n^3, n \geq 6$$

$$\text{Proof: } 6! = 720 > 216 = 6^3$$

Suppose  $k! > k^3$  for any  $k \geq 6$

$$\therefore (k+1)! = (k+1)k! > (k+1)k^3$$

$$= k^4 + k^3$$

Since  $k \geq 6$ , then  $k \geq 3$ , so  $k^2 \geq 3k$

Also,  $k \geq 1$ , so  $k^2 \geq k$ , and  $k^2 \geq k+1$

$$\text{So } k^4 = k^2 \cdot k^2 \geq 3k(k+1) = 3k^2 + 3k$$

$$\therefore k^3 + k^4 \geq k^3 + 3k^2 + 3k$$

$$\therefore k^4 + k^3 \geq k^3 + 3k^2 + 3k + 1 = (k+1)^3$$

$$\therefore (k+1)! > k^4 + k^3 \geq (k+1)^3$$

$$(k+1)! > (k+1)^3$$

$$\text{So, } k \Rightarrow k+1$$

$$7. \quad 1(1!) + 2(2!) + \dots + n(n!) = (n+1)! - 1, \quad n \geq 1$$

$$K=1: \quad 1(1!) = 1 = (1+1)! - 1 = 2! - 1 = 1$$

$$K \Rightarrow K+1: \text{Let } 1(1!) + 2(2!) + \dots + K(K!) = (K+1)! - 1$$

$$\text{Then } 1(1!) + \dots + (K+1)(K+1)!$$

$$= (K+1)! - 1 + (K+1)(K+1)!$$

$$= (K+1)! [1 + K+1] - 1$$

$$= (K+1)! (K+2) - 1$$

$$= (K+2)! - 1 \quad \text{So, true for } K+1$$

$$8. \text{a. } 2 \cdot 6 \cdot 10 \cdots (4n-2) = \frac{(2n)!}{n!}, \quad n \geq 1$$

$$K=1: \quad 2 = \frac{2!}{1!} = 2$$

$$K \Rightarrow K+1: \text{Let } 2 \cdot 6 \cdot 10 \cdots (4k-2) = \frac{(2k)!}{k!}$$

$$\text{Then } 2 \cdot 6 \cdot 10 \cdots (4k-2)(4k+2) =$$

$$\frac{(2k)!}{k!} (4k+2) = \frac{(2k)!}{k!} (2k+1) 2$$

$$= \frac{(2k)!}{k!} (2k+1) 2 \frac{(k+1)}{(k+1)}$$

$$= \frac{(2k)! (2k+1)(2k+2)}{k! (k+1)} = \frac{(2k+2)!}{(k+1)!}$$

So, true for  $k+1$

$$b. 2^n (n!)^2 \leq (2n)! , n \geq 1$$

$$\text{From (a), } (2n)! = 2 \cdot 6 \cdot 10 \cdots (4n-2) (n!)$$

So problem reduces to :

$$2^n (n!)^2 \leq 2 \cdot 6 \cdot 10 \cdots (4n-2) (n!)$$

$$\text{Or, } 2^n (n!) \leq 2 \cdot 6 \cdot 10 \cdots (4n-2)$$

$$\text{For } k=1: 2^1 (1!) = 2 \leq 2$$

$$K \Rightarrow K+1: L \vdash 2^k (k!) \leq 2 \cdot 6 \cdot 10 \cdots (4k-2)$$

$$2^{k+1}(k+1)! = 2^k(k!) \cdot 2 \cdot (k+1)$$

$$= 2^k(k!)(2k+2)$$

$$< 2^k(k!)(4k+2)$$

$$\leq 2 \cdot 6 \cdot 10 \cdots (4k-2) (4k+2)$$

$$= 2 \cdot 6 \cdot 10 \cdots (4(k+1)-2)$$

So, true for  $k+1$

9. If  $1+a > 0$ , Then  $(1+a)^n \geq 1+na$ ,  $n \geq 1$

$$K=1: 1+a \geq 1+a$$

$$K \Rightarrow K+1: \text{Let } (1+a)^K \geq 1+Ka$$

$$(1+a)^{K+1} = (1+a)^K(1+a)$$

$$\geq (1+Ka)(1+a)$$

$$= 1+Ka+a+Ka^2$$

$$\geq 1+Ka+a \quad (a^2 > 0, \text{ so } Ka^2 > 0)$$

$$= 1 + (k+1)a$$

$$\therefore (1+a)^{k+1} \geq 1 + (k+1)a$$

So, it's true for  $k+1$

10. a.  $\frac{1}{1^2} + \frac{1}{2^2} + \frac{1}{3^2} + \dots + \frac{1}{n^2} \leq 2 - \frac{1}{n}, n \geq 1$

$$k=1: \frac{1}{1^2} = 1 \leq 2 - \frac{1}{1} = 1$$

$$k \Rightarrow k+1: \text{Let } \frac{1}{1^2} + \frac{1}{2^2} + \dots + \frac{1}{k^2} \leq 2 - \frac{1}{k}$$

$$\text{Then, } \frac{1}{1^2} + \dots + \frac{1}{k^2} + \frac{1}{(k+1)^2} \leq 2 - \frac{1}{k} + \frac{1}{(k+1)^2}$$

Since  $k \geq 1$ , then  $k^2 + 2k < k^2 + 2k + 1$ ,

$$\text{or, } \frac{k^2 + 2k}{(k+1)^2} < 1, \text{ or } \frac{k(k+2)}{(k+1)^2} < 1$$

$$\therefore \frac{(k+1)+1}{(k+1)^2} < \frac{1}{k} \Rightarrow \frac{1}{k+1} + \frac{1}{(k+1)^2} < \frac{1}{k}$$

$$\therefore -\frac{1}{k} + \frac{1}{(k+1)^2} < -\frac{1}{k+1}$$

$$\therefore 2 - \frac{1}{k} + \frac{1}{(k+1)^2} < 2 - \frac{1}{k+1}$$

$$\therefore \frac{1}{1^2} + \frac{1}{2^2} + \dots + \frac{1}{(k+1)^2} < 2 - \frac{1}{k+1}$$

So,  $k \Rightarrow k+1$

$$b. \frac{1}{2} + \frac{2}{2^2} + \frac{3}{2^3} + \dots + \frac{n}{2^n} = 2 - \frac{n+2}{2^n}$$

$$K=1: \frac{1}{2} = 2 - \frac{1+2}{2^1} = 2 - \frac{3}{2} = \frac{1}{2}$$

$$K \Rightarrow K+1: \text{Let } \frac{1}{2} + \frac{2}{2^2} + \dots + \frac{K}{2^K} = 2 - \frac{K+2}{2^K}$$

$$\text{Then, } \frac{1}{2} + \dots + \frac{K}{2^K} + \frac{K+1}{2^{K+1}} = 2 - \frac{K+2}{2^K} + \frac{K+1}{2^{K+1}}$$

$$= 2 - \frac{K+2}{2^K} \cdot \frac{2}{2} + \frac{K+1}{2^{K+1}}$$

$$= 2 + \frac{(K+1) - (2K+4)}{2^{K+1}} = 2 + \frac{-K-3}{2^{K+1}}$$

$$= 2 - \frac{(K+1)+2}{2^{K+1}} \quad \text{So, } k \Rightarrow k+1$$

11.  $(2n)! / 2^n n!$  is an integer,  $n \geq 0$

$$n=0: 0! = 1 \text{ by definition. So } \frac{0!}{2^0 0!} = \frac{1}{1 \cdot 1} = 1$$

$k \Rightarrow k+1$ : Suppose  $\frac{(2k)!}{2^k k!}$  is an integer.

$$\frac{[2(k+1)]!}{2^{k+1} (k+1)!} = \frac{(2k)! (2k+1)(2k+2)}{2^k (k!) 2(k+1)}$$

$$= \frac{(2k)!}{2^k k!} \cdot \frac{(2k+1)(2k+2)}{2k+2}$$

$$= (\text{integer}) \cdot (2k+1) = \text{integer}$$

12.  $T(21) = 32 \quad T(23) = 35$

$$T(T(21)) = 16 \quad T(35) = 53$$

$$T(16) = 8 \quad T(53) = 80$$

$$T(8) = 4 \quad T(80) = 40$$

$$T(4) = 2 \quad T(40) = 20$$

$$T(2) = 1 \quad T(20) = 10$$

$$T(10) = 5$$

$$T(5) = 8$$

$$T(8) = 4$$

$$T(4) = 2$$

$$T(2) = 1$$

$$13. \quad a_1 = 1 \quad a_2 = 2 \quad a_3 = 3$$

$$a_n = a_{n-1} + a_{n-2} + a_{n-3}, \text{ for } n \geq 4$$

$$\text{Prove: } a_n < 2^n, \quad n \geq 1$$

$$\text{Proof: } 1 < 2^1, 2 < 2^2, 3 < 2^3$$

Let  $k \geq 4$ , and assume  $a_k < 2^k, k=4, \dots, k$

$$\text{Then } a_{k+1} = a_k + a_{k-1} + a_{k-2}$$

$$< 2^k + 2^{k-1} + 2^{k-2}$$

$$< 2^k + 2^{k-1} + 2^{k-1}$$

$$= 2^k + 2 \cdot 2^{k-1} = 2^k + 2^k$$

$$= 2 \cdot 2^k = 2^{k+1}$$

$$\therefore a_{k+1} < 2^{k+1}$$

$$14. \quad a_1 = 11, \quad a_2 = 21, \quad a_n = 3a_{n-1} - 2a_{n-2}, \quad n \geq 3$$

$$\text{Prove: } a_n = 5 \cdot 2^n + 1, \quad n \geq 1$$

$$\begin{aligned} \text{Proof: } a_1 &= 5 \cdot 2^1 + 1 = 11 \\ a_2 &= 5 \cdot 4 + 1 = 21 \end{aligned}$$

$$\text{Suppose } a_k = 5 \cdot 2^k + 1 \text{ for } 3, 4, \dots, k$$

$$\begin{aligned} \text{Then } a_{k+1} &= 3a_k - 2a_{k-1} \\ &= 3(5 \cdot 2^k + 1) - 2(5 \cdot 2^{k-1} + 1) \\ &= 15 \cdot 2^k + 3 - 5 \cdot 2^k - 2 \\ &= 10 \cdot 2^k + 1 \\ &= 5 \cdot 2 \cdot 2^k + 1 \\ &= 5 \cdot 2^{k+1} + 1 \end{aligned}$$

$\therefore$  if works for  $3, 4, \dots, k$ , Then works for  $k+1$ .

$\therefore$  Works for all  $k \geq 1$

## 1.2 The Binomial Theorem

Note Title

4/25/2004

1. a. Newton's identity

$$\binom{n}{k} \binom{k}{r} = \binom{n}{r} \binom{n-r}{k-r} \quad n \geq k \geq r \geq 0$$

$$\frac{n!}{k!(n-k)!} \cdot \frac{k!}{r!(k-r)!} = \frac{n!}{r!} \cdot \frac{1}{(n-k)!(k-r)!}$$
$$= \frac{n!}{r!} \cdot \frac{(n-r)!}{(n-r)!} \cdot \frac{1}{(n-k)!(k-r)!}$$

$$= \frac{n!}{r!(n-r)!} \cdot \frac{(n-r)!}{(k-r)!(n-k)!}$$

$$= \binom{n}{r} \cdot \frac{(n-r)!}{(k-r)!(n-r-(k-r))!} = \binom{n}{r} \binom{n-r}{k-r}$$

b.  $\binom{n}{k} = \frac{n-k+1}{k} \binom{n}{k-1} \quad n \geq k \geq 1$

Without using part (a),

$$\binom{n}{k} = \frac{n!}{k!(n-k)!} = \frac{n! \cdot (n-k+1)}{k(k-1)!(n-k+1)!}$$

$$= \frac{n!}{(k-1)! (n-k+1)!} \cdot \frac{(n-k+1)}{k} = \frac{(n-k+1)}{k} \binom{n}{k-1}$$

To use part (a), let  $r=1$

$$\text{Then } \binom{n}{k} \binom{k}{1} = \binom{n}{1} \binom{n-1}{k-1} \quad n \geq k \geq r \geq 0$$

$$\text{So, } \binom{n}{k} k = n \binom{n-1}{k-1}$$

$$= n \frac{(n-1)!}{(k-1)! (n-k)!}$$

$$= \frac{n!}{(k-1)! (n-k+1)!} \cdot (n-k+1)$$

$$\text{So, } \binom{n}{k} = \frac{n-k+1}{k} \binom{n}{k-1}$$

2. If  $2 \leq k \leq n-2$ , and  $n \geq 4$

$$\binom{n}{k} = \binom{n-2}{k-2} + 2 \binom{n-2}{k-1} + \binom{n-2}{k}$$

Working from the right hand side,

$$\begin{aligned}
& \frac{(n-2)!}{(k-2)!(n-k)!} + 2 \frac{(n-2)!}{(k-1)!(n-k-1)!} + \frac{(n-2)!}{k!(n-k-2)!} \\
&= \frac{k \cdot (k-1) (n-2)!}{k! (n-k)!} + \frac{2k(n-k)(n-2)!}{k! (n-k)!} + \frac{(n-k)(n-k-1)(n-2)!}{k! (n-k)!} \\
&= \frac{(n-2)! [k^2 - k + 2kn - 2k^2 + n^2 - nk - n - kn + k^2 + k]}{k! (n-k)!} \\
&= \frac{(n-2)! [n^2 - n]}{k! (n-k)!} = \frac{n(n-1)(n-2)!}{k! (n-k)!} = \binom{n}{k}
\end{aligned}$$

$2 \leq k$  for  $(k-2)!$  in denominator to work  
 $n-k-2 \geq 0$ , or  $n-2 \geq k \geq 2$ , so  $n \geq 4$  for  
 $(n-k-2)!$  in denominator to work.

3. a. From Binomial Theorem, letting  $a=b=1$ ,

$$(a+b)^n = 2^n = \sum_{k=0}^n \binom{n}{k} 1^{n-k} 1^k$$

$$\text{So, } 2^n = \binom{n}{0} + \binom{n}{1} + \dots + \binom{n}{n}$$

b. From Binomial Theorem, let  $a=1, b=-1$

$$0^n = 0 = \binom{n}{0} - \binom{n}{1} + \dots + (-1)^n \binom{n}{n}$$

$$\text{C. } \binom{n}{1} + 2\binom{n}{2} + 3\binom{n}{3} + \dots + n\binom{n}{n} = n2^{n-1}$$

In Binomial Theorem, let  $a=1$

$$\text{Then } (1+b)^{n-1} = \sum_{k=0}^{n-1} \binom{n-1}{k} b^k$$

$$\text{So, } n(1+b)^{n-1} = n \left[ \binom{n-1}{0} + \binom{n-1}{1} b + \dots + \binom{n-1}{n-1} b^{n-1} \right]$$

Now let  $b=1$ . Then

$$\begin{aligned} n2^{n-1} &= n \binom{n-1}{0} + n \binom{n-1}{1} + \dots + n \binom{n-1}{n-1} \\ &= \sum_{k=0}^{n-1} n \binom{n-1}{k} \end{aligned}$$

$$\text{But } n \binom{n-1}{k} = \frac{n(n-1)!}{k!(n-k-1)!} = \frac{n!}{k!(n-(k+1))!} \cdot \frac{(k+1)}{(k+1)}$$

$$= (k+1) \frac{n!}{(k+1)! (n-(k+1))!}$$

$$= (k+1) \binom{n}{k+1}$$

$$\therefore n2^{n-1} = \sum_{k=0}^{n-1} n \binom{n-1}{k} = \sum_{k=0}^{n-1} (k+1) \binom{n}{k+1}$$

$$= \binom{n}{1} + 2 \binom{n}{2} + 3 \binom{n}{3} + \dots + n \binom{n}{n}$$

$$1 \cdot \binom{n}{0} + 2 \binom{n}{1} + 2^2 \binom{n}{2} + \dots + 2^n \binom{n}{n} = 3^n$$

In Binomial Theorem, let  $a=1, b=2$

$$\begin{aligned} (a+b)^n &= 3^n = \binom{n}{0} 1^n + \binom{n}{1} 1^{n-1} 2^1 + \dots + \binom{n}{n} 2^n \\ &= \binom{n}{0} + 2 \binom{n}{1} + \dots + 2^n \binom{n}{n} \end{aligned}$$

$$c. \binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \dots = 2^{n-1}$$

$$\binom{n}{1} + \binom{n}{2} + \binom{n}{3} + \dots = 2^{n-1}$$

Proof: Add / Subtract results of (a) & (b)

If  $n$  is even, Then last term is positive

$$\begin{aligned} \binom{n}{0} + \binom{n}{1} + \dots + \binom{n}{n} &= 2^n \\ + \left[ \binom{n}{0} - \binom{n}{1} + \dots + \binom{n}{n} \right] &= 0 \\ \hline 2 \left[ \binom{n}{0} + \binom{n}{1} + \dots + \binom{n}{n} \right] &= 2^n \end{aligned}$$

If  $n$  is odd, last term is  $-\binom{n}{n}$

$$\begin{aligned} \binom{n}{0} + \binom{n}{1} + \dots + \binom{n}{n} &= 2^n \\ + \left[ \binom{n}{0} - \binom{n}{1} + \dots - \binom{n}{n} \right] &= 0 \\ \hline 2 \left[ \binom{n}{0} + \binom{n}{1} + \dots + \binom{n}{n-1} \right] &= 2^n \end{aligned}$$

$$\text{So, } \binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \dots = 2^{n-1}$$

If  $n$  is even, Then last term is positive

$$\begin{aligned} \binom{n}{0} + \binom{n}{1} + \dots + \binom{n}{n} &= 2^n \\ - \left[ \binom{n}{0} - \binom{n}{1} + \dots + \binom{n}{n} \right] &= 0 \\ \underline{2 \left[ \binom{n}{1} + \binom{n}{3} + \dots + \binom{n}{n-1} \right]} &= 2^n \end{aligned}$$

If  $n$  is odd, last term is  $- \binom{n}{n}$

$$\begin{aligned} \binom{n}{0} + \binom{n}{1} + \dots + \binom{n}{n} &= 2^n \\ - \left[ \binom{n}{0} - \binom{n}{1} + \dots - \binom{n}{n} \right] &= 0 \\ \underline{2 \left[ \binom{n}{1} + \binom{n}{3} + \dots + \binom{n}{n} \right]} &= 2^n \end{aligned}$$

So,  $\binom{n}{1} + \binom{n}{3} + \binom{n}{5} + \dots = 2^{n-1}$

$$f. \quad \binom{n}{0} - \frac{1}{2} \binom{n}{1} + \frac{1}{3} \binom{n}{2} - \dots + \frac{(-1)^n}{n+1} \binom{n}{n} = \frac{1}{n+1}$$

The terms look like the terms in (6) with coefficients. So, need a relation with coefficient in front of binomial term.

The " $k$ "th term can be written as :

$$(-1)^{k-1} \cdot \frac{1}{k} \binom{n}{k-1}$$

Note that  $\binom{n}{k-1} = \frac{n!}{(k-1)! (n-k+1)!}$

$$= \frac{k}{n+1} \cdot \frac{(n+1)!}{k! (n-k+1)!}$$

Thus,  $\frac{1}{k} \binom{n}{k-1} = \frac{1}{n+1} \binom{n+1}{k}$

So, problem is equivalent to :

$$\sum_{k=1}^n (-1)^k \binom{n+1}{k}$$

$$= \frac{1}{n+1} \binom{n+1}{1} - \frac{1}{n+1} \binom{n+1}{2} + \dots + \frac{(-1)^n}{n+1} \binom{n+1}{n+1}$$

$$= \frac{1}{n+1} \left[ \binom{n+1}{1} - \binom{n+1}{2} + \binom{n+1}{3} - \dots - (-1)^n \binom{n+1}{n+1} \right]$$

From (6),  $\binom{n}{0} = \binom{n}{1} - \binom{n}{2} + \dots - (-1)^n \binom{n}{n}$

Substituting  $n = s+1$ ,

$$\binom{s+1}{0} = \binom{s+1}{1} - \binom{s+1}{2} + \dots - (-1)^{s+1} \binom{s+1}{s+1}$$

$$1 = \binom{s+1}{1} - \binom{s+1}{2} + \dots + (-1)^s \binom{s+1}{s+1}$$

$$\therefore \binom{n}{0} - \frac{1}{2} \binom{n}{1} + \dots + \frac{(-1)^n}{n+1} \binom{n+1}{n+1}$$

$$= \frac{1}{n+1} \left[ \binom{n+1}{1} - \binom{n+1}{2} + \dots + (-1)^n \binom{n+1}{n+1} \right]$$

$$= \frac{1}{n+1} \left[ 1 \right] = \frac{1}{n+1}$$

4. a. For  $n \geq 1$ ,  $\binom{n}{r} < \binom{n}{r+1} \Leftrightarrow 0 \leq r < \frac{1}{2}(n-1)$

Proof:  $\binom{n}{r} < \binom{n}{r+1}$

$$\Leftrightarrow \frac{n!}{r!(n-r)!} < \frac{n!}{(r+1)!(n-r-1)!}, 0 \leq r, 0 \leq n-r-1$$

$$\Leftrightarrow \frac{(r+1)!}{r!} < \frac{(n-r)!}{(n-r-1)!} \quad 0 \leq r \leq n-1$$

$$\Leftrightarrow r+1 < n-r, \quad 0 \leq r \leq n-1$$

$$\Leftrightarrow 0 \leq 2r < n-1$$

$$\Leftrightarrow 0 \leq r < \frac{1}{2}(n-1)$$

b.  $\binom{n}{r} > \binom{n}{r+1} \Leftrightarrow n-1 \geq r > \frac{1}{2}(n-1)$

Proof:  $\binom{n}{r} > \binom{n}{r+1}$

$$\Leftrightarrow \frac{n!}{r!(n-r)!} > \frac{n!}{(r+1)!(n-r-1)!}, \quad r \geq 0, n-r-1 \geq 0$$

$$\Leftrightarrow \frac{(r+1)!}{r!} > \frac{(n-r)!}{(n-r-1)!}, \quad r \geq 0, n-r-1 \geq 0$$

$$\Leftrightarrow r+1 > n-r, \quad n-1 \geq r \geq 0$$

$$\Leftrightarrow 2r > n-1, \quad n-1 \geq r \geq 0$$

$$\Leftrightarrow n-1 \geq r > \frac{1}{2}(n-1) \geq 0$$

$$C. \quad \binom{n}{r} = \binom{n}{r+1} \Leftrightarrow r = \frac{1}{2}(n-1)$$

Proof: From The steps in (a) + (c),

$$\binom{n}{r} = \binom{n}{r+1} \Leftrightarrow r+1 = n-r, \quad n-1 \geq r \geq 0$$

$$\Leftrightarrow 2r = n-1, \quad n-1 \geq r \geq 0.$$

$$\Leftrightarrow r = \frac{1}{2}(n-1), \quad n-1 \geq r \geq 0$$

$$5.a. \text{ For } n \geq 2, \quad \binom{2}{2} + \binom{3}{2} + \dots + \binom{n}{2} = \binom{n+1}{3}$$

$$\text{Proof: For } k=2, \quad \binom{2}{2} = 1 = \binom{2+1}{3} = 1$$

$$k \Rightarrow k+1: \text{ Assume } \binom{2}{2} + \dots + \binom{k}{2} = \binom{k+1}{3}$$

$$\text{Then, } \binom{2}{2} + \dots + \binom{k}{2} + \binom{k+1}{2}$$

$$= \binom{k+1}{3} + \binom{k+1}{2}$$

$$= \binom{k+2}{3} \quad \text{From Pascal's identity}$$

$$\binom{r}{s} + \binom{r}{s-1} = \binom{r+1}{s}, \quad 1 \leq s \leq r$$

6. First,  $m^2 = 2 \binom{m}{2} + m$ ,  $m \geq 2$

$$2 \binom{m}{2} + m \Leftrightarrow 2 \frac{m!}{2!(m-2)!} + m, m \geq 2$$

$$\Leftrightarrow m(m-1) + m = m^2, m \geq 2$$

Now,  $1^2 + 2^2 + \dots + n^2 = \frac{n(n+1)(2n+1)}{6}$

Proof:  $1^2 + 2^2 + \dots + n^2$

$$= 1 + 2 \binom{2}{2} + 2 + 2 \binom{3}{2} + 3 + \dots + 2 \binom{n}{2} + n$$

$$= (1+2+\dots+n) + 2 \left[ \binom{2}{2} + \binom{3}{2} + \dots + \binom{n}{2} \right]$$

$$= (1+2+\dots+n) + 2 \binom{n+1}{3}$$

$$= (1+2+\dots+n) + 2 \frac{(n+1)!}{3 \cdot 2 \cdot (n-2)!}$$

$$= \frac{n(n+1)}{2} + \frac{(n+1)(n)(n-1)}{3}$$

$$= \frac{3n(n+1)}{6} + 2(n+1)(n)(n-1)$$

$$= \frac{n(n+1)[3+2n-2]}{6} = \frac{n(n+1)(2n+1)}{6}$$

$$C. 1 \cdot 2 + 2 \cdot 3 + 3 \cdot 4 + \dots + n(n+1) = \frac{n(n+1)(n+2)}{3}$$

Proof: From (5),  $m^2 = 2\binom{m}{2} + m$ , or

$$m(m-1) = 2\binom{m}{2}, m \geq 2$$

$$\therefore 1 \cdot 2 + 2 \cdot 3 + 3 \cdot 4 + \dots + n(n+1)$$

$$= 2\binom{2}{1} + 2\binom{3}{2} + 2\binom{4}{2} + \dots + 2\binom{n+1}{2}$$

$$= 2 \left[ \binom{n+2}{3} \right], \text{ from (a)}$$

$$= 2 \frac{(n+2)!}{3! (n-1)!} = \frac{2(n+2)(n+1)n}{3 \cdot 2 \cdot 1}$$

$$= \frac{n(n+1)(n+2)}{3}$$

$$6. \binom{2}{2} + \binom{4}{2} + \dots + \binom{2n}{2} = \frac{n(n+1)(4n-1)}{6}, n \geq 2$$

$$\text{Proof: First, } \binom{2m}{2} = \frac{(2m)!}{2!(2m-2)!} = \frac{2m(2m-1)}{2}$$

$$= 2m^2 - m = m^2 + m^2 - m$$

$$= m^2 + 2 \binom{m}{2}, m \geq 2, \text{ from } S(c)$$

$$\therefore \binom{2}{2} + \binom{4}{2} + \dots + \binom{2n}{2}$$

$$= 1 + \left[ 2^2 + 2 \binom{2}{2} + \dots + n^2 + 2 \binom{n}{2} \right]$$

$$= (1^2 + 2^2 + \dots + n^2) + 2 \left[ \binom{2}{2} + \dots + \binom{n}{2} \right]$$

$$= \frac{n(n+1)(2n+1)}{6} + 2 \binom{n+1}{3}, \text{ from } S(6), S(g) \\ n \geq 2$$

$$= \frac{n(n+1)(2n+1)}{6} + \frac{2(n+1)!}{3 \cdot 2 \cdot (n-2)!}$$

$$= \frac{n(n+1)(2n+1)}{6} + 2 \frac{(n+1)(n)(n-1)}{6}$$

$$= \frac{n(n+1)}{6} [2n+1 + 2n-2]$$

$$= \frac{n(n+1)(4n-1)}{6}$$

$$7. \text{ For } n \geq 1, 1^2 + 3^2 + \dots + (2n-1)^2 = \binom{2n+1}{3}$$

$$\text{Proof: } k=1 : 1^2 = 1 = \binom{2 \cdot 1 + 1}{3} = \binom{3}{3} = 1$$

$$k \Rightarrow k+1 : \text{Assume } 1^2 + 3^2 + \dots + (2k-1)^2 = \binom{2k+1}{3}$$

$$\text{Then, } 1^2 + 3^2 + \dots + (2k-1)^2 + (2(k+1)-1)^2$$

$$= 1^2 + \dots + (2k-1)^2 + (2k+1)^2$$

$$= \binom{2k+1}{3} + (2k+1)^2$$

$$= \frac{(2k+1)!}{3!(2k-2)!} + (2k+1)^2$$

$$= \frac{(2k+1)! (2k)(2k-1)}{3!(2k-2)!(2k)(2k-1)} + 6 \cdot \frac{(2k+1)^2 \cdot (2k)!}{6 \cdot (2k)!}$$

$$= \frac{(2k+1)! [ (2k)(2k-1) + 6(2k+1) ]}{3! (2k)!}$$

$$= \frac{(2k+1)! [ 4k^2 - 2k + 12k + 6 ]}{3! (2k)!}$$

$$= \frac{(2k+1)!}{3!} \left[ (2k+2)(2k+3) \right]$$

$$= \frac{(2k+3)!}{3!(2k+3-3)!} = \binom{2k+3}{3}$$

$$\text{So, } k \Rightarrow k+1$$

8. For  $n \geq 1$ ,  $\binom{2n}{n} = \frac{1 \cdot 3 \cdot 5 \cdots (2n-1)}{2 \cdot 4 \cdot 6 \cdots 2n} 2^{2n}$

$$k=1: \quad \binom{2}{1} = \frac{2!}{1!1!} = 2, \quad \frac{1}{2} 2^2 = \frac{4}{2} = 2$$

$$k \Rightarrow k+1: \text{ Suppose } \binom{2k}{k} = \frac{1 \cdot 3 \cdot 5 \cdots (2k-1)}{2 \cdot 4 \cdot 6 \cdots 2k} 2^{2k}$$

$$\text{Then } \binom{2k+2}{k+1} = \frac{(2k+2)!}{(k+1)!(k+1)!}$$

$$= \frac{(2k+2)(2k+1)}{(k+1)(k+1)} \frac{(2k)!}{k! k!}$$

$$= \frac{(2k+2)(2k+1)}{(k+1)(k+1)} \binom{2k}{k}$$

$$= \frac{(2k+2)(2k+1)}{(k+1)(k+1)} \cdot \frac{1 \cdot 3 \cdot 5 \cdots (2k-1)}{2 \cdot 4 \cdot 6 \cdots 2k} 2^{2k}$$

$$= \frac{2(k+1)}{(k+1)(k+1)} \cdot \frac{1 \cdot 3 \cdot 5 \cdots (2k-1)(2k+1)}{2 \cdot 4 \cdot 6 \cdots 2k} 2^{2k}$$

$$= \frac{2}{(k+1)} \cdot \frac{1 \cdot 3 \cdot 5 \cdots (2k+1)}{2 \cdot 4 \cdot 6 \cdots 2k} 2^{2k}$$

$$= \frac{4}{(2k+2)} \cdot \frac{1 \cdot 3 \cdot 5 \cdots (2k+1)}{2 \cdot 4 \cdot 6 \cdots 2k} 2^{2k}$$

$$= \frac{1 \cdot 3 \cdot 5 \cdots (2k+1)}{2 \cdot 4 \cdot 6 \cdots (2k)(2k+2)} \cdot 2^{2k+2}$$

So,  $k \Rightarrow k+1$

9.  $2^n < \binom{2n}{n} < 2^{2n}$ , for  $n \geq 1$

Proof:  $n! < 1 \cdot 3 \cdot 5 \cdots (2n-1)$ , for  $n \geq 1$

Since it's true for  $k=2$  ( $2 < 1 \cdot 3$ )

and if  $k! < 1 \cdot 3 \cdots (2k-1)$ , Then

$$(k+1)! = k!(k+1) < 1 \cdot 3 \cdot 5 \cdots (2k-1)(k+1) \\ < 1 \cdot 3 \cdot 5 \cdots (2k-1)(2k+1)$$

Also,  $2^n n! = 2 \cdot 4 \cdot 6 \cdots 2n$ , since it's true for  $k=1$ , and  $2^{k+1}(k+1)! = 2(k+1)2^k k! = 2(k+1) \cdot 2 \cdot 4 \cdot 6 \cdots 2k$   
 $= 2 \cdot 4 \cdot 6 \cdots 2k \cdot 2(k+1)$

$$\text{So, } 2^n n! < 1 \cdot 3 \cdot 5 \cdots (2n-1) 2^n$$

$$\Rightarrow 1 < \frac{1 \cdot 3 \cdot 5 \cdots (2n-1)}{2^n n!} 2^n \\ = \frac{1 \cdot 3 \cdot 5 \cdots (2n-1)}{2 \cdot 4 \cdots 2n} 2^n$$

$$\therefore 2^n < \frac{1 \cdot 3 \cdot 5 \cdots (2n-1)}{2 \cdot 4 \cdot 6 \cdots 2n} 2^{2n} = \binom{2n}{n}, \text{ by (8)}$$

Now, since  $2k-1 < 2k$  for  $k \geq 1$ ,

Then  $1 \cdot 3 \cdot 5 \cdots (2n-1) < 2 \cdot 4 \cdot 6 \cdots 2n$ ,

So,  $\frac{1 \cdot 3 \cdot 5 \cdots (2n-1)}{2 \cdot 4 \cdot 6 \cdots 2n} < 1$ , for  $n \geq 1$

$\therefore$  by (8),  $\binom{2n}{n} = \frac{1 \cdot 3 \cdot 5 \cdots (2n-1)}{2 \cdot 4 \cdot 6 \cdots 2n} 2^{2n} < 2^{2n}$ ,  $n \geq 1$

10. Given  $C_n = \frac{1}{n+1} \binom{2n}{n} = \frac{(2n)!}{n! \overbrace{(n+1)!}^{\text{?}}}, n \geq 0$

Prove:  $C_n = \frac{2(2n-1)}{n+1} C_{n-1}, n \geq 1$

Proof:  $k=1: C_1 = \frac{2!}{1! 2!} = 1, C_0 = \frac{0!}{0! 1!} = 1$

$$\therefore \frac{2(2-1)}{1+1} = 1,$$

$$\text{So, } C_1 = \frac{2(2-1)}{1+1} C_0$$

$k \Rightarrow k+1:$  Suppose  $C_k = \frac{2(2k-1)}{k+1} C_{k-1}$

Then  $C_{k+1} = \frac{(2k+2)!}{(k+1)! (k+2)!}$

$$= \frac{(2k+2)(2k+1)}{(k+1)(k+2)} \cdot \frac{(2k)!}{k! (k+1)!}$$

$$= \frac{2(2k+1)}{(k+2)} \cdot C_k = \frac{2(2k+1)}{(k+2)} \cdot \frac{2(2k-1)}{(k+1)} C_{k-1}$$

$$= \frac{2(2k+1) \cdot 2(2k-1)}{(k+2)(k+1)} \cdot \frac{(2k-2)!}{(k-1)! k!}$$

$$= \frac{2(2k+1)}{(k+2)} \cdot \frac{2 \cdot (2k-1)!}{(k-1)! (k+1)!}$$

$$= \frac{2(2k+1)}{(k+2)} \cdot \frac{2k}{k} \cdot \frac{(2k-1)!}{(k-1)! (k+1)!}$$

$$= \frac{2(2k+1)}{(k+2)} \cdot \frac{(2k)!}{k! (k+1)!}$$

$$= \frac{2[2(k+1)-1]}{[(k+1)+1]} C_{(k+1)-1}$$

$$S_0, k = 7 \quad k+1$$

## 1.3 Early Number Theory

Note Title

5/10/2004

1. a. A number is triangular  $\Leftrightarrow$  it is of the form  $\frac{n(n+1)}{2}$  for some  $n \geq 1$ .

Proof:  $1+2+3+\dots+n = \frac{n(n+1)}{2}$

from problem 1(a) of Problem Set 1.1.

So, if a number  $X$  is triangular  
Then for some  $n$ ,  $1+2+\dots+n = X$   
by definition, and so  $X = \frac{n(n+1)}{2}$

If  $X = \frac{n(n+1)}{2}$  for some  $n$ , then

$$X = 1+2+\dots+n$$

- b. An integer  $n$  is triangular  $\Leftrightarrow s_n + 1$  is a perfect square.

Proof: If  $n$  is triangular, Then there is a  $k$  such that  $n = \frac{k(k+1)}{2}$

$$\therefore s_n = 4k(k+1),$$

$$8n+1 = 4K(K+1) + 1$$

$$= 4K^2 + 4K + 1$$

$$= (2K+1)^2$$

$\therefore n$  triangular  $\Rightarrow 8n+1$  is a perfect square

If  $8n+1$  is a perfect square, Then There is an integer  $K$  such that  $K^2 = 8n+1$ .

Note That  $8n+1$  must be odd.

$\therefore K^2$  is odd, and so  $K$  is odd.

$\therefore$  There is an  $s$  such that  $2s+1 = K$

$$\therefore (2s+1)^2 = 8n+1$$

$$\therefore 4s^2 + 4s + 1 = 8n + 1$$

$$\therefore 4s(s+1) = 8n$$

$$\therefore \frac{s(s+1)}{2} = n$$

$\therefore 8n+1$  a perfect square  $\Rightarrow n$  triangular

c. If  $a$  and  $b$  are consecutive triangular numbers, Then  $a+b$  is a perfect square.

Proof: Let  $1+2+\dots+n = a$

Then  $1+2+\dots+n+n+1 = b$

$$\begin{aligned} \therefore a+b &= \frac{n(n+1)}{2} + \frac{n(n+1)}{2} + (n+1) \\ &= n(n+1) + (n+1) \\ &= (n+1)(n+1) \end{aligned}$$

So,  $a+b$  is a perfect square.

d. If  $n$  is triangular, Then so are

$9n+1$ ,  $25n+3$ , and  $49n+6$ .

Proof: Let  $1+2+\dots+k = n$

$$\text{Then } 9n+1 = 9 \frac{k(k+1)}{2} + 1 = \frac{9k^2 + 9k + 2}{2}$$

$$= \frac{(3k+1)(3k+2)}{2} = \frac{s(s+1)}{2}$$

for  $s = 3k+1$ , and so by 1(a),  $25n+3$  is triangular.

$$25n+3 = \frac{25k(k+1)}{2} + 3 = \frac{25k^2 + 25k + 6}{2}$$

$$= \frac{(5k+2)(5k+3)}{2} = \frac{s(s+1)}{2}$$

for  $s = 5k+2$ , and so by 1(a),  $25n+3$  is triangular.

$$49n+6 = \frac{49k(k+1)}{2} + 6 = \frac{49k^2 + 49k + 12}{2}$$

$$= \frac{(7k+3)(7k+4)}{2} = \frac{s(s+1)}{2}$$

for  $s = 7k+3$ , and so by 1(a),  $49n+6$  is triangular.

2.  $t_n = \binom{n+1}{2}$ ,  $n \geq 1$ ,  $t_n$  the  $n^{th}$  triangular.

$$\binom{n+1}{2} = \frac{(n+1)!}{2!(n-1)!} = \frac{(n+1)n}{2}, \text{ so by 1(a),}$$

$$t_n = \binom{n+1}{2}$$

3.  $t_1 + t_2 + \dots + t_n = \frac{n(n+1)(n+2)}{6}$ ,  $n \geq 1$

Proof: From problem 1(c) of problem set 1.1,

$$1 \cdot 2 + 2 \cdot 3 + \dots + n(n+1) = \frac{n(n+1)(n+2)}{3}, n \geq 1$$

$$\therefore \frac{1 \cdot 2}{2} + \frac{2 \cdot 3}{2} + \dots + \frac{n(n+1)}{2} = \frac{n(n+1)(n+2)}{6}$$

Note that each term  $k$  can be written as  $\frac{k(k+1)}{2} = t_k$

$$\therefore t_1 + t_2 + \dots + t_n = \frac{n(n+1)(n+2)}{6}$$

The hint given:  $t_{k-1} + t_k = k^2$

$$t_{k-1} = \frac{(k-1)(k-1+1)}{2} = \frac{k(k-1)}{2}$$

$$\therefore t_{k-1} + t_k = \frac{k(k-1)}{2} + \frac{k(k+1)}{2}$$

$$= \frac{k^2 - k + k^2 + k}{2} = k^2$$

You could prove the statement using

$$1^2 + 2^2 + \dots + n^2 = \frac{n(n+1)(2n+1)}{6} \text{ from}$$

5(6) of problem set 1.2, and breaking problem up into even + odd number of terms.

$$4. 9(2n+1)^2 = t_{9n+4} - t_{3n+1}$$

Proof: Since  $t_k = \frac{k(k+1)}{2}$ ,

$$t_{9n+4} = \frac{(9n+4)(9n+5)}{2}, \quad t_{3n+1} = \frac{(3n+1)(3n+2)}{2}$$

$$\therefore t_{9n+4} - t_{3n+1} = \frac{(81n^2 + 81n + 20) - (9n^2 + 9n + 2)}{2}$$

$$= \frac{72n^2 + 72n + 18}{2} = 36n^2 + 36n + 9$$

$$= 9(4n^2 + 4n + 1) = 9(2n+1)^2$$

5. a. Find two triangular numbers,  $t_r$  and  $t_s$ , such that  $t_r + t_s$  and  $t_r - t_s$  are triangular.

The triangular numbers are:

$$1, 3, 6, 10, 15, 21, 28, 36, 45, 55, \dots$$

$$15 + 21 = 36, \quad 21 - 15 = 6$$

b. Three successive triangular numbers whose product is a perfect square.

$$\frac{n(n+1)}{2} \cdot \frac{(n+1)(n+2)}{2} \cdot \frac{(n+2)(n+3)}{2} = k^2$$

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

So, if we can find an  $n$  such that

$\frac{n(n+3)}{2}$  is a perfect square, problem

would be solved. The perfect squares  
are 1, 4, 9, 16, 25, 36, 49, ...

By trial and error, if  $n=3$ , Then  $\frac{3(3+3)}{2}=9$

$$\text{So, } t_3 \cdot t_4 \cdot t_5 = 6 \cdot 10 \cdot 15 = 900 = 30^2$$

c. Three successive triangular numbers  
whose sum is a perfect square.

Trial & error works faster than trying  
to figure this out.

$$t_5 + t_6 + t_7 = 15 + 21 + 28 = 64 = 8^2$$

6.a. If  $t_n$  is a perfect square, then  
 $t_{4n(n+1)}$  is also a perfect square.

Proof: Assume  $t_n = k^2 = \frac{n(n+1)}{2}$

$$\text{Then } 2k^2 = n(n+1)$$

$$t_{4n(n+1)} = \frac{4n(n+1)(4n(n+1)+1)}{2}$$

$$= \frac{4 \cdot 2k^2 \cdot [4n^2 + 4n + 1]}{2}$$

$$= 4k^2 (2n+1)^2$$

$$= [2k(2n+1)]^2, \text{ and so is a square.}$$

6.  $t_1 = 1$  is a perfect square

$$t_{4 \cdot 1(1+1)} = t_8 = 36 \text{ is a perfect square}$$

$$t_{4 \cdot 8(8+1)} = t_{288} = \frac{288(288+1)}{2} = 41616 = 204^2$$

$$7. t_{n+1}^2 - t_n^2 = k^3, \text{ for some integer } k$$

$$\text{Proof: } t_{n+1} = \frac{(n+1)(n+2)}{2}, t_n = \frac{n(n+1)}{2}$$

$$\therefore t_{n+1}^2 - t_n^2 = \frac{(n+1)^2(n+2)^2 - (n+1)^2 n^2}{4}$$

$$= \frac{(n+1)^2 [n^2 + 4n + 4 - n^2]}{4}$$

$$= \frac{(n+1)^2 \cdot (4n+4)}{4} = (n+1)^3, \text{ for } n \geq 1$$

8.  $\frac{1}{1} + \frac{1}{3} + \frac{1}{6} + \dots + \frac{1}{t_n} < 2$

Proof: Each term can be written as

$$\frac{1}{\frac{k(k+1)}{2}} = \frac{2}{k(k+1)} = 2 \left[ \frac{1}{k} - \frac{1}{k+1} \right]$$

$$\begin{aligned} \therefore \frac{1}{1} + \frac{1}{3} + \dots + \frac{1}{t_n} &= 2 \left[ \frac{1}{1} - \frac{1}{2} \right] + 2 \left[ \frac{1}{2} - \frac{1}{3} \right] + \dots + 2 \left[ \frac{1}{n} - \frac{1}{n+1} \right] \\ &= 2 \left[ \frac{1}{1} - \frac{1}{n+1} \right] = 2 \left( 1 - \frac{1}{n+1} \right) \end{aligned}$$

Since  $n \geq 0$ , Then  $n+1 \geq 0$ , so  $\frac{1}{n+1} \geq 0$ ,

and  $- \frac{1}{n+1} \leq 0$ , so  $1 - \frac{1}{n+1} < 1$ ,

so  $2 \left( 1 - \frac{1}{n+1} \right) < 2$ .

$$\therefore \frac{1}{1} + \frac{1}{3} + \dots + \frac{1}{t_n} < 2$$

$$9. \text{ q. } t_x = t_y + t_z, x = \frac{n(n+3)}{2} + 1, y = n+1, z = \frac{n(n+3)}{2}$$

$$\text{Proof: } t_y + t_z = \frac{(n+1)(n+2)}{2} + \frac{n(n+3)}{2} \left[ \frac{n(n+3)}{2} + 1 \right]$$

$$= \frac{2(n+1)(n+2)}{2} + \frac{n(n+3)}{2} \left[ \frac{n(n+3)}{2} + 1 \right]$$

$$= \frac{2 \left[ \frac{n^2 + 3n + 2}{2} \right]}{2} + \frac{n(n+3)}{2} \left[ \frac{n(n+3)}{2} + 1 \right]$$

$$= \frac{2 \left[ \frac{n(n+3)}{2} + 1 \right]}{2} + \frac{n(n+3)}{2} \left[ \frac{n(n+3)}{2} + 1 \right]$$

$$= \frac{\left[ \frac{n(n+3)}{2} + 1 \right] \left[ \frac{n(n+3)}{2} + 1 + 1 \right]}{2}$$

$$= t_x, \text{ for } n \geq 1 \quad (\text{if } n=0, \text{ then } z=0)$$

$$6. n=1: t_3 = t_2 + t_2, \text{ or } 6 = 3 + 3$$

$$n=2: t_6 = t_3 + t_5, \text{ or } 21 = 6 + 15$$

$$n=3 : t_{10} = t_4 + t_9, \text{ or } 55^- = 10 + 45^-$$

## 2.1 The Division Algorithm

Note Title

9/13/2004

1.  $a, b$  integers,  $b > 0$ ,  $\exists$  unique  $q, r$  s.t.  
 $a = qb + r$ ,  $2b \leq r < 3b$

Pf: By Division Alg.,  $\exists$  unique  $q', r'$ , s.t.

$$a = q'b + r', \quad 0 \leq r' < b$$

$$\therefore a = q'b + r' + 2b - 2b = (q' - 2)b + r' + 2b$$

Let  $q = q' - 2$ ,  $r = r' + 2b$ .  $\therefore r, q$  unique

Since  $0 \leq r' < b$ , Then

$$2b \leq r' + 2b < b + 2b, \text{ or } 2b \leq r < 3b$$

2. If  $a = GK + 5$ , then for some  $j$ ,  $a = 3j + 2$

Pf:  $a = GK + 5 = 3 \cdot 2K + 3 + 2 = 3(2K + 1) + 2$

Let  $j = 2K + 1$ . Conversely, if  $a = 8 = 3(2) + 2$ ,  
 $8 = G(1) + 2$ , 1 and 2 are unique, so  $8 \neq GK + 5$ .

3. a. If  $a$  is an integer, Then  $a^2 = 3k$  or  $a^2 = 3k + 1$

Pf: By Division Algorithm,  $\exists$  a  $q$  s.t.

$a = 3q$  or  $a = 3q + 1$  or  $a = 3q + 2$

$$a = 3q : \therefore a^2 = 9q^2 = 3(3q^2). \text{ Let } k = 3q^2$$

$$a = 3q + 1 : \therefore a^2 = 9q^2 + 6q + 1 = 3(3q^2 + 2q) + 1 \\ \text{Let } k = 3q^2 + 2q$$

$$a = 3q + 2 : \therefore a^2 = 9q^2 + 6q + 4 = 9q^2 + 6q + 3 + 1 \\ = 3(3q^2 + 2q + 1) + 1 \\ \text{Let } k = 3q^2 + 2q + 1$$

6. If  $a$  an integer, Then  $a^3 = 9k$ , or  $9k+1$ , or  $9k+8$

Pf: Let  $a = 3q + r$ ,  $r = 0, 1, 2$

$$(3q)^3 = 27q^3 = 9(3q^3) = 9k$$

$$\begin{aligned} (3q+1)^3 &= \binom{3}{0}(3q)^3 + \binom{3}{1}(3q)^2 + \binom{3}{2}3q + \binom{3}{3} \\ &= 27q^3 + 27q^2 + 9q + 1 \\ &= 9(3q^3 + 3q^2 + q) + 1 = 9k + 1 \end{aligned}$$

$$\begin{aligned} (3q+2)^3 &= \binom{3}{0}(3q)^3 + \binom{3}{1}(3q)^2 \cdot 2 + \binom{3}{2}(3q)2^2 + \binom{3}{3}2^3 \\ &= 27q^3 + 54q^2 + 36q + 8 \\ &= 9(3q^3 + 6q^2 + 4q) + 8 = 9k + 8 \end{aligned}$$

C. If  $n$  an integer, Then  $n^4 = 5K$  or  $5K+1$

Pf: Let  $n = 5q + r$ ,  $0 \leq r < 5$

Consider  $n^4 = (5q + r)^4$

From binomial expansion, each term is a factor of 5 except last term:

$$\binom{4}{0}(5q)^4 + \binom{4}{1}(5q)^3r + \binom{4}{2}(5q)^2r^2 + \binom{4}{3}(5q)r^3 + r^4$$

$r=0$ , Then  $r^4=0$ , and  $n^4=5K$  as all other terms have 5 as a factor

$r=1$ , Then clearly  $n^4=5K+1$

$r=2$ , Then  $r^4=16=15+1$ , so all terms and 15 have 5 as a factor, so again,  $n=5K+1$

$r=3$ , Then  $r^4=81=80+1$ , and  $80=5 \cdot 16$ , so again,  $n^4=5K+1$

4. Prove  $3a^2-1$  is never a perfect square.

Pf: Suppose  $3a^2-1=n^2$ , some  $n$ . By 3(a),  $3a^2-1=5K+1$

or  $3a^2 - 1 = 3k \therefore 3(a^2 - k) = 2$  or  $3(a^2 - k) = 1$ , each impossible, since by Div. Alg.,  $2 = 3 \cdot 0 + 2$  and  $1 = 3 \cdot 0 + 1$ .

5. For  $n \geq 1$ , prove  $\frac{n(n+1)(2n+1)}{6}$  is an integer.

Pf:  $n = 6k+r$ ,  $0 \leq r < 6$ . Let  $A = \frac{n(n+1)(2n+1)}{6}$

$r=0$ : Then  $A = k(6k+1)(12k+1)$ , an integer

$$\begin{aligned} r=1: A &= \frac{(6k+1)(6k+2)(12k+3)}{6} \\ &= \frac{(6k+1)(72k^2 + 42k + 6)}{6} \\ &= (6k+1)(12k^2 + 7k + 1), \text{ an integer} \end{aligned}$$

$$\begin{aligned} r=2: A &= \frac{(6k+2)(6k+3)(12k+5)}{6} \\ &= \frac{(36k^2 + 30k + 6)(12k+5)}{6} \\ &= (6k^2 + 5k + 1)(12k+5), \text{ an integer} \end{aligned}$$

$$\begin{aligned} r=3: A &= \frac{(6k+3)(6k+4)(12k+7)}{6} \\ &= \frac{(36k^2 + 42k + 12)(12k+7)}{6} \\ &= (6k^2 + 7k + 2)(12k+7), \text{ an int.} \end{aligned}$$

$$\begin{aligned}
 r=4: A &= \underbrace{(6k+4)(6k+5)(12k+9)}_{6} \\
 &= \underbrace{(72k^2 + 102k + 36)}_{6}(6k+5) \\
 &= (12k^2 + 17k + 6)(6k+5), \text{ an int.}
 \end{aligned}$$

$$\begin{aligned}
 r=5: A &= \underbrace{(6k+5)(6k+6)(12k+11)}_{6} \\
 &= \underbrace{(36k^2 + 66k + 30)}_{6}(12k+11) \\
 &= (6k^2 + 11k + 5)(12k+11), \text{ an int.}
 \end{aligned}$$

C. If  $A$  an integer, then  $A^3 = 7k$  or  $7k \pm 1$ , some  $k$ .

$$\text{Pf: } A = 7q+r, \quad 0 \leq r < 7$$

$$r=0: A^3 = 7q^3 = 7(7^2 q^3). \quad \text{Let } k = 7^2 q^3$$

$$\begin{aligned}
 r=1: A^3 &= (7q+1)^3 = \binom{3}{0}(7q)^3 + \binom{3}{1}(7q)^2 + \binom{3}{2}(7q) + 1 \\
 &= 7\left(7^2 q^3 + 3 \cdot 7q^2 + 3q\right) + 1
 \end{aligned}$$

$$\begin{aligned}
 r=2: A^3 &= (7q+2)^3 = \binom{3}{0}(7q)^3 + \binom{3}{1}(7q)^2 + \binom{3}{2}(7q) + 2^3 \\
 &= 7[\dots] + 8 = 7[\dots] + 7 + 1 \\
 &= 7[\dots + 1] + 1
 \end{aligned}$$

$$r=3: A^3 = (7g+3)^3 = \binom{3}{0}(7g)^3 + \binom{3}{1}(7g)^2 \cdot 3 + \binom{3}{2}(7g) \cdot 3^2 + 3^3 \\ = 7[\dots] + 28 - 1 = 7[\dots + 4] - 1$$

$r=4: A^3 = (7g+4)^3$ . Last term is  $4^3 = 64 = 7 \cdot 9 + 1$

$$\text{So, } A^3 = 7[\dots + 9] + 1$$

$r=5: A^3 = (7g+5)^3$ . Last term  $= 5^3 = 125 = 7 \cdot 18 - 1$

$$\text{So, } A^3 = 7[\dots + 18] - 1$$

$r=6: A^3 = (7g+6)^3$ . Last term  $= 6^3 = 216 = 31 \cdot 7 - 1$

$$\therefore A^3 = 7[\dots + 31] - 1$$

7. For  $a, b$  s.t.  $b \neq 0$ ,  $\exists$  unique  $q, r$  s.t.  
 $a = qb + r$  and  $-\frac{1}{2}|b| < r \leq \frac{1}{2}|b|$

Pf.: Break up  $0 < |b|$  into  $0 < \frac{1}{2}|b|$  and  $\frac{1}{2}|b| < |b|$

$\exists$  unique  $q', r'$  s.t.  $a = bq' + r'$ ,  $0 \leq r' < |b|$

If  $0 \leq r' \leq \frac{1}{2}|b|$ , let  $r = r'$ ,  $q = q'$

If  $\frac{1}{2}|b| < r' < |b|$ , Then  $-\frac{1}{2}|b| < r' - |b| < 0$

$$\therefore a = bg' + r' - |b| + |b|$$

If  $s \geq 0$ , Then  $a = b(g'+1) + r' - |s|$ , so  
let  $r = r' - |b|$ ,  $g = g' + 1$

If  $b < 0$ , Then  $|b| = -b$ , so  $a = bg' + r' - |b| - b$   
 $a = b(g'-1) + r' - |b|$ , so  
let  $g = g'-1$ ,  $r = r' - |b|$

Q. None of integers in below sequence is a perfect square:

$$11, 111, 1111, 11111, \dots$$

Pf: Any number in sequence can be written as

$$A = 11 + 100 + 1000 + \dots = 11 + \sum_{i=2}^n 10^i$$

Each term of  $\sum_{i=2}^n 10^i$  is divisible by 4.

So,  $A_i = 11 + 4r_i = 4(r+2) + 3$ , for certain  $r_i$ .

$$\text{e.g., } 11 = 4(2+2) + 3, \quad 111 = 4(25+2) + 3$$

So  $A_i = 4r_i' + 3$ . By D.v. Alg.,  $r_i'$  and 3 are unique.

Suppose  $A_i = s^2$ . Let  $s = 4g + r$

$r \neq 0$ , as  $s^2 = 16g^2 + 8g + 1 = 4(4g^2 + 2g) + 1$ , which is not of  $4r_i' + 3$  form.

$r \neq 1$ :  $s^2 = 16g^2 + 8g + 1 = 4(4g^2 + 2g) + 1$   
and so not of  $4r_i' + 3$  form

$r \neq 2$ :  $s^2 = 16g^2 + 16g + 4 = 4(4g^2 + 4g + 1)$ ,  
and so not of  $4r_i' + 3$  form.

$r \neq 3$ :  $s^2 = 16g^2 + 24g + 9 = 4(4g^2 + 6g + 2) + 1$ ,  
and so not of form  $4r_i' + 3$  form.

$\therefore$  There is no  $s$  s.t.  $s^2 = 4r_i' + 3$ .

$\therefore$  All  $A_i$  are not perfect squares.

9. If integer  $A = r^2 = s^3$  for some  $r, g$ , Then  
 $A = 7k$  or  $A = 7k + 1$  for some  $k$ .

Pf: Let  $s = 7k + 6$ ,  $0 \leq k < 7$

From #G above  $s^3 = 7K_i$  if  $b=0$

$$s^3 = 7K_i + 1 \text{ if } b=1, 2, 4$$

$$s^3 = 7K_i - 1 \text{ if } b=3, 5, 6$$

for some  $K_i$  ( $i=0, 1, 2, \dots, 6$ )

Or,  $s^3 = 7K_i$  if  $b=0$

$$s^3 = 7K_i + 1 \text{ if } b=1, 2, 4$$

$$s^3 = 7K_i + 6 \text{ if } b=3, 5, 6$$

for some  $K_0, K_1, K_2, K_4, K_3, K_5, K_6$ ,

Now look at  $A = r^2$

Let  $r = 7c + d$ ,  $0 \leq d < 6$

$$d=0 : r^2 = 7(7c^2) = s^3 = 7K_0$$

$$d=1 : r^2 = 49c^2 + 14c + 1 = 7(7c^2 + 2c) + 1 = s^3 = 7K_1 + 1$$

$$d=2 : r^2 = 49c^2 + 28c + 4 = 7(7c^2 + 4c) + 4$$

$$d=3 : r^2 \text{ last term} = 9 = 7+2$$

$$\text{so } r^2 = 7K + 2$$

$$d=4 : r^2 \text{ last term} = 16 = 14+2,$$

$$\text{so } r^2 = 7K + 2$$

$$d=5 : r^2 \text{ last term} = 25 = 21+4$$

$$\text{so } r^2 = 7K + 4$$

$$d=6 : r^2 \text{ last term} = 36 = 35+1,$$

$$\text{so } r^2 = 7K + 1$$

Thus,  $r^2$  of form:  $7K, 7K+1, 7K+2, 7K+4$   
 $s^3$  of form  $7K, 7K+1, \text{ or } 7K+6$

By uniqueness part of Div. Algorithm,  
 $A$  must be either of form  $7K$  or  $7K+1$

10. For  $n \geq 1$ , show  $n(7n^2+5)$  is of form  $6K$

Pf: Let  $n = GK + r$ ,  $0 \leq r < 6$ . Let  $A = n(7n^2+5)$

$$r=0 : A = 6K(7(GK)^2 + 5) = 6[ \quad ]$$

$$\begin{aligned} r=1 : A &= (GK+1)(7(GK+1)^2 + 5) \\ &= 7(GK+1)^3 + 30K + 5 \\ &= 7[6(\dots) + 1] + 30K + 5 \\ &= 6 \cdot 7(\dots) + 7 + 6 \cdot 5K + 5 \\ &= 6[\dots + 5K] + 12 \\ &= 6[\dots + 5K + 2] = 6K' \end{aligned}$$

$$\begin{aligned} r=2 : A &= (GK+2)(7(GK+2)^2 + 5) \\ &= 7(GK+2)^3 + 30K + 10 \\ &= 7[6(\dots) + 8] + 30K + 10 \\ &= 6 \cdot 7(\dots) + 56 + 6 \cdot 5K + 10 \\ &= 6[\dots + 5K + 11] = 6K' \end{aligned}$$

$$\begin{aligned}
 r=3 : A &= (6k+3)(7(6k+3)^2 + 5) \\
 &= 7(6(\dots) + 27) + 6 \cdot 5k + 15 \\
 &= 6 \cdot 7(\dots) + 6 \cdot 5k + 7 \cdot 27 + 15 \\
 &= 6[7(\dots) + 5k + 34] = 6k'
 \end{aligned}$$

$$\begin{aligned}
 r=4 : A &= (6k+4)(7(6k+4)^2 + 5) \\
 &= 7[6(\dots) + 64] + 6 \cdot 5k + 20 \\
 &= 6 \cdot 7(\dots) + 6 \cdot 5k + 7 \cdot 64 + 20 \\
 &= 6[7(\dots) + 5k + 78] = 6k'
 \end{aligned}$$

$$\begin{aligned}
 r=5 : A &= (6k+5)(7(6k+5)^2 + 5) \\
 &= 7[6(\dots) + 125] + 6 \cdot 5k + 25 \\
 &= 6 \cdot 7(\dots) + 6 \cdot 5k + 7 \cdot 125 + 25 \\
 &= 6[7(\dots) + 5k + 150] = 6k'
 \end{aligned}$$

11. If  $n$  is odd, show  $n^4 + 4n^2 + 11$  is of form  $16k$ .

PF: Let  $n = 2k+1$

$$\begin{aligned}
 n^4 + 4n^2 + 11 &= (n^2 + 2)^2 + 7 \\
 &= [(2k+1)^2 + 2]^2 + 7 \\
 &= [4k^2 + 4k + 1 + 2]^2 + 7
 \end{aligned}$$

$$= (4K^2 + 4K + 3)^2 + 7$$

$$\begin{aligned} &= 16K^4 + 16K^3 + 12K^2 \\ &\quad + 16K^3 + 16K^2 + 12K \\ &\quad + 12K^2 + 12K + 9 + 7 \end{aligned}$$

$$= 16K^4 + 32K^3 + 40K^2 + 24K + 16$$

$$K = 2g \text{ or } 2g+1$$

$$\begin{aligned} K = 2g : \quad &16(2g)^4 + 32(2g)^3 + 40(2g)^2 + 24(2g) + 16 \\ &= 16 \left[ (2g)^4 + 2(2g)^3 + 10g^2 + 3g + 1 \right] \\ &= 16x \end{aligned}$$

$$\begin{aligned} K = 2g+1 : \quad &16(2g+1)^4 + 32(2g+1)^3 + 40(2g+1)^2 + 24(2g+1) + 16 \\ &= 16()^4 + 32()^3 + 160g^2 + 160g + 40 + 48g + 24 \\ &\quad + 16 \\ &= 16 \left[ ()^4 + 2()^3 + 10g^2 + 10g + 3g + 4 + 1 \right] \\ &= 16x \end{aligned}$$

## 2.2 The Greatest Common Divisor

Note Title

9/27/2004

Theorem 2.2 For integers  $a, b, c$

(a)  $a|0$  since  $a \cdot 0 = 0$

$1|a$  since  $1 \cdot a = a$

$a|a$  since  $a \cdot 1 = a$

(b)  $a|1 \Leftrightarrow a = \pm 1$

if  $a=1$ , Then  $a \cdot 1 = 1$

if  $a=-1$ , Then  $a \cdot (-1) = 1$

if  $a|1$ , Then  $a \cdot c = 1$  for some  $c$

$\because |c| \neq 1$ , Then  $|c| > 1$ . By def.,  $|a| \geq 1$

$\therefore |a||c| > 1$ , contradicting  $a \cdot c = 1$ .

$\therefore |c| = 1$ ,  $\therefore c = \pm 1$ . If  $c = 1$ , Then

$ac = a = 1$ . If  $c = -1$ , Then  $ac = -a = 1$ .

(c) if  $a|b$  and  $c|d$ , Then  $ac|bd$

$ax = b$ ,  $cy = d$ ,  $\therefore ac(y) = bd$

(d) if  $a|b$  and  $b|c$ , Then  $a|c$

$ax = b$ ,  $by = c$ ,  $\therefore ax(y) = a(xy) = c$

(e)  $a|b$  and  $b|a \Leftrightarrow a = \pm b$

$$a|b \Rightarrow ax = b \quad b|a \Rightarrow by = a$$

$\therefore axy = a$ ,  $xy = 1$ . Using (d),  $x = \pm 1$   
if  $x = 1$ , Then  $ax = b = a$   
(if  $x = -1$ , Then  $ax = b = -a$ )  
 $\therefore a = \pm b$

if  $a = b$ , Then  $a \cdot 1 = a = b$ , so  $a|b$

and  $b \cdot 1 = b = a$ , so  $b|a$

if  $a = -b$ , Then  $a \cdot (-1) = (-b)(-1) = b$ , so  $a|b$   
and  $b \cdot (-1) = -b = a$ , so  $b|a$

$\equiv$

## Problems 2. 2

1.  $a|b \Rightarrow \exists c$  s.t.  $a \cdot c = b$

$$(a) a \cdot c = (-a)(-c) = b \Rightarrow -a | b$$

$$(b) - (a \cdot c) = -b = a \cdot (-c) \Rightarrow a | (-b)$$

$$(c) - (a \cdot c) = -b = (-a) \cdot c = -b \Rightarrow (-a) | (-b)$$

2. (a)  $a|b \Rightarrow \exists x$  s.t.  $ax = b$ .

$$\therefore a \cdot x \cdot c = b \cdot c \Rightarrow a | bc$$

(b)  $a|b$ ,  $a|c \Rightarrow \exists x, y$  s.t.  $ax = b$ ,  $ay = c$

$$\therefore (ax)(ay) = bc = a^2xy \Rightarrow a^2 \mid bc$$

(c) if  $a \mid b$ , then  $\exists x$  s.t.  $ax = b$

$$\therefore acx = bc \Rightarrow ac \mid bc$$

if  $ac \mid bc$ , Then  $\exists x$  s.t.  $acx = bc$

$$\text{since } c \neq 0, ax = b \Rightarrow a \mid b$$

(d) if  $a \mid b$  and  $c \mid d$ , Then  $\exists x, y$  s.t.

$$ax = b, cy = d.$$

$$\therefore (ax)(cy) \neq ac(xy) = bd \Rightarrow ac \mid bd$$

3. Not true. Let  $a = 3, b = 2, c = 7$

$$\text{Then } a \mid (b+c) \equiv 3 \mid (2+7), \text{ but } 3 \nmid 2, 3 \nmid 7$$

$$4. (a) 8 \mid 5^{2n} + 7$$

$$\text{Pf: } n=1 : 5^{2n} + 7 = 32, \text{ and } 8 \mid 32$$

$$\text{Suppose } 8 \mid 5^{2k} + 7. \therefore \exists x \text{ s.t. } 8x = 5^{2k} + 7$$

$$\begin{aligned} 5^{2(k+1)} + 7 &= 5^2 \cdot 5^{2k} + 7 \\ &= 5^2(5^{2k} + 7) - 5^2 \cdot 7 + 7 \end{aligned}$$

$$= 5^2(8x) - 7(5^2 - 1)$$

$$= 5^2(8x) - 7(24)$$

$$= 8x(25) - 8(7 \cdot 3)$$

$$= 8[25x - 21]$$

$$\therefore 8(5^{2(k+1)})$$

$$(5) 15 | 2^{4n} - 1$$

$$n=1: 15 = 2^4 - 1 = 16 - 1$$

Assume  $15 | (2^{4k} - 1)$ .  $\therefore \exists x \text{ s.t. } 15x = 2^{4k} - 1$

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

$$= 2^4(2^{4k} - 1) + (2^4 - 1)$$

$$= 2^4(15x) + 15 = 15(x2^4 + 1)$$

$$\therefore 15 | 2^{4(k+1)} - 1$$

$$(c) 5 | (3^{3n+1} + 2^{n+1})$$

$$n=1 : 3^{3+1} + 2^2 = 81 + 4 = 85, \text{ and } 5 | 85$$

$$\text{Suppose } 5 | (3^{3k+1} + 2^{k+1})$$

$$\therefore 3 \times S.T. \quad \overline{Sx} = 3^{3k+1} + 2^{k+1}$$

$$3^{3(k+1)+1} + 2^{k+2} = 3^{3k+4} + 2^{k+2}$$

$$= 3^3 \cdot 3^{3k+1} + 2 \cdot 2^{k+1} + 3^3 \cdot 2^{k+1} - 3^3 \cdot 2^{k+1}$$

$$= 3^3 (3^{3k+1} + 2^{k+1}) - 2^{k+1} (3^3 - 2)$$

$$= 3^3 (\overline{Sx}) - 2^{k+1} (25)$$

$$= S(x 3^3 - 5 \cdot 2^{k+1})$$

$\therefore$  true for  $k+1$

$$(d) 21 \mid 4^{n+1} + 5^{2n-1}$$

$$n=1: 4^2 + 5^1 = 21$$

Suppose for  $k$   $21 \mid 4^{k+1} + 5^{2k-1}$

$$\therefore 3 \times S.T. \quad 21x = 4^{k+1} + 5^{2k-1}$$

$$4^{k+2} + 5^{2(k+1)-1} = 4^{k+2} + 5^{2k+1}$$

$$= 4 \cdot 4^{k+1} + 5^2 \cdot 5^{-2k-1} + 4 \cdot 5^{2k-1} - 4 \cdot 5^{2k-1}$$

$$= 4 \left( 4^{k+1} + 5^{2k-1} \right) + 21 \left( 5^{2k-1} \right)$$

$$= 4 (24_x) + 21 (5^{2k-1})$$

$\therefore$  true for  $k+1$

(e)  $24 \mid 2 \cdot 7^n + 3 \cdot 5^n - 5$

$$\text{for } n=1: 2 \cdot 7^1 + 3 \cdot 5^1 - 5 = 14 + 15 - 5 = 24$$

Suppose  $24 \mid 2 \cdot 7^k + 3 \cdot 5^k - 5$

$$\therefore 3 \times 5 \cdot 5 \mid 24_x = 2 \cdot 7^k + 3 \cdot 5^k - 5$$

$$\therefore 2 \cdot 7^{k+1} + 3 \cdot 5^{k+1} - 5 = 7(2 \cdot 7^k) + 5(3 \cdot 5^k) - 5$$

$$= 2(2 \cdot 7^k) + 5(2 \cdot 7^k) + 5(3 \cdot 5^k) - 5 + 5 \cdot 5 - 5 \cdot 5$$

$$= 5(2 \cdot 7^k + 3 \cdot 5^k - 5) + 2(2 \cdot 7^k) - 5 + 5 \cdot 5$$

$$= 5(24_x) + 2(2 \cdot 7^k) + 20 \quad [\text{Eq. 1}]$$

But  $24 \mid 4 \cdot 7^k + 20$

pf:  $k=1: 4 \cdot 7 + 20 = 48 = 24 \cdot 2$

Suppose  $24 \mid 4 \cdot 7^s + 20$

$$\therefore \exists y \text{ s.t. } 24y = 4 \cdot 7^s + 20$$

$$\therefore 4 \cdot 7^{s+1} + 20 = 7(4 \cdot 7^s) + 20$$

$$= 7(4 \cdot 7^s + 20) + 20 - 140$$

$$= 7(24y) - 24 \cdot 5$$

$$\therefore \exists q \text{ s.t. } 24q = 4 \cdot 7^k + 20$$

$$\therefore [Eq. 1] = \bar{s}(24x) + 24q$$

$\therefore$  True for  $k+1$

5. For integer  $a$ , one of  $a, a+2, a+4$  is divisible by 3.

Pf: (a) Suppose  $3 \nmid a$ .  $\therefore a = 3q_1 + 1$  or  $a = 3q_2 + 2$

$3q_1 + 1$ : Then  $a+2 = 3q_1 + 3 = 3(q_1 + 1)$ ,  
so  $3 \mid a+2$

$3q_2 + 2$ : Then  $a+4 = 3q_2 + 6 = 3(q_2 + 2)$   
so  $3 \mid a+4$

(b) Suppose  $3 \nmid a+2$ .  $\therefore a+2 = 3q_1 + 1$  or  
 $a+2 = 3q_2 + 2$

$$3q_1 + 1 : \therefore a = 3q_1 - 1, \text{ so } a+4 = 3q_1 + 3$$

$\therefore 3 \nmid a+4$

$$3q_2 + 2 : \therefore a = 3q_2, \text{ so } 3 \mid a$$

(C) Suppose  $3 \nmid a+4$ .  $\therefore a+4 = 3q_1 + 1$  or  $3q_2 + 2$

$$3q_1 + 1 : \therefore a = 3q_1 - 3, \text{ so } 3 \mid a$$

$$3q_2 + 2 : \therefore a = 3q_2 - 2, \text{ so } a+2 = 3q_2,$$

so  $3 \mid a+2$

C. (a).  $2 \mid a(a+1)$

Pf: By Div. Alg.  $a = 2g$  or  $a = 2g+1$

$$2g : \text{Then } a(a+1) = 2g(2g+1)$$

$$\therefore 2 \mid a(a+1)$$

$$2g+1 : \text{Then } a(a+1) = (2g+1)(2g+2)$$

$$= 2(2g+1)(g+1)$$

$\therefore 2 \mid a(a+1)$

$$3 \mid a(a+1)(a+2) \quad a = 3g, 3g+1, \text{ or } 3g+2$$

$$3g : a(a+1)(a+2) = 3g(3g+1)(3g+2)$$

$\therefore 3 \mid a(a+1)(a+2)$

$$3g+1: a(a+1)(a+2) = (3g+1)(3g+2)(3g+3) \\ = 3(3g+1)(3g+2)(g+1) \\ \therefore 3 \mid a(a+1)(a+2)$$

$$3g+2: a(a+1)(a+2) = (3g+2)(3g+3)(3g+4) \\ = 3(3g+2)(g+1)(3g+4) \\ \therefore 3 \mid a(a+1)(a+2)$$

$$(6) 3 \mid a(2a^2+7)$$

$$\text{Pf: } a = 3g, 3g+1, 3g+2$$

$$3g: a(2a^2+7) = 3g(\quad) \therefore 3 \mid a(2a^2+7)$$

$$3g+1: a(2a^2+7) = (3g+1)[2(3g+1)^2 + 7] \\ = (3g+1)[2(9g^2 + 6g + 1) + 7]$$

$$= (3g+1)(18g^2 + 12g + 9)$$

$$= 3(3g+1)(6g^2 + 4g + 3)$$

$$\therefore 3 \mid a(2a^2+7)$$

$$3g+2: a(2a^2+7) = (3g+2)[2(3g+2)^2 + 7]$$

$$\begin{aligned}
 &= (3q+2) [2(9q^2 + 12q + 4) + 7] \\
 &= (3q+2)(18q^2 + 24q + 15) \\
 &= 3(3q+2)(6q^2 + 8q + 5) \\
 \therefore 3 &\mid a(2a^2 + 7)
 \end{aligned}$$

(C)  $a$  is odd, Then  $32 \mid (a^2 + 3)(a^2 + 7)$

Pf:  $\exists q$  s.t.  $a = 2q + 1$

$$\begin{aligned}
 \therefore (a^2 + 3)(a^2 + 7) &= (4q^2 + 4q + 4)(4q^2 + 4q + 8) \\
 &= 16q^4 + 16q^3 + 32q^2 \\
 &\quad + 16q^3 + 16q^2 + 32q \\
 &\quad + 16q^2 + 16q + 32 \\
 &= 16q^4 + 32q^3 + 64q^2 + 48q + 32
 \end{aligned}$$

If  $q$  is even, Then  $q = 2x$ ,

$$\begin{aligned}
 \text{so } 16q^4 &= 16(2x)^4 = 32 \cdot 2^3 \cdot x^4 \\
 \text{and } 48q &= 96x
 \end{aligned}$$

$\therefore$  all terms divisible by 32

If  $a$  is odd,  $a = 2x + 1$ ,

$$\therefore 16a^4 + 32a^3 + 64a^2 + 48a + 32$$

$$= 16(2x+1)^4 + 32a^3 + 64a^2 + 48(2x+1) + 32$$

$$= 16(2x+1)^4 + 32a^3 + 64a^2 + 96x + 80$$

$$= 16 \left( 2^4 x^4 + \binom{4}{1} 2^3 x^3 + \binom{4}{2} 2^2 x^2 + \binom{4}{3} 2x + 1 \right) \\ + 32a^3 + 64a^2 + 76x + 80$$

$$= 32 \left( 2^3 x^4 + \binom{4}{1} 2^2 x^3 + \binom{4}{2} 2x^2 + \binom{4}{3} x \right) \\ + 32a^3 + 64a^2 + 96x + 96$$

So all terms divisible by 32.

7. If  $a, b$  are odd, Then  $16|a^4 + b^4 - 2$

Pf: Let  $a = 2r + 1, b = 2s + 1$

$$a^4 = (2r+1)^4 = 2^4 r^4 + \binom{4}{1} 2^3 r^3 + \binom{4}{2} 2^2 r^2 + \binom{4}{3} 2r + 1$$

$$= 16r^4 + 32r^3 + 24r^2 + 8r + 1$$

$$\therefore a^4 + b^4 - 2 = 16r^4 + 32r^3 + 24r^2 + 8r + \\ 16s^4 + 32s^3 + 24s^2 + 8s$$

All terms divisible by 16 except perhaps  
 $24r^2 + 8r, 24s^2 + 8s$

But if  $r$  is even, Then  $r = 2w$  for  
some  $w$ , and  $\therefore 24r^2 + 8r = 96w^2 + 16w$ ,  
which is divisible by 16.

If  $r$  is odd, Then  $r = 2w+1$ , some  $w$ .  
 $\therefore 24r^2 + 8r = 24(2w+1)^2 + 8(2w+1)$   
 $= 96w^2 + 96w + 24 + 16w + 8$   
 $= 96w^2 + 96w + 16w + 32$ ,  
which is divisible by 16.

Similarly for  $24s^2 + 8s$

$$\therefore 16 \mid a^4 + b^4 - 2$$

Q.(a) If  $a, b$  are odd, Then  $a^2 + b^2 \neq c^2$  for some integer  $c$ .

Pf: Let  $a = 2r+1, b = 2s+1$

$$\begin{aligned} \therefore a^2 + b^2 &= 4r^2 + 4r + 1 + 4s^2 + 4s + 1 \\ &= 4(K) + 2 = 2(K') \end{aligned}$$

$\therefore$  if  $c$  exists, it must be even

Let  $c = 2w$ , some unique  $w$ .

$$\therefore c^2 = 4w^2$$

By Div. Alg.,  $a^2 + b^2 = 4q + r$ , where  
 $q$  and  $r$  are unique. From above,  
 $a^2 + b^2 = 4K + 2$   
if  $a^2 + b^2 = c^2$ , Then  $a^2 + b^2 = 4w^2$ ,  
which means " $q$ " and " $r$ " are not  
unique.

$$\therefore a^2 + b^2 \neq c^2 \text{ if } a, b \text{ are odd}$$

(3) Let  $a, b, c, d$  be four consecutive integers.  
Then  $a \cdot b \cdot c \cdot d = e^2 - 1$ , for some  $e$ .

Pf: A few examples show that the product  
of the 1st & last terms is close to  
the product of the middle two terms,  
and that the perfect square in question  
is the average of the two products.  
An average exists because the two  
products are even.

$$\therefore a(a+1)(a+2)(a+3) = \left[ \frac{a(a+3) + (a+1)(a+2)}{2} \right]^2 - 1$$

Suppose  $a$  is even. Then  $a = 2n$

$$\begin{aligned}
\therefore a(a+1)(a+2)(a+3) &= 2n(2n+1)(2n+2)(2n+3) \\
&= (4n^2 + 2n)(4n^2 + 10n + 6) \\
&= 16n^4 + 40n^3 + 24n^2 \\
&\quad + 8n^3 + 20n^2 + 12n \\
&= 16n^4 + 48n^3 + 44n^2 + 12n \\
&= \left[ \frac{2n(2n+3)}{2} + (2n+1)(2n+2) \right]^2 - 1 \\
&= \left[ \frac{4n^2 + 6n + 4n^2 + 6n + 2}{2} \right]^2 - 1 \\
&= \left[ \frac{8n^2 + 12n + 2}{2} \right]^2 - 1 \\
&= (4n^2 + 6n + 1)^2 - 1 \\
&= (4n^2 + 6n + 1)(4n^2 + 6n + 1) - 1 \\
&= 16n^4 + 24n^3 + 4n^2 \\
&\quad + 24n^3 + 36n^2 + 6n \\
&\quad + 4n^2 + 6n + 1 - 1 \\
&= 16n^4 + 48n^3 + 44n^2 + 12n \quad \checkmark
\end{aligned}$$

If  $a$  is odd, Then  $a = 2n+1$

$$\begin{aligned}
\therefore a(a+1)(a+2)(a+3) &= (2n+1)(2n+2)(2n+3)(2n+4) \\
&= (4n^2 + 6n + 2)(4n^2 + 14n + 12) \\
&= 16n^4 + 56n^3 + 48n^2 \\
&\quad + 24n^3 + 84n^2 + 72n \\
&\quad + 8n^2 + 28n + 24
\end{aligned}$$

$$\begin{aligned}
&= 16n^4 + 80n^3 + 140n^2 + 100n + 24 \\
&\left[ \frac{a(a+3)}{2} + (a+1)(a+2) \right]^2 - 1 = \\
&\left[ \frac{(2n+1)(2n+4) + (2n+2)(2n+3)}{2} \right]^2 - 1 \\
&= \left[ \frac{4n^2 + 10n + 4 + 4n^2 + 10n + 6}{2} \right]^2 - 1 \\
&= (4n^2 + 10n + 5)^2 - 1 \\
&= (4n^2 + 10n + 5)(4n^2 + 10n + 5) - 1 \\
&= 16n^4 + 40n^3 + 20n^2 \\
&\quad + 40n^3 + 100n^2 + 50n \\
&\quad + 20n^2 + 50n + 25 - 1 \\
&= 16n^4 + 80n^3 + 140n^2 + 100n + 24 \quad \checkmark
\end{aligned}$$

9.  $(a+1)^3 - a^3$  is never divisible by 2

Pf: Suppose  $a$  is even.  $\therefore a = 2n$

$$\therefore (a+1)^3 - a^3 = (2n+1)^3 - (2n)^3$$

$$= 8n^3 + \binom{3}{1} 4n^2 + \binom{3}{2} 2n + 1 - 8n^3$$

$$= 12n^2 + 6n + 1$$

$$= 2(k) + 1, \text{ so } (a+1)^3 - a^3 \text{ is odd}$$

Suppose  $a$  is odd.  $\therefore a = 2n+1$

$$\therefore (a+1)^3 - a^3 = (2n+1+1)^3 - (2n+1)^3$$

$$= (2n+1)^3 + \binom{3}{1}(2n+1)^2 + \binom{3}{2}(2n+1) + 1 - (2n+1)^3$$

$$= (2n+1) \left[ 3(2n+1) + 3 \right] + 1$$

$$= (2n+1)(6n+6) + 1$$

$$= 2 \left[ (2n+1)(3n+3) \right] + 1$$

$$= 2(k) + 1, \text{ so } (a+1)^3 - a^3 \text{ is odd.}$$

$$10.(a) a \neq 0, \gcd(a, 0) = |a|$$

Pf: From Th. 2.2 (p. 21), we know that  
 $a|0$  and  $a|a$ .  $\therefore |a|$  is a common divisor.

Let  $c$  be another common divisor.

$\therefore c|a$  and  $\therefore |c| \leq |a|$  by Th. 2.2  
 $\therefore |a|$  is gcd

(b)  $a \neq 0$ ,  $\gcd(a, a) = |a|$

Pf: By Th. 2.2,  $a/a$ .  $\therefore |a|$  is a common divisor.

Let  $c$  be another common divisor.  
 $\therefore c/a$ , and  $\therefore |c| \leq |a|$ , by Th. 2.2  
 $\therefore |a|$  is gcd.

(c)  $a \neq 0$ ,  $\gcd(a, 1) = 1$

Pf: By Th. 2.2,  $1/a, 1/1$ .  $\therefore 1$  is a common divisor.

Let  $c$  be another common divisor.  
 $\therefore c/1$ , and  $\therefore |c| \leq 1$  (Th. 2.2)  
 $\therefore 1$  is gcd.

11.  $\gcd(a, b) = \gcd(-a, b) = \gcd(a, -b) = \gcd(-a, -b)$

Pf: Let  $x$  by the gcd of any one pair.

Since  $x|y \Leftrightarrow x|(-y)$ , then  
 $x$  is a common divisor of any other pair.

Let  $c$  be another common divisor.

Since  $c|a \Leftrightarrow c|(-a)$  and  $c|b \Leftrightarrow c|(-b)$ ,

Then  $c|x$  by Th. 2.6.  $\therefore |c| \leq |x|$ ,  
 $\therefore x$  is the gcd of the other pair.

12.  $n=0$ ,  $a$  any integer,  $\gcd(a, a+n) \mid n$

Pf: Let  $d = \gcd(a, a+n)$

$\therefore \exists x, y$  s.t.  $a = dx$ ,  $a+n = dy$

$\therefore dx + n = dy$ ,  $n = d(y-x)$ ,  $\therefore d \mid n$

And by Th. 2.2,  $d \mid 1 \iff d = \pm 1$ .

$\therefore \gcd(a, a+1) = 1$ .

13. (a). (1) Let  $x, y$  be any integers and let  $d = \gcd(a, b)$

$\therefore \exists m, n$  s.t.  $a = dm$  and  $b = dn$

$\therefore c = ax + by = dm x + dn y = d(mx + ny)$ .

$\therefore d \mid c$

(2) Suppose  $\gcd(a, b) \mid c$ . Let  $d = \gcd(a, b)$ .

$\therefore \exists x_0, y_0$  s.t.  $d = ax_0 + by_0$

But  $d \mid c$ , so that  $c = dp$ , for some  $p$

$\therefore c = dp = (ax_0 + by_0)p = ax_0 p + by_0 p$

$\therefore \text{Let } x = x_0 p, y = y_0 p$

(b) Let  $x, y$  be s.t.  $ax + by = \gcd(a, b)$ . Then  $\gcd(xy) = 1$

Pf: Let  $d = \gcd(a, b)$ .  $\therefore ax + by = d$   
 Since  $d|a$  and  $d|b$ , Then  $\frac{a}{d}$  and  $\frac{b}{d}$  are  
 integers.  $\therefore \frac{a}{d}x + \frac{b}{d}y = 1$ ,  
 and  $\therefore x$  and  $y$  are relatively prime.  
 $\therefore \gcd(x, y) = 1$ .

14. (a) Since  $9(2a+1) + (-2)(9a+4) = 1$ , Then  
 by Th. 2.4  $2a+1$  and  $9a+4$  are relatively  
 prime, so  $\gcd(2a+1, 9a+4) = 1$

$$(b) (-7)(5a+2) + 5(7a+3) = 1$$

$$\therefore \gcd(5a+2, 7a+3) = 1$$

(c)  $\gcd(3a, 3a+2) \mid 2$  by problem 12

$\therefore \gcd = 1$  or  $2$ . But  $a$  odd  $\Rightarrow 3a$  is odd.  
 $\therefore 2 \nmid 3a$ .  $\therefore \gcd = 1$

15  $\gcd(2a-3b, 4a-5b) \mid 6$

Pf: Let  $d = \gcd(2a-3b, 4a-5b)$

For all  $x, y$ , by Corollary on p. 23,  
 $x(2a-3b) + y(4a-5b)$  is a multiple of  $d$ .

$$\begin{aligned}\therefore \exists n \text{ s.t. } d_n &= (-2)(2a-3\beta) + (1)(4a-5\beta) \\ &= 5\end{aligned}$$

$$\therefore d \mid 5$$

$$\begin{aligned}\text{Now let } \beta = -1. \therefore \gcd(2a+3, 4a+5) \mid (-1) \\ \therefore \gcd = 1.\end{aligned}$$

16. If  $a$  is odd,  $12 \mid a^2 + (a+2)^2 + (a+4)^2 + 1$

$$\text{Pf: Let } a = 2n+1$$

$$\therefore (2n+1)^2 + (2n+3)^2 + (2n+5)^2 + 1$$

$$= 4n^2 + 4n + 1$$

$$+ 4n^2 + 12n + 9$$

$$+ 4n^2 + 20n + 25 + 1$$

$$= 12n^2 + 36n + 36 = 12(n^2 + 3n + 3)$$

17. For all  $n \geq 0$ ,  $(3n)! / (3!)^n$  is an integer

$$\text{Pf: } n=1 : 3! / 3! = 1$$

$k \Rightarrow k+1$ : Suppose  $(3k)! / (3!)^k = R$  is an integer

$$\therefore [3(k+1)]! / (3!)^{k+1}$$

$$= (3k+3)! / (3!)^k \cdot (3!)$$

$$= \frac{(3k+1)(3k+2)(3k+1)(3k)!}{3 \cdot 2 \cdot 1 \cdot (3!)^k}$$

$$= \frac{3(k+1)(3k+2)(3k+1)}{3 \cdot 2} \cdot R$$

$$= \frac{(k+1)(3k+2)(3k+1)}{2} \cdot R$$

If  $k$  is odd, Then  $k+1$  is even,  
 $\text{so } (k+1)/2 = x, \text{ some integer } x.$

If  $k$  is even, Then  $3k+2$  is even, so  
 $(3k+2)/2 = x, \text{ some integer } x.$

$\therefore$  entire expression is an integer.

18. (a).  $G \mid a(a+1)(a+2)$

Pf:  $G = 3 \cdot 2$ , and  $\gcd(2, 3) = 1$  (Problem 12).

Let  $R = a(a+1)(a+2)$

If  $a$  is even, Then  $2 \mid a, \therefore 2 \mid R$

If  $a$  is odd, Then  $2 \mid (a+1), \therefore 2 \mid R$

Let  $a = 3q + r$

if  $r=0$ , Then  $3|a$ ,  $\therefore 3|R$

if  $r=1$ , Then  $a+2 = 3q+3$ ,  $3|a+2$ ,  $3|R$

if  $r=2$ , Then  $a+1 = 3q+3$ ,  $3|a+1$ ,  $3|R$

$\therefore 3|R$  and  $2|R$ , and by Corollary 2  
on p. 24,  $3 \cdot 2 | R$   
 $\therefore 6 | a(a+1)(a+2)$

(b)  $24 | a(a+1)(a+2)(a+3)$

Pf:  $n=1 : 1 \cdot 2 \cdot 3 \cdot 4 = 24$

$k \Rightarrow k+1 : \text{Suppose } 24 | k(k+1)(k+2)(k+3)$   
 $\therefore 24p = k(k+1)(k+2)(k+3)$ , some  $p$

$$\begin{aligned}\therefore (k+1)(k+2)(k+3)(k+4) &= \\ k(k+1)(k+2)(k+3) + 4(k+1)(k+2)(k+3) &= \\ 24p + 4(k+1)(k+2)(k+3)\end{aligned}$$

But by (a),  $(k+1)(k+2)(k+3) = 6q$   
for some  $q$ .

$$\therefore (k+1)(k+2)(k+3)(k+4) = 24p + 24q$$

$$\therefore 24 | (k+1)(k+2)(k+3)(k+4)$$

$$(C) \quad 120 \mid a(a+1)(a+2)(a+3)(a+4)$$

$$Pf: n=1 : 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 = 120$$

$$K \Rightarrow K+1 : Suppose 120 \mid K(K+1)(K+2)(K+3)(K+4)$$

$$\therefore \exists p \text{ s.t. } 120p = K(K+1)(K+2)(K+3)(K+4)$$

$$\text{But } (K+1)(K+2)(K+3)(K+4)(K+5) =$$

$$K(K+1)(K+2)(K+3)(K+4) + 5(K+1)(K+2)(K+3)(K+4)$$

$$= 120p + 5 \cdot 24q, \text{ for some } q \\ \text{by (5) above.}$$

$$= 120(p+q)$$

$$\therefore 120 \mid (K+1)(K+2)(K+3)(K+4)(K+5)$$

$$19. (a) \quad G \mid a(a^2+11)$$

Pf: Let  $a = 6q + r$ , where  $0 \leq r < 6$   
 Consider each case for  $r$

$$r=0: a(a^2+11) = 6q \left[ (6q)^2 + 11 \right]. \therefore G \mid a(a^2+11)$$

$$\begin{aligned}
 r=1: a(a^2+11) &= (6g+1)(6g+1)^2 + (6g+1)11 \\
 &= 6g^3 + \binom{3}{1} (6g)^2 + \binom{3}{2} 6g + \binom{3}{0} + (6g)11 + 11 \\
 &= 6[\quad] + \binom{3}{0} + 11 \\
 &= 6[\quad] + 12 = 6\{\quad\} \\
 r=2: a(a^2+11) &= (6g+2)^3 + (6g+2)\cdot 11 \\
 &= 6[\quad] + \binom{3}{0} 2^3 + (6g)(11) + 22 \\
 &= 6[\quad] + 30 = 6[\quad]
 \end{aligned}$$

$$\begin{aligned}
 r=3: a(a^2+11) &= (6g+3)^3 + (6g+3)11 \\
 &= 6[\quad] + \binom{3}{0} \cdot 3^3 + 33 \\
 &= 6[\quad] + 27 + 33 = 6[\quad] + 60 \\
 &= 6[\quad]
 \end{aligned}$$

$$\begin{aligned}
 r=4: a(a^2+11) &= (6g+4)^3 + (6g+4)11 \\
 &= 6[\quad] + \binom{3}{0} 4^3 + 44 \\
 &= 6[\quad] + 64 + 44 = 6[\quad] + 108
 \end{aligned}$$

$$= 6[ ] + 6 \cdot 18 = 6[ ]$$

$$r=4: a(a^2+1) = (6g+5)^3 + (6g+5) \mid 11$$

$$= 6[ ] + \binom{3}{0} 5^3 + 55$$

$$= 6[ ] + 125 + 55 = 6[ ] + 6 \cdot 30$$

$$= 6[ ]$$

(6)  $a$  is odd, Then  $24 \mid a(a^2-1)$

Pf: First, show  $a^2$  is of form  $8K+1$

Let  $a = 4g+r$ .  $\therefore r=1$  or  $3$  since  
 $a$  is odd.

$$\therefore a^2 = 16g^2 + 8g + 1 = 8K + 1$$

$$\text{or } a^2 = 16g^2 + 24g + 9 = 8K' + 1$$

So,  $a(a^2-1) = a8K$ , for some  $K$ .

$$\therefore 8 \mid a(a^2-1)$$

By #18 above,  $6 \mid (a-1)(a)(a+1)$ , so

$$3 \mid (a-1)(a)(a+1) \equiv 3 \mid a(a^2-1)$$

Since  $\gcd(3, 8) = 1$ ,  $\therefore 24 \mid a(a^2 - 1)$   
by Corollary 2 on p. 24

$$(c) a, b \text{ odd} \Rightarrow 8 \mid (a^2 - b^2)$$

Pf: By (b) above,  $a^2$  is of form  $8k + 1$   
and  $b^2$  is of form  $8k' + 1$

$$\therefore a^2 - b^2 = 8k + 1 - (8k' + 1)$$

$$\therefore 8 \mid (a^2 - b^2) = 8(k + k'), \text{ some } k, k'$$

$$(d) 2 \nmid a, 3 \nmid a \Rightarrow 24 \mid (a^2 + 23)$$

Pf: Let  $a = 12q + r$ ,  $0 \leq r < 12$   
 $r$  can only be  $1, 3, 5, 7, 9, 11$  since  $2 \nmid a$ ,  
and since  $3 \nmid a$ ,  $r \neq 3$  or  $9$ .  
 $\therefore r$  can only be  $1, 5, 7, 11$ .

$$\therefore a^2 + 23 = (12q + r)^2 + 23$$

$$= 144q^2 + 24qr + r^2 + 23$$

$$= 24(6)q^2 + 24qr + r^2 + 23$$

$$= 24 \{ \} + r^2 + 23$$

$$r=1 : r^2 + 23 = 24$$

$$r=5 : r^2 + 23 = 48 = 24(2)$$

$$r=7 : r^2 + 23 = 72 = 24(3)$$

$$r=11 : r^2 + 23 = 144 = 24(6)$$

$$\begin{aligned}\therefore a^2 + 23 &= 24 \{ \} + r^2 + 23 \\ &= 24 \{ \} + 24k, \text{ some } k\end{aligned}$$

$$\therefore 24 \mid (a^2 + 23)$$

$$(c) 360 \mid a^2(a^2 - 1)(a^2 - 4)$$

$$\text{Pf: } a^2(a^2 - 1)(a^2 - 4) = a^2(a+1)(a-1)(a+2)(a-2)$$

$$= (a-2)(a-1)(a)(a+1)(a+2)(a)$$

$360 = 5 \cdot 9 \cdot 8$ , and 5, 9, 8 are relatively prime.

By #18,  $(a-2)(a-1)(a)(a+1)(a+2)$  is

divisible by 24 and 120.  $\therefore$  it is divisible by 8 and 5.

Also,  $(a-2)(a-1)a$  and  $a(a+1)(a+2)$  are both divisible by 6 and so are both divisible by 3, and  $\therefore$  the entire product is divisible by 9.

$\therefore$  Entire product divisible by 360  
by Corollary 2, p. 24

20. (a)  $\gcd(a, b) = 1$ ,  $\gcd(a, c) = 1$ , Then  $\gcd(a, bc) = 1$

Pf:  $l = ax + by = au + cv$  for some  $x, y, u, v$

$$\begin{aligned}\therefore l &= (ax + by)(au + cv) = a^2xy + abyu + a^2xu + bcyv \\ &= a(axy + byu + axu) + bcyv \\ &= aK_1 + bK_2\end{aligned}$$

$\therefore a, bc$  relatively prime.

(b)  $\gcd(a, b) = 1$ ,  $c/a$ , Then  $\gcd(b, c) = 1$

Pf:  $\exists x, y$  s.t.  $ax + by = 1$ , and  $\exists n$  s.t.  $cn = a$

$$\therefore cnx + by = 1 \Rightarrow \gcd(c, b) = 1$$

(c)  $\gcd(a, b) = 1$ , then  $\gcd(ac, b) = \gcd(c, b)$

Pf: Let  $d = \gcd(c, b)$ . Need to show

$$(1) d \mid ac \quad (d \mid b \text{ by def.})$$

(2) If  $k \mid ac$  and  $k \mid b$ , then  $k \mid d$

(1): Since  $d \mid c$ ,  $\exists n \text{ s.t. } dn = c$ , so  
 $d(na) = ca$ ,  $\Rightarrow d \mid ca$

(2)  $\exists x, y \text{ s.t. } d = cx + by$

Since  $k \mid b$ , Then  $\exists n \text{ s.t. } kn = b$

$$\therefore d = cx + kny$$

Since  $\gcd(a, b) = 1$ ,  $\exists p, q \text{ s.t. } ap + bq = 1$

$$\therefore apc + bq_c = c$$

$$\therefore d = (apc + bq_c)x + kny$$

$$= acpx + knqcx + kny$$

But  $k \mid ac \Rightarrow \exists r \text{ s.t. } kr = ac$

$$\begin{aligned}d &= krpx + knqx + kny \\&= k(rpx + nqx + ny)\end{aligned}$$

$$\therefore K \mid d$$

$\therefore$  By Theorem 2.6,  $\gcd(c, b) = \gcd(ac, b)$

(d)  $\gcd(a, b) = 1, c \mid a+b \Rightarrow \gcd(a, c) = \gcd(b, c) = 1$

Pf,  $\gcd(a, b) = 1 \Rightarrow \exists x, y \text{ s.t. } ax + by = 1$

$c \mid a+b \Rightarrow \exists n \text{ s.t. } cn = a+b$

$$\therefore cn - b = a$$

$$\therefore (cn - b)x + by = 1$$

$$cnx - bx + by = 1,$$

$$\text{so, } cnx + b(y-x) = 1 \Rightarrow \gcd(c, b) = 1$$

Similarly,  $cn - a = b$ , so

$$ax + (cn-a)x = 1$$

$$ax + cnx - ay = 1,$$

$$\text{so, } a(x-y) + cnx = 1 \Rightarrow \gcd(a, c) = 1$$

(c)  $\gcd(a, b) = 1$ ,  $d \mid ac$ ,  $d \mid bc$ , Then  $d \mid c$

Pf:  $\exists x, y$  s.t.  $ax + by = 1$ .  $\therefore ax + by = c$

But  $ac = d_n$  and  $bc = d_m$  for some  $n, m$

$$\therefore d_nx + d_my = c, d(nx + my) = c$$

$$\therefore d \mid c$$

(f)  $\gcd(a, b) = 1$ , Then  $\gcd(a^2, b^2) = 1$

Pf: From (c) above, let  $c = a$

$$\therefore \gcd(a, b) = 1 \Rightarrow \gcd(a^2, b^2) = \gcd(a, b) = 1$$

$$\text{Also, } \gcd(a, b) = \gcd(b, a) = \gcd(b^2, a)$$

$$= \gcd(b, a) = 1$$

$$\text{So, } \gcd(a^2, b^2) = \gcd(a, b^2) = 1$$

Now apply (c) again to get

$$\gcd(a \cdot a, b^2) = \gcd(a, b^2) = 1$$

$$\therefore \gcd(a^2, b^2) = 1$$

$$21. (a). d \mid n \Rightarrow 2^d - 1 \mid 2^n - 1$$

Pf: From Problems 1.1, #3,

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

$$\therefore 2^n - 1 = 2^{n-1} + 2^{n-2} + \dots + 2 + 1 \quad (\text{n terms})$$

$$2^d - 1 = 2^{d-1} + 2^{d-2} + \dots + 2 + 1 \quad (\text{d terms})$$

Since  $d \mid n$ ,  $\exists x$  s.t.  $dx = n$

$$\therefore 2^n - 1 = 2^{dx} - 1 = (2^d)^x - 1$$

$$= (2^d - 1)(2^{d(x-1)} + 2^{d(x-2)} + \dots + 2^d + 1)$$

$$\therefore 2^d - 1 \mid 2^n - 1$$

Could also look at this explicitly

$$\frac{2^n - 1}{2^d - 1} = \frac{n \text{ terms}}{d \text{ terms}} = \frac{dx \text{ terms}}{d \text{ terms}}$$

$$= \frac{(\underbrace{\quad}_{d \text{ terms}}) + (\underbrace{\quad}_{d \text{ terms}}) + \dots + (\underbrace{\quad}_{d \text{ terms}})}{(d \text{ terms})}$$

$$= 2^{d(x-1)} + 2^{d(x-2)} + \dots + 2^d + 1$$

(6)  $31 = 2^5 - 1$ . Since  $5 \mid 35$ ,  $2^5 - 1 \mid 2^{35} - 1$

$127 = 2^7 - 1$ , and  $7 \mid 35$ .  $\therefore 2^7 - 1 \mid 2^{35} - 1$

22. What values of  $n$  does  $t_n \mid t_1 + t_2 + \dots + t_n$

From Problems 1.3, #3,

$$t_1 + t_2 + \dots + t_n = \frac{n(n+1)(n+2)}{6}$$

and from Problems 1.3, #1(a),  $t_n = n \frac{(n+1)}{2}$

$$\therefore \frac{\frac{n(n+1)(n+2)}{6}}{\frac{n(n+1)}{2}} = \frac{n+2}{3}$$

$\therefore t_n$  divides  $t_1 + \dots + t_n$  when  $\frac{n+2}{3}$  is an

integer, or  $n = 1, 4, 7, 10, \dots$

23. If  $a \mid bc$ , show  $a \mid \gcd(a, c)\gcd(b, c)$

Pf: Let  $d_1 = \gcd(a, b)$ ,  $d_2 = \gcd(a, c)$

$\therefore \exists x, y, u, v$  s.t.  $d_1 = ax + by$

$$d_2 = au + cv$$

and  $\exists n$  s.t.  $an = bc$

$$\therefore d_1 d_2 = (ax + by)(au + cv)$$

$$= a^2 xu + acxv + abyu + bcyv$$

$$= a(axu + cxv + bry) + anyv$$

$$= a(axu + cxv + bry + nyv)$$

$$\therefore a \mid d_1 d_2$$

## 2.3 The Euclidean Algorithm

Note Title

11/1/2004

1. (a)  $\gcd(143, 227)$

$$227 = 1 \cdot 143 + 84$$

$$143 = 1 \cdot 84 + 59$$

$$84 = 1 \cdot 59 + 25$$

$$59 = 2 \cdot 25 + 9$$

$$25 = 2 \cdot 9 + 7$$

$$9 = 1 \cdot 7 + 2$$

$$7 = 3 \cdot 2 + 1$$

$$2 = 2 \cdot 1 + 0$$

$$\therefore \gcd(143, 227) = 1$$

(b)  $\gcd(306, 657)$

$$657 = 2 \cdot 306 + 45$$

$$306 = 6 \cdot 45 + 36$$

$$45 = 1 \cdot 36 + 9$$

$$36 = 4 \cdot 9 + 0$$

$$\therefore \gcd(306, 657) = 9$$

(c)  $\gcd(272, 1479)$

$$1479 = 5 \cdot 272 + 119$$

$$272 = 2 \cdot 119 + 34$$

$$119 = 3 \cdot 34 + 17$$

$$34 = 2 \cdot 17 + 0$$

$$\therefore \gcd(272, 1479) = 17$$

$$2. (a) \gcd(57, 72) = 56x + 72y$$

$$72 = 1 \cdot 56 + 16$$

$$56 = 3 \cdot 16 + 8$$

$$16 = 2 \cdot 8 + 0 \quad \gcd = 8$$

$$\begin{aligned} \therefore 8 &= 56 - 3 \cdot 16 \\ &= 56 - 3(72 - 56) \\ &= (4)56 - (3)72 \end{aligned}$$

$$(b) \gcd(24, 138) = 24x + 138y$$

$$138 = 5 \cdot 24 + 18$$

$$24 = 1 \cdot 18 + 6$$

$$18 = 3 \cdot 6 + 0 \quad \gcd = 6$$

$$\begin{aligned} \therefore 6 &= 24 - 18 \\ &= 24 - (138 - 5 \cdot 24) \\ &= (6)24 - 138 \end{aligned}$$

$$(c) \gcd(119, 272) = 119x + 272y$$

$$272 = 2 \cdot 119 + 34$$

$$\therefore 17 = 119 - 3 \cdot 34$$

$$119 = 3 \cdot 34 + 17$$

$$= 119 - 3(272 - 2 \cdot 119)$$

$$34 = 17 \cdot 2 + 0$$

$$= (3)119 - (3)272$$

$$\gcd = 17$$

$$(d) \quad \gcd(1769, 2378) = 1769x + 2378y$$

$$2378 = 1 \cdot 1769 + 609$$

$$1769 = 3 \cdot 609 - 58$$

$$609 = 10 \cdot 58 + 29$$

$$58 = 2 \cdot 29 + 0 \quad \gcd = 29$$

$$\begin{aligned} \therefore 29 &= 609 - 10 \cdot 58 \\ &= 609 - 10(3 \cdot 609 - 1769) \\ &= (-29) \cdot 609 + (10) \cdot 1769 \\ &= (-29)(2378 - 1769) + 10 \cdot 1769 \\ &= (39) \cdot 1769 - (29) \cdot 2378 \end{aligned}$$

$$3. \quad d|a, d|b \cdot d = \gcd(a, b) \Leftrightarrow \gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$$

Af: Let  $m, n$  be s.t.  $dm = a, dn = b$

(a) if  $d = \gcd(a, b)$ , Then, by Th. 2.7 (since  $d > 0$ )

$$d = \gcd(dm, dn) = d \cdot \gcd(m, n) = d \cdot \gcd\left(\frac{a}{d}, \frac{b}{d}\right)$$

$$\therefore 1 = \gcd\left(\frac{a}{d}, \frac{b}{d}\right)$$

(b) if  $\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$ , Then, by Th. 2.7,

$$\gcd(a, b) = \gcd\left(d \cdot \frac{a}{d}, d \cdot \frac{b}{d}\right) = |d| \cdot \gcd\left(\frac{a}{d}, \frac{b}{d}\right) = |d|$$

$$4. \quad \gcd(a, b) = 1$$

$$(a) \quad \gcd(a+b, a-b) = 1 \text{ or } 2$$

Pf: Let  $d = \gcd(a+b, a-b)$ .  $\therefore$  by Corollary p. 23,  
 $d$  is a divisor of all linear combinations  
of  $a+b$  and  $a-b$ .

$$\begin{aligned} \therefore d \mid (a+b) + (a-b) &\Rightarrow d \mid 2a \\ d \mid (a+b) - (a-b) &\Rightarrow d \mid 2b \end{aligned}$$

$$\therefore d \leq \gcd(2a, 2b) = 2 \gcd(a, b) = 2$$

$$\therefore d = 1 \text{ or } 2$$

$$(b) \quad \gcd(2a+b, a+2b) = 1 \text{ or } 3$$

Pf: Let  $d = \gcd(2a+b, a+2b)$

$$\begin{aligned} \therefore d \mid 2 \cdot (2a+b) - (a+2b) &\Leftrightarrow d \mid 3a \\ d \mid -1 \cdot (2a+b) + 2(a+2b) &\Leftrightarrow d \mid 3b \end{aligned}$$

$$\therefore d \leq \gcd(3a, 3b) = 3 \gcd(a, b) = 3$$

$$\therefore d = 1, 2, \text{ or } 3$$

if  $d=2$ , then  $d \mid 3a \rightarrow d/a, d \mid 3b \Rightarrow d \mid 6$   
since  $\gcd(2, 3) = 1$ , and by Th. 2.5 (Euclid's lemma)

But if  $z/a$  and  $z/b$ , then  $\gcd(a, b) \neq 1$ .

$$\therefore d \neq 2$$

$$\therefore d = 1 \text{ or } 3$$

(c)  $\gcd(a+b, a^2+b^2) = 1 \text{ or } 2$

Pf: Let  $d = \gcd(a+b, a^2+b^2)$

$$\text{Then } d | a^2+b^2 \Leftrightarrow d | (a+b)(a-b) + 2b^2$$

Since  $d | (a+b)$ , let  $x$  be s.t.  $d|x = a+b$

and let  $m$  be s.t.  $d|m = (a+b)(a-b) + 2b^2$

$$\therefore dm = dx(a-b) + 2b^2, \therefore d[m+x(a-b)] = 2b^2$$

$$\therefore d | 2b^2$$

By Problem 20(d) on p. 26,  $\gcd(a, b) = 1$  and  
 $d | a+b \Rightarrow \gcd(a, d) = \gcd(b, d) = 1$

$\therefore$  By Euclid's lemma,  $d | 2b^2$  and  $\gcd(d, b) = 1$   
means  $d | 2b \cdot b \Rightarrow d | 2b \Rightarrow d | 2$ .

$$\therefore d \leq 2 \Rightarrow d = 1 \text{ or } 2$$

(d)  $\gcd(a+b, a^2-ab+b^2) = 1 \text{ or } 3$

Pf: Let  $d = \gcd(a+b, a^2-ab+b^2)$

$$\therefore d \mid a^2-ab+b^2 \Rightarrow d \mid (a+b)^2 - 3ab$$

As in (c) above, since  $d \mid (a+b)$ , Then

$$d \mid 3ab.$$

Since  $d \mid a+b$  and  $\gcd(a, b) = 1$ , Then  
by Problem 20(d) p. 26,  
 $\gcd(a, d) = \gcd(b, d) = 1$ .

$\therefore$  By Euclid's lemma,  $d \mid 3ab \Rightarrow d \mid 3a \Rightarrow d \mid 3$

$\therefore d \leq 3$ . Since  $\gcd(2, 3) = 1$ , Then  
if  $d = 2$ , Then  $2 \mid 3ab \Rightarrow 2 \mid ab$   
 $\therefore 2 \mid a$  or  $2 \mid b$ , either of  
which contradicts  $\gcd(a, d) =$   
 $\gcd(b, d) = 1$ .  $\therefore d \neq 2$

$$\therefore d = 1 \text{ or } 3$$

Since  $a, b > 0$ ,  $n \geq 1$

(a) If  $\gcd(a, b) = 1$ , Then  $\gcd(a^n, b^n) = 1$

Pf:  $n=1$ ;  $\gcd(a, b) = 1$  was assumed

$K \Rightarrow K+1$ : Assume  $\gcd(a^K, b^K) = 1$   
By problem 20(a) p. 26,

$$\gcd(a^K, b^{K+1}) = \gcd(a^K, b^K) = 1$$

Since  $\gcd(a, b) = \gcd(b, a)$ ,  
Then  $\gcd(b^{K+1}, a^K) = 1$ , and  
∴ again by 20(a) p. 26,

$$\gcd(b^{K+1}, a^K) = \gcd(b^{K+1}, a^{K+1}) = 1$$

$$(6) a^n | b^n \Rightarrow a | b$$

Pf:  $n=1$ : Clearly,  $a' | b' = a | b$

$K \Rightarrow K+1$ : Assume  $a^K | b^K \Rightarrow a | b$

$$\exists x \text{ s.t. } x a^K = b^K, \exists y \text{ s.t. } a y = b$$
$$\therefore x a^{K+1} = a b^K = (\frac{x}{y}) b^K = \frac{b^{K+1}}{y}$$

$$\therefore x y a^{K+1} = b^{K+1}$$

$$\therefore a^{K+1} | b^{K+1}$$

Another proof, as suggested by author

Let  $d = \gcd(a, b)$ , and let  $r, s$  be s.t.

$$a = rd, b = sd$$

$\gcd(r, s) = 1$  by problem 13(b), p. 25

$\therefore \gcd(r^n, s^n) = 1$  by (a) above.

But since  $a^n = r^n d^n$ ,  $b^n = s^n d^n$ . Then  
since  $a^n | b^n$ , then  $r^n d^n | s^n d^n \Rightarrow r^n | s^n$   
 $\therefore \gcd(r^n, s^n) = r^n$ , so  $r = 1$ .

$\therefore$  from  $a = rd$ ,  $a = d$ , and from  $b = sd$ ,

$$\therefore b = sg, \therefore a | b$$

c.  $\gcd(a, b) = 1 \Rightarrow \gcd(a+b, ab) = 1$

Pf: Let  $c$  be a divisor of  $a+b$  and  $ab$

By 20(d) p. 26,  $\gcd(a, c) = \gcd(b, c) = 1$

Since  $c | ab$  and  $\gcd(c, a) = 1$ , then by

Euclid's lemma,  $c \nmid a$

Similarly,  $c | ab$  and  $\gcd(c, b) = 1 \Rightarrow c \nmid b$

So,  $c \nmid a$ ,  $c \nmid b$ .  $\therefore c \leq \gcd(a, b) = 1, \therefore c = 1$

7. (a)  $a | b \Leftrightarrow \gcd(a, b) = |a|$

Pf: (i)  $a | a$  and  $a | b$ .  $\therefore a$  is a common divisor.

Suppose  $d$  is another common divisor.

$$\therefore \exists n \text{ s.t. } a = dn, \therefore |a| = |d||n|$$

Since  $a \neq 0$ , and  $d \neq 0$ ,  $\therefore n \neq 0$

$$\therefore |n| \geq 1, \text{ otherwise } |a| = |d|.$$

$$\therefore |a| = |d||n| > |d|, \text{ so } |a| > |d|$$

$$\text{and } |a| = \gcd(a, b).$$

$$(2) \text{ Assume } \gcd(a, b) = |a|$$

$$\therefore \exists n \text{ s.t. } b = |a|n. \text{ If } a > 0, \text{ Then}$$

$$|a| = a, \text{ so That } b = an \Rightarrow a \mid b$$

$$\text{If } a < 0, \text{ Then } |a| = -a \Rightarrow b = (-a)n,$$

$$\therefore b = a(-n), \therefore a \mid b.$$

$$(3) a \mid b \Leftrightarrow \text{lcm}(a, b) = |b|$$

$$\text{Pf. (1)} a \mid b \Rightarrow a \mid |b|, \text{ and clearly } b \mid |b|$$

Let  $c$  be another common multiple

$$\therefore a \mid c \text{ and } b \mid c \text{ (and } c > 0\text{).}$$

$$b \mid c \Rightarrow \exists n \text{ s.t. } c = bn, \text{ and } |n| \geq 1.$$

$$\therefore |c| = |b||n| \geq |b|. \therefore |c| \geq |b|, \text{ and}$$

$$\therefore |b| = \text{lcm}(a, b) \text{ by def.}$$

$$(2) \text{lcm}(a, b) = |b| \Rightarrow a \mid |b| \text{ by def.}$$

$$\therefore \exists n \text{ s.t. } an = |b|$$

$$\text{if } b > 0, \text{ Then } an = b \Rightarrow a \mid b$$

$$\text{if } b < 0, \text{ Then } an = -b, a(-n) = b,$$

$$\therefore a \mid b.$$

(c) transitivity of (a) & (b) means  
 $\gcd(a, b) = |a| \Leftrightarrow \lcm(a, b) = |b|$

Or, directly,

$$(1) \text{ Assume } \gcd(a, b) = |a|$$

$$\therefore |a| \lcm(a, b) = |ab| = |a||b|$$

$$\therefore \lcm(a, b) = |b|$$

$$(2) \text{ Assume } \lcm(a, b) = |b|$$

$$\therefore a||b| \Rightarrow |a||b|$$

Let  $c$  be another common divisor

$$\therefore \exists n \text{ s.t. } a = cn \Rightarrow |a| = |c||n|$$

But  $|n| \geq 1 \therefore |c||n| \geq |c| \therefore |a| \geq |c|$ .

$$\therefore |a| = \gcd(a, b).$$

8. (a)  $\lcm(143, 227)$

$$227 = 1 \cdot 143 + 84$$

$$143 = 2 \cdot 84 - 25$$

$$84 = 3 \cdot 25 + 9$$

$$25 = 2 \cdot 9 + 7$$

$$9 = 7 + 2$$

$$7 = 3 - 2 + 1$$

$$\therefore \gcd(143, 227) = 1 \quad \therefore \lcm = 143 \cdot 227 = 32,461$$

$$(b) \text{lcm}(306, 657)$$

$$657 = 2 \cdot 306 + 45$$

$$306 = 7 \cdot 45 - 9$$

$$45 = 5 \cdot 9$$

$$\therefore \gcd = 9, \quad \therefore \text{lcm} = 306 \cdot 657 / 9 = 22,338$$

$$(c) \text{lcm}(272, 1479)$$

$$1479 = 5 \cdot 272 + 119$$

$$272 = 2 \cdot 119 + 34$$

$$119 = 4 \cdot 34 - 17$$

$$34 = 2 \cdot 17$$

$$\gcd = 17, \quad \therefore \text{lcm} = (272 \cdot 1479) / 17 = 23,664$$

$$9. \quad a, b > 0. \quad \gcd(a, b) \mid \text{lcm}(a, b)$$

Pf: Since  $\gcd(a, b) \cdot \text{lcm}(a, b) = ab$ , let   
 $d = \gcd(a, b)$ .  $\therefore \exists n, m \text{ s.t. } a = dn, b = dm$

$$\therefore d \cdot \text{lcm}(a, b) = (dn)(dm)$$

$$\therefore \text{lcm}(a, b) = d(nm) \Rightarrow d \mid \text{lcm}(a, b)$$

$$10. (a) \gcd(a, b) = \text{lcm}(a, b) \Leftrightarrow a = \pm b$$

Pf: (1) Let  $d = \gcd(a, b) = \text{lcm}(a, b)$

$$\therefore d \cdot d = ab$$

Since  $d | a$ ,  $\exists x \in \mathbb{Z}$  s.t.  $dx = a$ .

$$\therefore d \cdot d = dx \cdot b \Rightarrow d = x \cdot b \Rightarrow b | d.$$

$$\therefore d | b \text{ and } b | d$$

$$\therefore d = \pm b \text{ by Th. 2.2(e) on p. 21}$$

$$\text{Similarly, } d = \pm a.$$

$$\therefore |d| = |a| = |b| \Rightarrow a = \pm b$$

(2) If  $a = \pm b$ , Then  $a | b$  and  $b | a$

By problem (7) above,

$$\gcd(a, b) = \text{lcm}(a, b) = |a| = |b|$$

$$(3) k > 0, \text{lcm}(ka, kb) = k \text{lcm}(a, b)$$

Pf:  $\gcd(ka, kb) \cdot \text{lcm}(ka, kb) = k^2 |ab|$

$$\therefore k \gcd(a, b) \cdot \text{lcm}(ka, kb) = k^2 |ab|$$

$$\therefore \gcd(a, b) \cdot \text{lcm}(ka, kb) = k |ab|$$

$$= k \gcd(a, b) \cdot \text{lcm}(a, b)$$

$$\therefore \text{lcm}(ka, kb) = k \cdot \text{lcm}(a, b)$$

(c) If  $m$  is a common multiple of  $a, b$ ,  
Then  $\text{lcm}(a, b) \mid m$

Pf: Let  $l = \text{lcm}(a, b)$

Let  $q, r$  be s.t.  $m = lq + r, 0 \leq r < l$

If  $r = 0$ , Then  $l \mid m$ .

Assume  $0 < r < l$

$\therefore r = m - lq$ . Since  $m, l$  are multiples  
of  $a$  and  $b$ ,  $\exists x, y, u, v$

$$r = ax - ay q \\ = a(x - yq)$$

$$r = bu - bv q \\ = b(u - vq)$$

$\therefore r$  is a multiple of  $a, b$ , and

$\therefore r \geq l$ , which contradicts  $r < l$

II. Let  $a, b, c$  be s.t. no two of which are zero.

Let  $d = \gcd(a, b, c)$ .

(a)  $d = \gcd(\gcd(a, b), c)$

Pf: Let  $f = \gcd(a, b)$  and let  $g = \gcd(f, c)$

(i)  $g \mid f \Rightarrow g \mid a, g \mid b$ . Since  $g \mid c$ , Then  $g \leq d$

(2) Note That  $d \mid f$ .

Pf:  $f = ax + by$ , some  $x, y$  (Th.2.3)

$a = du, b = dv$ , some  $u, v$ .

$\therefore f = dux + dvy, \therefore d \mid f$

Since  $d \mid c$ , Then  $d \mid g$ .  $\therefore d \leq g$

$\therefore (1) + (2) \rightarrow d = g$ .

(3)  $d = \gcd(a, \gcd(b, c)) = \gcd(\gcd(a, c), b)$

Proofs identical to (1) above, switching letters.

12. Find  $x, y, z$  s.t.  $\gcd(198, 288, 512) = 198x + 288y + 512z$

From (1) above,

$$\gcd(198, 288, 512) = \gcd(\gcd(198, 288), 512)$$

$$\therefore 288 = 198 + 90$$

$$\therefore 18 = 198 - 2 \cdot 90$$

$$198 = 2 \cdot 90 + 18$$

$$= 198 - 2(288 - 198)$$

$$90 = 5 \cdot 18$$

$$= (-2) \cdot 288 + 3 \cdot 198$$

$$\therefore \gcd(198, 288) = 18$$

Now for  $\gcd(18, 512)$

$$512 = 28 \cdot 18 + 8$$

$$18 = 2 \cdot 8 + 2$$

$$8 = 4 \cdot 2$$

$$\therefore \gcd(18, 512) = 2$$

$$\therefore 2 = 18 - 2 \cdot 8$$

$$= 18 - 2(512 - 28 \cdot 18)$$

$$= 57 \cdot 18 - 2 \cdot 512$$

$$\therefore \gcd(198, 288, 512) = 2$$

$$\therefore 2 = 57 \cdot 18 - 2 \cdot 512$$

$$= 57 \cdot [3 \cdot 198 - 2 \cdot 288] - 2 \cdot 512$$

$$= 171 \cdot 198 - 114 \cdot 288 - 2 \cdot 512$$

## 2.4 The Diophantine Equation $ax + by = c$

Note Title

11/10/2004

1. (a)  $6x + 51y = 22$

$\gcd(6, 51) = 3$ , and  $3 \nmid 22$ .  $\therefore$  Can't be solved.

(b)  $33x + 14y = 115$

$\gcd(33, 14) = 1$ ,  $\therefore$  it can be solved.

(c)  $14x + 35y = 93$

$\gcd(14, 35) = 7$ ,  $7 \nmid 93$ .  $\therefore$  can't be solved.

2. Use Euclidean Alg. to get  $d = \gcd(a, b)$ , Then express  $d$  in terms of  $a, b$ , Then multiply  $d$  to get  $c$  and  $x_0, y_0$

(d)  $56x + 72y = 40$

$$72 = 56 + 16 \quad s = 56 - 3 \cdot 16$$

$$56 = 3 \cdot 16 + 8$$

$$= 56 - 3(72 - 56)$$

$$16 = 2 \cdot 8$$

$$= 4 \cdot 56 - 3 \cdot 72$$

$$\therefore \gcd = 8$$

$$\therefore 5 \cdot 8 = 40 = 20 \cdot 56 - 15 \cdot 72$$

$\therefore (20, -15)$  a solution

$$\therefore x = 20 + \frac{72}{8}t, y = -15 - \frac{56}{8}t$$

$$\text{or } x = 20 + 9t, y = -15 - 7t$$

$$(6) 24x + 138y = 18$$

$$138 = 5 \cdot 24 + 18$$

$$24 = 18 + 6$$

$$18 = 3 \cdot 6$$

$$\therefore \gcd = 6$$

$$6 = 24 - 18$$

$$= 24 - (138 - 5 \cdot 24)$$

$$= 6 \cdot 24 - 138$$

$$\therefore 18 - 3 \cdot 6 = (18)24 - (3)138$$

$\therefore (18, -3)$  is a solution

$$\therefore x = 18 + \frac{138}{6}t = 18 + 23t$$

$$y = -3 - \frac{24}{6}t = -3 - 4t$$

$$(C) 221x + 35y = 11$$

$$221 = 6 \cdot 35 + 11$$

$$35 = 3 \cdot 11 + 2$$

$$11 = 5 \cdot 2 + 1$$

$$2 = 2 \cdot 1$$

$$\therefore \gcd = 1$$

$$\therefore l = 11 - 5 \cdot 2$$

$$= 11 - 5(35 - 3 \cdot 11)$$

$$= 16 \cdot 11 - 5 \cdot 35$$

$$= 16(221 - 6 \cdot 35) - 5 \cdot 35$$

$$= 16 \cdot 221 - 101 \cdot 35$$

$$\therefore 11 = (11 \cdot 16)(221) - (11 \cdot 101)(35)$$

$\therefore (176, -111)$  a solution

$$\therefore x = 176 + 35t$$

$$y = -111 - 221t$$

$$3. (a) 18x + 5y = 48$$

$$18 = 3 \cdot 5 + 3$$

$$5 = 3 + 2$$

$$l = 3 - 2$$

$$= 3 - (5 - 3)$$

$$\begin{aligned}
 3 &= 2 + 1 & = 2 \cdot 3 - 5 \\
 2 &= 2 - 1 & = 2(18 - 3 \cdot 5) - 5 \\
 \therefore \gcd &= 1 & = 2 \cdot 18 - 7 \cdot 5 \\
 && \therefore 48 = 96 \cdot 18 - (48 \cdot 7) \cdot 5 \\
 && \therefore (96, -336) \text{ a solution} \\
 \therefore x &= 96 + 5t \\
 y &= -336 - 18t
 \end{aligned}$$

Since  $x, y > 0$ ,  $96 + 5t > 0 \Rightarrow t > -19.2$   
 $-336 - 18t > 0 \Rightarrow t < -18.7$

$$\begin{aligned}
 \therefore t &= 19 \\
 \therefore x &= 96 + 5(-19) = 1 \\
 y &= -336 - 18(-19) = 6
 \end{aligned}$$

$$(6) 54x + 21y = 906$$

$$\begin{aligned}
 54 &= 2 \cdot 21 + 12 \quad \therefore 3 = 12 - 9 \\
 21 &= 12 + 9 & = 12 - (21 - 12) = 2 \cdot 12 - 21 \\
 12 &= 9 + 3 & = 2(54 - 2 \cdot 21) - 21 \\
 9 &= 3 \cdot 3 & = 2 \cdot 54 - 5 \cdot 21 \\
 \gcd &= 3 & \therefore 906 = (302 \cdot 2)(54 - (302 \cdot 5)(21)) \\
 && \therefore (604, -1510) \text{ a solution}
 \end{aligned}$$

$$\begin{aligned}
 \therefore x &= 604 + 7t > 0 \Rightarrow t > -86.3 \\
 y &= -1510 - 18t > 0 \Rightarrow t < -83.9
 \end{aligned}$$

$$\therefore x = -84, -85, -86$$

$$\therefore (x, y) = (16, 2), (9, 20), (2, 38)$$

$$(C) 123x + 360y = 99$$

$$360 = 3 \cdot 123 - 9 \quad \therefore 3 = 14 \cdot 9 - 123$$

$$123 = 14 \cdot 9 - 3 \quad = 14(3 \cdot 123 - 360) - 123$$

$$9 = 3 \cdot 3 \quad = 41 \cdot 123 - 14 \cdot 360$$

$$\therefore \gcd = 3 \quad \therefore 99 = (33 \cdot 41)123 - (33 \cdot 14)360$$

$$\therefore (1353, -462) \text{ a solution}$$

$$\therefore x = 1353 + 120t > 0 \Rightarrow t > -11.275$$

$$y = -462 - 41t > 0 \Rightarrow t < -11.3$$

$\therefore$  no  $t$  exists, so no positive solutions

$$(d) 158x - 57y = 7$$

$$158 = 3 \cdot 57 - 13 \quad 1 = 3 - 2 \cdot 1 = 3 - (5 - 3)$$

$$57 = 4 \cdot 13 + 5 \quad = 2 \cdot 3 - 5 = 2(13 - 2 \cdot 5) - 5$$

$$13 = 2 \cdot 5 + 3 \quad = 2 \cdot 13 - 5 \cdot 5$$

$$5 = 3 + 2 \quad = 2 \cdot 13 - 5(57 - 4 \cdot 13)$$

$$3 = 2 + 1 \quad = 22 \cdot 13 - 5 \cdot 57$$

$$2 = 2 \cdot 1 \quad = 22(3 \cdot 57 - 158) - 5 \cdot 57$$

$$\therefore \gcd = 1 \quad = 61(57) - 22 \cdot 158$$

$$\therefore 7 = 427 \cdot 57 - 154 \cdot 158$$

$\therefore (-154, -427)$  a solution

$$\therefore x = -154 - 57t > 0 \Rightarrow t < -2.7 \Rightarrow t \leq -3$$

$$y = -427 - 158t > 0 \Rightarrow t < -2.7 \Rightarrow t \leq -3$$

4.  $\gcd(a, b) = 1$ , then  $ax - by = c$  has infinitely many positive solutions.

Pf: Assume  $a, b > 0$ .

Since  $1|c$ , a solution exists. Let  $x_0, y_0$  be a solution.  $\therefore ax_0 - by_0 = c$ . By corollary on p.36, all solutions are given by:

$$x = x_0 - bt \quad y = y_0 - at$$

$$\text{For } x, y > 0, \quad x_0 - bt > 0, \quad t < \frac{x_0}{b}$$

$$y_0 - at > 0, \quad t < \frac{y_0}{a}$$

$\therefore$  if  $t < \min\left(\frac{x_0}{b}, \frac{y_0}{a}\right)$ , Then

$$t < \frac{x_0}{b} \Rightarrow bt < x_0 \Rightarrow x_0 - bt > 0$$

$$t < \frac{y_0}{a} \Rightarrow at < y_0 \Rightarrow y_0 - at > 0$$

There are infinitely many  $t$  s.t.  $t < \min\left(\frac{x_0}{b}, \frac{y_0}{a}\right)$

5. (a)  $ax + by + cz = d$  is solvable in integers  $\Leftrightarrow \gcd(a, b, c) | d$

Pf: (1) Let  $g = \gcd(a, b, c)$ .  $\therefore \exists p, q, r$  s.t.  
 $gp = a$ ,  $gq = b$ ,  $gr = c$ .

$$\therefore gpx + gqy + grz = g(px + qy + rz) = d$$
$$\therefore g | d$$

(2) Let  $g = \gcd(a, b, c)$  and suppose  $g \nmid d$

By Lemma,  $\exists x_0, y_0, z_0$  s.t.  $g = ax_0 + by_0 + cz_0$ .  
Let  $t$  be s.t.  $gt = d$ .

$$\therefore d = gt = ax_0t + by_0t + cz_0t$$
$$\therefore a \text{ solution is } (x_0t, y_0t, z_0t)$$

Lemma: Given  $a, b, c$  not all of which  
are zero. There exist integers  
 $x, y, z$  s.t.

$$\gcd(a, b, c) = ax + by + cz$$

Pf: Analogous to proof of Th. 2.3.

$$\text{Let } S = \{au + bv + cw \mid au + bv + cw > 0, \\ u, v, w \text{ integers}\}$$

$S$  is non-empty: Suppose  $a \neq 0$ .

$$\therefore |a| = au + b \cdot 0 + c \cdot 0 > 0, \text{ where}$$

$$u = 1 \cdot \text{sign}(a)$$

By Well Ordering Principle,  $S$  has a minimum value,  $d$

By def. of  $S$ ,  $\exists$  integers  $x, y, z$  s.t.

$$d = ax + by + cz$$

Let  $q, r \in S$  s.t. (by Division Alg).

$$a = qd + r, \quad 0 \leq r < d$$

$$\therefore r = a - qd = a - q(ax + by + cz) \\ = a(1-q) - b(qy) - c(qz)$$

If  $r > 0$ , Then  $r \in S \Rightarrow r > d$

But  $d$  is smallest element.  $\therefore r = 0$

$$\therefore a = qd \Rightarrow d \mid a.$$

Similarly,  $d \mid b$ ,  $d \mid c$

$\therefore d$  is a common divisor.

Let  $e$  be any other common divisor  
of  $a, b, c$ . Let  $eh = a, ej = b, ek = c$

$$\therefore d = ax + by + cz = ehx + ejy + ezk \\ = e(hx + jy + kz) \Rightarrow e \mid d$$

By Th. 2.2 p. 21,  $|e| < |d|$ ,

$$\therefore d = \gcd(a, b, c)$$

Alternate Lemma: By #11, p. 32,

$$\gcd(a, b, c) = \gcd(\gcd(a, b), c).$$

Let  $u = \gcd(a, b)$ .  $\therefore \exists x, y$  s.t.

$u = ax + by$ . Also,  $\exists h, k$  s.t.

$$d = uh + ck = (ax + by)h + ck$$

$$= ah + bh + ck$$

$\therefore \exists$  integers  $p, q, r$  s.t.  $d = ap + bq + cr$

(6) Find all integer solutions of  $15x + 12y + 30z = 24$

$\gcd(15, 12, 30) = 3$ , and  $3 \mid 24$ , so integer solutions exist by (a) above.

Now divide by  $\gcd$  to simplify.

$$15x + 12y + 30z = 24 \Leftrightarrow 5x + 4y + 10z = 8$$

$\therefore 5x + 10z = 8 - 4y$ . Since  $\gcd(5, 10) = 5$ ,

$$5x + 10z = 5n, \text{ some } n. \quad \therefore 5n = 8 - 4y$$

$x = n, z = 0$  is a solution,  $\therefore$  by Th. 2.9,

$x = n + 2t, z = -t$ , gives all solutions for  $5x + 10z = 5n$

$\therefore (x, y, z)$  is a solution  $\Leftrightarrow$

$$x = n + 2t \quad \text{for some } n, t$$

$$z = -t$$

$$8 - 4y = 5n, \text{ or } 4y = 8 - 5n$$

$\therefore y = 2 - \frac{5n}{4}$ , which means  $4 \mid n$ ,  
so  $n$  must be divisible by 4.

$$\therefore \text{Let } n = 4k. \therefore y = 2 - 5k. \therefore x = 4k + 2t$$

$\therefore$  if  $k$  and  $t$  are any integers,

$$x = 4k + 2t$$

$$y = 2 - 5k$$

$$z = -t$$

6. (a) \$4.55 in dimes and quarters.

(1) Determine max + min. # of coins

(2) Can # dimes = # quarters?

$$(1) 10d + 25q = 455, d \geq 0, q \geq 0$$

$$\gcd(10, 25) = 5$$

Equation  $\equiv 2d + 5q = 91 \quad (3, 17) \text{ a solution.}$

$\therefore$  All solutions of form

$$d = 3 + 5t \quad d \geq 0 \Rightarrow 3 + 5t \geq 0, t \geq -\frac{3}{5}, t \geq 0$$

$$q = 17 - 2t \quad q \geq 0 \Rightarrow 17 - 2t \geq 0, t \leq \frac{17}{2}, t \leq 8$$

$$\therefore 0 \leq t \leq 8$$

Max # coins is when  $d+q$  is a max.

$d+q = 20 + 3t$ , so when  $t=8$ ,  
you will have 44 coins (43d, 1q)

Min # coins :  $t=0$ , or 20 coins (3d, 17q)

(2) For  $d=q$ ,  $3+5t = 17-2t$ ,  $7t = 14$ ,  $t=2$   
 $\therefore$  13 dimes, 13 quarters is a solution.

(3)  $180a + 75c = 9000$ ,  $a \geq c$  Also,  $a \geq 0, c \geq 0$

$$\gcd(75, 180) = 15$$

Reduce equation to  $12a + 5c = 600$

One solution is (50, 0)

$\therefore$  All solutions of form  $a = 50 + 5t$   
 $c = -12t$

$$a \geq c \Rightarrow 50 + 5t \geq -12t, 17t \geq -50, t \geq -\frac{50}{17} \approx -2.94$$

$$a \geq 0 \Rightarrow 5t \geq -50, t \geq -10$$

$$c \geq 0 \Rightarrow -12t \geq 0, t \leq 0$$

$$\therefore -2 \leq t \leq 0$$

$$\therefore t = 0, -1, -2$$

So, 50 adults, 0 children

45 adults, 12 children

40 adults, 24 children

$$(C) \begin{array}{l} 6x + 9y = 126 \\ 6y + 9x = 114 \end{array} \quad \begin{array}{l} 36x + 54y = 756 \\ 36x + 24y = 456 \end{array}$$

$$\therefore 30y = 300, y = 10$$

$$\therefore 6x + 9(10) = 126$$

$$6x = 36, x = 6$$

$$\therefore 6 \text{ sixes, } 10 \text{ nines}$$

7.  $c + l + p = 100$        $c, l, p \geq 1$

 $120c + 50l + 25p = 4000$ 
 $\gcd(120, 50, 25) = 5$ 
 $\therefore \text{Reduce to } 24c + 10l + 5p = 800$ 
 $p = 100 - c - l$ 
 $\therefore 24c + 10l + 5(100 - c - l) = 800$ 
 $19c + 5l = 300 \quad (0, 60) \text{ a solution}$ 
 $\therefore c = 5t$ 
 $l = 60 - 19t \quad \therefore p = 100 - 5t - (60 - 19t)$ 
 $p = 40 + 14t$

Now,  $5t \geq 1 \Rightarrow t \geq 1$

$60 - 19t \geq 1 \Rightarrow 19t \leq 59, t \leq 3$

$40 + 14t \geq 1 \Rightarrow 14t \geq -39, t \geq -2$

$\therefore 1 \leq t \leq 3$

$\therefore 5$  calves, 41 lambs, 54 piglets

10 calves, 22 lambs, 68 piglets

15 calves, 3 lambs, 82 piglets

8. Let original check be  $d$  dollars and  $c$  cents.  
 So, Mr. Smith was given  $100c + d$  cents.  
 Find smallest value of  $100d + c$ .

$$\therefore 100c + d - 68 = 2(100d + c), \quad d, c \geq 0$$

$$\begin{aligned} \therefore 98c - 199d &= 68 & \gcd(98, 199) &= 1 \\ 199 &= 2 \cdot 98 + 3 & \therefore 1 &= 3 - 2 \\ 98 &= 32 \cdot 3 + 2 & &= 3 - (98 - 32 \cdot 3) = 33 \cdot 3 - 98 \\ 3 &= 2 + 1 & &= 33(199 - 2 \cdot 98) - 98 \\ 2 &= 2 \cdot 1 & &= 33 \cdot 199 - 67 \cdot 98 \\ & & \therefore 68 &= (68 \cdot 33)199 - (68 \cdot 67)98 \\ \therefore (-4556, -2244) & \text{ is a solution.} \end{aligned}$$

$\therefore$  All solutions are of form:

$$c = -4556 - 199t \quad c \geq 0 \Rightarrow 199t \leq -4556, \quad t \leq -22.9$$

$$d = -2244 - 98t \quad d \geq 0 \Rightarrow 98t \leq -2244, \quad t \leq -22.9$$

$$\therefore t \leq -23$$

$$100d + c = -228956 - 9999t$$

This is smallest when  $t$  is biggest, so  $t = -23$   
 $\therefore 100d + c = -228956 - 9999(-23) \stackrel{!}{=} 1021 \text{ cents}$   
 or 10 dollars 21 cents

Check: 21 dollars 10 cents - 68 cents = 20 dollars 42 cents

9. (a)  $m + w + c = 100$ ,  $m, w, c \geq 0$

$$3m + 2w + \frac{1}{2}c = 100 \text{, or } 6m + 4w + c = 200$$

$$c = 100 - m - w$$

$$\therefore 5m + 3w = 100$$

One solution is  $(14, 10)$

$\therefore$  All solutions of form:

$$m = 14 + 3t \quad m \geq 0 \Rightarrow t \geq -\frac{14}{3}, t \geq -4$$

$$w = 10 - 5t \quad w \geq 0 \Rightarrow 5t \leq 10, t \leq 2$$

$$c = 76 + 2t \quad c \geq 0 \Rightarrow t \geq -38, t \geq -37$$

$$\therefore -4 \leq t \leq 2$$

$\therefore t = -4$  : 2 men, 30 women, 68 children

$t = -3$  : 5 men, 25 women, 70 children

$t = -2$  : 8 men, 20 women, 72 children

$t = -1$  : 11 men, 15 women, 74 children

$t = 0$  : 14 men, 10 women, 76 children

$t = 1$  : 17 men, 5 women, 78 children

(b) Let  $x$  = # plantain fruit in each of the 63 poles.

$$\therefore 63x + 7 = \text{total # fruit}, x > 0$$

Let  $y$  = # fruit to each of the 23 travelers.

$$\therefore 23y = \text{total # fruit}, y > 0$$

$$\therefore 63x + 7 = 23y, \text{ or } 63x - 23y = -7$$

$$63 = 3 \cdot 23 - 6 \quad \therefore 1 = 4 \cdot 6 - 23$$

$$23 = 4 \cdot 6 - 1 \quad = 4(3 \cdot 23 - 63) - 23 \\ 6 = 6 - 1 \quad = 11 \cdot 23 - 4 \cdot 63$$

$$\therefore -7 = -77 \cdot 23 + 28 \cdot 63$$

$\therefore (28, 77)$  a solution.

$\therefore$  All solutions of form:

$$x = 28 - 23t \quad x \geq 0 \Rightarrow 23t < 28, t \leq 1$$

$$y = 77 - 63t \quad y \geq 0 \Rightarrow 63t < 77, t \leq 1$$

$\therefore$  Infinitely many solutions

$$t=1 : x=5, y=14 \quad (5 \text{ fruits/pole}, 14/\text{traveler})$$

$$t=0 : x=28, y=77 \quad (28 \text{ fruits/pole}, 77/\text{traveler})$$

:

(c) Let  $x = \#$  coins on a string when make 77 strings.

$$\therefore 77x - 50 = \text{total } \# \text{ coins}$$

Let  $y = \#$  coins on a string when make 78 strings.

$$\therefore 78y = \text{total } \# \text{ coins.}$$

$$\therefore 77x - 50 = 78y, \text{ or } 77x - 78y = 50, x, y \geq 0$$

$$\gcd(77, 78) = 1$$

$$\therefore 78 = 77 + 1 \quad \therefore 50 = 50(78) - 50(77)$$

$$77 = 1 \cdot 77 \quad \therefore (-50, -50) \text{ a solution}$$

$\therefore$  All solutions of form:

$$x = -50 - 78t, x > 0 \Rightarrow 78t < -50, t \leq -\frac{50}{78}$$

$$y = -50 - 77t, y > 0 \Rightarrow 77t < -50, t \leq -\frac{50}{77}$$

Infinitely many solutions.

One solution is  $t = -1$ ,  $\therefore x = 28, y = 27$   
 $\therefore$  Total # coins is  $78(27) = 2106$

(d)  $m + w + c = 20, m, w, c \geq 0$   
 $3m + 2w + \frac{1}{2}c = 20, \text{ or } 6m + 4w + c = 40$   
 $c = 20 - m - w$

$$\therefore 5m + 3w = 20$$

One solution is  $(1, 5)$

$\therefore$  All solutions of form:

$$m = 1 + 3t \geq 0 \Rightarrow t \geq -\frac{1}{3}, t \geq 0$$

$$w = 5 - 5t \geq 0 \Rightarrow 5t \leq 5, t \leq 1$$

$$c = 14 + 2t \geq 0 \Rightarrow t \geq -7, t \geq -6$$

$$\therefore t = 0$$

$\therefore$  1 man, 5 women, 14 children

(e)  $100 = x + y, 7|x, 11|y, 0 \leq x, y \leq 100$

$$\text{Let } 7k = x, 11n = y$$

$$\therefore 7k + 11n = 100, 0 \leq 7k, 11n \leq 100$$

$$\begin{aligned}
 11 &= 7 + 4 \quad \therefore 1 = 4 - 3 = 4 - (7 - 4) = 2 \cdot 4 - 7 \\
 7 &= 4 + 3 \quad = 2(11 - 7) - 7 \\
 4 &= 3 + 1 \quad = 2 \cdot 11 - 3 \cdot 7 \\
 3 &= 3 \cdot 1 \quad \therefore 100 = 200 \cdot 11 - 300 \cdot 7 \\
 &\quad \therefore (-300, 200) \text{ a solution}
 \end{aligned}$$

$$\begin{aligned}
 \therefore K &= -300 + 11t \\
 n &= 200 - 7t
 \end{aligned}$$

$$\begin{aligned}
 \text{Now } 0 \leq 7K \leq 100 &\Rightarrow 0 \leq K \leq \frac{100}{7}, \quad 0 \leq K \leq 14 \\
 0 \leq 11n \leq 100 &\Rightarrow 0 \leq n \leq \frac{100}{11}, \quad 0 \leq n \leq 9
 \end{aligned}$$

$$\begin{aligned}
 \therefore 0 \leq -300 + 11t \leq 14 &\Rightarrow 300 \leq 11t \leq 314, \\
 28 \leq t \leq 28 \quad \therefore t &= 28
 \end{aligned}$$

$$\begin{aligned}
 0 \leq 200 - 7t \leq 9 &\Rightarrow -200 \leq -7t \leq -191 \\
 28.6 \geq t \geq 27.3, \quad t &= 28
 \end{aligned}$$

$$\begin{aligned}
 \therefore K &= -300 + 11(28) = 8 \quad \therefore 7K = 56 \\
 n &= 200 - 7(28) = 4 \quad 11n = 44
 \end{aligned}$$

Note on problem 5(6) - Author's solution

The choice of  $y = 3s - 5t$ ,  $z = -5 + 2t$

was ad hoc. Other choices for the coefficients of  $s$  and  $t$  are fine, as long as they are relatively prime. They were chosen so that  $12y + 30z$  would eliminate one variable.

You would then reduce 2 variables ( $y, z$ ) to one variable ( $s$ ), thereby solving an equation in two variables ( $x, s$ ) in terms of a parameter  $r$  using Th. 2.9. By substitution,  $y$  and  $z$  would then be expressed in terms of  $r$  and  $t$ .

Any value of  $y$  and  $z$  can be expressed in terms of  $s$  and  $t$ , as long as the coefficients are "non-parallel" lines, and are relatively prime. In other words,  $y = 3s - 10t$ ,  $z = -s + 4t$  would not work, as  $t = 2.5$  could give a solution in integers, but  $t = 2.5$  is not allowed. Relatively prime coefficients precludes this.

### 3.1 The Fundamental Theorem of Arithmetic

Note Title

11/24/2004

1.  $n^2 - 2$ :  
 $n = 2 \Rightarrow 2^2 - 2 = 2$       All primes  
 $n = 3 \Rightarrow 9 - 2 = 7$   
 $n = 5 \Rightarrow 25 - 2 = 23$   
 $n = 7 \Rightarrow 49 - 2 = 47$   
 $n = 9 \Rightarrow 81 - 2 = 79$

2.  $25 = p + a^2$ .  
 $a = 1 \quad p = 24 \quad \therefore \text{No prime}$   
 $a = 2 \quad p = 21 \quad p \text{ for all}$   
 $a = 3 \quad p = 16 \quad \text{possible values}$   
 $a = 4 \quad p = 9 \quad \text{of } a.$   
 $a = 5 \quad p = 0$

3. (a) If  $3n+1$  is prime, so is  $6m+1$

Pf:  $3n+1$  prime  $\Rightarrow 3n+1$  is odd. Let  
 $p = 3n+1$ , Then  $p-1 = 3n$  is even.  
 $\therefore n$  is even,  $\therefore n = 2m$ , some  $m$ ,  
 $\therefore p = 3(2m)+1 = 6m+1$

(b) Every integer of form  $3n+2$  has a prime factor of that form.

Pf: Let  $p$  be any prime factor of  $3n+2$   
 $\therefore p = 3k+1 \text{ or } 3k+2$ , some  $k$ , by  
Division Alg.

$\therefore 3^{n+2} = (3k_1 + 1)(3k_2 + 1) \dots (3k_r + 1)$ , by  
Fund. Th. of Arith.

But This latter product is of form  
 $[3^r k_1 \dots k_r + \dots + 1]$ , where every term,  
except 1, is a factor of 3.  $\therefore$  Product  
is of form  $3g + 1$ , a contradiction.

(c) The only prime of form  $n^3 - 1$  is ?.

$$\text{Pf: } n^3 - 1 = (n-1)(n^2 + n + 1)$$

For  $n^3 - 1$  to be prime,  $n = 1$

$$\text{For } n=2, n^3 - 1 = (2-1)(7) = 7$$

For any  $n > 2$ ,  $p = n^3 - 1$  will be a factor  
of two integers, neither of which  
is 1.  $\therefore$  for  $n \neq 2$ ,  $p$  can't be prime.

(d) The only prime  $p$  for which  $3p + 1$  is a  
perfect square is  $p = 5$ .

$$\text{Pf: } 3(5) + 1 = 16 = 4^2$$

Suppose  $3p + 1 = n^2$ , some  $n \neq 4$

$$\therefore 3p = n^2 - 1 = (n+1)(n-1)$$

If  $n+1 = p$ , Then  $n-1 = 3, n=4$   
 Assume  $n+1 \neq p$ .  $\therefore \gcd(n+1, p) = 1$ .  
 $\therefore n+1 \mid 3$ , by Euclid's Lemma.  
 $\therefore n+1 = 1 \text{ or } 3$ ,  $\therefore n=2$ .  $\therefore 3p+1=4$ ,  
 $p=1$ , a contradiction.  
 $\therefore n+1$  must be  $p$ , and  $\therefore n$  must be 4

Similar reasoning for  $n-1$ .

If  $n-1 = p$ , Then  $n+1 = 3, n=2$ , leading  
 to contradiction of  $3p+1=4, p=1$ .  
 $\therefore n-1 \neq p$ , Then  $\gcd(n-1, p) = 1$ ,  $\therefore$   
 $n-1 \mid 3$  by Euclid's Lemma.  $\therefore n-1 = 1 \text{ or } 3$ .  
 $\therefore n=4$ .

(e) The only prime of form  $n^2 - 4$  is 5.

Pf: Let  $p = n^2 - 4 = (n+2)(n-2)$

Since  $p$  is prime, one of the  
 factors must be 1 and the other  
 must be  $p$ .

Suppose  $n+2 = p$ ,  $\therefore n-2 = 1, \therefore n=3$ ,  
 $\therefore p=5$

Suppose  $n+2 = 1$ .  $\therefore n=-1$ , and  
 $\therefore p = n-2 = -3$ .  $\therefore n+2 \neq 1$ .  
 $\therefore$  only possibility is  $n=3, \therefore p=5$

4.  $p \geq 5$ , Then  $p^2 + 2$  is composite

Pf: By Div.Alg.,  $p = 6k+r$ ,  $0 \leq r < 6$

$r \neq 0$  as  $p = 6k \Rightarrow 6 | p$

$r \neq 2$  as  $p = 6k+2 \Rightarrow 2 | p$

$r \neq 3$  as  $p = 6k+3 \Rightarrow 3 | p$

$r \neq 4$  as  $p = 6k+4 \Rightarrow 2 | p$

$\therefore p = 6k+1$  or  $p = 6k+5$

$$\therefore p^2 + 2 = 36k^2 + 12k + 3 \text{ or}$$

$$p^2 + 2 = 36k^2 + 60k + 27$$

In either case,  $3 | p^2 + 2$ , so  
 $p^2 + 2$  is composite.

5. (a)  $p$  prime,  $p | a^n \Rightarrow p^n | a^n$

Pf: By Corollary 1 (p. 41),  $p | a^n \Rightarrow p | a$   
 $\therefore a = pk$ , some  $k$ , so  $a^n = p^n k^n \Rightarrow p^n | a^n$

(b) If  $\gcd(a, b) = p$ , Then by (a) above,  $p^2 | a^2$ ,  $p^2 | b^2$ ,  
so  $\gcd(a^2, b^2) = p^2$

$$\gcd(a^2, b) = p$$

$$\gcd(a^3, b^2) = p^2$$

6. (a) For all  $n \geq 1$ ,  $n^4 + 4$  is composite

$$\text{Pf: } n^4 + 4 = (n^2 - 2n + 2)(n^2 + 2n + 2)$$

Since  $n \geq 1$ ,  $n \geq 2$ ,  $n^2 \geq 2n$ , and  
 $\therefore n^2 - 2n \geq 0$ ,  $n^2 + 2n + 2 \geq 2 > 0$

$\therefore$  Both factors are positive.

Since  $n^4 + 4$  has two integer positive factors, it is composite.

Find the factors by guessing the roots (or using a calculator).

$$\text{Note that } (1+i)(1+i) = 2i, (2i)^2 = -4$$

$\therefore 1+i$  is a root, and  $\therefore$  so is  $1-i$

$$\therefore (n - 1 - i)(n - 1 + i) = (n - 1)^2 - i^2 \\ = n^2 - 2n + 1 + 1$$

$$= n^2 - 2n + 2,$$

and so  $n^2 - 2n + 2$  is a factor

Find the other by division.

(b) If  $n > 4$  is composite, then  $n$  divides  $(n-1)!$

Pf: Since  $n$  is composite, let  $n = p_1^{k_1} \cdots p_r^{k_r}$   
be the unique prime factorization.

If  $r > 1$ , Then  $n > p_1^{k_1}$ , so  $n-1 \geq p_1^{k_1}$   
 $\therefore$  since all integers  $\leq n-1$  are terms  
 of  $(n-1)!$ , Then each  $p_i^{k_i}$  is  
 represented by one of the terms of  
 $(n-1)!$ .  $\therefore p_1^{k_1} \cdots p_r^{k_r} \mid (n-1)!$

Suppose  $r=1$ , so  $n = p^k$ .  $k > 1$   
 since  $n$  is composite.  
 $\therefore n = p^{k-1} \cdot p$   
 $\therefore n > p$  and  $n > p^{k-1}$   
 $\therefore n-1 \geq p$  and  $n-1 \geq p^{k-1}$

If  $p \neq p^{k-1}$ , Then each is represented  
 in  $(n-1)!$ , so  $p \cdot p^{k-1} = n \mid (n-1)!$

Suppose  $p = p^{k-1}$ , so  $k=2$ .  $\therefore n = p^2$   
 $\therefore n > p$ , so  $n-1 \geq p$   
 Since  $n \geq 6$ , Then  $p \neq 2$   
 And  $2(n-1) < (n-1)!$  for  $n > 4$   
 $\therefore 2(n-1)$  is a term of  $(n-1)!$   
 $\therefore$  Each of  $p$  and  $2p$  are terms  
 of  $(n-1)!$   $\therefore 2p^2 \mid (n-1)!$ , so  
 $p^2 \mid (n-1)!$   $\therefore p^2 = n \mid (n-1)!$

(c)  $8^n + 1$ ,  $n \geq 1$ , is composite

Pf:  $a^3 + 1 = (a+1)(a^2 - a + 1)$   
 $\therefore (2^n)^3 + 1 = (2^n + 1)(2^{2n} - 2^n + 1)$   
 $\therefore 2^n + 1 \mid 2^{3n} + 1$   
and  $2^{3n} = 8^n$   
 $\therefore 2^n + 1 \mid 8^n + 1$

(d)  $n \geq 11$ , Then  $n$  is the sum of two composite numbers

Pf: Suppose  $n$  is even. Then  $\exists K$  s.t.  $n = 2K$ .

$$n = 2K = 6 + 2(K-3)$$

$\therefore n$  is the sum of 6 ( $= 2 \cdot 3$ ) and  $2(K-3)$

If  $K \geq 5$  ( $\Rightarrow K-3 > 1$ , so  $2(K-3)$  is product of two numbers  $> 1$ ), then  $2K \geq 10$ ,  $n \geq 11$ , and  $n$  is the sum of two composites.

Suppose  $n$  is odd. Then  $\exists K$  s.t.  $n = 2K+1$

$$\therefore n = 2K+1$$

$$= 2(K-1) + 3 \quad 3 \text{ is prime}$$

$$= 2(K-2) + 5 \quad 5 \text{ is prime}$$

$$= 2(K-3) + 7 \quad 7 \text{ is prime}$$

$$= 2(K-4) + 9$$

So, if  $K \geq 6$ , Then  $2(K-4)$  is the

product of two numbers  $> 1$ , so  
 $n = 2k+1 \geq 13$ , and  $n$  is the sum  
of two composites.

7. Find all primes that divide  $50!$ .

All primes  $< 50$  will divide  $50!$  since each  
is a term of  $50!$ .

By Fund. Th. of Arithmetic, each term  $k$  of  $50!$  that  
is non-prime has a unique prime factorization,  
and each term of the unique factorization of  $k$   
is smaller than  $k$ , and so is a prime that is  
 $< 50$ .  $\therefore$  There is no prime  $> 50$  represented  
in this factorization of  $k$ .

$\therefore$  All primes  $< 50$  are all the primes that  
divide  $50!$

8.  $p = q \geq 5$ , A9 primes,  $24 \mid p^2 - q^2$

Pf: From #4 above,  $p = 6r+1$  or  $6r+5$   
 $q = 6s+1$  or  $6s+5$

Three possibilities

$$(1) p = 6r+1, q = 6s+1$$

$$(2) p = 6r+5, q = 6s+5$$

$$(3) p = 6r+1, q = 6s+5$$

The situation of  $p = 6r + 5, q = 6s + 1$  is equivalent to  $\#(3)$ .

(1) Let  $p = 6r + 1, q = 6s + 1$  ( $r, s \geq 0, p, q \geq 7$ )

Since  $p, q \geq 5$ , Then  $r, s \neq 0$

$$\begin{aligned}\therefore p^2 - q^2 &= (p+q)(p-q) \\ &= (Gr+1+Gs+1)(Gr+1-[Gs+1]) \\ &= (Gr+Gs+2)(6r-6s) \\ &= 2 \cdot 6 (3r+3s+1)(r-s)\end{aligned}$$

if  $r, s$  are both even or both odd, Then

$r-s$  is even and  $\neq 0$ , so  $r-s = 2k$

$$\begin{aligned}\therefore p^2 - q^2 &= 2 \cdot 6 \cdot 2 (3r+3s+1)(k) \\ &= 24 (3r+3s+1)(k). \therefore 24 \mid p^2 - q^2\end{aligned}$$

if one is even and one is odd, Then

$3r+3s+1$  is even, so  $3r+3s+1 = 2k$

$$\therefore p^2 - q^2 = 2 \cdot 6 \cdot 2 (k)(r-s) = 24(k)(r-s)$$

$$\therefore 24 \mid p^2 - q^2$$

(2) Let  $p = 6r+5, q = 6s+5$  ( $r, s \geq 0, so p, q \geq 5$ )

$$\begin{aligned}\therefore p^2 - q^2 &= (p+q)(p-q) \\ &= (Gr+5+Gs+5)(Gr-6s) \\ &= (Gr+5+Gs+10)(Gr-6s) \\ &= 2 \cdot 6 (3r+3s+5)(r-s)\end{aligned}$$

if  $r, s$  are both even or both odd, Then

$r-s$  is even and  $\neq 0$ , so  $r-s = 2K$

$$\therefore p^2 - q^2 = 2 \cdot 6 \cdot 2(3r + 3s + 5)(K)$$

$$= 24(3r + 3s + 5)(K) \therefore 24 \mid p^2 - q^2$$

if one is even, one odd, Then

$3r + 3s + 5$  is even, so  $3r + 3s + 5 = 2K$

$$\therefore p^2 - q^2 = 2 \cdot 6 \cdot 2(K)(r-s) = 24(K)(r-s)$$

$$\therefore 24 \mid p^2 - q^2$$

$$(3) p = 6r+1, q = 6s+5 \quad (r \geq 0, s \geq 0, \text{ so } p, q \geq 5)$$

$$\therefore p^2 - q^2 = (p+q)(p-q)$$

$$= (6r+1+6s+5)(6r-6s-4)$$

$$= (6r+6s+6)(6r-6s-4)$$

$$= 6 \cdot 2(r+s+1)(3r-3s-2)$$

If one is even, one odd, Then  $r+s+1$  is even,

$$\text{so } r+s+1 = 2K.$$

$$\therefore p^2 - q^2 = 24(K)(3r-3s-2), \text{ so } 24 \mid p^2 - q^2$$

if both even or both odd, Then

$3r-3s-2$  is even, so  $3r-3s-2 = 2K$

$$\therefore p^2 - q^2 = 24(r+s+1)(K), \text{ so } 24 \mid p^2 - q^2$$

$$9. (a). 2^4 + 1 = 17$$

$$2^8 + 1 = 257$$

$$(b) 1^2 + 1 = 2 \quad 4^2 + 1 = 17 \quad 10^2 + 1 = 101$$

$$2^2 + 1 = 5$$

$$6^2 + 1 = 37$$

10.  $p \neq 5, p \neq 2$ , prove  $10 | p^2 - 1$  or  $10 | p^2 + 1$

Pf:  $p$  is of the form:  $10k+1, 10k+3,$   
 $10k+7, 10k+9.$

$10k + \text{even}$ : can factor out 2, so not prime.

$$(10k+1)^2 = 100k^2 + 20k + 1 \therefore 10 | p^2 - 1$$

$$(10k+3)^2 = 100k^2 + 60k + 9 \therefore 10 | p^2 + 1$$

$$(10k+7)^2 = 100k^2 + 140k + 49 \therefore 10 | p^2 + 1$$

$$(10k+9)^2 = 100k^2 + 180k + 81 \therefore 10 | p^2 - 1$$

11. (a)  $2^3 - 1 = 7$      $2^7 - 1 = 127$   
 $2^5 - 1 = 31$      $2^{13} - 1 = 8091$

(b) if  $p = 2^k - 1$  is prime, show  $k$  is odd &  $k \geq 2$

Pf:  $a^n - b^n = (a-b)(a^{n-1} + a^{n-2}b + \dots + ab^{n-2} + b^{n-1})$

$$\therefore 4^n - 1 = (4-1)(4^{n-1} + \dots + 1)$$

$$= 3(4^{n-1} + \dots + 1)$$

$$\therefore 3 | 4^n - 1 \Rightarrow 3 | 2^{2n} - 1 \quad (n \geq 1)$$

$2n$  is even, so if  $p = 2^k - 1$  is prime,  
 $k$  must be odd ( $n \geq 1 \Rightarrow 2n \geq 2$ , so  $k \geq 3$ ).

12.  $1234 = 2 \cdot 617$

$$\begin{aligned} 10 | 40 &= 10 \cdot 1014 = 2 \cdot 5 \cdot 2 \cdot 507 = 2^2 \cdot 5 \cdot 3 \cdot 13^2 \\ &= 2^2 \cdot 3 \cdot 5 \cdot 13^2 \end{aligned}$$

$$36000 = 36 \cdot 1000 = 2^2 \cdot 3^2 \cdot 10 \cdot 25 \cdot 4$$

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

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

13. If  $n > 1$  not of form  $6k+3$ , Then  $n^2 + 2^n$  is composite.

Pf:  $n$  of form  $6k, 6k+1, 6k+2, 6k+4, 6k+5$

$6k: n^2 + 2^n = 36k^2 + 2^{6k}$ . Since  $k > 0$ ,

$2 \mid 36k^2 + 2^{6k} \therefore$  composite

$$6k+1: n^2 + 2^n = (6k+1)^2 + 2^{6k+1}$$

$$= 36k^2 + 12k + 1 + 2^{6k+1}$$

$$= 36k^2 + 12k + 1 + 2^{6k+1}$$

$$\text{From } a^n - b^n = (a-b)(a^{n-1} + a^{n-2}b + \dots + ab^{n-2} + b^{n-1})$$

Substitute  $(-1 \cdot 6)$  for  $b$  and gcf,

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

$$\therefore a^{6k+1} - (-1)^{6k+1} b^{6k+1} = a^{6k+1} + b^{6k+1} = (a+b)(\quad)$$

$$\therefore n^2 + 2^n = 36k^2 + 12k + 2^{6k+1} + (\quad)$$

$$= 36k^2 + 12k + (2+1)(2^{6k} - \dots + (-1)^{6k} 1^{6k})$$

$$= 36k^2 + 12k + 3(2^{6k} - \dots + 1)$$

$$\therefore 3 \mid n^2 + 2^n$$

$$6k+2: n^2 + 2^n = (6k+2)^2 + 2^{6k+2}$$

$$= 36k^2 + 24k + 4 + 2^2 \cdot 2^{6k}$$

$$\therefore 2 \nmid n^2 + 2^n$$

$GK+4: n^2 + 2^n = 36k^2 + 48k + 16 + 2^{6k+4}$

$$\therefore 2 \nmid n^2 + 2^n$$

$$GK+5: n^2 + 2^n = 36k^2 + 60k + 25 + 2^{6k+5}$$

$$= 36k^2 + 60k + 24 + 2^{6k+5} + 1$$

$$= 36k^2 + 60k + 24 + (2+1)(2^{6k+4} \dots)$$

$$= 3 \left[ \dots \right] \text{ similar to } GK+1 \text{ above}$$

$$\therefore 3 \mid n^2 + 2^n$$

Note for,  $GK+3$ ,  $36k^2 + 36k + 9$ ,  $9 = 8+1$ ,  
so can't use the  $a^n + b^n = (a+b)(\dots)$  trick.

$14. 10 = 149 - 139$	$10 = 419 - 409$	$10 = 719 - 709$
$10 = 191 - 181$	$10 = 431 - 421$	$10 = 797 - 787$
$10 = 251 - 241$	$10 = 587 - 547$	$10 = 821 - 811$
$10 = 293 - 283$	$10 = 587 - 577$	$10 = 839 - 829$
$10 = 347 - 337$	$10 = 701 - 691$	$10 = 929 - 919$

$15.$   $a > 1$  is a square  $\Leftrightarrow a$  in canonical form has all even exponents for the primes.

Pf: Suppose  $a$  is a square.  $\therefore a = n^2$   
Let  $p_1^{k_1} p_2^{k_2} \dots p_r^{k_r} = n$ .  $\therefore n^2 = p_1^{2k_1} \dots p_r^{2k_r}$ ,

so all exponents are even.

Suppose all exponents of  $p_1^{k_1} \cdots p_r^{k_r} = a$  are even.  
 $\therefore k_i = 2m_i$ , some  $m_i$  for each  $k_i$   
 $\therefore a = p_1^{2m_1} p_2^{2m_2} \cdots p_r^{2m_r}$   
 $= (p_1^{m_1} \cdots p_r^{m_r})^2$

16. (a)  $n > 1$  is square free  $\Leftrightarrow n$  can be factored into a product of distinct primes.

Suppose  $n$  is square free, and let  $n = p_1^{k_1} \cdots p_r^{k_r}$  be the prime factorization.

Suppose any  $k_i > 1 \therefore k_i \geq 2$ , and  
 $\therefore p_i^2$  will divide  $n$ , a contradiction  
of def. of square free.  $\therefore$  each  $k_i = 1$ .

Suppose  $n = p_1 \cdots p_r$ , each  $p_i \neq p_k$ .

Suppose  $n$  is not square free, and  
let  $a^2 | n \therefore n = x a^2$ ,  $x$  an integer.  
Let  $a = q_1^{k_1} \cdots q_s^{k_s}$ .

$$\therefore p_1 \cdots p_r = x q_1^{2k_1} \cdots q_s^{2k_s} \therefore q_i | p_1 \cdots p_r$$

$\therefore$  By corollary 2 (p. 41),  $q_i = p_k$   
for some  $k$ ,  $1 \leq k \leq r$ .

After factoring out  $q_i$  and  $p_k$ ,  
we still have,

$$p_1 \cdots p_r = K q_1^{2k_1} \cdots q_s^{2k_s}, \text{ so that}$$

$q_i | p_1 \cdots p_r$ . But the original

factorization  $p_1 \cdots p_r$  was unique,  
and  $q_i$  was factored out.

$\therefore q_i$  can't divide the remaining  
factorization.  $\therefore n$  must be  
square free.

(b) Every  $n > 1$  is the product of a square free integer  
and a perfect square.

Pf: Let  $n = p_1^{k_1} \cdots p_s^{k_s}$  be the canonical form  
for  $n$ . If  $k_i$  is odd and  $k_i > 1$ , then  
 $k_i - 1$  is even. Let  $a = p_1^{k_1} p_2^{k_2} \cdots p_m^{k_m}$ ,

where  $1 \leq r_i \leq s$  and  $k_{r_i}$  is odd  
and  $k_{r_i} \geq 1$ .

Consider  $b = p_{r_1} \cdots p_{r_m}$ .

$$\therefore a = b p_{r_1}^{k_{r_1}-1} p_{r_2}^{k_{r_2}-1} \cdots p_{r_m}^{k_{r_m}-1}$$

Also,  $b$  is square free, by (a) above.

$$p_{r_i}^{k_{r_i}-1} = p_{r_i}^{2x_i} \text{ since each } k_{r_i}-1 \text{ is}$$

even. Let  $c = p_{r_1}^{x_1} \cdots p_{r_m}^{x_m}$

$$\therefore a = b c^2$$

Finally, let  $a/n = p_{t_1}^{k_{t_1}} \cdots p_{t_j}^{k_{t_j}}$ , where

all  $k_{t_i}$  are even since  $a/n$  has factored out all of the odd exponents in the canonical form of  $n$ .

By #15 above,  $a/n = d^2$

$$\therefore n = b c^2 d^2 = b (cd)^2,$$

where  $b$  is square free.

17.  $n = 2^k m$ ,  $n \neq 0$ ,  $k \geq 0$ ,  $m$  odd

Pf: Assume  $n > 0$  (if  $n < 0$ , choose  $k, m$  s.t.  $-n = 2^k m$ ,  $\therefore n = 2^k(-m)$ ).

If  $n$  is odd, choose  $k=0$ ,  $m=n$ .

If  $n$  is even, then  $n = 2^k$ . Note  $k < n$ .

If  $k_1$  is odd, choose  $k=1$ ,  $m=k_1$ .

If  $k_1$  is even, Then  $k_1 = 2k_2$ , so

$n = 2^2 k_2$ . Note  $k_2 < k_1$ .

Continue this process till  $k_i$  is odd.  $\therefore m = k_i$ ,  $k = i$ . Since  $k_{i+1} < k_i$ , this is a finite process (i.e., ultimately will reach 1 if no other odd integer reached by then).

18.	3, 53	47, 97	107, 157
	11, 61	53, 103	113, 163
	17, 67	59, 109	131, 181
	23, 73	83, 139	149, 199
	29, 79	101, 151	173, 223

19. If  $n > 0$  is square-full, then  $n = a^2 b^3$ ,  $a, b > 0$ .

Pf: Let  $n = p_1^{k_1} \dots p_r^{k_r}$ . Since  $n$  is square-full,  $k_i \geq 2$ .

Write  $p_1^{k_1} \dots p_r^{k_r} = q_{m_1}^{K_{m_1}} \dots q_{m_s}^{K_{m_s}} q_{n_1}^{K_{n_1}} \dots q_{n_t}^{K_{n_t}}$

where  $K_{m_i}$  are odd (so  $K_{m_i} \geq 3$ ), and

$K_{n_i}$  are even, such that

$K_{m_i} = k_j$  and  $K_{n_i} = k_w$  (i.e., writing

$n$  so that odd exponents listed first, even exponents listed last).

$$\therefore K_{n_i} = 2v_i, \text{ some } v_i$$

$$\begin{aligned}\therefore n &= q_{m_1}^{K_{m_1}} \cdots q_{m_s}^{K_{m_s}} \left( q_{n_1}^{2v_1} \cdots q_{n_T}^{2v_T} \right) \\ &= q_{m_1}^{K_{m_1}} \cdots q_{m_s}^{K_{m_s}} \left( q_{n_1}^{v_1} \cdots q_{n_T}^{v_T} \right)^2\end{aligned}$$

$$\therefore n = q_{m_1}^{K_{m_1}} \cdots q_{m_s}^{K_{m_s}} (x^2), X = q_{n_1}^{v_1} \cdots q_{n_T}^{v_T}$$

Since  $K_{m_i}$  is odd and  $\geq 3$ ,  $K_{m_i} - 3$  is even.

$$\therefore n = q_{m_1}^3 \cdots q_{m_s}^3 (q_{m_1}^{m_1-3} \cdots q_{m_s}^{m_s-3})(x^2)$$

$$\text{Let } m_i - 3 = 2w_i, q_{m_1} \cdots q_{m_s} = b, \quad$$

$$\therefore n = b^3 (q_{m_1}^{2w_1} \cdots q_{m_s}^{2w_s})(x^2). \text{ Let } y = q_{m_1}^{w_1} \cdots q_{m_s}^{w_s}$$

$$\therefore n = b^3 y^2 x^2. \text{ Let } a = yx,$$

$$\therefore n = a^2 b^3$$

### 3.2 The Sieve of Eratosthenes

Note Title

12/9/2004

1. Test all primes  $p \leq \sqrt{701}$  to see if 701 is prime.

$$\sqrt{701} = 26.5 \therefore \text{test } 2, 3, 5, 7, 11, 13, 17, 19, 23$$

All do not divide 701.  $\therefore 701$  is prime

$$\sqrt{1009} = 31.7, 1009 \text{ not divisible by } 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31.$$

101	102	103	104	105	106	107	108	109	110
111	112	113	114	115	116	117	118	119	120
121	122	123	124	125	126	127	128	129	130
131	132	133	134	135	136	137	138	139	140
141	142	143	144	145	146	147	148	149	150
151	152	153	154	155	156	157	158	159	160
161	162	163	164	165	166	167	168	169	170
171	172	173	174	175	176	177	178	179	180
181	182	183	184	185	186	187	188	189	190
191	192	193	194	195	196	197	198	199	200

$$14 < \sqrt{200} < 15, \therefore \text{stop at } p = 13$$

3. If  $p \nmid n$  for all primes  $p < \sqrt[3]{n}, n > 1$ , Then  $n$  is either prime or the product of two primes

Pf: Assume  $n$  is composite, and let  $n = p_1 p_2 \dots p_r$ , and assume  $r \geq 3$

Note:  $p_1$  not among primes  $p < \sqrt[3]{n}$ .  $\therefore p_1 \geq \sqrt[3]{n}$ ,  
 $p_2 \geq p_1 \geq \sqrt[3]{n}$ .

We know that  $1 < \sqrt[3]{n} < p_i \leq \sqrt{n}$

$$\therefore \sqrt[3]{n} \leq p_1 \leq \sqrt{n}$$

$$\sqrt[3]{n} < p_2 \leq \sqrt{n}$$

$$\sqrt[3]{n} < p_3 < \sqrt{n}$$

$$\therefore n = (\sqrt[3]{n})(\sqrt[3]{n})(\sqrt[3]{n}) < p_1 p_2 p_3 = n,$$

or  $n < n$ .  $\therefore r < 3$ , or  $r=2$  or  $r=1$ .

$\therefore n$  is either prime ( $r=1$ ) or  
is the product of two primes ( $r=2$ ).

4. (a)  $\sqrt{p}$  is irrational for any prime  $p$ .

Pf: Assume  $\sqrt{p} = \frac{r}{s}$ , some integers  $r, s$ .

Let  $d = \gcd(r, s)$ . Let  $r_p = \frac{r}{d}$ ,  $s_p = \frac{s}{d}$

$\therefore \gcd(r_p, s_p) = 1$ , by Corollary 1, p. 23

$$\text{Also } \frac{r}{s} = \frac{r_p}{s_p} \quad \therefore \sqrt{p} = \frac{r_p}{s_p}$$

$$\therefore p = \frac{r_p^2}{s_p^2}, \quad p s_p^2 = r_p^2 \quad \therefore p | r_p^2 \Rightarrow p | r_p$$

$$\therefore \text{Let } r_p = p x. \quad \therefore r_p^2 = p^2 x^2 = p s_p^2, \text{ or}$$

$$p x^2 = s_p^2. \quad \therefore p | s_p. \quad \therefore \gcd(r_p, s_p) \neq 1$$

$\therefore$  There doesn't exist integers  $r, s$  s.t.  
 $\sqrt[p]{a} = \frac{r}{s}$

(b)  $a > 0$ ,  $\sqrt[n]{a}$  rational, Then  $\sqrt[n]{a}$  is an integer.

Pf: Let  $\sqrt[n]{a} = \frac{r}{s}$ ,  $r, s$  integers, s.t.  
 $\text{gcd}(r, s) = 1$ .

Let  $r = p_1 \cdots p_x$ ,  $s = q_1 \cdots q_y$

$\therefore p_i \neq q_j$

$$\therefore (q_1^n \cdots q_y^n) a = p_1^n \cdots p_x^n$$

$\therefore p_1^n \cdots p_x^n \mid a \therefore$  Let  $a = (p_1^n \cdots p_x^n) z$

$$\therefore (q_1^n \cdots q_y^n)(p_1^n \cdots p_x^n) z = p_1^n \cdots p_x^n$$

$\therefore (q_1^n \cdots q_y^n) z = 1 \therefore q_j = 1$  for all  $j$ .

$\therefore s = 1 \therefore \frac{r}{s}$  is an integer.

(c) For  $n \geq 2$ ,  $\sqrt[n]{n}$  is irrational.

Pf: Suppose  $\sqrt[n]{n}$  is rational. From (b), it is an integer. Let  $\sqrt[n]{n} = a$ .

$\therefore n = a^n$ . But  $n < 2^n$ .

$\therefore a^n < 2^n$ , so  $a < 2$ , or  $a = 1$ .  
 $\therefore n = 1^n = 1$ , a contradiction.

5. Any composite 3-digit number must have a prime factor  $\leq 31$ .

Pf: 999 is largest 3-digit number.

$\sqrt{999} = 31.6\dots$  31 is prime, so if a is composite, largest prime divisor is  $\leq \sqrt{a}$ , so 31 is largest possible prime divisor.

C. Number of primes is infinite.

Pf: Assume only finite number:  $p_1, p_2, \dots, p_n$

Let A be the product of any r of these,

so  $A = p_{a_1} p_{a_2} \dots p_{a_r}$ ,  $a_i \in \{1, 2, \dots, n\}$

Consider  $B = p_1 p_2 \dots p_n / A$

$$= \frac{p_1 p_2 \dots p_n}{p_{a_1} p_{a_2} \dots p_{a_r}} = p_{b_1} p_{b_2} \dots p_{b_s}$$

where  $a_i \neq b_j$  (i.e., factoring out  $p_{a_i}$ ), so

$$\{p_{a_i}\} \cap \{p_{b_j}\} = \emptyset, \text{ and } \{p_{a_i}\} \cup \{p_{b_j}\} = \{p_1, p_2, \dots, p_n\}$$

So, A and B have no common factors.

Then each  $p_k$  of  $p_1, p_2, \dots, p_n$  divides either A or B, but not both.

Since  $A > 1$ ,  $B > 1$ , Then  $A+B > 1$ .  
A+B must have a prime factor,  $p_1$ ,  
and  $p \mid (A+B)$  is an integer, and  
 $p \in \{p_1, p_2, \dots, p_n\}$  since assuming finite primes

Suppose  $p \mid A$ .  $\therefore p^x = A+B$ , some x,  
and  $p^y = A$ , some y.  
 $\therefore p^x = p^y + B$ ,  $\therefore p^{(x-y)} = B$ , so  $p \mid B$ ,  
a contradiction.

7. Prove infinitely many primes using  $N = p! + 1$

Pf: Assume finitely many primes,  $p_n$  the largest.  
Consider  $N = p_1! + 1$

$$\therefore N = 1 \cdot 2 \cdots p_n + 1.$$

N must have a prime divisor  $p_k$ ,  $1 \leq k \leq n$ .  
Since assuming finite # primes.

And  $p_k \mid 1 \cdot 2 \cdot 3 \cdots p_n$  since  $p_k$  is one of  
the members of  $p_n!$ .

$\therefore p_k \mid (N - p_1 p_2 \cdots p_n)$ .  $\therefore p_k \mid 1, p_k = 1$ ,  
a contradiction.

8. Prove infinitude of primes using

$$N = p_2 \cdots p_n + p_1 p_3 \cdots p_n + \cdots + p_1 p_2 \cdots p_{n-1}$$

Pf: Assume finite # of primes  $p_1, p_2, \dots, p_n$

Consider  $g_k = p_1 p_2 \cdots p_n$ , s.t. each term  
 $p_i \neq g_k$ .

$$\therefore g_1 = p_2 p_3 \cdots p_n$$

$$g_2 = p_1 p_3 p_4 \cdots p_n$$

$$\vdots$$

$$g_n = p_1 p_2 p_3 \cdots p_{n-1}$$

$$\therefore p_k \nmid g_k$$

$$\text{Let } N = g_1 + g_2 + \cdots + g_n = \sum_{i=1}^n g_i$$

$N$  must have a prime divisor from  $p_1, \dots, p_n$ .  
Let  $p_k$  ( $1 \leq k \leq n$ ) be that prime divisor.

But since  $p_k | N$  and  $p_k | q_i$ , if  $k$ ,

Then  $p_k | (N - \sum_{i=1, i \neq k}^n q_i)$

But Then  $N - \sum_{i=1, i \neq k}^n q_i = q_k$

$\therefore p_k | q_k$ , a contradiction.

9. (a) if  $n > 2$ , Then  $\exists p$  s.t.  $n < p < n!$

Pf: For  $n > 2$ , clearly  $2n < n! = 1 \cdot 2 \cdots n$

From Bertrand's conjecture,  $\exists$  a prime  $p$   
s.t.  $n < p < 2n$   $\therefore n < p < 2n < n!$

Pf: (using author's hint)

For  $n > 3$ ,  $n < n! - 1 < n!$

If  $n! - 1$  is prime, we're done

If  $n! - 1$  is not prime, let  $p$  be  
a prime divisor.  $\therefore p < n! - 1$

Assume  $p \leq n$ . Then  $p$  is one of

The terms of  $1 \cdot 2 \cdot 3 \cdots n$ , so  $p | n!$   
 $\therefore p | n!$  and  $p | (n! - 1)$

$$\therefore p | n! - (n! - 1) = 1$$

$$\therefore p > n \quad \therefore n < p < n! - 1 < n!$$

(6). For  $n > 1$ , every prime divisor of  $n! + 1$   
is an odd integer  $> n$

Pf: First,  $n! + 1$  is odd, since  $n!$  is even, as it contains 2, and  $2x$  is even for all  $x$ .

$\therefore 2$  will never divide  $n! + 1$ , so  
every prime divisor of  $n! + 1$  is odd.

Now suppose every prime divisor  $p_i$  of  
 $n! + 1$  is s.t.  $p_i \leq n$ .

Let  $P = n! + 1$

Clearly,  $p_i | n!$ , since  $p_i$  is one of  
the members of  $n!$

Since  $p_i | P$ , Then  $p_i | (P - n!)$ , and

$P - n! = 1$ .  $\therefore p_i | 1$ , a contradiction

$\therefore p_i > n$

10. Let  $q_n$  be smallest prime s.t.  $q_n > P = p_1 p_2 \dots p_n + 1$   
 Show  $q_n - (p_1 p_2 \dots p_n)$  is prime for  $n = 1, 2, \dots, 5$

$$q_1: 2+1=3 \therefore q_1 = 5$$

$$q_2: 2 \cdot 3 + 1 = 7 \quad q_2 = 11$$

$$q_3: 2 \cdot 3 \cdot 5 + 1 = 31 \quad q_3 = 37$$

$$q_4: 2 \cdot 3 \cdot 5 \cdot 7 + 1 = 211 \quad q_4 = 223$$

$$q_5: 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 + 1 = 2311 \quad q_5 = 2333$$

$$\therefore q_1 - (p_1) = 5 - 2 = 3$$

$$q_2 - (p_1 p_2) = 11 - 6 = 5$$

$$q_3 - (p_1 p_2 p_3) = 37 - 30 = 7$$

$$q_4 - (p_1 p_2 p_3 p_4) = 223 - 210 = 13$$

$$q_5 - (p_1 p_2 p_3 p_4 p_5) = 2333 - 2310 = 23$$

11. Let  $d_n = p_{n+1} - p_n$ . Find five solutions to  $d_n = d_{n+1}$

$$d_1 = p_2 - p_1 = 3 - 2 = 1$$

$$d_2 = p_3 - p_2 = 5 - 3 = 2$$

$$d_3 = p_4 - p_3 = 7 - 5 = 2 \quad \therefore d_2 = d_3$$

$$d_4 = p_5 - p_4 = 11 - 7 = 4$$

$$d_5 = P_6 - P_5 = 13 - 11 = 2$$

$$d_6 = P_7 - P_6 = 17 - 13 = 4$$

$$d_7 = P_8 - P_7 = 19 - 17 = 2$$

$$d_8 = P_9 - P_8 = 23 - 19 = 4$$

$$d_9 = 29 - 23 = 6$$

$$d_{10} = 31 - 29 = 2$$

$$d_{11} = 37 - 31 = 6$$

$$d_{12} = 41 - 37 = 4$$

$$d_{13} = 43 - 41 = 2$$

$$d_{14} = 47 - 43 = 4$$

$$d_{15} = 53 - 47 = 6$$

$$d_{16} = 59 - 53 = 6 \quad \therefore d_{15} = d_{16}$$

$$51 - 59 = 2$$

$$67 - 61 = 6$$

:

$$157 - 151 = 6$$

$$163 - 157 = 6 \quad \therefore d_{35} = d_{37}$$

:

$$173 - 167 = 6$$

$$179 - 173 = 6 \quad \therefore d_{40} = d_{39}$$

:

$$211 - 199 = 12$$

$$223 - 211 = 12 \quad \therefore d_{47} = d_{46}$$

12. Let  $p_n$  be  $n$ -th prime number. Prove:

(a)  $p_n > 2n - 1$ , for  $n \geq 5$

Pf: For  $n=5$ ,  $p_5 = 11 > 2(5)-1 = 9$

Assume true for  $k$ :  $p_k > 2k - 1$

$$\therefore p_{k+1} + 2 > (2k-1) + 2 = 2(k+1) - 1$$

Since  $p_k + 1$  is even, Then next possible prime is  $p_k + 2$ .

$$\therefore p_{k+1} \geq p_k + 2$$

$$\therefore p_{k+1} > p_k + 2 > 2(k+1) - 1, \text{ so if}$$

assertion true for  $k$ , then it's true for  $k+1$ .

$\therefore$  True for all  $n \geq 5$

(b) None of  $P_n = p_1 p_2 \cdots p_n + 1$  is a perfect square.

Pf: First note that since  $p_1 = 2$ , Then  $p_1 p_2 \cdots p_n$  is even, so  $p_1 p_2 \cdots p_n + 1$  is odd.

By Division Algorithm,  $P_n = 4k+r$ ,  $r=0,1,2,3$   
But since  $P_n$  is odd,  $r=1,3$   
If  $r=1$ , Then  $p_1 p_2 \dots p_n + 1 = 4k+1$ , so

$$p_1 p_2 \dots p_n = 4k, \text{ so } p_2 p_3 \dots p_n = 2k$$

But  $p_2 \dots p_n$  is odd since all factors are  
odd, and  $2k$  is even.  
 $\therefore r \neq 1$ .

$$\therefore P_n = 4k+3 \text{ for all } n.$$

Suppose  $P_n = s^2$ , some  $s$ , and  $s^2 = 4k+3$

Since  $s^2$  is odd, so is  $s$ .  
 $\therefore s = 2a+1$ , some  $a$ .

$$\therefore s^2 = (2a+1)^2 = 4a^2 + 4a + 1 = 4k+3$$

$$\therefore 4a^2 + 4a = 4k+2$$

$$2a^2 + 2a = 2k+1$$

But  $2a^2 + 2a$  is even, and  $2k+1$  is odd.

$\therefore$  There is no  $s$  s.t.  $P_n = s^2$

(c)  $\frac{1}{p_1} + \frac{1}{p_2} + \dots + \frac{1}{p_n}$  is never an integer.

Pf: Let  $P = p_1 p_2 \dots p_n$ , and suppose

$$\frac{1}{p_1} + \frac{1}{p_2} + \dots + \frac{1}{p_n} = a, \text{ some integer } a.$$

$$\therefore \frac{P}{p_1} + \frac{P}{p_2} + \dots + \frac{P}{p_n} = a^P$$

For  $p_1, p_1 | a^P$  and  $p_1 | \frac{P}{p_2}, p_1 | \frac{P}{p_3}, \dots, p_1 | \frac{P}{p_n}$

$$\therefore p_1 | (P - p_2 - p_3 - \dots - p_n)$$

$$\therefore p_1 | \frac{P}{p_1} \Rightarrow p_1 | p_2 p_3 \dots p_n, \text{ a contradiction.}$$

Similar reasoning applies for  $p_2, \dots, p_n$

$\therefore$  No such integer  $a = \frac{1}{p_1} + \dots + \frac{1}{p_n}$  exists.

B. (a) If  $n|m$ , then  $R_n|R_m$

Pf: First prove Lemma:

If  $m = kn$ , then

$$x^m - 1 = (x^n - 1)(x^{(k-1)n} + x^{(k-2)n} + \dots + x^n + 1)$$

Pf: From problem #3, p. 7, we know that

$$a^k - 1 = (a-1)(a^{k-1} + a^{k-2} + \dots + a + 1)$$

$$\therefore \text{let } a = x^n$$

$$\therefore x^{kn} - 1 = (x^n - 1)(x^{n(k-1)} + x^{n(k-2)} + \dots + x^n + 1)$$

Since  $Kn = m$ ,

$$\therefore x^m - 1 = (x^{n(k-1)} + x^{n(k-2)} + \dots + x^n + 1)$$

Now  $R_n = \frac{(10^n - 1)}{9}$ ,  $R_m = \frac{(10^m - 1)}{9}$

$$\therefore \frac{R_m}{R_n} = \frac{10^m - 1}{10^n - 1} = \frac{10^{kn} - 1}{10^n - 1}$$

By The Lemma,  $10^{kn} - 1 = (10^n - 1)(10^{n(k-1)} + \dots + 10^n + 1)$

$$\begin{aligned} \therefore \frac{R_m}{R_n} &= \frac{(10^n - 1)(10^{n(k-1)} + \dots + 10^n + 1)}{10^n - 1} \\ &= (10^{n(k-1)} + \dots + 10^n + 1) \end{aligned}$$

$$\therefore n|m \Rightarrow R_n | R_m$$

(6) if  $d | R_n$  and  $d | R_m$ , Then  $d | R_{n+m}$

$$\text{Pf: } R_n = \frac{10^n - 1}{9}, R_m = \frac{10^m - 1}{9}$$

$$R_{n+m} = \frac{10^{n+m} - 1}{9} = \frac{10^n 10^m - 1}{9}$$

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

$$= \frac{10^m (10^n - 1) + 10^m - 1}{9}$$

$$= 10^m R_n + R_m$$

$$\therefore d | R_n \Rightarrow R_n = dr, \text{ some } r$$

$$d | R_m \Rightarrow R_m = ds, \text{ some } s$$

$$\begin{aligned} \therefore R_{n+m} &= 10^m R_n + R_m \\ &= 10^m dr + ds = d(10^m r + s) \end{aligned}$$

$$\therefore d | R_{n+m}$$

(C) If  $\gcd(n, m) = 1$ , Then  $\gcd(R_n, R_m) = 1$

Pf:  $\gcd(n, m) = 1 \Rightarrow 1 = an + bm$ , some  $a, b$ .

Let  $d = \gcd(R_n, R_m)$ .  $\therefore d | R_n, d | R_m$

Since  $n | an$ , Then  $R_n | R_{an}$  by (a)

Since  $m | bm$ , Then  $R_m | R_{bm}$  by (a)

Since  $d | R_n$  and  $R_n | R_{an}$ , Then  $d | R_{an}$

Since  $d | R_m$  and  $R_m | R_{bm}$ , Then  $d | R_{bm}$

$\therefore$  by (b)  $d | R_{an+bm}$

But  $R_{an+bm} = R_1 = 1$ .  $\therefore d | 1, \therefore d = 1$

14. Find prime factors of  $R_{10}$

Since  $2 | R_0$  and  $5 | R_0$ , Then by 13(a),  $R_2 | R_{10}$   
and  $R_5 | R_{10}$ .  $R_2 = 11$ ,  $R_5 = 41 \cdot 271$ .

$\therefore 11 \cdot 41 \cdot 271 | R_{10}$ . But  $\frac{R_{10}}{11 \cdot 41 \cdot 271} = 9091$ , a prime

$\therefore R_{10} = 11 \cdot 41 \cdot 271 \cdot 9091$

### 3.3 The Goldbach Conjecture

Note Title

12/27/2004

1. Verify 1949 and 1951 are twin primes.

From table of primes,  $p_{296} = 1949$ ,  $p_{297} = 1951$ .

Also,  $\sqrt{1951} = 44.2$ , and neither divisible by primes  $\leq 43$ .

2. (a).  $p_1, p_2$  twin primes, show  $n^2 = p_1 p_2 + 1$  for some  $n$ .

$$\text{Pf: } p_2 = p_1 + 2$$

$$\therefore p_1 p_2 + 1 = p_1(p_1 + 2) + 1$$

$$= p_1^2 + 2p_1 + 1 = (p_1 + 1)^2$$

$$\therefore \text{Let } n = p_1 + 1$$

(b) The sum of twin primes  $p, p+2$  is divisible by 12, assuming  $p > 3$ .

$$\text{Pf: Let } N = p + p + 2 = 2p + 2 = 2(p + 1)$$

Since  $p+1$  is even,  $p+1 = 2m$ , some  $m$ .

$$\therefore N = 4m, \therefore 4 | N.$$

Now let  $p = 3q + r$ ,  $r = 0, 1, 2$  by  
Div. Alg.

$r \neq 0$  since  $p$  is prime

If  $r = 1$ , Then  $p+2 = 3q+3$ , so  
 $3 | p+2$ . Since  $p+2$  is prime,  
 $r \neq 1$

$\therefore r = 2$ , and  $p = 3q + 2$

$$\therefore p+2 = 3q+4 = 3(q+1)+1$$

$$\begin{aligned}\therefore N = p + p+2 &= 3q+2 + 3(q+1)+1 \\ &= 3(2q+1) + 3\end{aligned}$$

$$\therefore 3 | N$$

$\therefore 3 | N$ ,  $4 | N$ , and since  $\gcd(3, 4) = 1$ ,  
 $3 \cdot 4 = 12 | N$  (corollary 2, p. 24).

$$\therefore 12 | p + (p+2)$$

3. Find all pairs of primes s.t.  $p - q = 3$ .

Pf: Since  $p = q+3$ , if  $q$  is odd,  $p$  is even.

And  $p > 3$ . But there is no even prime  $> 3$ .

$\therefore q$  is even, and  $\therefore q = 2$ .  $\therefore p = 5$ .

4. Every even integer  $2n \geq 4$  is the sum of two primes, one  $> n/2$ , the other  $< 3n/2$ .  
 Verify for integers  $6 \leq 2n \leq 76$

Test for  $3 \leq n \leq 38$

$2n$	$n$	$n/2$	$3n/2$
$6 = 3 + 3$	3	1.5	4.5
$8 = 3 + 5$	4	2	6
$10 = 3 + 7$	5	2.5	7.5
$12 = 5 + 7$	6	3	9
$14 = 7 + 7$	7	3.5	10.5
$16 = 5 + 11$	8	4	12
$18 = 7 + 11$	9	4.5	13.5
$20 = 7 + 13$	10	5	15
$22 = 11 + 11$	11	5.5	16.5
$24 = 11 + 13$	12	6	18
$26 = 13 + 13$	13	6.5	19.5
$28 = 11 + 17$	14	7	21
$30 = 11 + 19$	15	7.5	22.5
$32 = 13 + 19$	16	8	24
$34 = 11 + 23$	17	8.5	25.5
$36 = 13 + 23$	18	9	27
$38 = 19 + 19$	19	9.5	28.5
$40 = 17 + 23$	20	10	30

$42 = 19 + 23$	21	10.5	31.5
$44 = 13 + 31$	22	11	33
$46 = 17 + 29$	23	11.5	34.5
$48 = 19 + 29$	24	12	36
$50 = 19 + 31$	25	12.5	37.5
$52 = 23 + 29$	26	13	39
$54 = 23 + 31$	27	13.5	40.5
$56 = 19 + 37$	28	14	42
$58 = 29 + 29$	29	14.5	43.5
$60 = 29 + 31$	30	15	45
$62 = 31 + 31$	31	15.5	46.5
$64 = 23 + 41$	32	16	48
$66 = 23 + 43$	33	16.5	49.5
$68 = 31 + 37$	34	17	51
$70 = 23 + 47$	35	17.5	52.5
$72 = 29 + 43$	36	18	54
$74 = 31 + 43$	37	18.5	55.5
$76 = 29 + 47$	38	19	57

5. Every odd integer can be written as  $p + 2a^2$ ,  
 $p$  is prime or 1,  $a \geq 0$ . Show not true for 5777.

$$5777 = p + 2a^2, \quad a = \sqrt{\frac{5777 - p}{2}}$$

Minimum of  $p$  would be  $p = 2$ .

$\therefore$  Largest  $a$  would be  $\sqrt{\frac{5775}{2}} = 53.7$   
 Smallest  $a$  would be 0.

$\therefore$  Test  $0 \leq a \leq 53$ , or

test  $5777 - 2a^2$  for  
 $0 \leq a \leq 53$  and see if  
 it is prime.

From spreadsheet, left  
 column is  $a$ , middle  
 column is  $5777 - 2a^2$ , and  
 right column is a factor of  
 $5777 - 2a^2$ , showing  
 that the numbers are not  
 primes.

$\therefore$  No prime  $p$  exists s.t.

$$5777 = p + 2a^2$$

53	159	3
52	369	3
51	575	5
50	777	3
49	975	3
48	1169	7
47	1359	3
46	1545	3
45	1727	11
44	1905	3
43	2079	3
42	2249	13
41	2415	3
40	2577	3
39	2735	5
38	2889	3
37	3039	3
36	3185	5
35	3327	3
34	3465	3
33	3599	59
32	3729	3
31	3855	3
30	3977	41
29	4095	3
28	4209	3
27	4319	7
26	4425	3
25	4527	3
24	4625	5
23	4719	3
22	4809	3
21	4895	5
20	4977	3
19	5055	3
18	5129	23
17	5199	3
16	5265	3
15	5327	7
14	5385	3
13	5439	3
12	5489	11
11	5535	3
10	5577	3
9	5615	5
8	5649	3
7	5679	3
6	5705	5
5	5727	3
4	5745	3
3	5759	13
2	5769	3
1	5775	3
0	5777	53

6. Prove: (a) Every even integer  $> 2$  is the sum of two primes

$\Leftrightarrow$  (b) Every integer  $> 5$  is the sum of three primes

Pf: (a)  $\Rightarrow$  (b) Let  $N$  be any integer  $> 5$ .

If  $N$  is even, so is  $N-2$ , and  
 $N-2 > 3$ .  $\therefore$  by (a),

$$N-2 = p_1 + p_2, \therefore N = 2 + p_1 + p_2$$

If  $N$  is odd,  $N-3$  is even, and

$$N-3 > 2. \therefore \text{by (a)}, N-3 = p_1 + p_2,$$

$$\therefore N = 3 + p_1 + p_2.$$

$\therefore N$  is the sum of three primes.

(b)  $\Rightarrow$  (a) Let  $N$  be any even integer  $> 2$ .

Since  $4 = 2+2$ , let  $N \geq 6$ .

Consider  $N+2$ . From (b),  $N+2 > 5$ ,

$N+2 = p_1 + p_2 + p_3$ . Since  $N+2$  is even, not all of  $p_1, p_2, p_3$  is odd.

One of  $p_1, p_2, p_3$  must be even, and so one of  $p_1, p_2, p_3$  must be 2, the only even prime. Let it be  $p_1$ .

$$\therefore N+2 = 2 + p_2 + p_3, N = p_2 + p_3$$

7. Every odd integer  $> 5$  can be written as  $p_1 + 2p_2$   
 Confirm for all odd integers  $\leq 75$ .

Pf.	$7 = 3 + 2 \cdot 2$	$41 = 37 + 2 \cdot 2$
	$9 = 3 + 2 \cdot 3$	$43 = 29 + 2 \cdot 7$
	$11 = 5 + 2 \cdot 3$	$45 = 41 + 2 \cdot 2$
	$13 = 7 + 2 \cdot 3$	$47 = 37 + 2 \cdot 5$
	$15 = 11 + 2 \cdot 2$	$49 = 23 + 2 \cdot 13$
	$17 = 11 + 2 \cdot 3$	$51 = 29 + 2 \cdot 11$
	$19 = 13 + 2 \cdot 3$	$53 = 43 + 2 \cdot 5$
	$21 = 17 + 2 \cdot 2$	$55 = 29 + 2 \cdot 13$
	$23 = 17 + 2 \cdot 3$	$57 = 43 + 2 \cdot 7$
	$25 = 19 + 2 \cdot 3$	$59 = 37 + 2 \cdot 11$
	$27 = 23 + 2 \cdot 2$	$61 = 47 + 2 \cdot 7$
	$29 = 23 + 2 \cdot 3$	$63 = 59 + 2 \cdot 2$
	$31 = 17 + 2 \cdot 7$	$65 = 59 + 2 \cdot 3$
	$33 = 29 + 2 \cdot 2$	$67 = 53 + 2 \cdot 7$
	$35 = 29 + 2 \cdot 3$	$69 = 59 + 2 \cdot 5$
	$37 = 31 + 2 \cdot 3$	$71 = 67 + 2 \cdot 2$
	$39 = 29 + 2 \cdot 5$	$73 = 59 + 2 \cdot 7$
		$75 = 53 + 2 \cdot 11$

8.  $60 = p_1 + p_2$  in 6 ways

$60 = 53 + 7$	$60 = 43 + 17$	$60 = 37 + 23$
$60 = 47 + 13$	$60 = 41 + 19$	$60 = 31 + 29$

$78 = p_1 + p_2$  in 7 ways

$$78 = 73 + 5$$

$$78 = 61 + 17$$

$$78 = 41 + 37$$

$$78 = 71 + 7$$

$$78 = 59 + 19$$

$$78 = 67 + 11$$

$$78 = 47 + 31$$

$84 = p_1 + p_2$  in 8 ways

$$84 = 79 + 5$$

$$84 = 53 + 31$$

$$84 = 67 + 17$$

$$84 = 73 + 11$$

$$84 = 47 + 37$$

$$84 = 61 + 23$$

$$84 = 71 + 13$$

$$84 = 43 + 41$$

9. (a) For  $n > 3$ ,  $n, n+2, n+4$  cannot all be prime.

Pf: By Division Alg.,  $n$  can be expressed as

$$6g + r, \quad 0 \leq r \leq 5$$

$r \neq 0, 2, 4$ , for then  $n$  would be even.

$$\therefore r = 1, 3, 5$$

$r=1$ :  $n = 6g + 1$ , so  $n+2 = 6g+3$ , which is divisible by 3.  
 $\therefore r \neq 1$

$r=3$ :  $n = 6g + 3$ , but then  $3|n$ .  
so  $r \neq 3$ .

$r=5$ :  $n = 6g + 5$ , then  $n+4 = 6g+9$ ,  
so  $3|n+4$ .  $\therefore r \neq 5$ .

$\therefore$  for no value of  $r$  can all three numbers be prime.

(5) prime triplets :  $p, p+2, p+6$

$$5, 7, 11 \quad 41, 43, 47$$

$$11, 13, 17 \quad 101, 103, 107$$

$$17, 19, 23$$

10.  $(n+1)! - 2, (n+1)! - 3, \dots, (n+1)! - (n+1)$  produces  $n$  consecutive composite numbers.

Pf: For each  $k \leq n+1$ ,  $k$  is in the term  $(n+1)!$ , so that  $K \mid [(n+1)! - k]$

$$11. f(n) = n^2 + n + 17$$

$$g(n) = n^2 + 2n + 1$$

$$h(n) = 3n^2 + 3n + 23$$

Find smallest  $n$  for each function that makes value a composite.

$$f(16) = 289 = 17^2$$

$$g(18) = 703 = 19 \times 37$$

$$h(22) = 1541 = 23 \times 67$$

12. Let  $p_n$  be  $n^{th}$  prime number. For  $n \geq 3$ , prove

$$p_{n+3}^2 < p_n p_{n+1} p_{n+2}$$

Pf: From section 3.2,  $p_{n+1} < 2p_n$

$$\therefore p_{n+3} < 2p_{n+2}$$

$$\text{so } p_{n+3}^2 < 4p_{n+2}^2 < 4p_{n+2}(2p_{n+1}) = 8p_{n+2}p_{n+1}$$

$$\text{Since } p_5 = 11, 8p_{n+2}p_{n+1} < p_5 p_{n+2}p_{n+1}$$

$$\therefore p_{n+3}^2 < p_n p_{n+1} p_{n+2} \text{ if } n \geq 5$$

$$\text{For } n=4, p_7^2 = 17^2 = 289 < p_4 p_5 p_6 = 7 \cdot 11 \cdot 13 = 1001$$

$$n=3: p_6^2 = 13^2 = 169 < p_3 p_4 p_5 = 5 \cdot 7 \cdot 11 = 385$$

$$n=2: p_5^2 = 11^2 = 121 < p_2 p_3 p_4 = 3 \cdot 5 \cdot 7 = 105$$

$$\therefore \text{for } n \geq 3, p_{n+3}^2 < p_n p_{n+1} p_{n+2}$$

13. There are infinitely many primes of form:  $Gn + 5$

Pf: Assume only finite number of primes of form  $Gn + 5$ . Let these be  $q_1, q_2, q_3, \dots, q_s$

Consider  $N = Gq_1q_2 \dots q_s - 1 = G(q_1q_2 \dots q_s - 1) + 5$

Let  $N = r_1r_2 \dots r_t$  be the prime factorization.  
Since  $N$  is odd,  $r_i \neq 2$ , so each  $r_i$  can only  
be of form  $6n+1$ ,  $6n+3$ , or  $6n+5$ .

$$\begin{aligned} \text{Since } (6n+1)(6m+1) &= 36nm + 6m + 6n + 1 \\ &= G(6nm + m + n) + 1 \end{aligned}$$

product of two integers of  $6n+1$  form is  
same form.

$$\begin{aligned} \text{Since } (6n+3)(6m+3) &= 36nm + 18m + 18n + 9 \\ &= G(6nm + 3m + 3n + 3) + 3 \end{aligned}$$

product of two integers of  $6n+3$  form is  
same form.

$$\begin{aligned} \text{Since } (6n+1)(6m+3) &= 36nm + 6m + 18n + 3 \\ &= G(6nm + m + 3n) + 3 \end{aligned}$$

product of two integers of  $6n+1$  form  
and  $6n+3$  form is of  $6n+3$  form.

So, the only way for  $N$  to be of form  
 $6n+5$ , of which it is,  $N$  must contain  
at least one factor  $r_i$  of form  $6n+5$ .  
But can't find such a prime among

the  $q_1, q_2, \dots, q_s$ . If such a prime

existed, Then from construction of  
 $N$ ,

$$N - 6q_1q_2\dots q_s = -1, \text{ both}$$

terms on left side would be divisible  
by this prime of  $6n+5$  form, so  
 $-1$ , and thus,  $1$ , would be divisible  
by this prime, a contradiction.

$\therefore$  Can't be finite # of primes of  $6n+5$   
form.

14.  $4(3 \cdot 7 \cdot 11) - 1 = 13 \times 71$ ,  $71$  is of form  $4n+3$

$$4(3 \cdot 7 \cdot 11 \cdot 15) - 1 = 13,859, \text{ a prime of form } 4n+3$$

15. Five consecutive odd integers, 4 of which are prime.

$$3, 5, 7, 9, 11$$

$$11, 13, 15, 17, 19$$

$$19, 193, 195, 197, 199$$

$$5, 7, 9, 11, 13$$

$$101, 103, 105, 107, 109$$

16.  $23 = p_9 = p_{2 \cdot 4 + 1} = 2p_{2 \cdot 4} + \sum_{k=0}^{2 \cdot 4 - 1} e_k p_k$

$$= 2\rho_8 + \sum_{K=0}^7 \epsilon_k \rho_K$$

$$\therefore 23 = 2\cdot 19 + \epsilon_0 + 2\epsilon_1 + 3\epsilon_2 + 5\epsilon_3 + 7\epsilon_4 + 11\epsilon_5 + 13\epsilon_6 + 17\epsilon_7$$

$$= 38 + 1 + 2 + 3 + 5 - 7 + 11 - 13 - 17$$

$$= 38 + (2-17) + (1+3+5) + (-7+11-13)$$

$$= 38 - 15 + 9 - 9$$

$$29 = \rho_{10} = \rho_{2\cdot 5} = \rho_{2\cdot 5-1} + \sum_{K=0}^{2\cdot 5-2} = 23 + \sum_{K=0}^8 \epsilon_k \rho_K$$

$$= 23 + \epsilon_0 + 2\epsilon_1 + 3\epsilon_2 + 5\epsilon_3 + 7\epsilon_4 + 11\epsilon_5 + 13\epsilon_6 + 17\epsilon_7 + 19\epsilon_8$$

$$= 23 + 6 + 12 + 6 - 6$$

$$= 23 + (1+2+3) + (5+7) + (-11+17) + (13-19)$$

$$= 23 + 1 + 2 + 3 + 5 + 7 - 11 + 17 + 13 - 19$$

$$31 = \rho_{11} = \rho_{2\cdot 5+1} = 2\rho_{2\cdot 5} + \sum_{K=0}^{2\cdot 5-1} \epsilon_k \rho_K = 2\cdot 29 + \sum_{K=0}^9 \epsilon_k \rho_K$$

$$= 2 \cdot 29 + \epsilon_0 + 2\epsilon_1 + 3\epsilon_2 + 5\epsilon_3 + 7\epsilon_4 + 11\epsilon_5 + 13\epsilon_6 + 17\epsilon_7 +$$

$$31 = 5 \cdot 8 - 27, \text{ so find } -27$$

$$19\epsilon_8 + 23\epsilon_9$$

$$\begin{aligned} -27 &= 0 - 8 + (-11 - 4 \cdot 4) \\ &= (2+3-5) + (-(-7)) + (-11-4-4) \end{aligned}$$

$$\therefore -31 = 2 \cdot 29 - 1 + 2 + 3 - 5 - 7 - 11 + 13 - 17 + 19 - 23$$

$$37 = p_{12} = p_{2-6} = p_{2 \cdot 6 - 1} + \sum_{K=0}^{2 \cdot 6 - 2} \epsilon_k p_k = 31 + \sum_{K=0}^{10} \epsilon_k p_k$$

$$= 31 + \epsilon_6 + 2\epsilon_1 + 3\epsilon_2 + 5\epsilon_3 + 7\epsilon_4 + 11\epsilon_5 + 13\epsilon_6 + 17\epsilon_7 +$$

$$19\epsilon_8 + 23\epsilon_9 + 29\epsilon_{10}$$

$$\begin{aligned} 37 &= 31 + 6 = 31 + 6 + (-2 + -2 + -42) + 46 \\ &= 31 (1+2+3) + (5-7+11-13-19-23) + (17+29) \end{aligned}$$

$$\therefore 37 = 31 + 1 + 2 + 3 + 5 - 7 + 11 - 13 + 17 - 19 - 23 + 29$$

17. Show 509 and 877 can't be the sum of a prime and power of 2.

From spreadsheet,  
 1st column is  $n$ ,  
 2nd column is  $2^n$ ,  
 3rd column is  $509 - 2^n$   
 4th column is  $877 - 2^n$   
 None of the positive entries  
 in 3rd or 4th cols. is prime.

0	1	508	876
1	2	507	875
2	4	505	873
3	8	501	869
4	16	493	861
5	32	477	845
6	64	445	813
7	128	381	749
8	256	253	621
9	512	-3	365
10	1024	-515	-147

18. (a).  $p$  prime,  $p \nmid b$ , show every  $p$ th term in  
 $a, a+b, a+2b, \dots$  is divisible by  $p$ .

Better restatement: there is a term within  
 the first  $p$  terms that is divisible by  $p$ , and  
 every  $p$ th term thereafter is divisible by  $p$ .  
 (because the  $p$ th term from the beginning is not  
 always divisible by  $p$ ).

Pf: Since  $p \nmid b$ , and  $p$  is prime,  $\gcd(p, b) = 1$ .

$\therefore$  There exist integers  $r, s$  s.t.  $pr + bs = 1$  [1]

Consider  $n_k = kp - qs$ ,  $k = 1, 2, 3, \dots$

For  $k=1$ ,  $n_1 = p - qs$ , and clearly  $n_1 < p$ .  
 Note that  $n_2$  is the  $p$ th term after  $n_1$ ,  
 $n_3$  the  $p$ th term after  $n_2$ , etc.

$$\begin{aligned}
 a + n_k b &= a + (kp - as)b = a + kp b - abs \\
 &= a(1 - bs) + kp b \\
 &= a(pr) + kp b \quad (\text{using } [1])
 \end{aligned}$$

$\therefore p \mid a + n_k b$ , so there is a term

within the first  $p$  terms that is divisible by  $p$ , and every  $p$ th term after that is divisible by  $p$ .

(5) if  $b$  is odd in  $a, a+b, a+2b, \dots$

Then since  $2 \nmid b$  and 2 is prime,  
 by (a) either  $a$  or  $abs$  is divisible by  
 $2$ , and every 2nd term is also.  
 So every other term is even.

$$\begin{array}{ll}
 19. \quad 25 = 5 + 7 + 13 & 81 = 3 + 5 + 73 \\
 69 = 3 + 5 + 61 & 125 = 5 + 7 + 113
 \end{array}$$

20. If  $p$  and  $p^2 + 8$  are both prime, then  $p^3 + 4$  is prime.

Pf: As in prob. # 4 of Problem 3-1, if  $p > 3$  is prime it is of form  $6k+1$  or  $6k+5$ .

$$\therefore p^2 + 8 = 36k^2 + 12k + 9, \text{ or } 36k^2 + 60k + 33$$

$$\text{But } 3 \mid (36k^2 + 12k + 9)$$

$$\text{And } 3 \mid (36k^2 + 60k + 33)$$

So  $p^2 + 8$  is not prime if  $p > 3$ .

$$\therefore p = 3$$

$$p^2 + 8 = 17$$

$$p^3 + 4 = 31$$

21. (a). Let  $k > 0$  be any integer, and let  $a, b$  be integers with  $\gcd(a, b) = 1$ . Prove the series,

$a+b, a+2b, a+3b, \dots$  contains  $k$  consecutive composite terms.

Pf: Let  $k$  be any integer, and let  $n$  be the integer formed by:

$$n = (a+b)(a+2b) \dots (a+kb)$$

Consider the series of  $k$  terms :

$$a+(n+1)b, a+(n+2)b, \dots, a+(n+k)b$$

For the " $i$ "th term, ( $1 \leq i \leq k$ )

$$a+(n+i)b =$$

$$a + nb + i\delta = a + ib + n\delta$$

But  $n$  contains  $(a+ib)$  as one of its terms by definition of  $n$ .

$$\therefore (a+ib) \mid (a+(n+i)\delta) \text{ for all } i$$

$$\text{For } k \geq 2, a+ib < a+(n+i)\delta$$

For  $k=1$ ,  $n=a+\delta$ , and the " $i$ "th term of our series is  $a+(a+\delta+1)\delta =$

$$a+a\delta+\delta^2+\delta = a(1+\delta)+\delta(\delta+1) \\ = (a+\delta)(\delta+1)$$

$$\therefore a+\delta < a+(a+\delta+1)\delta$$

$$\therefore \text{for } k \geq 1, a+ib < a+(n+i)\delta$$

Also,  $1 < a+ib$  for all  $i$ .

$\therefore$  all  $K$  terms of  $a+(n+1)\delta, \dots, a+(n+k)\delta$  are divisible by an integer that is  $> 1$  and  $<$  the term.

$\therefore$  all  $K$  terms are composite.

Note: proof doesn't use  $\gcd(a, \delta) = 1$ .  
It does assume  $a, \delta \neq 0$ .

(b) From our construction, let

$$n = (6+5)(6+2 \cdot 5)(6+3 \cdot 5)(6+4 \cdot 5)(6+5 \cdot 5)$$

$$= 2978976$$

$$\begin{aligned} \therefore 6+(n+1)5 &= 14,894,891 \quad \div 6+5 = 11 \\ 6+(n+2)5 &= 14,894,896 \quad \div 6+2 \cdot 5 = 16 \\ 6+(n+3)5 &= 14,894,901 \quad \div 21 \\ 6+(n+4)5 &= 14,894,906 \quad \div 26 \\ 6+(n+5)5 &= 14,894,911 \quad \div 31 \end{aligned}$$

$\therefore$  The above 5 consecutive terms are composite.

22. Show 13 is largest prime that can divide two successive integers of form  $n^2 + 3$

Pf: First, look at first possibilities for  $n$

$n$	$n^2 + 3$	prime fac.	$n$	$n^2 + 3$	prime fac
0	3	3	9	84	$2^2 \times 3 \times 7$
1	4	$2^2$	10	103	103
2	7	7	11	124	$2^2 \times 31$
3	12	$2^2 \times 3$	12	147	$3 \times 7^2$
4	19	19	13	172	$2^2 \times 43$
5	28	$2^2 \times 7$	14	199	199
6	39	$3 \times 13$	15	228	$2^2 \times 3 \times 19$
7	52	$2^2 \times 13$	16	259	$7 \times 37$
8	67	67			

It seems that after  $n \geq 8$ , there are no common factors for adjacent terms.

Adjacent terms are  $n^2 + 3$

$$(n+1)^2 + 3 = n^2 + 2n + 4$$

Use Euclid's algorithm to find gcd for  $n \geq 8$

$\therefore$  Suppose 1st term is even, i.e.,  $n = 2s$ , and  $s \geq 4$

$$\therefore \text{terms are } (2s)^2 + 3 = 4s^2 + 3$$

$$(2s+1)^2 + 3 = 4s^2 + 4s + 4$$

$$4s^2 + 4s + 4 = 1 \cdot (4s^2 + 3) + 4s + 1 \quad 4s + 1 < 4s^2 + 3$$

$$4s^2 + 3 = s(4s+1) - s + 3 \quad \text{but } -s + 3 < 0 \text{ for } s \geq 4$$

$$\therefore 4s^2 + 3 = (s-1)(4s+1) + 3s + 4 \quad \text{and for } s \geq 4, 4s+1 > 3s+4$$

$$4s+1 = 1 \cdot (3s+4) + s-3 \quad 3s+4 > s-3, \text{ for } s \geq 4$$

$$3s+4 = 3 \cdot (s-3) + 13 \quad (*)$$

$$\gcd(s-3, 13) = 13 \text{ or } 1$$

So  $\gcd = 1, 13$  if  $s-3 > 13$ , or  $s > 16$

So, must prove  $\gcd = 1, 13$  for  $4 \leq s \leq 16$  for  $(*)$

So  $(*)$  becomes for each  $s$ :

$$3s+4 = a(s-3) + r$$

$$\therefore s=4 : 16 = 16 \cdot 1 \quad \gcd = 1$$

$$s=5 : 19 = 9 \cdot 2 + 1, \quad 2 = 2 \cdot 1, \quad \gcd = 1$$

$$\begin{aligned}
 s=6 : \quad 22 &= 7 \cdot 3 + 1, \quad 3 = 3 \cdot 1, \quad \gcd = 1 \\
 s=7 : \quad 25 &= 6 \cdot 4 + 1, \quad 4 = 4 \cdot 1, \quad \gcd = 1 \\
 s=8 : \quad 28 &= 5 \cdot 5 + 3, \quad 5 = 1 \cdot 3 + 2, \quad 3 = 1 \cdot 2 + 1, \quad 2 = 2 \cdot 1, \quad \gcd = 1 \\
 s=9 : \quad 31 &= 5 \cdot 6 + 1, \quad 6 = 6 \cdot 1, \quad \gcd = 1 \\
 s=10 : \quad 34 &= 4 \cdot 7 + 6, \quad 7 = 1 \cdot 6 + 1, \quad 6 = 6 \cdot 1, \quad \gcd = 1 \\
 s=11 : \quad 37 &= 4 \cdot 8 + 5, \quad 8 = 1 \cdot 5 + 3, \quad \gcd = 1 \\
 s=12 : \quad 40 &= 4 \cdot 9 + 4, \quad 9 = 2 \cdot 4 + 1, \quad \gcd = 1 \\
 s=13 : \quad 43 &= 4 \cdot 10 + 3, \quad 10 = 3 \cdot 3 + 1, \quad \gcd = 1 \\
 s=14 : \quad 46 &= 4 \cdot 11 + 2, \quad 11 = 5 \cdot 2 + 1, \quad \gcd = 1 \\
 s=15 : \quad 49 &= 4 \cdot 12 + 1, \quad 12 = 12 \cdot 1, \quad \gcd = 1 \\
 s=16 : \quad 52 &= 4 \cdot 13 \quad \gcd = 13
 \end{aligned}$$

$\therefore$  Examples show  $\gcd = 1$  or  $\gcd = 13$  for adjacent terms  $6 \leq n \leq 16$ , and above shows  $\gcd = 1$  or  $\gcd = 13$  for all  $n$ , if 1st term is even.

Now suppose first term is odd, i.e.,  $n = 2s + 1$ , and  $s \geq 4$

$$\begin{aligned}
 \therefore (2s+1)^2 + 3 &= 4s^2 + 4s + 4 \\
 (2s+2)^2 + 3 &= 4s^2 + 8s + 7
 \end{aligned}$$

$$\begin{aligned}
 4s^2 + 8s + 7 &= 1 \cdot (4s^2 + 4s + 4) + 4s + 3 \\
 4s^2 + 4s + 4 &= s(4s+3) + s + 4 \quad 4s+3 > s+4 \text{ for } s \geq 4
 \end{aligned}$$

$$4s+3 = 3(s+4) + s-9 \quad (*) \quad 0 < s-9 < s+4 \quad \text{if } s > 9$$

$$s+4 = 1 \cdot (s-9) + 13 \quad 13 < s-9, \text{ if } 22 < s$$

$$\gcd(s-9, 13) = 1 \text{ or } 13$$

$\therefore \gcd = 1$  if  $s > 22$ , and so must test (\*)  
for  $4 \leq s \leq 22$ . (\*) becomes

$$4s+3 = a(s+4) + r$$

$$s=4 : 19 = 2 \cdot 8 + 3, 8 = 2 \cdot 3 + 2, 3 = 1 \cdot 2 + 1 \quad \gcd = 1$$

$$s=5 : 23 = 2 \cdot 9 + 5, 9 = 1 \cdot 5 + 4, 5 = 4 + 1, \gcd = 1$$

$$s=6 : 27 = 2 \cdot 10 + 7 \quad \gcd = 1$$

$$s=7 : 31 = 2 \cdot 11 + 9 \quad \gcd = 1$$

$$s=8 : 35 = 2 \cdot 12 + 11 \quad \gcd = 1$$

$$s=9 : 39 = 3 \cdot 13 \quad \gcd = 13$$

$$s=10 : 43 = 3 \cdot 14 + 1 \quad \gcd = 1$$

$$s=11 : 47 = 3 \cdot 15 + 2 \quad \gcd = 1$$

$$s=12 : 51 = 3 \cdot 16 + 3 \quad \gcd = 1$$

$$s=13 : 55 = 3 \cdot 17 + 4 \quad \gcd = 1$$

$$s=14 : 59 = 3 \cdot 18 + 5 \quad \gcd = 1$$

$$s=15 : 63 = 3 \cdot 19 + 6 \quad \gcd = 1$$

$$s=16 : 67 = 3 \cdot 20 + 7 \quad \gcd = 1$$

$$s=17 : 71 = 3 \cdot 21 + 8 \quad \gcd = 1$$

$$s=18 : 75 = 3 \cdot 22 + 9 \quad \gcd = 1$$

$$s=19 : 79 = 3 \cdot 23 + 10, \quad \gcd = 1$$

$$s=20 : 83 = 3 \cdot 24 + 11 \quad \gcd = 1$$

$$s=21 : 87 = 3 \cdot 25 + 12, 25 = 2 \cdot 12 + 1, \quad \gcd = 1$$

$$s=22 : 91 = 3 \cdot 26 + 13, \quad \gcd = 13$$

$\therefore$  for  $4 \leq s \leq 22$ ,  $\gcd > 1$  or  $\gcd = 13$   
 for  $s > 22$ ,  $\gcd = 1$  or  $13$   
 $\therefore$  For all  $s \geq 4$ ,  $\gcd = 1$  or  $13$   
 $\therefore$  for all terms of  $n^2 + 3$ ,  $(n+1)^2 + 3$  beginning  
 with  $n$  odd and  $n \geq 9$ ,  $\gcd = 1$  or  $13$ .

$\therefore$  for all  $n \geq 0$ , adjacent terms have  
 gcd of 1 or 13

Note: it would have been difficult to  
 start with

$$n^2 + 2n + 4 = (n^2 + 3) + 2n + 1$$

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

This approach is not fruitful.

23. (a) Twin primes with a triangular mean

Some triangular numbers:  $1+2=3$ ,  $1+2+3=6$ ,  
 $1+2+3+4=10$ ,  $10+5=15$ ,  $15+6=21$ ,  $21+7=28$   
 $19, 23$  are adjacent but not twin primes.

$(5+7)/2 = 6$ , so 5, 7 work. Suppose  $p > 7$ .

From problem #1(a), sec. 1.3, a number is  
 triangular  $\Leftrightarrow$  it is of form  $n(n+1)/2$

$$\therefore (\rho + \rho + 2)/2 = n(n+1)/2$$

$$\therefore 2\rho + 2 = n^2 + n, \quad 2\rho = n^2 + n - 2 = (n+2)(n-1)$$

Since  $2\rho$  is even, one of  $n+2$  or  $n-1$  must be even.

$$\text{Suppose } n-1 = 2K. \quad \therefore n+2 = 2K+3$$

$$\therefore 2\rho = (2K+3)(2K)$$

$$\rho = (2K+3)(K)$$

For  $\rho$  to be prime,  $K=1, \therefore \rho=5$

$$\text{Suppose } n+2 = 2K. \quad \therefore n-1 = 2K-3$$

$$\therefore 2\rho = 2K(2K-3)$$

$$\rho = K(2K-3)$$

$$\therefore 2K-3 = 1, K=2, \text{ or}$$

$$K=1, 2K-3 = -1.$$

$$\therefore n+2 \neq 2K.$$

So, only possible twin primes are 5, 7.

(6) Twin primes with square mean.

$$\text{Suppose: } (\rho + \rho + 2)/2 = n^2$$

$$\therefore \rho + 1 = n^2, \quad \rho = n^2 - 1 = (n+1)(n-1)$$

For  $p$  to be prime,  $n-1=1$ ,  $\therefore n=2$   
 $\therefore \sqrt{2}=4$

$\therefore$  Only possibility is 3, 5

24. Determining all twin primes  $p$  and  $q=p+2$  for which  $pq-2$  is prime.

Pf: 3, 5 :  $3 \cdot 5 - 2 = 13$

Suppose  $p > 3$ . All primes  $> 3$  are of form  $6K+1$  or  $6K+5$ . But  $p$  must be of form  $6K+5$  since  $6K+1+2 = 6K+3 = 3(2K+1)$ .

$\therefore$  Let  $p = 6K+5$ ,  $q = 6K+7$

$$\begin{aligned}\therefore (6K+5)(6K+7)-2 &= 36K^2 + 72K + 35 - 2 \\ &= 36K^2 + 72K + 33 \\ &= 3(12K^2 + 24K + 11)\end{aligned}$$

$\therefore$  if  $p > 3$ , there are no twin primes such that  $pq-2$  is prime.  
3, 5 is the only pair.

25. Let  $p_n$  be  $n$ th prime. For  $n \geq 3$ , show  
 $p_n < p_1 + p_2 + \dots + p_{n-1}$

$$\text{Pf: } p_3 = 5 = 2 + 3 = p_1 + p_2$$

$$p_4 = 7 < 2 + 3 + 5 = p_1 + p_2 + p_3$$

$\therefore$  Assume for  $k \geq 4$ ,

$$p_k < p_1 + p_2 + \dots + p_{k-1}$$

$$\therefore 2p_k < p_1 + \dots + p_{k-1} + p_k$$

By Bertrand's conjecture,  $\exists p$  s.t.  
 $p_k < p < 2p_k$

$$\text{But } p_k < p_{k+1} \leq p$$

$$\therefore p_{k+1} \leq p < 2p_k < p_1 + \dots + p_{k-1} + p_k$$

$\therefore$  true for  $k+1$

$\therefore$  True for all  $n \geq 4$

2C. (a) Infinitely many primes ending in 33.

Pf:  $100 = 2^2 \times 5^2$  and  $33 = 3 \times 11$  are relatively prime.

$\therefore$  By Dirichlet's Theorem, The series  
 $33, 33+100, 33+2 \cdot 100, \dots$   
 $= 33, 133, 233, \dots$  contains infinitely  
many primes.

(6) Infinitely many primes which do not belong  
to any pair of twin primes.

Pf: 5 and 21 =  $3 \cdot 7$  are relatively prime.  
 $\therefore$  By Dirichlet's Theorem, The series,

$$5 + 21k, \text{ for } k = 1, 2, 3, \dots$$

contains infinitely many primes.

Let  $p$  be one such prime.

$\therefore$  For some  $K$ ,  $p = 5 + 21K$ .

$$\therefore p+2 = 7 + 21K = 7(1+3K)$$

$$p-2 = 3 + 21K = 3(1+7K).$$

$\therefore p+2$  and  $p-2$  can't be prime.

$\therefore$  all The primes contained in  
 $5 + 21k$  cannot be members of  
twin primes.

(c) There exists a prime ending in as many consecutive 1's as desired.

Pf:  $R_n = (10^n - 1)/9$  by def.

Since  $1 \cdot 10^n - 9 \cdot R_n = 1$ ,  $\gcd(10^n, R_n) = 1$   
∴ Using Dirichlet's Theorem, form the series

$$10^n \cdot k + R_n, \quad k=1, 2, 3, \dots$$

which is for  $n=1$ : 11, 21, 31, ...

$n=2$ : 111, 211, 311, ...

Each contains infinitely many primes.  
∴ each contains at least one prime ending in  $n$ 's.

(d) There are infinitely many primes that contain but do not end in the block of digits 123456789.

Pf: Consider  $10^n = 2^n \times 5^n$

The number 1234567891 is odd, so contains no factor of 2, and does not end in 0 or 5, so contains no factor of 5.

∴  $10^n$  and 1234567891 are relatively prime.

$\therefore$  By Dirichlet's theorem, The series

$10^n \cdot K + 1234567891$  contains infinitely many primes, and each number in the series contains 123456789 but ends in 1.

A few numbers in the series are:

11234567891, 21234567891, 31234567891, ...

27. For every  $n \geq 2$ , There exists a prime  $p \leq n < 2p$ .

Pf: Suppose  $n$  is odd.  $\therefore \exists K$  s.t.  $n = 2K+1$ , and since  $n \geq 2$ ,  $K \geq 1$ .

By Bertrand's conjecture, There is a prime  $p$  s.t.  $K < p < 2K$ .

$$\therefore p < p+1 < 2K+1 = n, \text{ so } p < n$$

$$\text{Also, } 2K < 2p, \text{ so } 2K+1 \leq 2p$$

$\therefore n \leq 2p$ . But  $2K+1$  is odd, and

$2p$  is even.  $\therefore n < 2p$

$\therefore \exists a p$  s.t.  $p < n < 2p$

Suppose  $n$  is even.  $\therefore \exists K$  s.t.  $n = 2K$ ,  $K \geq 1$

By Bertrand's conjecture, There is a prime  $p$  s.t.  $K < p < 2K = n$ , so  $p < n$

$$\begin{aligned}\therefore n = 2k < 2p, \text{ so } n < 2p \\ \therefore p < n < 2p\end{aligned}$$

28. (a) If  $n \geq 1$ , show that  $n!$  is never a perfect square.

ff: Lemma 1: If  $p_1 < p_2$  are adjacent primes,

Then if  $p_1 < N < p_2$ , Then  
The prime factors of  $N$  are  
(less than  $p_1$  (for  $p_1 > 3$ )).

pf: Let  $q_1 q_2 \dots q_r = N$ ,  $r \geq 2$ . Suppose  $q_i = p_i$  some i.

Since  $q_i \geq 2$  for all i,  $N = q_1 \dots q_r \geq p_i 2^{r-1}$

$$\therefore N = q_1 \dots q_r \geq p_i \cdot 2 \cdot 2^{r-2} > p_2$$

Since  $2p_1 > p_2$  (top p. 50, a  
direct consequence of Bertrand  
conjecture).  $\therefore N > p_2$ ,  
a contradiction.

Lemma 2: Let  $q_1^{k_1} q_2^{k_2} \dots q_r^{k_r}$  be the prime  
canonical factorization of  $n!$   
Then  $k_r = 1$  for all  $n \geq 2$ .

Pf: Clearly true for  $n=2, n=3$ .

Let  $N$  be any integer  $\geq 3$

Suppose true for  $N!$

$$\therefore N! = q_1^{k_1} \dots q_{r-1}^{k_{r-1}} q_r \quad (q_i < q_r)$$

Since each term of  $N!$  is  $< N$ , Then the prime factors of each term (which are  $<$  each term) are  $< N$ .  $\therefore q_i < N$ , and so  $q_r < N$ .

$$\text{Consider } (N+1)! = N! (N+1)$$

If  $N+1$  is prime, then  $q_r < N+1$ .

$$\therefore (N+1)! = q_1^{k_1} \dots q_{r-1}^{k_{r-1}} q_r (N+1)$$

$\therefore$  Lemma true

Suppose  $N+1$  is not prime.

Then  $q_r$  must be largest prime  $\leq N+1$ . If a larger prime existed, it would be a term in  $(N+1)!$ , and  $\therefore$  would be represented in the prime factorization:  $q_1^{k_1} \dots q_{r-1}^{k_{r-1}} q_r$

By Lemma 1 above, prime factors of  $N+1$  are  $< g_r$ .  
 $\therefore g_r$  remains largest prime factor and it has exponent 1.

$\therefore$  Lemma true for  $N+1$  when true for  $N$ .

Back to main problem:

$\therefore$  The prime factorization of  $n!$  has exponent 1 for largest factor.

$\therefore$  If  $n! = a^2$ , some  $a$ , all prime factors would have even exponents, as would the last factor.

$\therefore n! \neq a^2$  for any  $n \geq 2$ .

Note: By Lemma 2,  $n!$  can't be any power of any number.

(6). Find values of  $n \geq 1$  for which  $n! + (n+1)! + (n+2)!$  is a perfect square.

$$\begin{aligned}
 n! + (n+1)! + (n+2)! &= n! [1 + (n+1) + (n+1)(n+2)] \\
 &= n! [1 + (n+1) + n^2 + 3n + 2] \\
 &= n! [n^2 + 4n + 4] \\
 &= n! (n+2)^2
 \end{aligned}$$

$$\therefore \text{Let } a^2 = n! (n+2)^2$$

From (a), all the prime factors of  $a^2$  have even exponents.  $\therefore$  prime factors of  $n! (n+2)^2$  should have even exponents.

But  $n!$  has, for its largest prime factor  $(n+2)$ , an exponent of 1. (from (a) above). Call this factor  $p$ . Even if  $(n+2)^2$  had  $p$  as a factor, its exponent would be even.

Thus, the exponent of  $p$  in the factorization of  $n! (n+2)^2$  will be odd. This contradicts expectation of  $a^2$ .

$\therefore n$  can't be  $\geq 2$ .

$$\therefore \text{for } n=1, n! + (n+1)! + (n+2)! = 9 = 3^2.$$

$\therefore$  Only  $n=1$  is statement true.

## 4.2 Basic Properties of Congruence

Note Title

1/28/2005

Def: Complete set of residues modulo  $n$

A set  $A = \{a_1, a_2, \dots, a_n\}$  is said to form a complete set of residues modulo  $n \Leftrightarrow$  given any integer  $z$ , there is an  $a_i \in A$  s.t.  $a_i - z \equiv kn$  for some integer  $k$ , but for  $a_j \neq a_i$  and  $a_j \in A$ , there exist integers  $q, r$ ,  $0 < r < n$ , s.t.  $a_j - z \equiv qn + r$ .

Lemma: Let  $A = \{a_1, \dots, a_n\}$  be a complete set of residues modulo  $n$ , and let  $B = \{0, 1, 2, \dots, n-1\}$ . Then there is a one-to-one correspondence between  $A$  and  $B$ .

Pf: Let  $K \in B$ . By def. of complete set of residues, there is an  $a_i \in A$  s.t.  $K \equiv a_i \pmod{n}$ , and  $K \not\equiv a_j \pmod{n}$  for all  $a_j \neq a_i$ .

Since there are  $n$  elements in  $B$  and in  $A$ , each element of  $B$  is matched with one and only one element of  $A$ .

$\therefore$  Given any element of  $A$ , There is an element of  $B$  associated with it, and only one element of  $B$ . For if  $a_k \in A$  is associated with two elements of  $B$ , say  $b_i$  and  $b_j$ , Then  $a_k \equiv b_i \pmod{n}$  and  $a_k \equiv b_j \pmod{n}$ .  $\therefore b_i \equiv b_j \pmod{n}$ , which is impossible, since  $b_i < n$ ,  $b_j < n$ , so  $0 < |b_i - b_j| < n$ , and so  $n$  can't divide a number less than itself.

Theorem 1:  $A = \{a_1, a_2, \dots, a_n\}$  is a complete set of residues modulo  $n \Leftrightarrow$  for  $a_i, a_j \in A$ ,  $a_i \neq a_j$ ,  $a_i \not\equiv a_j \pmod{n}$

Pf: (1) Suppose  $A$  is a complete set, let  $a_i, a_j \in A$  s.t.  $a_i \neq a_j$ , and suppose  $a_i \equiv a_j \pmod{n}$

$$\therefore a_i - a_j = kn, \text{ some } k. [1]$$

Let  $z$  be s.t.  $z \equiv a_i \pmod{n}$ . Such a  $z$  exists since  $a_i + cn \equiv a_i \pmod{n}$ , where  $c$  is any integer.

$$\therefore z - a_i = sn, \text{ some } s. [2]$$

Adding  $\{1\}$  and  $\{2\}$ ,  $z - a_j = (k+s)n$ ,  
 $\therefore z \equiv a_j \pmod{n}$ , contradicting def of  
 complete set.  $\therefore a_i \not\equiv a_j \pmod{n}$

(2) Suppose  $a_i \not\equiv a_j \pmod{n}$  for  $a_i, a_j \in A$ ,  $i \neq j$

Consider  $a_i = q_i n + r_i$ , for  $1 \leq i \leq n$   
 $0 \leq r_i < n$

Then  $r_i \neq r_j$ , for  $i \neq j$ , because if  $r_i = r_j$

Then  $a_i - a_j \equiv (q_i - q_j)n$ , and  $\therefore a_i \equiv a_j \pmod{n}$

Since there are  $n$  members in set  $A$ ,

there are  $n$  different  $r_i$ ,  $0 \leq r_i < n$ , so

There is a one-to-one correspondence

between  $a_i$  and  $\{0, 1, \dots, n-1\}$ , i.e., given any

$r_i$  s.t.  $0 \leq r_i < n$ , there is an  $a_i$  s.t.  
 $a_i \equiv r_i \pmod{n}$ .

Now let  $z$  be any integer.

By Div. Algorithm,  $z = qn + r$ ,  $0 \leq r < n$

$\therefore$  From statement above, there is an

$a_i \in A$  s.t.  $a_i - r = kn$ , some  $k$ .

$\therefore z = qn + r = qn + (a_i - kn)$ , so

$$z = a_i + (q - k)n, [1]$$

$$\text{so } z \equiv a_i \pmod{n}$$

Suppose  $z \equiv a_j \pmod{n}$ ,  $a_j \neq a_i$

$\therefore z - a_j = sn$ , some  $s$ .  $\therefore$  From E13

$$a_i + (g-k)n - a_j = sn, a_i - a_j = (s-g+k)n,$$
$$\therefore a_i \equiv a_j \pmod{n}, \text{ a contradiction.}$$

$\therefore z$  is  $\equiv$  to one and only one of  
 $a_i \in A, \pmod{n}$

Theorem 2: if  $a b \equiv 0 \pmod{p}$ ,  $p$  prime, Then  
 $a \equiv 0 \pmod{p}$  or  $b \equiv 0 \pmod{p}$ .

Pf. Suppose  $a \not\equiv 0 \pmod{p}$

$\therefore a = qp + r$ ,  $0 < r < p$ . Thus,  
r and  $p$  are relatively prime.

Since  $\exists K$  s.t.  $ab = kp$ , Then

$$ab = qp b + r b, kp = qp b + r b,$$

$p(k-qb) = rb$ .  $\therefore$  By Euclid's  
Lemma,  $p \mid b$ .  $\therefore \exists s$  s.t.  $b = ps$ .

$$\therefore b \equiv 0 \pmod{p}$$

Theorem 3:  $z \equiv a \pmod{n} \Leftrightarrow z + cn \equiv a + dn \pmod{n}$

Pf: (1) Suppose  $z \equiv a \pmod{n}$

$$\therefore z - a = kn, \text{ some } k$$

$$\begin{aligned}\therefore z + cn - (a + dn) &= z - a + cn - dn \\ &= kn + (c - d)n \\ &= (k + c - d)n\end{aligned}$$

$$\therefore z + cn \equiv a + dn \pmod{n}$$

(2) Suppose  $z + cn \equiv a + dn \pmod{n}$

$$\therefore z + cn - (a + dn) = kn, \text{ some } k$$

$$\begin{aligned}\therefore z - a &= -cn + dn + kn \\ &= (k - c + d)n\end{aligned}$$

$$\therefore z \equiv a \pmod{n}$$

## Problems 4.2

1. (a). If  $a \equiv b \pmod{n}$  and  $m|n$ , Then  $a \equiv b \pmod{m}$

Pf:  $a \equiv b \pmod{n} \Rightarrow a - b = kn, \text{ some } k.$

$$m|n \Rightarrow n = rm, \text{ some } r.$$

$$\therefore a - b = kr m \Rightarrow a \equiv b \pmod{m}$$

(b). If  $a \equiv b \pmod{n}$ , and  $c > 0$ , Then  $ca \equiv cb \pmod{cn}$

Pf:  $a - b = kn$ , some  $k$ .  $\therefore ca - cb = kcn \Rightarrow$   
 $ca \equiv cb \pmod{cn}$

(c) If  $a \equiv b \pmod{n}$ , and  $a, b, d$  all divisible  
by  $d > 0$ , Then  $a/d \equiv b/d \pmod{n/d}$

Pf:  $a - b = kn$ , some  $k$ . By assumption,  
 $a = k_1 d \quad \therefore a/d = k_1$   
 $b = k_2 d \quad \therefore b/d = k_2$   
 $n = k_3 d \quad \therefore n/d = k_3$

$$\therefore k_1 d - k_2 d = k(k_3 d)$$

$$\therefore k_1 - k_2 = k k_3 \Rightarrow \frac{a}{d} - \frac{b}{d} = k \left( \frac{n}{d} \right)$$

$$\therefore a/d \equiv b/d \pmod{n/d}$$

2.  $a^2 \equiv b^2 \pmod{n} \not\Rightarrow a \equiv b \pmod{n}$

$5^2 \equiv 4^2 \pmod{3}$  since  $25 - 16 = 3 - 3$   
But  $5 \not\equiv 4 \pmod{3}$ .

3. If  $a \equiv b \pmod{n}$ , Then  $\gcd(a, n) = \gcd(b, n)$

PF:  $a - b = k_1$ , some  $k_1$ . Let  $d = \gcd(a, n)$   
 $\therefore a = dr$ ,  $n = ds$ , some  $r, s$ .

$$\therefore dr - b = k_1 ds, b = d(r - ks), \therefore d \mid b.$$

Let  $d' = \gcd(b, n)$ .  $\therefore$  Since  $d \mid n$  and  
 $d \mid b$ ,  $d \leq d'$

By similar reasoning as above,  $d' \mid a$ .  
 $\therefore d' \leq d$ .  
 $\therefore d' = d$

4. (a) Find remainder of  $2^{50} \div 7$ ,  $41^{65} \div 7$

$$2^{50} \div 7 : 2^{50} = (2^5)^{10}, 2^5 = 4 \cdot 7 + 4$$

$$\therefore 2^5 \equiv 4 \pmod{7}$$

$$\therefore 2^{50} \equiv 4^{10} \pmod{7}$$

$$\text{But } 4^{10} = 2^{20} = (2^5)^4$$

$$\text{From above, } 2^5 \equiv 4 \pmod{7}$$

$$\therefore 2^{20} \equiv 4^4 \pmod{7}$$

$$\text{But } 4^4 = 256 = 36 \cdot 7 + 4$$

$$\therefore 4^4 \equiv 4 \pmod{7}, \therefore 4^4 - 4 \equiv 0 \pmod{7}$$

$$\therefore 2^{50} - 4 \equiv 4^4 - 4 = 2^{20} - 4 \equiv 4^4 - 4 \equiv 0 \pmod{7}$$

$$\therefore 2^{5^0} \equiv 4 \pmod{7}, \text{ so}$$

$2^{5^0} \div 7$  has remainder 4

$$41^{65} \div 7: 41^{65} = (41^5)^{13}, 41 = 5 \cdot 7 + 6 \\ \therefore 41 \equiv 6 \pmod{7}$$

$$\therefore 41^5 \equiv 6^5 \pmod{7}$$

$$\text{But } 6^5 = 7776 \therefore 6^5 = 1110 \cdot 7 + 6 \\ \therefore 6^5 \equiv 6 \pmod{7}$$

$$\therefore 41^{65} \equiv (41^5)^{13} \equiv (6^5)^{13} \equiv 6^{13} \pmod{7}$$

$$6^2 = 5 \cdot 7 + 1, \therefore 6^2 \equiv 1 \pmod{7}$$

$$\therefore 6^{12} \equiv 1 \pmod{7}, \therefore 6^{13} \equiv 6 \pmod{7}$$

$$\therefore 41^{65} \equiv (6^5)^{13} \equiv 6^{13} \equiv 6 \pmod{7}$$

$\therefore 41^{65} \div 7$  has remainder 6

(b) What is remainder when  $1^2 + 2^5 + \dots + 100^5 \div 4$ ?

Since  $1^5 \equiv 1 \pmod{4}$ , and since  $1 \equiv 5 \equiv 9 \pmod{4}$

$$32 = 2^5 \equiv 0 \pmod{4}$$

$$2 \equiv 6 \equiv 10 \pmod{4}$$

$$243 = 3^5 \equiv 3 \pmod{4}$$

$$3 \equiv 7 \equiv 11 \pmod{4}$$

$$4^5 \equiv 0 \pmod{4}$$

$$4 \equiv 8 \equiv 12 \pmod{4}$$

Each block of 4 numbers will have same remainder sum.

Since  $1^5 + 2^5 + 3^5 + 4^5 \equiv 1 + 0 + 3 + 0 \equiv 4 \equiv 0 \pmod{4}$ ,  
Then the 25 blocks will all have remainder 0.  
 $\therefore$  Entire remainder is 0.

5. Prove  $53^{103} + 103^{53} \equiv 0 \pmod{39}$   
 $111^{333} + 333^{111} \equiv 0 \pmod{7}$

Pf:  $53^{103} + 103^{53} \equiv 0 \pmod{39}$

$$39 = 3 \cdot 13, \quad 53 = 3 \cdot 17 + 2 = 3 \cdot 18 - 1$$

$$103 = 34 \cdot 3 + 1$$

$$\therefore 53 \equiv -1 \pmod{3} \quad 103 \equiv 1 \pmod{3}$$

$$\therefore 53^{103} \equiv (-1)^{103} \pmod{3} \quad 103^{53} \equiv 1^{53} \pmod{3}$$

$$53 \equiv 1 \pmod{13} \quad 103 \equiv -1 \pmod{13}$$

$$\therefore 53^{103} \equiv 1 \pmod{13} \quad 103^{53} \equiv -1 \pmod{13}$$

$$\therefore 53^{103} + 103^{53} \equiv -1 + 1 \equiv 0 \pmod{3}$$

$$53^{103} + 103^{53} \equiv -1 + 1 \equiv 0 \pmod{13}$$

$\therefore$  Both 3 and 13 divide sum, and  
 $\gcd(3, 13) = 1$ , so by Corollary 2, p. 24,

$3 \cdot 13 = 39$  divides sum.

$$\therefore 53^{103} + 103^{53} \equiv 0 \pmod{39}$$

$$111^{333} + 333^{111} \equiv 0 \pmod{7}$$

$$111 = 7 \cdot 15 + 6, \therefore 111 \equiv 16 \cdot 7 + -1, \therefore 111 \equiv -1 \pmod{7}$$
$$\therefore 111^{333} \equiv (-1)^{333} \pmod{7}, \text{ or } 111^{333} \equiv (-1) \pmod{7}$$

$$333 = 47 \cdot 7 + 4, \therefore 333 \equiv 4 \pmod{7}, 333 \equiv 2^2 \pmod{7}$$
$$\therefore 333^{111} \equiv 2^{222} \pmod{7}$$

$$2^6 = 64 = 9 \cdot 7 + 1. \therefore 2^6 \equiv 1 \pmod{7}$$

$$\text{and } 222 = 6 \cdot 17. \therefore (2^6)^{17} \equiv 2^{222}$$

$$\therefore 2^{222} \equiv 1^{17} \pmod{7}, \text{ or } 2^{222} \equiv 1 \pmod{7}$$

$$\therefore 333^{111} \equiv 1 \pmod{7}$$

$$\therefore 111^{333} + 333^{111} \equiv (-1+1) \pmod{7}, \text{ or}$$

$$111^{333} + 333^{111} \equiv 0 \pmod{7}$$

6. (a)  $7 \mid (5^{2n} + 3 \cdot 2^{5n-2})$ ,  $n \geq 1$

$$\text{Pf: } n=1 : 5^{2n} + 3 \cdot 2^{5n-2} = 25 + 3 \cdot 8 = 49 = 7^2$$

$$\begin{aligned} n+1 : & 5^{2(n+1)} + 3 \cdot 2^{5(n+1)-2} \\ & = 5^{2n} \cdot 5^2 + 3 \cdot 2^{5n-2} \cdot 2^5 \end{aligned}$$

$$\begin{aligned}
 &= 5^{2n} (3 \cdot 7 + 4) + 3 \cdot 2^{5n-2} \cdot (4 \cdot 7 + 4) \\
 &= 3 \cdot 7 \cdot 5^{2n} + 4 \cdot 7 \cdot 3 \cdot 2^{5n-2} \\
 &\quad + 4 (5^{2n} + 3 \cdot 2^{5n-2}) \quad [1] \\
 &= 3 \cdot 7 \cdot 5^{2n} + 4 \cdot 7 \cdot 3 \cdot 2^{5n-2} + 4 \cdot 7x \\
 &= 7 (3 \cdot 5^{2n} + 4 \cdot 3 \cdot 2^{5n-2} + 4 \cdot x)
 \end{aligned}$$

where  $x$  is some integer since it was assumed that for  $n$ ,

$$5^{2n} + 3 \cdot 2^{5n-2} = 7x \text{ as in } [1].$$

$\therefore$  For  $n+1$ , number is divisible by 7.

$\therefore$  true for all  $n \geq 1$ .

$$\begin{aligned}
 &= \\
 \text{or, } 5^2 &= 25 \equiv 4 \pmod{7} \quad \therefore 5^{2n} \equiv 4^n \pmod{7}
 \end{aligned}$$

$$2^5 \equiv 4 \pmod{7} \quad 2^{5n} \equiv 4^n \pmod{7}$$

$$\text{For } n \geq 1, 2^{5n} \cdot 4^{-1} \equiv 4^n \cdot 4^{-1} \pmod{7}$$

$$\begin{aligned}
 &\therefore 2^{5n-2} \equiv 4^{n-1} \pmod{7} \\
 &\therefore 3 \cdot 2^{5n-2} \equiv 3 \cdot 4^{n-1} \pmod{7}
 \end{aligned}$$

$$\begin{aligned}
 \text{But } 4^n + 3 \cdot 4^{n-1} &= 4 \cdot 4^{n-1} + 3 \cdot 4^{n-1} \\
 &= 7 \cdot 4^{n-1}
 \end{aligned}$$

$$\therefore 5^{2n} + 3 \cdot 2^{5n-2} \equiv 7 \cdot 4^{n-1} \equiv 0 \pmod{7}$$

$$(6) 13 \mid (3^{n+2} + 4^{2n+1})$$

$$\text{Pf: } 3 \equiv 16 \pmod{13}, \quad 3 \equiv 4^2 \pmod{13}$$

$$\therefore 3^n \equiv 4^{2n} \pmod{13}$$

$$3^n \cdot 9 \equiv 4^{2n} \cdot 9 \pmod{13}, \quad 3^{n+2} \equiv 4^{2n} \cdot 9 \pmod{13}$$

$$\begin{aligned}\therefore 3^{n+2} + 4^{2n+1} &\equiv 4^{2n} \cdot 9 + 4^{2n+1} \pmod{13} \\ &\equiv 4^{2n}(9+4) \pmod{13} \\ &\equiv 4^{2n} \cdot 13 \pmod{13} \\ &\equiv 0 \pmod{13}\end{aligned}$$

$$(7) 27 \mid (2^{5n+1} + 5^{n+2})$$

$$\text{Pf: } 32 \equiv 5 \pmod{27}, \quad \therefore 2^5 \equiv 5 \pmod{27}$$

$$\therefore 2^{5n} \equiv 5^n \pmod{27}$$

$$2^{5n} \cdot 2 \equiv 2 \cdot 5^n \pmod{27}$$

$$\begin{aligned}\therefore 2^{5n+1} + 5^{n+2} &\equiv 2 \cdot 5^n + 5^{n+2} \pmod{27} \\ &\equiv 5^n(2 + 25) \pmod{27} \\ &\equiv 5^n \cdot 27 \pmod{27} \\ &\equiv 0 \pmod{27}\end{aligned}$$

$$(d) 43 \mid (6^{n+2} + 7^{2n+1})$$

$$\text{Pf: } 6 \equiv 49 \pmod{43}, 6 \equiv 7^2 \pmod{43}$$

$$\therefore 6^n \equiv 7^{2n} \pmod{43}$$

$$6^n \cdot 36 \equiv 7^{2n} \cdot 36 \pmod{43}$$

$$6^{n+2} + 7^{2n+1} \equiv 7^{2n} \cdot 36 + 7^{2n+1} \pmod{43}$$

$$\equiv 7^{2n}(36 + 7) \pmod{43}$$

$$\equiv 0$$

$$7. \text{ For } n \geq 1, (-13)^{n+1} \equiv (-13)^n + (-13)^{n-1} \pmod{181}$$

$$\text{Pf: } n=1. (-13)^2 = 169, 169 + 13 = 182$$

$$\therefore 169 \equiv (-13) + 1 \pmod{181}$$

$$K \Rightarrow K+1: \text{ Suppose } (-13)^{k+1} \equiv (-13)^k + (-13)^{k-1} \pmod{181}$$

$$\therefore (-13)^{k+1} \cdot (-13) \equiv (-13)^k \cdot (-13) + (-13)^{k-1} \cdot (-13) \pmod{181}$$

$$\therefore (-13)^{k+2} \equiv (-13)^{k+1} + (-13)^k \pmod{181}$$

$\therefore$  True for all  $n \geq 1$

$$8. (a) \text{ If } a \text{ is odd, Then } a^2 \equiv 1 \pmod{8}$$

Pf: By Div. Alg., a odd means

$a = 4k+1$  or  $a = 4k+3$ , some  $k$ .

$$\begin{aligned}\therefore a^2 &= 16k^2 + 8k + 1 \text{ or } a^2 = 16k^2 + 24k + 9 \\ \therefore a^2 - 1 &= 8(2k^2 + k) \text{ or } a^2 - 1 = 8(2k^2 + 3k + 1) \\ \therefore a^2 &\equiv 1 \pmod{8}\end{aligned}$$

(b) For any  $a$ ,  $a^3 \equiv 0, 1, \text{ or } 6 \pmod{7}$

Pf: By Div. Alg,  $a = 7k+r$ ,  $0 \leq r < 7$

$$a = 7k: a^3 = (7k)^3, \therefore a^3 = 7 \cdot 7^2 k^3, a^3 \equiv 0 \pmod{7}$$

$$\begin{aligned}a = 7k+1: a^3 &= (7k+1)^3 = 7^3 k^3 + (\ ) 7^2 k^2 + (\ ) 7k + 1 \\ \therefore a^3 - 1 &= 7 \{ \quad \}, \therefore a^3 \equiv 1 \pmod{7}\end{aligned}$$

$$\begin{aligned}a = 7k+2: a^3 &= 7^3 k^3 + (\ ) 7^2 k^2 \cdot 2 + (\ ) 7k \cdot 2^2 + 2^3 \\ \therefore a^3 - 1 &= 7 [ 7^2 k^3 + \dots + 1 ] \\ \therefore a^3 &\equiv 1 \pmod{7}\end{aligned}$$

$$\begin{aligned}a = 7k+3: a^3 &= 7^3 k^3 + (\ ) 7^2 k^2 \cdot 3 + (\ ) 7k \cdot 3^2 + 27 \\ a^3 - 6 &= 7 [ 7^2 k^3 + \dots + 3 ] \\ \therefore a^3 &\equiv 6 \pmod{7}\end{aligned}$$

$$\begin{aligned}a = 7k+4: a^3 &= 7^3 k^3 + \dots + 64 \\ a^3 - 1 &= 7^3 k^3 + \dots + 63 = 7 [ 7^2 k^3 + \dots + 9 ] \\ \therefore a^3 &\equiv 1 \pmod{7}\end{aligned}$$

$$a = 7k+5 : a^3 = 7^3 k^3 + \dots + 125 = 7k^3 + 119 + 6$$

$$\therefore a^3 - 6 = 7 [7^2 k^3 + \dots + 17]$$

$$\therefore a^3 \equiv 6 \pmod{7}$$

$$a = 7k+6 : a^3 = 7^3 k^3 + \dots + 218 = 7k^3 + \dots + 31 - 7 + 1$$

$$a^3 - 1 = 7 [7^2 k^3 + \dots + 31]$$

$$\therefore a^3 \equiv 1 \pmod{7}$$

(c) For any  $a$ ,  $a^4 \equiv 0$  or  $1 \pmod{5}$

Pf: By Dir. Alg.,  $a = 5k+r$ ,  $0 \leq r < 5$

$$a = 5k : a^4 = 5 \cdot 5^3 k^4, \therefore a^4 \equiv 0 \pmod{5}$$

$$a = 5k+1 : a^4 = 5^4 k^4 + ()5^3 k^3 + ()5^2 k^2 + ()5k + 1$$

$$\therefore a^4 - 1 = 5 [ \quad ]$$

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

$$a = 5k+2 : a^4 = 5^4 k^4 + \dots + 16 = 5^4 k^4 + \dots + 15 + 1$$

$$a^4 - 1 = 5 [ 5^3 k^4 + \dots + 3 ]$$

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

$$a = 5k+3 : a^4 = 5^4 k^4 + \dots + 3^4 = 5^4 k^4 + 5 \cdot 16 + 1$$

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

$$a = 5k+4 \therefore a^4 = 5^4 k^4 + \dots + 4^4 = 5^4 k^4 + \dots + 255 + 1$$

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

(d) If  $a$  is not divisible by 2 or 3, Then  
 $a^2 \equiv 1 \pmod{24}$

Pf: By Div. Alg.,  $a = 24k+r$ ,  $0 \leq r < 24$

Since  $a$  is not divisible by 2,  
 $r$  must be odd.

Since  $a$  is not divisible by 3,  
 $r = 1, 5, 7, 11, 13, 17, 19$

$$\therefore a^2 = (24k+r)^2 = 24^2 k^2 + 48kr + r^2$$

$$r=1 \therefore r^2=1 \therefore \text{Let } c=0$$

$$r=5 \therefore r^2=25=24+1 \therefore \text{Let } c=1$$

$$r=7 \therefore r^2=49=2 \cdot 24+1 \therefore \text{Let } c=2$$

$$r=11 \therefore r^2=121=5 \cdot 24+1 \therefore \text{Let } c=5$$

$$r=13 \therefore r^2=169=7 \cdot 24+1 \therefore \text{Let } c=7$$

$$r=17 \therefore r^2=289=12 \cdot 24+1 \therefore \text{Let } c=12$$

$$r=19 \therefore r^2=361=15 \cdot 24+1 \therefore \text{Let } c=15$$

$$\therefore a^2 = 24^2 k^2 + 48kr + 24 \cdot c + 1$$

$$= 24 [24k^2 + 2kr + c] + 1$$

$$\therefore a^2 \equiv 1 \pmod{24}$$

9. If  $p$  is prime s.t.  $n < p < 2n$ , then

$$\binom{2n}{n} \equiv 0 \pmod{p}$$

$$\text{Pf: } \binom{2n}{n} = \frac{1 \cdot 2 \cdot 3 \cdots n (n+1) \cdots (2n)}{n! n!} = \frac{(n+1) \cdots (2n)}{n!}$$

$$\therefore n! \binom{2n}{n} = (n+1) \cdots (2n)$$

Since  $n < p < 2n$ ,  $p$  must be one of the factors of  $(n+1) \cdots (2n)$

$$\therefore n! \binom{2n}{n} = Kp$$

Since  $p > n$ , it is greater than every term of  $n!$ , it is not a member of the prime factorization of each member.

$$\therefore \gcd(n!, p) = 1$$

$\therefore$  By Euclid's lemma,  $p \mid \binom{2n}{n}$

$$\therefore \binom{2n}{n} \equiv 0 \pmod{p}$$

10. If  $\{q_1, \dots, q_n\}$  is a complete set of residues mod  $n$  and  $\gcd(a, n) = 1$ , then  $\{aq_1, \dots, aq_n\}$  is a complete set of residues mod  $n$ .

Pf: Consider  $aq_i$  and  $aq_j$ ,  $i \neq j$ ,  $1 \leq i, j \leq n$

If  $aq_i$  and  $aq_j$  are congruent mod  $n$ , then  $aq_i - aq_j \equiv kn$ , some  $k$ .  $\therefore a(q_i - q_j) = kn$

Since  $\gcd(a, n) = 1$ , then by Euclid's lemma,  $n | (q_i - q_j)$ , contradicting that  $q_i \neq q_j$ .

$$\therefore aq_i \neq aq_j$$

By Theorem 1 at top,  $\{aq_1, \dots, aq_n\}$  is a complete set.

11. Show  $0, 1, 2, 2^2, \dots, 2^9$  is a complete set of residues mod 11, but that  $0, 1^2, 2^2, \dots, 10^2$  is not.

Pf: Since  $\gcd(11, 2^n) = 1$  for  $0 \leq n \leq 9$ , Then  $2^n \not\equiv 0 \pmod{11}$  for  $0 \leq n \leq 9$ .

$\therefore$  Consider  $2^r$  and  $2^s$ ,  $1 \leq r, s \leq 9$ ,  $r \neq s$ .

$$\text{Suppose } s > r. \therefore 2^s - 2^r = 2^r(2^{s-r} - 1)$$

Since  $\gcd(11, 2^r) = 1$ , and  $\gcd(2^{s-r} - 1, 11) = 1$

for  $0 \leq s-r \leq 8$ , Then There is no  $k > 1$   
 s.t.  $2^s - 2^r = 11k \therefore 2^s \not\equiv 2^r \pmod{11}$   
 $\therefore 0, 1, 2, 2^2, \dots, 2^9$  is a complete set of  
 residues mod 11.

Another proof (more obvious).

Look at remainders from Div. Alg.

$$0: r=0 \quad 2^4: 5 \quad 2^8: 3$$

$$1: r=1 \quad 2^5: 10 \quad 2^9: 6$$

$$2: r=2 \quad 2^6: 9$$

$$2^2: r=4 \quad 2^7: 7$$

$$2^3: r=8$$

$\because$  remainders are in 1-to-1 correspondence  
 to  $\{0, 1, \dots, 9, 10\}$ , and therefore  
 constitute a complete set of residues  
 mod 11.

$$\begin{array}{lll} 0: 0 & 4^2: 5 & 8^2: 9 \\ 1^2: 1 & 5^2: 3 & 9^2: 4 \\ 2^2: 4 & 6^2: 3 & 10^2: 1 \\ 3^2: 9 & 7^2: 5 \end{array}$$

$\therefore$  not a 1-to-1 correspondence  $\therefore$  not a  
 complete set of residues (Lemma at top  
 of this exercise set).

12. (a) If  $\gcd(a, n) = 1$ , Then

$c, c+a, c+2a, \dots, c+(n-1)a$  forms a complete set of residues mod  $n$ .

Pf: Consider  $c+ra$  and  $c+sa$ ,  $r \neq s$ ,  
 $0 \leq r, s \leq n-1$ . Suppose  $s > r$ .

$$\therefore c+sa - (c+ra) = (s-r)a$$

$s-r < n$  since  $s \leq n-1$ ,  $r \leq n-1$ .

$\therefore n \nmid (s-r)$ . Since  $\gcd(a, n) = 1$ ,  
Then There is no integer,  $K$ , S.t.  
 $(s-r)a = nk$ .

$\therefore c+sa \neq c+ra$ , so The above  
set is a complete set of residues.

(b) Any  $n$  consecutive integers form a complete set of residues mod  $n$ .

Pf: From (a) above, Let  $c$  = first of  
The consecutive list, Let  $a = 1$ .

$\therefore$  The list in (a) is  
 $c, c+1, c+2, \dots, c+(n-1)$

(C) The product of any set of  $n$  consecutive integers is divisible by  $n$

Pf: By (B) The set of  $n$  consecutive integers forms a complete set of residues mod  $n$ .  $\therefore$  One of the members is congruent to 0 mod  $n$ , which means one member is divisible by  $n$ .  
 $\therefore$  The entire product is divisible by  $n$ .

13. If  $a \equiv b \pmod{n_1}$ ,  $a \equiv b \pmod{n_2}$ , then  $a \equiv b \pmod{n}$ , where  $n = \text{lcm}(n_1, n_2)$

Pf: Let  $K_1, K_2$  be the integers such that

$$a - b = K_1 n_1 \quad \text{and} \quad a - b = K_2 n_2$$

Let  $d = \gcd(n_1, n_2)$ .  $\therefore n_1 = dr$ , some  $r$ ,  $1 = \frac{n_1}{dr}$

$$\therefore a - b = K_2 n_2 = K_2 n_2 \left( \frac{n_1}{dr} \right) = \frac{K_2}{r} \cdot n_1 n_2$$

But  $\frac{n_1 n_2}{d} = \text{lcm}(n_1, n_2)$  (Th 2.8, p. 30)

$$\therefore a - b = \frac{K_2}{r} \cdot \text{lcm}(n_1, n_2)$$

Is  $\frac{k_2}{r}$  an integer?

Let  $s \in \mathbb{Z}$  s.t.  $n_2 = ds$

Since  $a - b = k_1 n_1 = k_2 n_2$ ,

Then  $k_1 dr = k_2 ds$ , so  $k_1 r = k_2 s$

Since  $r$  and  $s$  are relatively prime,

(see proof of Corollary 1, p. 23)

by Euclid's lemma,  $r | k_2$ , so  $\frac{k_2}{r}$  is an integer.

14. Show That  $a^k \equiv b^k \pmod{n}$  and  $k \equiv j \pmod{n}$  need not imply  $a^j \equiv b^j \pmod{n}$

Pf:  $2^2 \equiv 3^2 \pmod{5}$  since  $4 \equiv 9 \pmod{5}$

$2 \equiv 7 \pmod{5}$

$2^7 \equiv 3^7 \pmod{5}$ ?

$2^7 = 128, 3^7 = 2187, 2187 - 128 = 2059$ ,

so  $2^7 \not\equiv 3^7$

15. If  $a$  is odd, Then for  $n \geq 1$ ,  $a^{2^n} \equiv 1 \pmod{2^{n+2}}$

Pf:  $n=1$ : is  $a^2 \equiv 1 \pmod{2^3}$ ?

Since  $a$  is odd,  $a = 4r+1$  or  $a = 4r+3$

$\therefore a^2 = 16r^2 + 8r + 1$  or  $a^2 = 16r^2 + 24r + 9$

$\therefore a^2 - 1 = 16r^2 + 8r = 8(2r^2 + r)$ , or

$a^2 - 1 = 16r^2 + 24r + 8 = 8(2r^2 + 3r + 1)$

$$\therefore a^2 \equiv 1 \pmod{8}$$

$K \Rightarrow K+1$ : Suppose  $a^{2^k} \equiv 1 \pmod{2^{k+2}}$

$$\therefore a^{2^k} - 1 = (2^{k+2})r, \text{ some } r$$

$$a^{2^{k+1}} - 1 = a^{2 \cdot 2^k} - 1 = (a^{2^k})^2 - 1$$

$$= (a^{2^k} - 1)(a^{2^k} + 1)$$

$$= (a^{2^k} + 1)(2^{k+2})r$$

$$= (2^{k+2}r + 2)(2^{k+2}r)$$

$$= 2^{2k+4}r^2 + 2 \cdot 2^{k+2}r$$

$$= 2^{2k+4}r^2 + 2^{k+3}r$$

$$= 2^{k+3}(2^{k+1}r^2 + r)$$

$$= 2^{(k+1)+2}s, \text{ where } s = 2^{k+1}r^2 + r$$

$\therefore$  When true for  $k$ , true for  $k+1$

16. (a) Show  $89/2^{44} - 1$

Idea: Look at multiples of 89 to see if close or off by 1 from powers of 2

$$2^8 \equiv (-11) \pmod{89}$$

$$2^5 \equiv 2^5 \cdot (-11) \equiv 1 \pmod{89}$$

$$2^5 = 32 \quad 2^8 = 256 \quad 3 \cdot 89 = 267$$

$$2^6 = 64 \quad 2^9 = 512 \quad 6 \cdot 89 = 534$$

$$2^7 = 128 \quad 2^{10} = 1024 \quad 11 \cdot 89 = 979$$

$$2^{11} = 2048 \quad 12 \cdot 89 = 1068$$

$$23 \cdot 89 = 2047$$

$$\therefore 2^{11} \equiv 1 \pmod{89}$$

$$\therefore 2^{44} \equiv 1^4 \pmod{89}$$

=

$$\text{Another way: } 2^8 \equiv (-11) \pmod{89} \quad (3 \cdot 89 = 267)$$

$$\therefore 2^3 \cdot 2^6 \equiv 2^3 \cdot (-11) \pmod{89}, \text{ and } 2^3 \cdot (-11) \equiv 1 \pmod{89}$$

$$\therefore 2^{11} \equiv 1 \pmod{89}, \therefore 2^{44} \equiv 1 \pmod{89}$$

$$(6) 97 \mid 2^{48}-1$$

97 is close to 100, so look at powers of 2  
close to 100's. We find that  $21 \cdot 97 = 2037$

$$\therefore 2^{11} = 2048 \equiv 11 \pmod{97}$$

$$\therefore 2^{12} = 4096 \equiv 2 \cdot 11 \pmod{97}$$

$$\therefore 2^{48} \equiv 2^4 \cdot 11^4 \pmod{97}$$

$$\text{But } 2^4 \cdot 11^4 = (4 \cdot (21))^2 = (484)^2, \text{ and}$$

$$5 \cdot 97 = 485$$

$$\therefore 484 \equiv (-1) \pmod{97}$$

$$\therefore (4 \cdot 121) \equiv (-1) \pmod{97}$$

$$\therefore 2^4 \cdot 11^4 = (4 \cdot 121)^2 \equiv 1 \pmod{97}$$

$$\therefore 2^{48} \equiv 1 \pmod{97}$$

17. If  $ab \equiv cd \pmod{n}$ ,  $b \equiv d \pmod{n}$ ,  $\gcd(b, n) = 1$ ,  
 Then  $a \equiv c \pmod{n}$

Pf: Let  $ab - cd = rn$ , some  $r$

$$b - d = sn, \text{ some } s$$

$$\therefore b - sn = d$$

$$\therefore ab - cd = ab - c(b - sn)$$

$$\therefore rn = ab - cb + csn$$

$$rn = (a - c)b + csn$$

$$rn - csn = (a - c)b$$

$$(r - cs)n = (a - c)b$$

$\therefore$  since  $\gcd(n, b) = 1$ , Then by Euclid's lemma,  
 $n \mid (a - c)$ .  $\therefore a \equiv c \pmod{n}$

Alternatively,  $b \equiv d \pmod{n} \Rightarrow cb \equiv cd \pmod{n}$

$\therefore$  since  $ab \equiv cd \pmod{n}$ , Then  $ab \equiv cb \pmod{n}$

Since  $\gcd(b, n) = 1$ , Then by Corollary 1, p. C8,  
 $a \equiv c \pmod{n}$ .

18. If  $a \equiv b \pmod{n_1}$  and  $a \equiv c \pmod{n_2}$ , Then  
 $b \equiv c \pmod{n}$ , where  $n = \gcd(n_1, n_2)$

Pf:  $a - b = K_1 n_1$ , some  $K_1$ . Since  $n \mid n_1$ , Then  
 $n_1 = rn$ , some  $r$ .  $\therefore a - b = K_1 rn$   
 $\therefore a \equiv b \pmod{n}$

Similarly, since  $n|n_2$  Then  $a \equiv c \pmod{n}$   
 $\therefore$  By Theorem 4.2(c),  $b \equiv c \pmod{n}$ .

## 4.3 Special Divisibility Tests

Note Title

2/18/2005

1. (a). For any integer  $a$ , The units digit of  $a^2$  is 0, 1, 4, 5, 6, or 9

Pf: Let  $a = a_n 10^n + \dots + a_1 10 + a_0$ ,  $0 \leq a_0 < 10$   
 $\therefore a - a_0 = 10(a_n 10^{n-1} + \dots + a_1)$   
 $\therefore a \equiv a_0 \pmod{10} \quad \therefore a^2 \equiv a_0^2 \pmod{10}$

Note that all the other  $a_i$  of  $a$  are associated with a factor of 10 in  $a^2$ , and so don't contribute to units digit.  
 $\therefore$  only  $a_0^2$  contributes to units digit of  $a^2$ .

$$a_0^2 = 0, 1, 4, 9, 16, 25, 36, 49, 64, 81$$

$$\therefore a_0^2 \equiv 0, 1, 4, 5, 6, \text{ or } 9 \pmod{10}$$

$$\therefore a^2 \equiv 0, 1, 4, 5, 6, \text{ or } 9 \pmod{10}$$

(b). Any integer  $a_0$ ,  $0 \leq a_0 \leq 9$ , can occur in units digit of  $a^3$

Pf: as in (a), Let  $a = a_n 10^n + \dots + a_0$ ,  $0 \leq a_0 < 10$   
 $\therefore a - a_0 = 10(a_n 10^{n-1} + \dots + a_1)$   
 $\therefore a \equiv a_0 \pmod{10} \quad \therefore a^3 \equiv a_0^3 \pmod{10}$

$$a_0^3 = 0, 1, 8, 27, 64, 125, 216, 343, 512, 729$$

$$\therefore a_0^3 \equiv 0, 1, 2, 3, 4, 5, 6, 7, 8, \text{ or } 9 \pmod{10}$$

(C). For any  $a$ , The units digit of  $a^4$  is 0, 1, 5, or 6.

Pf: As in (a), The only contributor to units digit in  $a^4$  is  $a_0^4$ . f. Look at all possibilities of  $a_0^4$ ,  $0 \leq a_0 \leq 9$ .

From (a),  $a_0^2 \equiv 0, 1, 4, 5, 6, 9 \pmod{10}$

$$\therefore a_0^4 \equiv 0, 1, 16, 25, 36, 81 \pmod{10}$$

$$\therefore a_0^4 \equiv 0, 1, 5, \text{ or } 6 \pmod{10}$$

(D). The units digit of a triangular number is 0, 1, 3, 5, 6, or 8.

Pf: A number  $a$  is triangular  $\Leftrightarrow$  There is a number  $n$ ,  $n \geq 1$ , s.t.  $a = \frac{n(n+1)}{2}$   
(Problems 1.3, 1(a)).

Let  $n = a_m 10^m + \dots + a_0$ ,  $\therefore n \equiv a_0 \pmod{10}$

$\therefore n+1 \equiv a_0+1 \pmod{10}$ . Either  $n$  or  $n+1$  is even.  $\therefore \frac{n}{2}$  or  $\frac{n+1}{2}$  is an integer. Similarly for  $\frac{a_0}{2}$  or  $(a_0+1)/2$ .

$$\therefore \frac{n(n+1)}{2} \equiv \frac{a_0(a_0+1)}{2} \pmod{10}$$

Consider all possibilities for  $a_0$ .

$a_0$	$\frac{a_0(a_0+1)}{2}$	$\text{mod } 10$	$+5 \pmod{10}$
0	0	0	5
1	1	1	6
2	3	3	8
3	6	6	1
4	10	0	5
5	15	5	0
6	21	1	6
7	28	8	3
8	36	6	1
9	45	5	0

Note that for the other  $a_i$ , if associated with a factor of 10, then  $a_i \cdot \frac{10^i}{2} \equiv 0 \text{ or } 5 \pmod{10}$

Thus, the column  $[+5 \pmod{10}]$  shows possibilities of other factors contributing to units digit if divided by 2.

$\therefore a \equiv 0, 1, 3, 5, 6, \text{ or } 8 \pmod{10}$  if  $a$  is triangular

2. Find the last two digits of  $9^{9^9}$ .

$$9^3 - 9 = 9(9^2 - 1) = 9(80) \quad \therefore 9^3 \equiv 9 \pmod{10}$$

$$\therefore 9^9 \equiv 9^3 \equiv 9 \pmod{10}$$

$$\therefore 9^9 - 9 = 10K, \text{ some } K, \text{ or } 9^9 \equiv 9 + 10K$$

$$\therefore 9^9 \equiv 9^{9+10K} = 9^9 \cdot 9^{10K}$$

Look at the last 2 digits of  $9^9$  and  $9^{10}$

yields:  $9^1: 9 \quad 9^4: 61 \quad 9^7: 69 \quad 9^{10}: 01$

$$9^2: 81 \quad 9^5: 49 \quad 9^8: 21$$

$$9^3: 29 \quad 9^6: 41 \quad 9^9: 89$$

$$\therefore 9^9 \equiv 89 \pmod{100} \text{ and } 9^{10} \equiv 1 \pmod{100}$$

$$\therefore 9^{10K} \equiv 1^K \equiv 1 \pmod{100}$$

$$\therefore 9^9 \cdot 9^{10K} \equiv 89 \cdot 1 \pmod{100}$$

But  $9^9 = 9^9 \cdot 9^{10K}$ .  $\therefore 9^9 \equiv 89 \pmod{100}$ .

$\therefore$  Last two digits of  $9^9$  are 89.

3. 176,521,221:  $1+7+6+5+2+1+2+2+1 = 27$

$\therefore$  divisible by 9

$$1-2+2-1+2-5+6-7+1 = -3$$

$\therefore$  not divisible by 11

149,235,678:  $1+4+9+2+3+5+6+7+8 = 36$

$\therefore$  divisible by 9

$$8-7+6-5+3-2+9-4+1 = 9$$

$\therefore$  not divisible by 11

4. (a) Prove: If  $N$  is represented in the base  $b$  by

$$N = a_m b^m + \dots + a_1 b + a_0, \quad 0 \leq a_k \leq b-1$$

$$\text{Then } (b-1) | N \Leftrightarrow (b-1) | (a_m + a_{m-1} + \dots + a_1 + a_0)$$

Pf: Consider  $P(x) = \sum_{k=0}^m a_k x^k$ , a polynomial

with integer coefficients.

Note that  $b \equiv 1 \pmod{b-1}$

$\therefore P(b) \equiv P(1) \pmod{b-1}$  by Th. 4.4.

But  $P(b) = N$ , and

$$P(1) = a_m + \dots + a_1 + a_0$$

$$\therefore N \equiv a_m + \dots + a_1 + a_0 \pmod{b-1}$$

$$\therefore N \equiv 0 \pmod{b-1} \Leftrightarrow a_m + \dots + a_0 \equiv 0 \pmod{b-1}$$

$$\therefore (b-1) | N \Leftrightarrow (b-1) | (a_m + \dots + a_0)$$

Note:  $(b-1)$  divides  $N$  (base 10)  $\Leftrightarrow$  sum of digits  
(base 10) is divisible by  $(b-1)$ .

(b) For  $N$  written in base 9

(1)  $N$  is divisible by 8  $\Leftrightarrow$  sum of digits of  $N$   
(in base 10) is divisible by 8 (in base 10).  
This follows from (a).

(2)  $N$  is divisible by 3  $\Leftrightarrow$  units digit is divisible by 3 since each term in the polynomial (other than units digit) contains a power of 9.

(c)  $(447836)_q$  is divisible by 3 since  $3 \nmid 6$   
 $4+4+7+8+3+6 = 32$  (base 10),  
so is also divisible by 8.

5. Find the missing digits

$$(a) 51840 - 273581 = 1418243 \times 040$$

$$5+1+8+4+0 = 18, \text{ so } 9 \mid 51840, \\ \therefore 9 \mid (1418243 \times 040), \text{ so } 1+4+1+8+2+4+3+x+4 = x+27 \\ \therefore 9 \mid (x+27). \therefore x=0 \text{ or } 9$$

Since  $1-8+5-3+7-2=0$ , Then  $11 \mid 273581$   
 $\therefore 0-4+0-x+3-4+2-8+1-4+1 = -13-x$   
 $\therefore 11 \mid (-13-x)$ ,  $\therefore x \neq 0$ , and  $x=9$

$$\therefore \underline{x=9}$$

$$(b), 2 \times 99561 = [3(523+x)]^2$$

Since  $3^2$  is on right side,  $9 \mid 2x99561$   
 $\therefore 2+x+9+9+5+6+1 = x+32, \therefore \underline{\underline{x=4}}$

$$(c) 2784_x = x \cdot 5569$$

$5+5+6+9 = 25$ . From proof of Th. 4.5,  
 $5569 \equiv 25 \pmod{9}$ , and  $25 \equiv (2+5) \pmod{9}$   
 $\therefore 5569 \equiv 7 \pmod{9}$ .

$$\begin{aligned} \therefore 5569x &\equiv 7x \pmod{9} \\ 2784_x &\equiv (2+7+8+4+x) \equiv (3+x) \pmod{9} \\ \therefore 7x &\equiv (3+x) \pmod{9}, \text{ or } 6x \equiv 3 \pmod{9} \\ \therefore 9 \mid (6x-3), \text{ so } x &= 2, 5, 8 \end{aligned}$$

$$\begin{aligned} 5569 &\equiv (9-6+5-5) \equiv 3 \pmod{11}, 5569x \equiv 3x \pmod{11} \\ 2784_x &\equiv (x-4+8-7+2) \equiv (x-1) \pmod{11} \\ \therefore 3x &\equiv (x-1) \pmod{11}, 2x \equiv -1 \equiv 10 \pmod{11} \\ \therefore x &= 5 \end{aligned}$$

$$(d) 512 \cdot 1 \times 53125 = 1,000,000,000$$

$$\begin{aligned} 512 &\equiv (5+1+2) = 8 \pmod{9} \\ 1 \times 53125 &\equiv (1+x+5+3+1+2+5) \equiv (8+x) \pmod{9} \\ \therefore 8 \cdot (8+x) &\equiv 1,000,000,000 \equiv 1 \pmod{9} \\ \therefore 64+x &\equiv 6+4+x \equiv (1+x) \equiv 1 \pmod{9} \\ \therefore x &= 0 \text{ or } x = 9 \end{aligned}$$

$$512 \equiv (2-1+5) = 6 \pmod{11}$$

$$(x53125 \equiv (5-2+1-3+5-x+1) \equiv (7-x) \pmod{11})$$

$$\therefore 6 \cdot (7-x) \equiv (0-0+0-0+0-0+0-0+0-1) \equiv -1 \pmod{11}$$

$$\therefore 42-6x \equiv -1 \pmod{11}, 43 \equiv 6x \pmod{11}$$

$$\therefore x=0, \text{ and for } x=9, 43 \equiv 54 \pmod{11}.$$

$$\therefore \underline{x=9}$$

6. (a). An integer is divisible by 2  $\Leftrightarrow$  its units digit is 0, 2, 4, 6, or 8.

Pf: Since  $10=5 \cdot 2$ , in the base 10 representation of an integer  $N=a_m 10^m + \dots + a_1 10 + a_0$ , each term, except  $a_0$ , contains a power of 10, and so is divisible by 2.

$\therefore N$  is divisible by 2  $\Leftrightarrow a_0$  is divisible by 2, so  $a_0 = 0, 2, 4, 6, \text{ or } 8$ .

(b) An integer is divisible by 3  $\Leftrightarrow$  The sum of its digits is divisible by 3.

Pf: Let  $N=a_m 10^m + \dots + a_1 10 + a_0$  be the decimal expansion of  $N$ ,  $0 \leq a_k < 10$ , and let  $S = a_m + \dots + a_1 + a_0$ .

Consider  $P(x) = \sum_{k=0}^m a_k x^k$ . Note  $P(10)=N$ ,  $P(1)=S$

Note also  $10 \equiv 1 \pmod{3}$ , so  $P(10) \equiv P(1) \pmod{3}$   
 $\therefore N \equiv S \pmod{3}$ .  
 $\therefore N \equiv 0 \pmod{3} \Leftrightarrow S \equiv 0 \pmod{3}$

(c) An integer is divisible by 4  $\Leftrightarrow$  The number formed by its tens and units digits is divisible by 4.

Pf: Let  $N = a_m 10^m + \dots + a_2 10^2 + a_1 10 + a_0$ ,  
 $0 \leq a_k < 10$ .

Let  $K \geq 2$ . Then  $10^K = 10^{K-2} \cdot 10^2 = 10^{K-2} (5 \cdot 2)^2$   
 $= 10^{K-2} \cdot 25 \cdot 4$   
 $\therefore$  Each term  $c_K = a_K 10^K$  is divisible by 4 if  $K \geq 2$ .

$\therefore N$  is divisible by 4  $\Leftrightarrow a_1 10 + a_0$  is divisible by 4.

(d) An integer is divisible by 5  $\Leftrightarrow$  its units digit is 0 or 5

Pf: Let  $N = a_m 10^m + \dots + a_2 10^2 + a_1 10 + a_0$ ,  
 $0 \leq a_k < 10$ .

$$\text{Let } c_K = a_K 10^K = a_K (5 \cdot 2)^K = a_K 5^K 2^K$$

$\therefore$  Each  $c_k$  is divisible by 5 if  $k \geq 1$ .

$\therefore N$  is divisible by 5  $\Leftrightarrow g_0$  is divisible by 5, and  $g_0$  is divisible by 5  $\Leftrightarrow g_0 = 0, 5$ .

7. For any integer  $a$ , show that  $a^2 - a + 7$  ends in one of the digits 3, 7, or 9.

PF: If  $a = g_m 10^m + \dots + g_1 10 + g_0$ , Then  $a \equiv g_0 \pmod{10}$   
 $\therefore a^2 \equiv g_0^2 \pmod{10}$ .  $\therefore a^2 - a + 7 \equiv g_0^2 - g_0 + 7 \pmod{10}$ .  
 $\therefore g_0 \quad g_0^2 - g_0 + 7 \quad \overbrace{g_0^2 - g_0 + 7 - 10k}^{= 0, 5}$

0	7	7	$k = 0$
1	7	7	$k = 0$
2	9	9	$k = 0$
3	13	3	$k = 1$
4	19	9	$k = 1$
5	27	7	$k = 2$
6	37	7	$k = 3$
7	49	9	$k = 4$
8	63	3	$k = 5$
9	79	9	$k = 7$

Since  $g_0^2 - g_0 + 7 \equiv g_0^2 - g_0 + 7 - 10k \pmod{10}$ , Then  
 $a^2 - a + 7 \equiv 3, 7, \text{ or } 9 \pmod{10}$

8. Find the remainder when  $4444^{4444}$  is divided by 9.

Note that  $4444 \pmod{9} \equiv (4+4+4+4) \equiv 16 \pmod{9}$   
 $16 = 2^3 - 2$ , so  $4444 \pmod{9} \equiv 2^3 - 2 \pmod{9}$

Since  $2^3 \equiv (-1) \pmod{9}$ , Then  $4444 \equiv (-1) \cdot 2 \pmod{9}$

$$\therefore 4444^{4444} \equiv (-1)^{4444} \cdot 2^{4444} \equiv 2^{4444} \pmod{9}$$

But  $4444 = 3 \cdot 1381 + 1$ , so

$$2^{4444} = (2^3)^{1381} \cdot 2 \quad \therefore 2^{4444} \equiv (-1)^{1381} \cdot 2 \pmod{9}$$

$$\therefore 4444^{4444} \equiv 2^{4444} \equiv (-1) \cdot 2 \equiv 7 \pmod{9}$$

∴ remainder is ?

9. Prove that no integer whose digits add up to 15 can be a square or cube.

Pf: Let  $N$  be any integer whose digits add up to 15.

$$\therefore N \equiv 15 \pmod{9} \quad (\text{see pf. to Th. 4.5}).$$

$$\text{But } 15 \equiv 6 \pmod{9}.$$

$$\therefore N \equiv 6 \pmod{9}$$

$$\text{Consider } a = a_m 9^m + \dots + a_1 9 + a_0$$

$\therefore a \equiv a_0 \pmod{9}$ , and  $\therefore a^2 \equiv a_0^2 \pmod{9}$   
 and  $a^3 \equiv a_0^3 \pmod{9}$ .  
 Consider all possibilities of  $a_0$ :

for  $(\text{mod } 9)$

$a_0$	$a_0^2$	$a_0^2 \pmod{9}$	$a_0^3$	$a_0^3 \pmod{9}$
0	0	0	0	0
1	1	1	1	1
2	4	4	8	8
3	9	0	27	0
4	16	7	64	1
5	25	7	125	8
6	36	0	216	0
7	49	4	343	1
8	64	1	512	8

$\therefore a^2 \equiv 0, 1, 4, \text{ or } 7 \pmod{9}$

$\therefore$  There is no  $a^2$  s.t.  $a^2 \equiv 6 \pmod{9}$

$a^3 \equiv 0, 1, \text{ or } 8 \pmod{9}$ , and so There is no  
 $a^3$  s.t.  $a^3 \equiv 6 \pmod{9}$ .

10. Assuming 495 divides  $273 \times 49y5$ , find  $x, y$ .

Let  $495 \cdot N = 273 \times 49y5$

$$495 \equiv 0 \pmod{9}, \therefore 495 \cdot N \equiv 0 \cdot N \equiv 0 \pmod{9}$$

$$\therefore 273 \times 49y5 \equiv 0 \pmod{9}$$

$$\therefore (2+7+3+x+y+9+5) = 30+x+y \equiv 3+x+y \pmod{9}$$

$$\text{so } 3+x+y \equiv 0 \pmod{9}, \text{ or } x+y \equiv 6 \pmod{8}$$

$$\text{and } x+y \equiv 15 \pmod{9}$$

Also,  $5-9+4=0$ , so  $495 \equiv 0 \pmod{11}$ ,

$$\therefore 495 \cdot N \equiv 0 \pmod{11}$$

$$\therefore 273 \times 49y5 \equiv 0 \pmod{11}$$

$$\therefore 5-y+9-4+x-3+7-2 = x-y+12 \equiv 0 \pmod{11}$$

$$\therefore x-y \equiv -1 \pmod{11}, \text{ or } y-x \equiv 1 \pmod{11}$$

$$\therefore x+y=6$$

$$y-x=1$$

$$\frac{2y}{2} = 7, \text{ no integer}$$

$$x+y=15$$

$$y-x=1$$

$$\frac{2y}{2} = 16, y = 8, \underline{\underline{x=7}}$$

11. Determine the last 3 digits of  $7^{999}$

Need to use mod 1000 since want last 3 digits.

$$\text{Also, } 7^4 = 2401 = (1+6 \cdot 400)$$

Since  $400^2 = 160000$ , Then  $400^n \equiv 0 \pmod{100}$

for  $n \geq 2$ .

$$\therefore 7^{4n} = (1 + 6 \cdot 400)^n = \sum_{k=0}^n \binom{n}{k} 1^{n-k} (6 \cdot 400)^k$$

So for  $k \geq 2$ ,  $\binom{n}{k} (6 \cdot 400)^k \equiv 0 \pmod{1000}$

$$\therefore 7^{4n} \equiv 1 + \binom{n}{1} 6 \cdot 400 \pmod{1000}$$

$$\text{Now } 999 = 4 \cdot 249 + 3$$

$$\therefore 7^{4 \cdot 249} \equiv 1 + \binom{249}{1} (6 \cdot 400) \equiv 1 + 249 \cdot 6 \cdot 400 \pmod{1000}$$

$$249 \cdot 6 \cdot 400 = (49 + 200)(400)(6) = (6)(49)(400) + 6 \cdot 400 \cdot 200$$

$$\therefore 249 \cdot 6 \cdot 400 \equiv 6 \cdot 49 \cdot 400 \pmod{1000}$$

$$\begin{aligned} \therefore 7^{4 \cdot 249} &\equiv 1 + 6 \cdot 49 \cdot 400 \pmod{1000} \\ &\equiv 1 + 6 \cdot 9 \cdot 400 \pmod{1000} \end{aligned}$$

$$6 \cdot 9 \cdot 4 = 216, \therefore 1 + 6 \cdot 9 \cdot 400 = 21601$$

$$\therefore 7^{996} \equiv 601 \pmod{1000}$$

$$\therefore 7^{999} \equiv 601 \cdot 7^3 \pmod{1000}$$

$$7^3 = 343, (601)(343) = 206143$$

$$\therefore 7^{999} \equiv 206143 \equiv 143 \pmod{1000}.$$

143 are the last 3 digits.

12. If  $t_n$  is the  $n$ th triangular number, show that  
 $t_{n+2k} \equiv t_n \pmod{k}$ .  $\therefore t_n, t_{n+20}$  have same  
last digit.

$$\begin{aligned}
\text{Pf: } t_{n+2k} &= \frac{(n+2k)(n+2k+1)}{2} \\
&= \frac{n^2 + 2Kn + n + 2Kn + 4K^2 + 2K}{2} \\
&= \frac{n^2 + n + 4Kn + 4K^2 + 2K}{2} \\
\therefore t_{n+2k} - t_n &= \frac{n^2 + n + 4Kn + 4K^2 + 2K}{2} - \frac{n(n+1)}{2} \\
&= \frac{4Kn + 4K^2 + 2K}{2} \\
&= k(2n + 2k + 1)
\end{aligned}$$

$$\therefore t_{n+2k} \equiv t_n \pmod{k}$$

$$\therefore t_{n+20} \equiv t_n \pmod{10}, \text{ or}$$

$$t_{n+20} = t_n + 10k, \text{ some } k$$

$$\therefore \text{if } t_n = (a_m a_{m-1} \dots a_2 a_1 a_0)_{10}, \text{ Then}$$

adding  $10K$  not affect  $a_0$ , so  
 $t_{n+20}$  and  $t_n$  have same units digit.

13. For any  $n \geq 1$ , prove There exists a prime with at least  $n$  of its digits equal to 0.

Pf: This follows from Dirichlet's Theorem (p.56).

From problem #12 of section 2-2,

$\gcd(a, a+1) = 1$ .  $\therefore$  consider 9, 10 and arithmetic progressions with powers of 10.

$\therefore 9 + 10K, K=1, 2, 3, \dots$  contains infinitely many primes.

$10^{n+1} + 9$  has  $n$  zeros, and There only a finite number less than  $10^{n+1} + 9$ .

By Dirichlet's Theorem, There must be a prime in The series  $K \cdot 10^{n+1} + 9$ , and each has  $n$  zeros.

14. Find the values of  $n \geq 1$  for which  $1! + 2! + \dots + n!$  is a perfect square.

$$1! = 1 \quad 3! = 6$$

$$2! = 2 \quad 4! = 24$$

Note that for  $n \geq 5$ ,  $\sum_{k=1}^n k!$  ends in 0.

$$\therefore 1! = 1^2$$

$$1! + 2! = 3$$

$$1! + 2! + 3! = 9 = 3^2$$

$$1! + 2! + 3! + 4! = 33$$

$\therefore$  The units digits of  $\sum_{k=1}^n k!$  will be 3  
for  $n \geq 4$

By problem 1(g), a perfect square can't end in 3.  $\therefore$  There is no perfect square for  $n \geq 4$

$\therefore n = 1, 3$  are the only values.

15. Show that  $2^n$  divides an integer  $N \Leftrightarrow 2^n$  divides  
the number made up of the last  $n$  digits of  $N$ .

Pf: Let  $N = a_{n+j} 10^{n+j} + \dots + a_n 10^n + a_{n-1} 10^{n-1} + \dots + a_1 10 + a_0$

be the decimal representation for  $N$ ,  $n \geq 1, j \geq 0$ .

(a) If  $2^n$  divides the last  $n$  digits of  $N$ , Then

$$2^n \mid (a_{n-1} 10^{n-1} + \dots + a_1 10 + a_0) \quad [1]$$

$$\text{But } a_{n+j} 10^{n+j} + \dots + a_n 10^n = 10^n (a_{n+j} 10^j + \dots + a_n)$$

$$= 2^n 5^n (a_{n+j} 10^j + \dots + a_n)$$

$$\therefore 2^n \mid (a_{n+j} \cdot 10^{n+j} + \dots + a_n \cdot 10^n) \quad [2]$$

From [1] and [2],

$$2^n \mid (a_{n+j} \cdot 10^{n+j} + \dots + a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \dots + a_0), \text{ so } 2^n \mid N$$

(b) Suppose  $2^n \mid N$ . Since  $2^n \mid 2^k 5^{-k}$ , Then

$$2^n \mid 10^n (a_{n+j} \cdot 10^j + \dots + a_n)$$

$$\therefore 2^n \mid (a_{n+j} \cdot 10^{n+j} + \dots + a_n \cdot 10^n)$$

$$\therefore 2^n \mid N - (a_{n+j} \cdot 10^{n+j} + \dots + a_n \cdot 10^n)$$

$$\Rightarrow 2^n \mid (a_{n-1} \cdot 10^{n-1} + \dots + a_1 \cdot 10 + a_0)$$

$\therefore 2^n$  divides the last  $n$  digits of  $N$ .

16. Let  $N = a_m \cdot 10^m + \dots + a_1 \cdot 10 + a_0$ ,  $0 \leq a_k \leq 9$ , be the decimal expansion of a positive integer  $N$ .

(a) Prove 7, 11, and 13 all divide  $N \iff 7, 11, \text{ and } 13$  divide the integer

$$M = (a_0 + 10a_1 + 100a_2) - (a_3 + 10a_4 + 100a_5) + (a_6 + 10a_7 + 100a_8) - \dots$$

PF: Since  $1001 = 1000 + 1 = 1000 - (-1)$ .

$$\therefore 10^3 \equiv -1 \pmod{1001}$$

$$\text{Also, } 10^6 - 1 = (10^3 - 1)(10^3 + 1) \equiv 999(1001)$$

$$\therefore 10^6 \equiv 1 \pmod{1001}$$

$$\text{Also, } 1001 = 7 \cdot 11 \cdot 13$$

Consider  $10^{3n}$

If  $n$  is odd,  $n = 2k + 1$  for some  $k$

$$\therefore 10^{3n} = 10^{3(2k+1)} = 10^{6k+3} = 10^{6k} \cdot 10^3$$

But  $10^6 \equiv 1 \pmod{1001}$ , so

$$10^{6k} \equiv 1^k = 1 \pmod{1001}$$

$$\therefore 10^{6k} \cdot 10^3 \equiv 1(-1) = -1 \pmod{1001}$$

$$\therefore n \text{ odd} \Rightarrow 10^{3n} \equiv -1 \pmod{1001} \quad [1]$$

If  $n$  is even, Then  $n = 2k$ , some  $k$ .

$$\therefore 10^{3n} = 10^{6k} \equiv 1^k = 1 \pmod{1001}$$

$$\therefore n \text{ even} \Rightarrow 10^{3n} \equiv 1 \pmod{1001} \quad [2]$$

$$\text{Note } N = (a_0 + 10a_1 + 100a_2) - (-a_3 10^3 - a_4 10^4 - a_5 10^5) - \dots$$

$$= 10^0 (a_0 + a_1 10 + a_2 100) - 10^3 (-a_3 - a_4 10 - a_5 100) - \dots$$

even

odd

$$\text{From [2], j even: } a_{3j} \cdot 10^{3j} \equiv a_{3j} \pmod{1001} \quad [3]$$

$$a_{3j+1} \cdot 10^{3j+1} \equiv a_{3j+1} \cdot 10 \pmod{1001} \quad [4]$$

$$a_{3j+2} \cdot 10^{3j+2} \equiv a_{3j+2} \cdot 100 \pmod{1001} [5]$$

$$\text{From } [1], k \text{ odd: } a_{3k} \cdot 10^{3k} \equiv -a_{3k} \pmod{1001} [6]$$

$$a_{3k+1} \cdot 10^{3k+1} \equiv -a_{3k+1} \cdot 10 \pmod{1001} [7]$$

$$a_{3k+2} \cdot 10^{3k+2} \equiv -a_{3k+2} \cdot 100 \pmod{1001} [8]$$

Adding [3] + [4] + [5],  $j$  even:

$$a_{3j} \cdot 10^{3j} + a_{3j+1} \cdot 10^{3j+1} + a_{3j+2} \cdot 10^{3j+2} \equiv a_{3j} + a_{3j+1} \cdot 10 + a_{3j+2} \cdot 100 \pmod{1001} [9]$$

Adding [6] + [7] + [8],  $k$  odd:

$$a_{3k} \cdot 10^{3k} + a_{3k+1} \cdot 10^{3k+1} + a_{3k+2} \cdot 10^{3k+2} \equiv -a_{3k} - a_{3k+1} \cdot 10 - a_{3k+2} \cdot 100 \pmod{1001} [10]$$

Now let  $3k = 3j+3$ .  $\therefore 3k$  is odd, as  $k$  is odd.

Adding [9] + [10],

$$\begin{aligned} & a_{3j} \cdot 10^{3j} + a_{3j+1} \cdot 10^{3j+1} + a_{3j+2} \cdot 10^{3j+2} + a_{3j+3} \cdot 10^{3j+3} + a_{3j+4} \cdot 10^{3j+4} + a_{3j+5} \cdot 10^{3j+5} \\ & \equiv (a_{3j} + 10a_{3j+1} + 100a_{3j+2}) - (a_{3j+3} + 10a_{3j+4} + 100a_{3j+5}) \pmod{1001} \end{aligned}$$

$\therefore N \equiv M \pmod{1001}$ ,  $\therefore N \equiv M \pmod{7 \cdot 11 \cdot 13}$

$$\therefore N \equiv 0 \pmod{7 \cdot 11 \cdot 13} \Leftrightarrow M \equiv 0 \pmod{7 \cdot 11 \cdot 13}$$

(b). Prove  $G | N \Leftrightarrow G$  divides the integer  
 $M = a_0 + 4a_1 + \dots + 4a_m$

Pf:  $10 \equiv 4 \pmod{G}$ , and  $40 \equiv 4 \pmod{G}$

Lemma:  $10^n \equiv 4 \pmod{G}$ ,  $n \geq 1$

Pf: True for  $n=1$ , since  $10 \equiv 4 \pmod{6}$

Suppose true for  $k$ :  $10^k \equiv 4 \pmod{G}$

$$\therefore 10^{k+1} = 10^k \cdot 10 \equiv 4 \cdot 10 = 40 \equiv 4 \pmod{G}$$

$\therefore$  true for  $k+1$ .

$$\therefore a_k 10^k \equiv 4a_k, k \geq 1$$

$$\therefore N = a_0 + a_1 10 + \dots + a_m 10^m \equiv a_0 + 4a_1 + \dots + 4a_m \pmod{G}$$

$$\therefore N \equiv M \pmod{G}$$

$$\therefore N \equiv 0 \pmod{G} \Leftrightarrow M \equiv 0 \pmod{G}$$

17. Is 1,010,908,899 divisible by 7, 11, and 13?

$$9 + 9 \cdot 10 + 8 \cdot 100 - (8 + 0 \cdot 10 + 9 \cdot 100) + (0 + 1 \cdot 10 + 0 \cdot 100) - (1)$$

$$= 1 + 90 - 100 + 10 - 1$$

$$= 0$$

$$\therefore N \equiv 0 \pmod{1001}, \therefore N \text{ divisible by } 7, 11, 13$$

18. (a) Given integer  $N$ , let  $M$  be the integer formed by reversing the order of digits of  $N$ . Show  $N-M$  is divisible by 9.

$$\text{Pf: Let } N = a_m 10^m + \dots + 10a_1 + a_0$$

$$\therefore M = a_0 10^m + \dots + a_k 10^{m-k} + \dots + a_{m-1} 10 + a_m$$

$$\therefore N-M = (a_m - a_0) 10^m + \dots + (a_1 - a_{m-1}) 10 + (a_0 - a_m)$$

The sum of the coefficients of  $N-M$  is:

$$(a_m + a_{m-1} + \dots + a_0) - (a_0 + \dots + a_{m-1} + a_m) = 0.$$

$\therefore$  By Th. 4.5, since  $9|0$ ,  $9|(N-M)$

(b) Prove any palindrome with an even number of digits is divisible by 11.

Pf: Let  $N = a_m 10^m + \dots + a_0$  have even number of digits.  $\therefore m$  is odd.

$$\text{Also, } N = a_0 10^m + \dots + a_{m-1} 10 + a_m$$

$\therefore a_m = a_0, a_{m-1} = a_1, \text{ and in general,}$

$$a_k = a_{m-k}, 0 \leq k \leq m$$

Look at  $T = (a_0 - a_1) + (a_2 - a_3) + \dots + (a_{m-1} - a_m)$

Since  $m$  is odd, There is no coefficient  
That is ungrouped.

Rearranging terms of  $T$ , by reversing the  
order of the negative coefficients,

$$T = (a_0 - a_m) + (a_2 - a_{m-1}) + \dots + (a_{m-1} - a_1)$$

$$\begin{aligned} &= 0 + 0 + \dots + 0 \\ &= 0 \end{aligned}$$

$\therefore$  By Th. 4.6, 11 (N).

19. Given repunit  $R_n$ , prove:

$$(a) 9 | R_n \Leftrightarrow 9 | n$$

Pf: Note for  $R_n$ , sum of digits,  $S$ , is  $n$   
since  $R_n = 11\dots1$  ( $n$  digits of 1).

$\therefore$  since  $R_n \equiv S \pmod{9}$  by Th. 4.5,  
 $\therefore R_n \equiv n \pmod{9}$ .

$$\therefore R_n \equiv 0 \pmod{9} \Leftrightarrow n \equiv 0 \pmod{9}$$

(6)  $11 \mid R_n \Leftrightarrow n$  is even

Pf: Let  $R_n = 1 \cdot 10^m + \dots + 1 \cdot 10 + 1$

$$\begin{aligned} \text{Look at } T &= (a_0 - a_1) + (a_2 - a_3) + \dots + (-1)^m a_m \\ &= (1-1) + (1-1) + \dots + (-1)^m a_m \end{aligned}$$

$T$  will be 0  $\Leftrightarrow$  can group terms, which means  $m$  is odd  
 $\therefore T = 0 \Leftrightarrow$  number terms is even.

$\therefore$  By Th. 4.6,  $11 \mid R_n \Leftrightarrow T = 0$

$\therefore 11 \mid R_n \Leftrightarrow n$  is even.

20. Factor  $R_6 = 111,111$  into a product of primes

Since  $R_6$  has an even number of groups of three coefficients, and

$$M = (1 + 1 \cdot 10 + 1 \cdot 100) - (1 + 1 \cdot 10 + 1 \cdot 100)$$

Then  $R_6 \stackrel{=0}{\equiv} 0 \pmod{1001}$  by prob. 16.(a).

$$\therefore R_6 = 111,111 = 7 \cdot 11 \cdot 13 \cdot k = 1001 \cdot k$$

Try  $k=111$  since  $111 \cdot 1,000 = 111,000$ .

Find that  $R_6 = 111 \cdot 1001$ , and  $111 = 3 \cdot 37$   
 $\therefore R_6 = 3 \cdot 7 \cdot 11 \cdot 13 \cdot 37$

21. Show why  $1 \cdot 9 + 2 = 11$   
 $12 \cdot 9 + 3 = 111$   
⋮

$$123456789 \cdot 9 + 10 = 11111111$$

i.e. show that

$$(10^{n-1} + 2 \cdot 10^{n-2} + \dots + n) \cdot 9 + (n+1) = \frac{10^{n+1} - 1}{9}$$

Since  $9 = 10 - 1$ , Then

$$\begin{aligned} (10^{n-1} + 2 \cdot 10^{n-2} + \dots + n) \cdot 9 &= (10^{n-1} + 2 \cdot 10^{n-2} + \dots + n)(10 - 1) \\ &= (10^{n-1} + 2 \cdot 10^{n-2} + \dots + (n-1) \cdot (10 + n)) \cdot 10 - (10^{n-1} + \dots + n) \\ &= 10^n + 2 \cdot 10^{n-1} + 3 \cdot 10^{n-2} + \dots + (n-1) \cdot 10^2 + n \cdot 10 - (10^{n-1} + \dots + n) \\ &= 10^n + 1 \cdot 10^{n-1} + 1 \cdot 10^{n-2} + \dots + 1 \cdot 10 - n \\ \therefore (10^{n-1} + 2 \cdot 10^{n-2} + \dots + n) \cdot 9 + (n+1) &= \\ &= 10^n + 1 \cdot 10^{n-1} + 1 \cdot 10^{n-2} + \dots + 1 \cdot 10 - n + (n+1) \end{aligned}$$

$$= 10^n + 1 \cdot 10^{n-1} + \dots + 1 \cdot 10 + 1 \quad [1]$$

This latter basically proves the assertion.  
However, to go further, multiply [1] by 9  
and add 1.

$$(10^n + 1 \cdot 10^{n-1} + \dots + 1 \cdot 10 + 1) \cdot 9 + 1$$

$$= (10^n + 10^{n-1} + \dots + 10 + 1)(10 - 1) + 1$$

$$\begin{aligned} &= 10^{n+1} + 10^n + \dots + 10^2 + 10 \\ &\quad - 10^n - 10^{n-1} - \dots - 10 - 1 + 1 \end{aligned}$$

$$= 10^{n+1}$$

$$\therefore 10^n + 1 \cdot 10^{n-1} + \dots + 1 \cdot 10 + 1 \quad [1]$$

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

$$\therefore (10^{n-1} + 2 \cdot 10^{n-2} + \dots + n) \cdot 9 + (n+1) = \frac{10^{n+1} - 1}{9}$$

22. An invoice shows that 72 canned hams were purchased for \$x 67.9y. Find the missing digits.

Solution:  $72 \cdot N = x679y$ , where  $N$  = cost in cents  
of one ham.

$$\text{Note } 72 = 8 \cdot 9 = 2^3 \cdot 9. \therefore 2^3 \mid x679y$$

$$\text{By problem 15, } 2^3 \mid 79y \therefore y=2$$

$$\text{Since } 79y \div 8 = 90 + 7y, \text{ and } \therefore 8 \mid 7y$$

$$\therefore x679y = x6792$$

$$\text{Since } 9 \mid 72, 9 \mid x6792, \therefore 9 \mid x+6+7+9+2$$

$$\therefore x=3$$

$$\therefore x679y = 36792 \quad (x=3, y=2)$$

23. If 792 divides  $13xy45z$ , find  $x, y, z$

Solution: Since  $792 = 8 \cdot 99$ ,  $8 \mid 722$ , so

$8 \mid 13xy45z$ , and by problem 15,  $8 \mid 45z$

$$45z = 8 \cdot 56 + 5z, \therefore 8 \mid 5z, \therefore z=6$$

Since  $9 \mid 13xy456$ ,  $9 \mid 1+3+x+y+4+5+6$ ,  
 $\therefore 9 \mid 1+x+y$ ,  $\therefore x+y+1=9, 18$ ,  $x+y=8, 17$

Also,  $6 \mid 792$ , so, by problem 16(5),

$$6 \mid 6+4 \cdot 5+4 \cdot 4+4y+4x+4 \cdot 3+4 \cdot 1, \text{ or}$$

$$6 \mid 4y+4x+58, \text{ or } 6 \mid 4x+4y+4$$

$$\therefore 6 \mid 4(1+x+y), \text{ so } 3 \mid (1+x+y)$$

This doesn't help since  $9 \mid (1+x+y)$ .

Note  $11 \mid 792$ , so  $11 \mid 13xy456$

$$\therefore 11 \mid 6 - 5 + 4 - y + x - 3 + 1, \text{ or } 11 \mid 3 + x - y$$

$$\therefore 3 + x - y = 11 \quad (\text{can't } = 22, \text{ since } x, y \leq 9)$$

$$\therefore x - y = 8$$

From  $9 \mid 1 + x + y$ ,  $x + y = 8, 17$

$$\begin{array}{ll} \therefore x + y = 8 & x + y = 17 \\ x - y = 8 & x - y = 8 \end{array}$$

$$\therefore x = 8, y = 0 \quad 2x = 25, \therefore \text{not a solution}$$

$$\therefore 13xy45z = 1380456$$

24. For any prime  $p > 3$ , prove  $13 \mid 10^{2p} - 10^p + 1$

Pf: Use result of problem 16(a) and look at possible coefficients of the constructed integer  $M$ , formed by alternately summing and subtracting blocks of 3 coefficients of the decimal expansion of  $N$ .

For an integer  $N$ , proof of 16(a) showed  $N \equiv M \pmod{7 \cdot 11 \cdot 13}$ .  $\therefore N \equiv m \pmod{13}$ .

$\therefore$  Goal is to show constructed  
 $M \equiv 0 \pmod{13}$ , and so  $N \equiv 0 \pmod{13}$ .

To analyze  $M$ , look at decimal expansion  
coefficients of  $N = 10^{2p} - 10^p + 1$ .

First consider  $10^p$ . Since  $p$  is prime,  
 $p$  is odd, so there will be an odd  
number of zeros in  $10^p$ .

$$\begin{aligned}\text{Example: } 10^5 &= 1 \cdot 10^5 + 0 \cdot 10^4 + \dots + 0 \cdot 10 + 0 \\ &= a_5 \cdot 10^5 + a_4 \cdot 10^4 + \dots + a_1 \cdot 10 + a_0\end{aligned}$$

Look at  $M$ :

Note  $p > 3$ .

For  $p = 5, 11, 17, \dots$   
 $m = -100$

For  $p = 7, 13, \dots$   
 $m = +10$

$p \neq 9, 15, \dots$  as  $p$   
is prime.

	100x	10x	1x	+/-
value of k	$a_{k+2}$	$a_{k+1}$	$a_k$	
	2	1	0	+
	5	4	3	-
	8	7	6	+
	11	10	9	-
	14	13	12	+
	17	16	15	-
			:	

From Div. Alg.,  $p = 3q + r$ , and as  $p$  is prime,  $r \neq 0$ .

$\therefore$  Can restrict considerations to  $p = 3q + 1$

or  $p = 3q + 2$ , as above, and  $p > 3$ .

For  $p = 3q + 1$ ,  $q$  must be even for  $p$  to be odd. Let  $q = 2K$ .  $\therefore p = 6K + 1$  ( $K = 1, 2, \dots$ )

For  $p = 3q + 2$ ,  $q$  must be odd. Let  $q = 2K' + 1$ .

$\therefore p = 6K' + 5$  ( $K' = 0, 1, \dots$ )

$\therefore p = 6K + 1$  ( $K = 1, 2, \dots$ ), or

$p = 6K' + 5$  ( $K' = 0, 1, 2, \dots$ )

$\therefore 10^p = 10^{6K} \cdot 10$  ( $K = 1, 2, \dots$ ), or

$10^p = 10^{6K'} \cdot 10^5$  ( $K' = 0, 1, 2, \dots$ )

From above, since  $M = -100$  for  $10^5$ , and since  $N \equiv M \pmod{13}$ , letting  $N = 10^5$ , Then  $10^5 \equiv -100 \pmod{13}$   
Similarly  $10 \equiv 10 \pmod{13}$

Since  $10^6 \equiv 1 \pmod{13}$ ,  $10^{6K} \equiv 1^k \equiv 1 \pmod{13}$

$\therefore 10^p = 10^{6K} \cdot 10 \equiv 10 \pmod{13}$  ( $K = 1, 2, \dots$ )

$10^p = 10^{6K'} \cdot 10^5 \equiv 10^5 \pmod{13}$  ( $K' = 0, 1, 2, \dots$ )

and  $10^5 \equiv -100 \pmod{13}$

$$\therefore 10^p \equiv 10 \pmod{13} \quad (k=1, 2, \dots) \quad [1]$$

or

$$10^p \equiv -100 \pmod{13} \quad (k'=0, 1, 2, \dots)$$

$$\text{For } 10^{2p}: \quad 2p = 12k + 2 \quad (k=1, 2, \dots)$$

$$2p = 12k' + 10 \quad (k'=0, 1, 2, \dots)$$

$$\therefore 10^{2p} = 10^{12k} \cdot 100 \quad (k=1, 2, \dots)$$

$$10^{2p} = 10^{12k'} \cdot 10^5 \cdot 10^5 \quad (k'=0, 1, 2, \dots)$$

Using  $N \equiv M \pmod{13}$ ,  $N = 10^{2p}$ , and  
using  $10^6 \equiv 1 \pmod{13}$ , so  $10^{12k} \equiv 1 \pmod{13}$ ,

$$\therefore 10^{2p} \equiv 100 \pmod{13} \quad (k=1, 2, \dots) \quad [2]$$

or

$$10^{2p} \equiv 10^5 \cdot 10^5 \pmod{13} \quad (k'=0, 1, 2, \dots)$$

From above,  $10^5 \equiv -100 \pmod{13}$

$$\therefore 10^5 \cdot 10^5 \equiv (-100)(-100) = 10000 \pmod{13}$$

Since  $\gcd(10, 13) = 1$ , Then

$$10^5 / 10 \equiv -100 / 10 \pmod{13}, \text{ so}$$

$$10000 \equiv -10 \pmod{13}$$

$$\therefore \text{From [2]}, \quad 10^{2p} \equiv 100 \pmod{13} \quad (k=1, 2, 3, \dots) \quad [2']$$

$$10^{2p} \equiv -10 \pmod{13} \quad (k'=0, 1, 2, \dots)$$

$$\therefore N = 10^{2p} - 10^p + 1 = [2'] - [1] + 1 \quad \text{becomes}$$

$$10^{2p} - 10^p + 1 \equiv 100 - 10 + 1 = 91 \pmod{13} \quad (k=1, 2, 3, \dots)$$

$$10^{2p} - 10^p + 1 \equiv -10 - (-100) + 1 = 91 \pmod{13} \quad (k'=0, 1, 2, \dots)$$

But  $91 = 7 \cdot 13$ , so  $91 \equiv 0 \pmod{13}$

$$\therefore 10^{2p} - 10^p + 1 \equiv 0 \pmod{13}, \text{ so}$$

$$13 \mid (10^{2p} - 10^p + 1).$$

## 4.4 Linear Congruences

Note Title

3/21/2005

Note that since  $\{0, 1, \dots, n-1\}$  is a complete set of residues mod  $n$ , Then  $\{0, c \cdot 1, c \cdot 2, \dots, c \cdot (n-1)\}$  is also a complete set mod  $n$  if  $\gcd(c, n) = 1$ , by prob. 10, p. 69

$\therefore$  for  $cx \equiv r \pmod{n}$ , to find a solution, you can just test for  $x = 0, 1, \dots, n-1$ , since  $r$  must be congruent to one of  $0, c, \dots, c \cdot (n-1)$  if  $\gcd(c, n) = 1$ .

$\therefore$  When solving for  $Nx \equiv 1 \pmod{n_K}$ , you can try  $x = 0, 1, \dots, n_K - 1$  to find one solution, provided  $\gcd(N, n_K) = 1$ .

1. (a).  $25x \equiv 15 \pmod{29}$

$\gcd(25, 29) = 1$ ,  $\therefore$  solution exists

$$-4x \equiv -14 \quad (\text{adding } -29)$$

$$2x \equiv 7 \quad (\gcd(2, 29) = 1)$$

$$30x \equiv 105 \quad (\text{mult. by } 15)$$

$$x \equiv 70 \quad (\text{adding } -29)$$

$$\therefore x \equiv 18 \pmod{29} \quad (\text{adding } -58 \text{ on right})$$

(b)  $5x \equiv 2 \pmod{26}$

$$\begin{aligned} \gcd(5, 26) &= 1, \therefore \text{solution exists.} \\ 25x &\equiv 10 \quad (\text{mult. by } 5) \\ 25x - 26x &\equiv 10 - 26 \quad (\bmod 26) \\ -x &\equiv -16 \\ \therefore x &\equiv 16 \quad (\bmod 26) \end{aligned}$$

$$(c) 6x \equiv 15 \quad (\bmod 21)$$

$$\begin{aligned} \gcd(6, 21) &= 3, 3 \mid 15, \therefore \text{solution exists.} \\ 2x &\equiv 5 \quad (\bmod 7) \quad (\text{divide by } 3) \\ 2x &\equiv 12 \quad (\bmod 7) \quad (\text{add } 7) \\ x &\equiv 6 \quad (\bmod 7) \quad (\gcd(2, 7) = 1, \text{ divide by } 2) \\ \therefore x &= 6 + 7t \end{aligned}$$

Since  $\gcd(6, 21) = 3$ , There are 3 mutually incongruent solutions, by Th. 4.7, and by Th. 4.7, they are  $t = 0, 1, 2$ .

$$\therefore x \equiv 6, 13, 20 \quad (\bmod 21)$$

$$(d) 36x \equiv 8 \quad (\bmod 102)$$

$\gcd(36, 102) = 6$ , and  $6 \nmid 8$ ,  $\therefore$  no solution

$$(e) 34x \equiv 60 \quad (\bmod 78)$$

$\gcd(34, 78) = 2$ ,  $2 \mid 60$ ,  $\therefore$  solution exists.

$$102x \equiv 180 \pmod{98} \quad (\text{mult. by } 3)$$

$$102x - 98x \equiv 180 - 2 \cdot 98 \pmod{98}$$

$$4x \equiv -16 \pmod{98}$$

$$2x \equiv -8 \pmod{49}$$

$$x \equiv -4 \pmod{49} \quad (\gcd(2, 49) = 1)$$

$$\therefore x = -4 + 49t$$

By Th. 4.7, two incongruent solutions exist.

$$\therefore t = 0, 1 \Rightarrow x \equiv -4, 45, \text{ or}$$

$$x \equiv 45, 98 \pmod{98}.$$

(f).  $140x \equiv 133 \pmod{301}$

$$140 = 2^2 \cdot 5 \cdot 7, \quad 301 = 7 \times 43, \quad \therefore \gcd(140, 301) = 7$$

and  $7 \nmid 133$ .  $\therefore 7$  incongruent solutions exist.

$$20x \equiv 19 \pmod{43} \quad (\text{divide by } 7)$$

$$40x \equiv 38 \pmod{43} \quad (\text{multiply by } 2)$$

$$43x - 40x \equiv 43 - 38 \pmod{43}$$

$$3x \equiv 5 \pmod{43}$$

$$42x \equiv 70 \pmod{43} \quad (\text{mult. by } 14)$$

$$43x - 42x \equiv 86 - 70 \pmod{43}$$

$$x \equiv 16 \pmod{43}$$

$$\therefore x = 16 + 43t, \quad \therefore 52t = 0, 1, 2, 3, 4, 5, 6$$

$$\therefore x \equiv 16, 59, 102, 145, 188, 231, 274 \pmod{301}$$

$$2.(a). 4x + 51y = 9$$

$$\begin{aligned} 4x &\equiv 9 \pmod{51} \\ 52x &\equiv 117 \quad (\text{mult. by 13}) \\ x &\equiv 15 \quad (\text{subtract } 51x, 102) \\ \therefore x &= 15 + 51t \end{aligned}$$

$$\begin{aligned} 51y &\equiv 9 \pmod{4} \\ 17y &\equiv 3 \pmod{4} \\ 17y - 16y &\equiv 3 \pmod{4} \\ y &\equiv 3 \pmod{4} \\ \therefore y &= 3 + 4s \end{aligned} \quad (\gcd(51, 4) = 1, \text{divide by 3})$$

$$\begin{aligned} \therefore 4x + 51y &= 4(15 + 51t) + 51(3 + 4s) \\ &= 60 + 204t + 153 + 204s \\ \therefore 9 &= 213 + 204t + 204s \\ \therefore -204 &= 204t + 204s \\ -1 &= t + s \\ 5 &= -1 - t \end{aligned}$$

$$\begin{aligned} \therefore x &= 15 + 51t \\ y &= 3 + 4(-1 - t) = -1 - 4t \end{aligned}$$

$$(6) 12x + 25y = 331$$

$$12x \equiv 331 \pmod{25}$$

$$24x \equiv 662$$

$$25\bar{x} - 24x \equiv 662 - 650 \pmod{25}$$

$$x \equiv 12 \pmod{25}$$

$$\therefore x = 12 + 25t$$

$$25y \equiv 331 \pmod{12}$$

$$25y - 24y \equiv 381 - 324 \pmod{12}$$

$$y \equiv 7 \pmod{12}$$

$$\therefore y = 7 + 12s$$

$$\begin{aligned}\therefore 12x + 25y &= 12(12 + 25t) + 25(7 + 12s) \\ &= 144 + 300t + 175 + 300s\end{aligned}$$

$$\therefore 331 = 319 + 300t + 300s$$

$$12 = 300t + 300s$$

$$1 = 25t + 25s$$

$$\therefore 25t = 1 - 25s$$

$$\therefore x = 12 + 25t = 13 - 25s$$

$$\therefore x = 13 - 25s$$

$$y = 7 + 12s$$

$$(C) 5x - 53y = 17$$

$$5x \equiv 17 \pmod{53}$$

$$55x \equiv 187 \pmod{53} \quad (\text{mult. by } 11)$$

$$55x - 53x \equiv 187 - 3 \cdot 53 \pmod{53}$$

$$2x \equiv 28 \pmod{53}$$

$$x \equiv 14 \pmod{53} \quad (\gcd(2, 53) = 1, \text{ divide by } 2)$$

$$\therefore x = 14 + 53t$$

$$-53y \equiv 17 \pmod{5}$$

$$-53y + 50y \equiv 17 \pmod{5}$$

$$-3y \equiv 17 \pmod{5}$$

$$-3y \equiv 51 \pmod{5} \quad (\text{mult. by } 3)$$

$$y \equiv 51 \pmod{5} \quad (\text{add } 10y)$$

$$\therefore y = 51 + 5s$$

$$\therefore 5x - 53y = 5(14 + 53t) - 53(51 + 5s)$$

$$17 = 70 + 265t - 2703 - 265s$$

$$2650 = 265t - 265s$$

$$10 = t - s, \quad s = t - 10$$

$$\therefore y = 51 + 5(t - 10) = 5t + 1$$

$$\therefore x = 14 + 53t$$

$$y = 1 + 5t$$

3. Find all solutions to  $3x - 7y \equiv 11 \pmod{13}$

$$3x \equiv 7y + 11 \pmod{13}$$

$\gcd(3, 13) = 1$ , so  $1 \mid (7y + 1)$ . There are 13 incongruent possibilities for  $y$  ( $0, 1, \dots, 12$ )

$\therefore$

$$y \equiv 0: 3x \equiv 11 \pmod{13}$$

$$12x \equiv 44$$

$$12x - 13x \equiv 44 - 3 \cdot 13$$

$$-x \equiv 5, x \equiv -5 + 13$$

$$x \equiv 8$$

$$y \equiv 1: 3x \equiv 18 \pmod{13}$$

$$12x \equiv 72$$

$$-x \equiv 72 - 5 \cdot 13$$

$$x \equiv -7 + 13$$

$$x \equiv 6$$

$$y \equiv 2: 3x \equiv 25 - 26 \pmod{13}$$

$$12x \equiv -4$$

$$12x - 13x \equiv -4$$

$$x \equiv 4$$

$$y \equiv 3: 3x \equiv 32 \pmod{13}$$

$$12x \equiv 4(32 - 3 \cdot 13)$$

$$12x - 13x \equiv -28 + 26$$

$$x \equiv 2$$

$$y \equiv 4: 3x \equiv 39 \pmod{13}$$

$$12x \equiv 4 \cdot (39 - 3 \cdot 13)$$

$$-x \equiv 0$$

$$x \equiv 0$$

$$y \equiv 5: 3x \equiv 46 \pmod{13}$$

$$12x \equiv 4(46 - 3 \cdot 13)$$

$$-x \equiv 28 - 26 = 2$$

$$x \equiv -2, x \equiv 11$$

$\therefore$  From pattern, all  $\pmod{13}$

$$\begin{aligned} y &\equiv 0, x \equiv 8 \\ y &\equiv 1, x \equiv 6 \\ y &\equiv 2, x \equiv 4 \\ y &\equiv 3, x \equiv 2 \end{aligned}$$

$$\begin{aligned} y &\equiv 4, x \equiv 0 \\ y &\equiv 5, x \equiv 11 \\ y &\equiv 6, x \equiv 9 \\ y &\equiv 7, x \equiv 7 \end{aligned}$$

$$\begin{aligned} y &\equiv 8, x \equiv 5 \\ y &\equiv 9, x \equiv 3 \\ y &\equiv 10, x \equiv 1 \\ y &\equiv 11, x \equiv 12 \quad (\equiv -1) \\ y &\equiv 12, x \equiv 10 \end{aligned}$$

4. (a).  $x \equiv 1 \pmod{3}$   
 $x \equiv 2 \pmod{5}$   
 $x \equiv 3 \pmod{7}$

$$N = 3 \cdot 5 \cdot 7 = 105$$

$$N_1 = \frac{105}{3} = 35, \quad N_2 = \frac{105}{5} = 21, \quad N_3 = \frac{105}{7} = 15$$

$$\begin{aligned} 35x &\equiv 1 \pmod{3} & 21x &\equiv 1 \pmod{5} & 15x &\equiv 1 \pmod{7} \\ 35x - 36x &\equiv 1 & 21x - 20x &\equiv 1 & 15x - 14x &\equiv 1 \\ -x &\equiv 1 & x &\equiv 1 \pmod{5} & x &\equiv 1 \pmod{7} \\ x &\equiv -1 \pmod{3} \end{aligned}$$

$\therefore x_1 = -1, x_2 = 1, x_3 = 1$

$$\begin{aligned} \therefore a_1 N_1 x_1 + a_2 N_2 x_2 + a_3 N_3 x_3 &= \\ 1 \cdot 35 \cdot (-1) + 2 \cdot 21 \cdot 1 + 3 \cdot 15 \cdot 1 &= 52 \end{aligned}$$

$$\therefore x \equiv 52 \pmod{105}$$

(b).  $x \equiv 5 \pmod{11}$   
 $x \equiv 14 \pmod{29}$   
 $x \equiv 15 \pmod{31}$

$$N = 11 \cdot 29 \cdot 31 = 9889$$

$$N_1 = 29 \cdot 31 = 889, \quad N_2 = 11 \cdot 31 = 341, \quad N_3 = 11 \cdot 29 = 319$$

$$\begin{array}{lll}
 899x \equiv 1 \pmod{11} & 341x \equiv 1 \pmod{29} & 319x \equiv 1 \pmod{31} \\
 899x - 81 \cdot 11x \equiv 1 & 341x - 12 \cdot 29x \equiv 1 & 319x - 310x \equiv 1 \\
 878x \equiv 1 & 341x - 348x \equiv 1 & 9x \equiv 1 \\
 8x \equiv 1 & -7x \equiv 1 & 63x \equiv 7 \\
 32x \equiv 4 & -28x \equiv 4 & x \equiv 7 \\
 32x - 33x \equiv 4 & x \equiv 4 & \\
 x \equiv -4 \pmod{11} & &
 \end{array}$$

$$\therefore x_1 = -4, x_2 = 4, x_3 = 7$$

$$\begin{aligned}
 & \because q_1 N_1 x_1 + q_2 N_2 x_2 + q_3 N_3 x_3 = \\
 & 5 \cdot 899 \cdot (-4) + 14 \cdot 341 \cdot 4 + 15 \cdot 319 \cdot 7 = 34,611
 \end{aligned}$$

$$\begin{aligned}
 & \therefore x \equiv 34,611 \equiv 34,611 - 3 \cdot 9889 \equiv 4,944 \\
 & \quad (\pmod{9889})
 \end{aligned}$$

$$\begin{array}{ll}
 \text{(C)} \quad x \equiv 5 \pmod{6} & N = 6 \cdot 11 \cdot 17 = 1122 \\
 x \equiv 4 \pmod{11} & N_1 = 11 \cdot 17 = 187 \\
 x \equiv 3 \pmod{17} & N_2 = 6 \cdot 17 = 102 \\
 & N_3 = 6 \cdot 11 = 66
 \end{array}$$

$$\begin{array}{lll}
 187x \equiv 1 \pmod{6} & 102x \equiv 1 \pmod{11} & 66x \equiv 1 \pmod{17} \\
 187x - 186x \equiv 1 & 102x - 99x = 3x \equiv 1 & 66x - 68x = -2x \equiv 1 \\
 x \equiv 1 & 21x \equiv 1 & 18x \equiv -9 \\
 21x - 22x \equiv -x \equiv 1 & & 18x - 17x = x \equiv -9
 \end{array}$$

$$\therefore x_1 = 1, x_2 = -7, x_3 = -9$$

$$\begin{aligned} & \because a_1 N_1 x_1 + a_2 N_2 x_2 + a_3 N_3 x_3 = \\ & 5 \cdot 187 \cdot 1 + 4 \cdot 102 \cdot (-7) + 3 \cdot 66 \cdot (-9) = -3703 \end{aligned}$$

$$\therefore x \equiv -3703 + 4 \cdot 1122 = 285 \pmod{1122}$$

$$\begin{aligned} (d). \quad 2x \equiv 1 \pmod{5} & : 4x \equiv 2, 4x - 5x = -x, x \equiv -2 \pmod{5} \\ 3x \equiv 9 \pmod{6} & : x \equiv 3 \pmod{2} \\ 4x \equiv 1 \pmod{7} & : 8x \equiv 2, 8x - 7x = x, x \equiv 2 \pmod{7} \\ 5x \equiv 9 \pmod{11} & : 10x \equiv 18, 10x - 11x = -x, x \equiv -18 \pmod{11} \end{aligned}$$

$$N = 5 \cdot 2 \cdot 7 \cdot 11 = 770 \quad N_1 = 2 \cdot 7 \cdot 11 = 154 \quad N_2 = 5 \cdot 2 \cdot 11 = 110$$

$$N_3 = 5 \cdot 7 \cdot 11 = 385 \quad N_4 = 5 \cdot 2 \cdot 7 = 70$$

$$\begin{aligned} 154x_1 & \equiv 1 \pmod{5} & 385x_2 & \equiv 1 \pmod{2} \\ x_1 & \equiv -1 & x_2 & \equiv 1 \end{aligned}$$

$$110x_3 \equiv 1 \pmod{7} \quad 70x_4 \equiv 1 \pmod{11}$$

$$110x_3 - 7 \cdot 15x_1 = 5x_3 \equiv 1 \quad 70x_4 - 66x_4 = 4x_4 \equiv 1$$

$$\begin{aligned} 15x_3 & \equiv 3 & 12x_4 & \equiv 3 \\ x_3 & \equiv 3 & x_4 & \equiv 3 \end{aligned}$$

$$\begin{aligned} & \therefore a_1 N_1 x_1 + a_2 N_2 x_2 + a_3 N_3 x_3 + a_4 N_4 x_4 = \\ & (-2)(154)(-1) + 3 \cdot 385 \cdot 1 + 2 \cdot 110 \cdot 3 + (-18) \cdot 70 \cdot 3 = -1657 \\ & \therefore x \equiv -1657 + 3 \cdot 770 = 653 \pmod{770} \end{aligned}$$

$$5. \quad 17x \equiv 3 \pmod{2 \cdot 3 \cdot 5 \cdot 7}$$

$$17x \equiv 3 \pmod{2} \Leftrightarrow x \equiv 1 \pmod{2} \Leftrightarrow x \equiv 1 \pmod{2}$$

$$17x \equiv 3 \pmod{3} \Leftrightarrow 2x \equiv 0 \pmod{3} \Leftrightarrow x \equiv 0 \pmod{3}$$

$$17x \equiv 3 \pmod{5} \Leftrightarrow 2x \equiv 3 \pmod{5} : 4x \equiv 6, x \equiv -6 \pmod{5}$$

$$17x \equiv 3 \pmod{7} \Leftrightarrow 3x \equiv 3 \pmod{7} : 6x \equiv 6, x \equiv -6 \pmod{7}$$

$$N = 2 \cdot 3 \cdot 5 \cdot 7 = 210 \quad N_1 = 3 \cdot 5 \cdot 7 = 105 \quad N_3 = 2 \cdot 3 \cdot 7 = 42$$

$$N_2 = 2 \cdot 5 \cdot 7 = 70 \quad N_4 = 2 \cdot 3 \cdot 5 = 30$$

$$105x_1 \equiv 1 \pmod{2} \quad 70x_2 \equiv 1 \pmod{3}$$

$$x_1 \equiv 1 \quad 70x_2 - 69x_2 = x_2 \equiv 1$$

$$42x_3 \equiv 1 \pmod{5}$$

$$30x_4 \equiv 1 \pmod{7}$$

$$84x_3 \equiv 2$$

$$90x_4 \equiv 3$$

$$84x_3 - 85x_3 = 2$$

$$90x_4 - 7 \cdot 13x_4 = -x_4 \equiv 3$$

$$x_3 \equiv -2$$

$$x_4 \equiv -3$$

$$\therefore a_1 N_1 x_1 + a_2 N_2 x_2 + a_3 N_3 x_3 + a_4 N_4 x_4 = \\ 1 \cdot 105 \cdot 1 + 0 \cdot 70 \cdot 1 + (-6)(42)(-2) + (-6)(30)(-3) = 1149$$

$$\therefore x \equiv 1149 - 5 \cdot 210 = 99 \pmod{210}$$

6. Find smallest integer  $a \geq 2$  s.t.

$$2|a, 3|a+1, 4|a+2, 5|a+3, 6|a+4$$

This is equivalent to:

$$\begin{array}{ll}
 a \equiv 0 \pmod{2} & \text{or} \\
 a+1 \equiv 0 \pmod{3} & \\
 a+2 \equiv 0 \pmod{4} & \\
 a+3 \equiv 0 \pmod{5} & \\
 a+4 \equiv 0 \pmod{6} & \\
 \end{array}
 \quad
 \begin{array}{ll}
 a \equiv 0 \pmod{2} & [1] \\
 a \equiv -1 \pmod{3} & [2] \\
 a \equiv -2 \pmod{4} & [3] \\
 a \equiv -3 \pmod{5} & [4] \\
 a \equiv -4 \pmod{6} & [5]
 \end{array}$$

Note that  $\gcd(2, 4) = 2$ . So eliminate #1, since if  $[3]$  is true,  $[1]$  is automatically true.

Also,  $\gcd(3, 6) \neq 1$ . Multiply  $[2]$  by 2 and get

$$(a+1) \cdot 2 \equiv 0 \cdot 2 \pmod{3 \cdot 2}, \text{ or}$$

$$2a+2 \equiv 0 \pmod{6}$$

Combine this with  $[5]$  and get

$$2a+2 \equiv 0 \equiv a+4 \pmod{6}$$

$$\therefore a \equiv 2 \pmod{6}$$

$\therefore$  If this is true, then  $[2]$  and  $[5]$  will be true.

$$\begin{array}{ll}
 \therefore \text{So far, we have } a \equiv -2 \pmod{4} & [1]' \\
 a \equiv -3 \pmod{5} & [2]', \\
 a \equiv 2 \pmod{6} & [3]'.
 \end{array}$$

Note  $\gcd(4, 6) \neq 1$ .  $\therefore$  Combine  
 $[1]'$  becomes  $3a \equiv -6 \pmod{12}$

$[3]$  becomes  $2a \equiv 4 \pmod{12}$

$$\therefore 3a + 12 \equiv -6 + 12 \equiv 6 \pmod{12}$$

$$2a + 2 \equiv 4 + 2 \equiv 6 \pmod{12}$$

$$\therefore 3a + 12 \equiv 2a + 2 \pmod{12}, \text{ or}$$

$$a \equiv -10 \pmod{12}$$

$\therefore$  The system reduces to:

$$a \equiv -3 \pmod{5}$$

$$a \equiv -10 \pmod{12}$$

$$\therefore N = 5 \cdot 12 = 60 \quad N_1 = 12, \quad N_2 = 5$$

$$\therefore 12x_1 \equiv 1 \pmod{5} \quad 5x_2 \equiv 1 \pmod{12}$$

$$24x_1 \equiv 2$$

$$25x_2 \equiv 5$$

$$24x_1 - 25x_1 = -x_1 \equiv 2$$

$$25x_2 - 24x_2 = x_2 \equiv 5$$

$$\therefore x_1 \equiv -2$$

$$\therefore a_1 N_1 x_1 + a_2 N_2 x_2 =$$

$$(-3)(12)(-2) + (-10)(5)(5) = 72 - 250 = -178$$

$$\therefore a \equiv -178 \pmod{60}, \text{ or } a \equiv 2 \pmod{60}$$

$$\therefore a \equiv 62 \pmod{60}. \quad \therefore \underline{\underline{a = 62}}$$

7. (a). Obtain three consecutive integers, each having a square factor.

An integer  $a$  satisfying the hint will do.

$$a \equiv 0 \pmod{2^2} \quad a+1 \equiv 0 \pmod{3^2} \quad a+2 \equiv 0 \pmod{5^2}$$

Note  $2^2, 3^2, 5^2$  are relatively prime, so can use Chinese Remainder Theorem.

$$\begin{aligned} \therefore a &\equiv 0 \pmod{4} & N = 4 \cdot 9 \cdot 25 = 900 \\ a &\equiv 1 \pmod{9} & N_1 = 9 \cdot 25 = 225 \\ a &\equiv -2 \pmod{25} & N_2 = 4 \cdot 25 = 100 \\ && N_3 = 4 \cdot 9 = 36 \end{aligned}$$

$$\begin{aligned} 225x_1 &\equiv 1 \pmod{4} & 100x_2 \equiv 1 \pmod{9} & 36x_3 \equiv 1 \pmod{25} \\ 225x_1 - 224x_1 &= x_1 & 100x_2 - 99x_2 &= x_2 \\ x_1 &\equiv 1 & x_2 &\equiv 1 \\ && 72x_3 - 75x_3 &= -3x_3 \\ && 3x_3 &\equiv -2 \\ && 24x_3 &\equiv -16 \\ && 24x_3 - 25x_3 &= -x_3 \\ && x_3 &\equiv 16 \end{aligned}$$

$$\begin{aligned} \therefore a_1 N_1 x_1 + a_2 N_2 x_2 + a_3 N_3 x_3 &= \\ 0 + (-1)(100)(1) + (-2)(36)(16) &= -1252 \\ \therefore x &\equiv -1252 + 2 \cdot 900 = 548 \pmod{900} \\ \therefore 548, 549, 550 \end{aligned}$$

(6). Obtain three consecutive integers, the first of which is divisible by a square, the second by a cube, and the third by a fourth power.

Consider  $a \equiv 0 \pmod{5^2}$   
 $a+1 \equiv 0 \pmod{3^3}$   
 $a+2 \equiv 0 \pmod{2^4}$

Choose reverse  
order to get  
small # for  $n^4$

$2^2, 3^3, 5^4$  are relatively prime, so can use Chinese Remainder Theorem.

$$\begin{aligned} \therefore a &\equiv 0 \pmod{25} & N &= 25 \cdot 27 \cdot 16 = 10,800 \\ a &\equiv -1 \pmod{27} & N_1 &= 27 \cdot 16 = 432 \\ a &\equiv -2 \pmod{16} & N_2 &= 25 \cdot 16 = 400 \\ & & N_3 &= 25 \cdot 27 = 675 \end{aligned}$$

$$\begin{aligned} 432x_1 &\equiv 1 \pmod{25} & 400x_2 &\equiv 1 \pmod{27} \\ 432x_1 - 425x_1 &= 7x_1 & 400x_2 - 15 \cdot 27x_2 &= -5x_2 \\ 7x_1 &\equiv 1, \quad 49x_1 & -5x_2 &\equiv 11, \quad -x_2 &\equiv 11 \\ -x_1 &\equiv 7, \quad x_1 & & x_2 &\equiv -11 \end{aligned}$$

$$\begin{aligned} 675x_3 &\equiv 1 \pmod{16} \\ 675x_3 - 42 \cdot 16x_3 &= 3x_3 \\ 15x_3 &\equiv 5, \quad -x_3 &\equiv 5 \\ x_3 &\equiv -5 \end{aligned}$$

$$\begin{aligned} \therefore a_1 N_1 x_1 + a_2 N_2 x_2 + a_3 N_3 x_3 &= \\ 0 + (-1)(400)(-1) + (-2)(675)(-5) &= 11150 \\ \therefore 11150 - 10800 &= 350 \\ \therefore 11150 &\equiv 350 \pmod{25 \cdot 27 \cdot 16} \end{aligned}$$

$\therefore 350, 351, 352$

Eggs removed from a basket	Remaining Eggs
2 at a time	1
3 at a time	2
4 "	3
5 "	4
6 "	5
7 "	0

Find smallest number of eggs in basket.

$$\begin{aligned} x &\equiv 1 \pmod{2} \quad [1] \\ x &\equiv 2 \pmod{3} \quad [2] \\ x &\equiv 3 \pmod{4} \quad [3] \\ x &\equiv 4 \pmod{5} \quad [4] \\ x &\equiv 5 \pmod{6} \quad [5] \\ x &\equiv 0 \pmod{7} \quad [6] \end{aligned}$$

Need to eliminate the non-relatively prime conditions!

If [3] is true, then  $x = 3 + 4n = 1 + 2 + 4n = 1 + (1+2n) \cdot 2$ , so  $x \equiv 1 \pmod{2}$ .  
 $\therefore$  Eliminate [1]

Now look at  $[2]$  since  $\gcd(3, 6) \neq 1$

Multiply  $[2]$  by 2 and get  $2x \equiv 4 \pmod{3 \cdot 2}$

Can combine with  $[5]$

$$\therefore 2x - 4 \equiv x - 5 \pmod{6}$$

$$\therefore x \equiv -1 \pmod{6}$$

$\therefore$  If  $[5']$  is true,  $[2]$  and  $[5]$  will be true.

$$\therefore \text{We now have } x \equiv 3 \pmod{4} \quad [3]$$

$$x \equiv 4 \pmod{5} \quad [4]$$

$$x \equiv -1 \pmod{6} \quad [5']$$

$$x \equiv 0 \pmod{7} \quad [6]$$

But  $\gcd(4, 6) \neq 1$ .  $\therefore$  Multiply  $[3]$  by 3 and  $[5']$  by 2.

$$\therefore 3x \equiv 9 \pmod{12}$$

$$2x \equiv -2 \pmod{12}$$

$$\therefore 3x - 9 \equiv 2x + 2 \pmod{12}$$

$$x \equiv 11 \pmod{12}$$

$\therefore$  Everything reduces to:

$$x \equiv 4 \pmod{5} \quad [4]$$

$$x \equiv 11 \pmod{12} \quad [5'']$$

$$x \equiv 0 \pmod{7} \quad [6]$$

5, 12, 7 are relatively prime, so now can use Chinese Remainder Theorem.

$$N = 5 \cdot 12 \cdot 7 = 420$$

$$N_1 = 12 \cdot 7 = 84$$

$$N_2 = 5 \cdot 7 = 35$$

$$N_3 = 5 \cdot 12 = 60$$

$$\begin{aligned} \therefore 84x_1 &\equiv 1 \pmod{5} & 35x_2 &\equiv 1 \pmod{12} \\ 84x_1 - 85x_1 &= -x_1 \equiv 1 & 35x_2 - 36x_2 &= -x_2 \equiv 1 \\ x_1 &\equiv -1 & x_2 &\equiv -1 \end{aligned}$$

$$60x_3 \equiv 1 \pmod{7}$$

$$60x_3 - 56x_3 = 4x_3 \equiv 1$$

$$8x_3 \equiv 2, \quad 8x_3 - 7x_3 = x_3$$

$$x_3 \equiv 2$$

$$\begin{aligned} \therefore a_1 N_1 x_1 + a_2 N_2 x_2 + a_3 N_3 x_3 &= \\ 4 \cdot 84 \cdot (-1) + 11 \cdot 35 \cdot (-1) + 0 &= -721 \\ -721 + 2 \cdot 420 &= 119 \end{aligned}$$

$\therefore \underline{\underline{119}}$  eggs in the basket

9. Basket-of-eggs problem: One egg remains when the eggs are removed from the basket 2, 3, 4, 5, or 6 at a time; but no eggs remain if removed 7 at a time. Find smallest number of eggs in the basket.

$$\begin{array}{ll}
 x \equiv 1 \pmod{2} & [2] \\
 x \equiv 1 \pmod{3} & [?] \\
 x \equiv 1 \pmod{4} & [4] \\
 x \equiv 1 \pmod{5} & [5] \\
 x \equiv 1 \pmod{6} & [6] \\
 x \equiv 0 \pmod{7} & [7]
 \end{array}$$

Need to consolidate  
 since  $\gcd(2, 4) \neq 1$ ,  
 $\gcd(3, 6) \neq 1$ ,  
 $\gcd(4, 6) \neq 1$

If  $[4]$  is true, Then  $x = 1 + 4n = 1 + 2(2n)$ , and  
 so  $[2]$  must be true.  $\therefore$  Eliminate  $[2]$ .

If  $[6]$  is true, Then  $x = 1 + 6n = 1 + 3(2n)$ , and  
 so  $[3]$  is true.  $\therefore$  Eliminate  $[3]$

Now multiply  $[4]$  by 3 and  $[6]$  by 2 to get:

$$\begin{array}{ll}
 3x \equiv 3 \pmod{3 \cdot 4} = 3 \pmod{12} & [4'] \\
 2x = 2 \pmod{2 \cdot 6} = 2 \pmod{12} & [6']
 \end{array}$$

$$\begin{aligned}
 \therefore 3x - 3 &\equiv 2x - 2 \pmod{12} \\
 x &\equiv 1 \pmod{12}
 \end{aligned}$$

If  $[12]$  is true, then so must  $[4]$  and  $[6]$   
 $\therefore$  Now have:

$$\begin{array}{ll}
 x \equiv 1 \pmod{5} & 5, 7, 12 \text{ relatively} \\
 x \equiv 0 \pmod{7} & \text{prime} \\
 x \equiv 1 \pmod{12}
 \end{array}$$

$$\therefore N = 5 \cdot 7 \cdot 12 = 420 \quad N_1 = 7 \cdot 12 = 84 \\ N_2 = 5 \cdot 12 = 60 \\ N_3 = 5 \cdot 7 = 35$$

$$\therefore 84x_1 \equiv 1 \pmod{5} \quad 35x_3 \equiv 1 \pmod{12} \\ 84x_1 - 85x_1 = -x_1 \equiv 1 \\ x_1 \equiv -1 \pmod{5} \quad 35x_3 - 36x_3 = -x_3 \equiv 1 \\ x_3 \equiv -1 \pmod{12}$$

$$60x_2 \equiv 1 \pmod{7} \\ \text{irrelevant since } a_2 = 0$$

$$a_1 N_1 x_1 + a_2 N_2 x_2 + a_3 N_3 x_3 = 1 \cdot 84 \cdot (-1) + 0 + 1 \cdot 35 \cdot (-1) \\ = -84 - 35 \\ = -119$$

$$\therefore -119 + 420 = 301 \\ \therefore \underline{\underline{301}} \text{ eggs in basket.}$$

10. 10. (Ancient Chinese Problem.) A band of 17 pirates stole a sack of gold coins. When they tried to divide the fortune into equal portions, 3 coins remained. In the ensuing brawl over who should get the extra coins, one pirate was killed. The wealth was redistributed, but this time an equal division left 10 coins. Again an argument developed in which another pirate was killed. But now the total fortune was evenly distributed among the survivors. What was the least number of coins that could have been stolen?

$$x \equiv 3 \pmod{17} \quad 17, 16, 15 \text{ are relatively prime.} \\ x \equiv 10 \pmod{16} \\ x \equiv 0 \pmod{15}$$

$$N = 17 \cdot 16 \cdot 15 = 4080 \quad N_1 = 16 \cdot 15 = 240$$

$$N_2 = 17 \cdot 15 = 255$$

$$N_3 = 17 \cdot 16 = 272$$

$$240x_1 \equiv 1 \pmod{17}$$

$$240x_1 - 14 \cdot 17x_1 = 2x_1$$

$$2x_1 \equiv 1, \quad 18x_1 \equiv 9$$

$$\therefore x_1 \equiv 9 \pmod{17}$$

$$255x_2 \equiv 1 \pmod{16}$$

$$255x_2 - 16 \cdot 16x_2 = -x_2$$

$$\therefore x_2 \equiv -1 \pmod{16}$$

$$N_3x_3 \equiv 1 \pmod{15}$$

irrelevant since  $a_3 = 0$

$$\begin{aligned} \therefore a_1 N_1 x_1 + a_2 N_2 x_2 + a_3 N_3 x_3 &= 3 \cdot 240 \cdot 9 + 10 \cdot 255 \cdot (-1) + 0 \\ &= 3930 \end{aligned}$$

∴ 3930 coins.

The solutions manual uses different approach.

$$x \equiv 3 \pmod{17} \Rightarrow x = 3 + 17t$$

$$x \equiv 10 \pmod{16} \Rightarrow 3 + 17t \equiv 10 \pmod{16}, \text{ or}$$

$$17t \equiv 7 \pmod{16}, \therefore 17t - 16t = t \equiv 7 \pmod{16}$$

$$\Rightarrow t = 7 + 16k$$

$$\therefore x = 3 + 17(7 + 16k) = 122 + 272k$$

The third condition means  $122 + 272k \equiv 0 \pmod{15}$ ,

$$122 + 272k - 18 \cdot 15k \equiv 0, \text{ or } 122 + 2k \equiv 0 \pmod{15},$$

$$122 - 8 \cdot 15 + 2k \equiv 0, \quad 2k \equiv -2, \quad 2k \equiv 13 \pmod{15},$$

$$16k \equiv 104, \quad \therefore k \equiv 14 \pmod{15}, \quad \therefore k = 14 + 15r$$

$$\therefore x = 122 + 272(14 + 15r) = 3930 + 4080r$$

11. Prove  $x \equiv a \pmod{n}$  and  $x \equiv b \pmod{m}$   
 admit a simultaneous solution  $\Leftrightarrow$   
 $\gcd(n, m) \mid a - b$ ; if a solution exists, confirm  
 it is unique modulo  $\text{lcm}(n, m)$ .

Pf: (1) Suppose a solution exists for  $x$ .

$$\text{Let } d = \gcd(n, m) \therefore n = dr, m = ds$$

$$x \equiv a \pmod{n} \Rightarrow x = a + nt, \text{ some integer } t \\ x \equiv b \pmod{m} \Rightarrow x = b + mk, \text{ some integer } k$$

$$\therefore a + nt = b + mk, \text{ or } nt - mk = b - a$$

Substituting for  $n$  and  $m$ ,

$$drt - ds k = b - a,$$

$$d(rt - sk) = a - b \therefore d = \gcd(n, m) \mid a - b$$

(2) Let  $d = \gcd(n, m)$ , and suppose  $d \mid a - b$

$$\therefore dt = a - b, \text{ some integer } t.$$

By Th. 2.3, There are integers  $x_0$  and  $y_0$   
 s.t.  $nx_0 + my_0 = d$

$$\therefore dt = nx_0 t + my_0 t = a - b$$

$$\therefore my_0 t + b = a - x_0 t n$$

$$\text{Let } x = a + (-x_0 t)n = b + (y_0 t)m$$

$\therefore x \equiv a \pmod{n}$       So There is a  
 $x \equiv b \pmod{m}$       simultaneous solution.

Now let  $y$  be any other solution

$$\begin{aligned} \therefore x &\equiv a \pmod{n} & \text{and } y &\equiv a \pmod{n} \\ x &\equiv b \pmod{m} & y &\equiv b \pmod{m} \end{aligned}$$

$$\begin{aligned} \therefore x &\equiv y \pmod{n} \\ x &\equiv y \pmod{m} \end{aligned}$$

By Section 4.2, problem 13, p. 69,

$$x \equiv y \pmod{\text{lcm}(n, m)}$$

12.  $x \equiv 5 \pmod{6}$  and  $x \equiv 7 \pmod{15}$

$\gcd(6, 15) = 3$ . Since  $3 \nmid (7-5)$ , there is no solution.

13. If  $x \equiv a \pmod{n}$ , prove either  $x \equiv a \pmod{2n}$  or  $x \equiv a + n \pmod{2n}$

Pf:  $x \equiv a \pmod{n} \Rightarrow x = a + kn$ , some  $k$ .

If  $k$  is even, Then  $k = 2r$ , some  $r$ .  
 $\therefore x = a + r(2n) \Rightarrow x \equiv a \pmod{2n}$

If  $k$  is odd, Then  $k = 2r + 1$ , some  $r$ .  
 $\therefore x = a + (2r+1)n = a + n + r2n \Rightarrow$   
 $x \equiv a + n \pmod{2n}$

14.  $x \equiv 1 \pmod{9}$  and  $1 < x < 1200$   
 $x \equiv 2 \pmod{11}$   
 $x \equiv 6 \pmod{13}$

9, 11, 13 are rel. prime, so can use Chinese Remainder Theorem.

$$N = 9 \cdot 11 \cdot 13 = 1287$$

$$N_1 = 11 \cdot 13 = 143 \quad N_2 = 9 \cdot 13 = 117 \quad N_3 = 9 \cdot 11 = 99$$

$$143x_1 \equiv 1 \pmod{9}$$

$$143x_1 - 9 \cdot 15x_1 \equiv 8x_1$$

$$8x_1 - 9x_1 \equiv -x_1 \equiv 1$$

$$x_1 \equiv -1$$

$$117x_2 \equiv 1 \pmod{11}$$

$$117x_2 - 121x_2 \equiv -4x_2$$

$$-12x_2 \equiv 3 \quad -x_2 \equiv 3$$

$$x_2 \equiv -3$$

$$99x_3 \equiv 1 \pmod{13}$$

$$99x_3 - 8 \cdot 13x_3 = -5x_3$$

$$-15x_3 \equiv 3, \quad -2x_3 \equiv 3$$

$$-12x_3 \equiv 18$$

$$x_3 \equiv 18$$

$$\therefore a_1 N_1 x_1 + a_2 N_2 x_2 + a_3 N_3 x_3 = \\ 1 \cdot 143 \cdot (-1) + 2 \cdot 117 \cdot (-3) + 6 \cdot 99(18) = 9847$$

$$9847 - 7 \cdot 1287 = 838$$

$$\underline{-\quad 838}$$

15. (a). Find an integer having the remainders 1, 2, 5, 5 when divided by 2, 3, 6, 12 respectively.

$$x \equiv 1 \pmod{2} \quad [2] \text{ divisors not relatively prime,}$$

$$x \equiv 2 \pmod{3} \quad [3] \text{ so simplify}$$

$$x \equiv 5 \pmod{6} \quad [6]$$

$$x \equiv 5 \pmod{12} \quad [12]$$

$$\gcd(3, 6) \neq 1, \text{ so multiply } [3] \text{ by 2}$$

$$\therefore 2x \equiv 4 \pmod{6}$$

$$x \equiv 2 \pmod{6}$$

$$\therefore 2x - 4 \equiv x - 5 \pmod{6}, \text{ or } x \equiv -1 \pmod{6} \quad [6']$$

$\therefore$  if  $[6]$  is true, then so is  $[6]$  and  $[3]$   
But  $[6]$  is the same as  $x \equiv -1 + 6 = 5 \pmod{6}$ ,  
which is  $[6]$ .  $\therefore$  can drop  $[3]$

$\gcd(6, 12) \neq 1$ , so multiply  $[6]$  by 2

$$\therefore 2x \equiv 10 \pmod{12}$$

$$x \equiv 5 \pmod{12}$$

$\therefore x \equiv 5 \pmod{12}$ , which is  $[12]$ .

$\therefore$  if  $[12]$  is true, so is  $[6]$ , and so is  $[3]$

$\therefore$  can drop  $[8]$  and  $[6]$ .

$$\therefore x \equiv 1 \pmod{2} \quad [2]$$

$$x \equiv 5 \pmod{12} \quad [12]$$

But  $\gcd(2, 12) \neq 1$ .  $\therefore$  multiply  $[2]$  by 6.

$$\therefore 6x \equiv 6 \pmod{12}$$

$$x \equiv 5 \pmod{12}$$

$$\therefore 5x \equiv 1 \pmod{12}$$

$$7 \cdot 5x \equiv 7, \text{ or } 35x \equiv 7$$

$$35x - 36x = -x \equiv 7$$

$$x \equiv -7 + 12 = 5$$

$$\therefore x \equiv 5 \pmod{12}$$

$$\therefore x = 5 + 12k$$

Since want  $x > 12$ , choose  $x = 5 + 12 = \underline{\underline{17}}$

(6) Find an integer with remainders 2, 3, 4, 5  
when divided by 3, 4, 5, 6 respectively.

$$\begin{array}{ll} x \equiv 2 \pmod{3} & [3] \\ x \equiv 3 \pmod{4} & [4] \\ x \equiv 4 \pmod{5} & [5] \\ x \equiv 5 \pmod{6} & [6] \end{array}$$

Divisors not relatively prime, so simplify.

Multiply  $[3]$  by 2 :  $2x \equiv 4 \pmod{6}$   
 $x \equiv 5 \pmod{6}$   $[6]$

$\therefore x \equiv -1 \pmod{6}$ , or

$x \equiv 5 \pmod{6}$ , which is  $[6]$

$\therefore [3]$  is superfluous since if  $[6]$  is true,  
so is  $[3]$

Now examine  $[4]$  and  $[6]$ . Multiply  $[4]$  by 3  
and  $[6]$  by 2.

$\therefore 3x \equiv 9 \pmod{12}$

$2x \equiv 10 \pmod{12}$

$\therefore x \equiv -1$ , or  $x \equiv 11 \pmod{12}$   $[12]$

$\therefore$  if  $[12]$  is true, so is  $[4]$  and  $[6]$

$\therefore x \equiv 4 \pmod{5}$

$x \equiv 11 \pmod{12}$

$\gcd(5, 12) = 1$ ,  $\therefore$  use Chinese Remainder Th.

$$N = 5 \cdot 12 = 60 \quad N_1 = 12 \quad N_2 = 5$$

$$12x_1 \equiv 1 \pmod{5} \quad 5x_2 \equiv 1 \pmod{12}$$

$$24x_1 \equiv 2$$

$$24x_1 - 25x_1 = -x_1$$

$$-x_1 \equiv 2, \quad x_1 \equiv -2$$

$$x_1 \equiv -2 + 5 = 3$$

$$25x_2 \equiv 5$$

$$25x_2 - 24x_2 = 5$$

$$x_2 \equiv 5$$

$$\therefore a_1 N_1 x_1 + a_2 N_2 x_2 = 4 \cdot 12 \cdot 3 + 11 \cdot 5 \cdot 5 = 419$$

$$\therefore x \equiv 419 \pmod{60}, \text{ or } x \equiv 419 - 6 \cdot 60$$

$$x \equiv 59 \pmod{60}$$

$$\therefore x = \underline{\underline{59}}$$

(c) Find an integer having remainders 3, 11, 15 when divided by 10, 13, 17 respectively.

$$x \equiv 3 \pmod{10} \quad \text{All divisors are relatively prime.} \quad \therefore \text{Use Chinese Remainder Thm.}$$

$$x \equiv 11 \pmod{13}$$

$$x \equiv 15 \pmod{17}$$

All divisors are relatively prime.  $\therefore$  Use Chinese Remainder Thm.

$$N = 10 \cdot 13 \cdot 17 = 2210 \quad N_1 = 13 \cdot 17 = 221$$

$$N_2 = 10 \cdot 17 = 170$$

$$N_3 = 10 \cdot 13 = 130$$

$$221x_1 \equiv 1 \pmod{10} \quad 170x_2 \equiv 1 \pmod{13}$$

$$221x_1 - 220x_1 = x_1 \quad 170x_2 - 13 \cdot 13x_2 = x_2$$

$$x_1 \equiv 1 \quad x_2 \equiv 1$$

$$130x_3 \equiv 1 \pmod{17}$$

$$130x_3 - 8 \cdot 17x_3 = -6x_3$$

$$-6x_3 \equiv 1, \quad 18x_3 \equiv -3$$

$$18x_3 - 17x_3 = x_3$$

$$\therefore x_3 \equiv -3$$

$$\therefore a_1 A_1 x_1 + a_2 A_2 x_2 + a_3 A_3 x_3 =$$

$$3 \cdot 221 \cdot 1 + 11 \cdot 170 \cdot 1 + 15 \cdot 130 \cdot (-3) = -3317$$

$$\therefore -3317 + 2 \cdot (2210) = 1103$$

$$\therefore x = \underline{1103}$$

16. Let  $t_n$  be the  $n^{\text{th}}$  triangular number.  
 For which values of  $n$  does  $t_n$  divide  $t_1^2 + t_2^2 + \dots + t_n^2$ ?

$$t_1^2 + t_2^2 + \dots + t_n^2 = t_n(3n^3 + 12n^2 + 13n + 2)/30$$

Pf: By induction, if  $n=1$ ,  $t_1 = \frac{n(n+1)}{2} = 1$   
 $\therefore t_1^2 = 1, \quad t_n(3n^3 + 12n^2 + 13n + 2)/30 =$   
 $1(3 + 12 + 13 + 2)/30 = 1$

Now suppose, for  $K > 1$ ,

$$t_1^2 + \dots + t_k^2 = t_k (3k^3 + 12k^2 + 13k + 2) / 30 \quad [1]$$

$$\therefore t_1^2 + \dots + t_k^2 + t_{k+1}^2 =$$

$$t_k (3k^3 + 12k^2 + 13k + 2) / 30 + \left[ \frac{(k+1)(k+2)}{2} \right]^2$$

$$= \frac{k(k+1)}{2} \left( \frac{3k^3 + 12k^2 + 13k + 2}{30} \right) + \frac{(k+1)^2(k+2)^2}{2^2}$$

$$= \frac{(k+1)}{2} \left[ \frac{k(3k^3 + 12k^2 + 13k + 2)}{30} + \frac{(k+1)(k+2)^2}{2} \right]$$

$$= \frac{(k+1)}{2} \left[ \frac{3k^4 + 12k^3 + 13k^2 + 2k}{30} + \frac{k^3 + 5k^2 + 8k + 4}{2} \right]$$

$$= \frac{(k+1)}{2} \left[ \frac{3k^4 + 27k^3 + 88k^2 + 122k + 60}{30} \right] \quad [2]$$

Now look at right side of [1] using  $k+1$ .

$$t_{k+1} (3(k+1)^3 + 12(k+1)^2 + 13(k+1) + 2) / 30$$

$$= \frac{(k+1)(k+2)}{2} \left[ \frac{3k^3 + 9k^2 + 9k + 3 + 12k^2 + 24k + 12 + 13k + 15}{30} \right]$$

$$= \frac{(k+1)}{2} (k+2) \left[ \frac{3k^3 + 21k^2 + 46k + 30}{30} \right]$$

$$= \frac{(k+1)}{2} \left[ \frac{3k^4 + 21k^3 + 46k^2 + 30k + 6k^3 + 42k^2 + 92k + 60}{30} \right]$$

$$= \frac{(k+1)}{2} \left[ \frac{3k^4 + 27k^3 + 88k^2 + 122k + 60}{30} \right] \quad [3]$$

$\therefore [2] = [3]$ , so  $k \Rightarrow k+1$

$$\therefore t_1^2 + \dots + t_n^2 = t_n (3n^3 + 12n^2 + 13n + 2) / 30$$

$\therefore t_n \mid (t_1^2 + \dots + t_n^2) \Leftrightarrow \frac{(3n^3 + 12n^2 + 13n + 2)}{30}$  is  
an integer, i.e.,

$$(3n^3 + 12n^2 + 13n + 2) \equiv 0 \pmod{30}, \text{ or}$$

$$(3n^3 + 12n^2 + 13n + 2) \equiv 0 \pmod{2 \cdot 3 \cdot 5}, \text{ or}$$

$$(3n^3 + 12n^2 + 13n + 2) \equiv 0 \pmod{2} \quad [2]$$

$$(3n^3 + 12n^2 + 13n + 2) \equiv 0 \pmod{3} \quad [3]$$

$$(3n^3 + 12n^2 + 13n + 2) \equiv 0 \pmod{5} \quad [4]$$

since unique solutions are  $\equiv 0 \pmod{30}$  by

## Chinese Remainder Theorem.

For [2],  $3n^3 - 2n^3 + 12n^2 - 6 \cdot 2n^2 + 13n - 2 \cdot 6n + 2 \equiv 2 = n^3 + n = n(n^2 + 1) \equiv 0 \pmod{2}$

If  $n$  is even, then  $n(n^2 + 1)$  is even, and so  $n^2(n+1) \equiv 0 \pmod{2}$

If  $n$  is odd,  $n^2$  is odd, and  $n^2 + 1$  is even, so  $n(n^2 + 1)$  is even, so  $n(n^2 + 1) \equiv 0 \pmod{2}$

So [2] puts no restrictions on  $n$ .

For [3],  $3n^3 - 3n^3 + 12n^2 - 3 \cdot 4n^2 + 13n - 3 \cdot 4n + 2 = n + 2 \equiv 0 \pmod{3}$   
 $\therefore n \equiv 1 \pmod{3}$

For [5],  $3n^3 + 12n^2 - 5 \cdot 2n^2 + 13n - 5 \cdot 2n + 2 = 3n^3 + 2n^2 + 3n + 2 = n^2(3n+2) + 3n + 2 = (n^2 + 1)(3n + 2) \equiv 0 \pmod{5}$   
 $\therefore (n^2 + 1) \equiv 0 \pmod{5}$  or  $(3n + 2) \equiv 0 \pmod{5}$   
 (using  $a \bar{b} \equiv 0 \pmod{p}$ ,  $p$  prime,  $\Rightarrow a \equiv 0 \pmod{p}$   
 or  $b \equiv 0 \pmod{p}$  — see comments at  
 end of section 4.2, and proof of  
 Theorem 2 in Problems 4.2).

$\therefore$  Problem reduces to  $\boxed{n \equiv 1 \pmod{3}}$   
 and  $(n^2 + 1) \equiv 0 \pmod{5}$  or  $(3n + 2) \equiv 0 \pmod{5}$

$$\begin{aligned}
 & 3n+2 \equiv 0 \pmod{5} \\
 & 3n \equiv -2, \quad 6n \equiv -4 \\
 & n \equiv -4, \quad n \equiv 1 \\
 & \therefore n \equiv 1 \pmod{5}
 \end{aligned}
 \quad \left\{
 \begin{aligned}
 & n \equiv 1 \pmod{5} \Rightarrow 3n \equiv 3 \pmod{15} \\
 & n \equiv 1 \pmod{3} \Rightarrow 5n \equiv 5 \pmod{15} \\
 & \therefore 5n - 3n \equiv 5 - 3 \pmod{15} \\
 & 2n \equiv 2 \pmod{15} \\
 & \underline{n \equiv 1 \pmod{15}}
 \end{aligned}
 \right.$$

$$\begin{aligned}
 & n^2 + 1 \equiv 0 \pmod{5} \\
 & n^2 \equiv -1, \quad n^2 \equiv 4 \\
 & \therefore n \equiv 2, \text{ or } n \equiv -2 \\
 & \therefore n \equiv 2 \pmod{5} \\
 & \text{or } n \equiv 3 \pmod{5}
 \end{aligned}
 \quad \left\{
 \begin{aligned}
 & n \equiv 2 \pmod{5} \Rightarrow 3n \equiv 6 \pmod{15} \\
 & n \equiv 1 \pmod{3} \Rightarrow 5n \equiv 5 \pmod{15} \\
 & \therefore 5n - 3n \equiv 5 - 6, \quad 2n \equiv -1, \\
 & 2n \equiv -1 + 15, \quad 2n \equiv 14, \\
 & \therefore n \equiv 7 \pmod{15}
 \end{aligned}
 \right.$$
  

$$\begin{aligned}
 & n \equiv 3 \pmod{5} \Rightarrow 3n \equiv 9 \pmod{15} \\
 & n \equiv 1 \pmod{3} \Rightarrow 5n \equiv 5 \pmod{15} \\
 & 5n - 3n \equiv 5 - 9 = -4, \quad 2n \equiv -4, \\
 & n \equiv -2, \quad n \equiv -2 + 15, \\
 & \underline{n \equiv 13 \pmod{15}}
 \end{aligned}$$

$$\therefore n \equiv 1, \text{ or } 7, \text{ or } 13 \pmod{15}$$

17. Find solutions of

$$\begin{cases} 3x + 4y \equiv 5 \pmod{13} \\ 2x + 5y \equiv 7 \pmod{13} \end{cases}
 \quad \begin{matrix} [1] \\ [2] \end{matrix}$$

$$\begin{aligned}
 & \text{Mult. [1] by 5:} \quad 15x + 20y \equiv 25 \pmod{13} \quad [1'] \\
 & \text{Mult. [2] by 4:} \quad 8x + 20y \equiv 28 \pmod{13} \quad [2']
 \end{aligned}$$

$$\begin{aligned} [1'] - [2'] : \quad 7x &\equiv -3 \pmod{13} \\ \therefore 14x &\equiv -6 \\ 14x - 13x &\equiv -6 + 13 \\ x &\equiv 7 \pmod{13} \quad [3'] \end{aligned}$$

$$\begin{aligned} \text{Substitute } [3'] \text{ into } [1]: \quad 3x &\equiv 21 \pmod{13} \quad [3'] \\ 3x &\equiv 5 - 4y \pmod{13} \quad [1] \\ \therefore 21 &\equiv 5 - 4y \pmod{13} \\ 16 &\equiv -4y \\ 48 &\equiv -12y \\ 48 - 3 \cdot 13 &\equiv -12y + 13y \\ 9 &\equiv y \pmod{13} \\ \therefore x &\equiv 7 \pmod{13} \\ y &\equiv 9 \pmod{13} \end{aligned}$$

18. Obtain the two incongruent solutions mod 210 of the system:

$$\begin{aligned} 2x &\equiv 3 \pmod{5} & [5] \\ 4x &\equiv 2 \pmod{6} & [6] \\ 3x &\equiv 2 \pmod{7} & [7] \end{aligned}$$

$$\begin{aligned} \text{From } [5]: \quad 4x &\equiv 6 \\ 4x - 5x &\equiv 6 - 5 \\ -x &\equiv 1 \\ x &\equiv -1 + 5 \\ x &\equiv 4 \pmod{5} \end{aligned}$$

$$\begin{aligned} \text{From } [6]: \quad 4x/2 &\equiv 2/2 \pmod{G/2} \\ 2x &\equiv 1 \pmod{3} \\ 4x &\equiv 2 \\ 4x - 3x &= x \equiv 2 \pmod{3}, \therefore x \equiv 2 \pmod{G} \end{aligned}$$

Since  $\gcd(4, 6) = 2$ , Th. 4.7 says Th.  
2 incongruent solutions are  $x_0, x_0 + \frac{6}{2}$ ,  
where  $x_0$  is a solution.  $x=2$  is a  
solution, so  $2 + \frac{6}{2} = 5$  is the other.  
 $\therefore x \equiv 5 \pmod{G}$  is the other.

$$\begin{aligned} \text{From } [7]: \quad 6x &\equiv 4 \pmod{7} \\ 6x - 7x &\equiv 4 - 7 \\ -x &\equiv -3 \\ x &\equiv 3 \pmod{7} \end{aligned}$$

$$\begin{aligned} \therefore x &\equiv 4 \pmod{5} \\ x &\equiv 2 \pmod{6} \quad \text{or} \quad x \equiv 5 \pmod{6} \\ x &\equiv 3 \pmod{7} \end{aligned}$$

$$\begin{aligned} N &= 5 \cdot 6 \cdot 7 = 210 & N_1 &= 6 \cdot 7 = 42 \\ N_2 &= 5 \cdot 7 = 35 \\ N_3 &= 5 \cdot 6 = 30 \end{aligned}$$

$$\begin{aligned}\therefore 42x_1 &\equiv 1 \pmod{5} \\ 42x_1 - 40x_1 &= 2x_1 \equiv 1 \\ 6x_1 &\equiv 3, 6x_1 - 5x_1 = x_1 \\ \therefore x_1 &\equiv 3 \pmod{5}\end{aligned}$$

$$\begin{aligned}35x_2 &\equiv 1 \pmod{6} \\ 35x_2 - 36x_2 &= -x_2 \\ \therefore x_2 &\equiv -1 + 6 = 5 \\ x_2 &\equiv 5 \pmod{6}\end{aligned}$$

$$\begin{aligned}30x_3 &\equiv 1 \pmod{7} \\ 30x_3 - 28x_3 &= 2x_3 \\ 2x_3 &\equiv 1, 8x_3 \equiv 4 \\ 8x_3 - 7x_3 &= x_3 \equiv 4 \\ \therefore x_3 &\equiv 4 \pmod{7}\end{aligned}$$

$$\therefore a_1 N_1 x_1 + a_2 N_2 x_2 + a_3 N_3 x_3 =$$

$$4(42)(3) + 2(35)(5) + 3(30)(4) = 1214$$

or  $4(42)(3) + 5(35)(5) + 3(30)(4) = 1739$

$$\begin{aligned}\therefore x &\equiv 1214 \pmod{210} \Rightarrow \boxed{x \equiv 164 \pmod{210}} \\ \text{or } x &\equiv 1739 \pmod{210} \Rightarrow \boxed{x \equiv 59 \pmod{210}}\end{aligned}$$

19. Obtain the 8 incongruent solutions of  $3x + 4y \equiv 5 \pmod{8}$ .

Set  $3x \equiv 5 - 4y \pmod{8}$ . Since  $\gcd(3, 8) = 1$ , and  $1 | (5 - 4y)$ , Th. 4.7 says there is one solution for any value of  $y$ . Since there

are 8 incongruent values of  $5-4y$  ( $y=0, 1, \dots, 7$ )  
Solve for each value of  $y$ .

$$\begin{aligned} \therefore 3x &\equiv 5 \pmod{8} & 15x &\equiv 25, 15x - 16x \equiv 25 - 24 \\ && x &\equiv 1, x \equiv 7 \\ \therefore x &\equiv ?, y \equiv 0 \pmod{8} \end{aligned}$$

$$\begin{aligned} 3x &\equiv 1 \pmod{8} & 15x &\equiv 5, -x \equiv 5, x \equiv -5, \\ && x &\equiv 3 \\ \therefore x &\equiv 3, y \equiv 1 \pmod{8} \end{aligned}$$

$$\begin{aligned} 3x &\equiv -3 \pmod{8} & 15x &\equiv -15, -x \equiv 1, x \equiv -1, \\ && x &\equiv 7 \\ \therefore x &\equiv ?, y \equiv 2 \pmod{8} \end{aligned}$$

$$\begin{aligned} 3x &\equiv -7 \pmod{8}, 3x \equiv 1, 15x \equiv 5, -x \equiv 5, \\ && x &\equiv 3 \\ \therefore x &\equiv 3, y \equiv 3 \pmod{8} \end{aligned}$$

$$\begin{aligned} 3x &\equiv -11 \pmod{8}, 3x \equiv 5, 15x \equiv 25, -x \equiv 1 \\ && x &\equiv -1, x \equiv 7 \\ \therefore x &\equiv 7, y \equiv 4 \pmod{8} \end{aligned}$$

$$\begin{aligned} 3x &\equiv -15 \pmod{8}, 3x \equiv 1, 15x \equiv 5, -x \equiv 5, \\ && x &\equiv -5, x \equiv 3 \\ \therefore x &\equiv 3, y \equiv 5 \pmod{8} \end{aligned}$$

$$3x \equiv -19 \pmod{8}, \quad 3x \equiv -3, \quad x \equiv 7 \text{ from above} \\ \therefore x \equiv 7, y \equiv 6 \pmod{8}$$

$$3x \equiv -23 \pmod{8}, \quad 3x \equiv 1, \quad \therefore x \equiv 3 \text{ from above} \\ \therefore x \equiv 3, y \equiv 7 \pmod{8}$$

20. Find solutions to the following systems.

$$(i). \begin{aligned} 5x + 3y &\equiv 1 \pmod{7} & [1] \\ 3x + 2y &\equiv 4 \pmod{7} & [2] \end{aligned}$$

$$\begin{aligned} 10x + 6y &\equiv 2 \pmod{7} & [1'] = [1] \times 2 \\ 9x + 6y &\equiv 12 \pmod{7} & [2'] = [2] \times 3 \end{aligned}$$

$$\begin{aligned} x &\equiv -10 \pmod{7} & [1'] - [2'] \\ x &\equiv -10 + 14 = 4 \\ x &\equiv 4 \pmod{7} & [3] \end{aligned}$$

$$5x \equiv 20 \pmod{7} \quad [3'] = [3] \times 5 \\ \therefore 1-3y \equiv 20 \pmod{7} \quad [3'] \text{ in } [1]$$

$$-3y \equiv 19 - 14 = 5$$

$$-6y \equiv 10$$

$$-6y + 7y \equiv 10$$

$$y \equiv 10 \pmod{7}$$

$$\therefore x \equiv 4 \pmod{7} \\ y \equiv 10 \pmod{7}$$

$$(6) \begin{aligned} 7x + 3y &\equiv 6 \pmod{11} & [1] \\ 4x + 2y &\equiv 9 \pmod{11} & [2] \end{aligned}$$

$$\begin{aligned} 14x + 6y &\equiv 12 \pmod{11} & [1'] = [1] \times 2 \\ 12x + 6y &\equiv 27 \pmod{11} & [2'] = [2] \times 3 \end{aligned}$$

$$2x \equiv -15 \pmod{11} \quad [1'] - [2']$$

$$2x \equiv -15 + 22 = 7$$

$$10x \equiv 35$$

$$10x - 11x \equiv 35 - 3 \cdot 11$$

$$-x \equiv 2, x \equiv -2$$

$$x \equiv -2 + 11 = 9 \quad [3]$$

$$4x \equiv 36 \pmod{11} \quad [3] \times 4$$

$$4x \equiv 36 - 33 = 3 \pmod{11} \quad [3']$$

$$3 \equiv 9 - 2y \pmod{11} \quad [3'] \text{ in } [2]$$

$$-2y \equiv -6$$

$$-10y \equiv -30$$

$$-10y + 11y \equiv -30 + 3 - 11$$

$$y \equiv 3 \pmod{11}$$

$$\begin{aligned} \therefore x &\equiv 9 \pmod{11} \\ y &\equiv 3 \pmod{11} \end{aligned}$$

$$(c) \begin{aligned} 11x + 5y &\equiv 7 \pmod{20} & [1] \\ 6x + 3y &\equiv 8 \pmod{20} & [2] \end{aligned}$$

$$\begin{aligned} 17x + 8y &\equiv 15 \pmod{20} \\ 12x + 6y &\equiv 14 \pmod{20} \end{aligned}$$

$$33x + 15y \equiv 21 \pmod{20} \quad [1'] = [13x]$$

$$30x + 15y \equiv 40 \pmod{20} \quad [2'] = [23x]$$

$$3x \equiv -19 \pmod{20} \quad [3] = [1'] - [2']$$

$$3x \equiv -19 + 20 = 1 \quad [3']$$

$$21x \equiv 7 \quad [3'] \times 7$$

$$21x - 20x \equiv 7$$

$$x \equiv 7 \pmod{20} \quad [4]$$

$$6x \equiv 42 \pmod{20}$$

$$\therefore 42 \equiv 8 - 3y \pmod{20} \quad [4'] \text{ in } [2]$$

$$-3y \equiv 34 - 20 = 14 \quad [4'']$$

$$-21y \equiv 98$$

$$-21y + 20y \equiv 98 - 5 \cdot 20$$

$$-y \equiv -2$$

$$y \equiv 2$$

$$\therefore x \equiv 7 \pmod{20}$$

$$y \equiv 2 \pmod{20}$$

## 5.2 Fermat's Factorization Method

Note Title

4/27/2005

### Problems 5-2

1. Use Fermat's method to factor each number

(a). 2279

$$47^2 < 2279 < 48^2 \quad \frac{2279+1}{2} = 1140$$

$$\therefore 48^2 - 2279 = 25 = 5^2$$

$$\therefore 48 - 5 = 43, \quad 48 + 5 = 53$$

$$\therefore 2279 = 43 \cdot 53$$

(b) 10541      $102^2 < 10541 < 103^2, \quad \frac{10541+1}{2} = 5271$

$$\therefore 103^2 - 10541 = 68$$

$$104^2 - 10541 = 275$$

$$105^2 - 10541 = 484 = 22^2$$

$$\therefore 105 - 22 = 83, \quad 105 + 22 = 127$$

$$\therefore 10541 = 83 \cdot 127$$

(c) 340663      $588^2 < 340663 < 584^2, \quad \frac{340663+1}{2} = 170332$

$$584^2 - 340663 = 393$$

	A	B	C	D	E
1	k	$k^2$	340663	$k^2 - 340663$	$\sqrt{0}$
2	584	341056	340663	393	19.82423
3	585	342225	340663	1562	39.52215
4	586	343396	340663	2733	52.2781
5	587	344569	340663	3906	62.498
6	588	345744	340663	5081	71.28113
7	589	346921	340663	6258	79.10752
8	590	348100	340663	7437	86.23804
9	591	349281	340663	8618	92.83318
10	592	350464	340663	9801	99

From spreadsheet,

$$\begin{aligned} 592^2 - 340663 &= 9801 \\ &= 99^2 \end{aligned}$$

$$\therefore 592 - 99 = 493, 592 + 99 = 691$$

691 is prime (from table of primes), 493 not

$$\therefore 22^2 < 493 < 23^2, \frac{493+1}{2} = 247$$

$$23^2 - 493 = 36 = 6^2$$

$$\therefore 23 + 6 = 29, 23 - 6 = 17$$

$$\therefore 493 = 17 \cdot 29$$

$$\therefore 340663 = 17 \cdot 29 \cdot 691$$

2. Prove a perfect square must end in one of the following digits:

00	16	29	49	69	89
01	21	36	56	76	96
04	24	41	61	81	
09	25	44	64	84	

If: First note  $(x+50)^2 = x^2 + 100x + 2500$ , so

$x^2 \equiv (x+50)^2 \pmod{100}$ . This means you only need to examine last two digits of

$x = 0, 1, 2, \dots, 49$  since  $0^2 \equiv 50^2 \pmod{100}$ ,  $1^2 \equiv 51^2 \pmod{100}$ , ...

But  $(x-50)^2 = x^2 - 100x + 2500$ , so  $x^2 \equiv (x-50)^2 \pmod{100}$   
 $\therefore x^2 \equiv (50-x)^2 \pmod{100}$ , so for  $x = 26, 27, \dots, 48$   
 $26^2 \equiv 24^2, 27^2 \equiv 23^2, \dots, 48^2 \equiv 1^2$ .

$\therefore$  Only need to look at digits  $x=0, 1, 2, \dots, 25$

$x$	$x^2 \pmod{100}$	$x$	$x^2 \pmod{100}$	$x$	$x^2 \pmod{100}$		
0	00	10	00	*	20	00	*
1	01	11	21	21	41		
2	04	12	44	22	84		
3	09	13	69	23	29		
4	16	14	96	24	76		
5	25	15	25	*	25	25	*
6	36	16	56				
7	49	17	89				
8	64	18	24				
9	81	19	61				

\* = duplicated  
ending

$\therefore$  The above endings are the ones that were to be proved.

3. Factor the number  $2^{11}-1$  using Fermat's method.

$$2^{11}-1 = 2047, 45^2 < 2047 < 46^2$$

$$\text{From spreadsheet, } 56^2 - 2047 = 1089 = 33^2$$

A	B	C
1	x	$x^2 - 2047$
2	46	69
3	47	162
4	48	257
5	49	354
6	50	453
7	51	554
8	52	657
9	53	762
10	54	869
11	55	978
12	56	1089
13	57	1202
		sqrt()
		8.306624
		12.72792
		16.03122
		18.81489
		21.2838
		23.5372
		25.63201
		27.60435
		29.47881
		31.27299
		33
		34.66987

$$\therefore 56^2 - N^2 = 33^2 \quad N = (56+33)(56-33), \\ \text{or } N = 89-23 \\ \therefore 2''-1 = 89-23$$

4. If  $n^2 = a^2 + b^2 = c^2 + d^2$ ,  $\gcd(a, b) = \gcd(c, d) = 1$ ,

Then  $n = \frac{(ac+bd)(ac-bd)}{(a+d)(a-d)}$

$$(a). \text{ Factor } 493 = 18^2 + 13^2 = 22^2 + 3^2$$

$$493 = \frac{(18 \cdot 22 + 13 \cdot 3)(18 \cdot 22 - 13 \cdot 3)}{(18+3)(18-3)} = \frac{(435)(357)}{(21)(15)} \\ = \frac{435}{15} \cdot \frac{357}{21} = 29 \cdot 17$$

$$(b) 38025 = 168^2 + 99^2 = 156^2 + 117^2$$

$$= \frac{(168 \cdot 156 + 99 \cdot 117)(168 \cdot 156 - 99 \cdot 117)}{(168+117)(168-117)}$$

$$= \frac{(37791)(14625)}{(285)(51)} = \frac{14625}{285} \cdot \frac{37791}{51}$$

$$= \frac{14625}{285} \cdot 741$$

But 241 is not prime:  $741 = 3 \cdot 247 = 3 \cdot 13 \cdot 19$

$$\therefore 38025 = \frac{14625}{285} \cdot (3 \cdot 13 \cdot 19)$$

$\frac{14625}{285}$  is not an integer

$$\frac{14625}{285} = \frac{5 \cdot 2925}{5 \cdot 57} = \frac{25 \cdot 117}{3 \cdot 19} = \frac{5^2 \cdot 9 \cdot 13}{3 \cdot 19}$$

$$\therefore 38025 = \frac{5^2 \cdot 9 \cdot 13}{3 \cdot 19} \cdot 3 \cdot 13 \cdot 19$$

$$= \frac{5^2 \cdot 3^2 \cdot 13}{19} \cdot 13 \cdot 19$$

$$= 3^2 \cdot 5^2 \cdot 13^2$$

5. Use generalized Fermat method to factor.

(a). 2911 Use hint:  $138^2 \equiv 67 \pmod{2911}$

$\therefore \gcd(138 - 67, 2911) = \gcd(71, 2911)$   
Using Euclidean Algorithm,

$2911 = 41 \cdot 71$ , and  $71 + 41$  60th prime.

(b)  $4573$  dscr hint:  $177^2 \equiv 92^2 \pmod{4573}$

$$\therefore \gcd(177-92, 4573) = \gcd(85, 4573)$$

$$4573 = 53 \cdot 85 + 68$$

$$85 = 1 \cdot 68 + 17$$

$$68 = 4 \cdot 17 \quad \therefore \gcd = 17$$

$$\gcd(177+92, 4573) = \gcd(269, 4573)$$

$$\therefore 4573 = 17 \cdot 269, \quad \therefore \gcd = 17$$

Also,  $269$  is prime,  $\therefore \underline{\underline{4573 = 17 \cdot 269}}$

(c)  $6923$  From hint:  $208^2 \equiv 93^2 \pmod{6923}$

$$\therefore \gcd(208-93, 6923) = \gcd(115, 6923)$$

$$6923 = 60 \cdot 115 + 23$$

$$115 = 5 \cdot 23 \quad \therefore \gcd = 23$$

$$\gcd(208+93, 6923) = \gcd(301, 6923)$$

$$\therefore 6923 = 23 \cdot 301, \quad \therefore \gcd = 301$$

$$\text{and } 301 = 7 \cdot 43$$

$$\therefore 6923 = \underline{\underline{7 \cdot 23 \cdot 43}}$$

c. Factor 13561

$$\begin{aligned} \text{From } 233^2 &\equiv 3^2 \cdot 5 \pmod{13561}, \\ 1281^2 &\equiv 2^4 \cdot 5 \pmod{13561} \end{aligned}$$

$$(233 \cdot 1281)^2 \equiv 2^4 \cdot 3^2 \cdot 5^2 \equiv (2^2 \cdot 3 \cdot 5)^2 \pmod{13561}$$

$$\therefore 298473 \equiv 60^2 \pmod{13561}$$

$$\text{and } 298473 - 22 \cdot 13561 = 131 \not\equiv \pm 60 \pmod{13561}$$

$$\therefore \gcd(298473 - 60, 13561) = \gcd(298413, 13561)$$

$$298413 = 22 \cdot 13561 + 71$$

$$13561 = 191 \cdot 71, \quad \therefore \gcd = 71 \text{ (a prime)}$$

and 71 is prime.

$$\therefore 13561 = \underline{\underline{71 \cdot 191}}$$

7. (a). Factor 4537 by searching for  $x$  s.t.  
 $x^2 - k \cdot 4537$  is the product of small primes.

$$\sqrt{4537} = 67.4$$

$$\therefore 67^2 - 2 \cdot 4537 = -48 = -2^4 \cdot 3$$

$$68^2 - 2 \cdot 4537 = 87 = 3 \cdot 29$$

$\{1\}$

$\{1'\}$

$$\sqrt{2 \cdot 4537} = 95.3$$

$$95^2 - 2 \cdot 4537 = -49 = -7^2$$

$$96^2 - 2 \cdot 4537 = 142 = 2 \cdot 71$$

$\{2\}$

$\{2'\}$

$$\sqrt{3 \cdot 4537} = 116.7$$

$$116^2 - 3 \cdot 4537 = -155 = -5 \cdot 31$$

$$117^2 - 3 \cdot 4537 = 78 = 2 \cdot 3 \cdot 13$$

$\{3\}$

$\{3'\}$

$$\sqrt{4 \cdot 4537} = 134.7$$

$$134^2 - 4 \cdot 4537 = -192 = -2 \cdot 2 \cdot 48 = -2^6 \cdot 3$$

$$135^2 - 4 \cdot 4537 = 77 = 7 \cdot 11$$

Note:  $\gcd = 1$  from  $\{1\}, \{4\}$

$$\sqrt{5 \cdot 4537} = 150.6$$

$$150^2 - 5 \cdot 4537 = -185 = -5 \cdot 37$$

$$151^2 - 5 \cdot 4537 = 116 = 4 \cdot 29$$

$\{5\}$

$\{5'\}$

$$\sqrt{6 \cdot 4537} = 164.99$$

$$165^2 - 6 \cdot 4537 = 3$$

$\{6\}$

$\{6'\}$

$$\sqrt{7 \cdot 4537} = 178.2$$

$$178^2 - 7 \cdot 4537 = -75 = -3 \cdot 5^2$$

$$179^2 - 7 \cdot 4537 = 282 = 2 \cdot 141 = 2 \cdot 3 \cdot 47$$

[7]

[7']

$$\sqrt{8 \cdot 4537} = 190.5$$

$$190^2 - 8 \cdot 4537 = -196 = -2 \cdot 98 = -2 \cdot 7^2$$

[8]

$$191^2 - 8 \cdot 4537 = 185 = 5 \cdot 37$$

[8']

Note:  $\gcd = 1$  from [2], [8]

$\gcd = 1$  from [5], [8']

$$\sqrt{9 \cdot 4537} = 202.1$$

$$202^2 - 9 \cdot 4537 = -29$$

[9]

$\therefore$  look at [9], [5]

$$\therefore (202 \cdot 151)^2 \equiv (2 \cdot 29)^2 \pmod{4537}$$

$$(30502)^2 \equiv (58)^2 \pmod{4537}$$

$$\gcd(30502 - 58, 4537) = \gcd(30444, 4537) = 1$$

$$\gcd(30502 + 58, 4537) = \gcd(30560, 4537) = 1$$

$$203^2 - 9 \cdot 4537 = 376 = 2^3 \cdot 47$$

[9']

$\therefore$  look at [6'], [7'], [9']

$$(165 \cdot 179 \cdot 203)^2 \equiv (2^2 \cdot 3 \cdot 47)^2 \pmod{4537}$$

$$(5995605)^2 \equiv (564)^2 \pmod{4537}$$

$$\gcd(5995605 - 564, 4537) = \gcd(5995041, 4537)$$

$$5995041 = 1321 \cdot 4537 + 1664$$

$$4537 = 2 \cdot 1664 + 1209$$

$$1664 = 1 \cdot 1209 + 455$$

$$1209 = 3 \cdot 455 - 156$$

$$455 = 3 \cdot 156 - 13$$

$$156 = 12 \cdot 13$$

$$\gcd = 13$$

$\therefore 4537 = 13 \cdot \underline{349}$ , and  $349$  is prime

(b). Factor  $14429$  using method on (a).

Use hint

$$120^2 - 14429 = -29$$

$$3003^2 - 625 \cdot 14429 = -116 = -2^2 \cdot 29$$

$$\therefore (120 \cdot 3003)^2 \equiv (2 \cdot 29)^2 \pmod{14429}$$

$$(360360)^2 \equiv (58)^2 \pmod{14429}$$

$$\gcd(360360 - 58, 14429) = \gcd(360302, 14429)$$

$$360302 = 25 \cdot 14429 - 423$$

$$14429 = 34 \cdot 423 + 47$$

$$423 = 9 \cdot 47$$

$$\therefore \gcd = 47 \text{ (a prime)}$$

$$\gcd(360360 + 58, 14429) = \gcd(360418, 14429)$$

$$360418 = 25 \cdot 14429 - 307$$

$$14429 = 47 \cdot 307$$

$$\therefore \gcd = 307$$

$$\therefore 14429 = 47 \cdot 307$$

Q. Use Kraitchik's method to factor 20437

$$\sqrt{20437} = 142.9$$

$$143^2 - 20437 = 12 = 2^2 \cdot 3 \quad [1]$$

$$144^2 - 20437 = 299 = 13 \cdot 23$$

$$145^2 - " = 588 = 2^2 \cdot 3 \cdot 7^2 \quad [3]$$

$$146^2 - " = 879 = 3 \cdot 293$$

$$147^2 - " = 1172 = 2^2 \cdot 293$$

$$148^2 - " = 1467 = 3^2 \cdot 163$$

$$\text{From } [1], [3], (143 \cdot 145)^2 = (2^2 \cdot 3 \cdot 7)^2 \pmod{20437}$$

$$(20735)^2 \equiv (84)^2 \pmod{20437}$$

$$\gcd(20735 - 84, 20437) = \gcd(20651, 20437)$$

$$20651 = 1 \cdot 20437 + 214$$

$$20437 = 95 \cdot 214 + 107$$

$$214 = 2 \cdot 107$$

$$\therefore \gcd = 107 \text{ (a prime)}$$

$$\gcd(20735 + 84, 20437) = \gcd(20819, 20437)$$

$$\therefore 20819 = 1 \cdot 20437 + 382$$

$$20437 = 53 \cdot 382 + 191$$

$$382 = 2 \cdot 191$$

$$\therefore \gcd = 191 \text{ (a prime)}$$

$$\therefore 20437 = 107 \cdot 191$$

## 5.3 The Little Theorem

Note Title

5/9/2005

1. Use Fermat's Theorem to verify  $17 \mid (11^{104} + 1)$

Since  $17 \nmid 11$ ,  $11^{16} \equiv 1 \pmod{17}$  (Fermat's Th.)

$$\therefore (11^{16})^6 = 11^{96} \equiv 1 \pmod{17}$$

But  $121 = 11^2$  and  $7 \cdot 17 = 119 = 121 - 2$

$$\therefore 11^2 \equiv 2 \pmod{17}$$

$$\therefore 11^8 \equiv 2^4 = 16 \pmod{17}$$

$$\therefore 11^{96} - 11^8 \equiv 16 \pmod{17}$$

$$11^{104} \equiv 16 \pmod{17}$$

But  $16 \equiv -1 \pmod{17}$

$$\therefore 11^{104} \equiv -1 \pmod{17} \Rightarrow 17 \mid 11^{104} + 1$$

2. (a). If  $\gcd(a, 35) = 1$ , show  $a^{12} \equiv 1 \pmod{35}$

Since  $35 = 7 \cdot 5$ , Then  $\gcd(a, 7) = 1$ ,  $\gcd(a, 5) = 1$

$\therefore$  By Fermat's Theorem,

$$a^6 \equiv 1 \pmod{7} \text{ and } a^4 \equiv 1 \pmod{5}$$

$$\therefore a^{12} = a^6 \cdot a^6 \equiv 1 \pmod{7}, (a^4)^3 = a^{12} \equiv 1^3 \pmod{5}$$

Since  $\gcd(5, 7) = 1$ , by corollary 2, section 2.2,  
 $35 \mid a^{12} - 1 \Rightarrow a^{12} \equiv 1 \pmod{35}$

(b). If  $\gcd(a, 42) = 1$ , show  $168 = 3 \cdot 7 \cdot 8$  divides  $a^6 - 1$

Since  $42 = 2 \cdot 3 \cdot 7$ ,  $\gcd(a, 7) = \gcd(a, 3) = \gcd(a, 2) = 1$

By Fermat's Th.

$a^6 \equiv 1 \pmod{7}$ ,  $a^2 \equiv 1 \pmod{3}$ ,  $a \equiv 1 \pmod{2}$

But  $a^2 \equiv 1 \pmod{3} \Rightarrow a^6 = (a^2)^3 \equiv 1^3 \equiv 1 \pmod{3}$ , so

$$a^6 \equiv 1 \pmod{3}$$

$$\begin{aligned} \text{Also, } a^{6-1} &= (a-1)(a^5 + a^4 + a^3 + a^2 + a + 1) \\ &= (a-1)[a^3(a^2 + a + 1) + a^2 + a + 1] \\ &= (a-1)(a^3 + 1)(a^2 + a + 1) \\ &= (a-1)(a+1)(a^2 - a + 1)(a^2 + a + 1) \end{aligned}$$

Assume  $|a| > 1$ . Since  $a$  is odd,

if  $a \geq 0$ , Then  $a \geq 3$ , so  $2 \nmid a-1$  and

$$4 \mid a+1 \therefore 8 \mid a^6 - 1$$

if  $a < 0$ , Then  $a \leq -3$  so  $4 \mid a-1$  and  $2 \mid a+1$ , so

$$8 \mid a^6 - 1$$

Since  $7 \mid a^6 - 1$ ,  $3 \mid a^6 - 1$ , and  $8 \mid a^6 - 1$ , and  
 $3, 7, 8$  are relatively prime, Then

$$3 \cdot 7 \cdot 8 = 168 \mid a^6 - 1$$

(c). If  $\gcd(a, 133) = \gcd(6, 133) = 1$ , show  $133 \mid a^{18} - 6^{18}$

$133 = 7 \cdot 19 \therefore \gcd(a, 19) = \gcd(6, 19) = 1$

By Fermat's Th.,

$$a^{18} \equiv 1 \pmod{19}, 6^{18} \equiv 1 \pmod{19}$$

$$\therefore a^{18} - b^{18} \equiv 1 - 1 = 0 \pmod{19}, \therefore 19 \mid a^{18} - b^{18}$$

Also, since  $\gcd(a, 7) = \gcd(b, 7) = 1$ , by

Fermat's Th.,

$$a^6 \equiv 1 \pmod{7}, b^6 \equiv 1 \pmod{7}$$

$$\therefore a^6 - b^6 \equiv 0 \pmod{7}, \therefore 7 \mid a^6 - b^6$$

$$\text{Since } a^{18} - b^{18} = (a^6)^3 - (b^6)^3 =$$

$$(a^6 - b^6)((a^6)^2 + a^6 b^6 + (b^6)^2), \text{ Then } 7 \mid a^{18} - b^{18}$$

$$\therefore 7 \cdot 19 = 133 \mid a^{18} - b^{18}$$

3. From Fermat's Th., show for any integer  $n \geq 0$ ,  $13 \mid 11^{12n+6} + 1$

Since  $13 \nmid 11$ ,  $11^{12} \equiv 1 \pmod{13}$  by Fermat's Th.

$$\therefore 11^{12n} \equiv 1^n \equiv 1 \pmod{13}.$$

But  $11^2 \equiv 121 \pmod{13}$  and  $9 \cdot 13 = 117$ .  $\therefore 11^2 \equiv 4 \pmod{13}$

$$\therefore 11^6 \equiv 4^3 \equiv 64 \pmod{13}. \therefore 11^6 \equiv 64 - 13 \cdot 5 \equiv -1 \pmod{13}$$

$$\therefore 11^{12n} \cdot 11^6 \equiv 1 \cdot (-1) \pmod{13}, \text{ or } 11^{12n+6} \equiv -1 \pmod{13}$$

$$\therefore 13 \mid 11^{12n+6} + 1$$

4. Derive each congruence

(a).  $a^{21} \equiv a \pmod{15}$  for all  $a$ .

$$a^5 \equiv a \pmod{5} \text{ by Fermat's Th.}$$
$$\therefore (a^5)^4 \equiv a^4 \pmod{5}, \text{ or } a^{20} \equiv a^4 \pmod{5}$$
$$\therefore a^{21} \equiv a^5 \equiv a \pmod{5}$$

Also,  $a^3 \equiv a \pmod{3}$ ,  $\therefore a^7 \equiv a^7 \pmod{3}$ ,  
and  $(a^3)^2 \equiv a^2 \pmod{3}$ , or  $a^6 \equiv a^2 \pmod{3}$   
 $\therefore a^7 \equiv a^3 \equiv a \pmod{3}$ .  $\therefore a^{21} \equiv a \pmod{3}$

$$\therefore 5 \mid a^{21}-a \text{ and } 3 \mid a^{21}-a, \therefore 3 \cdot 5 \mid a^{21}-a,$$

$$\therefore a^{21} \equiv a \pmod{15}$$

(b)  $a^7 \equiv a \pmod{42}$  for all  $a$

$$42 = 7 \cdot 3 \cdot 2. \text{ By Fermat's Th., } a^7 \equiv a \pmod{7}$$

Also,  $a^3 \equiv a \pmod{3}$ , so  $a^6 \equiv a^2 \pmod{3}$ ,  
 $\therefore a^7 \equiv a^3 \equiv a \pmod{3}$

Also,  $a^2 \equiv a \pmod{2}$ ,  $\therefore a^3 \equiv a^2 \equiv a \pmod{2}$

$$\therefore (a^2)^3 \equiv a^3 \equiv a \pmod{2}. \therefore a^6 \equiv a \pmod{2}$$
$$\therefore a^7 \equiv a^2 \equiv a \pmod{2}$$

$$\therefore 7 \mid a^7-a, 3 \mid a^7-a, 2 \mid a^7-a. \therefore a^7 \equiv a \pmod{7 \cdot 3 \cdot 2}$$

(c)  $a^{13} \equiv a \pmod{3 \cdot 7 \cdot 13}$  for all  $a$ .

By Fermat's Th.,  $a^3 \equiv a \pmod{13}$

Also,  $a^7 \equiv a \pmod{7}$ .  $\therefore a^7 \cdot a^6 \equiv a \cdot a^6 \pmod{7}$ ,  
so  $a^{13} \equiv a^7 \equiv a \pmod{7}$

Also,  $a^3 \equiv a \pmod{3}$ , and  $\therefore a^4 \equiv a^2 \pmod{3}$   
 $\therefore (a^3)^4 \equiv a^4 \equiv a^2 \pmod{3}$ , or  $a^{12} \equiv a^2 \pmod{3}$   
 $\therefore a^{13} \equiv a^{12} \cdot a \equiv a^2 \cdot a = a^3 \equiv a \pmod{3}$

$\therefore 3 | a^{13} - a$ ,  $7 | a^{13} - a$ , and  $13 | a^{13} - a$ .

$\therefore a^{13} \equiv a \pmod{3 \cdot 7 \cdot 13}$  by Corollary 2, Sec. 2.2

(d).  $a^9 \equiv a \pmod{30}$  for all  $a$ .

$30 = 5 \cdot 3 \cdot 2$ . Using Fermat's Th.,

$a^5 \equiv a \pmod{5}$ .  $\therefore a^9 = a^5 \cdot a^4 \equiv a \cdot a^4 = a^5 \equiv a$

$\therefore a^9 \equiv a \pmod{5}$

$a^3 \equiv a \pmod{3}$ .  $\therefore (a^3)^3 \equiv a^3 \equiv a \pmod{3}$

$\therefore a^9 \equiv a \pmod{3}$

$a^2 \equiv a \pmod{2}$ .  $\therefore a^8 = (a^2)^4 \equiv a^4 \pmod{2}$ ,

$a^4 = (a^2)^2 \equiv a^2 \equiv a \pmod{2}$ .  $\therefore a^8 \equiv a \pmod{2}$

$\therefore a^9 = a^8 \cdot a \equiv a \cdot a = a^2 \equiv a \pmod{2}$

$\therefore 5 | a^9 - a$ ,  $3 | a^9 - a$ , and  $2 | a^9 - a$ , so

$a^9 \equiv a \pmod{5 \cdot 3 \cdot 2}$

5. If  $\gcd(a, 30) = 1$ , show that 60 divides  $a^4 + 59$

$$\gcd(a, 30) = 1 \Rightarrow \gcd(a, 2) = \gcd(a, 3) = \gcd(a, 5) = 1$$

A/so,  $\gcd(a, 4) = \gcd(a, 2^2) = 1$

$$60 = 2^2 \cdot 3 \cdot 5. \quad 60 \mid a^4 + 59 \text{ is the same as}$$
$$a^4 \equiv -59 \pmod{60}, \text{ or } a^4 \equiv 1 \pmod{60}$$

$$\gcd(a, 5) = 1 \Rightarrow a^4 \equiv 1 \pmod{5} \text{ by Fermat's Th.}$$

$$\gcd(a, 3) = 1 \Rightarrow a^2 \equiv 1 \pmod{3}. \quad \therefore a^4 \equiv 1 \pmod{3}$$

$$\gcd(a, 2) = 1 \Rightarrow a \equiv 1 \pmod{2}, \quad \therefore a^2 \equiv 1 \pmod{2}$$

$$\therefore a^2 \equiv 1-2 = -1 \pmod{2}$$

$$\therefore 2 \mid a^2 - 1, \quad 2 \mid a^2 + 1, \quad \therefore 4 \mid (a^2 + 1)(a^2 - 1) = a^4 - 1$$

$$\therefore 5 \mid a^4 - 1, \quad 3 \mid a^4 - 1, \quad 4 \mid a^4 - 1, \text{ and}$$

$$\gcd(5, a) = \gcd(3, a) = \gcd(4, a) = 1$$

$$\therefore \text{By corollary 2, sec. 2.2, } 60 \mid a^4 - 1$$

$$\therefore a^4 \equiv 1 \pmod{60}, \quad a^4 \equiv 1 - 60 = -59 \pmod{60}$$

$$\therefore 60 \mid a^4 + 59$$

6. (a). Find the units digit of  $3^{100}$  using Fermat's Th.

We need something mod 10.  $10 = 5 \cdot 2$

By Fermat's Th.,  $3^4 \equiv 1 \pmod{5}$

$$\therefore (3^4)^{25} = 3^{100} \equiv 1 \pmod{5}$$

Also,  $3 \equiv 1 \pmod{2}$ .  $\therefore 3^{100} \equiv 1 \pmod{2}$

$\therefore 5 \mid 3^{100} - 1$  and  $2 \mid 3^{100} - 1$ .

$\therefore 5 \cdot 2 \mid 3^{100} - 1$  by corollary 2, sec. 2.2

$$\therefore 3^{100} \equiv 1 \pmod{10}$$

$\therefore$  units digit of  $3^{100}$  is 1.

(b). For any integer  $a$ , verify that  $a^5$  and  $a$  have same units digit.

By Fermat's Th.,  $a^5 \equiv a \pmod{5}$

Also,  $a^2 \equiv a \pmod{2}$ ,  $\therefore a^4 \equiv a^2 \equiv a \pmod{2}$ ,  
 $\therefore a^5 = a^4 \cdot a \equiv a \cdot a = a^2 \equiv a \pmod{2}$

$\therefore 5 \mid a^5 - a$  and  $2 \mid a^5 - a$ .  $\therefore 10 \mid a^5 - a$

$\therefore a^5 \equiv a \pmod{10}$  Let  $0 \leq r < 10$

$$\therefore a^5 - r \equiv a - r \pmod{10}$$

$$\therefore a^5 - r \equiv 0 \pmod{10} \Leftrightarrow a - r \equiv 0 \pmod{10}$$

$\therefore$  units digit is the same.

7. If  $7 \nmid a$ , prove either  $7 \mid a^3 + 1$  or  $7 \mid a^3 - 1$

Pf: By Fermat's Th.,  $a^6 \equiv 1 \pmod{7}$

$$\therefore 7 \mid a^6 - 1. \text{ But } a^6 - 1 = (a^3 + 1)(a^3 - 1)$$

Suppose  $7 \nmid a^3 + 1$ .  $\therefore \gcd(7, a^3 + 1) = 1$ ,  
and so by Euclid's lemma,  
 $7 \mid a^3 - 1$ .

8. Prove

$$1835^{1910} + 1986^{2061} \equiv 0 \pmod{7}$$

Pf:  $1835 = 7 \cdot 262 + 1 \therefore 1835 \equiv 1 \pmod{7}$

$$\therefore 1835^{1910} \equiv 1 \pmod{7}$$

$$1986 = 7 \cdot 283 + 5 \therefore 1986 \equiv 5 \pmod{7}$$

Note also  $5^3 = 125 \equiv 126 - 1$ , and

$$126 = 7 \cdot 18 \therefore 5^3 \equiv -1 \pmod{7}$$

$$2061 = 3 \cdot 687$$

$$\therefore 1986^{2061} \equiv 5^{2061} = (5^3)^{687} \equiv (-1)^{687} \equiv -1 \pmod{7}$$

$$\therefore 1986^{2061} \equiv -1^{687} = -1 \pmod{7}$$

$$\therefore 1835^{1910} + 1986^{2061} \equiv 1 + (-1) = 0 \pmod{7}$$

9. (a) Let  $p$  be prime,  $\gcd(a, p) = 1$ . Use Fermat's Th. to verify that  $x \equiv a^{p-2} b \pmod{p}$  is a solution to  $ax \equiv b \pmod{p}$ .

$$\begin{aligned} \text{Pf: } ax \equiv b \pmod{p} &\Rightarrow ax \cdot a^{p-2} \equiv b \cdot a^{p-2} \pmod{p} \\ &\Rightarrow x a^{p-1} \equiv b a^{p-2} \pmod{p} \end{aligned}$$

But  $a^{p-1} \equiv 1 \pmod{p}$  by Fermat's Th.

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

$$\therefore x \equiv x a^{p-1} \equiv b a^{p-2} \pmod{p}$$

$$\therefore ax \equiv b \pmod{p} \Rightarrow x \equiv b a^{p-2} \pmod{p}$$

$$(b) 2x \equiv 1 \pmod{31} \Rightarrow x \equiv 2^{31-2} = 2^{29} \pmod{31}$$

But  $2^5 = 32 = 31 + 1 \therefore 2^5 \equiv 1 \pmod{31}$

$$\therefore (2^5)^5 = 2^{25} \equiv 1 \pmod{31}.$$

$$\therefore 2^{29} = 2^{25} \cdot 2^4 \equiv 2^4 = 16 \pmod{31}$$

$$\therefore 2x \equiv 1 \pmod{31} \Rightarrow x \equiv 16 \pmod{31}$$

$$6x \equiv 5 \pmod{11} \Rightarrow x \equiv 5 \cdot 6^{11-2} = 5 \cdot 6^9 \pmod{11}$$

But  $6^2 = 36 = 33 + 3 \therefore 6^2 \equiv 3 \pmod{11}$

$$\therefore 6^9 = (6^2)^4 \cdot 6 \equiv 3^4 \cdot 6 \pmod{11}$$

$$3^4 = 81 = 7 \cdot 11 + 4 \therefore 3^4 \cdot 6 \equiv 4 \cdot 6 \pmod{11}$$

$$\therefore x \equiv 5 \cdot 6^9 \equiv 5 \cdot (4 \cdot 6) = 120 \equiv 10 \pmod{11}$$

$$\therefore \underline{\underline{x \equiv 10 \pmod{11}}}$$

$$3x \equiv 17 \pmod{29} \Rightarrow x \equiv 17 \cdot 3^{29-2} \pmod{29}$$

$$3^3 = 27, \therefore 3^3 \equiv -2 \pmod{29}$$

$$\therefore 3^{27} \equiv (-2)^9, (-2)^5 = -32 \equiv -3 \pmod{29}$$

$$\therefore 3^{27} \equiv (-2)^9 = (-2)^5 \cdot (-2)^4 \equiv (-3)(16) = -48$$

$$\therefore 3^{27} \equiv -48 \equiv -48 + 58 = 10 \pmod{29}$$

$$\therefore 17 \cdot 3^{27} \equiv 17 \cdot 10 = 170 = 5 \cdot 29 + 25 \pmod{29}$$

$$\therefore \underline{\underline{x \equiv 25 \pmod{29}}}$$

10. Assume  $p \nmid a, p \nmid b, p$  prime

(a). If  $a^p \equiv b^p \pmod{p}$ , Then  $a \equiv b \pmod{p}$

Pf:  $a^p \equiv a \pmod{p}, b^p \equiv b \pmod{p}$  for

any integers  $a, b$ .

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

(b) If  $a^p \equiv b^p \pmod{p}$ , Then  $a^p \equiv b^p \pmod{p^2}$

By (a),  $a = b + pk$ , some  $k$ .

$$\begin{aligned}\therefore a^p - b^p &= (b + pk)^p - b^p \\ &= b^p + \sum_{i=1}^p \binom{p}{i} b^{p-i} (pk)^i - b^p \\ &= \sum_{i=1}^p \frac{p!}{i!(p-i)!} b^{p-i} (pk)^i\end{aligned}$$

Clearly, when  $i > 2$ , each term is divisible by  $p^2$  since  $(pk)^i$  has at least  $p^2$  in the term.

$$\therefore \text{Look at } i=1 \text{ term : } \frac{p!}{1!(p-1)!} b^{p-1} \cdot pk$$

$$= p \cdot b^{p-1} \cdot pk = p^2 k b^{p-1}.$$

So this is also divisible by  $p^2$ .  
 $\therefore a^p - b^p$  is divisible by  $p^2$ .

11. Use Fermat's Th. to prove that if  $p$  is an odd prime,

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

Pf: Since  $p$  is prime  $\geq 3$ , Then  $p \nmid a$  if  $a < p$ .  
 $\therefore$  By Fermat's Th.,  $a^{p-1} \equiv 1 \pmod{p}$ .  
There are  $p-1$  terms in  $1^{p-1} + 2^{p-1} + \dots + (p-1)^{p-1}$

$$\therefore 1^{p-1} + 2^{p-1} + \dots + (p-1)^{p-1} \equiv (p-1) \cdot 1 \pmod{p}$$
$$(p-1) \cdot 1 = p-1. \text{ Since } p \equiv 0 \pmod{p},$$

$$1^{p-1} + 2^{p-1} + \dots + (p-1)^{p-1} \equiv -1 \pmod{p}$$

Note: it's true even if  $p=2$

$$(b) 1^p + 2^p + \dots + (p-1)^p \equiv 0 \pmod{p}$$

Pf: By corollary to Fermat's Th.,  $a^p \equiv a \pmod{p}$

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

Since  $1+2+\dots+n = n(n+1)/2$ ,

$$1+2+\dots+(p-1) = (p-1)(p-1+1)/2 = p(p-1)/2$$

As  $p$  is an odd prime,  $p-1$  is even, so

$$p-1 = 2k, \text{ some } k.$$

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

$$\therefore 1^p + 2^p + \dots + (p-1)^p \equiv pk \equiv 0 \pmod{p}$$

12. Prove that if  $p$  is an odd prime,  $k$  an integer s.t.  $1 \leq k \leq p-1$ ,  
Then  $\binom{p-1}{k} \equiv (-1)^k \pmod{p}$

$$\text{Pf: } \binom{p-1}{k} = \frac{(p-1)!}{k!(p-k)!} = \frac{(p-1)(p-2)\dots(p-k)}{k!}$$

$$\therefore k! \binom{p-1}{k} = (p-1)(p-2)\dots(p-k)$$

$$\text{But } p-j \equiv -j \pmod{p}$$

$$\therefore (p-1)(p-2)\dots(p-k) \equiv (-1)(-2)\dots(-k) \pmod{p}$$

$$(-1)(-2)\dots(-k) = (-1)^k k!$$

$$\therefore k! \binom{p-1}{k} \equiv (-1)^k k! \pmod{p}$$

Since  $p-1 \geq k$ ,  $p > k$ ,  $\therefore p \nmid 1, 2, 3, \dots, k$   
 $\therefore \gcd(p, a) = 1$ ,  $1 \leq a \leq k$ .  $\therefore$  By Corollary 1, sec. 42,

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

13. If  $p, q$  are distinct odd primes s.t.  $p-1 \nmid q-1$ , and if  $\gcd(a, pq) = 1$ , show  $a^{q-1} \equiv 1 \pmod{pq}$

Pf:  $\gcd(a, pq) = 1 \Rightarrow \gcd(a, p) = \gcd(a, q) = 1$  since  $p, q$  are distinct primes.

$$\therefore a^{p-1} \equiv 1 \pmod{p} \text{ and } a^{q-1} \equiv 1 \pmod{q}$$

Since  $p-1 \nmid q-1$ , then  $q-1 = k(p-1)$ , some  $k$ .

$$\begin{aligned} \therefore a^{p-1} \equiv 1 \pmod{p} &\Rightarrow a^{k(p-1)} \equiv 1 \pmod{p} \\ &\Rightarrow a^{q-1} \equiv 1 \pmod{p} \end{aligned}$$

$$\therefore p \mid a^{q-1} - 1 \text{ and } q \mid a^{q-1} - 1$$

$\therefore pq \mid a^{q-1} - 1$  by corollary 2, sec. 2.2

$$\therefore a^{q-1} \equiv 1 \pmod{pq}$$

14. If  $p, q$  are distinct primes, prove

$$p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}$$

Pf: By Fermat's Th.,  $p^{q-1} \equiv 1 \pmod{q}$   
 Clearly,  $q \mid q^{p-1}$ , so  $q^{p-1} \equiv 0 \pmod{q}$

$$\therefore p^{q-1} + q^{p-1} \equiv 1 \pmod{q}$$

Similarly,  $p \mid p^{q-1}$  so  $p^{q-1} \equiv 0 \pmod{p}$ ,

and  $q^{p-1} \equiv 1 \pmod{p}$  by Fermat's Th.

$$\therefore p^{q-1} + q^{p-1} \equiv 1 \pmod{p}.$$

$$\therefore q \mid (p^{q-1} + q^{p-1} - 1) \text{ and } p \mid (p^{q-1} + q^{p-1} - 1),$$

and  $\gcd(p, q) = 1$ .  $\therefore$  By corollary 2 sec. 22,

$$pq \mid (p^{q-1} + q^{p-1} - 1)$$

$$\therefore p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}$$

15. Establish the following.

(a) If  $M_p = 2^p - 1$  is composite,  $p$  prime, then  $M_p$  is pseudoprime.

Pf: Must show  $2^{M_p} \equiv 2 \pmod{M_p}$

Proof is much like proof to Th. 5.2.

Since  $2^p - 1$  is composite,  $p \neq 2$ , so  $p \nmid 2$ .

By Fermat's Pl. (Pl's corollary),  $2^p \equiv 2 \pmod{p}$

$$\therefore 2^p - 2 = kp, \text{ some } k$$

$$\therefore 2^{m_p-1} = 2^{2^p-1-1} = 2^{2^p-2} = 2^{kp}$$

$$\begin{aligned}\therefore 2^{m_p-1} - 1 &= 2^{kp} - 1 \\ &= (2^p - 1)(2^{p(k-1)} + 2^{p(k-2)} + \dots + 2^p + 1) \\ &= m_p (2^{p(k-1)} + 2^{p(k-2)} + \dots + 2^p + 1) \\ &\equiv 0^p \pmod{m_p}\end{aligned}$$

$$\therefore 2^{m_p-1} \equiv 1 \pmod{m_p}$$

$$2 \cdot 2^{m_p-1} \equiv 2 \pmod{m_p}$$

$$\therefore 2^{m_p} \equiv 2 \pmod{m_p}$$

By def.,  $m_p$  is a pseudoprime.

(6). Every composite number  $F_n = 2^{2^n} + 1$  is a pseudoprime ( $n = 0, 1, 2, \dots$ ).

Pf: Since  $n+1 \leq 2^n$  for  $n \geq 0$ , Then

$$2^{n+1} \leq 2^{2^n}, \text{ so } 2^{n+1} \mid 2^{2^n} + 1$$

$\therefore$  By problem #21, since  $2 \cdot 2$ ,

$$(2^{2^n+1}-1) \mid (2^{2^n}-1), \text{ or } (2^{2^n+1}) \mid (2^{F_n-1}-1) \quad [1]$$

$$\text{But } 2^{2^{n+1}} = 2^{2 \cdot 2^n} = 2^{(2^n)2} = (2^{2^n})^2$$

$$\therefore 2^{2^{n+1}} - 1 = (2^{2^n})^2 - 1 = (2^{2^n} + 1)(2^{2^n} - 1)$$

$$= (F_n)(2^{2^n}-1) \quad [2]$$

$$\therefore \text{From [2], } F_n \mid (2^{2^{n+1}}-1) \quad [3]$$

$$\therefore \text{From [1] and [3], } F_n \mid (2^{F_n-1}-1)$$

$$\therefore F_n \mid 2(2^{F_n-1}-1) = 2^{F_n} - 2$$

$\therefore F_n$  is pseudoprime (whenever  $F_n$  is composite).

16. Confirm the following are absolute pseudoprimes

(a).  $1105 = 5 \cdot 13 \cdot 17$ . Let  $a$  be any integer

If  $1105 \nmid a$ , Then  $5 \nmid a$ ,  $13 \nmid a$ ,  $17 \nmid a$

$\therefore$  By Fermat's Th.,

$$a^4 \equiv 1 \pmod{5}, \quad a^{12} \equiv 1 \pmod{13}, \quad a^{16} \equiv 1 \pmod{17}$$

$$\therefore a^{1104} = (a^4)^{276} \equiv 1 \pmod{5}$$

$$a^{1104} = (a^{12})^{92} \equiv 1 \pmod{13}$$

$$a^{1104} = (a^{16})^{69} \equiv 1 \pmod{17}$$

$\therefore a^{1104} \equiv 1 \pmod{5 \cdot 13 \cdot 17}$  when  $1105 \nmid a$

$\therefore a^{1105} \equiv a \pmod{1105}$  when  $1105 \nmid a$

But when  $1105 \mid a$ , clearly  $1105 \mid a^{1105} - a$

$\therefore a^{1105} \equiv a \pmod{1105}$  for all  $a$ .

(b).  $2821 = 7 \cdot 13 \cdot 31$  Let  $a$  be any integer

If  $2821 \nmid a$ , then  $7 \nmid a, 13 \nmid a, 31 \nmid a$

$\therefore a^6 \equiv 1 \pmod{7}, a^{12} \equiv 1 \pmod{13}, a^{30} \equiv 1 \pmod{31}$

$$\therefore a^{2820} = (a^6)^{470} \equiv 1 \pmod{7}$$

$$a^{2820} = (a^{12})^{235} \equiv 1 \pmod{13}$$

$$a^{2820} = (a^{30})^{94} \equiv 1 \pmod{31}$$

$$\therefore a^{2820} \equiv 1 \pmod{7 \cdot 13 \cdot 31} \text{ when } 2821 \nmid a$$

$$\therefore a^{2821} \equiv a \pmod{2821} \text{ when } 2821 \nmid a$$

But when  $2821 \mid a$ , clearly  $a^{2821} \equiv a \pmod{2821}$

$$\therefore \text{For all } a, a^{2821} \equiv a \pmod{2821}$$

(c)  $2465 = 5 \cdot 17 \cdot 29$  Let  $a$  be any integer

If  $2465 \nmid a$ , Then  $5 \nmid a$ ,  $17 \nmid a$ ,  $29 \nmid a$

$$\therefore a^4 \equiv 1 \pmod{5}, a^{16} \equiv 1 \pmod{17}, a^{28} \equiv 1 \pmod{29}$$

$$a^{2464} = (a^4)^{616} \equiv 1 \pmod{5}$$

$$a^{2464} = (a^{16})^{154} \equiv 1 \pmod{17}$$

$$a^{2464} = (a^{28})^{88} \equiv 1 \pmod{29}$$

$$\therefore a^{2464} \equiv 1 \pmod{5 \cdot 17 \cdot 29} \text{ when } 2465 \nmid a$$

$$\therefore a^{2465} \equiv a \pmod{2465} \text{ when } 2465 \nmid a$$

But when  $2465 \mid a$ , clearly  $a^{2465} \equiv a \pmod{2465}$

$$\therefore \text{For all } a, a^{2465} \equiv a \pmod{2465}$$

17. Show that the smallest pseudoprime 341 is not an absolute prime by showing  $11^{341} \not\equiv 11 \pmod{341}$

$$341 = 11 \cdot 31. \text{ Suppose } 11^{341} \equiv 11 \pmod{341}$$

$$\text{Then } 11^{341} \equiv 11 \pmod{31}. \text{ But } 11^2 = 121 \equiv -3 \pmod{31}$$

$$\therefore 11^{2 \cdot 170} \equiv (-3)^{170} \pmod{31}$$

$$\text{But } (-3)^9 = -19683 \text{ and } -635 \cdot 31 = -19685$$

$$\therefore (-3)^9 \equiv 2 \pmod{31}$$

$$\therefore (-3)^{9 \cdot 18} = (-3)^{162} \equiv 2^{18} \pmod{31}$$

$$\text{But } 2^{10} = 1024 \equiv 1 \pmod{31} \quad (31 - 33 = 1023)$$

$$2^8 = 256 = 8 \cdot 31 + 8 \equiv 8 \pmod{31}$$

$$\therefore 2^{18} \equiv 8 \pmod{31}$$

$$\therefore (-3)^{162} \equiv 8 \pmod{31}$$

$$(-3)^4 = 81 = 2 \cdot 31 + 19 \equiv 19 \pmod{31}$$

$$\therefore (-3)^8 \equiv 19^2 = 361 = 31 \cdot 11 + 20 \equiv 20 \pmod{31}$$

$$\therefore (-3)^{162} \cdot (-3)^8 \equiv 8 \cdot 20 = 160 = 5 \cdot 31 + 5 \equiv 5 \pmod{31}$$

$$\therefore 11^{340} \equiv (-3)^{170} \equiv 5 \pmod{31}$$

$$\therefore 11^{341} \equiv 55 \cdot 11 = 55 = 31 + 24 \equiv 24 \pmod{31}$$

$$\therefore 11^{341} \equiv 24 \pmod{31}, \text{ so } 11^{341} \not\equiv 11 \pmod{341}$$

$\therefore$  Contradiction reached, so  $11^{341} \not\equiv 11 \pmod{341}$

=

Note: assuming  $11^{341} \equiv 11 \pmod{341} \Rightarrow 11^{341} \equiv 11 \pmod{11}$   
 But since  $11^6 \equiv 1 \pmod{11}$ ,  $11^{340} \equiv 1 \pmod{11}$ ,  
 and  $\therefore 11^{341} \equiv 11 \pmod{11}$ . That's why  
 attacked problem using mod 31.

18. (a) When  $n=2p$ ,  $p$  an odd prime, prove  $a^{n-1} \equiv a \pmod{n}$   
 for any integer  $a$ .

Pf:  $a^{p-1} \equiv 1 \pmod{p}$  (Fermat Th.), and  $a^p \equiv a \pmod{p}$

$$\therefore a^p \cdot a^{p-1} = a^{2p-1} \equiv a^p \equiv a \pmod{p}$$

As  $2p=n$ ,  $\therefore a^{n-1} \equiv a \pmod{p}$ , so  $p \mid a^{n-1} - a$ .

Now, if  $a$  is even, let  $a=2x$ , some  $x$

$$\therefore a^{n-1} - a = (2x)^{n-1} - 2x = 2^{n-1}x^{n-1} - 2x \\ = 2(2^{n-2}x^{n-1} - x)$$

Since  $n \geq 2$ , Then  $2 \mid a^{n-1} - a$

Suppose  $a$  is odd. Since  $2p$  is even,

$n-1$  is odd.  $\therefore a^{n-1}$  is odd, and  
 $\therefore a^{n-1} - a$  is even, so  $2 \mid a^{n-1} - a$ .

$\therefore$  Both 2 and  $p$  divide  $a^{n-1} - a$ .

Since  $\gcd(2, p) = 1$ , Then  $2p \mid a^{n-1} - a$ ,

$$\text{so } a^{n-1} \equiv a \pmod{n}$$

(b) For  $n = 195 = 3 \cdot 5 \cdot 13$ , verify  $a^{n-2} \equiv a \pmod{n}$   
for any integer  $a$ .

Pf: If  $195 \mid a$ , Then clearly  $195 \mid a^{n-2} - a$   
 $\therefore$  Assume  $195 \nmid a$ .

$\therefore 3 \nmid a, 5 \nmid a, 13 \nmid a$ .

$\therefore$  By Fermat's Th.,  $a^2 \equiv 1 \pmod{3}$

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

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

$$\therefore a^{192} = a^{2 \cdot 96} \equiv 1 \pmod{3}$$

$$a^{192} = a^{4 \cdot 48} \equiv 1 \pmod{5}$$

$$a^{192} = a^{12 \cdot 16} \equiv 1 \pmod{13}$$

$$\therefore a^{192} \equiv 1 \pmod{3 \cdot 5 \cdot 13}$$

$$\therefore a^{193} \equiv a \pmod{n}$$

$$\therefore a^{n-2} \equiv a \pmod{n}$$

19. Prove any integer of the form

$$n = (6k+1)(12k+1)(18k+1)$$

is an absolute pseudoprime if all three factors are prime

Pf: Let  $\rho_1 = 6k+1$ ,  $\rho_2 = 12k+1$ ,  $\rho_3 = 18k+1$

Assume  $\rho_1, \rho_2, \rho_3$  are prime.

$$\begin{aligned} n &= (72k^2 + 18k + 1)(18k + 1) \\ &= 18 \cdot 72k^3 + 72k^2 + 18 \cdot 18k^2 + 18k + 18k + 1 \\ &= 36 \cdot 36k^3 + 36 \cdot 2k^2 + 36 \cdot 9k^2 + 36k + 1 \\ \therefore n-1 &= 36k[36k^2 + 11k^2 + 1] \\ \therefore (\rho_1-1) &| (n-1), (\rho_2-1) | (n-1), (\rho_3-1) | n-1 \end{aligned}$$

Since  $\rho_1, \rho_2, \rho_3$  are distinct primes, and  
n is square-free (each prime of power 1),  
Then n is absolute pseudoprime by Th. 5.3

20. Show that 561 |  $2^{561}-2$  and  $561 | 3^{561}-3$

(a).  $2^2 \equiv 1 \pmod{3}$ ,  $\therefore (2^2)^{280} = 2^{560} \equiv 1 \pmod{3}$

$$2^{10} \equiv 1 \pmod{11} \quad (\text{Fermat's Th.})$$

$$\therefore (2^{10})^{56} = 2^{560} \equiv 1 \pmod{11}$$

$$2^{16} \equiv 1 \pmod{17} \quad (\text{Fermat's Th.})$$

$$\therefore (2^{16})^{35} = 2^{560} \equiv 1 \pmod{17}$$

$$\therefore 2^{560} \equiv 1 \pmod{3 \cdot 11 \cdot 17}, \text{ and } 3 \cdot 11 \cdot 17 = 561$$

$$\therefore 2^{560} - 2 \equiv 2 \pmod{561}, \therefore 561 \mid 2^{561} - 2$$

(b) By Fermat's Th.,  $3^{10} \equiv 1 \pmod{11}$ ,  $3^{16} \equiv 1 \pmod{17}$

$$\therefore 3^{560} \equiv 1 \pmod{11}, 3^{560} \equiv 1 \pmod{17}$$

$$\therefore 11 \mid 3^{561} - 3, 17 \mid 3^{561} - 3,$$

$$\therefore 11 \cdot 17 \mid 3^{561} - 3. \text{ Clearly } 3 \nmid 3^{561} - 3$$

$$\therefore 3 \cdot 11 \cdot 17 \mid 3^{561} - 3 \text{ since } \gcd(3, 11, 17) = 1$$

$$\therefore \text{Alternatively, } 3^7 = 2187 = 4 \cdot 561 - 57,$$

$$\therefore 3^7 \equiv -57 \pmod{561}$$

$$\therefore (3^7)^{80} = 3^{560} \equiv (-57)^{80} \pmod{561}$$

$$\text{But } 57^2 = 3249 = 6 \cdot 561 - 117$$

$$\therefore 57^2 \equiv (-117) \pmod{561}, \text{ and } (57^2)^{40} \equiv (-57)^{80}$$

$$\therefore 3^{560} \equiv (-117)^{40} \pmod{561}$$

$$(-117)^2 = 13689 = 24 \cdot 561 + 225$$

$$\therefore (-117)^2 \equiv 225 \pmod{561}$$

$$\therefore 3^{560} \equiv (-117)^{40} \equiv 225^{20} \pmod{561}$$

$$225^2 = 50625 = 90 \cdot 561 + 135$$

$$\therefore 225^2 \equiv 135 \pmod{561}$$

$$\therefore 3^{560} \equiv 225^{20} \equiv 135^{10} \pmod{561}$$

$$135^2 = 18225 = 32 \cdot 561 + 273$$

$$\therefore 135^2 \equiv 273 \pmod{561}$$

$$\therefore 3^{560} \equiv 135^{10} \equiv 273^5 \pmod{561}$$

$$273^2 = 74529 = 133 \cdot 561 - 84$$

$$\therefore 273^2 \equiv -84 \pmod{561}$$

$$\therefore (273)^4 = (-84)^2 = 2056 = 12 \cdot 561 + 324$$

$$\begin{aligned}\therefore 3^{560} &\equiv 273^5 = 273^4 \cdot 273 \\ &\equiv (-324) \cdot 273 \pmod{561}\end{aligned}$$

$$\text{But } -324 \cdot 273 = -88452 = -157 \cdot 561 - 375$$

$$\begin{aligned}\therefore 3^{560} &\equiv (-324) \cdot 273 \equiv -375 \pmod{561} \\ &\equiv 186 \pmod{561}\end{aligned}$$

$$\therefore 3^{561} \equiv 3 \cdot 186 = 558 \pmod{561}$$

$$\therefore 3^{561} + 3 \equiv 558 + 3 \equiv 0 \pmod{561},$$

$$\therefore 3^{561} \equiv 3 \pmod{561}$$

$$21. \text{ Show } 2222^{5555} + 5555^{2222} \equiv 0 \pmod{7}$$

$$1111 = 159 \cdot 7 - 2 \quad \therefore 1111 \equiv -2 \pmod{7}$$

$$\therefore 2222 \equiv -4 \pmod{7}, 5555 \equiv -10 \equiv -10 + 14 = 4 \pmod{7}$$

$$\therefore 2222^{5555} \equiv (-4)^{5555} \pmod{7}$$

$$\text{But } (-4)^2 = 16 \equiv 2 \pmod{7}, 5555 = 2(2777) + 1$$

$$\therefore (-4)^{5555} = (-4)^{2(2777)+1} \equiv 2 \cdot (-4) \pmod{7}$$

$$\therefore 2222^{5555} \equiv -2^{2779} \pmod{7}$$

But  $2^3 \equiv 1 \pmod{7}$ , and  $3 \cdot 926 = 2778$

$$\therefore (2^3)^{926} = 2^{2778} \equiv 1 \pmod{7}$$

$$\therefore 2222^{5555} \equiv -2^{2778} = -2^{2778} \pmod{7}$$

$$\text{Now } 5555 \equiv 4 \pmod{7} \Rightarrow 5555^{2222} \equiv 4^{2222} \pmod{7}$$

$$\therefore 5555^{2222} \equiv 2^{4444} \pmod{7}$$

and  $4444 = 1481 \cdot 3 + 1$ , and  $2^3 \equiv 1 \pmod{7}$

$$\therefore 5555^{2222} \equiv (2^3)^{1481} \cdot 2 \equiv 1 \cdot 2 = 2 \pmod{7}$$

$$\therefore 2222^{5555} + 5555^{2222} \equiv -2 + 2 = 0 \pmod{7}$$

$\equiv$

Theorem 5.3 - a more explicit proof

Let  $n$  be a composite square-free integer,  
say,  $n = p_1 p_2 p_3 \dots p_{r-1}$ , each  $p_i$  distinct.

If  $(p_i - 1) | (n - 1)$  for  $i = 1, 2, \dots, r$ , Then  $n$  is  
absolute prime.

Pf: Suppose initially  $a$  is some integer s.t.

$$\gcd(a, n) = 1. \therefore \gcd(a, p_i) = 1 \text{ for each } i$$

Fermat's Th. yields  $p_i \mid a^{p_i-1} - 1$

Since  $(p_i-1) \mid (n-1)$ , Then  $n-1 = k(p_i-1)$ ,  
some  $k$ .

$$\therefore a^{k(p_i-1)} - 1 = (a^{p_i-1} - 1)(a^{(p_i-1)(k-1)} + \dots + a^{p_i-1} + 1)$$

$$\therefore p_i \mid a^{n-1} - 1 \text{ for all } i.$$

$$\therefore p_i \mid a^n - a \text{ for all } i.$$

$\therefore$  From corollary 2, Th. 2.4 (sec. 2.2),

$$n \mid a^n - a$$

Now if  $\gcd(a, n) \neq 1$ , Then let

$$\gcd(a, n) = p_{j_1} p_{j_2} \dots p_{j_s}, \text{ where } p_{j_x} \in \{p_1, \dots, p_r\}$$

Since  $n$  is square-free and composed of  
distinct primes, Then  $p_{j_x}$  are all distinct

and have exponents of 1.

$$\text{Let } a' = a / p_{j_1} p_{j_2} \cdots p_{j_s}$$

$$\therefore a = (p_{j_1} \cdot p_{j_2} \cdots p_{j_s}) (a') \quad [1]$$

$\therefore \gcd(a', n) = 1$ , and from above,

$$n \mid (a')^n - a$$

$$\therefore n \mid ((p_{j_1} \cdot p_{j_2} \cdots p_{j_s})^n (a')^n - (p_{j_1} \cdot p_{j_2} \cdots p_{j_s}) (a'))$$

From [1] above,  $(p_{j_1} \cdot p_{j_2} \cdots p_{j_s}) (a') = q$

$$\therefore n \mid a^n - a \text{ if } \gcd(a, n) \neq 1$$

$$\therefore n \mid a^n - a \text{ for all } a.$$

## 5.4 Wilson's Theorem

Note Title

5/25/2005

1. (a). Find the remainder when  $15!$  is divided by 17.

Since  $(17-1)! \equiv -1 \pmod{17}$ , Then  $16! \equiv -1 \pmod{17}$

But  $16 \equiv -1 \pmod{17}$

$\therefore 16! \equiv 16 \pmod{17}$ .  $\gcd(16, 17) = 1$ ,

$\therefore 16!/16 \equiv 16/16 \pmod{17}$

$\therefore 15! \equiv 1 \pmod{17}$

(b) Find the remainder when  $2(26!)$  is divided by 29

By Wilson's Th.,  $28! \equiv -1 \pmod{29}$

$\therefore 28! \equiv 28 \pmod{29}$ , Since  $\gcd(28, 29) = 1$ ,

$\therefore 27! \equiv 1 \pmod{29}$ ,  $\therefore 27! \equiv 1+29 \pmod{29}$

$\therefore 27! \equiv 30 \pmod{29}$ ,  $9 \cdot 3 \cdot 26! \equiv 30 \pmod{29}$ ,

$\therefore 9 \cdot 26! \equiv 10 \pmod{29}$  since  $\gcd(3, 29) = 1$

$\therefore 9 \cdot 26! \equiv 39 \pmod{29}$

$3 \cdot 26! \equiv 13 \pmod{29}$

$\therefore 3 \cdot 26! \equiv 13 + 29 = 42 \equiv 3 \cdot 14 \pmod{29}$

$\therefore 26! \equiv 14 \pmod{29}$ ,  $\therefore 2 \cdot 26! \equiv 28 \pmod{29}$

2. Determine whether 17 is a prime by deciding whether  $16! \equiv -1 \pmod{17}$

$$4 \cdot 3 \cdot 2 \cdot 1 = 24 = 17 + 7 \equiv 7 \pmod{17}$$

$$\therefore 5! \equiv 5 \cdot 7 = 35 = 2 \cdot 17 + 1 \equiv 1 \pmod{17}$$

$$\therefore 6! \equiv 6 \pmod{17},$$

$$7! \equiv 42 = 34 + 8 \equiv 8 \pmod{17}$$

$$8! \equiv 64 = 68 - 4 \equiv -4 \pmod{17}$$

$$9! \equiv -36 = -34 - 2 \equiv -2 \pmod{17}$$

$$10! \equiv -20 \equiv -3 \pmod{17}$$

$$11! \equiv -33 \equiv -34 + 1 \equiv 1 \pmod{17}$$

$$12! \equiv 12 = 17 - 5 \equiv -5 \pmod{17}$$

$$13! \equiv -5 \cdot 13 = -65 = -68 + 3 \equiv 3 \pmod{17}$$

$$14! \equiv 3 \cdot 14 = 42 = 34 + 8 \equiv 8 \pmod{17}$$

$$15! \equiv 8 \cdot 15 = 120 = 7 \cdot 17 + 1 \pmod{17}$$

$$16! \equiv 16 = 17 - 1 \equiv -1 \pmod{17}$$

3. Arrange 2, 3, 4, ..., 21 in pairs to satisfy  $ab \equiv 1 \pmod{23}$

Look for  $23+1=24$ , not  $2 \cdot 23+1=47$  (prime),  $3 \cdot 23+1=70$ ,

$$4 \cdot 23+1=93, 5 \cdot 23+1=116, 6 \cdot 23+1=138, 7 \cdot 23+1=162$$

$$8 \cdot 23+1=185, 9 \cdot 23+1=208, 10 \cdot 23+1=231$$

$$11 \cdot 23+1=254, 12 \cdot 23+1=277, 13 \cdot 23+1=300, 14 \cdot 23+1=323$$

$$2 \cdot 12 = 24 \equiv 1 \pmod{23}$$

$$3 \cdot 8 = 24 \equiv 1$$

$$4 \cdot 6 = 24 \equiv 1$$

$$5 \cdot 14 = 20 \equiv 1$$

$$7 \cdot 10 = 20 \equiv 1$$

$$9 \cdot 18 = 162 \equiv 1$$

$$11 \cdot 21 = 231 \equiv 1$$

$$13 \cdot 16 = 208 \equiv 1$$

$$15 \cdot 20 = 300 \equiv 1$$

$$17 \cdot 19 = 323 \equiv 1$$

4. Show That  $18! \equiv -1 \pmod{437}$

$19 \mid 437$  since  $19 \cdot 23 = 437$

By Wilson's Th.,  $18! \equiv -1 \pmod{19}$

Must show  $23 \mid 18! + 1$

By Wilson's Th.,  $22! \equiv -1 \equiv 22 \pmod{23}$

$$\therefore 22!/22 \equiv 22/22 \equiv 1 \pmod{23} \quad \gcd(22, 23) = 1$$

$$\therefore 21! \equiv 1 \equiv 1 + 23 = 24 \pmod{23}$$

$$\therefore 21 \cdot 20! \equiv 8 \cdot 3 \pmod{23}$$

$$\therefore 7 \cdot 20! \equiv 8 \pmod{23} \quad \gcd(3, 23) = 1$$

$$\therefore 7 \cdot 20 \cdot 19! \equiv 8 \pmod{23}$$

$$7 \cdot 5 \cdot 19! \equiv 2 \pmod{23} \quad \gcd(4, 23) = 1$$

$$7 \cdot 5 \cdot 19 \cdot 18! \equiv 2 \pmod{23}$$

$$\therefore 7 \cdot 5 \cdot 19 \cdot 18! \equiv 2 + 23 = 25 \pmod{23}$$

$$\therefore 7 \cdot 19 \cdot 18! \equiv 5 \pmod{23} \quad \gcd(5, 23) = 1$$

$$7 \cdot 19 \cdot 18! \equiv 5 + 23 = 28 \pmod{23}$$

$$\therefore 19 \cdot 18! \equiv 4 \pmod{23} \quad \gcd(7, 23) = 1$$

$$19 \cdot 18! \equiv 4 - 23 = -19 \pmod{23}$$

$$\therefore 18! \equiv -1 \pmod{23} \quad \gcd(19, 23) = 1$$

$$\therefore 23 \mid 18! + 1 \text{ and } 19 \mid 18! + 1$$

$$\therefore 19 \cdot 23 = 437 \mid 18! + 1$$

5. (a) Prove  $n > 1$  is prime  $\Leftrightarrow (n-2)! \equiv 1 \pmod{n}$

Pf: By Wilson's Th and its converse,

$$n \text{ is prime} \Leftrightarrow (n-1)! \equiv -1 \pmod{n}$$

$$\equiv -1 + n = n-1 \pmod{n}$$

Since  $\gcd(n, n-1) = 1$  (prob. #12, sec. 2.2),

$$\therefore (n-1)! / (n-1) \equiv (n-1) / (n-1) \pmod{n}, \text{ or}$$

$$(n-1)! \equiv -1 \pmod{n} \Leftrightarrow (n-2)! \equiv 1 \pmod{n}$$

$$\therefore n \text{ is prime} \Leftrightarrow (n-2)! \equiv 1 \pmod{n}$$

(b) If  $n$  is composite, show  $(n-1)! \equiv 0 \pmod{n}$ , except when  $n=4$ !

Pf: For  $n=4$ ,  $(4-1)! = 3! = 6 \equiv 2 \pmod{4}$ .  $\therefore$  Assume  $n > 4$ .

Since  $n$  is composite, let  $r \cdot s = n$ .

Since  $\gcd(n, n-1) = 1$  by prob. #12, sec. 2.2,  
 $1 < r < n-1$ .  $\therefore r$  must be one of the factors of  $(n-1)!$

Similarly,  $1 < s < n-1$ .

If  $r \neq s$ , then  $r$  and  $s$  are different factors in  $(n-1)!$ , so  $n = rs \mid (n-1)!$   
 $\therefore (n-1)! \equiv 0 \pmod{n}$

Suppose  $r=s$ .  $\therefore n = r^2$

Now  $r < \frac{n}{2}$ . For if  $r \geq \frac{n}{2}$ , then

$$n = r^2 \geq \frac{n^2}{4}, \text{ or } 4n \geq n^2, \text{ or } 4 \geq n$$

But  $n=4$ ,  $\therefore r < \frac{n}{2}$

$\therefore 2r < n$ , or  $2r \leq n-1$

$\therefore$  Both  $r$  and  $2r \neq r$  are factors of  $(n-1)!$

$\therefore r(2r) \mid (n-1)!$ , so  $r^2 \mid (n-1)!$   
 $\therefore (n-1)! \equiv 0 \pmod{n}$

6. Given a prime number  $p$ , establish

$$(p-1)! \equiv p-1 \pmod{1+2+\dots+(p-1)}$$

Pf.: From Wilson's Th.,  $(p-1)! \equiv -1 \pmod{p}$

$$\therefore p \mid (p-1)! - (p-1)$$

Now  $1+2+\dots+n = \frac{n(n+1)}{2}$  for all  $n$ .

$$\therefore 1+2+\dots+(p-1) = \frac{(p-1)p}{2}$$

Since  $p-1$  is even,  $(p-1)/2$  is an integer,  
and clearly,  $\frac{(p-1)}{2} < p-1$

$$\text{Also, } (p-1) \mid (p-1)! - (p-1)$$

$$\therefore \frac{(p-1)}{2} \mid (p-1)! - (p-1)$$

Also,  $\gcd\left(\frac{p-1}{2}, p\right) = 1$  since  $p$  is prime.

$\therefore p$  and  $\frac{p-1}{2}$  divide  $(p-1)! - (p-1)$ , so

$$p \left( \frac{p-1}{2} \right) = 1+2+\dots+(p-1) \text{ divides } (p-1)! - (p-1)$$

$$\therefore (p-1)! \equiv p-1 \pmod{1+2+\dots+(p-1)}$$

? If  $p$  is prime, prove that for any  $a$ ,

$$p \mid a^p + (p-1)! a \quad \text{and} \quad p \mid (p-1)! a^p + a$$

$$(a) p \mid a^p + (p-1)! a$$

Pf: By corollary to Fermat's Th,  $a^p \equiv a \pmod{p}$ ,  
for any  $a$ .

By Wilson's Th.,  $-1 \equiv (p-1)! \pmod{p}$

$\therefore$  By multiplying,  $-a^p \equiv (p-1)! a \pmod{p}$ ,

or,  $a^p \equiv - (p-1)! a \pmod{p}$

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

$$(b) p \mid (p-1)! a^p + a$$

Pf: As in (a),  $(p-1)! \equiv -1 \pmod{p}$

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

Multiplying together,  $a^p (p-1)! \equiv -a \pmod{p}$ , or

$$p \mid a^p (p-1)! + a$$

Q. Find two odd primes  $p \leq 13$  s.t.  $(p-1)! \equiv -1 \pmod{p^2}$

S:  $4! + 1 = 25$ , so  $p^2 \mid (p-1)! + 1$

$$7: 6! + 1 = 721, 7^2 \nmid 721$$

$$9: 8! + 1 = 40321, 9 \nmid 40321$$

$$11: 10! + 1 = 3,628,801, 11^2 \nmid 3,628,801$$

$$13: 12! + 1 = 479,001,601, \text{ and } 13^2 \nmid 479,001,601$$

9. Prove for any odd prime,  $1^2 \cdot 3^2 \cdot 5^2 \cdots (\rho-2)^2 \equiv (-1)^{\frac{\rho+1}{2}} \pmod{\rho}$

$$\text{Pf: } K \equiv k - p = -(p-k) \pmod{p}$$

$$\begin{aligned} \therefore 2 &\equiv -(p-2) \pmod{p} \\ 4 &\equiv -(p-4) \pmod{p} \\ &\vdots \\ p-1 &\equiv -1 \pmod{p} \end{aligned} \quad \left. \begin{array}{l} \\ \\ \end{array} \right\} \begin{array}{l} \frac{p-1}{2} \text{ factors} \\ (\rho > 2) \end{array}$$

$$\therefore 2 \cdot 4 \cdots (p-1) \equiv (-1)(-3) \cdots [-(p-2)] \pmod{p}, \rho > 2$$

There are  $(p-1)/2$  factors, so

$$2 \cdot 4 \cdots (p-1) \equiv (-1)^{\frac{p-1}{2}} \cdot 1 \cdot 3 \cdots (p-2) \pmod{p}$$

Now, multiply both sides by  $1 \cdot 3 \cdot 5 \cdots (p-2)$

$$\therefore 1 \cdot 2 \cdot 3 \cdot 4 \cdots (p-2) \cdot (p-1) = (p-1)! \equiv (-1)^{\frac{p-1}{2}} 1^2 \cdot 3^2 \cdots (p-2)^2 \pmod{p}$$

$$\text{Or, } (p-1)! \equiv (-1)^{\frac{p-1}{2}} 1^2 \cdot 3^2 \cdots (p-2)^2 \pmod{p}$$

By Wilson's Th.,  $-1 \equiv (p-1)! \pmod{p}$

$$\therefore -1 \equiv (-1)^{\frac{p-1}{2}} 1^2 \cdot 3^2 \cdots (p-2)^2 \pmod{p}$$

Multiplying both sides by  $(-1)^{\frac{p-1}{2}}$ , and  
noting that  $\left[(-1)^{\frac{p-1}{2}}\right]^2 = 1$  since  $(-1)^{\frac{p-1}{2}} = 1$  or  $-1$ ,

$$\text{and noting } -1 = (-1)^{\frac{p-1}{2}},$$

$$(-1)^{\frac{p-1}{2}} (-1)^{\frac{p-1}{2}} \equiv 1^2 \cdot 3^2 \cdots (p-2)^2 \pmod{p}$$

$$\therefore (-1)^{\frac{p+1}{2}} \equiv 1^2 \cdot 3^2 \cdots (p-2)^2 \pmod{p}$$

10. (a) For a prime  $p$  of the form  $4k+3$ , prove either

$$\left(\frac{p-1}{2}\right)! \equiv 1 \pmod{p} \quad \text{or} \quad \left(\frac{p-1}{2}\right)! \equiv -1 \pmod{p}$$

Pf: If  $p$  is any prime,  $a^2 \equiv 0 \pmod{p} \Rightarrow$   
 $a \equiv 0 \pmod{p}$  or  $b \equiv 0 \pmod{p}$  (second of

Section 4.2, proved a beginning of solutions to problems of 4.2, labelled Theorem 2).

$\therefore$  If  $a$  is any integer,  $a^2 \equiv 1 \pmod{p} \Rightarrow$   
 $a^2 - 1 \equiv 0 \pmod{p}$ ,  $\therefore a+1 \equiv 0 \pmod{p}$  or  
 $a-1 \equiv 0 \pmod{p}$   
 $\therefore a^2 \equiv 1 \pmod{p} \Rightarrow a \equiv 1 \pmod{p}$  or  $a \equiv -1 \pmod{p}$

In the proof to Theorem 5.5 on p. 100,

$$(-1) \equiv (-1)^{\frac{p-1}{2}} \left[ \left( \frac{p-1}{2} \right)! \right]^2 \pmod{p}$$

Multiplying both sides by  $(-1)^{\frac{p-1}{2}}$  and

$$\text{noting } (-1) = (-1)^{\frac{2}{2}},$$

$$(-1)^{\frac{p+1}{2}} \equiv \left[ \left( \frac{p-1}{2} \right)! \right]^2 \pmod{p}$$

Now, if  $p$  is of the form  $4k+3$ , then

$$(-1)^{\frac{4k+4}{2}} = (-1)^{2k+2} = 1 \equiv \left[ \left( \frac{p-1}{2} \right)! \right]^2 \pmod{p}$$

$\therefore$  From above,  $\left( \frac{p-1}{2} \right)! \equiv 1 \pmod{p}$ , or

$$\left( \frac{p-1}{2} \right)! \equiv -1 \pmod{p}$$

(6) If  $p = 4k+3$  is prime, Then the product of all the even integers  $< p$  is congruent mod  $p$  to either 1 or -1.

Pf: Let  $2, 4, 6, \dots, a$  be all even integers  $< p$

$$\therefore a = p-1.$$

Consider  $2 \cdot 4 \cdot 6 \cdots a = 2^k (1 \cdot 2 \cdot 3 \cdots \frac{p-1}{2})$ ,

where  $k = \#$  of terms in  $2, 4, 6, \dots, a$

Since  $a/2 = (p-1)/2$ , Then  $k = (p-1)/2$

$$\therefore 2 \cdot 4 \cdot 6 \cdots a = 2^{\frac{p-1}{2}} (1 \cdot 2 \cdot 3 \cdots (\frac{p-1}{2}))$$

$$= 2^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)!$$

[1]

By Fermat's Th.,  $2^{p-1} \equiv 1 \pmod{p}$ , since  $p \nmid 2$  as  $p$  is an odd prime.

$$\therefore 2^{p-1} = \left(2^{\frac{p-1}{2}}\right)^2 \equiv 1 \pmod{p}, \text{ so}$$

$$2^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$$

Multiplying both sides by  $\left(\frac{p-1}{2}\right)!$ ,

$$2^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! \equiv 1 \pmod{p} \text{ or } 2^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! \equiv -1 \pmod{p}$$

$\therefore$  From [1] above,

$$2 \cdot 4 \cdot 6 \cdots a \equiv 1 \pmod{p} \text{ or } 2 \cdot 4 \cdot 6 \cdots a \equiv (-1) \pmod{p}$$

Note: above just used  $p$  as an odd prime.  
Could be of  $4k+1$  form as well.

11. Obtain two solutions to  $x^2 \equiv -1 \pmod{29}$  and  
 $x^2 \equiv -1 \pmod{37}$

(a)  $x^2 \equiv -1 \pmod{29}$

As,  $29 \equiv 1 \pmod{4}$ , There is a solution, and  
The proof of Th. 5.5 shows that

$$\left[ \left( \frac{p-1}{2} \right)! \right]^2 \equiv (-1) \pmod{p}. \quad \therefore \pm \left( \frac{29-1}{2} \right)! = \pm 14!$$

$\therefore 14!$  or  $-14!$  is a solution

(1)  $x^2 \equiv -1 \pmod{37}$ . As  $37 \equiv 1 \pmod{4}$ , as in (a),

$$\left( \frac{37-1}{2} \right)! = 18! \quad \therefore 18! \text{ or } -18! \text{ is a solution.}$$

12. Show That if  $p = 4k+3$  is prime and  $a^2 + b^2 \equiv 0 \pmod{p}$ ,  
Then  $a \equiv b \equiv 0 \pmod{p}$

If: Suppose  $a \not\equiv 0 \pmod{p}$ .  $\therefore p \nmid a$

Consider  $ax \equiv 1 \pmod{p}$ . By Th. 4.7, There is a unique solution  $\pmod{p}$ , and so There is a unique integer  $c$  s.t.  $1 \leq c \leq p-1$  and  $ac \equiv 1 \pmod{p}$ .  $\therefore a^2c^2 \equiv 1 \pmod{p}$

From  $a^2 + b^2 \equiv 0 \pmod{p}$ , after multiplying both sides by  $c^2$ , you get

$$a^2c^2 + b^2c^2 \equiv 0 \pmod{p} . \text{ But } a^2c^2 \equiv 1 \pmod{p}$$

$$\therefore 1 + b^2c^2 \equiv 0 \pmod{p}$$

$\therefore x = bc$  is a solution to  $x^2 + 1 \equiv 0 \pmod{p}$ , which, by Th. 5.5, means  $p \equiv 1 \pmod{4}$   
But This contradicts  $p = 4k+3 \Rightarrow p \equiv 3 \pmod{4}$

$$\therefore a \equiv 0 \pmod{p}$$

The exact same reasoning applies to  $b$ , so that  $b \equiv 0 \pmod{p}$ .

13. Supply details in the proof that  $\sqrt{2}$  is irrational.

Pf: Suppose  $\sqrt{2} = a/b$ ,  $\gcd(a,b) = 1$

$$\text{Then } a^2 = 2b^2$$

$$\therefore a^2 + b^2 = 3b^2, \text{ and } \therefore 3 \mid (a^2 + b^2), \text{ or}$$
$$a^2 + b^2 \equiv 0 \pmod{3}$$

$\therefore$  From problem #12 above, since 3 is a prime of form  $p = 4k+3$ , then

$$a \equiv b \equiv 0 \pmod{3}$$

$\therefore 3 \mid a$  and  $3 \mid b$ , contradicting  $\gcd(a,b) = 1$ .

14. Prove the odd prime divisors of  $n^2 + 1$  are of the form  $4k+1$ .

Pf: Let  $p$  be an odd prime divisor of  $n^2 + 1$

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

$\therefore n$  is a solution to  $x^2 + 1 \equiv 0 \pmod{p}$ , and by Th. 5.5,  $p$  is of form  $4k+1$

15. Verify  $4(29!) + 5!$  is divisible by 31.

By Wilson's Th.,  $30! \equiv -1 \pmod{31}$

$$\therefore 30 \cdot 29! \equiv 31 - 1 = 30 \pmod{31}$$

$$\therefore 29! \equiv 1 \pmod{31} \text{ as } \gcd(30, 31) = 1$$

$$\therefore 4(29!) \equiv 4 \pmod{31}$$

$$5! = 120 \quad \therefore 4(29!) + 5! \equiv 4 + 120 = 124 \pmod{31}$$

But  $124 = 4 \cdot 31$

$$\therefore 4(29!) + 5! \equiv 0 \pmod{31}$$

$$\Rightarrow 31 \mid (4(29!) + 5!)$$

16. For a prime  $p$  and  $0 \leq k \leq p-1$ , show that

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

$$\begin{aligned} \text{PF: } (p-1)! &= 1 \cdot 2 \cdot 3 \cdots (p-k-1)(p-k) \cdots (p-2)(p-1) \\ &= (p-k-1)! (p-k) \cdots (p-2)(p-1) \end{aligned}$$

$$\begin{aligned} \text{But } p-1 &\equiv -1 \pmod{p} \\ p-2 &\equiv -2 \pmod{p} \\ &\vdots \\ p-k &\equiv -k \pmod{p} \end{aligned}$$

$$\therefore (p-k) \cdots (p-2)(p-1) \equiv (-k) \cdots (-2)(-1) \pmod{p}$$

$$\text{But } (-k) \cdots (-2)(-1) = (-1)^k k!$$

$$\therefore (\rho-k)\cdots(\rho-2)(\rho-1) \equiv (-1)^k k! \pmod{\rho}$$

$$\therefore (\rho-k-1)! (\rho-k)\cdots(\rho-2)(\rho-1) \equiv (-1)^k k! (\rho-k-1)! \pmod{\rho}$$

$$\therefore (\rho-1)! \equiv (-1)^k k! (\rho-k-1)! \pmod{\rho}$$

By Wilson's Th.,  $(\rho-1)! \equiv -1 \pmod{\rho}$

$$\therefore (-1) \equiv (-1)^k k! (\rho-k-1)! \pmod{\rho} \quad [1]$$

Since  $(-1)^k \cdot (-1)^k = 1$ , and  $(-1)(-1)^k = (-1)^{k+1}$ ,  
after multiplying both sides of [1] by  $(-1)^k$ ,  
you get  $(-1)^{k+1} \equiv k! (\rho-k-1)! \pmod{\rho}$

17. If  $p, q$  are distinct primes, prove for any integer  $a$ ,

$$pq \mid a^{pq} - a^p - a^q + a$$

Pf: Consider  $(a^p)^q - a^p$ . By the corollary to  
Fermat's Th.,  $x^q \equiv x \pmod{q}$ , so letting  $x = a^p$ ,  
 $q \mid (a^p)^q - a^p$ . Also  $a^q \equiv a \pmod{q}$ .  $\therefore q \mid a^q - a$ .

$$\therefore q \mid [(a^p)^q - a^p] - (a^q - a) = a^{pq} - a^p - a^q + a$$

Similarly,  $p \mid (a^q)^p - a^q$  and  $p \mid a^p - a$

$$\therefore p \mid [(a^q)^p - a^q] - (a^p - a) = a^{pq} - a^p - a^q + a$$

$\therefore$  Both  $p$  and  $q$  divide  $a^{pq} - a^p - a^q + a$ , and  
so by corollary 2, sec. 2-2,

$$pq \mid a^{pq} - a^p - a^q + a$$

18. Prove if  $p$  and  $p+2$  are twin primes, Then

$$4((p-1)! + 1) + p \equiv 0 \pmod{p(p+2)}$$

Pf:  $(p-1)! \equiv -1 \pmod{p}$  Wilson's Th.

$$\therefore (p-1)! + 1 \equiv 0 \pmod{p}$$

$$\therefore 4[(p-1)! + 1] \equiv 0 \pmod{p}$$

$$\therefore 4[(p-1)! + 1] + p \equiv 0 \pmod{p} \quad [1]$$

Also,  $(p+2-1)! = (p+1)! \equiv -1 \pmod{(p+2)}$  Wilson's Th.

$$\therefore (p+1)p! \equiv -1 + p+2 = p+1 \pmod{(p+2)}$$

$$\therefore p! \equiv 1 \pmod{p+2} \text{ as } \gcd(p+1, p+2) = 1$$

$$\therefore 4p! \equiv 4 = 4 + 2p - 2p \equiv 2(p+2) - 2p \pmod{p+2}$$

$$\therefore 4p(p-1)! \equiv -2p \pmod{p+2}$$

$$\therefore 4(p-1)! \equiv -2 \pmod{p+2} \quad \gcd(p, p+2) = 1$$

$$\therefore 4(p-1)! + p+2 \equiv -2 \pmod{p+2}$$

$$\therefore 4(p-1)! + p+4 \equiv 0 \pmod{p+2}$$

$$\therefore 4[(p-1)! + 1] + p \equiv 0 \pmod{p+2} \quad [2]$$

$\therefore p$  and  $p+2$  divide  $4[(p-1)! + 1] + p$  by  $[1], [2]$

$\therefore p(p+2)$  divides  $4[(p-1)! + 1] + p$  by corollary 2,  
section 2.2.

$$\therefore 4[(p-1)! + 1] + p \equiv 0 \pmod{p(p+2)}$$

## 6.1 The Functions tau and sigma

Note Title

6/3/2005

1. Let  $m, n$  be positive integers, and  $p_1, p_2, \dots, p_r$  be the distinct primes that divide at least one of  $m$  or  $n$ .  
Let  $m = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$ ,  $k_i \geq 0$  for  $i = 1, 2, 3, \dots, r$

$$n = p_1^{j_1} p_2^{j_2} \dots p_r^{j_r}, j_i \geq 0 \text{ for } i = 1, 2, 3, \dots, r$$

Prove  $\gcd(m, n) = p_1^{u_1} p_2^{u_2} \dots p_r^{u_r}$ ,  $\text{lcm}(m, n) = p_1^{v_1} \dots p_r^{v_r}$

where  $u_i = \min\{k_i, j_i\}$ ,  $v_i = \max\{k_i, j_i\}$

Pf: (a) Consider the integer  $a = p_1^{u_1} p_2^{u_2} \dots p_r^{u_r}$

(1)  $u_i = \min\{k_i, j_i\} \Rightarrow 0 \leq u_i \leq k_i \therefore \text{By Th. G.I., } a \mid m$

$$u_i = \min\{k_i, j_i\} \Rightarrow 0 \leq u_i \leq j_i \therefore \text{By Th. G.I., } a \mid n$$

(2) Let  $d$  be any other divisor of  $m$  and  $n$

By Th. G.I.,  $d = p_1^{s_1} p_2^{s_2} \dots p_r^{s_r}$ , where

$$0 \leq s_i \leq k_i \text{ since } d \mid m \text{ and}$$

$$0 \leq s_i \leq j_i \text{ since } d \mid n.$$

If  $k_i = j_i$ , then by def of  $u_i$ ,  $u_i = k_i = j_i$

$$\therefore s_i \leq u_i$$

If  $k_i < j_i$ , Then  $v_i = k_i$ .  $s_i \leq k_i \Rightarrow s_i \leq v_i$

If  $j_i < k_i$ , Then  $v_i = j_i$ .  $s_i \leq j_i \Rightarrow s_i \leq v_i$

$\therefore s_i \leq v_i$  so that  $a | a$ .

$\therefore a = \gcd(m, n)$  by (1) + (2)

(6) Let  $a = p_1^{v_1} p_2^{v_2} \dots p_r^{v_r}$ .

(1)  $v_i = \max\{k_i, j_i\} \Rightarrow k_i \leq v_i$  and  $j_i \leq v_i$

$\therefore p_i^{k_i} | p_i^{v_i}$  and  $p_i^{j_i} | p_i^{v_i}$

$\therefore m | a$  and  $n | a$ , so  $a$  is a multiple of  $m$  and  $n$ .

(2) Suppose  $m | b$  and  $n | b$  ( $b$  any other multiple)

$\therefore m | b \Rightarrow p_i^{k_i} | b$   $n | b \Rightarrow p_i^{j_i} | b$

If  $k_i = j_i$ , Then  $v_i = \max\{k_i, j_i\} \Rightarrow v_i = k_i = j_i$

$\therefore p_i^{v_i} | b$ , and  $\therefore$  by corollary 2, Sec. 2.2,  
 $p_1^{v_1} p_2^{v_2} \dots p_r^{v_r} | b$ , so  $a | b$

If  $k_i < j_i$ , Then  $v_i = \max\{k_i, j_i\} \Rightarrow r_i = j_i$

$$\therefore p_i^{j_i} | b \Rightarrow p_i^{v_i} | b, \text{ so } p_1^{r_1} p_2^{r_2} \dots p_r^{r_r} | b$$

By corollary 2, Sec. 2.2.  $\therefore a | b$

If  $j_i < k_i$ , Then  $v_i = \max\{k_i, j_i\} \Rightarrow v_i = k_i$

$$\therefore p_i^{k_i} | b \Rightarrow p_i^{v_i} | b, \text{ so } p_1^{r_1} p_2^{r_2} \dots p_r^{r_r} | b$$

By corollary 2, Sec. 2.2.  $\therefore a | b$

$\therefore$  By (1) + (2),  $a = \text{lcm}(m, n)$

2. Calculate  $\gcd(12378, 3054)$  and  $\text{lcm}(12378, 3054)$

$$12378 = 2 \cdot 6189 = 2 \cdot 3 \cdot 2063, \text{ and } 2063 \text{ is prime.}$$

$$3054 = 2 \cdot 1527 = 2 \cdot 3 \cdot 509, \text{ and } 509 \text{ is prime.}$$

$$\therefore \gcd(12378, 3054) = 2 \cdot 3 = 6$$

$$\text{lcm}(12378, 3054) = 2 \cdot 3 \cdot 509 \cdot 2063 = 6300402$$

3. Use Problem 1 to show that  $\gcd(m, n) \cdot \text{lcm}(m, n) = mn$

$$\text{Pf: } mn = p_1^{k_1+j_1} p_2^{k_2+j_2} \dots p_r^{k_r+j_r}$$

$\therefore$  For any  $i$ , need to show  $k_i + j_i = u_i + v_i$ ,

where  $u_i = \min\{k_i, j_i\}$ ,  $v_i = \max\{k_i, j_i\}$

(1) If  $k_i = j_i$ , Then  $u_i = k_i = j_i$ ,  $v_i = k_i = j_i$

$$\therefore k_i + j_i = u_i + v_i$$

(2) If  $k_i > j_i$ , Then  $u_i = j_i$ ,  $v_i = k_i$

$$\therefore k_i + j_i = v_i + u_i$$

(3) If  $k_i < j_i$ , Then  $u_i = k_i$ ,  $v_i = j_i$

$$\therefore k_i + j_i = u_i + v_i$$

$$\therefore (1), (2), (3) \Rightarrow mn = \gcd(m, n) \mid \text{lcm}(m, n)$$

4. Using notation of Problem 1, show  $\gcd(m, n) = 1 \iff k_i j_i = 0$  for  $i = 1, 2, \dots, r$

Pf:  $\gcd(m, n) = p_1^{u_1} p_2^{u_2} \dots p_r^{u_r}$ , where  $u_i = \min\{k_i, j_i\}$

(1) If  $\gcd(m, n) = 1$ , Then  $u_1 = 0, u_2 = 0, \dots, u_r = 0$ , so  $u_i = 0$  for  $i = 1, 2, \dots, r$

$\therefore 0 = \min\{k_i, j_i\}$ , so one of  $k_i$  or  $j_i$  must be 0, so  $k_i j_i = 0$ .

(2) If  $k_i j_i = 0$  for  $i = 1, 2, \dots, r$ , then

either  $k_i = 0$  or  $j_i = 0$ .  $\therefore \min\{k_i, j_i\} = 0$

$\therefore u_i = 0$  for  $i = 1, 2, \dots, r$

$$\therefore p_1^{u_1} p_2^{u_2} \cdots p_r^{u_r} = 1 = \gcd(m, n)$$

5. (a). Verify  $\tilde{T}(n) = \tilde{T}(n+1) = \tilde{T}(n+2) = \tilde{T}(n+3)$  for  
 $n = 3655$  and  $n = 4503$

$$3655 = 5 \cdot 7 \cdot 43 \quad \therefore \tilde{T}(n) = 2 \cdot 2 \cdot 2 = 8$$

$$3656 = 2^3 \cdot 457 \quad \therefore \tilde{T}(n+1) = 4 \cdot 2 = 8$$

$$3657 = 3 \cdot 23 \cdot 53 \quad \therefore \tilde{T}(n+2) = 2 \cdot 2 \cdot 2 = 8$$

$$3658 = 2 \cdot 31 \cdot 59 \quad \therefore \tilde{T}(n+3) = 2 \cdot 2 \cdot 2 = 8$$

$$4503 = 3 \cdot 19 \cdot 79 \quad \therefore \tilde{T}(n) = 2 \cdot 2 \cdot 2 = 8$$

$$4504 = 2^3 \cdot 563 \quad \therefore \tilde{T}(n+1) = 4 \cdot 2 = 8$$

$$4505 = 5 \cdot 17 \cdot 63 \quad \therefore \tilde{T}(n+2) = 2 \cdot 2 \cdot 2 = 8$$

$$4506 = 2 \cdot 3 \cdot 751 \quad \therefore \tilde{T}(n+3) = 2 \cdot 2 \cdot 2 = 8$$

(b) Show  $\sigma(n) = T(n+1)$  when  $n = 14, 206$ , or  $957$

$$\sigma(14) = \sigma(2 \cdot 7) = \sigma(2) \sigma(7) = 3 \cdot 8 = 24$$

$$\sigma(15) = \sigma(3 \cdot 5) = \sigma(3) \cdot \sigma(5) = 4 \cdot 6 = 24$$

$$\sigma(206) = \sigma(2 \cdot 103) = \sigma(2) \sigma(103) = 3 \cdot 104 = 312$$

$$\sigma(207) = \sigma(9 \cdot 23) = \sigma(3^2) \sigma(23) = \frac{27-1}{2} \cdot 24 = 312$$

$$\sigma(957) = \sigma(3 \cdot 11 \cdot 29) = \sigma(3) \sigma(11) \sigma(29) = 4 \cdot 12 \cdot 30 = 1440$$

$$\sigma(958) = \sigma(2 \cdot 479) = \sigma(2) \sigma(479) = 3 \cdot 480 = 1440$$

1. For any  $n \geq 1$ , show  $\tau(n) \leq 2\sqrt{n}$

Pf: Note if  $d|n$ , Then either  $d \leq \sqrt{n}$  or  $n/d \leq \sqrt{n}$   
 For if both  $d > \sqrt{n}$  and  $n/d > \sqrt{n}$ , Then  
 $d \cdot \frac{n}{d} = n > \sqrt{n} \cdot \sqrt{n} = n$ , a contradiction.

Let  $d_1, d_2, \dots, d_k$  be the divisors of  $n$ ,

where  $d_1 < d_2 < \dots < d_k$ . Clearly,  $d_1 = 1, d_k = n$ .

Since whenever  $d_i$  is a divisor of  $n$ , so is  $n/d_i$ , and so  $n/d_i$  must be one of the  $d_i$ .

Pair up the divisors so that  $d_i d_j = n$ , where  $d_j = n/d_i$ . Either  $d_i \leq d_j$  or  $d_j \leq d_i$  for each.

(1) If  $K$  is even, we have  $\frac{K}{2}$  unique pairs  $(d_i, d_j)$   $\{d_i, d_j\}$  s.t.  $d_i d_j = n$ . For each pair, arrange

them so that  $d_i < d_j$

Let  $d_{k'}$  be the largest of the  $d_i$

It must be that  $\frac{K}{2} \leq d_{k'}$  since there are  $\frac{K}{2}$  unique pairs.

But  $T(n) = k$ , and from above,  $d_{k'} \leq \sqrt{n}$

$$\therefore \frac{T(n)}{2} \leq \sqrt{n}, \text{ so } T(n) \leq 2\sqrt{n}$$

(2) If  $K$  is odd, we have  $\frac{K-1}{2}$  unique pairs  $\{d_i, d_j\}$  s.t.  $d_i d_j = n$  and one pair  $\{d_r, d_r\}$  where  $d_r \cdot d_r = n$ .

For the unique  $\frac{K-1}{2}$  unique pairs, arrange them so that  $d_i < d_j$ .

Let  $d_{k'}$  be the largest of the  $d_i$ .

$$\therefore d_{k'} < d_r, \text{ for if } d_r < d_{k'}, \text{ let } d_j \text{ be}$$

The associated pair with  $d_{k'}$ . By def. of  $d_{k'}$ ,  $d_{k'} < d_j$  and  $d_{k'} d_j = n$

$\therefore d_r < d_{k'}$  and  $d_r < d_j$ , so  $d_r \cdot d_r < d_{k'} \cdot d_j$ ,  
or  $n < n$ .  $\therefore d_{k'} < d_r$

But  $d_r^2 = n$ , so  $d_r = \sqrt{n}$

As in (1),  $\frac{k-1}{2} \leq d_{k'}$  and  $k = \tau(n)$

$\therefore \frac{\tau(n)-1}{2} \leq d_{k'} < d_r = \sqrt{n}$

$\therefore \frac{\tau(n)-1}{2} < \sqrt{n}$ ,  $\tau(n)-1 < 2\sqrt{n}$ , so

$\tau(n) \leq 2\sqrt{n}$ .

$\therefore$  where  $\tau(n)$  is even or odd,  $\underline{\tau(n) \leq 2\sqrt{n}}$

7. (a) Prove  $\tau(n)$  is odd  $\Leftrightarrow n$  is a perfect square.

(1) Let  $n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$

Suppose  $\tau(n)$  is odd. Since, by Th. 6.2,

$$\tau(n) = (k_1+1)(k_2+1)\cdots(k_r+1), \text{ Then each}$$

$(k_i+1)$  must be odd, so  $k_i$  is even,

$$\therefore k_i = 2j_i, \text{ so}$$

$$n = p_1^{2j_1} p_2^{2j_2} \cdots p_r^{2j_r} = (p_1^{j_1} p_2^{j_2} \cdots p_r^{j_r})^2,$$

so  $n$  is a perfect square.

(2) Suppose  $n$  is a perfect square.

$$\therefore n = a^2, \text{ some } a = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$$

$$\therefore n = p_1^{2k_1} p_2^{2k_2} \cdots p_r^{2k_r}$$

$$\therefore \text{By Th. 6.2, } \tau(n) = (2k_1+1)(2k_2+1)\cdots(2k_r+1)$$

Since each  $2k_i+1$  is odd,  $\tau(n)$  is odd.

(3).  $\tau(n)$  is odd  $\Leftrightarrow n$  is a perfect square or twice a perfect square.

(1) Suppose  $\sigma(n)$  is odd.

Let  $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ . As discussed in

The proof to Th. 6.2,

$$\sigma(n) = (1 + p_1 + p_1^2 + \cdots + p_1^{k_1}) \cdots (1 + p_r + p_r^2 + \cdots + p_r^{k_r})$$

$\therefore$  Each term  $(1 + p_i + p_i^2 + \cdots + p_i^{k_i})$  must be odd.

If  $p_i = 2$ , Then each  $p_i^n$  is even, so  $1 + 2 + 2^2 + \cdots + 2^n$  is odd.

$\therefore$  consider  $p_i$  to be odd.  $\therefore p_i^n$  is odd.

If  $k_i$  is odd, Then you have an odd number of terms:  $p_i + p_i^2 + \cdots + p_i^{k_i}$ ,

which must be odd.  $\therefore 1 + p_i + \cdots + p_i^{k_i}$  must be even.

$\therefore k_i$  must be even for  $1 + p_i + \cdots + p_i^{k_i}$  to be odd.

$$\therefore p_i^{k_i} = p_i^{2j_i} = (p_i^{j_i})^2$$

$\therefore$  If 2 is a factor of  $n$ ,

$$n = 2^k (p_1^{j_1} p_2^{j_2} \cdots p_r^{j_r})^2, k=1, 2, \dots$$

$$= 2^k a^2, k=1, 2, \dots a = p_1^{j_1} \cdots p_r^{j_r}$$

For  $k$  even,  $k=2s$ , so  $n = (2^s a)^2$ , so

$n$  is a perfect square.

For  $k$  odd,  $k=2s+1$ , so  $n = 2^{2s+1} a^2$ .

$2 \cdot 2^{2s} a^2 = 2 (2^s a)^2$ , so  $n$  is twice a perfect square.

If 2 is not a factor of  $n$ , Then

$$n = (p_1^{j_1} p_2^{j_2} \cdots p_r^{j_r})^2, \text{ so } n \text{ is a}$$

perfect square.

(2) Suppose  $n$  is a perfect square or twice a perfect square.

(a) Let  $n = a^2$ , let  $a = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ .

$\therefore n = p_1^{2k_1} \cdots p_r^{2k_r}$ . As in the proof to

$$\text{Th. 6.2, } \sigma(n) = (1+p_1+\dots+p_1^{2k_1}) \cdots (1+p_r+\dots+p_r^{2k_r})$$

If  $p_1 = 2$ , Then  $(1+p_1+p_1^{2k_1})$  is odd.

If  $p_i$  is odd,  $p_i^n$  is odd. There are an even number of terms in  $p_1 + \dots + p_1^{2k_1}$ ,

which means the sum is even (odd times even is even).  $\therefore 1+p_1+\dots+p_1^{2k_1}$  is odd.

$\therefore \sigma(n)$  is odd

(b) suppose  $n = 2a^2$

$$\text{Let } a = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}. \therefore n = 2(p_1^{k_1} \cdots p_r^{k_r})^2 =$$

$$2 p_1^{2k_1} \cdots p_r^{2k_r}, p_1 < p_2 < \cdots < p_r \text{ (canonical form).}$$

If  $p_1 = 2$ , Then  $n = 2^k p_2^{2k_2} \cdots p_r^{2k_r}$ , and all of  $2, p_i$  are relatively prime.

$$\therefore \sigma(n) = \frac{2^{k+1}-1}{2-1} \cdot \sigma(p_2^{2k_2}) \cdots \sigma(p_r^{2k_r})$$

$$\text{But } \sigma(p_i^{2k_i}) = 1 + p_i + p_i^2 + \cdots + p_i^{2k_i}. \text{ As}$$

$p_i^s$  is odd for any  $s$  ( $p_i$  is odd),

$\therefore p_i + p_i^2 + \dots + p_i^{2k_i}$  is even as

There are an even # of terms.

$\therefore \sigma(p_i^{2k_i}) = 1 + p_i + \dots + p_i^{2k_i}$  is odd.

$2^{k+1} - 1$  is odd, so  $\sigma(n)$  is odd.

If  $p_i \neq 2$ , Then  $n = 2^{k_1} p_1^{2k_1} \dots p_r^{2k_r}$ .

As all  $2, p_i$  are relatively prime,

$$\sigma(n) = \sigma(2) \sigma(p_1^{2k_1}) \dots \sigma(p_r^{2k_r})$$

But  $\sigma(2) = 1 + 2 = 3$ .

As in (a) above,  $\sigma(p_i^{2k_i})$  is odd.

$\therefore \sigma(n)$  is odd.

8. Show That  $\sum_{d|n} \frac{1}{d} = \sigma(n)/n$  for all  $n > 0$

Pf: Note that  $d$  is a divisor of  $n \Leftrightarrow \frac{n}{d}$  is a

divisor of  $n$ , since  $d \cdot \frac{n}{d} = n$ .

$\therefore$  The set of divisors of  $n = \{d_1, \dots, d_k\}$

Can also be written as  $\left\{ \frac{n}{d_1}, \dots, \frac{n}{d_k} \right\}$

$$\begin{aligned}\therefore \sigma(n) &= d_1 + d_2 + \dots + d_k = \frac{n}{d_1} + \frac{n}{d_2} + \dots + \frac{n}{d_k} \\ &= n \left( \frac{1}{d_1} + \frac{1}{d_2} + \dots + \frac{1}{d_k} \right)\end{aligned}$$

$$\therefore \frac{\sigma(n)}{n} = \frac{1}{d_1} + \frac{1}{d_2} + \dots + \frac{1}{d_k} = \sum_{d|n} \frac{1}{d}$$

9. If  $n$  is a square free integer, prove  $\tilde{\tau}(n) = 2^r$ , where  $r$  is the number of prime divisors of  $n$ .

Pf:  $n$  square-free  $\Rightarrow n = p_1 p_2 \dots p_r$ , where each  $p_i$  is distinct and of exponent power 1 (see problem 16(a), section 3.1).

$\therefore$  By Th. 6.2,  $\tau(n) = (k_1 + 1) \dots (k_r + 1)$ , and here, each  $k_i = 1$ .  
 $\therefore \tilde{\tau}(n) = (1+1) \dots (1+1) = (2) \dots (2)$ . As there are  $r$  terms,  $\tilde{\tau}(n) = 2^r$

10. Establish the assertions below:

(a) If  $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$  for  $n > 1$ , Then

$$1 > \frac{n}{\sigma(n)} > \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_r}\right)$$

Since the divisors of  $n$  include 1 and  $n$ ,  
 $\sigma(n) \geq n + 1 > n$ , so  $\sigma(n) > n$ ,  $\therefore$ .

$$1 > \frac{n}{\sigma(n)}$$

$$\text{By Th. 6.2, } \sigma(n) = \frac{p_1^{k_1+1}-1}{p_1-1} \cdots \frac{p_r^{k_r+1}-1}{p_r-1}$$

$$\therefore \frac{n}{\sigma(n)} = \frac{p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}}{\frac{(p_1^{k_1+1}-1) \cdots (p_r^{k_r+1}-1)}{(p_1-1) \cdots (p_r-1)}}$$

$$= \frac{p_1^{k_1} \cdots p_r^{k_r} (p_1-1) \cdots (p_r-1)}{(p_1^{k_1+1}-1) \cdots (p_r^{k_r+1}-1)}$$

$$\begin{aligned}
 &= \frac{(p_1 - 1) \cdots (p_r - 1)}{\frac{(p_1^{k_1+1} - 1) \cdots (p_r^{k_r+1} - 1)}{p_1^{k_1} \cdots p_r^{k_r}}} \\
 &= \frac{(p_1 - 1) \cdots (p_r - 1)}{\left(p_1 - \frac{1}{p_1^{k_1}}\right) \cdots \left(p_r - \frac{1}{p_r^{k_r}}\right)} \quad [1]
 \end{aligned}$$

$$\text{But } p_i > p_i - \frac{1}{p_i^{k_i}}, \therefore \frac{1}{p_i - \frac{1}{p_i^{k_i}}} > \frac{1}{p_i}$$

$$\begin{aligned}
 \therefore \text{From } \Sigma 3, \frac{n}{C(n)} &= \frac{(p_1 - 1) \cdots (p_r - 1)}{\left(p_1 - \frac{1}{p_1^{k_1}}\right) \cdots \left(p_r - \frac{1}{p_r^{k_r}}\right)} > \frac{(p_1 - 1) \cdots (p_r - 1)}{p_1 \cdots p_r} \\
 &= \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_r}\right)
 \end{aligned}$$

$$\therefore 1 > \frac{n}{C(n)} > \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_r}\right)$$

(6) For any positive integer  $n$ ,

$$\frac{\sigma(n!)}{n!} \geq 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}$$

Clearly, all  $1, 2, 3, 4, \dots, n$  are divisors for  $n!$ .  
 There are more divisors of  $n!$  (including  $n!$ )  
 since  $n! > n$  for  $n \geq 3$ , and  $n! = n$  for  $n=2$ .

$$\text{From prob. 8, } \frac{\sigma(n!)}{n!} = \sum_{d|n!} \frac{1}{d} = \frac{1}{1} + \frac{1}{2} + \dots + \frac{1}{n} + \dots + \frac{1}{n!} \\ \geq 1 + \frac{1}{2} + \dots + \frac{1}{n}$$

(C) If  $n > 1$  is a composite number, then  
 $\sigma(n) > n + \sqrt{n}$

Since  $\sigma(n) = 1 + d_1 + \dots + d_K + n$ , it suffices to show  $1 + d_1 + \dots + d_K > \sqrt{n}$

Since  $n$  is composite, there is a  $d_i$  s.t.  
 $1 < d_i < n$  and  $d_i | n$ .  $\therefore \frac{n}{d_i} | n$ , and

$$d_i < n \Rightarrow 1 < \frac{n}{d_i}, \text{ and } 1 < d_i \Rightarrow \frac{1}{d_i} < 1 \Rightarrow \\ \frac{n}{d_i} < n. \therefore 1 < \frac{n}{d_i} < n \quad [1]$$

(i) If  $d_i > \sqrt{n}$ , then clearly  $1 + d_i > \sqrt{n}$ , so

$$\sigma(n) = 1 + d_1 + \dots + n > n + \sqrt{n}$$

(b) Suppose  $d_i \leq \sqrt{n}$ .  $\therefore \frac{1}{\sqrt{n}} \leq \frac{1}{d_i} \Rightarrow$

$\sqrt{n} = \frac{n}{d_i} \leq \frac{n}{1}$ . Let  $d_j = \frac{n}{d_i}$ , and

$d_j$  is a divisor of  $n$  and  $\therefore d_j \geq \sqrt{n}$

$$\therefore 1 + d_j + n > n + \sqrt{n}$$

$\therefore$  From  $\sigma(n) = 1 + d_1 + d_2 + \dots + n$ ,

$$\sigma(n) > n + \sqrt{n}$$

$\therefore$  From (a)+(b),  $\sigma(n) > n + \sqrt{n}$

11. Given integer  $K \geq 1$ , show there are infinitely many integers  $n$  for which  $T(n) = K$ , but at most finitely many  $n$  with  $\sigma(n) = K$ .

(a) Let  $p$  be any prime, let  $n = p^{K-1}$

$\therefore T(n) = K$  by Th. 6.2. Since there are infinitely many primes, there are infinitely many  $n$  s.t.  $n = p^{K-1}$  and  $T(n) = K$ .

(6) By problem 10(a),  $1 > \frac{n}{\sigma(n)}$  for any  $n$ .

$$\therefore \sigma(n) > n$$

$\therefore$  Given any  $k$ , if  $\sigma(n)$  is to equal  $k$ ,  
then  $k$  serves as an upper bound to  $n$ .

In fact, for any  $n \geq k$ ,  $\sigma(n) > k$  by  
problem 10(a).  $\therefore$  There are at most  $k$   
positive integers s.t.  $\sigma(n) \leq k$ .

12. (a). Find the form of all positive integers  $n$   
satisfying  $\tau(n) = 10$ . What is the smallest  
positive integer for which this is true?

Since  $\tau(n) = (k_1 + 1)(k_2 + 1) \cdots (k_r + 1)$  if  
 $n = p_1^{k_1} \cdots p_r^{k_r}$ , Then  $10 = (k_1 + 1) \cdots (k_r + 1)$

Possibilities include  $10 = 10$  or  
 $10 = 5 \cdot 2$

$$\therefore (k_1 + 1) = 10 \text{ or } (k_1 + 1)(k_2 + 1) = 5 \cdot 2$$

$$\therefore n = p_1^9 \text{ or } n = p_1^4 p_2^4, p_1, p_2 \text{ distinct primes.}$$

The smallest such integer would be  
 $2^9$  or  $2^4 \cdot 3$  or  $3^4 \cdot 2$ . Of the three,  
 The smallest is  $\underline{\underline{2^4 \cdot 3 = 48}}$

(b) Show There are no positive integers  $n$  satisfying  $\sigma(n) = 10!$

From proof of problem 11, The only possible integers under consideration would be  
 $1, 2, 3, \dots, 9$ .  $\sigma(1) = 1$ . For  $2, 3, 5, 7$ ,  $\sigma(n) = 2$

$$\sigma(4) = 7 \quad (1+2+4)$$

$$\sigma(6) = 12 \quad (1+2+3+6)$$

$$\sigma(8) = 15 \quad (1+2+4+8)$$

$$\sigma(9) = 13 \quad (1+3+9)$$

$\therefore$  No positive integers  $n$  s.t.  $\sigma(n) > 10$

13. Prove There are infinitely many pairs of integers  $m, n$  s.t.  $\sigma(m^2) = \sigma(n^2)$

Pf: There are infinitely many  $K$  s.t.  $\gcd(K, 10) = 1$   
 Consider  $m = 5K$ ,  $n = 4K$ .  $\therefore$  There are infinitely many such  $m, n$ . Let  $K = p$ , a prime s.t.  $p \neq 2$  or  $5$ .

$$m^2 = 5^2 p^2 \text{ and } n^2 = 4^2 p^2 = 2^4 p^2$$

$\therefore$  By Th. G.2,

$$\sigma(m^2) = \frac{5^3 - 1}{5-1} \cdot \frac{p^3 - 1}{p-1} = \frac{124}{4} \cdot \frac{p^3 - 1}{p-1} = 31 \left( \frac{p^3 - 1}{p-1} \right)$$

$$\sigma(n^2) = \frac{2^5 - 1}{2-1} \cdot \frac{p^3 - 1}{p-1} = 31 \left( \frac{p^3 - 1}{p-1} \right)$$

$\therefore$  There are infinitely many  $m, n$ , s.t.

$$\sigma(m^2) = \sigma(n^2)$$

14. For  $k \geq 2$ , show each of the following:

(a)  $n = 2^{k-1}$  satisfies  $\sigma(n) = 2n - 1$

$$\text{By Th. G.2, } \sigma(n) = \frac{2^{k-1+1} - 1}{2-1} = 2^k - 1$$

$$\text{But } 2n - 1 = 2(2^{k-1}) - 1 = 2^k - 1. \therefore \sigma(n) = 2n - 1$$

(b) If  $2^k - 1$  is prime, Then  $n = 2^{k-1}(2^k - 1)$  satisfies  $\sigma(n) = 2n$

If  $2^k - 1$  is prime, Then  $2^k - 1 \neq 2$  since

$K=2$ .  $\therefore$  Let  $p = 2^k - 1$ .

By Th. 6.2,

$$\sigma(n) = \frac{2^{k-1+1}-1}{2-1} \cdot \frac{p^2-1}{p-1} = (2^{k-1})(p+1)$$
$$= (2^{k-1})(2^k)$$

$$\text{But } 2n = 2(2^{k-1})(2^{k-1}) = 2^k(2^{k-1})$$

$$\therefore \sigma(n) = 2n$$

(c) If  $2^k - 3$  is prime, then  $n = 2^{k-1}(2^k - 3)$   
satisfies  $\sigma(n) = 2n + 2$

Let  $p = 2^k - 3$ . Since  $p$  is prime,  $k \geq 3$ , so  $p \neq 2$ .

$\therefore n = 2^{k-1} \cdot p$ , and by Th. 6.2,

$$\sigma(n) = \frac{2^{k-1+1}-1}{2-1} \cdot \frac{p^2-1}{p-1} = (2^{k-1})(p+1)$$

$$= (2^{k-1})(2^k - 3 + 1) = (2^{k-1})(2^k - 2)$$

$$= 2^{2k} - 3 \cdot 2^k + 2$$

$$\text{But } 2n+2 = 2(2^{k-1})(2^k - 3) + 2$$

$$= 2^k(2^k - 3) + 2 = 2^{2k} - 3 \cdot 2^k + 2$$

$$\therefore \tau(n) = 2n+2$$

15. If  $n$  and  $n+2$  are a pair of twin primes, show that  $\tau(n+2) = \tau(n)+2$ .

Pf: For any prime,  $p$ , the only divisors are 1 and  $p$ .  $\therefore \tau(p) = p+1$

$$\therefore \tau(n+2) = (n+2) + 1 = n+3$$

$$\tau(n) + 2 = (n+1) + 2 = n+3$$

$$\therefore n \text{ and } n+2 \text{ prime} \Rightarrow \tau(n+2) = \tau(n) + 2$$

16. (a) For any integer  $n > 1$ , prove there exists integers  $n_1$  and  $n_2$  s.t.  $\tau(n_1) + \tau(n_2) = n$

Pf: If  $n$  is prime,  $\tau(n) = 2$ . Since  $\tau(1) = 1$ , Then let  $n_1 = n_2 = 1$ .  $\therefore \tau(n_1) + \tau(n_2) = \tau(n)$

If  $n$  is composite, let  $n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$  be the canonical prime factorization.

Since  $n$  is composite, at least one of the  $k_i \geq 2$ . Let  $p_j^{k_j}$  be that factor.

$$\begin{aligned}\therefore T(n) &= (k_1+1)(k_2+1)\cdots(k_j+1)\cdots(k_r+1) \\ &= k_j (k_1+1)(k_2+1)\cdots(k_r+1) \\ &\quad + (k_1+1)(k_2+1)\cdots(k_r+1) \\ &= (k_{j-1}+1)(k_1+1)(k_2+1)\cdots(k_r+1) \\ &\quad + (k_1+1)(k_2+1)\cdots(k_r+1)\end{aligned}$$

$\therefore$  Let  $n_1 = p_1^{k_1} p_2^{k_2} \cdots p_{j-1}^{k_{j-1}} \cdots p_r^{k_r}$  and

$$\text{Let } n_2 = n / p_j^{k_j} = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r} (p_i \neq p_j)$$

$$\begin{aligned}\therefore T(n_1) &= (k_1+1)(k_2+2)\cdots(k_{j-1}+1)\cdots(k_r+1) \\ &= k_j (k_1+1)\cdots(k_r+1)\end{aligned}$$

$$T(n_2) = (k_1+1)(k_2+1)\cdots(k_r+1)$$

$$\therefore T(n) = T(n_1) + T(n_2)$$

(b) Prove the Goldbach conjecture implies that

for each even integer  $2n$ , There exist integers  $n_1$  and  $n_2$  with  $\sigma(n_1) + \sigma(n_2) = 2n$

Pf: Since  $2n$  is even, so is  $2n-2$

Assume  $2n-2 > 4$ . Goldbach conjecture states There exist odd primes,  $p_1$  and  $p_2$ , s.t.  $p_1 + p_2 = 2n-2$

$$\therefore \text{Let } n_1 = p_1, n_2 = p_2$$

$$\begin{aligned} \therefore \sigma(n_1) + \sigma(n_2) &= (p_1+1) + (p_2+1) = p_1 + p_2 + 2 \\ &= 2n-2 + 2 = 2n \end{aligned}$$

17. For a fixed integer  $K$ , show the function  $f$  defined by  $f(n) = n^K$  is multiplicative.

Pf:  $f(mn) = (mn)^K = m^K n^K = f(m) \cdot f(n)$   
 m and n don't even have to be relatively prime.

18. Let  $f, g$  be multiplicative, not identically zero, and s.t.  $f(p^K) = g(p^K)$  for each prime  $p$  and  $K \geq 1$ . Prove  $f = g$

Pf: Let  $n$  be any positive integer  $> 1$

Let  $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$  be the prime factorization

$$\begin{aligned}\therefore f(n) &= f(p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}) = f(p_1^{k_1}) \cdots f(p_r^{k_r}) \\ &= g(p_1^{k_1}) \cdots g(p_r^{k_r}) = g(p_1^{k_1} \cdots p_r^{k_r}) \\ &= g(n)\end{aligned}$$

If  $n=1$ , then  $f(1)=g(1)=1$  by discussion  
on p. 107.

$$\therefore f = g$$

19. Prove if  $f$  and  $g$  are multiplicative functions,  
Then so is  $f \cdot g$  and  $f/g$  (whenever  $f/g$  is defined).

Pf: Let  $m, n$  be integers s.t.  $\gcd(m, n) = 1$ .

$$\begin{aligned}f \cdot g(mn) &= f(mn) \cdot g(mn) \\ &= f(m) \cdot f(n) \cdot g(m) \cdot g(n) \\ &= f(m) \cdot g(m) \cdot f(n) \cdot g(n) \\ &= f \cdot g(m) \cdot f \cdot g(n)\end{aligned}$$

$$\begin{aligned}
 f/g(mn) &= f(mn)/g(mn) \\
 &= f(m) \cdot f(n) / g(m) \cdot g(n) \\
 &= \frac{f(m)}{g(m)} \cdot \frac{f(n)}{g(n)} \\
 &= f/g(m) \cdot f/g(n)
 \end{aligned}$$

20. Let  $w(n)$  denote the number of distinct prime divisors of  $n > 1$ , with  $w(1) = 0$ . For example,  $w(360) = w(2^3 \cdot 3^2 \cdot 5) = 3$ .

(a) Show  $2^{w(n)}$  is a multiplicative function

Let  $m, n$  be integers s.t.  $\gcd(m, n) = 1$ , and

let  $f(n) = 2^{w(n)}$

Let  $n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$  and  $m = q_1^{j_1} q_2^{j_2} \dots q_s^{j_s}$

Since  $\gcd(m, n) = 1$ , then  $p_u \neq q_v$  for  $1 \leq u \leq r$ ,  $1 \leq v \leq s$ .

$\therefore n$  has  $r$  distinct primes,  $m$  has  $s$  distinct primes.

$\therefore nm = p_1^{k_1} \dots p_r^{k_r} q_1^{j_1} \dots q_s^{j_s}$  has  $r+s$  distinct primes (Fund. Th. of Arith. says this is unique).

$\therefore w(n) = r$ ,  $w(m) = s$ , and  $w(nm) = r+s$

$$\therefore f(nm) = 2^{w(nm)} = 2^{w(n)+w(m)} = 2^{w(n)} \cdot 2^{w(m)} \\ = f(n) \cdot f(m)$$

$\therefore 2^{w(n)}$  is multiplicative.

(5) For a positive integer  $n$ , establish

$$F(n^2) = \sum_{d|n} 2^{w(d)}$$

From (a),  $F(n) = \sum_{d|n} 2^{w(d)}$  is multiplicative

$$\therefore \text{Let } n = p_1^{k_1} \cdots p_r^{k_r}$$

$$\therefore F(n) = F(p_1^{k_1} \cdots p_r^{k_r})$$

$$= F(p_1^{k_1}) \cdots F(p_r^{k_r})$$

$$= \sum_{d|p_1^{k_1}} 2^{w(d)} \cdots \sum_{d|p_r^{k_r}} 2^{w(d)}$$

All the divisors of  $p_i^{k_i}$  are  $1, p_i, p_i^2, \dots, p_i^{k_i}$

by Th. G.1. Also,  $w(p_i^{a_i}) = 1$  for  $1 \leq a_i \leq k_i$   
 and  $w(p_i^0) = 0$ .

$$\therefore \sum_{d|p_i^{k_i}} 2^{w(d)} = 2^0 + \underbrace{2^1 + \cdots + 2^1}_{k_i \text{ terms}}$$

$$= (1 + k_i 2^1) = 1 + 2k_i$$

$$\begin{aligned} \therefore F(n) &= \sum_{d|p_1^{k_1}} 2^{w(d)} \cdots \sum_{d|p_r^{k_r}} 2^{w(d)} \\ &= (1 + 2k_1) \cdots (1 + 2k_r) \end{aligned}$$

But  $n^2 = p_1^{2k_1} \cdots p_r^{2k_r}$ , so by Th. G.2

$$\tau(n^2) = (2k_1 + 1) \cdots (2k_r + 1)$$

$$\therefore \tau(n^2) = F(n) = \sum_{d|n} 2^{w(d)}$$

21. For any positive integer  $n$ , prove

$$\sum_{d|n} \tau(d)^3 = \left( \sum_{d|n} \tau(d) \right)^2$$

Pf:  $\tau(n)$  is a multiplicative function

$$\text{Since } [\tau(mn)]^3 = [\tau(m)\tau(n)]^3 \\ = \tau(m)^3 \cdot \tau(n)^3,$$

Then  $\tau(n)^3$  is multiplicative.

$\therefore$  By Th. 6.4.,  $F(n) = \sum_{d|n} \tau(d)^3$  is multiplicative.

Also,  $G(n) = \sum_{d|n} \tau(d)$  is multiplicative,

so  $H(n) = G^2(n)$  is multiplicative, since  
 $H(mn) = G^2(mn) = [G(mn)]^2 = [G(m)G(n)]^2$   
 $= G^2(m) \cdot G^2(n).$

Let  $n = p_1^{k_1} \cdots p_r^{k_r}$ .

If  $F(n) = H(n)$  for  $n = p^k$ , Then since  $F$  and  $H$  are multiplicative, the statement will also be true for  $n = p_1^{k_1} \cdots p_r^{k_r}$ , since

$$F(p_1^{k_1} \cdots p_r^{k_r}) = F(p_1^{k_1}) \cdots F(p_r^{k_r}) = H(p_1^{k_1}) \cdots H(p_r^{k_r}) \\ = H(p_1^{k_1} \cdots p_r^{k_r})$$

$\therefore$  Consider  $n = p^k$ . By Th. 6.1, all the divisors of  $n$  are  $1, p, p^2, \dots, p^k$

$$\begin{aligned}\therefore \sum_{d|p^k} \tau(d)^3 &= \tau(1)^3 + \tau(p)^3 + \tau(p^2)^3 + \dots + \tau(p^k)^3 \\ &= 1 + (1+1)^3 + (2+1)^3 + \dots + (k+1)^3 \\ &= 1 + 2^3 + 3^3 + \dots + (k+1)^3 \\ &= \left[ \frac{(k+1)(k+2)}{2} \right]^2 \text{ by prob. 1.e, Sec. 1.1.}\end{aligned}$$

$$\begin{aligned}\left[ \sum_{d|p^k} \tau(d) \right]^2 &= \left[ \tau(1) + \tau(p) + \dots + \tau(p^k) \right]^2 \\ &= [1 + 2 + \dots + (k+1)]^2 \\ &= \left[ \frac{(k+1)(k+2)}{2} \right]^2 \text{ by prob. 1.g, Sec. 1.1.}\end{aligned}$$

$$\therefore \sum_{d|p^k} \tau(d)^3 = \left[ \sum_{d|p^k} \tau(d) \right]^2, \text{ so } F(n) = H(n) \text{ for } n = p^k$$

22. Given  $n \geq 1$ , let  $\sigma_s(n)$  denote the sum of the  $s$ th powers of the positive divisors of  $n$ ; that is,

$$\sigma_s(n) = \sum_{d|n} d^s$$

Verify the following:

(a)  $\sigma_0 = r$  and  $\sigma_1 = \tau$

(1) since  $d^0 = 1$  for all  $d \geq 1$ ,  $\sigma_0(n) = \sum_{d|n} 1 = \tau(n)$   
by definition.

(2) since  $d^1 = d$  for all  $d \geq 1$ ,  $\sigma_1(n) = \sum_{d|n} d = \tau(n)$   
by definition.

(b)  $\sigma_s$  is a multiplicative function.

Pf: If  $f(n) = n^s$  can be shown to be multiplicative, then by Th. 6-4,

$\sum_{d|n} f(d) = \sum_{d|n} d^s = \sigma_s(n)$  will be multiplicative.

$\therefore$  Consider  $f(n) = n^s$

$$f(mn) = (mn)^s = m^s n^s = f(m) \cdot f(n),$$

so  $f(n) = n^s$  is multiplicative, and  
 $\therefore$  so is  $\sigma_s(n)$ .

(C) If  $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$  is the prime factorization,

$$\text{Then } \sigma_s(n) = \left( \frac{p_1^{s(k_1+1)} - 1}{p_1^s - 1} \right) \cdots \left( \frac{p_r^{s(k_r+1)} - 1}{p_r^s - 1} \right)$$

Pf: By Th. 6.1, all positive divisors of  $n$  are of the form  $p_1^{a_1} \cdots p_r^{a_r}$ ,  $0 \leq a_i \leq k_i$ .

$\therefore$  all the  $s$ th powers of the divisors of  $n$  are of the form  $p_1^{a_1 s} p_2^{a_2 s} \cdots p_r^{a_r s}$ .

$\therefore$  Consider the sum:

$$(1 + p_1^s + p_1^{2s} + \cdots + p_1^{k_1 s}) \cdots (1 + p_r^s + \cdots + p_r^{k_r s})$$

Each positive divisor to the  $s$ th power occurs once and only once as a term in the expansion of the product.

$$\therefore \Gamma_S(n) = (1 + p_1^s + p_1^{2s} + \dots + p_1^{k_1 s}) \cdots (1 + p_r^s + \dots + p_r^{k_r s})$$

Using the formula for the sum of a finite geometric series,

$$1 + p_1^s + p_1^{2s} + \dots + p_1^{k_1 s} = \frac{p_1^{s(k_1+1)} - 1}{p_1^s - 1},$$

$$\therefore \Gamma_S(n) = \left( \frac{p_1^{s(k_1+1)} - 1}{p_1^s - 1} \right) \cdots \left( \frac{p_r^{s(k_r+1)} - 1}{p_r^s - 1} \right)$$

23. For any positive integer  $n$ , show the following:

$$(a) \sum_{d|n} \tau(d) = \sum_{d|n} \left( \frac{n}{d} \right) \tau(d)$$

Pf: (1) First note that since  $\tau(n)$  is multiplicative,  $H(n) = \sum_{d|n} \frac{n}{d} \tau(d)$  is multiplicative.

$$\text{Pf: } H(mn) = \sum_{d|mn} \frac{mn}{d} \tau(d) = \sum_{\substack{d_1|m \\ d_2|n}} \frac{mn}{d_1 d_2} \tau(d_1 d_2)$$

$$= \sum_{\substack{d_1 \mid m \\ d_2 \mid n}} \frac{m}{d_1 d_2} T(d_1) T(d_2)$$

$$= \sum_{\substack{d_1 \mid m \\ d_2 \mid n}} \frac{m}{d_1} T(d_1) \frac{n}{d_2} T(d_2)$$

$$= \left( \sum_{d_1 \mid m} \frac{m}{d_1} T(d_1) \right) \left( \sum_{d_2 \mid n} \frac{n}{d_2} T(d_2) \right)$$

$$= H(m) \cdot H(n)$$

$\therefore$  The functions

$$F(n) = \sum_{d \mid n} \sigma(d) \text{ and } G(n) = \sum_{d \mid n} \frac{n}{d} T(d)$$

are multiplicative.

(2) Now, let  $n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$  be the prime

factorization of  $n$ . If it can be

shown that  $F(p^k) = G(p^k)$ , then  $F(n) =$

$$F(p_1^{k_1} \cdots p_r^{k_r}) = F(p_1^{k_1}) \cdots F(p_r^{k_r}) = G(p_1^{k_1}) \cdots G(p_r^{k_r})$$

$$= G(p_1^{k_1} \cdots p_r^{k_r}) = G(n).$$

$$(3) \therefore F(p^k) = \sum_{d|p^k} \tau(d) = (p^0) + (p^0 + p^1) + \cdots + (p^0 + p^1 + \cdots + p^k)$$

$$= (k+1)p^0 + (k)p^1 + \cdots + (1)p^k$$

$$= (1) \cdot p^k + \cdots + (k)p + (k+1) \quad [1]$$

$$G(p^k) = \sum_{d|p^k} \frac{p^k}{d} \tau(d)$$

$$= \left( \frac{p^k}{p^0} \cdot \tau(p^0) \right) + \left( \frac{p^k}{p^1} \cdot \tau(p^1) \right) + \cdots + \left( \frac{p^k}{p^k} \cdot \tau(p^k) \right)$$

$$= (1) \cdot p^k + 2 \cdot p^{k-1} + \cdots + (k)p + (k+1) \quad [2]$$

$\therefore$  Since  $[1] = [2]$ , Then  $F(p^k) = G(p^k)$

$\therefore$  As stated in (2), because of (3),  $\sum_{d|n} \sigma(d) = \sum_{d|n} \frac{n}{d} \tau(d)$

$$(6) \sum_{d|n} \left(\frac{n}{d}\right) \tau(d) = \sum_{d|n} d \tau(d)$$

Pf: Since  $f(n) = n$  is multiplicative, so is  $f \cdot \tau$   
 $\therefore G(n) = \sum_{d|n} d \tau(d)$  is multiplicative.

As in (a), the proof that  $F(n) = \sum_{d|n} \left(\frac{n}{d}\right) \tau(d)$   
 is multiplicative is identical to Th. 6.4.

So, as in (a) it suffices to prove

$$F(n) = G(n) \text{ for } n = p^k.$$

$$F(p^k) = \sum_{d|p^k} \left(\frac{p^k}{d}\right) \tau(d)$$

$$= p^{k-1} \cdot p^0$$

$$+ p^{k-1} (p^0 + p)$$

$$+ p^{k-2} (p^0 + p + p^2)$$

+ ...

$$+ p^0 (p^0 + p + \dots + p^k)$$

$$= (k+1)\rho^k + k \cdot \rho^{k-1} + (k-1)\rho^{k-2} + \dots + 1$$

$$= 1 + \sum_{i=1}^k (i+1)\rho^i \quad [1]$$

$$G(\rho^k) = \sum_{d|p^k} d F(d)$$

$$= 1 \cdot 1$$

$$+ \rho \cdot (1+1)$$

$$+ \rho^2 \cdot (1+1+1)$$

+ ...

$$+ \rho^k (k+1)$$

$$= 1 + \sum_{i=1}^k \rho^i (i+1) \quad [2]$$

$$\text{Since } [1] = [2], \quad F(\rho^k) = G(\rho^k)$$

## 6.2 The Möbius Inversion Formula

Note Title

7/4/2005

1. (a). For each positive integer  $n$ , show

$$\mu(n)\mu(n+1)\mu(n+2)\mu(n+3) = 0$$

Pf: From The Division Algorithm, let

$$n = 4a + b, \text{ where } 0 \leq b < 4$$

If  $b = 0$ , Then  $4|n \Rightarrow 2^2|n$  so  $\mu(n) = 0$

If  $b = 1$ , Then  $n+3 = 4a+4$ , so  $4|n+3$ ,  
so  $\mu(n+3) = 0$

If  $b = 2$ ,  $n+2 = 4a+4$ , so  $4|n+2 \Rightarrow \mu(n+2) = 0$

If  $b = 3$ ,  $n+1 = 4a+4$ , so  $4|n+1 \Rightarrow \mu(n+1) = 0$

$\therefore$  for any  $n$ , at least one factor  
will yield  $\mu = 0$ .

(b). For any integer  $n \geq 3$ , show  $\sum_{k=1}^n \mu(k!) = 1$

Pf:  $\mu(4) = 0$  since  $4 = 2^2$ .

If  $n \geq 4$ , Then  $n!$  will contain 4 as a  
factor.

$\mu$  is multiplicative, so for  $n \geq 4$ ,  
 $\mu(n!) = \mu(n) \cdots \mu(4) \mu(3) \mu(2) \mu(1) = 0$ .

$\therefore$  Only need to consider cases of  $n=3$

$$\mu(1) = 1, \mu(2) = -1, \mu(3) = -1.$$

$$\begin{aligned}\therefore \sum_{k=1}^3 \mu(k!) &= \mu(1!) + \mu(2!) + \mu(3!) \\ &= \mu(1) + \mu(2) + \mu(6) \\ &= 1 + (-1) + 1 = 1.\end{aligned}$$

2. The Mangoldt function  $\Lambda$  is defined by

$$\Lambda(n) = \begin{cases} \log(p), & \text{if } n = p^k, p \text{ prime, } k \geq 1 \\ 0 & \text{otherwise} \end{cases}$$

$$\text{Prove } \Lambda(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) \log(d) = -\sum_{d|n} \mu(d) \log(d)$$

Pf: Let  $n = p^k$

$$\begin{aligned}(a) \therefore \sum_{d|n} \mu\left(\frac{n}{d}\right) \log(d) &= \mu(p^k) \log(1) \\ &\quad + \mu(p^{k-1}) \log(p) \\ &\quad + \dots \\ &\quad + \dots \mu(p^{k-i}) \log(p^i) \\ &\quad + \dots \\ &\quad + \mu(p^0) \log(p^k)\end{aligned}$$

$$\text{If } k=1, \text{ The sum is } \mu(p') \log(1) + \mu(p^o) \log(p') \\ = \mu(1) \log(p) = \log(p)$$

If  $k > 1$ ,  $\mu(p^{k-i}) = 0$  except for  $i=1, 2$ ,  
and then the sum is the same as for  
 $k=1$ .

$$\therefore \sum_{d|n} \mu\left(\frac{n}{d}\right) \log(d) = \log(p) = \Lambda(n)$$

$$(1) \sum_{d|n} \mu(d) \log(d) = \mu(p^o) \log(1) \\ + \mu(p') \log(p') \\ + \cdots \\ + \mu(p^i) \log(p^i) \\ + \cdots \\ + \mu(p^k) \log(p^k)$$

Because  $\mu(p^k) = 0$  for  $k \geq 1$ , The  
above sum reduces to, for all  $k$ ,

$$\mu(p^o) \log(1) + \mu(p) \log(p) = -\log(p)$$

$$\therefore \sum_{d|n} \mu(d) \log(d) = -\Lambda(n)$$

3. Let  $n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$  for  $n > 1$ . If  $f$  is a multiplicative function not identically 0, prove that

$$\sum_{d|n} \mu(d) f(d) = (1-f(p_1)) (1-f(p_2)) \dots (1-f(p_r))$$

Pf: Since  $\mu$  and  $f$  are multiplicative, Then  
 $\mu f$  is multiplicative (prob. #19, sec. 6.1).

$\therefore$  By Th. 6.4,  $F(n) = \sum_{d|n} \mu(d) f(d)$  is  
multiplicative.  $\therefore$  If prove for  $F(p^k)$  Then,  
since  $F(p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}) = F(p_1^{k_1}) \dots F(p_r^{k_r})$ , will  
have proven for  $F(n)$ .

$$\therefore \text{Consider } F(p^k) = \sum_{d|p^k} \mu(d) f(d)$$

$$= \mu(1)f(1) + \mu(p)f(p) + \dots + \mu(p^k)f(p^k)$$

$$= \mu(1)f(1) + \mu(p)f(p) \quad [\mu(p^i) = 0 \text{ for } i \geq 2]$$

$$= 1 \cdot f(1) + (-1) \cdot f(p) = 1 - f(p)$$

Since, for a multiplicative function not identically zero,  $f(1) = 1$  (see Sec. 6.1).

$$\therefore F(p^k) = 1 - f(p).$$

$$\therefore \sum_{d|n} \mu(d)f(d) = (1-f(p_1)) \cdots (1-f(p_r))$$

4. Let  $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ . Establish the following:

$$(a) \sum_{d|n} \mu(d)\tau(d) = (-1)^r$$

Pf: By Prob. #3 above,

$$\sum_{d|n} \mu(d)\tau(d) = [1 - \tau(p_1)] \cdot [1 - \tau(p_2)] \cdots [1 - \tau(p_r)]$$

But  $\tau(p) = 2$ , for any prime  $p$ .  $\therefore 1 - \tau(p) = -1$ .

$$\therefore \sum_{d|n} \mu(d)\tau(d) = (-1)^r$$

$$(6) \sum_{d|n} \mu(d) \sigma(d) = (-1)^r p_1 p_2 \cdots p_r$$

Pf: By Prob. #3 above,

$$\sum_{d|n} \mu(d) \sigma(d) = [1 - \sigma(p_1)] [1 - \sigma(p_2)] \cdots [1 - \sigma(p_r)]$$

But  $\sigma(p) = 1 + p$  for any prime  $p$ .  
 $\therefore 1 - \sigma(p) = -p$

$$\begin{aligned} \therefore \sum_{d|n} \mu(d) \sigma(d) &= (-p_1)(-p_2) \cdots (-p_r) \\ &= (-1)^r p_1 p_2 \cdots p_r \end{aligned}$$

$$(C) \sum_{d|n} \mu(d)/d = \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_r}\right)$$

Pf: First,  $f(n) = \frac{1}{n}$  is multiplicative  
 $\because f(mn) = \frac{1}{mn} = \frac{1}{m} \cdot \frac{1}{n} = f(m)f(n)$ .

$\therefore$  By Prob. #3 above, where  $f(n) = \frac{1}{n}$

$$\sum_{d|n} \mu(d) \frac{1}{d} = \left(1 - f(p_1)\right) \cdots \left(1 - f(p_r)\right) = \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_r}\right)$$

$$(d) \sum_{d|n} d \mu(d) = (1-p_1)(1-p_2) \cdots (1-p_r)$$

Pf: Let  $f(n) = n$ .  $f$  is clearly multiplicative.  
 $\therefore$  By Prob. #3 above,

$$\begin{aligned} \sum_{d|n} d \mu(d) &= \sum_{d|n} f(d) \mu(d) = (1-f(p_1)) \cdots (1-f(p_r)) \\ &= (1-p_1) \cdots (1-p_r) \end{aligned}$$

5. Let  $s(n)$  denote the number of square-free divisors of  $n$ . Establish that

$$s(n) = \sum_{d|n} |\mu(d)| = 2^{w(n)}, \text{ where}$$

$w(n)$  = number of distinct prime divisors of  $n$ .

Pf: Note that  $|\mu(n)| = \begin{cases} 1 & \text{if } n=1 \\ 0 & \text{if } p^2|n, p \text{ prime} \\ 1 & \text{if } n=p_1 \cdots p_r, p_i \text{ distinct} \end{cases}$

Let  $f(n) = |\mu(n)|$ . Let  $m, n$  be relatively prime.

Clearly,  $f(1) = 1$

If  $m=1$ ,  $f(mn) = f(n) = f(m)f(n)$

Let  $m, n$  be relatively prime.

If  $p^2 \mid m$ , then  $p^2 \mid mn$ .  $\therefore f(mn) = 0$  and  
 $f(m) = 0$ .  $\therefore f(mn) = f(m)f(n)$

$\therefore$  Assume both  $m, n$  are square-free.

Let  $m = p_1 \dots p_r$ ,  $n = q_1 \dots q_s$ .  $p_i \neq q_j$  since

$\gcd(m, n) = 1$ . Clearly,  $f(m) = 1, f(n) = 1$ ,  
and  $f(mn) = 1$ .  $\therefore f(mn) = f(m)f(n)$ .

$\therefore |\mu(n)|$  is multiplicative.

$\therefore$  By Th. 6.4,  $\sum_{d|n} |\mu(d)|$  is multiplicative.

$\therefore S(n)$  is multiplicative.

Consider  $n = p^k$ . The divisors of  $n$  are  
 $1, p, p^2, \dots, p^k$ .

$$\begin{aligned}\therefore \sum_{d|n} |\mu(d)| &= |\mu(1)| + |\mu(p)| + |\mu(p^2)| + \dots + |\mu(p^k)| \\ &= 1 + 1 + 0 + \dots + 0 = 2\end{aligned}$$

The number of square-free divisors of  $p^k$   
is 2 and is defined by  $\sum_{d|n} |\mu(d)|$

Consider  $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ . From Th. G.1,

all the square-free divisors of  $n$  are represented by  $n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$ ,  $0 \leq a_i \leq 1$

Since the number of square-free divisors from  $p_1$  is 2 (1 and  $p_1$ ), from  $p_2$  is 2, ... from  $p_r$  is 2, the total number

of square-free divisors is  $2^r$ , or  $2^{\omega(n)}$ ,

where  $\omega(n) = r = \# \text{ of distinct prime divisors of } n$ .

$$\begin{aligned} \therefore S(n) &= S(p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}) = S(p_1^{k_1}) S(p_2^{k_2}) \cdots S(p_r^{k_r}) \\ &= \left( \sum_{d|p_1^{k_1}} |\mu(p_1^{k_1})| \right) \cdots \left( \sum_{d|p_r^{k_r}} |\mu(p_r^{k_r})| \right) \\ &= (2) \cdots (2) = 2^r = 2^{\omega(n)} \end{aligned}$$

6. Find formulas for  $\sum_{d|n} \frac{\mu^2(d)}{\tau(d)}$  and  $\sum_{d|n} \frac{\mu^2(d)}{\sigma(d)}$   
in terms of the prime factorization of  $n$ .

From Prob. # 19, Sec. 6.1,  $\frac{\mu^2(n)}{T(n)}$  and  $\frac{\mu^2(n)}{G(n)}$   
 are both multiplicative.

$\therefore$  First consider case for  $n = p^k$

$$\begin{aligned} \sum_{d|n} \frac{\mu^2(d)}{T(d)} &= \frac{\mu^2(1)}{T(1)} + \frac{\mu^2(p)}{T(p)} + \frac{\mu^2(p^2)}{T(p^2)} + \dots + \frac{\mu^2(p^k)}{T(p^k)} \\ &= \frac{1}{1} + \frac{1}{2} + 0 + \dots + 0 \end{aligned}$$

$$= \frac{3}{2}$$

$$\begin{aligned} \sum_{d|n} \frac{\mu^2(d)}{G(d)} &= \frac{\mu^2(1)}{G(1)} + \frac{\mu^2(p)}{G(p)} + \frac{\mu^2(p^2)}{G(p^2)} + \dots + \frac{\mu^2(p^k)}{G(p^k)} \\ &= \frac{1}{1} + \frac{1}{p+1} + 0 + \dots 0 \\ &= \frac{p+2}{p+1} \end{aligned}$$

$\therefore$  Let  $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$

$$F(n) = \sum_{d|n} \frac{\mu^2(d)}{T(d)}, \quad G(n) = \sum_{d|n} \frac{\mu^2(d)}{G(d)}$$

Both  $F$  and  $G$  are multiplicative,

$$\therefore F(n) = F(p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}) = F(p_1^{k_1}) F(p_2^{k_2}) \dots F(p_r^{k_r})$$

$$\text{and } G(n) = G(p_1^{k_1}) G(p_2^{k_2}) \dots G(p_r^{k_r})$$

$$\therefore \sum_{d|n} \frac{\mu^2(d)}{\tau(d)} = F(p_1^{k_1}) \dots F(p_r^{k_r}) = \left(\frac{3}{2}\right) \dots \left(\frac{3}{2}\right)$$

$$= \left(\frac{3}{2}\right)^r, \quad r = \# \text{ distinct primes.}$$

$$\begin{aligned} \sum_{d|n} \frac{\mu^2(d)}{\sigma(d)} &= G(p_1^{k_1}) \dots G(p_r^{k_r}) \\ &= \left(\frac{p_1+2}{p_1+1}\right) \left(\frac{p_2+2}{p_2+1}\right) \dots \left(\frac{p_r+2}{p_r+1}\right) \end{aligned}$$

7. The Liouville  $\lambda$ -function is defined by :

$$\lambda(1) = 1$$

$$\lambda(n) = (-1)^{k_1 + k_2 + \dots + k_r}, \quad n > 1, \quad n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$$

(a) Prove  $\lambda$  is a multiplicative function

Pf: Let  $m, n$  be relatively prime,

$$m = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}, \quad n = q_1^{j_1} q_2^{j_2} \dots q_s^{j_s}$$

$$mn = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r} q_1^{j_1} \dots q_s^{j_s}, \text{ where } p_i \neq q_j$$

since  $\gcd(m, n) = 1$ .

$$\begin{aligned}\therefore \lambda(mn) &= (-1)^{k_1 + \dots + k_r + j_1 + \dots + j_s} \\ &= (-1)^{k_1 + \dots + k_r} \cdot (-1)^{j_1 + \dots + j_s} \\ &= \lambda(m) \cdot \lambda(n)\end{aligned}$$

(6). Given  $n > 0$ , verify

$$\sum_{d|n} \lambda(d) = \begin{cases} 1 & \text{if } n = m^2, \text{ some } m \\ 0 & \text{otherwise} \end{cases}$$

Pf: Let  $F(n) = \sum_{d|n} \lambda(d)$ .  $F$  is multiplicative

by Th. G. 4. Plan is to prove for  $n = p^k$ ,  
then extrapolate.

Let  $n = p^k$ .

$$\begin{aligned}\therefore F(n) &= \lambda(1) + \lambda(p) + \dots + \lambda(p^k) \\ &= 1 + (-1) + (-1)^2 + (-1)^3 + \dots + (-1)^{k-1} + (-1)^k\end{aligned}$$

If  $K$  is even,  $n = p^{2w}$ , where  $K = 2w$ .  
 $\therefore$  Let  $m = p^w$ ,  $\therefore n = m^2$   
Also,  $F(n) = 1$

If  $K$  is odd,  $F(p^K) = 0$

$\therefore$  Now let  $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$   
 $\therefore F(n) = F(p_1^{k_1}) \cdots F(p_r^{k_r})$

If  $n = m^2$  for some  $m$ , Then all the  $k_i$  are even, so  $F(p_i^{k_i}) = 1$  from above.  
 $\therefore F(n) = 1$

If any one of the  $k_i$  is odd, Then  
 $F(p_i^{k_i}) = 0$ , so  $F(n) = 0$ .

8. For any integer  $n \geq 1$ , verify formulas below:

$$(a) \sum_{d|n} \mu(d) \lambda(d) = 2^{w(n)}, w(n) = \# \text{distinct prime divisors of } n$$

Pf:  $\mu \cdot \lambda$  is multiplicative (Prob. 19, Sec. 6-1)

$\therefore$  Consider  $n = p^K$

$$\begin{aligned}
 \therefore \sum_{d|n} \mu(d) \lambda(d) &= \mu(1) \lambda(1) \\
 &\quad + \mu(p) \lambda(p) + \cdots + \mu(p^k) \lambda(p^k) \\
 &= 1 \cdot 1 + (-1)(-1) + \cdots + 0 \cdot (-1)^k \\
 &= 2
 \end{aligned}$$

That is, for  $n = p^k$ ,  $F(n) = \sum_{d|n} \mu(d) \lambda(d) = 2$

$$\begin{aligned}
 \therefore \text{for } n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}, \\
 F(n) &= F(p_1^{k_1}) F(p_2^{k_2}) \cdots F(p_r^{k_r}) \\
 &= 2 \cdot 2 \cdots 2 = 2^r = 2^{\omega(n)} \\
 &\text{since } \omega(n) = r.
 \end{aligned}$$

$$(6) \sum_{d|n} \lambda\left(\frac{n}{d}\right) 2^{\omega(d)} = 1$$

Pf: Lemma: If  $f(n), g(n)$  are multiplicative,  
 Then so is  $F(n) = \sum_{d|n} f\left(\frac{n}{d}\right) \cdot g(d)$

Pf: Let  $m, n$  be relatively prime

positive integers.

$$\therefore F(mn) = \sum_{d|mn} f\left(\frac{mn}{d}\right) \cdot g(d) =$$

$$\begin{aligned} \sum_{\substack{d_1|m \\ d_2|n}} f\left(\frac{mn}{d_1d_2}\right) \cdot g(d_1, d_2) &= \sum_{\substack{d_1|m \\ d_2|n}} f\left(\frac{m}{d_1}\right) f\left(\frac{n}{d_2}\right) g(d_1) g(d_2) \\ &= \sum_{\substack{d_1|m \\ d_2|n}} f\left(\frac{m}{d_1}\right) g(d_1) f\left(\frac{n}{d_2}\right) g(d_2) \\ &= \left( \sum_{d_1|m} f\left(\frac{m}{d_1}\right) g(d_1) \right) \left( \sum_{d_2|n} f\left(\frac{n}{d_2}\right) g(d_2) \right) = F(m) F(n) \end{aligned}$$

$\therefore F(n) = \sum_{d|n} \lambda\left(\frac{n}{d}\right) 2^{w(d)}$  is multiplicative.  
by above Lemma and  
problems 19, 20(a), Sec. 6.1

$\therefore$  consider  $n = p^k$

$$F(p^k) = \sum_{d|p^k} \lambda\left(\frac{p^k}{d}\right) 2^{w(d)}$$

$$= \lambda\left(\frac{p^k}{1}\right) 2^{w(1)} + \lambda\left(\frac{p^k}{p}\right) 2^{w(p)} + \dots + \lambda\left(\frac{p^k}{p^{k-1}}\right) 2^{w(p^{k-1})} + \lambda\left(\frac{p^k}{p^k}\right) 2^{w(p^k)}$$

$$= (-1)^k \cdot 1 + (-1)^{k-1} \cdot 2 + \dots + (-1)^1 \cdot 2 + 1 \cdot 2$$

There are  $k$  terms of  $(-1)^{k-1} \cdot 2 + \dots + (-1)^1 \cdot 2 + 1 \cdot 2$

$\therefore$  If  $k$  is even,  $(-1)^k \cdot 1 = 1$ , and

$$\underbrace{[(-1)^{k-1} + (-1)^{k-2} + \dots + (-1)^1 + 1]}_{k = \text{even } \# \text{ terms, alternating signs}} \cdot 2 = 0 \cdot 2 = 0$$

$k = \text{even } \# \text{ terms, alternating signs}$

$$\therefore F(\rho^k) = 1 + 0 = 1$$

If  $k$  is odd,  $(-1)^k \cdot 1 = -1$ , and

$$\underbrace{[(-1)^{k-1} + (-1)^{k-2} + \dots + (-1)^1 + 1]}_{k-1 = \text{even } \# \text{ terms, alternating signs}} \cdot 2 = [0+1] \cdot 2 = 2$$

$k-1 = \text{even } \# \text{ terms, alternating signs}$

$$\therefore F(\rho^k) = (-1) + 2 = 1$$

$\therefore$  If  $n = \rho_1^{k_1} \rho_2^{k_2} \dots \rho_r^{k_r}$ ,

$$F(n) = F(\rho_1^{k_1}) F(\rho_2^{k_2}) \dots F(\rho_r^{k_r}) = 1 \cdot 1 \cdots 1 = 1$$

## 6.3 The Greatest Integer Function

Note Title

7/21/2005

1. Given integers  $a, b > 0$ , show there exists a unique integer  $r$  with  $0 \leq r < b$  satisfying  $a = \lfloor a/b \rfloor b + r$ .

Pf: By def.,  $a/b - 1 < \lfloor a/b \rfloor \leq a/b$

$$\therefore \lfloor a/b \rfloor b \leq (a/b) \cdot b = a, \therefore 0 \leq a - \lfloor a/b \rfloor b$$

$$\text{Let } r = a - \lfloor a/b \rfloor b \quad \therefore 0 \leq r$$

Also,  $(a/b - 1)b < \lfloor a/b \rfloor b$ , so  $a \cdot b < \lfloor a/b \rfloor b$ , or  $a - \lfloor a/b \rfloor b < b$

$\therefore r < b \quad \therefore \text{With } r = a - \lfloor a/b \rfloor b, 0 \leq r < b$

$r$  is unique: let  $r' b < s.t. a = \lfloor a/b \rfloor b + r'$

$$\therefore r' = a - \lfloor a/b \rfloor b, \text{ so } r' = r$$

2. Let  $x, y$  be real numbers. Prove the greatest integer function satisfies the following properties:

(a)  $\lfloor x+n \rfloor = \lfloor x \rfloor + n$  for any integer  $n$ .

By def.,  $x-1 < \lfloor x \rfloor \leq x$

$$\therefore x-1+n < \lfloor x \rfloor + n \leq x+n \quad [1]$$

Also, by def of  $\lfloor x+n \rfloor$ ,

$$x+n-1 < \lfloor x+n \rfloor \leq x+n \quad [2]$$

$$\therefore x+n < \lfloor x+n \rfloor + 1 \quad [3]$$

$$[1] \text{ and } [3] \text{ yield } \lfloor x \rfloor + n < \lfloor x+n \rfloor + 1 \quad [4]$$

From [2],  $\lfloor x+n \rfloor - 1 \leq x+n-1$

and from [1],  $x+n-1 < \lfloor x \rfloor + n$

$$\therefore \lfloor x+n \rfloor - 1 < \lfloor x \rfloor + n \quad [5]$$

$$[4] \text{ and } [5] \text{ yield } \lfloor x+n \rfloor - 1 < \lfloor x \rfloor + n < \lfloor x+n \rfloor + 1$$

$$\therefore -1 < \lfloor x \rfloor + n - (\lfloor x+n \rfloor) < 1$$

Since all quantities are integers,

$$\lfloor x \rfloor + n - (\lfloor x+n \rfloor) = 0, \text{ or } \lfloor x \rfloor + n = \lfloor x+n \rfloor$$

(6)  $\lfloor x \rfloor + \lceil -x \rceil = 0 \text{ or } -1$ , according as  $x$  is an integer or not.

(1) If  $x$  is an integer,  $\lfloor x \rfloor = x$  and  $\lfloor -x \rfloor = -x$   
 $\therefore \lfloor x \rfloor + \lfloor -x \rfloor = 0$

(2) If  $x$  is not an integer,  $x = \lfloor x \rfloor + \theta$ ,  $0 < \theta < 1$   
 $-x = \lfloor -x \rfloor + \theta'$ ,  $0 < \theta' < 1$   
Adding,  $x + (-x) = \lfloor x \rfloor + \lfloor -x \rfloor + \theta + \theta'$ , or

$$0 = \lfloor x \rfloor + \lfloor -x \rfloor + \theta + \theta'$$

But  $0 < \theta + \theta' < 2$ , and  $\theta + \theta' = -(\lfloor x \rfloor + \lfloor -x \rfloor)$   
 $\therefore 0 < -(\lfloor x \rfloor + \lfloor -x \rfloor) < 2$ , or  $-2 < \lfloor x \rfloor + \lfloor -x \rfloor < 0$

$\lfloor x \rfloor + \lfloor -x \rfloor$  is an integer, so  $\lfloor x \rfloor + \lfloor -x \rfloor = -1$ .

(c)  $\lfloor x \rfloor + \lfloor y \rfloor \leq \lfloor x+y \rfloor$ , and when  $x > 0, y > 0$ ,  $\lfloor x \rfloor \lfloor y \rfloor \leq \lfloor xy \rfloor$

(1)  $\lfloor x \rfloor + \lfloor y \rfloor \leq \lfloor x+y \rfloor$

If  $x, y$  are both integers,  $\lfloor x \rfloor = x$ ,  $\lfloor y \rfloor = y$ ,  
 $\lfloor x+y \rfloor = x+y$ .  $\therefore \lfloor x \rfloor + \lfloor y \rfloor = \lfloor x+y \rfloor$

If one of  $x, y$  is an integer, say  $y$ ,  
then  $\lfloor x \rfloor + \lfloor y \rfloor = \lfloor x \rfloor + y$   
By (a),  $\lfloor x+y \rfloor = \lfloor x \rfloor + y$ .

$$\therefore [x] + [y] = [x+y]$$

Suppose both  $x$  and  $y$  are not integers.

$$\therefore \text{By def., } x-1 < [x] < x \\ y-1 < [y] < y$$

$$\therefore [x] + [y] - 1 < x+y - 1 \quad [1]$$

From the def. of  $[x+y]$ ,

$$x+y-1 < [x+y] \leq x+y \quad [2]$$

From [1] and [2],

$$[x] + [y] - 1 < [x+y] \quad [3]$$

Since all quantities are integers in [3],

$$[x] + [y] \leq [x+y]$$

(2)  $[x][y] \leq [xy]$  when  $x > 0, y > 0$

$$\text{Let } x = [x] + \theta, \quad 0 \leq \theta < 1 \\ y = [y] + \theta', \quad 0 \leq \theta' < 1$$

$$\begin{aligned}
 \therefore [xy] &= [(x+\theta)(y+\theta')] \\
 &= [xy] + \theta[y] + \theta'[x] + \theta\theta' \\
 &= [xy] + [\theta[y] + \theta'[x] + \theta\theta'], \text{ by} \\
 &\quad (\text{a) above since } [xy] \text{ is an integer.}
 \end{aligned}$$

All quantities in  $[\theta[y] + \theta'[x] + \theta\theta']$   
are positive.

$$\therefore [xy] \geq [xy]$$

(d)  $[x/n] = [\frac{x}{n}]$  for any positive integer  $n$ .

$$\text{Let } x/n = [\frac{x}{n}] + \theta, \quad 0 \leq \theta < 1.$$

$$\therefore x = [\frac{x}{n}] \cdot n + \theta n$$

$$\therefore [x] = [\frac{x}{n}] \cdot n + \theta n]$$

$$= [\frac{x}{n}] \cdot n + [\theta n], \text{ by (a) since } [\frac{x}{n}] \cdot n \text{ is an integer}$$

$$\therefore [x]/n = [\frac{x}{n}] + [\theta n]/n \quad [1]$$

But since  $0 \leq \theta < 1$ , Then  $0 \leq \theta n < n$   
 $\therefore 0 \leq [\theta n] \leq \theta n < n$

$$\therefore 0 \leq [\theta n]/n < 1, \therefore [\theta n]/n = 0$$

$$\therefore \text{From } [1], \quad [x]/n = [x/n]$$

(e)  $[nm/k] \geq n[m/k]$  for positive integers  $n, m, k$ .

$$\text{From (c), } [nm/k] \geq [n][m/k]$$

But  $[n] = n$  for positive integer  $n$ .

$$\therefore [nm/k] \geq n[m/k]$$

$$(f) [x] + [y] + [x+y] \leq [2x] + [2y]$$

$$\text{Let } x = [x] + \theta, 0 \leq \theta < 1$$

$$y = [y] + \theta', 0 \leq \theta' < 1$$

$$\therefore x+y = [x] + [y] + \theta + \theta'$$

$$\therefore [x+y] = [x] + [y] + [\theta + \theta'], \text{ and using (a)}$$

$$= [x] + [y] + [\theta + \theta'] \quad [1]$$

(1) Suppose  $0 \leq \theta < 0.5$ ,  $0 \leq \theta' < 0.5$

$$\therefore 0 \leq \theta + \theta' < 1, \text{ so } [\theta + \theta'] = 0$$

$\therefore$  Equation [1] becomes  $[x+y] = [x] + [y]$

$$\therefore [x] + [y] + [x+y] = 2[x] + 2[y]$$

But  $2[x] = 2x - 2\theta$ , so  $2x = 2[x] + 2\theta$

$$\begin{aligned} \therefore [2x] &= [2[x] + 2\theta] \\ &= 2[x] + [2\theta] \quad \text{by (a)} \end{aligned}$$

Since  $0 \leq \theta < 0.5$ ,  $0 \leq 2\theta < 1$ .

$$\therefore [2\theta] = 0$$

$$\therefore [2x] = 2[x]$$

$$\text{Similarly, } [2y] = 2[y]$$

$$\therefore [x] + [y] + [x+y] = 2[x] + 2[y] = [2x] + [2y]$$

$$\text{Or, } [x] + [y] + [x+y] = [2x] + [2y]$$

(2) Suppose  $0 \leq \theta < 0.5$ ,  $0.5 \leq \theta' < 1$

$$\therefore 0 < \theta + \theta' < 1.5, \text{ so } 0 \leq [\theta + \theta'] \leq 1$$

$\therefore$  From Equation [1],  $[x+y] \leq [x] + [y] + 1$

$$\therefore [x] + [y] + [x+y] \leq 2[x] + 2[y] + 1 \quad [2]$$

But  $2[x] = 2x - 2\theta$ , so  $2x = 2[x] + 2\theta$   
 $\therefore [2x] = [2[x] + 2\theta]$

$$= 2[x] + [2\theta] \text{ by (a)}$$

And  $0 \leq 2\theta < 1$ ,  $\therefore [2\theta] = 0$

$$\therefore [2x] = 2[x] \quad [3]$$

Also  $2[y] = 2y - 2\theta'$ , so  $2y = 2[y] + 2\theta'$   
 $\therefore [2y] = [2[y] + 2\theta']$

$$= 2[y] + [2\theta'] \text{ by (a)}$$

And  $1 \leq 2\theta' < 2$

$$\therefore [2\theta'] = 1$$

$$\therefore [2y] = 2[y] + 1$$

Or,  $2[y] = [2y] - 1 \quad [4]$

Substituting [3] and [4] into [2],

$$[x] + [y] + [x+y] \leq [2x] + [2y] - 1 + 1 \\ = [2x] + [2y]$$

Similarly, if  $0.5 \leq \theta < 1$ ,  $0 \leq \theta' < 0.5$ ,

$$[x] + [y] + [x+y] \leq [2x] + [2y]$$

(3) Suppose  $0.5 \leq \theta < 1$ ,  $0.5 \leq \theta' < 1$

$$\therefore 1 \leq \theta + \theta' < 2, \text{ so } \lceil \theta + \theta' \rceil = 1$$

$\therefore$  Equation  $\lceil s \rceil$  becomes  $\lceil x+y \rceil = \lceil x \rceil + \lceil y \rceil + 1$

$$\therefore \lceil x \rceil + \lceil y \rceil + \lceil x+y \rceil = 2\lceil x \rceil + 2\lceil y \rceil + 1 \quad [5]$$

But  $2x = 2\lceil x \rceil + 2\theta$

$$\begin{aligned} \therefore \lceil 2x \rceil &= \lceil 2\lceil x \rceil + 2\theta \rceil \\ &= 2\lceil x \rceil + \lceil 2\theta \rceil \quad \text{by (a)} \end{aligned}$$

And  $1 \leq 2\theta < 2$ , so  $\lceil 2\theta \rceil = 1$

$$\therefore \lceil 2x \rceil = 2\lceil x \rceil + 1$$

Similarly,  $\lceil 2y \rceil = 2\lceil y \rceil + 1$

Substituting into  $\lceil s \rceil$ ,

$$\lceil x \rceil + \lceil y \rceil + \lceil x+y \rceil = \lceil 2x \rceil - 1 + \lceil 2y \rceil - 1 + 1$$

$$= \lceil 2x \rceil + \lceil 2y \rceil - 1$$

$$< \lceil 2x \rceil + \lceil 2y \rceil$$

$$\therefore \lceil x \rceil + \lceil y \rceil + \lceil x+y \rceil < \lceil 2x \rceil + \lceil 2y \rceil$$

$\therefore (1), (2), \text{ and } (3) \text{ yield:}$

$$\lfloor x \rfloor + \lfloor y \rfloor + \lfloor x+y \rfloor \leq \lfloor 2x \rfloor + \lfloor 2y \rfloor$$

3. Find the highest power of 5 dividing  $1000!$   
and the highest power of 7 dividing  $2000!$

(a).  $\left\lfloor \frac{1000}{5} \right\rfloor + \left\lfloor \frac{1000}{5^2} \right\rfloor + \left\lfloor \frac{1000}{5^3} \right\rfloor + \left\lfloor \frac{1000}{5^4} \right\rfloor$   
 $= 200 + 40 + 8 + 1 = 249$

$\therefore 5^{249}$  divides  $1000!$

(b)  $\left\lfloor \frac{2000}{7} \right\rfloor + \left\lfloor \frac{2000}{7^2} \right\rfloor + \left\lfloor \frac{2000}{7^3} \right\rfloor$   
 $= 285 + 40 + 5 = 330$

$\therefore 7^{330}$  divides  $2000!$

4. For an integer  $n \geq 0$ , show  $\left\lceil \frac{n}{2} \right\rceil - \left\lfloor -\frac{n}{2} \right\rfloor = n$

Pf: By def.,  $\frac{n}{2} - 1 < \left\lceil \frac{n}{2} \right\rceil \leq \frac{n}{2}$  [1]

and  $-\frac{n}{2} - 1 < \left\lfloor -\frac{n}{2} \right\rfloor \leq -\frac{n}{2}$  [2]

From  $\{2\}$ ,  $-\left\lceil -\frac{n}{2} \right\rceil < \frac{n}{2} + 1$

Adding to  $\{1\}$ ,  $\left\lceil \frac{n}{2} \right\rceil - \left\lceil -\frac{n}{2} \right\rceil < \frac{n}{2} + \frac{n}{2} + 1 = n + 1$

$$\therefore \left\lceil \frac{n}{2} \right\rceil - \left\lceil -\frac{n}{2} \right\rceil \leq n \quad \{3\}$$

Also from  $\{2\}$ ,  $\frac{n}{2} \leq -\left\lceil -\frac{n}{2} \right\rceil$

Adding to  $\{1\}$ ,  $\frac{n}{2} + \frac{n}{2} - 1 < \left\lceil \frac{n}{2} \right\rceil - \left\lceil -\frac{n}{2} \right\rceil$ ,

$$\text{or, } n - 1 < \left\lceil \frac{n}{2} \right\rceil - \left\lceil -\frac{n}{2} \right\rceil$$

$$\therefore n \leq \left\lceil \frac{n}{2} \right\rceil - \left\lceil -\frac{n}{2} \right\rceil \quad \{4\}$$

$$\{3\} \text{ and } \{4\} \Rightarrow \left\lceil \frac{n}{2} \right\rceil - \left\lceil -\frac{n}{2} \right\rceil = n$$

5. (a) Verify that  $1000!$  terminates in 249 zeros.

From #3,  $5^{249}$  divides  $1000!$ , but  $5^{250}$  does not

The greatest power of 2 dividing  $1000!$   
is greater than 500 since  $\left\lceil \frac{1000}{2} \right\rceil = 500$

$\therefore (2 \cdot 5)^{249}$  divides  $1000!$  but

$(2 \cdot 5)^{250}$  does not.

$\therefore 1000! = n \times 10^{249}$ , but  $1000! \neq n \times 10^{250}$

$\therefore 1000!$  ends in 249 zeros.

(6) For what value of  $n$  does  $n!$  terminate in 37 zeros?

Must find  $n$  s.t.  $2^{37} \mid n!$  and  $5^{37} \mid n!$ ,  
but either  $2^{38} \nmid n!$  or  $5^{38} \nmid n!$

$\therefore$  Consider  $\left[\frac{n}{5}\right] \leq 37$  since  $\left[\frac{n}{5}\right] > \left[\frac{n}{5^2}\right]$

$$\therefore n \leq 5 \cdot 37 = 185$$

2 is not the limiting factor since  
 $\left[\frac{185}{2}\right] = 92$

Since  $5^2 = 25$ ,  $5^3 = 125$ ,  $5^2$  will contribute 6 powers of 5 for  $n \geq 150$ , and  $5^3$  will contribute at least 1 power.

For  $n \geq 150$ , 5 contributes  $\frac{150}{5} = 30$

For  $n \geq 155$ , 5 contributes 31 powers.

$\therefore$  For  $n \geq 155$ , 5,  $5^2$ ,  $5^3$  will contribute  $31 + 6 + 1 = 38$  powers, which is too big.

$\therefore$  For  $150 \leq n \leq 154$ , 5 contributes

exactly 37 powers of 5.

For  $n = 149$ , 5 contributes 29 powers,

$5^2$  contributes 5 powers,

$5^3$  contributes 1 power.

$\therefore n = 149 \rightarrow 35$  powers of 5, too small.

For  $150 \leq n \leq 154$ , 2 easily contributes at least 37 powers as  $150/2 = 75$ .

$\therefore$  For  $150 \leq n \leq 154$ ,  $n!$  will terminate in 37 zeros.

6. If  $n \geq 1$  and  $p$  is a prime, prove that

(a)  $(2n)!/(n!)^2$  is an even integer

Pf: From Th. G.10, letting  $n=2n$  and  $r=n$  in the formula

$$\text{Then } \binom{2n}{n} = \frac{(2n)!}{n!(2n-n)!} = \frac{(2n)!}{(n!)^2} \text{ is an integer}$$

$$\text{But } \frac{(2n)!}{(n!)^2} = \frac{2n \cdot (2n-1) \cdots (n+1) \cdot n!}{(n!)^2}$$

$$= \frac{2n (2n-1) \cdots (n+1)}{n!}$$

This is an integer containing 2 as a factor, and so it is even.

(5) The exponent of the highest power of  $p$  that divides  $\frac{(2n)!}{(n!)^2}$  is  $\sum_{k=1}^{\infty} \left( \left[ \frac{2n}{p^k} \right] - 2 \left[ \frac{n}{p^k} \right] \right)$

Pf: For any prime  $p$ , let  $s$  be the highest power of  $p$  that divides  $(2n)!$ .  
If  $p$  also divides  $n!$ , let  $K$  be the highest power of  $p$  dividing  $n!$ .

$\therefore \frac{p^s}{p^K} = p^{s-K}$ , so  $s-K$  is the highest power of  $p$  dividing  $\frac{(2n)!}{n!}$ .

$\therefore \frac{p^s}{p^K \cdot p^K} = p^{s-2K}$ , so  $s-2K$  is the highest power of  $p$  dividing  $\frac{(2n)!}{(n!)^2}$ .

By Th. 6.9, the highest power of  $p$  dividing  $(2n)!$  is  $\sum_{k=1}^{\infty} \left[ \frac{2n}{p^k} \right]$

and the highest power of  $p$  dividing  $n!$  is:

$$\sum_{k=1}^{\infty} \left\{ \frac{n}{p^k} \right\}$$

$\therefore$  The highest power of  $p$  dividing  $\frac{(2n)!}{(n!)^2}$

$$\text{is: } \sum_{k=1}^{\infty} \left[ \frac{2n}{p^k} \right] - 2 \sum_{k=1}^{\infty} \left\{ \frac{n}{p^k} \right\}$$

$$= \sum_{k=1}^{\infty} \left( \left[ \frac{2n}{p^k} \right] - 2 \left[ \frac{n}{p^k} \right] \right)$$

(c) In the prime factorization of  $\frac{(2n)!}{(n!)^2}$ , the exponent of any prime  $p$  s.t.  $n < p < 2n$  is 1.

PF: Since  $n < p$ , Then  $\frac{n}{p} < 1$ , so  $\left[ \frac{n}{p} \right] = 0$ .

$\therefore$  For any  $k > 0$ ,  $\left[ \frac{n}{p^k} \right] = 0$ .

$\therefore$  From (6), The highest power of  $p$  is:  $\sum_{k=1}^{\infty} \left[ \frac{2n}{p^k} \right]$  since the contribution by  $2 \left[ \frac{n}{p^k} \right] = 0$ .

But since  $n < p$ ,  $\frac{n}{p} < 1$ , so  $\frac{2n}{p} < 2$   
As  $p < 2n$ ,  $1 < \frac{2n}{p}$ .  $\therefore \left[ \frac{2n}{p} \right] = 1$  and

$\frac{2n}{p \cdot p^k} < \frac{2}{p^k} < 1$  if  $p \geq 2$ .  $\therefore \left[ \frac{2n}{p^k} \right] = 0$  for  $k > 1$

$$\therefore \sum_{k=1}^{\infty} \left\lfloor \frac{2^n}{p^k} \right\rfloor = 1 \text{ for any } n < p < 2n,$$

so the highest power of  $p$  is 1.

$$7. \text{ Let } n = a_k p^k + a_{k-1} p^{k-1} + \dots + a_1 p + a_0, \text{ where } 0 \leq a_i < p.$$

Show the exponent of highest power of  $p$  appearing in the prime factorization of  $n!$  is:

$$\frac{n - (a_k + \dots + a_2 + a_1 + a_0)}{p-1}$$

Pf: The exponent of the highest power of  $p$ , by Th. 6.9, is:

$$\sum_{i=1}^{\infty} \left\lfloor \frac{n}{p^i} \right\rfloor = \left[ a_k p^{k-1} + \dots + a_1 + \frac{a_0}{p} \right] + \left[ a_k p^{k-2} + \dots + a_2 + \frac{a_1}{p} + \frac{a_0}{p^2} \right]$$

+

⋮

$$+ \left[ a_k + \dots + \frac{a_1}{p^{k-1}} + \frac{a_0}{p^k} \right]$$

$$+ \left[ \frac{a_k}{p} + \dots + \frac{a_1}{p^k} + \frac{a_0}{p^{k+1}} \right]$$

[1]

Lemma: for  $p > 1$ ,  $n \geq 1$ ,  $(p-1)(\frac{1}{p} + \frac{1}{p^2} + \dots + \frac{1}{p^n}) < 1$

By induction, let  $k = 1$ .

$$(p-1)\left(\frac{1}{p}\right) = 1 - \frac{1}{p} < 1$$

Suppose true for  $k$

$$\begin{aligned} \therefore (p-1)\left(\frac{1}{p} + \dots + \frac{1}{p^k} + \frac{1}{p^{k+1}}\right) &= \\ (p-1)\left(\frac{1}{p} + \dots + \frac{1}{p^k}\right) + \frac{p-1}{p^{k+1}} &= \\ p\left(\frac{1}{p} + \dots + \frac{1}{p^k}\right) - \frac{1}{p} - \dots - \frac{1}{p^k} + \frac{1}{p^k} - \frac{1}{p^{k+1}} \end{aligned}$$

But by assumption,

$$p\left(\frac{1}{p} + \dots + \frac{1}{p^k}\right) - \frac{1}{p} - \dots - \frac{1}{p^k} < 1$$

$$\therefore p\left(\frac{1}{p} + \dots + \frac{1}{p^k}\right) - \frac{1}{p} - \dots - \frac{1}{p^k} + \frac{1}{p^k} - \frac{1}{p^{k+1}} < 1 + \frac{1}{p^k} - \frac{1}{p^{k+1}}$$

$$\text{or, } p\left(\frac{1}{p} + \dots + \frac{1}{p^k}\right) - \frac{1}{p} - \dots - \frac{1}{p^k} - \frac{1}{p^{k+1}} < 1 - \frac{1}{p^{k+1}} < 1$$

$\therefore$  True for  $k+1$  also.

$\therefore$  True for all  $n \geq 1$ .

In  $\Sigma$ ], all  $0 \leq a_i \leq p-1$

$\therefore$  By the lemma, all terms in  $[1]$  divided by  $p^k$  add up to less than 1,  $[1]$  becomes:

$$\left[ \frac{n}{p} \right] = a_k p^{k-1} + \dots + a_2 p + a_1 \quad [a_1]$$

$$\left[ \frac{n}{p^2} \right] = a_k p^{k-2} + \dots + a_2 \quad [a_2]$$

$$\left[ \frac{n}{p^{k-1}} \right] = a_k p + a_{k-1} \quad [a_{k-1}]$$

$$\left[ \frac{n}{p^k} \right] = a_k \quad [a_k]$$

Note that  $\left[ \frac{n}{p^k} \right] p = a_k p = \left[ \frac{n}{p^{k-1}} \right] - a_{k-1}$

$$\therefore \left[ \frac{n}{p} \right] p = n - a_0$$

$$\left[ \frac{n}{p^2} \right] p = \left[ \frac{n}{p} \right] - a_1$$

$$\vdots$$

$$\left[ \frac{n}{p^{k-1}} \right] p = \left[ \frac{n}{p^{k-2}} \right] - a_{k-2}$$

$$\left[ \frac{n}{p^k} \right] p = \left[ \frac{n}{p^{k-1}} \right] - a_{k-1}$$

$$0 = \left[ \frac{n}{p^k} \right] - a_k$$

Adding the left column entries and right column entries, you get:

$$\left( \left[ \frac{n}{p} \right] + \left[ \frac{n}{p^2} \right] + \dots + \left[ \frac{n}{p^k} \right] \right) p = \left[ \frac{n}{p} \right] + \left[ \frac{n}{p^2} \right] + \dots + \left[ \frac{n}{p^k} \right] + n - (a_0 + \dots + a_k)$$

$$\therefore \left( \left[ \frac{n}{p} \right] + \left[ \frac{n}{p^2} \right] + \dots + \left[ \frac{n}{p^k} \right] \right) (p-1) = n - (a_0 + \dots + a_k)$$

or  $\sum_{k=1}^{\infty} \left[ \frac{n}{p^k} \right] = \frac{n - (a_0 + a_1 + \dots + a_k)}{p-1}$

8. (a). Using #7, show that the exponent of highest power of  $p$  dividing  $(p^k-1)!$  is:  $\frac{p^k-(p-1)k-1}{p-1}$

Strategy: find coefficients for the  $p$ -based expansion of  $p^k-1$  ( $0 \leq a_i < p$ ).

$$\begin{aligned} \text{First note } p^k-1 &= (p-1)(p^{k-1} + p^{k-2} + \dots + p + 1) \\ &= (p-1)p^{k-1} + (p-1)p^{k-2} + \dots + (p-1)p + (p-1) \end{aligned}$$

Since  $p$  is prime,  $0 \leq p-1 < p$ , so

$$a_{k-1} = p-1, a_{k-2} = p-1, \dots, a_1 = p-1, a_0 = p-1$$

$\therefore$  Using  $n = p^k - 1$ , The formula in (a) becomes:

$$\frac{(p^{k-1}) - \left[ (p-1) + (p-1) + \dots + (p-1) \right]}{p-1}$$

$$= \frac{(p^{k-1}) - [k(p-1)]}{p-1}$$

(b). Determine The highest power of 3 dividing  $80!$  and The highest power of 7 dividing  $2400!$ .

(1)  $80 = 81 - 1 = 3^4 - 1$ , here  $k = 4, p = 3$

Using The formula in (a),  $\frac{(3^4 - 1) - [4(3-1)]}{3-1}$

$$= \frac{80 - 8}{2} = 36$$

$\therefore 3^{36} \mid 80!$ , 36 is the highest power of 3.

(2)  $2400 = 7^4 - 1$ , here  $k = 4, p = 7$

Using The formula in (a),  $\frac{(7^4 - 1) - [4(7-1)]}{7-1}$

$$= \frac{2400 - 24}{6} = 400 - 4 = 396$$

$\therefore 7^{396} \mid 2400!$ , 396 is the highest power of 7.

9. Find an integer  $n \geq 1$  s.t. The highest power of 5 contained in  $n!$  is 100.

Using problem #7, express  $n$  as a  $p$ -based number and use formula:  $\frac{n-r}{p-1}$ , where  $r = \sum a_i$  coefficients,  $r > 0$ .

$$\therefore 100 = \frac{n-r}{5-1} = \frac{n-r}{4}. \quad \therefore 400 = n-r$$

$$\text{If } r=1, n=401. \quad 401 = 3 \cdot 5^3 + 1 \cdot 5^2 + 1, \\ r=3+1+1=5$$

Because  $n$  must be  $\geq 400$ , for  $a_3 \cdot 5^3$ ,  $a_3=3$ .  
 $\therefore r$  must be at least 3.

$$\text{Try } n=404, \quad 404 = 3 \cdot 5^3 + 1 \cdot 5^2 + 4, \\ r=3+1+4=8$$

$$\text{Try } n=405, \quad 405 = 3 \cdot 5^3 + 1 \cdot 5^2 + 1 \cdot 5 + 0 \\ r=3+1+1=5$$

$\therefore$  When  $n=405$ , highest power of 5 dividing  $405!$  is 100.

10. Given a positive integer  $N$ , show the following:

$$(a) \sum_{n=1}^N \mu(n) \left[ \frac{N}{n} \right] = 1$$

Pf: Let  $F(n) = \sum_{d|n} \mu(d)$

By Th. 6.C,  $F(n) = 1$  if  $n=1$ ,  $F(n)=0$ ,  $n>1$ .

By Th. 6.II,  $\sum_{k=1}^N F(k) = \sum_{n=1}^N \mu(n) \left[ \frac{N}{n} \right]$

But  $\sum_{k=1}^N F(k) = F(1) + F(2) + \dots + F(N)$   
 $= 1 + 0 + \dots + 0$   
 $= 1$

$$\therefore \sum_{n=1}^N \mu(n) \left[ \frac{N}{n} \right] = 1$$

$$(b) \left| \sum_{n=1}^N \frac{\mu(n)}{n} \right| \leq 1$$

Pf: From Professor David M. Burton

From (a),  $\sum_{n=1}^{N-1} \mu(n) \left[ \frac{N}{n} \right] + \mu(N) \left[ \frac{N}{N} \right] = 1$

But  $\left[ \frac{N}{N} \right] = 1$ , so  $\sum_{n=1}^{N-1} \mu(n) \left[ \frac{N}{n} \right] + \mu(N) = 1$

Dividing by  $N$ ,

$$\frac{\mu(N)}{N} = \frac{1}{N} - \frac{1}{N} \sum_{n=1}^{N-1} \mu(n) \left[ \frac{N}{n} \right] \quad [1]$$

$$\begin{aligned} \text{Now, } \sum_{n=1}^N \frac{\mu(n)}{n} &= \sum_{n=1}^{N-1} \frac{\mu(n)}{n} + \frac{\mu(N)}{N} \\ &= \frac{1}{N} \sum_{n=1}^{N-1} \mu(n) \frac{N}{n} + \frac{\mu(N)}{N} \quad [2] \end{aligned}$$

Substituting [1] into [2],

$$\begin{aligned} \sum_{n=1}^N \frac{\mu(n)}{n} &= \frac{1}{N} \sum_{n=1}^{N-1} \mu(n) \frac{N}{n} + \frac{1}{N} - \frac{1}{N} \sum_{n=1}^{N-1} \mu(n) \left[ \frac{N}{n} \right] \\ &= \frac{1}{N} \sum_{n=1}^{N-1} \mu(n) \left( \frac{N}{n} - \left[ \frac{N}{n} \right] \right) + \frac{1}{N} \end{aligned}$$

Since  $|a+b| \leq |a| + |b|$ , and  $0 \leq \left| \frac{N}{n} - \left[ \frac{N}{n} \right] \right| < 1$ ,  
and  $\left| \frac{1}{N} \right| = \frac{1}{N}$ , and  $|a \cdot b| = |a| \cdot |b|$ ,

$$\begin{aligned} \left| \sum_{n=1}^N \frac{\mu(n)}{n} \right| &\leq \frac{1}{N} \sum_{n=1}^{N-1} |\mu(n)| \left| \frac{N}{n} - \left[ \frac{N}{n} \right] \right| + \frac{1}{N} \\ &\leq \frac{1}{N} \sum_{n=1}^{N-1} |\mu(n)| + \frac{1}{N} \quad (\text{and } |\mu(n)| \leq 1) \\ &\leq \frac{1}{N} (N-1) + \frac{1}{N} = 1 \end{aligned}$$

11. Illustrate problem 10 when  $N=6$

$$(1) \sum_{n=1}^6 \mu(n) \left\lceil \frac{6}{n} \right\rceil = \mu(1) \left\lceil \frac{6}{1} \right\rceil + \mu(2) \left\lceil \frac{6}{2} \right\rceil + \\ \mu(3) \left\lceil \frac{6}{3} \right\rceil + \mu(4) \left\lceil \frac{6}{4} \right\rceil + \mu(5) \left\lceil \frac{6}{5} \right\rceil + \mu(6) \left\lceil \frac{6}{6} \right\rceil$$

$$= 1 \cdot 6 + (-1) \cdot 3 + (-1) \cdot 2 + 0 \cdot 1 + (-1) \cdot 1 + 1 \cdot 1$$

$$= 6 - 3 - 2 + 0 - 1 + 1$$

$$= 1$$

$$(2) \left| \sum_{n=1}^6 \frac{\mu(n)}{n} \right| = \left| \frac{\mu(1)}{1} + \frac{\mu(2)}{2} + \frac{\mu(3)}{3} + \frac{\mu(4)}{4} + \frac{\mu(5)}{5} + \frac{\mu(6)}{6} \right| \\ = \left| 1 + \left(-\frac{1}{2}\right) + \left(-\frac{1}{3}\right) + \frac{0}{4} + \left(-\frac{1}{5}\right) + \frac{1}{6} \right| \\ = \left| 1 + \left(-\frac{5}{6}\right) + \left(-\frac{1}{5}\right) + \frac{1}{6} \right| \\ = \left| 1 + \left(-\frac{2}{3}\right) + \left(-\frac{1}{5}\right) \right| \\ = \left| 1 + \left(-\frac{13}{15}\right) \right| = \left| \frac{2}{15} \right| < 1$$

12. Verify That The formula  $\sum_{n=1}^N \lambda(n) \left[ \frac{N}{n} \right] = \lfloor \sqrt{N} \rfloor$   
 hold for any positive integer  $N$ .

Pf: Let  $F(n) = \sum_{d|n} \lambda(d)$  ( $\lambda$ -function defined on page 116, # 7, Sec. 6.2).

$$\therefore \text{By Th. 6.11, } \sum_{n=1}^N F(n) = \sum_{n=1}^N \lambda(n) \left[ \frac{N}{n} \right]$$

By Prob. # 7(6), Sec. 6.2,

$$F(n) = \begin{cases} 1 & \text{if } n = m^2 \text{ for some integer } m \\ 0 & \text{otherwise} \end{cases}$$

$\therefore \sum_{n=1}^N F(n)$  keeps track of the number of perfect

squares  $\leq N$ , as  $F()$  assigns a value of 1 to each  $n$  that can be expressed as a perfect square.

$$\therefore \sum_{n=1}^N \lambda(n) \left[ \frac{N}{n} \right] = \# \text{ perfect squares } \leq N.$$

Now consider  $\lfloor \sqrt{N} \rfloor$  and perfect squares.  
 The perfect squares are  $1^2, 2^2, 3^2, \dots$

$\therefore$  For any  $N = m^2$ , There are exactly  $m$  perfect squares (positive integers) less than or equal to  $N$ .

Suppose  $\sqrt{N}$  is not an integer.

Let  $m$  be the largest integer s.t.

$$m^2 < N$$

$$\therefore N < (m+1)^2$$

$$\therefore m < \sqrt{N} < m+1$$

Since  $m = \lfloor \sqrt{N} \rfloor$ , Then  $\lfloor \sqrt{N} \rfloor$  is the number of perfect squares  $\leq N$ .

$$\therefore \sum_{n=1}^N \lambda(n) \left[ \frac{N}{n} \right] = \lfloor \sqrt{N} \rfloor$$

13. If  $N$  is a positive integer, establish the following:

$$(a) N = \sum_{n=1}^{2N} \tau(n) - \sum_{n=1}^N \left\lfloor \frac{2N}{n} \right\rfloor$$

By Corollary 1 to Th. 6.11,  $\sum_{n=1}^N \tau(n) = \sum_{n=1}^N \left[ \frac{N}{n} \right]$

$$\therefore \sum_{n=1}^{2N} \tau(n) = \sum_{n=1}^{2N} \left[ \frac{2N}{n} \right]$$

$$\begin{aligned}
 & \therefore \sum_{n=1}^{2N} \tau(n) - \sum_{n=1}^N \left\lceil \frac{2N}{n} \right\rceil \\
 & = \sum_{n=1}^{2N} \left\lceil \frac{2N}{n} \right\rceil - \sum_{n=1}^N \left\lceil \frac{2N}{n} \right\rceil \\
 & = \sum_{n=N+1}^{2N} \left\lceil \frac{2N}{n} \right\rceil
 \end{aligned}$$

But  $1 \leq \frac{2N}{N+k} < 2$  for all  $1 \leq k \leq N$

$$\begin{aligned}
 \text{Pf: } k \leq N & \Rightarrow N+k \leq N+N = 2N \\
 \therefore 1 & \leq \frac{2N}{N+k}
 \end{aligned}$$

$$\begin{aligned}
 \text{Also, } 1 \leq k & \Rightarrow 0 < k \Rightarrow 0 < 2k \\
 \therefore 2N & < 2N + 2k = 2(N+k) \\
 \therefore \frac{2N}{N+k} & < 2
 \end{aligned}$$

$$\therefore \left\lceil \frac{2N}{n} \right\rceil = 1 \text{ for all } N+1 \leq n \leq 2N$$

$$\therefore \sum_{n=N+1}^{2N} \left\lceil \frac{2N}{n} \right\rceil = N \cdot 1 = N$$

$$\therefore \sum_{n=1}^{2N} \tau(n) - \sum_{n=1}^N \left\lceil \frac{2N}{n} \right\rceil = N$$

$$(6) \quad \tau(N) = \sum_{n=1}^N \left( \left\{ \frac{N}{n} \right\} - \left[ \frac{N-1}{n} \right] \right)$$

By Corollary 1 to Th. G.11,

$$\sum_{n=1}^N \left\{ \frac{N}{n} \right\} = \sum_{n=1}^N \tau(n)$$

$$\begin{aligned} \therefore \sum_{n=1}^N \left[ \frac{N-1}{n} \right] &= \sum_{n=1}^{N-1} \left[ \frac{N-1}{n} \right] + \left[ \frac{N-1}{N} \right] \\ &= \sum_{n=1}^{N-1} \tau(n) + \left[ \frac{N-1}{N} \right] \end{aligned}$$

But  $\frac{N-1}{N} < 1$  for all  $N > 0$ .  $\therefore \left[ \frac{N-1}{N} \right] = 0$

$$\therefore \sum_{n=1}^N \left[ \frac{N-1}{n} \right] = \sum_{n=1}^{N-1} \tau(n)$$

$$\therefore \sum_{n=1}^N \left( \left\{ \frac{N}{n} \right\} - \left[ \frac{N-1}{n} \right] \right) = \sum_{n=1}^N \tau(n) - \sum_{n=1}^{N-1} \tau(n)$$

$$= \tilde{\tau}(N)$$

## 6.4 An Application to the Calendar

Note Title

8/11/2005

1. Find The number  $n$  of leap years s.t.  $1600 < n < Y$ , for  
(a)  $Y = 1825$  ( $c = 18, y = 25$ )

$$L = 24c + \left\lfloor \frac{c}{4} \right\rfloor + \left\lfloor \frac{Y}{4} \right\rfloor - 388,$$

$$= 24(18) + \left\lfloor \frac{18}{4} \right\rfloor + \left\lfloor \frac{25}{4} \right\rfloor - 388$$

$$= 432 + 4 + 6 - 388 = \underline{\underline{54}}$$

(b)  $Y = 1950$  ( $c = 19, y = 50$ )

$$L = 24c + \left\lfloor \frac{c}{4} \right\rfloor + \left\lfloor \frac{Y}{4} \right\rfloor - 388$$

$$= 24(19) + \left\lfloor \frac{19}{4} \right\rfloor + \left\lfloor \frac{50}{4} \right\rfloor - 388$$

$$= 456 + 4 + 12 - 388 = \underline{\underline{84}}$$

(c)  $Y = 2075$  ( $c = 20, y = 75$ )

$$L = 24c + \left\lfloor \frac{c}{4} \right\rfloor + \left\lfloor \frac{Y}{4} \right\rfloor - 388$$

$$= 24(20) + \left\lfloor \frac{20}{4} \right\rfloor + \left\lfloor \frac{75}{4} \right\rfloor - 388$$

$$= 480 + 5 + 18 - 388 = \underline{\underline{115}}$$

2. Determine the day of the week for which you were born.

Jan. 12, 1952.  $c = 19$ ,  $y = 51$ ,  $m = 11$ ,  $d = 12$

$$\begin{aligned} w &\equiv d + \left\lfloor (2.6)m - 0.2 \right\rfloor - 2c + y + \left\lfloor \frac{c}{4} \right\rfloor + \left\lfloor \frac{y}{4} \right\rfloor \pmod{7} \\ &= 12 + \left\lfloor 2.6(11) - 0.2 \right\rfloor - 2(19) + 51 + \left\lfloor \frac{19}{4} \right\rfloor + \left\lfloor \frac{51}{4} \right\rfloor \pmod{7} \\ &= 12 + 28 - 38 + 51 + 4 + 12 \pmod{7} \\ &= 69 = 9 \cdot 7 + 6 \equiv 6 \pmod{7} \quad 6 \Rightarrow \underline{\text{Sat}} \end{aligned}$$

3. Find the day of the week for the important dates:

(a) November 19, 1863 (Lincoln's Gettysburg Address).

$$\begin{aligned} w &\equiv d + \left\lfloor 2.6m - 0.2 \right\rfloor - 2c + y + \left\lfloor \frac{c}{4} \right\rfloor + \left\lfloor \frac{y}{4} \right\rfloor \pmod{7} \\ &= 19 + \left\lfloor 2.6(9) - 0.2 \right\rfloor - 2(18) + 63 + \left\lfloor \frac{18}{4} \right\rfloor + \left\lfloor \frac{63}{4} \right\rfloor \\ &= 19 + 23 - 36 + 63 + 4 + 15 = 88 = 7 \cdot 12 + 4 \\ &\equiv 4 \pmod{7} \Rightarrow \underline{\text{Thu}} \end{aligned}$$

(b) April 18, 1906 (S.F. earthquake)

$$w \equiv d + [2.6m - 0.2] - 2c + y \left[ \frac{c}{4} \right] + \left[ \frac{y}{4} \right] \pmod{7}$$

$$= 18 + [2.6(2) - 0.2] - 2(19) + 6 + \left[ \frac{19}{4} \right] + \left[ \frac{6}{4} \right]$$

$$= 18 + 5 - 38 + 6 + 4 + 1 = -4 \equiv 3 \pmod{7} \Rightarrow \underline{\text{Wed}}$$

(c) Nov. 11, 1918 (Great War ends)

$$w \equiv 11 + [2.6(9) - 0.2] - 2(19) + 18 + \left[ \frac{19}{4} \right] + \left[ \frac{18}{4} \right]$$

$$= 11 + 23 - 38 + 18 + 4 + 4 = 22 \equiv 1 \pmod{7} \Rightarrow \underline{\text{Mon}}$$

(d) Oct. 24, 1929 (N.Y. stock market crash)

$$w \equiv 24 + [2.6(8) - 0.2] - 2(19) + 29 + \left[ \frac{19}{4} \right] + \left[ \frac{29}{4} \right]$$

$$= 24 + 20 - 38 + 29 + 4 + 7 = 46 \equiv 4 \pmod{7}$$

$\Rightarrow \underline{\text{Thu}}$

(e) June 6, 1944 (D-Day, Allies land in Normandy)

$$w \equiv 6 + [2.6(4) - 0.2] - 2(19) + 44 + \left[ \frac{19}{4} \right] + \left[ \frac{44}{4} \right]$$

$$= 6 + 10 - 38 + 44 + 4 + 11 = 37 \equiv 2 \pmod{7}$$

$\Rightarrow \underline{\text{Tue}}$

(f) Feb. 15, 1898 (Battleship Maine blown up).

$$w \equiv 15 + [2.6(12) - 0.2] - 2(18) + 97 + \left[ \frac{18}{4} \right] + \left[ \frac{87}{4} \right]$$

$$= 15 + 31 - 36 + 97 + 4 + 24 = 135 = 7 \cdot 19 + 2$$

$\equiv 2 \pmod{7} \Rightarrow \underline{\text{Tue}}$

4. Show that days with the identical calendar date in the years 1999 and 1915 fell on the same day of the week.

Pf: Let  $w_1$  = weekday for any day in 1915

$w_2$  = weekday for any day in 1999

The months and days will be the same.

$\therefore$  For 1915:

$$w_1 \equiv d + [2.6m - 0.2] - 2(19) + 15 + \left[ \frac{9}{4} \right] + \left[ \frac{15}{4} \right]$$

$$\equiv d + [2.6m - 0.2] - 38 + 15 + 4 + 3$$

$$\equiv d + [2.6m - 0.2] - 16 \pmod{7}$$

$$\equiv d + [2.6m - 0.2] + 5 \pmod{7}$$

For 1999:

$$w_2 \equiv d + [2.6m - 0.2] - 2(19) + 99 + \left[ \frac{1}{4} \right] + \left[ \frac{99}{4} \right]$$

$$\equiv d + [2.6m - 0.2] - 38 + 99 + 4 + 24$$

$$\equiv d + [2.6m - 0.2] + 89 \pmod{7}$$

$$\equiv d + [2.6m - 0.2] + 5 \pmod{7}$$

$$\therefore w_1 - w_2 \equiv 0 \pmod{7}, \text{ or } w_1 \equiv w_2 \pmod{7}$$

5. For the year 2010, determine the following:

(a) The calendar dates on which Mondays will occur in March.

Monday  $\Rightarrow 1$ , so

$$1 \equiv d + [2.6(1) - 0.2] - 2(20) + 10 + \left[ \frac{20}{4} \right] + \left[ \frac{10}{4} \right]$$

$$= d + 2 - 40 + 10 + 5 + 2 = d - 21 \pmod{7}$$

$$\therefore 22 \equiv d \pmod{7}, \text{ or } 1 \equiv d \pmod{7}$$

$\therefore$  March 1, 8, 15, 22, and 29 will all be Mondays in 2010

(6) The months in which the 13<sup>th</sup> will fall on Fri.

Friday  $\Rightarrow 5$ , so

$$5 \equiv 13 + [2.6m - 0.2] - 2(20) + 10 + \left\lceil \frac{20}{4} \right\rceil + \left\lceil \frac{10}{9} \right\rceil$$

$$= [2.6m - 0.2] + 13 - 40 + 10 + 5 + 2$$

$$= [2.6m - 0.2] - 10 \pmod{7}$$

$$\therefore 15 \equiv 1 \equiv [2.6m - 0.2] \pmod{7}$$

$m = 1, 2, \dots, 9, 10$ ,  $[2.6m - 0.2]$  becomes

2, 5, 7, 10, 12, 15, 18, 20, 23, 25

$\pmod{7}$ . These values are 2, 7, 0, 3, 5, 1, 4, 6, 2, 4

$\therefore$  When  $m = 6$ ,  $[2.6m - 0.2] \equiv 1 \pmod{7}$

$m = 6 \Rightarrow$  August, so August 2010 will contain a Friday 13.

Now must check Jan + Feb 2010,  
which are in year 2009 for the formula.

$$S \equiv 13 + [2.6m - 0.2] - 2(20) + 9 + \left[ \frac{20}{4} \right] + \left[ \frac{9}{4} \right]$$

$$= [2.6m - 0.2] - 40 + 9 + 5 + 2$$

$$= [2.6m - 0.2] - 24 \pmod{7}$$

$$\therefore 29 \equiv 1 \equiv [2.6m - 0.2] \pmod{7}$$

For  $m = 11, 12$ ,  $[2.6m - 0.2] = 28, 31$

And  $28 \not\equiv 1$  and  $31 \not\equiv 1 \pmod{7}$ , so  
Jan, Feb. contain no Fri. 13 for 2010.

$\therefore$  For 2010, August is only month with Fri. 13

6. Find the years in the decade 2000 to 2009  
when Nov. 29 is on a Sunday.

$$\text{Nov.} \Rightarrow m = 9, \text{ Sunday} \Rightarrow w = 0$$

$$\therefore 0 \equiv 29 + [2.6(9) - 0.2] - 2(20) + y + \left[ \frac{20}{4} \right] + \left[ \frac{y}{4} \right]$$

$$= 29 + 23 - 40 + r + 5 + \left\{ \frac{y}{4} \right\}$$

$$= 17 + y + \left\{ \frac{y}{4} \right\}$$

$$\therefore 4 \equiv y + \left\{ \frac{y}{4} \right\} \pmod{7}, \quad 0 \leq y \leq 9$$

For  $y = 0, 1, 2, 3, 4, 5, 6, 7, 8 \quad 4 \not\equiv y + \left\{ \frac{y}{4} \right\} \pmod{7}$

For  $y = 9, \quad y + \left\{ \frac{y}{4} \right\} = 11 \equiv 4 \pmod{7}$

$\therefore$  Nov. 29 is a Sunday only for 2009.

## 7.2 Euler's Phi-Function

Note Title

10/3/2005

1. Calculate  $\phi(1001)$ ,  $\phi(5040)$ ,  $\phi(36,000)$

$$\phi(1001) : 1001 = 7 \times 11 \times 13$$

$$\therefore \phi(1001) = 1001 \left(1 - \frac{1}{7}\right) \left(1 - \frac{1}{11}\right) \left(1 - \frac{1}{13}\right)$$

$$= 1001 \left(\frac{6}{7}\right) \left(\frac{10}{11}\right) \left(\frac{12}{13}\right)$$

$$= (6)(10)(12) = \underline{\underline{720}}$$

$$\phi(5040) : 5040 = 2^4 \cdot 3^2 \cdot 5 \cdot 7$$

$$\therefore \phi(5040) = 5040 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{3}\right) \left(1 - \frac{1}{5}\right) \left(1 - \frac{1}{7}\right)$$

$$= \frac{5040}{2 \cdot 10} (2)(4)(6) = \underline{\underline{1152}}$$

$$\phi(36,000) : 36,000 = 2^5 \cdot 3^2 \cdot 5^3$$

$$\therefore \phi(36,000) = 36000 \left(\frac{1}{2}\right) \left(\frac{2}{3}\right) \left(\frac{4}{5}\right)$$

$$= 36000 \left(\frac{4}{15}\right) = \underline{\underline{9600}}$$

2. Verify  $\phi(n) = \phi(n+1) = \phi(n+2)$  is true for  $n = 5186$

$$5186 = 2 \cdot 2593 \quad \phi(5186) = 5186 \left(\frac{1}{2}\right) \left(\frac{2592}{2593}\right) = 2592$$

$$5187 = 3 \cdot 7 \cdot 13 \cdot 19 \quad \phi(5187) = 5187 \left(\frac{2}{3}\right) \left(\frac{6}{7}\right) \left(\frac{12}{13}\right) \left(\frac{18}{19}\right) = 2592$$

$$5188 = 2^2 \cdot 1297 \quad \phi(5188) = 5188 \left(\frac{1}{2}\right) \left(\frac{1296}{1297}\right) = 2592$$

3. Show that  $m = 3^k \cdot 568$  and  $n = 3^k \cdot 638$ ,  $k \geq 0$   
 satisfy simultaneously  $\tilde{\tau}(m) = \tilde{\tau}(n)$ ,  $\tilde{\sigma}(m) = \tilde{\sigma}(n)$ , and  
 $\phi(m) = \phi(n)$

$$568 = 2^3 \cdot 71 \quad 638 = 2 \cdot 11 \cdot 29$$

$$\therefore \tilde{\tau}(m) = (k+1)(3+1)(1+1) = 6(k+1)$$

$$\tilde{\tau}(n) = (k+1)(1+1)(1+1)(1+1) = 6(k+1)$$

$$\begin{aligned} \tilde{\sigma}(m) &= \frac{(3^{k+1}-1)}{(3-1)} \cdot \frac{(2^4-1)}{(2-1)} \cdot \frac{(71^2-1)}{(71-1)} = \frac{(3^{k+1}-1)(15)(5040)}{(2)(70)} \\ &= (3^{k+1}-1)(540) \end{aligned}$$

$$\begin{aligned} \tilde{\sigma}(n) &= \frac{(3^{k+1}-1)}{(3-1)} \cdot \frac{(2^2-1)}{(2-1)} \cdot \frac{(11^2-1)}{(11-1)} \cdot \frac{(29^2-1)}{(29-1)} \\ &= \frac{(3^{k+1}-1)}{2} \cdot (3)(12)(30) \end{aligned}$$

$$= (3^{k+1}-1) \cdot (3)(12)(30) = (3^{k+1}-1)(540)$$

$$\begin{aligned}\phi(n) &= 3^k \cdot 568 \left(1 - \frac{1}{3}\right) \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{71}\right) \\ &= 3^k \cdot 2^3 \cdot 71 \left(\frac{2}{3}\right) \left(\frac{1}{2}\right) \left(\frac{20}{71}\right) \\ &= 3^{k-1} \cdot 2^3 \cdot 70 = 560 \cdot 3^{k-1}\end{aligned}$$

$$\begin{aligned}\phi(n) &= 3^k \cdot 638 \left(1 - \frac{1}{3}\right) \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{11}\right) \left(1 - \frac{1}{29}\right) \\ &= 3^k \cdot 2 \cdot 11 \cdot 29 \left(\frac{2}{3}\right) \left(\frac{1}{2}\right) \left(\frac{10}{11}\right) \left(\frac{28}{29}\right) \\ &= 3^{k-1} \cdot 20 \cdot 28 = 560 \cdot 3^{k-1}\end{aligned}$$

4. Establish each of the assertions below:

(a) If  $n$  is odd, then  $\phi(2n) = \phi(n)$

Pf: Let  $n = p_1^{k_1} \cdots p_r^{k_r}$ .  $n$  odd  $\Rightarrow p_1 \neq 2$

$$\therefore 2n = 2p_1^{k_1} \cdots p_r^{k_r}$$

$$\begin{aligned}\therefore \phi(2n) &= 2n \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_r}\right) \\ &= n \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_r}\right)\end{aligned}$$

$$= \phi(n)$$

Another proof:  $n$  odd  $\Rightarrow \gcd(2, n) = 1$   
 $\phi$  multiplicative  $\Rightarrow \phi(2n) = \phi(2)\phi(n) = \phi(n)$

(b) If  $n$  is even,  $\phi(2n) = 2\phi(n)$

$$\text{Pf: } n \text{ even} \Rightarrow n = 2^k p_2^{k_2} \cdots p_r^{k_r}$$

$$\therefore 2n = 2^{k+1} p_2^{k_2} \cdots p_r^{k_r}$$

$$\begin{aligned}\therefore \phi(2n) &= 2n \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_r}\right) \\ &= n \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_r}\right)\end{aligned}$$

$$\begin{aligned}2\phi(n) &= 2 \cdot n \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_r}\right) \\ &= n \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_r}\right)\end{aligned}$$

$$\therefore \phi(2n) = 2\phi(n)$$

(c)  $\phi(3n) = 3\phi(n) \Leftrightarrow 3|n$

$$\text{Let } n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$$

(1)  $3|n \Rightarrow$  one of  $p_i = 3$ .  $\therefore$  Let  $n = 3^k q$ , where  
 $\gcd(3, q) = 1$

$$\begin{aligned}\therefore 3\phi(n) &= 3\phi(3^k q) = 3\phi(3^k)\phi(q) \\ &= 3 \cdot 3^k \left(1 - \frac{1}{3}\right) \phi(q) = 2 \cdot 3^k \phi(q)\end{aligned}$$

$$\begin{aligned}\phi(3n) &= \phi(3^{k+1}q) = \phi(3^{k+1})\phi(q) \\ &= 3^{k+1} \left(1 - \frac{1}{3}\right) \phi(q) = 2 \cdot 3^k \phi(q)\end{aligned}$$

$$\therefore \phi(3n) = 3\phi(n)$$

(2) Suppose  $\phi(3n) = 3\phi(n)$

If  $3 \nmid n$ , Then for  $n = p_1^{k_1} \cdots p_r^{k_r}$ ,  $p_i \neq 3$

$$\begin{aligned}\therefore \gcd(3, n) &= 1 \Rightarrow \phi(3n) = \phi(3)\phi(n) \\ &= 2\phi(n)\end{aligned}$$

This contradicts  $\phi(3n) = 3\phi(n)$ .

$$\therefore 3 \mid n$$

$$(d) \phi(3n) = 2\phi(n) \Leftrightarrow 3 \mid n$$

(1) As in (c)(2) above,  $3 \nmid n \Rightarrow \phi(3n) = 2\phi(n)$

(2) Suppose  $\phi(3n) = 2\phi(n)$

From (c) above, if  $3|n$ , Then

$$\phi(3n) = 3\phi(n). \therefore 3 \nmid n$$

(e)  $\phi(n) = n/2 \iff n = 2^k$  for some  $k \geq 1$

(1) If  $n = 2^k$ , Then  $\phi(n) = \phi(2^k) = 2^k(1 - \frac{1}{2})$

$$= 2^k(\frac{1}{2}) = n/2$$

(2) If  $\phi(n) = n/2$ , Then for  $n/2$  to be an integer,  $n$  must be even.

$\therefore$  Let  $n = 2^k p_2^{k_2} \cdots p_r^{k_r}$ , and assume  $k \neq 0$

Let  $q = p_2^{k_2} \cdots p_r^{k_r}$ , so  $q > 1$  and  $\gcd(2^k, q) = 1$

$$\therefore \phi(n) = \phi(2^k q) = \phi(2^k) \phi(q)$$

$$= 2^k(1 - \frac{1}{2}) \phi(q) = 2^{k-1} \phi(q)$$

$$\therefore \phi(n) = n/2 = 2^{k-1} \phi(q), n = 2^k \phi(q)$$

$$\therefore p_2^{k_2} \cdots p_r^{k_r} = \phi(7) = \phi(p_2^{k_2} \cdots p_r^{k_r})$$

$$= p_2^{k_2} \cdots p_r^{k_r} \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_r}\right)$$

$$\therefore p_2 \cdots p_r = (p_2 - 1) \cdots (p_r - 1)$$

$\therefore$  for each  $p_i$ ,  $p_i = (p_j - 1)$  for some  $j$ .

This is impossible if  $k_i \neq 0$ .  $\therefore k_i = 0$ ,

$$\therefore \text{for } n = 2^k p_2^{k_2} \cdots p_r^{k_r} = 2^k$$

5. Prove  $\phi(n) = \phi(n+2)$  is satisfied by  $n = 2(2p-1)$  whenever  $p$  and  $2p-1$  are both odd primes.

Pf:  $2p-1$  an odd prime  $\Rightarrow \gcd(2, 2p-1) = 1$ .

$$\begin{aligned} \therefore \phi(n) &= \phi(2) \phi(2p-1) = (2p-1) \left(1 - \frac{1}{2p-1}\right) \\ &= 2p-2 \end{aligned}$$

$$n+2 = 2(2p-1) + 2 = 4p, \text{ and } p \text{ odd prime}$$

$$\Rightarrow \gcd(4, p) = 1.$$

$$\begin{aligned}\therefore \phi(n+2) &= \phi(4)\phi(p) = 2 \cdot p\left(1 - \frac{1}{p}\right) \\ &= 2p-2\end{aligned}$$

$$\therefore \phi(n) = \phi(n+2)$$

G. Show there are infinitely many integers for which  $\phi(n)$  is a perfect square.

$$\text{Pf: for } k \geq 1, \phi(2^k) = 2^k \left(1 - \frac{1}{2}\right) = 2^{k-1}$$

If  $k$  is odd, then  $k-1$  is even.

Let  $k = 2m + 1$ , some  $m$

$$\therefore \phi(2^k) = \phi(2^{2m+1}) = 2^{2m+1-1} = 2^m = (2^m)^2$$

$(2^m)^2$  is a perfect square.

There are infinitely many odd integers,  
 $\therefore$  infinitely many  $n = 2^k$ ,  $k$  odd,  
and  $\phi(n)$  is a perfect square.

? Verify The following.

(a) For any positive integer  $n$ ,  $\frac{1}{2}\sqrt{n} \leq \phi(n) \leq n$ .

By def.,  $\phi(n) \leq n$

(1) If  $n=1$ ,  $\frac{1}{2}\sqrt{1} = \frac{1}{2}$ ,  $\phi(1)=1$ , so  $\frac{1}{2}\sqrt{n} < \phi(n)$

(2) If  $n=2$ , Then  $\phi(2)=1$ , and  $\therefore \frac{1}{2}\sqrt{2} < \phi(2)$

If  $n=2^k$ , for  $k \geq 1$ , Then  $\phi(2^k) = 2^{k-1}$

$\frac{1}{2}\sqrt{2^k} = 2^{-\frac{1}{2}} \cdot 2^{\frac{k}{2}} = 2^{\frac{k}{2}-\frac{1}{2}} < 2^{k-1}$ , as  $\frac{k}{2} < k$   
 $\therefore \frac{1}{2}\sqrt{n} < \phi(n)$

(3) If  $n=p^k$ ,  $p \geq 2$ ,  $k \geq 1$ , Then  $\phi(n)=p^{k-1}(p-1)$   
by Th. 7.1.

But for  $p \geq 2$ ,  $p^2 \geq 3p$ , so  $p^2+1 \geq 3p$ , so

$p^2-2p+1 \geq p$ ,  $\therefore (p-1)^2 \geq p$ ,  $p-1 \geq \sqrt{p}$

$\therefore p^{k-1}(p-1) \geq p^{k-1}\sqrt{p} \geq p^{\frac{k-1}{2}} \cdot p^{\frac{1}{2}} = p^{\frac{k}{2}}$

$\therefore \phi(p^k) \geq p^{\frac{k}{2}}$

$\therefore \phi(n) \geq \sqrt{n}$  if  $n=p^k$  and  $p \geq 3$

(4)  $\phi$  is multiplicative. Let  $n=2^k p_1^{k_1} \cdots p_r^{k_r}$ ,  
 $k \geq 0, k_i \geq 0$

$$\begin{aligned}
 \therefore \phi(n) &= \phi(2^k) \phi(p_1^{k_1}) \phi(p_2^{k_2}) \cdots \phi(p_r^{k_r}) \\
 &> \left(\frac{1}{2} \sqrt{2^k}\right) \left(\sqrt{p_1^{k_1}}\right) \left(\sqrt{p_2^{k_2}}\right) \cdots \left(\sqrt{p_r^{k_r}}\right) \text{ by (2), (3)} \\
 &= \frac{1}{2} \sqrt{2^k p_1^{k_1} \cdots p_r^{k_r}} \\
 &= \frac{1}{2} \sqrt{n}
 \end{aligned}$$

$$\therefore \frac{1}{2} \sqrt{n} < \phi(n)$$

(3) If  $n > 1$  has  $r$  distinct prime factors, Then  
 $\phi(n) \geq n/2^r$

$$\text{Let } n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$$

$$\therefore \phi(n) = n \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_r}\right)$$

$$\text{But } p_i \geq 2, \text{ so } \frac{1}{2} \geq \frac{1}{p_i}, -\frac{1}{p_i} \geq -\frac{1}{2},$$

$$\therefore \left(1 - \frac{1}{p_i}\right) \geq 1 - \frac{1}{2} = \frac{1}{2}$$

$$\therefore \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_r}\right) \geq \left(\frac{1}{2}\right) \cdots \left(\frac{1}{2}\right) = \frac{1}{2^r}$$

$$\therefore \phi(n) \geq n \cdot \frac{1}{2^r} = n/2^r$$

(c) If  $n > 1$  is composite, Then  $\phi(n) \leq n - \sqrt{n}$

Let  $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ ,  $p_1 < p_2 < \cdots < p_r$ ,  $k_i \geq 1$ .

$$= p_1(b), \text{ and } p_1 \leq b \Rightarrow p_1^2 \leq p_1 b \Rightarrow p_1 \leq \sqrt{n}$$

$$\therefore \frac{1}{\sqrt{n}} \leq \frac{1}{p_1}, \text{ or } \frac{\sqrt{n}}{n} \leq \frac{1}{p_1}, \text{ so } \sqrt{n} \leq \frac{n}{p_1}$$

$$\therefore -\frac{n}{p_1} \leq -\sqrt{n}$$

$$\phi(n) = n \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_r}\right)$$

$$\leq n \left(1 - \frac{1}{p_1}\right), \text{ since } 1 - \frac{1}{p_1} < 1$$

$$= n - \frac{n}{p_1} \leq n - \sqrt{n}$$

8. Prove if  $n$  has  $r$  distinct odd prime factors, then  $2^r \mid \phi(n)$

Pf: Let  $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ ,  $p_i > 2$

$$\therefore \phi(n) = p_1^{k_1-1}(p_1-1) p_2^{k_2-1}(p_2-1) \cdots p_r^{k_r-1}(p_r-1)$$

As each  $p_i$  is odd, let  $p_i = 2s_i + 1$ , some  $s_i$ .

$$\begin{aligned}\therefore \phi(n) &= p_1^{k_1-1} p_2^{k_2-1} \cdots p_r^{k_r-1} (2s_1)(2s_2) \cdots (2s_r) \\ &= 2^r p_1^{k_1-1} p_2^{k_2-1} \cdots p_r^{k_r-1} s_1 s_2 \cdots s_r \\ \therefore 2^r &\mid \phi(n)\end{aligned}$$

9. Prove the following:

(a) If  $n$  and  $n+2$  are twin primes, Then  
 $\phi(n+2) = \phi(n) + 2$

Pf: For any prime  $p$ ,  $\phi(p) = p-1$ .

$$\begin{aligned}\therefore \phi(n+2) &= (n+2)-1 = n+1 \\ \phi(n) &= n-1\end{aligned}$$

$$\therefore \phi(n)+2 = n-1+2 = n+1 = \phi(n+2)$$

(b) If  $p$  and  $2p+1$  are both odd primes, Then  
 $n = 4p$  satisfies  $\phi(n+2) = \phi(n) + 2$

Pf: Since  $p$  is odd, Then  $\gcd(4, p) = 1$ ,  
so  $\phi(n) = \phi(4p) = \phi(4) \cdot \phi(p) = 2 \cdot (p-1)$

$$\therefore \phi(n)+2 = 2 \cdot (p-1) + 2 = 2p$$

Since  $2p+1$  is prime,  $\phi(2p+1) = (2p+1) - 1 = 2p$   
 $\therefore \phi(n)+2 = \phi(n+2)$  for  $n=4p$

10. If every prime that divides  $n$  also divides  $m$ , establish that  $\phi(n \cdot m) = n \phi(m)$ .

Pf: Let  $p_1, p_2, \dots, p_r$  be all the primes of  $n$  that divide  $m$ .

$$\text{Let } n = p_1^{k_1} \cdots p_r^{k_r}$$

$$m = p_1^{j_1} \cdots p_r^{j_r} q_1^{m_1} \cdots q_s^{m_s}, \quad q_i \text{ prime}$$

so that  $q_i \neq p_j$ .

$$\therefore nm = p_1^{k_1+j_1} \cdots p_r^{k_r+j_r} q_1^{m_1} \cdots q_s^{m_s}$$

$$\phi(nm) = p_1^{k_1+j_1} \cdots p_r^{k_r+j_r} q_1^{m_1} \cdots q_s^{m_s} \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_r}\right) \left(1 - \frac{1}{q_1}\right) \cdots \left(1 - \frac{1}{q_s}\right)$$

$$= p_1^{j_1} \cdots p_r^{j_r} \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_r}\right) \left(1 - \frac{1}{q_1}\right) \cdots \left(1 - \frac{1}{q_s}\right) p_1^{k_1} \cdots p_r^{k_r}$$

$$= \phi(m) \cdot p_1^{k_1} \cdots p_r^{k_r} = \phi(m) \cdot n$$

11. (a) If  $\phi(n) \mid n-1$ , prove  $n$  is square-free.

Pf: Let  $n = p_1^{k_1} \cdots p_r^{k_r}$ , and assume  $n$  is not square-free, so that  $k_i \geq 2$  for some  $i$ .

$$\phi(n) = (p_1^{k_1} - p_1^{k_1-1}) \cdots (p_i^{k_i} - p_i^{k_i-1}) \cdots (p_r^{k_r} - p_r^{k_r-1})$$

Since  $k_i \geq 2$ ,  $k_i-1 \geq 1$ , so  $p_i \mid p_i^{k_i-1}(p_i-1)$

$$\therefore p_i \mid (p_i^{k_i} - p_i^{k_i-1}) \Rightarrow p_i \mid \phi(n)$$

By assumption,  $\phi(n) \mid n-1$ , so that

$p_i \mid n-1$ . Clearly  $p_i \mid n$ ,

$$\therefore p_i \mid n - (n-1) \Rightarrow p_i \mid 1, \text{ a contradiction.}$$

$\therefore k_i = 1$  for all  $i \Rightarrow n$  is square-free.

(b) Show that if  $n = 2^k$  or  $2^k 3^j$ ,  $k, j$  positive,  
Then  $\phi(n) \mid n$

Pf: If  $n = 2^k$ ,  $\phi(n) = 2^{k-1}$ , and  $k-1 \geq 0$   
since  $k > 0$ .  $\therefore \phi(n) \mid n$

If  $n = 2^k 3^j$ , Then  $\phi(n) = 2^k 3^j (1 - \frac{1}{2})(1 - \frac{1}{3})$

$$= 2^k 3^j \left(\frac{1}{2}\right) \left(\frac{2}{3}\right) = 2^k 3^{j-1} \text{ Since } j > 0,$$

$$j-1 \geq 0 \therefore \phi(n) | n .$$

12. If  $n = p_1^{k_1} \cdots p_r^{k_r}$ , derive the following inequalities:

$$(a) \sigma(n) \phi(n) \geq n^2 \left(1 - \frac{1}{p_1^2}\right) \cdots \left(1 - \frac{1}{p_r^2}\right)$$

$$\text{Pf: } \sigma(n) = \frac{p_1^{k_1+1}-1}{p_1-1} \cdots \frac{p_r^{k_r+1}-1}{p_r-1}$$

$$\phi(n) = p_1^{k_1-1}(p_1-1) \cdots p_r^{k_r-1}(p_r-1)$$

$$\therefore \sigma(n) \phi(n) = (p_1^{k_1+1}-1) p_1^{k_1-1} \cdots (p_r^{k_r+1}-1) p_r^{k_r-1} \\ = (p_1^{2k_1} - p_1^{k_1-1}) \cdots (p_r^{2k_r} - p_r^{k_r-1})$$

$$\text{But } p_i^{2k_i} - p_i^{k_i-1} = p_i^{2k_i} \left(1 - \frac{p_i^{k_i-1}}{p_i^{2k_i}}\right)$$

$$= (p_i^{k_i})^2 \left(1 - \frac{1}{p_i^{k_i+1}}\right)$$

$$\text{For } k_i \geq 1, p_i^{k_i+1} \geq p_i^2, \text{ so } \frac{1}{p_i^2} \geq \frac{1}{p_i^{k_i+1}}$$

$$\therefore -\frac{1}{p_i^{k_i+1}} \geq -\frac{1}{p_i^2}, \text{ so } 1 - \frac{1}{p_i^{k_i+1}} \geq 1 - \frac{1}{p_i^2}$$

$$\therefore p_i^{2k_i} - p_i^{k_i-1} \geq (p_i^{k_i})^2 \left(1 - \frac{1}{p_i^2}\right)$$

$$\begin{aligned} \therefore \sigma(n) \phi(n) &\geq (p_1^{k_1})^2 \left(1 - \frac{1}{p_1^2}\right) \cdots (p_r^{k_r})^2 \left(1 - \frac{1}{p_r^2}\right) \\ &= (p_1^{k_1} \cdots p_r^{k_r})^2 \left(1 - \frac{1}{p_1^2}\right) \cdots \left(1 - \frac{1}{p_r^2}\right) \\ &= n^2 \left(1 - \frac{1}{p_1^2}\right) \cdots \left(1 - \frac{1}{p_r^2}\right) \end{aligned}$$

$$\therefore \sigma(n) \phi(n) \geq n^2 \left(1 - \frac{1}{p_1^2}\right) \cdots \left(1 - \frac{1}{p_r^2}\right)$$

$$(6) T(n) \phi(n) \geq n$$

Pf: If  $2 \leq p$ , then  $\frac{1}{p} \leq \frac{1}{2}$ ,  $-\frac{1}{2} \leq -\frac{1}{p}$ ,  $\frac{1}{2} \leq 1 - \frac{1}{p}$

If  $1 \leq k$ , then  $2 \leq k+1$ , so  $2 \cdot \frac{1}{2} \leq (k+1)(1 - \frac{1}{p})$ ,  
or  $1 \leq (k+1)(1 - \frac{1}{p})$

$$\therefore \text{Let } n = p_1^{k_1} \cdots p_r^{k_r}, k_i \geq 1$$

$$\therefore T(n) \phi(n) = (k_1+1) \cdots (k_r+1) \cdot n \cdot \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_r}\right)$$

$$= n \cdot \left(1 - \frac{1}{p_1}\right)(k_1+1) \cdots \left(1 - \frac{1}{p_r}\right)(k_r+1)$$

$$\geq n \cdot 1 \cdots 1 = n$$

$$\therefore \tau(n) \phi(n) \geq n$$

13. Assuming That  $d|n$ , prove  $\phi(d) | \phi(n)$

Pf: Let  $n = p_1^{k_1} \cdots p_r^{k_r}$ . Then, by Th. 6.1,

$$d = p_1^{a_1} \cdots p_r^{a_r}, \text{ where } 0 \leq a_i \leq k_i$$

$$\text{Let } d = q_1^{\delta_1} \cdots q_s^{\delta_s}, \text{ where } q_i \in \{p_1, \dots, p_r\}$$

$$\text{and } 1 \leq \delta_i$$

$$\therefore \phi(d) = d \left(1 - \frac{1}{q_1}\right) \cdots \left(1 - \frac{1}{q_s}\right)$$

Since each  $q_i = p_j$ , some  $j$  s.t.  $1 \leq j \leq r$ ,

Then  $1 - \frac{1}{q_i} = 1 - \frac{1}{p_j}$ . Name This  $p_j$

$$p_j; \therefore 1 - \frac{1}{q_i} = 1 - \frac{1}{p_j}$$

$$\therefore \phi(d) = d \left(1 - \frac{1}{p_j}\right) \cdots \left(1 - \frac{1}{p_j}\right)$$

As each  $p_{j_i} \in \{p_1, \dots, p_r\}$ , Then

$$(1 - \frac{1}{p_{j_1}}) \cdots (1 - \frac{1}{p_{j_s}}) \mid (1 - \frac{1}{p_1}) \cdots (1 - \frac{1}{p_r})$$

Since  $d \mid n$ , Then

$$d(1 - \frac{1}{p_{j_1}}) \cdots (1 - \frac{1}{p_{j_s}}) \mid n(1 - \frac{1}{p_1}) \cdots (1 - \frac{1}{p_r})$$

$$\therefore \phi(d) \mid \phi(n)$$

14. Obtain the following two generalizations of Th. 7.2:

(a) For positive integers  $m$  and  $n$ ,  $d = \gcd(m, n)$ ,

$$\phi(m)\phi(n) = \phi(mn) \underbrace{\phi(d)}_{d}$$

Pf: (1) If  $m=1$  or  $n=1$ , Then  $d=1$ ,  $\phi(d)=1$ .  
and clearly  $\phi(m)\phi(n) = \phi(mn) \underbrace{\phi(d)}_{d}$

(2)  $\therefore$  Assume both  $m, n > 1$ .

If  $m=n$ , Then  $m=\gcd(m, n)$

$$\text{Let } m=n=p_1^{k_1} \cdots p_r^{k_r}, mn=p_1^{2k_1} \cdots p_r^{2k_r}$$

$$\begin{aligned}
\therefore \phi(mn) \frac{\phi(d)}{d} &= mn \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_r}\right) m \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_r}\right) \frac{m}{m} \\
&= mn \left(1 - \frac{1}{p_1}\right)^2 \cdots \left(1 - \frac{1}{p_r}\right)^2 \\
&= m \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_r}\right) n \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_r}\right) \\
&= \phi(m) \phi(n)
\end{aligned}$$

(3) Now assume  $m \neq n$ ,  $m, n > 1$ .

If  $\gcd(m, n) = 1$ , Then  $d = 1$ ,  $\phi(d) = 1$ ,

and  $\phi(m) \phi(n) = \phi(mn) \frac{\phi(d)}{d}$  by Th. 7.2.

(4) Assume  $m \neq n$ ,  $m, n > 1$ ,  $\gcd(m, n) > 1$ .

Let  $d = p_1^{k_1} \cdots p_r^{k_r}$ ,  $k_i \geq 1$ .

$m = p_1^{a_1} \cdots p_r^{a_r} q_1^{u_1} \cdots q_s^{u_s}$ ,  $a_i \geq k_i$ ,  $u_i \geq 0$

$n = p_1^{b_1} \cdots p_r^{b_r} w_1^{v_1} \cdots w_t^{v_t}$ ,  $b_i \geq k_i$ ,  $v_i \geq 0$

where  $p_i, q_i, w_i$  are prime, and  
 $p_i \neq w_j$ ,  $p_i \neq q_j$ ,  $p_i \neq w_j$ , for any  $i, j$ .

$$\therefore mn = P_1^{a_1+b_1} \cdots P_r^{a_r+b_r} q_1^{u_1} \cdots q_s^{u_s} w_1^{v_1} \cdots w_t^{v_t}$$

$$\therefore \frac{\phi(mn)}{d} = \left[ P_1^{a_1+b_1} \cdots P_r^{a_r+b_r} q_1^{u_1} \cdots q_s^{u_s} w_1^{v_1} \cdots w_t^{v_t} \right].$$

$$\left[ \left( 1 - \frac{1}{P_1} \right) \cdots \left( 1 - \frac{1}{P_r} \right) \left( 1 - \frac{1}{q_1} \right) \cdots \left( 1 - \frac{1}{q_s} \right) \left( 1 - \frac{1}{w_1} \right) \cdots \left( 1 - \frac{1}{w_t} \right) \right].$$

$$\left[ \frac{d}{d} \left( 1 - \frac{1}{P_1} \right) \cdots \left( 1 - \frac{1}{P_r} \right) \right]$$

$$= \left[ P_1^{a_1} \cdots P_r^{a_r} P_1^{b_1} \cdots P_r^{b_r} q_1^{u_1} \cdots q_s^{u_s} w_1^{v_1} \cdots w_t^{v_t} \right].$$

$$\left[ \left( 1 - \frac{1}{P_1} \right)^2 \cdots \left( 1 - \frac{1}{P_r} \right)^2 \left( 1 - \frac{1}{q_1} \right) \cdots \left( 1 - \frac{1}{q_s} \right) \left( 1 - \frac{1}{w_1} \right) \cdots \left( 1 - \frac{1}{w_t} \right) \right]$$

$$= \left[ P_1^{a_1} \cdots P_r^{a_r} \left( 1 - \frac{1}{P_1} \right) \cdots \left( 1 - \frac{1}{P_r} \right) \left( 1 - \frac{1}{q_1} \right) \cdots \left( 1 - \frac{1}{q_s} \right) \right].$$

$$\left[ P_1^{b_1} \cdots P_r^{b_r} \left( 1 - \frac{1}{P_1} \right) \cdots \left( 1 - \frac{1}{P_r} \right) \left( 1 - \frac{1}{w_1} \right) \cdots \left( 1 - \frac{1}{w_t} \right) \right]$$

$$= \phi(m) \phi(n)$$

Note if any  $u_i = 0$  or  $v_j = 0$ , some  $i$ , some  $j$ ,  
 Then The corresponding term  $\left( 1 - \frac{1}{u_i} \right)$  or  
 $\left( 1 - \frac{1}{v_j} \right)$  is not present.

(b) For positive integers  $m, n$ ,

$$\phi(m)\phi(n) = \phi(\gcd(m, n))\phi(\operatorname{lcm}(m, n))$$

Pf: If  $m=1$ , Then  $\gcd(m, n)=1$  and  $\operatorname{lcm}(m, n)=n$   
 $\therefore$  Clearly  $\phi(m)\phi(n) = \phi(\gcd(m, n))\cdot\phi(\operatorname{lcm}(m, n))$

Similar reasoning applies for  $n=1$ .

If  $\gcd(m, n)=1$ , Then  $\operatorname{lcm}(m, n)=mn$ ,  
and so the relation holds.

If  $m=n$ ,  $\gcd(m, n)=m=\operatorname{lcm}(m, n)$ , so  
the relation holds.

If  $\gcd(m, n)=m$ , Then  $\operatorname{lcm}(m, n)=n$ ,  
so the relation holds, and similarly for  
 $\gcd(m, n)=n$ .

$\therefore$  Assume  $m \neq n$ ,  $\gcd(m, n) > 1$ , and  
 $\gcd(m, n) \neq m$  or  $n$ .

$$\therefore \text{Let } d = \gcd(m, n) = p_1^{k_1} \cdots p_r^{k_r}, k_i \geq 1$$

$$m = p_1^{a_1} \cdots p_r^{a_r} q_1^{u_1} \cdots q_s^{u_s}, a_i \geq k_i, u_i \geq 0$$

$$n = p_1^{b_1} \cdots p_r^{b_r} w_1^{v_1} \cdots w_t^{v_t}, b_i \geq k_i, v_i \geq 0$$

with  $p_i, q_i, w_i$  prime,

$$p_i \neq q_j, 1 \leq i \leq r, 1 \leq j \leq s$$

$$p_i \neq w_j, 1 \leq i \leq r, 1 \leq j \leq t$$

$$q_i \neq w_j, 1 \leq i \leq r, 1 \leq j \leq t$$

and  $U_i \neq 0$  some  $i$ ,  $V_j \neq 0$  some  $j$  since  
 $\gcd(m, n) \neq m$  or  $n$ .

Since  $mn = \gcd(m, n) \cdot \text{lcm}(m, n)$ ,

$$\text{lcm}(m, n) = mn / \gcd(m, n)$$

$$= p_1^{a_1+b_1-k_1} \cdots p_r^{a_r+b_r-k_r} q_1^{u_1} \cdots q_s^{u_s} w_1^{v_1} \cdots w_t^{v_t}$$

where  $a_i + b_i - k_i \geq 0$  since  $a_i \geq k_i, b_i \geq k_i$

$$\therefore \phi(\gcd(m, n)) \cdot \phi(\text{lcm}(m, n)) = \left[ p_1^{k_1} \cdots p_r^{k_r} \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_r}\right) \right] \cdot$$

$$\left[ p_1^{a_1+b_1-k_1} \cdots p_r^{a_r+b_r-k_r} q_1^{u_1} \cdots q_s^{u_s} w_1^{v_1} \cdots w_t^{v_t} \right].$$

$$\begin{aligned}
 & \left[ \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_r}\right) \left(1 - \frac{1}{q_1}\right) \cdots \left(1 - \frac{1}{q_s}\right) \left(1 - \frac{1}{w_1}\right) \cdots \left(1 - \frac{1}{w_t}\right) \right] \\
 &= \left[ p_1^{a_1+b_1} \cdots p_r^{a_r+b_r} q_1^{u_1} \cdots q_s^{u_s} w_1^{v_1} \cdots w_t^{v_t} \right]. \\
 & \left[ \left(1 - \frac{1}{p_1}\right)^2 \cdots \left(1 - \frac{1}{p_r}\right)^2 \left(1 - \frac{1}{q_1}\right) \cdots \left(1 - \frac{1}{q_s}\right) \left(1 - \frac{1}{w_1}\right) \cdots \left(1 - \frac{1}{w_t}\right) \right] \\
 &= \left[ p_1^{a_1} \cdots p_r^{a_r} q_1^{u_1} \cdots q_s^{u_s} \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_r}\right) \left(1 - \frac{1}{q_1}\right) \cdots \left(1 - \frac{1}{q_s}\right) \right]. \\
 & \left[ p_1^{b_1} \cdots p_r^{b_r} w_1^{v_1} \cdots w_s^{v_s} \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_r}\right) \left(1 - \frac{1}{w_1}\right) \cdots \left(1 - \frac{1}{w_t}\right) \right]
 \end{aligned}$$

$$\phi(m) - \phi(n)$$

15. Prove The following:

(a) There are infinitely many  $n$  for which  $\phi(n) = n/3$ .

Pf: consider  $n = 2^i 3^j$ ,  $i, j \geq 1$

$$\therefore \phi(n) = n \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{3}\right) = n \left(\frac{1}{2}\right) \left(\frac{2}{3}\right) = n/3$$

(b) There are no integers  $n$  for which  $\phi(n) = n/4$ .

Pf:  $\phi(1) = 1, \phi(2) = 1, \phi(3) = 2, \phi(4) = 2$ .

So for  $n = 1, 2, 3, 4$ ,  $\phi(n) \neq n/4$ .

Assume  $n > 4$  and  $\phi(n) = n/4$ .

Let  $n = p_1^{k_1} \cdots p_r^{k_r}$ ,  $k_i \geq 1$

$$\therefore \phi(n) = n \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_r}\right) = n/4$$

$$\therefore \frac{(p_1-1)\cdots(p_r-1)}{p_1\cdots p_r} = \frac{1}{4}, \text{ or}$$

$$4(p_1-1)\cdots(p_r-1) = p_1\cdots p_r$$

If  $p_1 = 2$ , Then  $2(p_2-1)\cdots(p_r-1) = p_2\cdots p_r$

But  $p_2\cdots p_r$  is odd since  $p_2, \dots, p_r$  are all odd.

And  $2(p_2-1)\cdots(p_r-1)$  is even.

$\therefore$  Can't work for  $p_1 = 2$ .

And if all  $p_1, \dots, p_r$  are odd, so is  $p_1\cdots p_r$  and  $4(p_1-1)\cdots(p_r-1)$  is even.

$\therefore$  No such  $n$  exists.

16. Show that the Goldbach conjecture implies that for each even integer  $2n$  there exists integers  $n_1$  and  $n_2$  with  $\phi(n_1) + \phi(n_2) = 2n$

Pf: Goldbach conjecture says for any even integer greater than 4, there are two odd primes,  $n_1$  and  $n_2$ , s.t.  $n_1 + n_2 = \text{The even integer}$ .

Let  $2n+2$  be such an even integer, so that  $n_1 + n_2 = 2n+2$ ,  $n_1, n_2 = \text{odd primes}$ .

If  $n_1$  and  $n_2$  are both prime, then  $\phi(n_1) = n_1 - 1$ ,  $\phi(n_2) = n_2 - 1$

$$\therefore \phi(n_1) + \phi(n_2) = n_1 + n_2 - 2 = 2n+2-2=2n$$

And if  $2n = 4$ , choose  $n_1 = n_2 = 4$ , so that  $\phi(4) + \phi(4) = 2+2 = 4 = 2n$

If  $2n = 2$ , choose  $n_1 = n_2 = 1$ , so that  $\phi(1) + \phi(1) = 2$

17. Given a positive integer  $K$ , show:

(a) There are at most a finite number of integers  $n$  for which  $\phi(n) = K$ .

Pf: Need to find an integer,  $z$ , s.t. whenever  $n \geq z$ ,  $\phi(n) > k$ . Thus, There are at most a finite # of integers,  $1, 2, \dots, z-1$ , for which  $\phi(n)$  may be equal to  $k$ .

By problem 7(a) above, it was proved that  $\phi(n) > \frac{1}{2}\sqrt{n}$ , for all  $n$ .

$$\therefore \text{choose } z = 4k^2. \quad \therefore \phi(z) > \frac{1}{2}\sqrt{4k^2} = k$$

$\therefore$  For all integers  $n > 4k^2$ ,  $\phi(n) > k$

$\therefore$  There are at most  $n = 4k^2$  integers for which  $\phi(n)$  may be  $k$ .

Note: it was important in 7(a) to prove  $\phi(n) > \frac{1}{2}\sqrt{n}$ , not just  $\phi(n) \geq \frac{1}{2}\sqrt{n}$   
 " $\geq$ " does not give proper bound.

(b) If The equation  $\phi(n)=k$  has a unique solution, say  $n=n_0$ , Then  $4|n_0$ .

Pf: Suppose  $\phi(n_0)=k$ , and  $n_0$  is unique

If  $n_0$  is odd, Then by problem 4(a),

$\phi(2n_0) = \phi(n_0) = k$ , so that  $n_0$  is not unique.

$\therefore n_0$  is even, so  $n_0 = 2r$ , some  $r$ .

If  $r$  is odd, Then  $\gcd(2, r) = 1$ , so  
 $\phi(n_0) = \phi(2r) = \phi(2)\phi(r) = \phi(r) = k$ ,  
so, again, uniqueness of  $n_0 \Rightarrow r$  is  
even  $\Rightarrow r = 2s$ , some  $s$ .

$\therefore n_0 = 2(2s) = 4s \Rightarrow 4 \mid n_0$ .

18. Find all solutions  $\phi(n) = 16$  and  $\phi(n) = 24$

Note: if  $n = p_1^{k_1} \cdots p_r^{k_r}$ , Then  $\phi(n) = (p_1^{k_1} - p_1^{k_1-1}) \cdots (p_r^{k_r} - p_r^{k_r-1})$

Since  $(p_i - 1) \mid p_i^{k_i} - p_i^{k_i-1}$ , Then  $(p_i - 1) \mid \phi(n)$ ,

(a) For  $\phi(n) = 16$ ,  $(p_i - 1) \mid 2^4$

$\therefore p_i - 1 = 1, 2, 4, 8, \text{ or } 16$

$\therefore p_i = 2, 3, 5, 9, \text{ or } 17$ , and 9 not prime,  
so  $p_i = 2, 3, 5, \text{ or } 17$

$\therefore n = 2^{k_1} 3^{k_2} 5^{k_3} 17^{k_4}$

$$16 = (2^{k_1} - 2^{k_1-1})(3^{k_2} - 3^{k_2-1})(5^{k_3} - 5^{k_3-1})(17^{k_4} - 17^{k_4-1})$$

$$= 2^{k_1-1} \cdot (3^{k_2-1} \cdot 2) \cdot (5^{k_3-1} \cdot 4) \cdot (17^{k_4-1} \cdot 16)$$

16 clearly has an upper bound effect.  
 $\therefore k_4 \leq 1, k_3 \leq 1, k_2 \leq 3, k_1 \leq 5$

If  $k_4 = 1, 17^{k_4-1} \cdot 16 = 16$   
 $\therefore k_2 = k_3 = 0, k_1 = 0 \quad n = 17$   
or  $k_1 = 1 \quad n = 34$

$\therefore$  Consider cases for  $k_4 = 0$ .

$$\therefore 16 = 2^{k_1-1} \cdot (3^{k_2-1} \cdot 2)(5^{k_3-1} \cdot 4)$$

If  $k_3 = 1$ , Then  $k_2 = 1, k_1 = 2, n = 60$   
or  $k_2 = 0, k_1 = 3 \quad n = 40$

If  $k_3 = 0$ , Then  $k_2 = 1, k_1 = 4 \quad n = 48$   
or  $k_2 = 0, k_1 = 5 \quad n = 32$

$\therefore$  For  $\phi(n) = 16, n = 17, 34, 40, 60, 32, 48$

(5) For  $\phi(n) = 24, (\rho_i - 1) \mid 2^3 \cdot 3$

$$\therefore (\rho_i - 1) \mid 2^3 \text{ or } (\rho_i - 1) \mid 3$$

$$\therefore p_i - 1 = 1, 2, 4, 8 \quad \text{or} \quad p_i - 1 = 3, 6, 12, 24$$

$$\therefore p_i = 2, 3, 5 \quad \text{or} \quad p_i = 7, 13$$

$$\therefore n = 2^{k_1} 3^{k_2} 5^{k_3} 7^{k_4} 13^{k_5}$$

$$\therefore 24 = (2^{k_1-1})(3^{k_2-1}) (5^{k_3-1}) (7^{k_4-1}) (13^{k_5-1})$$

$$\therefore k_5 \leq 1, k_4 \leq 1, k_3 \leq 2, k_2 \leq 3, k_1 \leq 5$$

$$\text{For } k_5 = 1, k_3 = 0, k_4 = 0. \quad k_2 = 1, k_1 = 0 \quad n = 39$$

$$k_2 = 1, k_1 = 1 \quad n = 78$$

$$k_2 = 0, k_1 = 2 \quad n = 52$$

$$\therefore \text{Now assume } k_5 = 0 \quad (n = 2^{k_1} 3^{k_2} 5^{k_3} 7^{k_4})$$

$$\therefore 24 = (2^{k_1-1}) (3^{k_2-1}) (5^{k_3-1}) (7^{k_4-1})$$

$$\text{If } k_4 = 1, \quad 4 = (2^{k_1-1}) (3^{k_2-1}) (5^{k_3-1})$$

$$k_3 = 1, k_2 = 0, k_1 = 0 \quad n = 35$$

$$k_3 = 1, k_2 = 0, k_1 = 1 \quad n = 70$$

$$k_3 = 0, k_2 = 0, k_1 = 3 \quad n = 56$$

$$k_3 = 0, k_2 = 1, k_1 = 2 \quad n = 84$$

$$\text{Now assume } k_5 = 0, k_4 = 0 \quad (n = 2^{k_1} 3^{k_2} 5^{k_3})$$

$$\therefore 24 = (2^{k_1-1})(3^{k_2-1} \cdot 2)(5^{k_3-1} \cdot 4). \quad \therefore k_3 \leq 1$$

$$\therefore \text{If } k_3 = 1, \quad G = (2^{k_1-1})(3^{k_2-1} \cdot 2)$$

$$k_2 \neq 0, k_2 \neq 1$$

$$k_2 = 2, \quad k_1 = 0 \quad n = 45$$

$$k_2 = 2, \quad k_1 = 1 \quad n = 70$$

$$\therefore \text{Assume } k_5 = k_4 = k_3 = 0 \quad (n = 2^{k_1} 3^{k_2})$$

$$\therefore 24 = (2^{k_1-1})(3^{k_2-1} \cdot 2).$$

If  $k_2 = 0$ , no solution

If  $k_2 = 1$ , no solution

If  $k_2 = 2$ ,  $k_1 = 3 \quad n = 72$

If  $k_3 = 3$ , no solution

=

$\therefore$  For  $\phi(n) = 24$ ,

$$n = 39, 78, 52, 35, 70, 56, 84, 45, 90, 72$$

19. (a). Prove That The equation  $\phi(n) = 2p$ , where  $p$  is prime and  $2p+1$  is composite, is not solvable.

Pf: Let  $n = p_1^{k_1} \cdots p_r^{k_r}$ .

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

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

Suppose  $\phi(n) = 2p$  ( $2p+1$  is composite).  
Then  $p \neq 2$  as  $2p+1=5$ . Also,  $n \neq 1$ .

(a) Suppose  $n$  consists of more than one odd prime factor,  $p_j, p_k$ .

$$\therefore \text{In } \phi(n), (p_j-1)(p_k-1) = 2a_j \cdot 2a_k$$

$$\therefore \phi(n) = 2a_j \cdot 2a_k \cdot Q = 2p, \text{ where } Q = \text{other factors in } \phi(n)$$

$\therefore a_j \cdot 2a_k \cdot Q = p$ , so  $p$  is even  
 $\Rightarrow p=2$ . But  $2p+1=5$  is not composite.

$\therefore n$  can consist of at most one odd prime factor.

(b)  $\therefore$  Let  $n = 2^k p_1^{k_1}$ ,  $k \geq 0, k_1 \geq 0$

(i) Suppose  $k=0$ , so  $n = p_1^{k_1}$ ,  $k_1 > 0$

$$\therefore \phi(n) = p_1^{k_1-1} (p_1-1) = 2p$$

If  $k_1 = 1$ , Then  $p_1 - 1 = 2p$ ,  $p_1 = 2p + 1$ ,  
and  $2p + 1$  composite  $\Rightarrow p_1$  is not prime.

If  $k_1 > 1$ , Then let  $p_1 - 1 = 2r$

$$\therefore \phi(n) = p_1^{k_1-1} \cdot 2r = 2p,$$

$$p_1^{k_1-1} \cdot r = p \Rightarrow r = p_1 = p$$

$$\therefore p_1^{k_1-1} = 1 \Rightarrow k_1 = 1$$

$$\therefore \phi(n) = (p-1) = 2p, 0 = p+1.$$

$$\therefore k \neq 0, n = 2^k p_1^{k_1}, k > 0, k_1 \geq 0$$

(ii) Assume  $k = 1$

(1) If  $k_1 = 0$ , Then  $n = 2$ ,  $\phi(n) = 1 \neq 2p$

(2) If  $k_1 = 1$ , Then  $n = 2p_1$ ,  $\phi(n) = p_1 - 1$   
 $\therefore p_1 - 1 = 2p_1$ ,  $p_1 = 2p + 1 \Rightarrow p_1$  composite.

(3) If  $k_1 > 1$ , Then  $n = 2p_1^{k_1}$ ,

$$\phi(n) = p_1^{k_1-1} (p_1 - 1) = 2p$$

$$\text{Let } p_1 - 1 = 2r, \therefore p_1^{k_1-1} \cdot 2r = 2p,$$

$$\therefore p_1^{k_1-1} \cdot r = p \text{ prime} \Rightarrow r=1 \\ \text{and } k_1=2 \Rightarrow p_1=p.$$

$$\therefore n = 2p^2, \phi(n) = p(p-1) = 2p \\ \Rightarrow p-1 = 2, p=3 \Rightarrow 2p+1=7, \\ \text{which is not composite.}$$

$$\therefore (1), (2), (3) \Rightarrow k \neq 1$$

$$\therefore (i), (ii) \Rightarrow k > 1$$

$$(iii) \therefore n = 2^k p_1^{k_1}, k > 1, k_1 \geq 0$$

$$(1) \text{ If } k_1=0, n = 2^k, \phi(n) = 2^{k-1} = 2p \\ \therefore p=2 \Rightarrow 2p+1=5 \text{ is composite.}$$

$$(2) \text{ If } k_1=1, \text{ Then } n = 2^k p_1,$$

$$\therefore \phi(n) = 2^{k-1}(p_1-1) = 2p$$

$$\therefore 2^{k-2}(p_1-1) = p$$

Only possibility is  $p=2$  or  $p_1-1=p$   
 $p=2 \Rightarrow 2p+1=5$  is composite

$p_1 - 1 = p \Rightarrow p_1 = p + 1 \Rightarrow p_1$  is even  
and  $p_1$  is supposed to be odd.

$$(iv) \therefore n = 2^k p_1^{k_1}, k > 1, k_1 > 1$$

$$\therefore \phi(n) = 2^{k-1} p_1^{k_1-1} (p_1 - 1) = 2p$$

$$\Rightarrow p_1^{k_1-1} (p_1 - 1) = p$$

$p \neq 2$  as  $2p+1$  must be composite.

$\therefore p$  is odd but  $(p_1 - 1)$  is even, so  
 $p_1^{k_1-1} (p_1 - 1)$  is even.

$\therefore (i), (ii), (iii),$  and  $(iv) \Rightarrow$  There is no

$k, k_1$  s.t.  $n = 2^k p_1^{k_1}$ , with  $\phi(n) = 2p$   
and  $2p+1$  composite

==

(6) Prove There is no solution to the equation  
 $\phi(n) = 14$ , and That 14 is the smallest  
positive even integer with this property.

Pf: From (a)  $\phi(n) = 2 \cdot 7$ , and

$2(7)+1=15$  is composite.  
 $\therefore \phi(n)=14$  is not solvable.

$$\begin{aligned}\phi(13) &= 12, \quad \phi(11) = 10, \quad \phi(7) = 6, \\ \phi(5) &= 4, \quad \phi(3) = 2\end{aligned}$$

for  $\phi(n)=8$ , note if  $n=2^k$ ,  $\phi(n)=2^{k-1}$   
 $\therefore 2^3=8=2^{4-1}$ , so  $n=16$   
 $\therefore \phi(16)=8$

20. If  $p$  is prime and  $k \geq 2$ , show that

$$\phi(\phi(p^k)) = p^{k-2} \phi((p-1)^2)$$

Pf:  $\phi(p^k) = p^{k-1}(p-1)$

Since  $\gcd(p, p-1) = 1$ , Then  $\gcd(p^{k-1}, p-1) = 1$

$\phi$  is multiplicative,

$$\begin{aligned}\therefore \phi(\phi(p^k)) &= \phi(p^{k-1}(p-1)) \\ &= \phi(p^{k-1}) \phi(p-1) \\ &= p^{k-2}(p-1) \phi(p-1)\end{aligned}$$

From problem 10,  $\phi(n^2) = n\phi(n)$  for every positive integer  $n$ .

$$\therefore (\rho - 1)\phi(\rho - 1) = \phi((\rho - 1)^2)$$

$$\therefore \phi(\phi(\rho^k)) = \rho^{k-2}(\rho - 1)\phi(\rho - 1) = \rho^{k-2}\phi((\rho - 1)^2)$$

21. Verify that  $\phi(n)\tau(n)$  is a perfect square when  $n = 63457 = 23 \cdot 31 \cdot 89$ .

Pf: If  $n = p_1^{k_1} \cdots p_r^{k_r}$ , and  $k_i = 1$ , Then

$$\phi(n) = (p_1 - 1) \cdots (p_r - 1)$$

$$\tau(n) = \underbrace{(p_1^{k_1+1} - 1)}_{p_1 - 1} \cdots \underbrace{(p_r^{k_r+1} - 1)}_{p_r - 1}$$

$$\therefore \phi(n)\tau(n) = (p_1^2 - 1) \cdots (p_r^2 - 1) = (p_1 - 1)(p_1 + 1) \cdots (p_r - 1)(p_r + 1)$$

$\therefore$  for  $n = 23 \cdot 31 \cdot 89$ ,

$$\phi(n)\tau(n) = (23^2 - 1)(31^2 - 1)(89^2 - 1)$$

$$= (22)(24)(30)(32)(88)(90)$$

$$= (2 \cdot 11)(2^3 \cdot 3)(2 \cdot 3 \cdot 5)(2^5)(2^3 \cdot 11)(2 \cdot 3^2 \cdot 5)$$

$$= 2^4 \cdot 3^4 \cdot 5^2 \cdot 11^2$$

$$= (2^7 \cdot 3^2 \cdot 5 \cdot 11)^2$$

### 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  $a$ ,  $a^{37} \equiv a \pmod{1729}$

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

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

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

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

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

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

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

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

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

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

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

$$a^6 \equiv 1 \pmod{7} \Rightarrow a^{12} \equiv 1 \pmod{7}$$
$$a^{12} \equiv 1 \pmod{13}$$

$$\therefore a^{12} \equiv 1 \pmod{2 \cdot 3 \cdot 5 \cdot 7 \cdot 13} \quad [\text{prob. #13, Sec. 4.2}]$$
$$\therefore a^{13} \equiv a \pmod{2730}$$

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

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

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

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

$$\phi(30) = 8 \Rightarrow a^8 \equiv 1 \pmod{30}$$
$$\Rightarrow a^{32} \equiv 1 \pmod{30}$$

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

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

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

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

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

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

$$\phi(16) = 8, \therefore a^8 \equiv 1 \pmod{16}$$
$$\therefore a^{32} \equiv 1 \pmod{16}$$

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

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

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

2. Use Euler's Theorem to confirm that, for any integer  $n \geq 0$ ,

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

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

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

$$\therefore 10^{32n} \equiv 1 \pmod{51} \quad \Sigma 13$$

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

$$10 \equiv 7 \pmod{3}$$

$$10 \equiv 1 \pmod{3} \Rightarrow 10^8 \equiv 1 \pmod{3}$$

$$\therefore 10^9 = 10^8 \cdot 10 \equiv 1 \cdot 10 \equiv 7 \pmod{3}, \text{ or}$$

$$10^9 \equiv 7 \pmod{3} \quad [23]$$

$$-10 \equiv 7 \pmod{17}$$

$$\therefore (-10)^2 \equiv 7^2 = 49 \equiv -2 \pmod{17}$$

$$\therefore (-10)^8 = 10^8 \equiv (-2)^4 = 16 \equiv -1 \pmod{17}$$

$$\therefore 10^9 \equiv -10 \equiv 7 \pmod{17} \quad [3]$$

$$[23] + [3] \Rightarrow 10^9 \equiv 7 \pmod{51} \quad [43]$$

$$[13] + [43] \Rightarrow 10^{32n} \cdot 10^9 \equiv 1 \cdot 7 \pmod{51}, \text{ or}$$

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

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

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

$$\begin{aligned} \text{Pf: } a^{15} - a^3 &= a^3(a^{12}-1) = a^3(a^6+1)(a^6-1) \\ &= a^3(a^6+1)(a^5+1)(a^5-1) \\ &= a^3(a^6+1)(a^3+1)(a^2+a+1)(a-1) \end{aligned}$$

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

$$\begin{aligned}
 &= 2^3 (2^6+1)(2^3+1)(2^3-1) \\
 &= 2^3 (2^6+1)(2^3+1)(2^2+2+1)(2-1) \\
 &= 8 (65) (9) (7) \\
 &= 8 \cdot 5 \cdot 13 \cdot 9 \cdot 7 = 2^3 \cdot 3^2 \cdot 5 \cdot 7 \cdot 13
 \end{aligned}$$

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

$$\begin{array}{lll}
 \gcd(a, 8) = 1 & \gcd(a, 13) = 1 & \gcd(a, 7) = 1 \\
 \gcd(a, 5) = 1 & \gcd(a, 9) = 1 &
 \end{array}$$

$$\begin{array}{lll}
 \therefore a^4 \equiv 1 \pmod{8} & a^{12} \equiv 1 \pmod{13} & a^6 \equiv 1 \pmod{7} \\
 a^4 \equiv 1 \pmod{5} & a^6 \equiv 1 \pmod{9} &
 \end{array}$$

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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,  $m^{\phi(n)} + n^{\phi(m)} \equiv 1 \pmod{mn}$

C. 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

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

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

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

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

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

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

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

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

$\therefore a^{p^{(k+1)-1}(p-1)} = 1 + q' p^{k+1}$  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 accidentally left in.

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

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

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

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

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

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

(b) Use (a) to solve the linear congruences

$$3x \equiv 5 \pmod{26}, \quad 13x \equiv 2 \pmod{40}, \quad 10x \equiv 21 \pmod{49}$$

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

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

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

To simplify,  $3^4 = 81 = 3 \cdot 26 \equiv 3 \pmod{26}$   
 $\therefore 3^8 \equiv 9 \pmod{26}$

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

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

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

=

$$13x \equiv 2 \pmod{40}$$

$$\gcd(13, 40) = 1$$

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

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

To simplify,  $13^2 = 169 \equiv 9 \pmod{40}$   
 $\therefore 13^4 \equiv 81 \equiv 1 \pmod{40}$

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

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

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

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

=

$$10x \equiv 21 \pmod{49}$$

$$\gcd(10, 49) = 1$$

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

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

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

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

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

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

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

$$\begin{aligned}\gcd(2, 77) &= 1. \quad \therefore 2^{\phi(77)} \equiv 1 \pmod{77} \\ \phi(77) &= 6 \cdot 10 = 60. \quad \therefore 2^{60} \equiv 1 \pmod{77} \\ \therefore 2^{60000} &\equiv 1 \pmod{77}, \quad (2^{60})^{300} = 2^{18000} \equiv 1 \pmod{77} \\ &\quad \therefore 2^{36000} \equiv 1 \pmod{77} \\ \therefore 2^{96000} &\equiv 1 \pmod{77}, \quad 2^{18000} \equiv 1 \pmod{77} \\ &\quad 2^{36000} \equiv 1 \pmod{77} \\ \therefore 2^{99600} &\equiv 1 \pmod{77}, \quad 2^{180} \equiv 1 \pmod{77} \\ &\quad \therefore 2^{360} \equiv 1 \pmod{77} \\ \therefore 2^{99960} &\equiv 1 \pmod{77}\end{aligned}$$

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

$$\therefore 2^{40} \equiv 23^4 \pmod{77}$$

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

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

$$\therefore 23^4 \equiv 100 \equiv 23 \pmod{77}$$

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

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  $n \geq 0$ .

(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  $\therefore a \equiv 0 \pmod{10}$ ,  $a^{4n+1} = (10x)^{4n+1}$   
 $= 10^{4n+1} \times x^{4n+1}$ .  $\therefore a^{4n+1} \equiv 0 \pmod{10}$ , 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  $a = 5^x p_1^{k_1} \cdots p_r^{k_r}$ ,  $p_i \neq 2$ ,  $x \geq 1$

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

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

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

$$\begin{aligned}a^{4n+1} &= (5^x)^{4n+1} (p_1^{k_1} \cdots p_r^{k_r})^{4n+1} \\ &= 5^{4xn+x} \cdot p_1^{k_1'} \cdots p_r^{k_r'}\end{aligned}$$

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

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

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

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

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

(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  $p_1^{k_1} \cdots p_r^{k_r} = 5g + r, 0 < r < 5$

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

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

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

Pf: Clearly true for  $n=0$

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

Assume true for  $k$ .

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

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

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

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

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

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

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

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

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

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

by Lemma above.

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

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

This is same as case  $r=1$ .

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

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

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

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

—  
by Lemma above.

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

Pf: Clearly true for  $n=0$

Assume true for  $K \geq 1$

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

$$3^4 = 81 = 80 + 1$$

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

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

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

$$\equiv 3 \pmod{10}$$

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

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

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

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

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

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

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

$$(a) \tilde{T}(p!) = 2 \tilde{T}((p-1)!)$$

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

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

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

$$\begin{aligned} \tilde{T}(p!) &= \tilde{T}(p \cdot p_1^{k_1} \cdots p_r^{k_r}) = \tilde{T}(p) \cdot \tilde{T}(p_1^{k_1} \cdots p_r^{k_r}) \\ &= \tilde{T}(p) \cdot \tilde{T}((p-1)!) \end{aligned}$$

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

$$(b) \tau(p!) = (p+1) \tau((p-1)!)$$

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

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

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

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

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

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

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

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.

$$-31 = -4 \cdot 9 + 5$$

$$-16 = -2 \cdot 9 + 2$$

$$-8 = -1 \cdot 9 + 1$$

$$13 = 1 \cdot 9 + 4$$

$$25 = 2 \cdot 9 + 7$$

$$80 = 8 \cdot 9 + 8$$

$\therefore \{-31, -16, -8, 13, 25, 80\}$  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

$\therefore$  a reduced set of residues mod 14.

(c) The integers  $1, 2, 2^2, 2^3, \dots, 2^{18}$  form a reduced set of residues mod 27.

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

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

Since  $\phi(27) = 18$ , and there are 18 numbers:  $2^1, 2^{12}, \dots, 2^{18}$ , only have to show the numbers are incongruent to each other mod 27.

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

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

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

$\therefore 2^{17} \not\equiv 1 \pmod{27}$ , for if  $2^{17} \equiv 1 \pmod{27}$ , then  $2^{18} = 2^{17} \cdot 2 \equiv 1 \cdot 2 \equiv 2 \pmod{27}$ , 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  $a, b \in \left\{-\frac{p-1}{2}, \dots, -2, -1\right\}$

and  $a \equiv b \pmod{p}$ , then  $-a \equiv -b \pmod{p}$ ,  
contradicting the incongruity of  
 $\left\{1, 2, \dots, \frac{p-1}{2}\right\}$ .

$\therefore$  Need only need to show if  $a \in \left\{1, 2, \dots, \frac{p-1}{2}\right\}$   
and  $b \in \left\{-\frac{p-1}{2}, \dots, -2, -1\right\}$ , 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 :

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

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

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

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

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

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

## 7-4 Some Properties of The Phi-Function

Note Title

11/2/2005

1. For a positive integer  $n$ , prove

$$\sum_{d|n} (-1)^{n/d} \phi(d) = \begin{cases} 0 & \text{if } n \text{ is even} \\ -n & \text{if } n \text{ is odd} \end{cases}$$

Pf: (1) If  $n$  is even, Then  $n = 2^k N$ , where  $N = p_1^{k_1} \dots p_r^{k_r}$ ,  $p_i \neq 2$ , and so  $N$  is odd.

Now break up the summation of  $d|n$  into sums of divisors that always contain  $2^k$  and all the other divisors.

For divisors that always contain  $2^k$  as a factor, This can be expressed as

$$\sum_{d|N} (-1)^{2^k N / 2^k d} \phi(2^k d) = \sum_{d|N} (-1)^{N/d} \phi(2^k d)$$

But  $N$  is odd, so is  $d$ , so  $N/d$  is odd, and so  $(-1)^{N/d} = -1$  [ $d = p_1^{s_1} \dots p_r^{s_r}$ ,  $0 \leq s_i \leq k_i$ ,  $p_i \neq 2$ ]

$$\therefore \sum_{d|N} (-1)^{2^k N / 2^k d} \phi(2^k d) = - \sum_{d|N} \phi(2^k d)$$

All the other divisors run over  $2^{k-1} N$

$$\therefore \sum_{d|n} (-1)^{n/d} \phi(d) = \sum_{d|2^{k-1} N} (-1)^{2^k N / d} \phi(d) - \sum_{d|N} \phi(2^k d)$$

But as  $d$  runs over  $2^{k-1}N$ ,  $2^{kN}/d$  will always be even as the highest power of 2 for  $d$  is  $2^{k-1}$ , so  $2^k N$  will always have a factor of 2.  $\therefore (-1)^{2^{kN}/d} = 1$

$$\therefore \sum_{d|n} (-1)^{n/d} \phi(d) = \sum_{d|2^{k-1}N} \phi(d) - \sum_{d|N} \phi(2^k d)$$

By Th. 7.6 from Gauss,  $n = \sum_{d|n} \phi(d)$ , so

$$\sum_{d|2^{k-1}N} \phi(d) = 2^{k-1}N. \text{ Also, } \phi \text{ is multiplicative, so } \phi(2^k d) = \phi(2^k) \phi(d)$$

$$\begin{aligned} \therefore \sum_{d|n} (-1)^{n/d} \phi(d) &= 2^{k-1}N - \phi(2^k) \sum_{d|N} \phi(d) \\ &= 2^{k-1}N - (2^k - 2^{k-1})(N) \end{aligned}$$

$$= 2^{k-1}N - 2^k N + 2^{k-1}N$$

$$= 2 \cdot 2^{k-1}N - 2^k N = 0$$

$$\therefore n \text{ even} \Rightarrow \sum_{d|n} (-1)^{n/d} \phi(d) = 0$$

(2) If  $n$  is odd, Then  $n = p_1^{k_1} \cdots p_r^{k_r}$ ,  $p_i \neq 2$ .  
 $\therefore d = p_1^{s_1} \cdots p_r^{s_r}$ ,  $0 \leq s_i \leq k_i$ , by Th. G.1

$\therefore d$  is odd

$\therefore$  as  $d$  runs over  $n$ ,  $n/d$  is odd, so  $(-1)^{n/d} = -1$

$$\therefore \sum_{d|n} (-1)^{n/d} \phi(d) = - \sum_{d|n} \phi(d) = -n$$

$$\therefore n \text{ odd} \Rightarrow \sum_{d|n} (-1)^{n/d} \phi(d) = -n$$

2. Confirm That  $\sum_{d|36} \phi(d) = 36$  and  $\sum_{d|36} (-1)^{36/d} \phi(d) = 0$

The divisors,  $d$ , of  $36$  are:  $1, 2, 3, 4, 6, 9, 12, 18, 36$   
 $\phi(d)$ :  $1, 1, 2, 2, 2, 6, 4, 6, 12$

$$\therefore \sum_{d|36} \phi(d) = 1 + 1 + 2 + 2 + 2 + 6 + 4 + 6 + 12 = 36$$

$$\sum_{d|36} (-1)^{36/d} \phi(d) = 1 + 1 + 2 - 2 + 2 + 6 - 4 + 6 - 12 = 0$$

3. For a positive integer  $n$ , prove that

$$\sum_{d|n} \mu^2(d) / \phi(d) = n / \phi(n)$$

Pf: By prop. # 19, Sec. 6-1, if  $f$  and  $g$  are multiplicative, so is  $f \cdot g$  and  $f/g$ .

$$\therefore F(n) = \sum_{d|n} \frac{\mu^2(d)}{\phi(d)} \text{ is multiplicative.}$$

$$\text{Let } n = p^k$$

$$\begin{aligned} \therefore F(p^k) &= \sum_{d|p^k} \frac{\mu^2(d)}{\phi(d)} = \frac{\mu^2(1)}{\phi(1)} + \frac{\mu^2(p)}{\phi(p)} + \dots + \frac{\mu^2(p^k)}{\phi(p^k)} \\ &= 1 + \frac{1}{p-1} + \dots + 0 \\ &= 1 + \frac{1}{p-1} = \frac{p}{p-1} \end{aligned}$$

$$\text{as } \mu(p^k) = 0 \text{ for } k \geq 2$$

$$\therefore \text{if } n = p_1^{k_1} \cdots p_r^{k_r}, \text{ then}$$

$$\begin{aligned} F(n) &= F(p_1^{k_1} \cdots p_r^{k_r}) = F(p_1^{k_1}) \cdots F(p_r^{k_r}) \\ &= \frac{p_1}{p_1-1} \cdots \frac{p_r}{p_r-1} \end{aligned}$$

$$\text{From Th. 7.3, } d(n) = n \left( \frac{p_1-1}{p_1} \right) \cdots \left( \frac{p_r-1}{p_r} \right)$$

$$\therefore \left( \frac{p_1-1}{p_1} \right) \cdots \left( \frac{p_r-1}{p_r} \right) = \frac{\phi(n)}{n}$$

$$\therefore F(n) = \sum_{d|n} \frac{\mu^2(d)}{\phi(d)} = \frac{n}{\phi(n)}$$

4. Use problem 4(c), Sec. 6.2, to give a proof of the fact that  $n \sum_{d|n} \mu(d)/d = \phi(n)$ .

Pf: Prob. 4(c) states  $\sum_{d|n} \mu(d)/d = (1 - \frac{1}{p_1}) \cdots (1 - \frac{1}{p_r})$

$$\text{if } n = p_1^{k_1} \cdots p_r^{k_r}.$$

$$\begin{aligned} \therefore n \sum_{d|n} \mu(d)/d &= n(1 - \frac{1}{p_1}) \cdots (1 - \frac{1}{p_r}) \\ &= \phi(n) \text{ by Th. 7.3} \end{aligned}$$

5. If  $n > 1$  has the prime factorization  $n = p_1^{k_1} \cdots p_r^{k_r}$ , establish each of the following:

$$(a) \sum_{d|n} \mu(d) \phi(d) = (2 - p_1)(2 - p_2) \cdots (2 - p_r)$$

Pf: Since  $\mu$  and  $\phi$  are multiplicative, then  $\mu \cdot \phi$  is multiplicative (prob. 19, Sec. 6.1).

$\therefore F(n) = \sum_{d|n} \mu(d) \phi(d)$  is multiplicative.

$$F(p^k) = \sum_{d|p^k} \mu(d) \phi(d)$$

$$= \mu(1) \cdot \phi(1) + \mu(p) \cdot \phi(p) + \dots + \mu(p^k) \cdot \phi(p^k)$$

$$= 1 + (-1)(p-1) + 0 + 0 + \dots + 0 = 2-p,$$

since  $\mu(p^k) = 0$  for  $k \geq 2$

$$\therefore F(n) = F(p_1^{k_1} \dots p_r^{k_r}) = F(p_1^{k_1}) \dots F(p_r^{k_r})$$

$$= (2-p_1) \dots (2-p_r)$$

$=$

Could also have used prob. 3, Sec. 6-2,  
which says,

$$\sum_{d|n} \mu(d) f(d) = (1-f(p_1)) \dots (1-f(p_r))$$

where  $f$  is multiplicative, not identically zero. But  $\phi$  is multiplicative and not identically zero (e.g.,  $\phi(1)=1$ ,  $\phi(p)=p-1$ ).

$$\therefore \sum_{d|n} \mu(d) \phi(d) = (1-\phi(p_1)) \dots (1-\phi(p_r))$$

$$= (1-(p_1-1)) \dots (1-(p_r-1))$$

$$= (2-p_1) \dots (2-p_r)$$

$$(6) \sum_{d|n} d \cdot \phi(d) = \left( \frac{p_1^{2k_1+1} + 1}{p_1 + 1} \right) \cdots \left( \frac{p_r^{2k_r+1} + 1}{p_r + 1} \right)$$

Pf:  $f(x) = x$  is multiplicative,  $\therefore f \cdot \phi$  is also.

$\therefore F(n) = \sum_{d|n} d \cdot \phi(d)$  is multiplicative.

$$(1) \text{ Consider } F(p^k) = \sum_{d|p^k} d \cdot \phi(d)$$

$$= 1 \cdot \phi(1) + p \cdot \phi(p) + p^2 \cdot \phi(p^2) + \cdots + p^k \cdot \phi(p^k)$$

$$= 1 + p(p-1) + p^2(p^2-p) + \cdots + p^k(p^k-p^{k-1})$$

$$= (1 + p^2 - p + p^4 - p^3 + p^6 - p^5 + \cdots + p^{2k} - p^{2k-1})$$

$$= 1 + (-1)^1 p + (-1)^2 p^2 + (-1)^3 p^3 + \cdots + (-1)^{2k} p^{2k}$$

$$\text{But } (a^{2r+1} + 1) = (a+1)(a^{2r} - a^{2r-1} + a^{2r-2} - a^{2r-3} + \cdots + r^2 - r + 1)$$

(i.e., coefficient of 1 for even exponents,  
-1 for odd exponents).

$$\therefore (p^{2k+1} + 1) = (p+1)(p^{2k} - p^{2k-1} + \cdots + p^2 - p + 1)$$

$$\therefore \frac{p^{2k+1} + 1}{p+1} = p^{2k} - p^{2k-1} + \dots + p^2 - p + 1$$

$$\therefore F(p^k) = \frac{p^{2k+1} + 1}{p+1}$$

$$(2) \quad \therefore \sum_{d|n} d \cdot \phi(d) = F(n) = F(p_1^{k_1} \cdots p_r^{k_r})$$

$$= F(p_1^{k_1}) \cdots F(p_r^{k_r})$$

$$= \left( \frac{p_1^{2k_1+1} + 1}{p_1 + 1} \right) \cdots \left( \frac{p_r^{2k_r+1} + 1}{p_r + 1} \right)$$

$$(C) \quad \sum_{d|n} \frac{\phi(d)}{d} = \left( 1 + \frac{k_1(p_1 - 1)}{p_1} \right) \cdots \left( 1 + \frac{k_r(p_r - 1)}{p_r} \right)$$

$\rho f: f(r) = \frac{1}{r^k}$  is multiplicative.

$\therefore F(n) = \sum_{d|n} \frac{\phi(d)}{d}$  is multiplicative

$$(1) \text{ Consider } F(p^k) = \sum_{d|p^k} \frac{\phi(d)}{d}$$

$$= \frac{\phi(1)}{1} + \frac{\phi(p)}{p} + \dots + \frac{\phi(p^k)}{p^k}$$

$$= 1 + \frac{p^{-1}}{p} + \frac{p^2 - p}{p^2} + \dots + \frac{p^k - p^{k-1}}{p^k}$$

$$= 1 + \frac{p^{-1}}{p} + p \frac{(p-1)}{p^2} + \dots + p^{k-1} \frac{(p-1)}{p^k}$$

$$= 1 + \frac{p^{-1}}{p} + \frac{p^{-1}}{p} + \dots + \frac{p^{-1}}{p}$$

$$= 1 + k \left( \frac{p^{-1}}{p} \right)$$

$$(2) \therefore \sum_{d|n} \frac{\phi(d)}{d} = F(n) = F(p_1^{k_1} \cdots p_r^{k_r}) \\ = F(p_1^{k_1}) \cdots F(p_r^{k_r})$$

$$= \left( 1 + k_1 \frac{(p_1 - 1)}{p_1} \right) \cdots \left( 1 + k_r \frac{(p_r - 1)}{p_r} \right)$$

C. Verify the formula  $\sum_{d=1}^n \phi(d) \left[ \frac{n}{d} \right] = n \frac{(n+1)}{2}$ ,  $n > 0$ .

Pf: From Th. 7.6, if  $n > 0$ ,  $n = \sum_{d|n} \phi(d)$

$$\text{Let } F(n) = \sum_{d|n} \phi(d)$$

$$\text{Since } F(n) = n, \text{ Then } \sum_{d=1}^n F(d) = \frac{n(n+1)}{2}$$

But by Th. G.11,  $\sum_{d=1}^N F(d) = \sum_{d=1}^N \phi(d) \left[ \frac{N}{d} \right]$

$$\therefore \sum_{d=1}^N \phi(d) \left[ \frac{N}{d} \right] = \frac{N(N+1)}{2}$$

7. If  $n$  is square-free, prove  $\sum_{d|n} \sigma(d^{k-1}) \phi(d) = n^k$   
for  $k \geq 2$ .

Pf:  $\sigma$  and  $\phi$  are multiplicative, so

$$F(n) = \sum_{d|n} \sigma(d^{k-1}) \phi(d) = \sum_{d|n} \underbrace{\sigma(d) \dots \sigma(d)}_{k-1 \text{ times}} \cdot \phi(d)$$

is also multiplicative.

(1) Consider  $n = p$  ( $n$  is square-free)

$$\begin{aligned} \therefore F(p) &= \sum_{d|p} \sigma(d^{k-1}) \phi(d) \\ &= \sigma(1)\phi(1) + \sigma(p^{k-1})\phi(p) \\ &= 1 + \frac{p^{k-1+1}-1}{p-1} \cdot (p-1) = p^k = n^k \end{aligned}$$

(2)  $\therefore$  if  $n = p_1 p_2 \dots p_r$ , Then

$$\sum_{d|n} \sigma(d^{k-1}) \phi(d) = F(n) = F(p_1) F(p_2) \cdots F(p_r)$$

$$= p_1^k p_2^k \cdots p_r^k = (p_1 p_2 \cdots p_r)^k = n^k$$

8. For a square-free integer  $n \geq 1$ , show that  $T(n^2) = n$  if and only if  $n = 3$ .

Pf: (1) If  $n = 3$ , Then  $T(n^2) = T(3^2) = 2+1 = 3$   
by Th. 6.2

(2) Suppose  $n$  is square-free,  $n \geq 1$ , and  $T(n^2) = n$

Let  $n = p_1 p_2 \cdots p_r$ , where  $p_i \neq p_j$  since  
 $n$  is square-free.

$$\text{By Th. 6.2, } T(n^2) = T(p_1^2 p_2^2 \cdots p_r^2)$$

$$= (2+1)(2+1)\cdots(2+1) = 3^r$$

$$\therefore T(n^2) = n = p_1 p_2 \cdots p_r = 3^r$$

By Th. 3.1 and its corollaries, all  $p_i = 3$ ,  
which mean  $n = 3$  and  $r = 1$ .

9. Prove that  $3 | \sigma(3n+2)$  and  $4 | \sigma(4n+3)$  for any positive integer  $n$ .

$$(a) 3 \mid \sigma(3n+2)$$

$$\text{Let } 3n+2 = p_1^{k_1} \cdots p_r^{k_r}$$

Since  $3 \equiv 0 \pmod{3}$  and  $3n+2 \equiv 2 \pmod{3}$ ,  
 Then  $p_i^{k_i} \not\equiv 0 \pmod{3}$  for  $i = 1, 2, \dots, r$

If all  $p_i^{k_i} \equiv 1 \pmod{3}$ , Then  $p_1^{k_1} \cdots p_r^{k_r} \equiv 1 \pmod{3}$   
 Since  $p_1^{k_1} \cdots p_r^{k_r} \equiv 2 \pmod{3}$ , There must  
 be one  $p_i$  s.t.  $p_i^{k_i} \equiv 2 \pmod{3}$   
 (and  $\because p_i^{k_i} \equiv 2 \pmod{3}$ , for if  $p_i \equiv 0$ , Then  
 $p_i^{k_i} \equiv 0$ , and if  $p_i \equiv 1$ , Then  $p_i^{k_i} \equiv 1$ )

Since  $p_i \equiv 2 \pmod{3}$ , Then  
 $p_i^2 \equiv 4 \equiv 1 \pmod{3}$   
 $p_i^3 \equiv 2 \pmod{3}$

$\therefore$  if  $p_i^r \equiv 2 \pmod{3}$ , Then  $r$  is odd.

$\therefore$  for  $p_i^{k_i} \equiv 2 \pmod{3}$ ,  $k_i$  is odd.

$$\begin{aligned}\therefore \sigma(p_i^{k_i}) &= \frac{p_i^{k_i+1}-1}{p_i-1} = \frac{(p_i-1)(p_i^{k_i} + p_i^{k_i-1} + \dots + p_i + 1)}{p_i-1} \\ &= p_i^{k_i} + p_i^{k_i-1} + \dots + p_i + 1, \text{ and } k_i \text{ is odd.}\end{aligned}$$

Note  $2 \equiv -1 \pmod{3}$ , so

$$\text{if } r \text{ is odd, } p_i^r \equiv -1 \pmod{3}$$

$$\text{if } r \text{ is even, } p_i^r \equiv 1 \pmod{3}$$

$$\therefore \tau(p_i^{k_i}) = p_i^{k_i} + p_i^{k_i-1} + \dots + p_i + 1$$

$$\equiv (-1) + 1 + \dots + (-1) + 1 \pmod{3}$$

$$\equiv 0 \pmod{3}$$

$$\therefore 3 \mid \tau(p_i^{k_i}) \Rightarrow 3 \mid \tau(p_1^{k_1}) \dots \tau(p_i^{k_i}) \dots \tau(p_r^{k_r})$$

$$\Rightarrow 3 \mid \tau(p_1^{k_1} \dots p_r^{k_r}) \quad [\tau \text{ is multiplicative}]$$

$$\Rightarrow 3 \mid \tau(3n+2)$$

(6)  $4 \mid \tau(4n+3)$

$$\text{Let } 4n+3 = p_1^{k_1} \dots p_r^{k_r}$$

$$4n+3 \equiv 3 \equiv -1 \pmod{4}$$

As in (a), all  $p_i^{k_i} \not\equiv 1 \pmod{4}$ , and  $p_i^{k_i} \not\equiv 0 \pmod{4}$   
since if  $p_i^{k_i} \equiv 0 \pmod{4} \Rightarrow 4n+3 \equiv 0 \pmod{4}$

If  $p_i^{k_i} \equiv 2 \pmod{4}$  for any  $i$ , Then

$$p_1^{k_1} \cdots p_r^{k_r} \equiv 2 \text{ or } 3 \pmod{4}, p_j \neq p_i, \text{ so}$$

$$\begin{aligned} 4n+3 &= p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r} \equiv 2 \cdot 2 \text{ or } 2 \cdot 3 \pmod{4} \\ &\equiv 0 \text{ or } 2 \pmod{4} \end{aligned}$$

$\therefore p_i^{k_i} \not\equiv 2 \pmod{4}$  for any  $i$ .

$\therefore p_i^{k_i} \equiv 3 \equiv -1 \pmod{4}$  for some  $i$ ,

and  $\therefore p_i \equiv 3 \pmod{4}$

for  $p_i \equiv 0 \Rightarrow p_i^{k_i} \equiv 0 \pmod{4}$

$p_i \equiv 1 \Rightarrow p_i^{k_i} \equiv 1 \pmod{4}$

$p_i \equiv 2 \Rightarrow p_i^{k_i} \equiv 2 \pmod{4}$

$\therefore p_i^2 \equiv 9 \equiv 1 \pmod{4} \Rightarrow p_i^{2K} \equiv 1 \pmod{4}$

$\therefore$  if  $s$  is even,  $p_i^s \equiv 1 \pmod{4}$  for all  $K$

$\therefore p_i^{k_i} \equiv -1 \pmod{4} \Rightarrow k_i$  is odd

$$\begin{aligned} \text{As in (a)} \quad \sigma(p_i^{k_i}) &= p_i^{k_i} + p_i^{k_i-1} + \cdots + p_i + 1 \\ &\equiv (-1) + 1 + \cdots + (-1) + 1 \end{aligned}$$

$$\equiv 0 \pmod{4}$$

$$\therefore 4 \mid \tau(p_i^{k_i})$$

$$\therefore 4 \mid \tau(p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}) \Rightarrow 4 \mid \tau(4n+3)$$

10. (a) Given  $K > 0$ , establish that there exists a sequence of  $K$  consecutive integers  $n+1, n+2, \dots, n+K$  satisfying

$$\mu(n+1) = \mu(n+2) = \dots = \mu(n+K) = 0$$

Pf: Use the author's hint. Let  $p_k$  be the  $k$ th prime.

$$\therefore \gcd(p_i^2, p_j^2) = 1 \text{ for } i \neq j.$$

$\therefore$  By the Chinese Remainder Th., there is a solution to:  $x \equiv -1 \pmod{p_1^2}$   
 $x \equiv -2 \pmod{p_2^2}$   
 $\vdots$   
 $x \equiv -K \pmod{p_K^2}$

where  $p_1 = 2, p_2 = 3, \dots, p_K = K+1$  prime

By the discussion on p. 138, if  $n = p_1 p_2 \cdots p_K$  and  $N_i = n/p_i$ , then a simultaneous solution is:

$$x = (-1)N_1^{\phi(p_1^2)} + (-2)N_2^{\phi(p_2^2)} + \cdots + (-K)N_K^{\phi(p_K^2)}$$

$$\therefore x = -N_1^{\phi(2^2)} - 2N_2^{\phi(3^2)} - \dots - kN_k^{\phi(p_k^2)}$$

$$\therefore x+i \equiv 0 \pmod{p_i^2} \text{ for } i=1, 2, \dots, k$$

$$\therefore x+i = a p_i^2, \text{ some } a$$

$$\text{so } \mu(x+i) = 0, i=1, 2, \dots, k$$

(b) Find four consecutive integers for which  $\mu(n) = 0$

By (a), consider  $x \equiv -1 \pmod{2^2}$

$$x \equiv -2 \pmod{3^2}$$

$$x \equiv -3 \pmod{5^2}$$

$$x \equiv -4 \pmod{7^2}$$

$$\text{Let } s = 2^2 \cdot 3^2 \cdot 5^2 \cdot 7^2 = 44100$$

$$N_1 = s/2^2 = 3^2 \cdot 5^2 \cdot 7^2 = 11025$$

$$N_2 = s/3^2 = 2^2 \cdot 5^2 \cdot 7^2 = 4900$$

$$N_3 = s/5^2 = 2^2 \cdot 3^2 \cdot 7^2 = 1764$$

$$N_4 = s/7^2 = 2^2 \cdot 3^2 \cdot 5^2 = 900$$

$$\text{Also, } \phi(2^2) = 2, \phi(3^2) = 6, \phi(5^2) = 20, \phi(7^2) = 42$$

$\therefore$  a simultaneous solution is:

$$x = -(11025)^2 - 2(4900)^6 - 3(1764)^{20} - 4(900)^{42}$$

$$\therefore \mu(x+1) = \mu(x+2) = \mu(x+3) = \mu(x+4) = 0$$

But this is a rather awkward number.

$\therefore$  solve by method developed in proof of Chinese Remainder Th. in sec. 4.4.

Using  $N_1, N_2, N_3, N_4$  as above, and  
 $a_1 = -1, a_2 = -2, a_3 = -3, a_4 = -4$

$$11025x_1 \equiv 1 \pmod{4} \quad 4900x_2 \equiv 1 \pmod{9}$$

$$\therefore 11025x_1 - 11024 \equiv 1 \quad 4900x_2 - 4 \cdot 544x_2 \equiv 1$$

$$x_1 \equiv 1 \pmod{4}$$

$$4x_2 \equiv 1 + 3 \cdot 9 = 28$$

$$x_2 \equiv 7 \pmod{9}$$

$$1764x_3 \equiv 1 \pmod{25}$$

$$\therefore 1764x_3 - 1750x_3 \equiv 1$$

$$14x_3 \equiv 1, 28x_3 \equiv 2$$

$$3x_3 \equiv 2 + 25 = 27$$

$$\therefore x_3 \equiv 9 \pmod{25}$$

$$900x_4 \equiv 1 \pmod{49}$$

$$900x_4 - 18 \cdot 49x_4 \equiv 1$$

$$18x_4 \equiv 1, 54x_4 \equiv 3$$

$$54x_4 - 49x_4 \equiv 3$$

$$5x_4 \equiv 3, 50x_4 \equiv 30$$

$$\therefore x_4 \equiv 30$$

$$\therefore x = a_1N_1x_1 + a_2N_2x_2 + a_3N_3x_3 + a_4N_4x_4$$

$$= -11025(1) - 2(4900)(7) - 3(1764)(9) - 4(900)(30)$$

$$= -11025 - 68600 - 47628 - 108000$$

$$= -235253$$

$\therefore x = -235,253$  is a solution.

Can make this number smaller noting that  
 The solution is unique modulo  $2^2 \cdot 3^2 \cdot 5^2 \cdot 7^2 = 44,100$ .

$$\therefore x = -235,253 + 6(44,100) = 29,347$$

$$\begin{aligned} \therefore x+1 &= 29,348 &= 2^2 \cdot 11 \cdot 23 \cdot 29 \\ x+2 &= 29,349 &= 3^3 \cdot 1087 \\ x+3 &= 29,350 &= 2 \cdot 5^2 \cdot 587 \\ x+4 &= 29,351 &= 7^2 \cdot 599 \end{aligned}$$

$$\therefore \mu(x+1) = \mu(x+2) = \mu(x+3) = \mu(x+4) = 0$$

11. Modify the proof of Gauss's Th. to establish

$$\sum_{k=1}^n \gcd(k, n) = \sum_{d|n} d \cdot \phi\left(\frac{n}{d}\right) = n \sum_{d|n} \frac{\phi(d)}{d}, \text{ for } n \geq 1$$

Pf: Let  $d$  be a divisor of  $n$ . Create set  $S_d$  s.t.

$$S_d = \{m : \gcd(m, n) = d ; 1 \leq m \leq n\}$$

Let  $N = \{1, 2, \dots, n\}$

If  $a \in N$ , Then if  $\gcd(a, n) = 1$ , Then  $a \in S_1$ ,

If  $\gcd(a, n) = c > 1$ , Then  $a \in S_c$ .

$\therefore a \in N$  is in at least one set  $S_i$

But every  $a \in N$  is in at most one set  $S_i$ .

For if  $a \in S_i$ ,  $a \in S_j$ ,  $i \neq j$ , Then

$$\gcd(a, n) = i = j.$$

$\therefore$  The sets  $S_i$  partition  $N$  into a finite number of sets.

$$\gcd(m, n) = d \Leftrightarrow \gcd(m/d, n/d) = 1 \quad [1]$$

Pf: (a) By corollary 1 to Th. 2.4 in Sec. 2.2,

$$\gcd(m, n) = d \Rightarrow \gcd(m/d, n/d) = 1$$

(b) Suppose  $\gcd(m/d, n/d) = 1$

$\therefore$  There are integers  $x, y$  s.t.

$$\frac{m}{d}x + \frac{n}{d}y = 1, \therefore mx + ny = d$$

Suppose  $\gcd(m, n) = c \therefore m = ac, n = bc$

$$\therefore (ac)x + (bc)y = d \Rightarrow c | d$$

$\therefore$  By Th. 2.5, Sec. 2.2,  $d = \gcd(m, n)$

Also, for  $S_d$ ,  $1 \leq m \leq n$ , so  $m/d \leq \frac{n}{d}$ .

$\therefore$  From [1], # elements in  $S_d$  = # positive integers,  $\leq \frac{n}{d}$ , that are relatively prime to  $\frac{n}{d}$ , and this is  $\phi\left(\frac{n}{d}\right)$ .

Thus, # elements in  $S_d$  =  $\phi\left(\frac{n}{d}\right)$

$$\therefore \sum_{k \in S_d} \gcd(k, n) = d \cdot \phi\left(\frac{n}{d}\right), \text{ since } \gcd(k, n) = d$$

As mentioned above,  $S_d$  exactly partitions  $N$ .

$$\therefore \sum_{k=1}^n \gcd(k, n) = \sum_{d|n} d \cdot \phi\left(\frac{n}{d}\right)$$

Now when  $d|n$ , there is a  $d'$  s.t.  $d \cdot d' = n$ ,  
so that  $\{d : d|n\} = \{d' : d|n\}$

$$\therefore \sum_{d|n} d \cdot \phi\left(\frac{n}{d}\right) = \sum_{d'|n} d' \cdot \phi\left(\frac{n}{d'}\right)$$

$$= \sum_{\substack{d|n \\ d \neq n}} \frac{n}{d} \cdot \phi\left(\frac{n}{d}\right) = n \sum_{d|n} \frac{\phi(d)}{d}$$

12. For  $n \geq 2$ , establish  $\phi(n^2) + \phi((n+1)^2) \leq 2n^2$

Pf: Relation does work for  $n=2$

$$\phi(2^2) + \phi((2+1)^2) = \phi(4) + \phi(9) = 2+6 = 8 \leq 2 \cdot 2^2 = 8$$

By problem 7(c), Sec. 7.2, if  $K$  is composite,  
 $\phi(K) \leq K - \tau K$

$n^2$  is composite, so is  $(n+1)^2$

$$\therefore \phi(n^2) \leq n^2 - \tau n^2 = n^2 - n$$

$$\begin{aligned}\phi((n+1)^2) &\leq (n+1)^2 - \tau(n+1)^2 \\ &= n^2 + 2n + 1 - (n+1) \\ &= n^2 + n\end{aligned}$$

$$\therefore \phi(n^2) + \phi((n+1)^2) \leq n^2 - n + n^2 + n = 2n^2$$

13. Given integer  $n$ , prove There exists at least one  $K$  for which  $n \mid \phi(K)$ .

Pf: If  $K = p_1^{k_1} \cdots p_r^{k_r}$  so that

$$\phi(K) = p_1^{k_1-1} \cdots p_r^{k_r-1} (p_1-1) \cdots (p_r-1)$$

We want  $n = p_1^{K_1-1} \cdots p_r^{K_r-1}$

$\therefore$  Let  $n = q_1^{a_1} \cdots q_s^{a_s}$

Then choose  $K = q_1^{a_1+1} \cdots q_s^{a_s+1}$

$\therefore \phi(K) = q_1^{a_1} \cdots q_s^{a_s} (q_1 - 1) \cdots (q_s - 1)$

and clearly  $n \mid \phi(K)$

14. Show that if  $n$  is the product of twin primes, say  $n = p(p+2)$ , Then  $\phi(n)\sigma(n) = (n+1)(n-3)$

If:  $\gcd(p, p+2) = 1$ , so

$$\phi(n) = \phi(p) \cdot \phi(p+2) = (p-1)(p+2-1) = (p-1)(p+1)$$

$$\text{But } \sigma(n) = \sigma(p) \sigma(p+2) = (p+1)(p+3)$$

$$\therefore \phi(n)\sigma(n) = (p-1)(p+1)^2(p+3)$$

$$\begin{aligned} \text{Now } (n+1)(n-3) &= (p^2 + 2p + 1)(p^2 + 2p - 3) \\ &= (p+1)^2(p+3)(p-1) \end{aligned}$$

$$\therefore \phi(n)\sigma(n) = (n+1)(n-3)$$

15. Prove (a)  $\sum_{d|n} \tau(d) \phi(n/d) = n \tau(n)$  and

$$(b) \sum_{d|n} \tau(d) \phi(n/d) = \tau(n)$$

Lemma: if  $d|n$ , then  $F(d) = \phi(\frac{n}{d})$  is multiplicative

Pf: For any number theoretic function  $f$ ,

$$\sum_{d|n} f(d) = \sum_{d|n} f\left(\frac{n}{d}\right)$$

$$\therefore \text{Let } F(n) = \sum_{d|n} \phi(d)$$

Since  $\phi$  is multiplicative, by Th. 6.4,  
 $F$  is multiplicative.

$$\text{Let } g(d) = \phi\left(\frac{n}{d}\right)$$

$$\therefore F(n) = \sum_{d|n} \phi(d) = \sum_{d|n} \phi\left(\frac{n}{d}\right) = \sum_{d|n} g(d)$$

By Th. 6.8,  $g(d) = \phi\left(\frac{n}{d}\right)$  is multiplicative

$$\therefore \text{if } \gcd(r, s) = 1 \text{ and } rs|n, \text{ then}$$
$$g(rs) = \phi\left(\frac{n}{rs}\right) = g(r)g(s) = \phi\left(\frac{n}{r}\right)\phi\left(\frac{n}{s}\right)$$

(a) Since  $F(n) = \sum_{d|n} \sigma(d) \phi\left(\frac{n}{d}\right)$  is multiplicative

by Lemma above and prob. 19, Sec. 6.1,

it suffices to show for  $n = p^k$ ,  $p$  prime,  
That

$$F(p^k) = p^k \bar{\tau}(p^k)$$

because if  $n = p_1^{k_1} \cdots p_r^{k_r}$ , Then

$$F(n) = F(p_1^{k_1} \cdots p_r^{k_r}) = F(p_1^{k_1}) \cdots F(p_r^{k_r}) =$$

$$p_1^{k_1} \bar{\tau}(p_1^{k_1}) \cdots p_r^{k_r} \bar{\tau}(p_r^{k_r}) = n \bar{\tau}(p_1^{k_1} \cdots p_r^{k_r})$$

$$= n \bar{\tau}(n)$$

The divisors of  $p^k$  are  $1, p, p^2, \dots, p^{k-1}, p^k$   
 $(k+1)$  divisors  $= \bar{\tau}(p^k)$

$$\therefore F(p^k) = \sum_{d|p^k} \sigma(d) \phi\left(\frac{p^k}{d}\right)$$

$$= \sigma(1) \phi\left(\frac{p^k}{1}\right) + \sigma(p) \phi\left(\frac{p^k}{p}\right) + \dots + \sigma(p^{k-1}) \phi\left(\frac{p^k}{p^{k-1}}\right) + \sigma(p^k) \phi\left(\frac{p^k}{p^k}\right)$$

$$= 1 \cdot (p^k - p^{k-1}) + (p+1)(p^{k-1} - p^{k-2}) + \dots +$$

$$\begin{aligned}
& \frac{\rho^k - 1}{\rho - 1} \cdot (\rho - 1) + \frac{\rho^{k+1} - 1}{\rho - 1} \cdot 1 \\
&= (\rho^k - \rho^{k-1}) + (\rho^k - \rho^{k-1} + \rho^{k-1} - \rho^{k-2}) + \dots + \\
&\quad (\rho^{k-1}) + (\rho^k + \rho^{k-1} + \rho^{k-2} + \dots + \rho + 1) \\
&= (\rho^k - \rho^{k-1}) + (\rho^k - \rho^{k-2}) + \dots + (\rho^{k-1}) + (\rho^k + \rho^{k-1} + \dots + \rho + 1) \\
&= (k+1)\rho^k \\
&= \rho^k \tau(\rho^k) \\
\therefore F(\rho^k) &= \rho^k \tau(\rho^k) \\
\therefore \sum_{d|n} \tau(d) \phi\left(\frac{n}{d}\right) &= n \tau(n)
\end{aligned}$$

(b) Since, as in (a),  $\tilde{F}(n) = \sum_{d|n} \tau(d) \phi\left(\frac{n}{d}\right)$  is multiplicative, it suffices to show, for  $p$  prime,  $\tilde{F}(p^k) = \tau(p^k)$ , for then  $\sum_{d|n} \tau(d) \phi\left(\frac{n}{d}\right) = \tau(n)$

$$\therefore F(p^k) = \sum_{d|p^k} \tau(d) \phi\left(\frac{p^k}{d}\right)$$

$$\begin{aligned}
&= \tau(1)\phi\left(\frac{\rho^k}{1}\right) + \tau(\rho)\phi\left(\frac{\rho^k}{\rho}\right) + \dots + \tau(\rho^{k-1})\phi\left(\frac{\rho^k}{\rho^{k-1}}\right) + \tau(\rho^k)\phi\left(\frac{\rho^k}{\rho^k}\right) \\
&= 1 \cdot (\rho^k - \rho^{k-1}) + (2) \cdot (\rho^{k-1} - \rho^{k-2}) + \dots + (k) \cdot (\rho - 1) + (k+1) \cdot 1 \\
&= \rho^k - \underbrace{\rho^{k-1}}_{\substack{1 \\ 1}} + 2 \cdot \underbrace{\rho^{k-1}}_{\substack{1 \\ 1}} - \underbrace{2\rho^{k-2}}_{\substack{1 \\ 1}} + \dots + \underbrace{(k-1)\rho^2}_{\substack{1 \\ 1}} - \underbrace{(k-1)\rho}_{\substack{1 \\ 1}} + k\rho - \underbrace{k+1}_{\substack{1 \\ 1}} \\
&= \rho^k + \rho^{k-1} + \rho^{k-2} + \dots + \rho + 1 \\
&= \frac{\rho^{k+1} - 1}{\rho - 1} = \tau(\rho^k) \\
\therefore F(\rho^k) &= \tau(\rho^k) \\
\therefore \sum_{d|n} \tau(d)\phi\left(\frac{n}{d}\right) &= \tau(n)
\end{aligned}$$

16. If  $a_1, a_2, \dots, a_{\phi(n)}$  is a reduced set of residues modulo  $n$ , show  $a_1 + a_2 + \dots + a_{\phi(n)} \equiv 0 \pmod{n}$ ,  $n \geq 2$

Pf: Let  $b_1, b_2, \dots, b_{\phi(n)}$  be the positive integers, less than  $n$ , that are relatively prime to  $n$ . Then by Th. 7.7, for  $n \geq 2$ ,  $b_1 + b_2 + \dots + b_{\phi(n)} = \frac{1}{2}n\phi(n)$

But  $n \equiv 0 \pmod{n}$ . For  $n > 2$ ,  $\phi(n)$  is even, so  $\frac{1}{2}\phi(n)$  is an integer, so

$$\sum_1 + \dots + \sum_{\phi(n)} = \frac{1}{2}n\phi(n) \equiv 0 \pmod{n}$$

Also,  $b_i \not\equiv b_j \pmod{n}$  since  $1 \leq b_i, b_j < n$

Now,  $a_1, a_2, \dots, a_{\phi(n)}$  are congruent, not necessarily in order of appearance, to  $b_1, b_2, \dots, b_{\phi(n)}$ , since both are reduced sets of residues.

$$\therefore a_1' \equiv b_1' \pmod{n}$$

$$a_2' \equiv b_2' \pmod{n}$$

$$a_{\phi(n)}' \equiv b_{\phi(n)}' \pmod{n}$$

where  $b_1', \dots, b_{\phi(n)}'$  are the integers

$b_1, \dots, b_{\phi(n)}$  in some order.

$$\therefore a_1 + \dots + a_{\phi(n)} \equiv b_1' + \dots + b_{\phi(n)}' = \sum_1 + \dots + \sum_{\phi(n)} \equiv 0 \pmod{n}$$

$$\therefore a_1 + \dots + a_{\phi(n)} \equiv 0 \pmod{n} \quad (n > 2)$$

## 7.5 An Application to Cryptography

Note Title

11/21/2005

1. Encrypt the message RETURN HOME using the Caesar cipher.

Using  $A=00, B=01, \dots, Z=25$ , and a space stays as a space,

R	E	T	U	N	H	O	M	E		
17	04	19	20	17	13	07	14	12	04	+3
20	7	22	23	20	16	10	17	15	07	2

$\therefore$  UHWXUQ KRPHT

2. If the Caesar cipher produced KLOSSB ELUWKGD, what is the plaintext message.

K	O	S	S	B	E	L	U	W	K	G	D	B	
10	03	18	18	01	04	11	20	22	10	06	03	01	-3
07	00	15	15	24	01	08	17	19	07	03	00	24	2
H	A	P	P	Y	B	I	R	T	H	D	A	Y	

3. (a). A linear cipher is defined by  $C \equiv aP + b \pmod{26}$ , where  $a, b$  are integers,  $\gcd(a, 26) = 1$ . Show the decrypting sequence is:  $P \equiv a'(C-b) \pmod{26}$  where  $a'$  satisfies:  $aa' \equiv 1 \pmod{26}$ .

Pf: Since  $\gcd(a, 26) = 1$ , Then by corollary to Th. 4.7 (p. 76), The linear congruence  $ax \equiv 1 \pmod{26}$  has a unique solution.  
 Let it be  $a'$ .  $\therefore aa' \equiv 1 \pmod{26}$ .

$$\text{From } C \equiv aP + b \pmod{26},$$

$$C - b \equiv aP \pmod{26},$$

$$a'(C - b) \equiv a'aP \equiv P \pmod{26}$$

since  $a'a \equiv 1 \pmod{26}$

$$\therefore P \equiv a'(C - b) \pmod{26}$$

(b) Using the linear cipher  $C \equiv 5P + 11 \pmod{26}$ ,  
 encrypt the message:

NUMBER THEORY IS EASY

Using  $A = 00, B = 01, \dots, Z = 25$ ,

N	U	M	B	E	R	T	H	E	O	R	Y	I	S	E	A	S	Y
13	20	12	1	4	17	19	7	4	14	17	24	8	18	4	0	18	24
76	111	71	16	31	96	106	46	31	81	96	131	51	101	31	11	101	131
24	7	19	16	5	18	2	20	5	3	18	1	25	23	5	11	23	1
Y	H	T	Q	F	S	C	U	F	D	S	B	Z	X	F	L	X	B

(c) Decrypt RZQTGU HOZTKGH AJ KTKMMTG,  
 which was produced using the linear cipher  
 $C \equiv 3P + 7 \pmod{26}$ .

$$\text{From (a), } 3x \equiv 1 \pmod{26}$$

$$\therefore 27x \equiv 9 \pmod{26}$$

$$\therefore x \equiv 9 \pmod{26}$$

$$\therefore 1 + a' = 9 \text{ as in (a)}$$

$$\therefore 9(C-7) \equiv 9(3P) = 27P \equiv P \pmod{26}$$

$$\therefore P \equiv 9C - 63 \equiv 9C + 15 \pmod{26}$$

RZQTGU

$$C: 17, 25, 16, 19, 6, 20$$

$$9(C-7): 90, 162, 81, 108, -9, 117$$

$$9(C-7) \pmod{26}: 12, 6, 3, 4, 17, 13$$

$$P: M G D E R N$$

(should have been RXQTGU  $\Rightarrow$  MODERN)

HOZTKGH

$$C: 7, 14, 25, 19, 10, 6, 7$$

$$9(C-7): 0, 63, 162, 108, 27, -9, 0$$

$$9(C-7) \pmod{26}: 0, 11, 6, 4, 1, 17, 0$$

$$P: A L G E B R A$$

A J

C: 3, 9

(should have been  
F G  $\Rightarrow$  I S)

9(C-7): -36, 18

9(C-7)(mod 26): 16, 18  
P: Q S

KTKMMMTG C: 10, 19, 10, 12, 12, 19, 6

9(C-7): 27, 108, 27, 45, 45, 108, -9

9(C-7)(mod 26): 1, 4, 1, 19, 19, 4, 17  
P: B E B T T E R

(should have been KTMMMTG)

4. In a lengthy ciphertext message, sent using a linear cipher  $C \equiv aP + b \pmod{26}$ , the most frequently occurring letter is Q and the second most frequent is J.

(a) Break the cipher by determining the values of a and b.

Q  $\Rightarrow$  16, J  $\Rightarrow$  9

$$\begin{aligned} \therefore 16 &\equiv aP_1 + b \pmod{26} \\ 9 &\equiv aP_2 + b \pmod{26} \end{aligned}$$

As the message is lengthy,  $P_1$  likely is E and  $P_2$  likely is T.

$$\therefore P_1 = E \Rightarrow 4$$

$$P_2 = T \Rightarrow 19$$

$$\therefore 16 \equiv 4a + 6 \pmod{26}$$

$$9 \equiv 19a + 6 \pmod{26}$$

$$\therefore 7 \equiv -15a \pmod{26}$$

$$30a \equiv -14, 30a - 26a \equiv -14, 4a \equiv -14, 4a \equiv 12,$$

$$a \equiv 3 \pmod{26}$$

$$\therefore 4a \equiv 12, \therefore 6 \equiv 4 \pmod{26}$$

$$\therefore a = 3, b = 4$$

(b) Using (a),  $C \equiv 3P + 4 \pmod{26}$ ,

$$C - 4 \equiv 3P \pmod{26}$$

$$9(C-4) \equiv 27P \equiv P \pmod{26}$$

$$\therefore P = 9(C-4) \pmod{26}$$

WCPQ      C: 22, 2, 15, 16

$$9(C-4): 162, -18, 99, 108$$

$$9(C-4) \pmod{26}: 6, 8, 21, 4$$

$$P: G I V E$$

JZQO      C: 9, 25, 16, 14  
 $g(c-4)$ : 45, 189, 108, 90  
 $g(c-4)(\text{mod } 26)$ : 17, 7, 4, 12  
 $P$ : T H E M

MX      C: 12, 23  
 $g(c-4)$ : 72, 171  
 $g(c-4)(\text{mod } 26)$ : 20, 15  
 $P$ : U P

5. (a) Encipher the message HAVE A NICE TRIP using a Vigenère cipher with the keyword MATH.

MATH  $\Rightarrow$  12 00 19 07

H	A	V	E	A	N	I	C	E	T	R	I	P
7	0	21	4	0	13	8	2	4	19	17	8	15
+ 12	0	19	7	12	0	19	7	12	0	19	7	12
19	0	40	11	12	13	27	9	16	19	36	15	27
19	0	14	11	12	13	1	9	16	19	10	15	1 (mod 26)

T A O L    M    N B J Q    T K P B

(b) The ciphertext BS FMX KFSGR JAPWL is

Known to have resulted from a Vigenère cipher, whose Keyword is YES. Obtain the deciphering congruences and read the message.

$YES = 24 \ 4 \ 18$ . Subtract YES (mod 26)  
from ciphertext to get plaintext.

B	S	F	M	X	K	F	S	G	R	J	A	P	W	L
1	18	5	12	23	10	5	18	6	17	9	0	15	22	11
24	4	18	24	4	18	24	4	18	24	4	18	24	4	18
														YES
														-YES
3	14	13	14	19	18	7	14	14	19	5	8	17	18	19
0	0	N	O	T	S	H	O	O	T	F	I	R	S	T
(mod 26)														

6.(a). Use the Hill cipher  $C_1 \equiv 5P_1 + 2P_2 \pmod{26}$   
 $C_2 \equiv 3P_1 + 4P_2 \pmod{26}$

to encipher GIVE THEM TIME

Note  $\gcd(5 \cdot 4 - 3 \cdot 2, 26) = \gcd(14, 26) = 2$ ,  
so you can encipher, but not decipher.

G	I	V	E	T	H	E	M	T	I	M	E
6	8	21	4	19	7	4	12	19	8	12	4

Break up text in blocks of 2 letters.

$$GI: C_1 \equiv 5(6) + 2(8) = 40 \equiv 14 \pmod{26} \Rightarrow O$$
$$C_2 \equiv 3(6) + 4(8) = 50 \equiv 24 \pmod{26} \Rightarrow Y$$

$$VE: C_1 \equiv 5(21) + 2(4) = 113 \equiv 9 \Rightarrow J$$
$$C_2 \equiv 3(21) + 4(4) = 79 \equiv 1 \Rightarrow B$$

$$TH: C_1 \equiv 5(19) + 2(7) = 109 \equiv 5 \Rightarrow F$$
$$C_2 \equiv 3(19) + 4(7) = 85 \equiv 7 \Rightarrow H$$

$$EM: C_1 \equiv 5(4) + 2(12) = 44 \equiv 18 \Rightarrow S$$
$$C_2 \equiv 3(4) + 4(12) = 60 \equiv 8 \Rightarrow I$$

$$TI: C_1 \equiv 5(19) + 2(8) = 111 \equiv 7 \Rightarrow H$$
$$C_2 \equiv 3(19) + 4(8) = 89 \equiv 11 \Rightarrow L$$

$$ME: C_1 \equiv 5(12) + 2(4) = 68 \equiv 16 \Rightarrow Q$$
$$C_2 \equiv 3(12) + 4(4) = 52 \equiv 0 \Rightarrow A$$

$\therefore OYJB FHSI HLQA$

(6). The ciphertext ALXWU VAOCOJO has been enciphered using  $C_1 \equiv 4P_1 + 11P_2 \pmod{26}$   
 $C_2 \equiv 3P_1 + 8P_2 \pmod{26}$

Derive the plaintext.

$$\text{Note } \gcd(4 \cdot 8 - 3 \cdot 11, 26) = \gcd(-1, 26) = 1$$

$$\begin{array}{l} 3C_1 \equiv 12P_1 + 33P_2 \pmod{26} \\ 4C_2 \equiv 12P_1 + 32P_2 \pmod{26} \end{array}$$

---

$$\begin{array}{l} 8C_1 \equiv 32P_1 + 88P_2 \\ 11C_2 \equiv 33P_1 + 88P_2 \end{array}$$

$$3C_1 - 4C_2 \equiv P_2 \pmod{26} \quad 11C_2 - 8C_1 \equiv P_1 \pmod{26}$$

A L X W U V A D C O J O  
0 11 23 22 20 21 0 3 2 14 9 14

$$\begin{array}{l} AL: P_1 \equiv -8(0) + 11(11) = 121 \equiv 17 \Rightarrow R \\ P_2 \equiv 3(0) - 4(11) = -44 \equiv 8 \Rightarrow I \end{array}$$

$$\begin{array}{l} LW: P_1 \equiv -8(23) + 11(22) = 58 \equiv C \Rightarrow G \\ P_2 \equiv 3(23) - 4(22) = -19 \equiv 7 \Rightarrow H \end{array}$$

$$\begin{array}{l} UV: P_1 \equiv -8(20) + 11(21) = 71 \equiv 19 \Rightarrow T \\ P_2 \equiv 3(20) - 4(21) = -24 \equiv 2 \Rightarrow C \end{array}$$

$$\begin{array}{l} AD: P_1 \equiv -8(0) + 11(3) = 33 \equiv 7 \Rightarrow H \\ P_2 \equiv 3(0) - 4(3) = -12 \equiv 14 \Rightarrow O \end{array}$$

$$\begin{array}{l} CO: P_1 \equiv -8(2) + 11(14) = 138 \equiv 8 \Rightarrow I \\ P_2 \equiv 3(2) - 4(14) = -50 \equiv 2 \Rightarrow C \end{array}$$

$$\begin{aligned} \text{JO: } P_1 &\equiv -8(9) + 11(14) = 82 \equiv 4 \Rightarrow E \\ P_2 &\equiv 3(9) - 4(14) = -29 \equiv 23 \Rightarrow X \end{aligned}$$

$\therefore$  RIGHT CHOICES

(Last two enciphered letters should have been GA to make plaintext CHOICES).

7. A long string of ciphertext resulting from a Hill cipher

$$C_1 \equiv aP_1 + bP_2 \pmod{26}$$

$$C_2 \equiv cP_1 + dP_2 \pmod{26}$$

revealed that the most frequently occurring two-letter blocks were HO and PP, in that order.

(a) Find the values of  $a, b, c, d$

Using the hint that the most common 2-letter blocks in English are TH and then HE, we have:

$$\begin{aligned} H &\equiv a(T) + b(H) \pmod{26} \quad [1] \\ O &\equiv c(T) + d(H) \pmod{26} \quad [2] \end{aligned}$$

$$\begin{aligned} \text{and: } P &\equiv a(H) + b(E) \pmod{26} \quad [3] \\ P &\equiv c(H) + d(E) \pmod{26} \quad [4] \end{aligned}$$

Or, using  $00 \Rightarrow A, \dots, 25 \Rightarrow Z$

$$\begin{aligned} 7 &\equiv 19a + 7b \pmod{26} & [1] \\ 14 &\equiv 19c + 7d \pmod{26} & [2] \end{aligned}$$

$$\begin{aligned} 15 &\equiv 7a + 4b \pmod{26} & [3] \\ 15 &\equiv 7c + 4d \pmod{26} & [4] \end{aligned}$$

From [1] and [3],  $7 \equiv 19a + 7b \pmod{26}$   
 $15 \equiv 7a + 4b \pmod{26}$

Note that  $\gcd(19 \cdot 4 - 7 \cdot 7, 26) = \gcd(27, 26) = 1$

$$\begin{aligned} \therefore 28 &\equiv 76a + 28b \\ 105 &\equiv 49a + 28b \\ \hline -77 &\equiv 27a \pmod{26} \\ -77 + 3 \cdot 26 &\equiv 27a - 26a \\ 1 &\equiv a \pmod{26} \end{aligned} \quad \left. \begin{array}{l} \therefore 7 \equiv 19 + 7b \\ -12 \equiv 7b \\ 14 \equiv 7b \\ 2 \equiv b \pmod{26} \\ \text{as } \gcd(7, 26) = 1 \end{array} \right\}$$

$$\therefore a = 1, b = 2$$

$$\begin{aligned} \text{From [2], [4], } 14 &\equiv 19c + 7d \pmod{26} \\ 15 &\equiv 7c + 4d \pmod{26} \\ \text{and } \gcd(4 \cdot 19 - 7 \cdot 7, 26) &= \gcd(27, 26) = 1 \end{aligned}$$

$$\begin{aligned} \therefore 5G &\equiv 76C + 28d \Rightarrow 14 \equiv 57 + 7d, -43 \equiv 7d, \\ \frac{105}{-49} &\equiv \frac{49C + 28d}{27C} \quad | \quad 9 \equiv 7d, 99 \equiv 77d, \\ \therefore 3 &\equiv C \pmod{26} \quad | \quad 21 \equiv -d, d \equiv -21, \\ & \qquad \qquad \qquad d \equiv 5 \end{aligned}$$

$$\therefore \underline{\underline{C = 3, d = 5}}$$

$$\begin{aligned} \therefore C_1 &\equiv P_1 + 2P_2 \pmod{26} \\ C_2 &\equiv 3P_1 + 5P_2 \pmod{26} \end{aligned}$$

(5) What is the plain text for the intercepted message: PPIH HOG RAPVT

$$\begin{array}{l} \text{From (a)} \quad 3C_1 \equiv 3P_1 + 6P_2 \quad 5C_1 \equiv 5P_1 + 10P_2 \\ \underline{C_2 \equiv 3P_1 + 5P_2} \quad \underline{2C_2 \equiv 6P_1 + 10P_2} \\ 3C_1 - C_2 \equiv \quad P_2 \quad 2C_2 - 5C_1 \equiv P_1 \end{array}$$

$$\begin{aligned} \therefore P_1 &\equiv -5C_1 + 2C_2 \pmod{26} \\ P_2 &\equiv 3C_1 - C_2 \pmod{26} \end{aligned}$$

P	P	I	H	H	O	G	R	A	P	V	T
15	15	8	7	7	14	6	17	0	15	21	19

PP: HE

IH: 8, 7     $P_1 \equiv -5(8) + 2(7) = -26 \equiv 0 \Rightarrow A$   
 $P_2 \equiv 3(8) - 7 = 17 \Rightarrow R$

HO : THT

GR: 6, 17     $P_1 \equiv -5(6) + 2(17) = 4 \Rightarrow E$   
 $P_2 \equiv 3(6) - 17 = 1 \Rightarrow B$

AP: 0, 15     $P_1 \equiv -5(0) + 2(15) = 30 \equiv 4 \Rightarrow E$   
 $P_2 \equiv 3(0) - 15 = -15 \equiv 11 \Rightarrow L$

VT: 21, 19     $P_1 \equiv -5(21) + 2(19) = -67 \equiv 11 \Rightarrow L$   
 $P_2 \equiv 3(21) - 19 = 44 \equiv 18 \Rightarrow S$

-: HEAR THE BELLS

8. If  $n = pq = 274279$ , and  $\phi(n) = 272376$ , find the primes  $p$  and  $q$ .

Use the hint. Note, since  $n = pq$ ,  $\phi(n) = (p-1)(q-1)$   
-:  $n - \phi(n) = pq - (p-1)(q-1)$

$$= pq - [pq - p - q + 1] = p + q - 1$$

$$\therefore p+q = n - \phi(n) + 1$$

$$\text{Also, } p-q = \left[ (p-q)^2 \right]^{\frac{1}{2}} = \left[ p^2 - 2pq + q^2 \right]^{\frac{1}{2}}$$

$$= \left[ p^2 + 2pq + q^2 - 4pq \right]^{\frac{1}{2}}$$

$$= \left[ (p+q)^2 - 4n \right]^{\frac{1}{2}}$$

$$\therefore p+q = n - \phi(n) + 1 = 274279 - 272376 + 1 = 1904$$

$$p-q = \left[ (p+q)^2 - 4n \right]^{\frac{1}{2}}$$

$$\therefore 2p = n - \phi(n) + 1 + \left[ (n - \phi(n) + 1)^2 - 4n \right]^{\frac{1}{2}}$$

$$= 1904 + \left[ 1904^2 - 4(274279) \right]^{\frac{1}{2}}$$

$$= 1904 + \left[ 2528100 \right]^{\frac{1}{2}} = 1904 + 1590$$

$$= 3494$$

$$\therefore \underline{p} = 1747, \underline{q} = 157$$

9. When the RSA algorithm is based on the key  $(n, k) = (3233, 37)$  what is the

recovery exponent for the cryptosystem?

The recovery exponent is integer  $j$  satisfying

$$k_j \equiv 1 \pmod{\phi(n)}, \text{ or}$$

$$37j \equiv 1 \pmod{\phi(3233)}$$

The prime factorization of 3233:

$$\sqrt{3233} = 56.8, \text{ so } p \leq 56. \quad 3233 = 53 \cdot 61$$

$$\therefore \phi(n) = 52(60) = 3120$$

$$\therefore 37j \equiv 1 \pmod{3120}$$

Now  $\gcd(37, 3120) = 1$  since

$$\begin{aligned} 3120 &= 10(312) = 5 \cdot 2 \cdot 2 \cdot 156 = 2^2 \cdot 5 \cdot (3 \cdot 2 \cdot 26) \\ &= 2^4 \cdot 3 \cdot 5 \cdot 13 \end{aligned}$$

$\therefore$  By prob. # 8(a), sec. 7.3, The solution

$$\text{is } j \equiv 37^{\phi(3120)-1} \pmod{3120}$$

$$\phi(3120) = (2^4 \cdot 2^3) \cdot (2)(4)(12) = 768$$

$$\therefore j \equiv 37^{767} \pmod{3120}$$

Note that since  $3120 = 2^4 \cdot 3 \cdot 5 \cdot 13$ , gcd of 37 and any of these factors is 1.

$$\begin{aligned}\therefore \phi(13) &= 12, \text{ so by Euler's Th., } 37^{12} \equiv 1 \pmod{13} \\ \therefore 37^{12} &\equiv 1 \pmod{3120}\end{aligned}$$

$$767 = 12 \cdot 63 + 11$$

$$\therefore 37^{767} = (37^{12})^{63} \cdot 37^{11} \equiv 1^{63} \cdot 37^{11} \equiv 37^{11} \pmod{3120}$$

$$\therefore j \equiv 37^{11} \pmod{3120}$$

$$37^3 = 50653 = 3120 \cdot 16 + 733$$

$$\therefore 37^3 \equiv 733 \pmod{3120}$$

$$\therefore 37^6 \equiv 733^2 = 537289 = 172 \cdot 3120 + 649$$

$$\therefore 37^6 \equiv 649 \pmod{3120}$$

$$\therefore 37^9 \equiv 733 \cdot 649 = 475717 = 152 \cdot 3120 + 1477$$

$$\therefore 37^9 \equiv 1477 \pmod{3120}$$

$$37^2 = 1369$$

$$\therefore 37^{11} \equiv 1477 \cdot 1369 = 2022013 = 648 \cdot 3120 + 253$$

$$\therefore 37^{11} \equiv 253 \pmod{3120}$$

$$\therefore j \equiv \underline{\underline{253}} \pmod{3120}$$

10. Encrypt the plaintext message GOLD MEDAL using the RSA algorithm with key  $(n, k) = (2419, 3)$ .

Using 99 for the space between words,

G	O	L	D	M	E	D	A	L	
06	14	11	03	99	12	04	03	00	11

$$\therefore m' = 6141103991204030011$$

With  $n = 2419$ ,  $m'$  is broken into blocks of 3 digits, starting from the right.

$$\therefore 006 \ 141 \ 103 \ 991 \ 204 \ 030 \ 011$$

Now convert each block using:

$$m_i^k \equiv r \pmod{n}, \text{ or } m_i^3 \equiv r \pmod{2419}$$

$$006 : 6^3 \equiv 216 \pmod{2419}$$

$$141 : 141^3 = 2803221 = 1158 \cdot 2419 + 2019$$

$$\therefore 141^3 \equiv 2019 \pmod{2419}$$

$$103 : 103^3 = 1092727 = 451 \cdot 2419 + 1758$$
$$\therefore 103^3 \equiv 1758 \pmod{2419}$$

$$991: 991^3 = 973242271 = 402332 \cdot 2419 + 1163$$

$$\therefore 991^3 \equiv 1163 \pmod{2419}$$

$$204: 204^3 = 8489664 = 3509 \cdot 2419 + 1393$$

$$\therefore 204^3 \equiv 1393 \pmod{2419}$$

$$030: 30^3 = 27000 = 11 \cdot 2419 + 391$$

$$\therefore 30^3 \equiv 391 \pmod{2419}$$

$$011: 11^3 = 1331$$

$$\therefore 11^3 \equiv 1331 \pmod{2419}$$

$\therefore$  Ciphertext is:

0216 2019 1758 1163 1393 0391 1331

=

To check, note  $2419 = 41 \cdot 59$ ,

$$\therefore \phi(2419) = 40 \cdot 58 = 2320$$

$$\therefore k_j \equiv 1 \pmod{\phi(n)} \Rightarrow 3_j \equiv 1 \pmod{2320}$$

$$\therefore 773 \cdot 3_j \equiv 773, 2319_j \equiv 773, -j \equiv 773,$$

$$\therefore j \equiv -773 \equiv 2320 - 773 = 1547$$

$$\therefore j \equiv 1547 \pmod{2320}$$

$$\therefore 216^{1547} = (6^3)^{1547} = 6^{4641} = 6^{2 \cdot 2320 + 1}$$

$$\equiv 6 \pmod{2320}$$

∴ First code is 006

So can reconstitute  $m'$ , which is then broken into 2-digit numbers (starting from right) to get the letters.

11. The ciphertext message produced by the RSA algorithm with key  $(n, k) = (1643, 223)$  is:

0833 0823 1130 0055 0329 1099

Determine the original/plaintext message.

Note: to get  $j=7$  for recovery exponent,  $k=223$ , not 233. Both are prime, but assume a typo in book.

On the receiving side,  $1643 = 31 \cdot 53$

$$\therefore \phi(n) = 30 \cdot 52 = 1560$$

Recovery exponent:  $K_j \equiv 1 \pmod{\phi(n)}$ , or  
 $223^j \equiv 1 \pmod{1560}$

From 8.(g), sec. 7.3, solution is  $j \equiv 223^{\phi(1560)-1} \pmod{1560}$   
 $1560 = 2^3 \cdot 3 \cdot 5 \cdot 13$

$$\therefore \phi(1560) = 4 \cdot 2 \cdot 4 \cdot 12 = 384$$

$$\therefore j \equiv 223^{383} \pmod{1560}$$

$$\text{Since } \gcd(13, 223) = 1, 223^{12} \equiv 1 \pmod{13}$$

$$\therefore 223^{12} \equiv 1 \pmod{1560}$$

$$383 = 31 \cdot 12 + 11$$

$$\therefore 223^{383} = (223^{12})^{31} \cdot 223^{11} \equiv 223^{11} \pmod{1560}$$

$$\therefore j \equiv 223^{11} \pmod{1560}$$

$$223^2 = 32 \cdot 1560 - 191, \therefore 223^2 \equiv -191 \pmod{1560}$$

$$223^4 = (-191)^2 = 23 \cdot 1560 + 601$$

$$\therefore 223^8 \equiv 601^2 = 231 \cdot 1560 + 841$$

$$\therefore 223^8 \equiv 841, \therefore 223^{10} \equiv (841)(-191) = -160631$$

$$= -103 \cdot 1560 + 49$$

$$\therefore 223^{10} \equiv 49 \pmod{1560}$$

$$\therefore 223^{11} \equiv 49 \cdot 223 = 10927 = 7 \cdot 1560 + 7$$

$$\therefore j \equiv 223^{11} \equiv 7 \pmod{1560}$$

$\therefore$  recovery exponent is  $j = 7$

$\therefore$  modulo 1643

$$\text{0833: } 833^7 : 833^2 = 693889 = 422 \cdot 1643 + 543$$

$$833^4 \equiv 543^2 = 294849 = 179 \cdot 1643 + 752$$

$$833^6 \equiv 543 \cdot 752 = 248 \cdot 1643 + 872$$

$$\therefore 833^7 \equiv 872 \cdot 833 = 442 \cdot 1643 + 170$$

$$\therefore 833^7 \equiv \underline{170} \pmod{1643}$$

$$0823: 823^7 : \begin{aligned} 823^2 &\equiv 413 \\ 823^4 &\equiv 1340 \\ 823^6 &\equiv 1372 \\ 823^7 &\equiv \underline{\underline{415}} \end{aligned} \quad (\text{using a calculator})$$

$$1130 : 1130^7 : \begin{aligned} 1130^2 &\equiv 289 \\ 1130^4 &\equiv 1371 \\ 1130^6 &\equiv 256 \\ 1130^7 &\equiv \underline{\underline{112}} \end{aligned}$$

$$0055: 55^7 : \begin{aligned} 55^3 &\equiv 432 \\ 55^5 &\equiv 965 \\ 55^7 &\equiv \underline{\underline{499}} \end{aligned}$$

$$0329: 329^7 : \begin{aligned} 329^3 &\equiv 807 \\ 329^5 &\equiv 1149 \\ 329^7 &\equiv \underline{\underline{131}} \end{aligned}$$

$$1099 : 1099^7 : \begin{aligned} 1099^3 &\equiv 171 \\ 1099^5 &\equiv 1310 \\ 1099^7 &\equiv \underline{\underline{422}} \end{aligned}$$

$$\begin{aligned} \therefore M &= (70415112499131422 \\ &\quad 170415112499131422 \\ \therefore & R E P L Y \sqsubset N O W \end{aligned}$$

## 12. Decrypt the ciphertext

1369 1436 0119 0385 0434 1580 0690

That was encrypted using the RSA algorithm with key  $(n, k) = (2419, 211)$ .

$$n = 2419 = 41 \cdot 59 \quad \therefore \phi(n) = 40 \cdot 58 = 2320 = 2^4 \cdot 5 \cdot 29$$

$$\therefore 211_j \equiv 1 \pmod{2320} \quad \gcd(2320, 211) = 1$$

Using prob. 8.c., sec. 2.3,

$$\phi(2320) = 8 \cdot 4 \cdot 28 = 896, \quad \therefore j \equiv 211^{895} \pmod{2320}$$

$$\gcd(29, 211) = 1, \quad \therefore 211^{28} \equiv 1 \pmod{29} \text{ by Fermat's Theorem}$$

$$895 = 31 \cdot 28 + 27 \quad \therefore 211^{895} \equiv (211^{28})^{31} \cdot 211^{27}$$

$$\therefore j \equiv 211^{895} \equiv 211^{27} \pmod{2320}$$

$$211^3 \equiv 251 \pmod{2320} \quad [\text{calculator}]$$

$$211^6 \equiv 251^2 \equiv 361 \pmod{2320}$$

$$211^{12} \equiv 361^2 \equiv 401$$

$$211^{24} \equiv 401^2 \equiv 721$$

$$\therefore 211^7 \equiv 251 \cdot 721 \equiv 11 \pmod{2320}$$

$\therefore$  recovery exponent = 11

$\therefore$  modulo 2419,

$$1369 : 1369^2 \equiv 1855$$

$$1369^4 \equiv 1855^2 \equiv 1207$$

$$1369^8 \equiv 1207^2 \equiv 611$$

$$1369^{10} \equiv 611 \cdot 1855 \equiv 1313$$

$$1369^{11} \equiv 1313 \cdot 1369 \equiv \underline{180}$$

$$1436 : 1436^2 \equiv 1108$$

$$1436^4 \equiv 1231$$

$$1436^8 \equiv 1067$$

$$1436^{10} \equiv 1764$$

$$1436^{11} \equiv 1764 \cdot 1436 \equiv \underline{411}$$

$$0119 : 119^3 \equiv 1535$$

$$119^6 \equiv 119$$

$$119^8 \equiv 1535 \cdot 119 \equiv 1240$$

$$119^{11} \equiv 1240 \cdot 119^2 \equiv \underline{119}$$

$$0385 : 385^2 \equiv 666 \quad 385^8 \equiv 980 \quad 385^{11} \equiv \underline{918}$$

$$385^4 \equiv 879 \quad 385^{10} \equiv 1969$$

$$\begin{aligned}
 0434 : \quad & 434^2 \equiv 2093 \\
 & 434^4 \equiv 2259 \\
 & 434^8 \equiv 1410 \\
 & 434^{10} \equiv 2369 \\
 & 434^{11} \equiv \underline{71} \quad \Rightarrow 071
 \end{aligned}$$

$$\begin{aligned}
 1580 : \quad & 1580^2 \equiv 2411 \\
 & 1580^4 \equiv 64 \\
 & 1580^8 \equiv 1677 \\
 & 1580^{10} \equiv 1098 \\
 & 1580^{11} \equiv \underline{417}
 \end{aligned}$$

$$\begin{aligned}
 0690 : \quad & 690^2 \equiv 1976 \\
 & 690^4 \equiv 310 \\
 & 690^8 \equiv 1759 \\
 & 690^{10} \equiv 2100 \\
 & 690^{11} \equiv \underline{19} \quad \Rightarrow
 \end{aligned}$$

Since  $n = 2419$ , plaintext should have been broken up into 3-digit blocks.

$\therefore 1804111991807141719$   
 18 04 11 11 99 18 07 14 17 19  
 S E L C U S H O R T

So, wasn't enciphered properly, since only 10

2-digits codis (20 numbers).

Should have been (multiple of 3):

018 041 111 991 807 141 719

and ∵ 018, 041, 111, 991, 807, 141, 719

i.e., for consistency, how do you know to precede 71 above so it's 071, but 19 isn't translated to 019.

The only way to know is always precede a 2-digit decrypted number with 0 until get to end: if need it, add the 0, if don't, don't do it: confusing.

i.e., when decrypting, must know size of block of plaintext that was enciphered. Should then use same block size when deciphering.

13. Obtain all solutions of the knapsack problem

$$ZI = 2x_1 + 3x_2 + 5x_3 + 7x_4 + 9x_5 + 11x_6$$

Let  $x_6 = 1$  ∵  $x_5 \neq 1$  since no possible "1"

$$\therefore x_5 = 0$$

$$\therefore 10 = 2x_1 + 3x_2 + 5x_3 + 7x_4$$

$$x_4 = 1 : x_1 = 0, x_2 = 1, x_3 = 0$$

$$x_4 = 0 : x_1 = 1, x_2 = 1, x_3 = 1$$

$$\therefore \{x_1, x_2, x_3, x_4, x_5, x_6\} = \{0, 1, 0, 1, 0, 1\}$$

or  $\{1, 1, 1, 0, 0, 1\}$

Let  $x_6 = 0$  :  $21 = 2x_1 + 3x_2 + 5x_3 + 7x_4 + 9x_5$

Let  $x_5 = 1$  :  $12 = 2x_1 + 3x_2 + 5x_3 + 7x_4$

$$\therefore x_1 = 0, x_2 = 0, x_3 = 1, x_4 = 1$$

$$x_1 = 1, x_2 = 1, x_3 = 0, x_4 = 1$$

No solution if  $x_4 = 0$

$$\therefore \{0, 0, 1, 1, 1, 0\},$$

$$\{1, 1, 0, 1, 1, 0\}$$

Let  $x_5 = 0$  :  $21 = 2x_1 + 3x_2 + 5x_3 + 7x_4$

No solution even if all = 1.

=

$\therefore$  All solutions :  $x_1 \ x_2 \ x_3 \ x_4 \ x_5 \ x_6$

0	1	0	1	0	1
1	1	1	0	0	1
0	0	1	1	1	0
1	1	0	1	1	0

14. Determine which of the sequences below is superincreasing:

(a) 3, 13, 20, 37, 81

$3 < 13, 3 + 13 < 20, 3 + 13 + 20 < 37, 3 + 13 + 20 + 37 < 81$   
 $\therefore$  yes, it is superincreasing

(b) 5, 13, 25, 42, 90

No, since  $5 + 13 + 25 = 43 > 42$

(c) 7, 27, 47, 97, 197, 397

$7 + 27 < 47, 2(47) < 97, 2(97) < 197, 2(197) < 397$   
 $\therefore$  yes, it's superincreasing

15. Find the unique solution of each of the following superincreasing Knapsack problems:

(a)  $118 = 4x_1 + 5x_2 + 10x_3 + 20x_4 + 41x_5 + 99x_6$

Since  $4 + 5 + 10 + 20 + 41 = 80 < 118$ , then  $x_6 \neq 0$

$\therefore x_6 = 1, \therefore 19 = 4x_1 + 5x_2 + 10x_3 + 20x_4 + 41x_5$

$\therefore x_5 = 0 \quad (41 > 19)$

$x_4 = 0 \quad (20 > 19)$

$\therefore \{x_1, x_2, x_3, x_4, x_5, x_6\} = \{1, 1, 1, 0, 0, 1\}$

$$(b) 51 = 3x_1 + 5x_2 + 9x_3 + 18x_4 + 37x_5$$

Since  $3+5+9+18=35 < 51$ ,  $x_5$  must be 1.

$$\therefore x_5 = 1, 14 = 3x_1 + 5x_2 + 9x_3 + 18x_4$$

$$\therefore x_4 = 0 \quad (18 > 14)$$

If  $x_3 = 1$ , Then  $x_2 = 1, x_1 = 0$   
 $x_3 = 0$ , no solution.

$$\therefore \{x_1, x_2, x_3, x_4, x_5\} = \{0, 1, 1, 0, 1\}$$

$$(c) 54 = x_1 + 2x_2 + 5x_3 + 9x_4 + 18x_5 + 40x_6$$

Since  $1+2+5+9+18=35 < 54$ ,  $x_6$  must be 1

$$\therefore x_6 = 1 : 14 = x_1 + 2x_2 + 5x_3 + 9x_4 + 18x_5$$

$$\therefore x_5 = 0 \quad (18 > 14)$$

Let  $x_4 = 1$ .  $\therefore x_1 = 0, x_2 = 0, x_3 = 1$

$x_4 = 0$  : no solution

$$\therefore \{x_1, x_2, x_3, x_4, x_5, x_6\} = \{0, 0, 1, 1, 0, 1\}$$

16. Consider a sequence of positive integers  $a_1, \dots, a_n$ , where  $a_{i+1} > 2a_i$ , for  $i=1, \dots, n-1$ . Show that the sequence is superincreasing.

Pf: By induction, for  $n=2$ ,  $a_2 > 2a_1$ , so  $a_2 > a_1$ .

$$\begin{aligned} \text{For } n = 3, \quad a_3 &> 2a_2 = a_2 + a_2 > a_2 + (2a_1) \\ &> a_2 + a_1 \end{aligned}$$

$\therefore$  Assume sequence is superincreasing  
for  $k \geq 3$  ( $i.e., a_k > a_1 + a_2 + \dots + a_{k-1}$ )

$$\therefore a_{k+1} > 2a_k, \text{ by definition}$$

$$\begin{aligned} \therefore a_{k+1} &> a_k + a_k \\ &> a_k + (a_1 + a_2 + \dots + a_{k-1}) \end{aligned}$$

$$\therefore a_{k+1} > a_1 + a_2 + \dots + a_{k-1} + a_k$$

$\therefore$  Superincreasing for all  $n$

17. A user of the Knapsack cryptosystem has the sequence 49, 32, 36, 43 as a listed encryption key. If the user's private key involves the modulus  $m = 50$  and multiplier  $a = 33$ , determine the secret superincreasing sequence.

Let  $a_1, a_2, a_3, a_4$  be the superincreasing sequence

Note that  $\gcd(33, 50) = 1$ , so  $s_i \equiv 33a_i \pmod{50}$

has a unique solution for  $a_i$ , given  $b$ . (by corollary to Th. 4.7, sec. 4.4, on p. 76).

$$\begin{array}{ll} \therefore 33a_1 \equiv 49 \pmod{50} & 33a_2 \equiv 32 \pmod{50} \\ 99a_1 \equiv 3(49) - 150 & 99a_2 \equiv 96 - 100 \\ -a_1 \equiv -3 & -a_2 \equiv -4 \\ a_1 \equiv 3 & a_2 \equiv 4 \end{array}$$

$$\begin{array}{ll} 33a_3 \equiv 30 \pmod{50} & 33a_4 \equiv 43 \pmod{50} \\ 99a_3 \equiv 90 - 100 & 99a_4 \equiv 3(43) - 150 \\ -a_3 \equiv -10 & -a_4 \equiv -21 \\ a_3 \equiv 10 & a_4 \equiv 21 \end{array}$$

$$\therefore a_1, a_2, a_3, a_4 = 3, 4, 10, 21$$

18. The ciphertext message produced by the Knapsack cryptosystem employing the superincreasing sequence  $1, 3, 5, 11, 35$ , modulus  $m=73$  and multiplier  $a=5$  is:  $55, 15, 124, 109, 25, 34$   
Obtain the plaintext message.

(i) First find The unique solution to:

(multiplier)  $x \equiv 1 \pmod{\text{modulus}}$ , or

$$5x \equiv 1 \pmod{73} \quad (\text{note } \gcd(5, 73) = 1).$$

$$29(5x) \equiv 29, \quad 145x - 146x \equiv 29, \\ x \equiv -29 + 73, \quad \underline{x \equiv 44}$$

(2) Now convert ciphertext using  
 $s' \equiv 44s \pmod{73}$

$$55: s' \equiv 44(55) \pmod{73} \quad (\text{using calculator})$$
$$s' \equiv \underline{\underline{11}}$$

$$15: s' \equiv 44(15) \pmod{73}$$
$$s' \equiv \underline{\underline{3}}$$

$$124: s' \equiv 44(124) \pmod{73}$$
$$s' \equiv \underline{\underline{54}}$$

$$109: s' \equiv 44(109) \pmod{73}$$
$$s' \equiv \underline{\underline{51}}$$

$$25: s' \equiv 44(25) \pmod{73}$$
$$s' \equiv \underline{\underline{5}}$$

$$34: s' \equiv 44(34) \pmod{73}$$
$$s' \equiv \underline{\underline{36}}$$

(3) Now solve knapsack problems using secret sequence, noting that  $s' \equiv 44s \pmod{73}$ ,  
 $s' \equiv 44(b_1x_1 + \dots + b_5x_5)$ ,  $b_i = aq_i$ ,  $a$  = multiplier,  
so  $s' \equiv 44aq_1x_1 + \dots + 44aq_5x_5$ , and since

$44a \equiv 1 \pmod{73}$ , Then,  $S' = a_1x_1 + \dots + a_5x_5$ ,  
 where  $x_i$  is the binary code of the plaintext letter.

$$\therefore S' = 11, 3, 54, 51, 5, 36$$

$$a_1, a_2, a_3, a_4, a_5 = 1, 3, 5, 11, 35$$

$$\begin{aligned} \therefore 11: 11 &= x_1 + 3x_2 + 5x_3 + 11x_4 + 35x_5 \\ &\because x_1 = x_2 = x_3 = 0, x_4 = 1, x_5 = 0 \end{aligned}$$

$$\therefore 00010 \Rightarrow \underline{\underline{C}}$$

$$\begin{aligned} 3: 3 &= x_1 + 3x_2 + 5x_3 + 11x_4 + 35x_5 \\ &\therefore x_1 = 0, x_2 = 1, x_3 = x_4 = x_5 = 0 \end{aligned}$$

$$\therefore 01000 \Rightarrow \underline{I}$$

$$\begin{aligned} 54: 54 &= x_1 + 3x_2 + 5x_3 + 11x_4 + 35x_5 \\ &\therefore x_1 = 0, x_2 = x_3 = x_4 = x_5 = 1 \end{aligned}$$

$$\therefore 01111 \Rightarrow \underline{P}$$

$$\begin{aligned} 51: 51 &= x_1 + 3x_2 + 5x_3 + 11x_4 + 35x_5 \\ &\therefore x_1 = x_2 = 0, x_3 = x_4 = x_5 = 1 \\ &\therefore 00111 \Rightarrow \underline{H} \end{aligned}$$

$$5: 5 = x_1 + 3x_2 + 5x_3 + 11x_4 + 35x_5$$

$$\therefore x_1 = x_2 = 0, x_3 = 1, x_4 = x_5 = 0$$

$$\therefore 00100 \Rightarrow \underline{E}$$

$$36: 36 = x_1 + 3x_2 + 5x_3 + 11x_4 + 35x_5$$

$$\therefore x_1 = 1, x_2 = x_3 = x_4 = 0, x_5 = 1$$

$$\therefore 10001 \Rightarrow \underline{R}$$

CIPHER

19. A user of the knapsack cryptosystem has a private key consisting of the superincreasing sequence  $[2, 3, 7, 13, 27]$ , modulus  $m = 60$ , and multiplier  $a = 7$ .

(a) Find the user's listed public key

$$7(2) = 14$$

$$7(3) = 21$$

$$7(7) = 49$$

$$7(13) = 91 \equiv 31 \pmod{60}$$

$$7(27) = 189 \equiv 9 \pmod{60}$$

$$\therefore 14, 21, 49, 31, 9$$

(6) With the aid of the public key, encrypt the message: SEND MONEY.

First convert to binary equivalent:

$$SEND \Rightarrow 10010 \quad 00100 \quad 01101 \quad 00011$$

$$MONEY \Rightarrow 01100 \quad 01110 \quad 01101 \quad 00100 \quad 11000$$

The public key has 5 terms, so need blocks of 5 binary digits, which in this case is each letter (represented by 5 digits).

$$\therefore 10010 \Rightarrow [1, 0, 0, 1, 0] \cdot [14, 21, 49, 31, 9] = 14 + 31 = 45$$

$$00100 \Rightarrow [0, 0, 1, 0, 0] \cdot [14, 21, 49, 31, 9] = 49$$

$$01101 \Rightarrow [0, 1, 1, 0, 1] \cdot [14, 21, 49, 31, 9] = 21 + 49 + 9 = 79$$

$$00011 \Rightarrow [0, 0, 0, 1, 1] \cdot [14, 21, 49, 31, 9] = 31 + 9 = 40$$

$$01100 \Rightarrow [0, 1, 1, 0, 0] \cdot [14, 21, 49, 31, 9] = 21 + 49 = 70$$

$$01110 \Rightarrow [0, 1, 1, 1, 0] \cdot [14, 21, 49, 31, 9] = 21 + 49 + 31 = 101$$

$$01101 \Rightarrow [0, 1, 1, 0, 1] \cdot [14, 21, 49, 31, 9] = 21 + 49 + 9 = 79$$

$$00100 \Rightarrow [0, 0, 1, 0, 0] \cdot [14, 21, 49, 31, 9] = 49$$

$$11000 \Rightarrow [1, 1, 0, 0, 0] \cdot [14, 21, 49, 31, 9] = 14 + 21 = 35$$

$$\therefore 45, 49, 79, 40, 70, 101, 79, 49, 35$$

## 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

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

$$2^2 \equiv 4, 2^4 \equiv 16, 2^8 \equiv 1 \pmod{17}$$

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

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

$$\therefore \text{ord}(2) = 8 \pmod{17}$$

$$\text{ord}(3) = 16 \pmod{17}$$

$$\text{ord}(5) = 16 \pmod{17}$$

- (b) modulo 19

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

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

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

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

- (c) modulo 23

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

$$2^2 \equiv 4, 2'' \equiv 1, \therefore \text{Ord}(2) = 11$$

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

$$5^2 \equiv 2, 5''' \equiv 22, 5^{22} \equiv 1, \therefore \text{Ord}(5) = 22$$

2. Establish each of the statements below:

(a) If  $a$  has order  $hk$  modulo  $n$ , Then  $a^h$  has order  $k$  modulo  $n$ .

$$\text{Pf: } a^{hk} \equiv 1 \pmod{n} \Rightarrow (a^h)^k \equiv 1 \pmod{n}$$

$$\text{Suppose } (a^h)^r \equiv 1 \pmod{n}, 0 < r < k$$

$\therefore 0 < hr < hk$ . 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.

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

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

$$\therefore p | (a^{k-1})(a^{k+1})$$

If  $p | (a^{k-1})$ , Then  $a^k \equiv 1 \pmod{p}$ , so

$a$  would not have order  $2k$ .

$$\therefore p \nmid a^{k-1}, \text{ so } p \nmid (a^k + 1) \quad (\text{by Th. 3.1})$$

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

(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  $\phi(n) \leq n-2$ . 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  $2^n - 1$ .

$$\therefore 2^k \equiv 1 \pmod{2^n - 1}, \text{ or } 2^k - 1 = a(2^n - 1), a > 0$$

But  $2^k > 1$  for  $k \geq 1$ , 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  $2 \pmod{2^n - 1}$  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  $a \pmod{n}$  is  $h$ , and  
order of  $b \pmod{n}$  is  $K$

Show the order of  $ab \pmod{n}$  divides  $hk$ .

In particular, if  $\gcd(h, K) = 1$ , then  $ab$  has order  $hk$ .

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

$$\begin{aligned} \therefore a^{hk} &\equiv 1^K \equiv 1 \pmod{n} \\ b^{kh} &\equiv 1^h \equiv 1 \pmod{n} \end{aligned}$$

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

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

(2) Suppose  $\gcd(h, K) \neq 1$

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  $w = \text{order of } aS$ . 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  $0 \leq l_i \leq h_i$ ,  $0 \leq m_i \leq k_i$ .

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  $h = h' h_x$ ,  $k = k' k_y$

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

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

But  $(a^{h_x k_y} b^{h_x k_y})^{h'} = a^{h' h_x k_y} b^{h' h_x k_y}$

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

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

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

Since order of  $b$  is  $K$ , Then by Th. 8.1,

$k|h k_y$ . Since  $\gcd(h, K) = 1$ , Then  $k|k_y$

$\therefore k_y|K$  and  $k|k_y \Rightarrow k_y = k$ .

Similarly,  $h_x = h$ .

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

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

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

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

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

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

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

$$(a+1)^3 \equiv a(a+1) = a^2 + a \equiv -1 \pmod{p} \quad [\text{from L1}]$$

$$(a+1)^4 = [(a+1)^2]^2 = a^2 \quad \therefore \text{order } a+1 \neq 4$$

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

$$(a+1)^6 = [(a+1)^3]^2 \equiv (-1)^2 = 1 \pmod{p}. \quad \therefore \text{order } a+1 \neq 5$$

Also,  $a+1 \neq 1$ . If true, then  $a \equiv 0 \Rightarrow a^3 \equiv 0$   
contradicting order of  $a$  is 3.

Also,  $a \neq -1$ , since if true,  $a$  would have  
order 1.

$\therefore$  Order  $(a+1) \pmod{p}$  is 6.

C. 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  $n = kp$ ,  $n^2 = k^2 p^2$ ,  
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  $n \pmod{p}$ .  $\therefore$  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  $n \pmod{p}$  is 4.

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

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

(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  $n \pmod{p}$ .

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

$\therefore r = 1, 2, 4, \text{ or } 8$

Order of  $n$  can't be 1, for  $n = 1 \Rightarrow n^4 \equiv 1$ .

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  $n \pmod{p}$  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  $\geq 2$ . For  $n=1$ ,  $n^2+n+1=3$ , so not of form  $6k+1$ .  $\therefore$  Consider  $p \geq 3$ .

Assume  $p$  prime  $\geq 3$ , and

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

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

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

$$\text{and } (n-1)(n^2+n+1) = n^3 - 1.$$

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

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  $n^2 = k^2 p^2$ .  $\therefore n^2 + n = k^2 p^2 + kp = (k^2 + k)p$   
 $\therefore p \mid (n^2 + n)$ . 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  $(2p_1 p_2 \cdots p_r)^2 + 1$ .

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  $p_1, \dots, p_r$ .

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

$$\therefore q \mid 1, \text{ a contradiction.}$$

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

(b)  $6k+1$

Assume finitely many primes of form  $6k+1$ ,  $p_1, p_2, \dots, p_r$ . Note that all  $p_i$  are thus odd.

Consider the integer  $(3p_1 p_2 \cdots p_r)^2 + (3p_1 p_2 \cdots p_r) + 1$

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  $3 \nmid 1$ , 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  $a \pmod{q}$ .

$\therefore$  By Th. 8.1,  $r \mid p$ . Since  $p$  is prime,  
 $r = 1$  or  $p$ .

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

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  $k$ .

$\therefore p(2k) = q-1$ ,  $q = \underline{\underline{2pk+1}}$ , 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 (6), 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 (6), prime divisors are of form

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

$\therefore$  Primes of form  $58K+1$  are:

59, 233, ...

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

$$2^6 = 64 \equiv 5 \pmod{59}$$

$$2^{24} \equiv 5^4 = 625 \equiv 35 \pmod{59}$$

$$2^5 \equiv 32 \pmod{59}$$

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

$$2^{29} \stackrel{?}{=} 1 \pmod{233}$$

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

$$2^8 \equiv 256 \equiv 23$$

$$2^{12} \equiv 23^2 = 529 \equiv 63 \pmod{233}$$

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

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

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

$\therefore 233$  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  $q_1, q_2, \dots, q_r$

Let  $a = 2^{q_1 q_2 \dots q_r}$ , and consider the

$$\text{integer } (2^{q_1 q_2 \dots q_r})^p - 1 = a^p - 1$$

Plan: Use  $\varphi(a)$  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.

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

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

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

If  $a$  is even,  $a^{p-1} + a^{p-2} + \dots + 1$  is odd

If  $a$  is odd, since  $p$  is odd,

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

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

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

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

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

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

Suppose  $q \mid (a-1)$ .  $\therefore a \equiv 1 \pmod{q}$   
 $\therefore a^2 \equiv 1, a^3 \equiv 1, \text{ etc.}$

$\therefore a^{p-1} + a^{p-2} + \dots + 1 \equiv p \pmod{q}$  [2]  
since There are  $p$  terms in  
 $a^{p-1} + a^{p-2} + \dots + 1.$

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

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

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

But  $a = 2q_1 q_2 \dots q_r$

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

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.

$\therefore q | (2q_1q_2\dots q_r)$  and since

$q | a^p - 1$ , then  $q | (2q_1q_2\dots q_r)^p - 1$ ,

so  $q | 1$ , 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.

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

$$2^2 \equiv 4 \pmod{19}$$

$$2^3 \equiv 8 \pmod{19}$$

$$\therefore 2^{18} = (2^6)^3 \equiv 8^3 \equiv 1 \pmod{19}$$

$$\therefore 2^{18} \equiv 1 \pmod{19}$$

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

$2 \pmod{17}$  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

$$1: 1^1 \equiv 1 \pmod{15} \quad 1 < 8 \Rightarrow 1 \text{ not a primitive root}$$

$$2: 2^4 \equiv 16 \equiv 1 \pmod{15} \quad 4 < 8 \Rightarrow 2 \text{ not a prim. root}$$

$$4: 4^2 \equiv 16 \equiv 1 \pmod{15} \quad 2 < 8 \Rightarrow 4 \text{ not a prim. root}$$

$$7: 7^2 \equiv 49 \equiv 4$$

$$\therefore 7^4 \equiv 16 \equiv 1 \pmod{15} \quad 4 < 8 \Rightarrow 7 \text{ not a prim. root}$$

$$8: 8^2 \equiv 64 \equiv 4 \pmod{15}$$

$$8^4 \equiv 16 \equiv 1 \pmod{15} \quad 4 < 8 \Rightarrow 8 \text{ not a prim. root}$$

$$11: 11^2 \equiv 121 \equiv 1 \pmod{15} \quad 2 < 8 \Rightarrow 11 \text{ not a prim. root}$$

$$13: 13^2 \equiv 169 \equiv 4 \pmod{15}$$

$$13^4 \equiv 16 \equiv 1 \pmod{15} \quad 4 < 8 \Rightarrow 13 \text{ not a prim. root}$$

$$14: 14^2 \equiv 196 \equiv 1 \pmod{15} \quad 2 < 8 \Rightarrow 14 \text{ not a prim. root}$$

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.

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

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.

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

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

$$7: 7^2 \equiv 9 \pmod{10} \therefore 7^4 \equiv 81 \equiv 1 \pmod{10}$$

$$7^1 \equiv 7, 7^2 = 49 \equiv 9, 7^3 \equiv 63 \equiv 3 \pmod{10}$$

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

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

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

$$\text{Note } \phi(\phi(17)) = \phi(16) = 2^4 \cdot 2^3 = 8$$

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

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

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

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

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

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

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

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

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

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

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

By prob. 8a,  $q | 10-1$  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 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  $q = 2k(7) + 1$

$$\therefore q = 14k + 1$$

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

By trial, 239 |  $R_7$  is the smallest

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

Pf:  $p | R_n \Rightarrow$  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  $m \geq 1$ ,  $9 \nmid 10^m - 1$

$\therefore 9 \nmid kp$ , so  $9 \nmid k$  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  $10 \pmod{p}$  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 [13],  $n \mid \underline{p-1}$

(b) Find the smallest  $R_n$  divisible by 13.

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

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

$13 \times R_1$  since  $13 \times 1$

$13 \times R_2$  since  $13 \times 11$

$13 \times R_3$  since  $13 \times 111$

$13 \times R_4$  since  $13 \times 1111$

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

## 8.2 Primitive Roots for Primes

Note Title

2/16/2006

1. If  $p$  is an odd prime, prove:

(a) The only incongruent solutions of  $x^2 \equiv 1 \pmod{p}$  are  $1$  and  $p-1$ .

Pf: Since  $p$  is odd prime,  $2 \mid p-1$ .

$\therefore$  By Corollary to Lagrange Th. 8.5,  
The congruence  $x^2 - 1 \equiv 0 \pmod{p}$   
has exactly 2 solutions.

Clearly,  $1$  is a solution since  $1 \equiv 1 \pmod{p}$

$p-1$  is also a solution since  
 $(p-1)^2 = p^2 - 2p + 1 \equiv 1 \pmod{p}$

$\therefore 1$  and  $p-1$  are solutions and they  
are incongruent mod  $p$ .

$$(1 \equiv p-1 \pmod{p}) \Rightarrow 1 \equiv -1 \pmod{p}.$$

(b) The congruence  $x^{p-2} + \dots + x^2 + x + 1 \equiv 1 \pmod{p}$   
has exactly  $p-2$  incongruent solutions,  
and they are  $2, 3, \dots, p-1$ .

Pf: By Fermat's Th., when  $\gcd(x, p) = 1$ ,

Then  $x^{p-1} \equiv 1 \pmod{p}$ .

$\gcd(x, p) = 1$  for  $x = 1, 2, 3, \dots, p-1$ ,  
and these are all incongruent mod  $p$ .

$\therefore x^{p-1} - 1 \equiv 0$  has exactly  $p-1$  solutions  
and they are  $1, 2, 3, \dots, p-1$ .

$$x^{p-1} - 1 = (x-1)(x^{p-2} + x^{p-3} + \dots + x^2 + x + 1)$$

Since  $p$  is odd,  $p \geq 3$ , so  $p-2$  is a  
valid exponent.

Since  $x-1 \equiv 0 \pmod{p}$  has exactly  
one solution ( $x \equiv 1$ ), then  
 $x^{p-2} + \dots + x + 1$  has exactly  $(p-1)-1 = p-2$   
solutions. Since  $x \not\equiv 1 \pmod{p}$  for  
 $x = 2, \dots, p-1$ , and  $x^{p-1} - 1 \equiv 0$  for  
 $x = 2, \dots, p-1$ , then  $x^{p-2} + \dots + x + 1 \equiv 0$   
for  $x = 2, \dots, p-1$ .

Thus, the  $p-2$  solutions for  
 $x^{p-2} + \dots + x + 1 \equiv 0 \pmod{p}$   
are  $x = 2, 3, \dots, p-1$ .

2. Verify that each of the congruences:

$$x^2 \equiv 1 \pmod{15}$$

$$x^2 \equiv -1 \pmod{65}$$

$$x^2 \equiv -2 \pmod{33}$$

has four incongruent solutions; hence Lagrange's Theorem need not hold if the modulus is a composite number.

Pf: By Corollary 2 to Th. 2.4 (p. 24), if  $p$  and  $q$  are primes,  $p \neq q$ , and  $p \mid c$  and  $q \mid c$ , Then  $pq \mid c$ .

In problems above, if  $p, q$  are prime,  $p \neq q$ , Then if  $x_1^2 \equiv a \pmod{p}$ , and  $x_1^2 \equiv a \pmod{q}$

$$\text{Then } x_1^2 \equiv a \pmod{pq}$$

Pf:  $p \mid x_1^2 - a$ ,  $q \mid x_1^2 - a$ , and so  $pq \mid x_1^2 - a$  by above statement.

$\therefore$  Strategy is to break up the congruence into two parts, solve each part, find common congruent solutions

$$x^2 \equiv 1 \pmod{15} \Leftrightarrow x^2 \equiv 1 \pmod{3}, x^2 \equiv 1 \pmod{5}$$

$$(x+1)(x-1) \equiv 0 \quad (x+1)(x-1) \equiv 0$$

$$x \equiv 1, 4, 7, 10, 13 \quad x \equiv 1, 6, 11, 14$$

$$x \equiv -1, 2, 5, 8, 11, 14 \quad x \equiv -1, 4, 9, 14$$

$$\therefore x \equiv \underline{1, 4, 11, 14} \pmod{15}$$

$$x^2 \equiv -1 \pmod{65} \Leftrightarrow$$

$$x^2 \equiv -1 \pmod{5}$$

$$x^2 \equiv 4$$

$$(x+2)(x-2) \equiv 0$$

$$x \equiv -2, 3, 8, 13, 18, 23, 28, 33, 38, 43 \quad x \equiv -5, 8, 21, 34, 47, 60$$

$$x \equiv 2, 7, 12, 17, 22, 27, 32, 37, 42, 47, 52, 57 \quad x \equiv 5, 18, 31, 44, 57$$

$$x^2 \equiv -1 \pmod{13}$$

$$x^2 \equiv 12, x^2 \equiv 25$$

$$(x+5)(x-5) \equiv 0$$

$$\therefore x \equiv \underline{8, 18, 47, 57} \pmod{65}$$

$$x^2 \equiv -2 \pmod{33} \Leftrightarrow$$

$$x^2 \equiv -2 \pmod{3}$$

$$x^2 \equiv 1$$

$$(x+1)(x-1) \equiv 0$$

$$x \equiv -1, 2, 5, 8, 11, 14, 17, 20, 23, 26, 29 \quad x \equiv -3, 8, 19, 30$$

$$x \equiv 1, 4, 7, 10, 13, 16, 19, 22, 25, 28, 31 \quad x \equiv 3, 14, 25$$

$$x^2 \equiv -2 \pmod{11}$$

$$x^2 \equiv 9$$

$$(x+3)(x-3) \equiv 0$$

$$\therefore x \equiv \underline{8, 14, 19, 25} \pmod{33}$$

3. Determine all the primitive roots of the primes  $p = 11, 19$ , and  $23$ , expressing each as a power of some one of the roots.

$\text{II: There are } \phi(10) = (5-1)(2-1) = 4 \text{ primitive roots}$

$$\text{Try 2: } 2^5 \equiv 10, \therefore 2^{10} \equiv 100 \equiv 1 \pmod{11}$$

$$\text{Divisors of } 10: 1, 2, 5. \quad 2^1=2, 2^2=4, 2^5=10$$

$\therefore 2$  is a primitive root of  $11$ .

Any integer relatively prime to  $11$  is congruent mod  $11$  to  $2^k$ ,  $1 \leq k \leq 10$ , since there are  $\phi(11) = 10$  such numbers, and  $2^k$ ,  $1 \leq k \leq 10$ , are incongruent by Th. 8.4.  
 $\therefore$  Other primitive roots must be among the  $2^k$ .

By Th. 8.3, These integers,  $2^k$ , will have order  $10$  also if  $\gcd(k, 10) = 1$ .  
 $\therefore k = 1, 3, 7, 9$

$\therefore$  Primitive roots of  $11$  are:  $2^1, 2^3, 2^7, 2^9$   
 or  $2, 6 (= 2^3), 7 (= 2^7), 8$

$19: \text{There are } \phi(18) = (2-1)(3^2-3^1) = 6 \text{ primitive roots}$

$$\text{Try 2: } 2^5 \equiv 13, 2^6 \equiv 26 \equiv 7, \therefore 2'' \equiv 81 \equiv -4$$

$$\therefore 2^{17} \equiv (7)(-4) = -28 \equiv 10, 2^{18} \equiv 20 \equiv 1 \pmod{19}$$

Divisors of 18: 1, 2, 3, 6, 9, 18  
 $2^1, 2^2, 2^3 \not\equiv 1, 2^6 \equiv 7 \not\equiv 1, 2^9 \equiv 2^6 \cdot 2^3 \equiv 7 \cdot 8 = 56 \equiv 18$

$\therefore 2$  is a primitive root of 19

Other primitive roots are congruent to  $2^k, 1 \leq k \leq 18$   
 By Th. 8.3, need to select  $k$  s.t.  $\gcd(k, 18) = 1$ .  
 $\therefore k = 1, 5, 7, 11, 13, 17$

$\therefore$  Primitive roots are  $\underline{\underline{2^1, 2^5, 2^7, 2^{11}, 2^{13}, 2^{17}}}$

or  $2, 13 (= 2^5), 14 (= 2^7), 15 (= 2^{11}), 3 (= 2^{13}), 10 (= 2^{17})$

Q3: There are  $\phi(22) = (2-1)(11-1) = 10$  primitive roots.

From table on p. 166, 5 is the smallest primitive root.

All primitive roots are congruent to  $5^k, 1 \leq k \leq 22$   
 By Th. 8.3, need to select  $k$  s.t.  $\gcd(22, k) = 1$ .  
 $\therefore k = 1, 3, 5, 7, 9, 13, 15, 17, 19, 21$

$\therefore$  Primitive roots are  $5^1, 5^3, \underline{5^5, 5^7, 5^9, 5^{13}, 5^{15}, 5^{17}, 5^{19}, 5^{21}}$

Note  $5^2 = 25 \equiv 2$

$$\begin{array}{ll} \therefore 5 (\equiv 5^1) & 21 (\equiv -2 \equiv 5^{13}) \\ 10 (\equiv 5^3) & 19 (\equiv -4 \equiv 5^{15}) \\ 20 (\equiv 5^5) & 15 (\equiv -8 \equiv 5^{17}) \\ 17 (\equiv 5^7) & 7 (\equiv 5^{19}) \\ 11 (\equiv 5^9) & 14 (\equiv 5^{21}) \end{array}$$

4. Given that 3 is a primitive root of 43, find the following:

(a) All positive integers less than 43 having order 6 mod 43.

$3^k$ ,  $1 \leq k \leq 42$  are incongruent by Th. 8.2

$\therefore$  All integers  $< 43$  are congruent to  $3^k$ .

$3^k$  has order  $42/\gcd(k, 42)$  mod 43  
by Th. 8.3

$$\frac{42}{\gcd(k, 42)} = 6 \Rightarrow \gcd(k, 42) = 7$$

$$\therefore k = 7, 35$$

$\therefore 3^7, 3^{35}$  have order 6 mod 43.

$$3^3 \equiv 27, 3^4 \equiv 81 \equiv -5, \therefore 3^7 \equiv -135 \equiv -(35 + 3 \cdot 43) \equiv -6 \equiv 37$$

$$3^7 \cdot 3^7 \equiv (-6)(-6) \equiv 36 \equiv (-7), 3^{18} \equiv (-7)(-5) \equiv 35 \equiv -8$$

$$3^{32} = 3^{14} \cdot 3^{18} \equiv (-7)(-8) = 56 \equiv 13$$

$$3^{33} \equiv 39 \equiv -4, \therefore 3^{35} \equiv 9(-4) = -36 \equiv 7$$

$\therefore$  Only 7 ( $\equiv 3^{35}$ ) and 37 ( $\equiv 3^7$ ) have order 6 mod 43.

(6). All positive integers less than 43 having order 21 mod 43.

As in (5), all such integers are congruent to  $3^k$ ,  $1 \leq k \leq 42$

$$\therefore \frac{42}{\gcd(42, k)} = 21 \Rightarrow \gcd(42, k) = 2$$

$$42 = 2 \cdot 3 \cdot 7$$

$$\therefore 2, 2^2, 2^3, 2^4, 2^5 \quad (= 2, 4, 8, 16, 32)$$

$$2 \cdot 5, 2 \cdot 11, 2 \cdot 13, 2 \cdot 17, 2 \cdot 19 \quad \left\{ \begin{array}{l} = 10, 22, 26, 34, 38 \\ = 20 \end{array} \right.$$

$$2^2 \cdot 5 \quad (= 40)$$

$$\therefore 3^2, 3^4, 3^8, 3^{10}, 3^{16}, 3^{20}, 3^{22}, 3^{26}, 3^{32}, 3^{34}, 3^{38}, 3^{40}$$

$$3^2 \equiv 9$$

$$3^{16} \equiv 25^2 \equiv 23$$

$$3^{82} \equiv 400 \equiv 13$$

$$3^4 \equiv 81 \equiv -5 \equiv 38$$

$$3^{20} \equiv 23 \cdot 38 \equiv 14$$

$$3^{34} \equiv 31$$

$$3^8 \equiv 25$$

$$3^{22} \equiv 40$$

$$3^{38} \equiv 31 \cdot 38 \equiv 17$$

$$3^{10} \equiv 225 \equiv 10$$

$$3^{26} \equiv 3^{10} \cdot 3^{16} \equiv 250 \equiv 15$$

$$3^{40} \equiv 9 \cdot 17 \equiv 24$$

$$\therefore \underline{\underline{9, 10, 13, 14, 15, 17, 23, 24, 25, 31, 38, 40}}$$

all have order 21 mod 43.

5. Find all positive integers less than 61 having order 4 mod 61.

Table p. 166 indicates 2 is a primitive root of 61.

$\therefore 2^k, 1 \leq k \leq 60$  are incongruent

$$\therefore \frac{60}{\gcd(60, k)} = 4 \Rightarrow \gcd(60, k) = 15 \text{ by Th. 8.3}$$

$$60 = 2^2 \cdot 3 \cdot 5. \quad \therefore 3 \cdot 5, 3^2 \cdot 5 \Rightarrow 15, 45$$

$\therefore 2^{15}, 2^{45}$  have order 4 mod 61.

$$2^6 = 64 \equiv -3, \quad 2^{12} \equiv 9, \quad 2^{15} \equiv 9 \cdot 8 = 72 \equiv 11$$

$$2^{30} \equiv 121 \equiv -1, \quad 2^{45} \equiv (-1)(11) = -11 \equiv 50$$

$\therefore$  Only 11, 50 have order 4 mod 61.

C. Assuming that  $r$  is a primitive root of the odd prime  $p$ , establish the following facts:

(a) The congruence  $r^{\frac{(p-1)}{2}} \equiv -1 \pmod{p}$  holds.

Pf: We know  $r^{p-1} \equiv 1 \pmod{p}$  by Fermat's Th.

As  $\frac{p-1}{2}$  is an integer,  $r^{\frac{p-1}{2}}$  exists,

$$\therefore r^{\frac{p-1}{2}} - 1 \equiv 0 \Rightarrow (r^{\frac{p-1}{2}} - 1)(r^{\frac{p-1}{2}} + 1) \equiv 0$$

If  $r^{\frac{p-1}{2}} - 1 \equiv 0 \pmod{p}$  Then since  $\frac{p-1}{2} < p-1$ ,  
 $r$  wouldn't have order  $p-1$ .

$$\therefore r^{\frac{p-1}{2}} + 1 \equiv 0 \Rightarrow r^{\frac{p-1}{2}} \equiv -1 \pmod{p}$$

(b) If  $r'$  is any other primitive root of  $p$ , Then  $rr'$  is not a primitive root of  $p$ .

If  $rr'$  were a primitive root, its order would be  $p-1$ .

But by (a),  $r^{\frac{p-1}{2}} \equiv -1$  and  $(r')^{\frac{p-1}{2}} \equiv -1$ ,

so  $(r^{\frac{p-1}{2}})((r')^{\frac{p-1}{2}}) \equiv (-1)(-1) \pmod{p}$ , or

$(rr')^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ . Since  $\frac{p-1}{2} < p-1$ , this contradicts assumption of order of  $rr'$ .

$\therefore rr'$  not a primitive root of  $p$ .

(c) If the integer  $r'$  is such that  $rr' \equiv 1 \pmod{p}$ ,  
Then  $r'$  is a primitive root of  $p$ .

Pf: We can assume  $1 \leq r' \leq p-1$ .

For, if  $r' = p$ , Then  $r' \equiv 0$ , so  $rr' \not\equiv 1$ .

If  $r' > p$ , Then by Div. Alg.,  
 $r' = qp + s$ ,  $0 \leq s < p-1$ , so  $r' \equiv s \pmod{p}$   
and  $\therefore r'$  and  $s$  have same order.

$\therefore \gcd(r', p) = 1$ .

Consider  $(r')^k$ ,  $1 \leq k \leq p-1$ .

If  $k < p-1$  and  $(r')^k \equiv 1 \pmod{p}$ , then

$$1 \equiv 1^k \equiv (rr')^k = r^k(r')^k \equiv r^k \pmod{p}$$

contradicting order of  $r = p-1$ .

$$\therefore 1 = 1^{p-1} \equiv (rr')^{p-1} = r^{p-1}(r')^{p-1} \equiv (r')^{p-1} \pmod{p}$$

$$\therefore (r')^{p-1} \equiv 1 \pmod{p},$$

$(r')^k \not\equiv 1 \pmod{p}$  for  $1 \leq k < p-1$ , and

$$\gcd(r', p) = 1.$$

$\therefore$  By def.,  $r'$  is a primitive root of  $p$ .

7. For a prime  $p > 3$ , prove that the primitive roots of  $p$  occur in incongruent pairs  $r, r'$  where  $rr' \equiv 1 \pmod{p}$ !

Pf: By Th. 7.4, for  $n \geq 2$ ,  $\phi(n)$  is an even integer, so that  $\phi(n) \geq 2$ .

Let  $r$  be one primitive root of  $p$ .

By Th. 8.4,  $r, r^2, \dots, r^{p-1}$  are

congruent to  $1, 2, \dots, p-1$  in some order,

and so  $r, r^2, \dots, r^{p-1}$  are incongruent.

Since  $p > 3$ , there are at least 3 members in this list.

Let  $r' = r^{p-2}$ .  $\therefore r$  and  $r'$  are incongruent,

and  $rr' = r \cdot r^{p-2} = r^{p-1} \equiv 1 \pmod{p}$ .

By 6(c) above,  $r'$  is a primitive root.

$\therefore$  If  $r$  is a primitive root of  $p$ ,  $p > 3$ , we can always find an  $r'$  incongruent to  $r$  s.t.  $rr' \equiv 1 \pmod{p}$ .

8. Let  $r$  be a primitive root of the odd prime  $p$ .  
Prove the following:

(a) If  $p \equiv 1 \pmod{4}$ , then  $-r$  is also a primitive root of  $p$ .

Pf: Let  $k$  b.c s.t.  $p-1 = 4k$   
 $r$  a primitive root of  $p \Rightarrow r^{p-1} \equiv 1 \pmod{p}$   
 $\therefore r^{4k} \equiv 1 \pmod{p}$

$$\therefore (-r)^{p-1} = (-r)^{4k} = r^{4k} \equiv 1 \pmod{p}$$

Let  $1 \leq s < p-1$ , and consider  $(-r)^s$

s even:  $(-r)^s = r^s \not\equiv 1 \pmod{p}$  as  
 $r$  is a primitive root, and by def.,  
 $r^s \not\equiv 1$  if for  $1 \leq s < p-1$ .

$$s \text{ odd: } (-r)^s = -r^s$$

For  $s$  to be odd,  $s = 4k-3$  or  $4k-1$   
for some  $k$ .

$$4k-1: \text{ Assume } -r^{4k-1} \equiv 1 \pmod{p}$$

$$\therefore (-r)(-r^{4k-1}) = r^{4k} \equiv -r$$

$$\text{But } r^{4k} = r^{p-1} \equiv 1, \text{ so}$$

$$-r \equiv 1 \Rightarrow r^2 \equiv 1 \text{ contradicting}$$

$r$  having order  $p-1$ .

$$4k-3: \text{ Assume } -r^{4k-3} \equiv 1 \pmod{p}$$

$$\therefore (-r^3)(-r^{4k-3}) = r^{4k} \equiv -r^3$$

$$\text{But } r^{4k} = r^{p-1} \equiv 1, \text{ so}$$

$$-r^3 \equiv 1, \text{ or } r^3 + 1 \equiv 0 \pmod{p}$$

$$\therefore (r+1)(r^2+r+1) \equiv 0$$

$$\therefore r+1 \equiv 0 \text{ or } r^2+r+1 \equiv 0$$

If  $r+1 \equiv 0$ , Then  $r \equiv -1 \Rightarrow r^2 \equiv 1$ ,

contradicting order of  $r$  as  $p-1$ .

If  $r^2+r+1 \equiv 0$ , Then

$$(r^{p-1})(r^2+r+1) \equiv 0$$

$$r^{p+1} + r^p + r^{p-1} \equiv r^{p+1} + r^p \equiv 0$$

$\therefore$  Since  $\gcd(r, p) = 1$ ,  $\gcd(r^p, p) = 1$ ,

dividing by  $r^p$ ,

$$r+1 \equiv 0 \Rightarrow r \equiv -1, r^2 \equiv 1,$$

contradicting  $p-1$  as order of  $r$ .

$\therefore$  for  $1 \leq s < p-1$ ,  $(-r)^s \not\equiv 1 \pmod{p}$

but  $(-r)^{p-1} \equiv 1 \pmod{p}$

$\therefore -r$  is a primitive root of  $p$ .

(b). If  $p \equiv 3 \pmod{4}$ , Then  $-r$  has order  $(p-1)/2 \pmod{p}$

Pf:  $p = 3 + 4k$ , some  $k \geq 0$ .  $\therefore p-1 = 2+4k$ ,

$\therefore \frac{p-1}{2} = 1+2k$ , some  $k \geq 0$ .

$\therefore \frac{p-1}{2}$  is odd.  $\therefore (-r)^{\frac{p-1}{2}} = -r^{\frac{p-1}{2}}$

(a) Since  $r^{p-1} \equiv 1 \pmod{p}$  [ $r$  a prim. root],

Then  $r^{p-1} - 1 \equiv 0 \Rightarrow (r^{\frac{p-1}{2}} + 1)(r^{\frac{p-1}{2}} - 1) \equiv 0$

But  $r^{\frac{p-1}{2}} - 1 \neq 0$ . If so,  $r^{\frac{p-1}{2}} \equiv 1$ , contradicting order of  $r$  as  $p-1$ .

$\therefore r^{\frac{p-1}{2}} + 1 \equiv 0 \Rightarrow r^{\frac{p-1}{2}} \equiv -1 \Rightarrow$

$(-r)^{\frac{p-1}{2}} = -r^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ .

(6) Now suppose  $-r$  has order  $s$ ,  $1 \leq s < \frac{p-1}{2}$

$s$  can't be even. If so, then  $(-r)^s = r^s \equiv 1$ , so order of  $r$  would be less than  $p-1$ , a contradiction.

$\therefore s$  is odd,  $2s < p-1$

$$\therefore (-r)^s \equiv 1 \Rightarrow (-r)^{2s} = r^{2s} \equiv 1$$

This contradicts order of  $r$  as  $p-1$ .

$\therefore$  order of  $-r$  can't be  $< \frac{p-1}{2}$ .

(a) + (6)  $\Rightarrow$  order of  $-r$  is  $\frac{p-1}{2}$ .

9. Give a different proof of Th. 5.5 by showing that if  $r$  is a primitive root of the prime  $p \equiv 1 \pmod{4}$ , then  $r^{\frac{(p-1)}{4}}$  satisfies the quadratic congruence  $x^2 + 1 \equiv 0 \pmod{p}$

Pf:  $r$  a primitive root  $\Rightarrow r^{p-1} \equiv 1 \pmod{p}$

Since  $p-1 = 4k$ , some  $k$ , Then

$(p-1)/4 = K$ , some integer.

Consider  $x^4 \equiv 1 \pmod{p}$ .

$r^{\frac{p-1}{4}}$  is a solution.

$$\therefore x^4 - 1 = (x^2 + 1)(x^2 - 1) \equiv 0 \pmod{p}$$

If  $r^{\frac{p-1}{4}}$  is a solution to  $x^2 - 1 \equiv 0$ ,  
Then  $r^{\frac{p-1}{2}} \equiv 1$ , contradicting order  
of  $r$  as  $p-1$ .

$\therefore r^{\frac{p-1}{4}}$  is a solution to  $x^2 + 1 \equiv 0 \pmod{p}$ .

Th. 5.5 says  $x^2 + 1 \equiv 0 \pmod{p}$ ,  $p$  odd, has a  
solution  $\iff p \equiv 1 \pmod{4}$ .

(a) if  $p \equiv 1 \pmod{4}$ ,  $p$  has a primitive  
root, since  $p$  is prime. Call it  $r$ .  
Above shows  $r^{\frac{(p-1)}{4}}$  is a solution.

(b) Suppose  $x^2 + 1 \equiv 0 \pmod{p}$  has a solution  
Proof is same as given in text  
on p. 99.

10. Use the fact that each prime  $p$  has a primitive  
root to give a different proof of Wilson's  
Theorem.

PF: Let  $r$  be a primitive root of  $p$ .

$1, 2, 3, \dots, p-1$  are the positive integers less than  $p$  that are relatively prime to  $p$ . Also,  $\phi(p) = p-1$ .

$\therefore$  By Th. 8.4,  $r, r^2, \dots, r^{p-1}$  are congruent mod  $p$  to  $1, 2, \dots, p-1$ , in some order.

$$\therefore 1 \cdot 2 \cdot 3 \cdots (p-1) \equiv r \cdot r^2 \cdot r^3 \cdots r^{p-1} \pmod{p}, \text{ or}$$

$$(p-1)! \equiv r^{1+2+\cdots+(p-1)} \pmod{p}$$

$$\text{But } 1+2+\cdots+(p-1) = \frac{(p-1)p}{2}$$

$$\therefore (p-1)! \equiv r^{\frac{(p-1)p}{2}} \pmod{p}$$

$$\therefore [(p-1)!]^2 \equiv (r^{p-1})^p \pmod{p}$$

But, since  $r$  is a primitive root of  $p$ ,

$$\therefore r^{p-1} \equiv 1 \pmod{p}, \text{ so } (r^{p-1})^p \equiv 1 \pmod{p}$$

$$\therefore [(p-1)!]^2 \equiv 1 \pmod{p}$$

$$\therefore [(p-1)!]^2 - 1 \equiv 0 \pmod{p}, \text{ so}$$

$$[(p-1)! + 1][(p-1)! - 1] \equiv 0 \pmod{p}$$

$$\text{If } (p-1)! - 1 = 0, \text{ Then } r^{\frac{(p-1)p}{2}} \equiv (p-1)! \equiv 1$$

$$\text{But } r^{p-1} \equiv 1, \text{ so } r^p \equiv r$$

$$\therefore r^{\frac{(p-1)p}{2}} = (r^p)^{\frac{p-1}{2}} \equiv r^{\frac{p-1}{2}} \equiv 1 \pmod{p},$$

which contradicts order of  $r = p-1$ ,  
since  $\frac{p-1}{2} < p-1$ .

$$\therefore (p-1)! + 1 \equiv 0 \pmod{p}, \text{ so } \underline{\underline{(p-1)! \equiv -1 \pmod{p}}}$$

11. If  $p$  is a prime, show that the product of the  $\phi(p-1)$  primitive roots of  $p$  is congruent mod  $p$  to  $(-1)^{\phi(p-1)}$

Pf: By Th. 8.4, since  $r$  is a primitive root,  
Then  $r^1, r^2, \dots, r^{p-1}$  are congruent to  
 $1, 2, \dots, p-1$  in some order.

If  $s$  is any other primitive root, it must be congruent to one of  $1, 2, \dots, p-1$ , and  $\therefore s$  is congruent to one of  $r^1, r^2, \dots, r^{p-1}$ .

$\therefore$  All primitive roots of  $p$  are of the form  $r^k$ , where  $1 \leq k \leq p-1$ .

By Th. 8.3,  $r^k$  will have order  $p-1$  if  $\gcd(k, p-1) = 1$ . Clearly,  $k \neq p-1$  for this to be true, so  $k$  must be of the form  $1 \leq k < p-1$ .

Call these  $\phi(p-1)$  integers  $k_1, k_2, \dots, k_{\phi(p-1)}$ , where  $1 \leq k_i < p-1$ .

$\therefore$  The product of these primitive roots

$$\text{is } r^{k_1} \cdot r^{k_2} \cdots r^{k_{\phi(p-1)}} = r^{k_1 + k_2 + \cdots + k_{\phi(p-1)}}$$

By Th. 7.?,  $k_1 + k_2 + \cdots + k_{\phi(p-1)} = \frac{1}{2}(p-1)\phi(p-1)$

$$\therefore r^{k_1 + k_2 + \cdots + k_{\phi(p-1)}} = r^{\frac{1}{2}(p-1)\phi(p-1)}$$

For  $p > 2$ ,  $\phi(p-1)$  is even by Th. 7.4, so  $2 \mid \phi(p-1)$

$$\therefore r^{\frac{1}{2}(p-1)\phi(p-1)} = (r^{p-1})^{\frac{1}{2}\phi(p-1)}$$

$$\equiv (1)^{\frac{1}{2}\phi(p-1)} \equiv 1 \pmod{p}$$

since  $\frac{1}{2}\phi(p-1) \geq 1$  for  $p > 2$ .

Since  $\phi(p-1)$  is even,  $(-1)^{\phi(p-1)} = 1$ ,

so

$$r^{k_1 + k_2 + \dots + k_{\phi(p-1)}} \equiv (-1)^{\phi(p-1)} \pmod{p}$$

For  $p=2$ , the only primitive root is 1,  
 $\phi(2)=1$ , and so,

$$r^{k_1 + \dots + k_{\phi(p-1)}} = 1 \equiv (-1)^{\phi(2-1)} = -1 \pmod{2}$$

since  $1 \equiv -1 \pmod{2}$ .

$\therefore$  the formula holds for  $p=2$ .

12. For an odd prime  $p$ , verify that the sum

$$1^n + 2^n + 3^n + \dots + (p-1)^n \equiv \begin{cases} 0 \pmod{p} & \text{if } (p-1) \nmid n \\ -1 \pmod{p} & \text{if } (p-1) \mid n \end{cases}$$

Pf:  $p$  odd means  $p \neq 2$ , so sum doesn't reduce to  $1^n = 1$ . But for  $p=2$ ,  $p-1 \mid n$  for all  $n$ , and since  $1^n = 1 \equiv -1 \pmod{2}$ , so formula works even for  $p=2$ .

$\therefore$  Let  $p$  be an odd prime, let  $r$  be a primitive root.

$\therefore r, r^2, \dots, r^{p-1}$  are congruent mod  $p$  to  $1, 2, \dots, p-1$  in some order by Th. 8.4

Since  $r^k \equiv j \pmod{p}$ ,  $1 \leq k \leq p-1$ ,  $1 \leq j \leq p-1$ ,

Then  $r^{kn} \equiv j^n \pmod{p}$

Thus,  $r^n, r^{2n}, \dots, r^{(p-1)n}$  are congruent mod  $p$  to

$1^n, 2^n, \dots, (p-1)^n$  in some order.

$$\therefore 1^n + 2^n + \dots + (p-1)^n \equiv r^n + r^{2n} + \dots + r^{(p-1)n} \pmod{p}$$

Since  $r$  is a primitive root of  $p$ ,

$$r^{p-1} \equiv 1 \pmod{p}, \text{ so } r^{(p-1)n} \equiv 1 \pmod{p}.$$

$$\therefore 1^n + 2^n + \dots + (p-1)^n \equiv 1 + r^n + r^{2n} + \dots + r^{(p-2)n} \pmod{p}$$

But since  $p \geq 3$ ,  $r^{(p-2)n}$  makes sense.

Suppose  $(p-1) \mid n$ . Then  $n = (p-1)k$ , some  $k$ .

$$\therefore \text{For } 1 \leq s \leq p-2, r^{sn} = r^{(p-1)ks}$$

$\therefore$  Since  $r^{(p-1)ks} \equiv 1^{ks} \equiv 1 \pmod{p}$ , Then  $r^{sn} \equiv 1$ .

There are  $(p-2)$  terms in  $r^n + r^{2n} + \dots + r^{(p-2)n}$

$$\begin{aligned}\therefore 1 + r^n + r^{2n} + \dots + r^{(p-2)n} &\equiv 1 + [1 + 1 + \dots + 1] \\ &\equiv 1 + (p-2) \\ &\equiv p-1 \\ &\equiv -1 \pmod{p}\end{aligned}$$

$\therefore$  For  $(p-1) \mid n$ ,

$$1^n + 2^n + \dots + (p-1)^n \equiv -1 \pmod{p} \quad [1]$$

Suppose  $(p-1) \nmid n \therefore n = a(p-1) + b$ ,  $0 < b < (p-1)$   
by Div. Alg.

$$\begin{aligned}\therefore r^n &= r^{a(p-1)+b} = [r^{(p-1)}]^a \cdot r^b \\ &\equiv 1^a \cdot r^b \equiv r^b \pmod{p}\end{aligned}$$

since  $r$  a prim. root of  $p \Rightarrow r^{p-1} \equiv 1 \pmod{p}$ .

$\therefore r^b \not\equiv 1 \pmod{p}$  since  $b < p-1$  and prim. root means  $p-1$  is the smallest order for  $r$ .

$$\therefore r^n - 1 \equiv r^b - 1 \not\equiv 0 \pmod{p} \quad [2]$$

$$\text{Let } S = 1 + r^n + r^{2n} + \dots + r^{(p-2)n} \quad [3]$$

$$\therefore r^n S = r^n + r^{2n} + r^{3n} + \dots + r^{(p-2)n} + r^{(p-1)n} \quad [4]$$

Subtracting [3] from [4],

$$r^n S - S = (r^n - 1)S = r^{(p-1)n} - 1, \text{ or}$$

$$(r^n - 1)(1 + r^n + r^{2n} + \dots + r^{(p-2)n}) = r^{(p-1)n} - 1$$

But  $r^{(p-1)} \equiv 1 \pmod{p}$ , so  $r^{(p-1)n} - 1 \equiv 0 \pmod{p}$

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

From [2],  $r^n - 1 \not\equiv 0 \pmod{p}$ .

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

$\therefore$  when  $(p-1) \nmid n$ ,

$$1^n + 2^n + \dots + (p-1)^n \equiv 1 + r^n + \dots + r^{(p-2)n} \equiv 0 \pmod{p} \quad [5]$$

$\therefore$  [1] and [5] give

$$1^n + 2^n + \dots + (p-1)^n \equiv \begin{cases} 0 \pmod{p} & \text{if } (p-1) \nmid n \\ -1 \pmod{p} & \text{if } (p-1) \mid n \end{cases}$$

## 8.3 Composite Numbers Having Primitive Roots

Note Title

3/10/2006

1. (a) Find the four primitive roots of 26 and the eight primitive roots of 25

Proof of Corollary to Th. 8.9 shows that if  $r$  is an odd primitive root of  $p^k$ , then it is a primitive root of  $2p^k$ .

$\therefore$  Since  $26 = 2 \cdot 13$ , find odd primitive roots of 13. There are  $\phi(13-1) = \phi(12)$  incongruent primitive roots of 13.  
 $\phi(12) = (2^{2-2})(3-1) = 4$

Check  $2^{12}$ : By Euler's Th.,  $2^{\phi(13)} = 2^{12} \equiv 1 \pmod{13}$   
Order of 2 mod 13 must divide 12 (Th. 8.1),  
and  $2^1, 2^2, 2^3, 2^4, 2^5, 2^6 \not\equiv 1 \pmod{13}$ .  
 $\therefore 2$  is a primitive root of 13.

By Th. 8.3, other integers having order 12 mod 13 are powers of 2<sup>k</sup> s.t.  $\gcd(k, 12) = 1$   
 $\therefore k = 1, 5, 7, 11$ .

$\therefore 2^1 \equiv 2, 2^5 \equiv 6, 2^7 \equiv 11, 2^{11} \equiv 7 \pmod{13}$ .  
So, four incongruent prim. roots of 13  
are 2, 6, 7, 14.

$\therefore$  Four odd primitive roots of 13 are  
 $(2+13), (6+13), 7, 11$ , or  $7, 11, 15, 19$

$\therefore \underline{7, 11, 15, 19}$  will be prim. roots for  $2 \cdot 13 = 26$

For  $25$ ,  $25 = 5^2$ . Proof of Lemma 2 and Th. 8.9  
Show if  $r$  is a primitive root of  $p$  s.t.  
 $r^{p-1} \not\equiv 1 \pmod{p^2}$ , Then  $r$  is a prim. root of  $p^k$ .

$2^{5-1} = 16 \not\equiv 1 \pmod{5^2} \Rightarrow 2$  a prim. root of  $25$   
since 2 is a prim. root of 5.

$$\phi(25) = 5^2 - 5 = 20$$

$\therefore$  Look at  $2^k$  s.t.  $\gcd(k, 20) = 1$ .

$\therefore k = 1, 3, 7, 9, 11, 13, 17, 19$  and  $2^k \equiv 1 \pmod{25}$

$$2^3 \equiv 8, 2^7 \equiv 128 \equiv 3, 2^9 \equiv 2^7 \cdot 2^2 \equiv 12,$$

$$2^{11} \equiv 2^9 \cdot 2^2 \equiv 12 \cdot 4 \equiv 48 \equiv 23$$

$$2^{13} \equiv 2^{11} \cdot 2^2 \equiv 23 \cdot 4 \equiv 92 \equiv 17$$

$$2^{17} \equiv 2^9 \cdot 2^7 \cdot 2 \equiv 12 \cdot 3 \cdot 2 \equiv 72 \equiv 22$$

$$2^{19} \equiv 2^{17} \cdot 2^2 \equiv 22 \cdot 4 \equiv 88 \equiv 13$$

$\therefore$  Primitive roots of  $25$ :  $2, 3, 8, 12, 13, 17, 22, 23$

(5). Determine all the primitive roots of  $3^2$ ,  $3^3$ , and  $3^4$ .

Note  $3^k$  has primitive roots by Th. 8.10

2 is a primitive root of 3

$\therefore$  either 2 or  $2+3$  will be primitive roots  
of  $3^k$ ,  $k \geq 2$ .

Since, if  $r$  is a prim. root of  $p$ , then order of  
 $r \pmod{p^2}$  is  $(p-1)$  or  $p(p-1)$

$\therefore$  Order of  $2 \pmod{3^2}$  is  $(3-1)$  or  $\phi(3^2)$ ,  
But  $2^2 = 4 \not\equiv 1 \pmod{3^2}$ , so  $2^{\phi(3^2)} \equiv 1 \pmod{3^2}$ ,  
so 2 is a primitive root of  $3^2$ ,  $3^3$ , and  $3^4$

$3^2$ : There are  $\phi(\phi(3^2)) = \phi(6) = 2$  prim. roots  
Since  $\phi(3^2) = 6$ , By Th. 8.3,  $2^h$  will  
have order 6  $\Leftrightarrow \gcd(h, 6) = 1$ , or  $h = 1, 5$   
 $\therefore 2^5 = 32 \equiv 5 \pmod{3^2}$   
 $\therefore$  primitive roots are 2, 5

$3^3$ :  $\phi(3^3) = 3^3 - 3^2 = 18$ ,  $\phi(18) = 6$

$\therefore 6$  prim. roots, and all are of form  
 $2^k$ , s.t.  $\gcd(K, 18) = 1$ , or  $K = 1, 5, 7, 11, 13, 17$   
 $2^5 = 32 \equiv 5 \pmod{27}$

$$2^7 \equiv 5 \cdot 2^2 = 20 \pmod{27}$$

$$2^{11} \equiv 5 \cdot 5 \cdot 2 = 50 \equiv 23 \pmod{27}$$

$$2^{13} \equiv 23 \cdot 2^2 = 92 \equiv 11 \pmod{27}$$

$$2^{17} = 2^{11} \cdot 2^5 \cdot 2 \equiv 23 \cdot 5 \cdot 2 = 230 \equiv -40 \equiv 14 \pmod{27}$$

$\therefore$  prim. roots are 2, 5, 11, 14, 20, 23

$$3^4: \phi(3^4) = 3^4 - 3^3 = 81 - 27 = 54 = 2 \cdot 3^3$$

$$\phi(5^4) = \phi(3^3) = 18$$

$\therefore$  18 primitive roots, all of form

$$2^K \text{ s.t. } \gcd(K, 54) = 1.$$

$$\therefore K = 1, 5, 5^2, 7, 7^2, 5 \cdot 7, 11, 13, 17, 19, 23, 29, 31, 37, \\ 41, 43, 47, 53$$

$$\therefore 2^1 = \underline{2}, 2^5 = \underline{32}, 2^7 = 128 \equiv \underline{47}$$

$$2^{11} \equiv 47 \cdot 2^4 \equiv \underline{23}, 2^{13} \equiv 23 \cdot 2^2 \equiv \underline{11}$$

$$2^{17} \equiv 11 \cdot 2^4 \equiv \underline{14}, 2^{19} \equiv 14 \cdot 2^2 \equiv \underline{56}$$

$$2^{23} \equiv 56 \cdot 2^4 \equiv \underline{5}, 2^{29} \equiv 5 \cdot 2^4 \cdot 2 = 320 \equiv \underline{77}$$

$$2^{31} \equiv 77 \cdot 2^2 \equiv \underline{65}, 2^{37} \equiv 65 \cdot 2^5 \cdot 2 \equiv \underline{29}$$

$$2^{41} \equiv 29 \cdot 2^4 \equiv \underline{59}, 2^{43} \equiv 59 \cdot 2^2 \equiv \underline{74}$$

$$2^{47} \equiv 74 \cdot 2^4 \equiv \underline{50}, 2^{53} \equiv 50 \cdot 2^6 \equiv \underline{41}$$

$$2^{52} = 2^{25} \equiv 5 \cdot 2^2 \equiv \underline{20}, 2^{72} = 2^{49} \equiv 50 \cdot 4 \equiv \underline{38}$$

$$2^{57} = 2^{35} \equiv 65 \cdot 2^4 \equiv \underline{68}$$

$\therefore 2, 5, 11, 14, 20, 23, 29, 32, 38, 41, 47, 50, 56, 59, \\ 65, 68, 74, 77$  are prim. roots

2. For an odd prime  $p$ , establish:

{incongruent}

(a) There are as many primitive roots of  $2p^n$  as  $p^n$

Pf: By Th. 8.7 and its corollary,  $p^n$  and  $2p^n$  have prim. roots, where  $p$  is an odd prime and  $n \geq 1$ .

By corollary to Th. 8.4 (p. 161), There are exactly  $\phi(\phi(2p^n))$  prim. roots for  $2p^n$ , and exactly  $\phi(\phi(p^n))$  prim. roots for  $p^n$ .  
(i.e., incongruent prim. roots).

For  $m, n$  s.t.  $\gcd(m, n) = 1$ ,  $\phi(mn) = \phi(m)\phi(n)$ , and  $\gcd(2, p^n) = 1$  since  $p$  is odd.

$$\therefore \phi(2p^n) = \phi(2)\phi(p^n) = \phi(p^n) \text{ as } \phi(2) = 1.$$

$$\therefore \phi(2p^n) = \phi(p^n) \Rightarrow \underline{\phi(\phi(2p^n)) = \phi(\phi(p^n))}$$

Note also that proof of corollary to Th. 8.9 shows if  $r$  is an odd prim. root of  $p^k$ , it is also a prim. root of  $2p^k$ .

Similarly, if  $r$  is a primitive root of  $2p^k$ ,

Then  $\gcd(r, 2p^k) = 1$ ,  $r$  is odd.

If  $n$  is order of  $r \pmod{p^k}$ , Then  $n \leq \phi(p^k)$

Also,  $r^n \equiv 1 \pmod{p^k} \Rightarrow r^{n-1} = xp^k$ , some  $x$ .

But  $r^{n-1}$  is even, so  $x = 2y$ , some  $y$ ,

so  $r^n \equiv 1 \pmod{2p^k}$ .

$\therefore n \geq \phi(2p^k) = \phi(p^k)$ .

$\therefore n \geq \phi(p^k)$  and  $n \leq \phi(p^k) \Rightarrow n = \phi(p^k)$

$\therefore r$  is a primitive root of  $p^k$ .

So, if  $r$  is an even prim. root of  $p^k$ , Then  
choose  $r'$  to be  $r + p^k$  so  $r'$  is odd and  
 $\therefore$  a prim. root of  $2p^k$ .

(b) Any primitive root  $r$  of  $p^n$  is a primitive root of  $p$ .

Pf:  $\gcd(r, p^n) = 1 \Rightarrow \gcd(r, p) = 1$ .

Let  $K$  be order of  $r \pmod{p}$

$\therefore r^K \equiv 1 \pmod{p}$

$\therefore K \mid \phi(p) \Rightarrow K \mid (p-1)$  [1]

Also,  $r^K = 1 + sp$ , some  $s$ .

So, for  $n > 1$ ,

$$\begin{aligned} r^{kp^{n-1}} &= (1 + sp)^{p^{n-1}} \\ &= 1 + \binom{p^{n-1}}{1}sp + \binom{p^{n-1}}{2}(sp)^2 + \dots + (sp)^{p^{n-1}} \end{aligned}$$

But  $p^{n-1} \mid \binom{p^{n-1}}{k}$ , for  $1 \leq k < p^{n-1}$ , and

$p \mid (sp)^k$ , for  $1 \leq k \leq p^{n-1}$ .

$$\therefore p^n \mid \left[ \binom{p^{n-1}}{1}sp + \binom{p^{n-1}}{2}(sp)^2 + \dots + (sp)^{p^{n-1}} \right]$$

$$\therefore r^{kp^{n-1}} \equiv 1 \pmod{p^n}$$

$\therefore$  Since  $r$  is a prim. root of  $p^n$ , Then

$$\phi(p^n) \mid kp^{n-1}, \text{ by Th. 8.1.}$$

$$\phi(p^n) = p^{n-1}(p-1).$$

$$\therefore (p-1) \mid k \quad [2]$$

[1] and [2]  $\Rightarrow k = p-1$ , so order  
of  $r \pmod{p}$  is  $p-1$ , so  
 $r$  is a prim. root of  $p$ .

(c) A primitive root of  $p^2$  is also a prim. root of  $p^n$  for  $n \geq 2$ .

Pf: Let  $r$  be a primitive root of  $p^2$ .

By (b),  $r$  is also a prim. root of  $p$ .

Note  $r^{p-1} \not\equiv 1 \pmod{p^2}$  since  $\phi(p^2) = p(p-1)$  and  $r$  is a prim. root of  $p^2$ .

$\therefore r$  is a prim. root of  $p$  s.t.  $r^{p-1} \not\equiv 1 \pmod{p^2}$ , and proof to Th. 8.9 shows this  $r$  is a prim. root of  $p^n$  for  $n \geq 1$ .

$\therefore$  This  $r$  is certainly a prim. root for  $p^n$ ,  $n \geq 2$ .

3. If  $r$  is a primitive root of  $p^2$ ,  $p$  being an odd prime, show that the solutions of the congruence  $x^{p-1} \equiv 1 \pmod{p^2}$  are precisely the integers  $r^p, r^{2p}, \dots, r^{(p-1)p}$ .

Pf: Note if  $x$  is a solution to  $x^{p-1} \equiv 1 \pmod{p^2}$ , then it is a solution to  $x^{p-1} \equiv 1 \pmod{p}$ , since  $a \equiv 6 \pmod{p^2} \Rightarrow a \equiv 6 \pmod{p}$ .

Corollary to Th. 8.5 says  $x^{p-1} \equiv 1 \pmod{p}$  has exactly  $p-1$  solutions.

$\therefore x^{p-1} \equiv 1 \pmod{p^2}$  has at most  $(p-1)$  solutions.

Note that for  $k \geq 1$ ,

$$(r^{kp})^{p-1} = (r^{p(p-1)})^k = (r^{\varphi(p^2)})^k \equiv 1^k = 1 \pmod{p^2},$$

as  $r$  is a prim. root of  $p^2$ .

$\therefore$  The  $p-1$  integers  $r^p, r^{(p-1)p}, \dots, r^{(p-1)p}$  satisfy  $x^{p-1} \equiv 1 \pmod{p^2}$

Note that  $r^p, r^{2p}, \dots, r^{(p-1)p}$  are incongruent.

For let  $r^{ap} \equiv r^{bp} \pmod{p^2}$  for  $1 \leq a, b \leq p-1$ ,

$a \neq b$ . Assume  $a > b$  (same proof for  $b > a$ ).

$\therefore r^{(a-b)p} \equiv 1 \pmod{p^2}$  contradicting order of  $r$  as  $p(p-1)$  since  $a-b < p-1$ .

$\therefore$  The  $p-1$  integers  $r^p, r^{(p-1)p}, \dots, r^{(p-1)p}$  are incongruent solutions to  $x^{p-1} \equiv 1 \pmod{p^2}$  and so are a complete set of solutions.

4. (a) Prove that 3 is a primitive root of all integers of the form  $7^k$  and  $2 \cdot 7^k$

Pf:  $3^1 \not\equiv 1 \pmod{7}$ ,  $3^2 \equiv 2$ ,  $3^3 \equiv 6$ ,  $3^4 \equiv 4$ ,  $3^5 \equiv 5$ ,  
 $3^6 \equiv 1 \pmod{7}$

$\therefore 3^{\phi(7)} = 3^6 \equiv 1 \pmod{7}$ , and so  
3 is a primitive root of 7.

$\therefore$  order of 3 mod  $7^2$  is  $(7-1)$  or  $7(7-1)$

But  $3^4 = 81 \equiv 32 \pmod{7^2}$

$\therefore 3^6 \equiv 9 \cdot 32 \equiv 43 \pmod{7^2}$

$\therefore 3^6 \not\equiv 1 \pmod{7^2}$

$\therefore$  order of  $3 \pmod{7^2}$  is  $>(7-1) = \phi(7^2)$

$\therefore$  Lemma 2 (p.170) shows that for  $k \geq 2$ ,

$3^{7^{k-2}(7-1)} \not\equiv 1 \pmod{7^k}$

And Th. 8.9 shows 3 is a prim. root  
of  $7^k$  for  $k \geq 1$ .

Since 3 is an odd prim. root for  $7^k$ ,  
Corollary (p.171) shows 3 is a  
prim. root of  $2 \cdot 7^k$

[i.e., just need to show 3 a prim. root of  $p$   
and  $3^{p-1} \not\equiv 1 \pmod{p^2}$ . Then 3 a prim. root of  $7^k$   
for  $2 \cdot 7^k$ , now just need 3 is odd.]

(6) Find a primitive root for any integer of the form  $17^k$ .

Just need to find a prim. root  $r$  of  $17$  s.t.  
 $r^{16} \not\equiv 1 \pmod{17^2}$ .

Try 2:  $2^4 \equiv 16 \equiv -1 \pmod{17}$   
 $\therefore 2^8 \equiv 1 \pmod{17}$

$\therefore$  order of  $2 \pmod{17} \neq \phi(17)$

Try 3:  $3^3 \equiv 10 \pmod{17}$   
 $3^4 \equiv -4 \pmod{17}$ ,  $3^5 \equiv -12 \equiv 5$ ,  $3^6 \equiv 15$   
 $3^7 \equiv -40 \equiv -6$ ,  $3^8 \equiv -18 \equiv -1$ ,  $3^9 \equiv -3$ ,  $3^{10} \equiv -9$   
 $3^{11} \equiv -27 \equiv 7$ ,  $3^{12} \equiv 21 \equiv 4$ ,  $3^{13} \equiv 12$   
 $3^{14} \equiv 36 \equiv 2$ ,  $3^{15} \equiv 6$   
 $\therefore 3^{16} \equiv 18 \equiv 1 \pmod{17}$

$\therefore 3$  a primitive root of  $17$

$$3^4 \equiv 81 \pmod{17^2}, 3^8 \equiv 81^2 \equiv 6561 \equiv 203$$
$$\therefore 3^{16} \equiv 203^2 \equiv 41209 \equiv 171 \not\equiv 1 \pmod{17^2}.$$

$\therefore 3$  is a primitive root of  $17^k$ ,  $k \geq 1$ .

5. Obtain all the primitive roots of  $41$  and  $82$ .

Table on p. 166 states  $6$  is a prim. root of  $41$ .

Proof of Th. 8.4 shows all other primitive roots  
are congruent to one of  $6^1, \dots, 6^{40}$   
41 has  $\phi(\phi(41)) = \phi(40) = (2^3 - 2^2)(5 - 1) = 16$  incongruent  
prim. roots.

By Th. 8.3, since 6 has order 40, then  $6^h$  has  
order  $40/\gcd(h, 40)$ .  $\therefore$  If  $\gcd(h, 40) = 1$ , then  
 $6^h$  will have order 40, and  $\therefore$  be a prim. root.  
 $\gcd(h, 40) = 1 \Rightarrow$   
 $h = 1, 3, 7, 9, 11, 13, 17, 19, 21, 23, 27, 29, 31, 33, 37, 39$

For 82,  $\phi(82) = \phi(2 \cdot 41) = \phi(41)$

$\therefore$  82 also has 16 prim. roots.

$\therefore$  if  $r$  is a prim. root of 41, then  
 $r$  or  $r+41$ , whichever is odd, will also  
be a prim. root of 82.

$$\therefore \text{For } 41: 6^1 \equiv 6, 6^3 \equiv 11, 6^7 \equiv 29, 6^9 \equiv 19, 6^{11} \equiv 28, 6^{13} \equiv 24,$$

$$6^{17} \equiv 26, 6^{19} \equiv 34, 6^{21} \equiv 35, 6^{23} \equiv 30, 6^{27} \equiv 12,$$

$$6^{29} \equiv 22, 6^{31} \equiv 13, 6^{33} \equiv 17, 6^{37} \equiv 15, 6^{39} \equiv 7$$

$$\therefore 6, 7, 11, 12, 13, 15, 17, 19, 23, 24, 26, 28, 29, 30, 34, 35$$

$$\therefore \text{For } 82: 47, 7, 11, 53, 13, 15, 17, 19, 63, 65, 67, 69, 29, 71, 75, 35$$

or  $7, 11, 13, 15, 17, 19, 29, 35, 47, 53, 63, 65, 67, 69, 71, 75$

6.(a) Prove that a prim. root  $r$  of  $p^k$ ,  $p$  an odd prime, is a prim. root of  $2p^k \Leftrightarrow r$  is an odd integer.

(1) If  $r$  is odd, Then  $\gcd(r, 2p^k) = 1$ . [13]

Let  $n$  be order of  $r \pmod{2p^k}$ .

$\therefore n$  must divide, (by Th. 8.1),  $\phi(2p^k)$

$$\text{But } \phi(2p^k) = \phi(2)\phi(p^k) = \phi(p^k)$$

by [13] and  $\phi$  multiplicative

$$\begin{aligned} \text{But } r^n &\equiv 1 \pmod{2p^k} \Rightarrow r^n - 1 = a2p^k, \text{ some } a, \\ &\Rightarrow r^n - 1 = (2a)p^k \\ &\Rightarrow r^n \equiv 1 \pmod{p^k}. \end{aligned}$$

But  $r$  a prim. root of  $p^k \Rightarrow \phi(p^k) | n$  by Th. 8.1.

$\therefore n | \phi(p^k)$  and  $\phi(p^k) | n \Rightarrow n = \phi(p^k)$ .

$\therefore$  odd  $r$  prim. root of  $p^k \Rightarrow r$  a prim. root of  $2p^k$

(2) Let  $r$  be a prim. root of  $p^k$ ,  $p$  odd, and suppose  $r$  is also a prim. root of  $2p^k$ .

Then clearly  $\gcd(r, 2p^k) = 1$ , and since  $2p^k$  is even, Then  $r$  is odd.

(6) Confirm that  $3, 3^3, 3^5$ , and  $3^9$  are prim. roots of  $578 = 2 \cdot 17^2$ , but that  $3^4$  and  $3^{17}$  are not.

By 4(6),  $3$  is a prim. root of  $17^2$  and so by 6(a),  $3^h$  is a prim. root of  $2 \cdot 17^2$ .

By Th. 8-3,  $3^h$  will also have order  $\phi(17^2)$  if  $\gcd(h, \phi(17^2)) = 1$

$$\text{But } \phi(17^2) = 17^2 - 17 = 17(16) = 2^4 \cdot 17$$

Since for  $h = 1, 3, 5, 9$   $\gcd(h, 2^4 \cdot 17) = 1$ , then  $3^1, 3^3, 3^5, 3^9$  will also have order  $\phi(17^2)$

$\therefore 3, 3^3, 3^5, 3^9$  are all prim. roots of  $17^2$ , and are all odd, so by 6(a), are also prim. roots of  $2 \cdot 17^2$ .

For  $3^4$ ,  $\gcd(4, 2^4 \cdot 17) = 4$ , so order of  $3^4 \pmod{17^2}$  is  $\frac{\phi(17^2)}{4} = 2^2 \cdot 17 \neq \phi(17^2)$

For  $3^{17}$ ,  $\gcd(17, 2^4 \cdot 17) = 17$ , so order of  $3^{17} \pmod{17^2}$  is  $\frac{\phi(17^2)}{17} = 2^4 \neq \phi(17^2)$

$\therefore 3^4$  and  $3^{17}$  are not prim. roots of  $17^2$

The note written in problem 2(a) shows that if  $r$  is a prim. root of  $2p^k$ , then it is a prim. root of  $p^k$ .

$\therefore 3^4$  and  $3^{17}$  are not prim. roots of  $2 \cdot 17^2$ .

7. Assume  $r$  is a primitive root of the odd prime  $p$  and  $(r+t_p)^{p-1} \not\equiv 1 \pmod{p^2}$ . Show  $r+t_p$  is a primitive root of  $p^k$  for each  $k \geq 1$ .

Pf; Since  $r \equiv r+t_p \pmod{p}$ , Then  $r$  and  $r+t_p$  have same order.  $\therefore r+t_p$  is also a prim. root of  $p$ .

Since any prim. root of  $p$  has order mod  $p^2$  of  $(p-1)$  or  $p(p-1)$ , Then  $r+t_p$  has order mod  $p^2$  of  $(p-1)$  or  $p(p-1)$ .

Since  $(r+t_p)^{p-1} \not\equiv 1 \pmod{p^2}$ , order of  $r+t_p$  is not  $(p-1)$ , and so must be  $p(p-1) = \phi(p^2)$ .

$\therefore r+t_p$ , a prim. root of  $p$ , is also a

prim. root of  $p^2$ , and The proof of Lemma 2 and Th. 8-9 show That  $r + t\rho$  is a prim. root of  $p^k$ ,  $k \geq 1$ .

8. If  $n = 2^{k_0} p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$  is the prime factorization of  $n > 1$ ,

define The universal exponent  $\lambda(n)$  of  $n$  by

$$\lambda(n) = \text{lcm}(\lambda(2^{k_0}), \phi(p_1^{k_1}), \dots, \phi(p_r^{k_r}))$$

where  $\lambda(2) = 1$ ,  $\lambda(2^2) = 2$ ,  $\lambda(2^k) = 2^{k-2}$  for  $k \geq 3$ .

Prove The following statements concerning The universal exponent:

(a) For  $n = 2, 4, p^k, 2p^k$ , where  $p$  is an odd prime,

$$\lambda(n) = \phi(n)$$

Pf:  $\lambda(2) = 1$  by def.,  $\phi(2) = 2^1 - 2^0 = 1$  by Th. 7.3

$\lambda(4) = \lambda(2^2) = 2$  by def.,  $\phi(2^2) = 2^2 - 2^1 = 2$

For  $n = 2p^k$ , note  $\text{lcm}(1, x) = x$ .

$$\lambda(n) = \text{lcm}(\lambda(2), \phi(p^k))$$

$$= \text{lcm}(1, \phi(p^k)) = \phi(p^k) = \phi(n)$$

For  $n = p^k$ ,  $\lambda(n) = \text{lcm}(\phi(p^k)) = \phi(p^k) = \phi(n)$

(b) If  $\gcd(a, 2^k) = 1$ , Then  $a^{\lambda(2^k)} \equiv 1 \pmod{2^k}$

Pf: By Euler's Th.,  $a^{\phi(2^k)} \equiv 1 \pmod{2^k}$

$$\phi(2^k) = 2^k - 2^{k-1} = 2^{k-1}$$

For  $k=1$ ,  $\phi(2^k) = 1 = \lambda(2^k)$

$k=2$ ,  $\phi(2^k) = 2 = \lambda(2^2) = \lambda(2^k)$

$\therefore$  For  $k=1, 2$ ,  $a^{\lambda(2^k)} \equiv 1 \pmod{2^k}$

For  $k \geq 3$ ,  $\lambda(2^k) = 2^{k-2}$

Proof of Th. 8.3 showed for  $k \geq 3$ ,

$$\underline{\underline{a^{2^{k-2}} \equiv 1 \pmod{2^k}}} \quad \therefore a^{\lambda(2^k)} \equiv 1 \pmod{2^k}$$

$$\begin{aligned} \text{Alternatively, } \lambda(2^{k+1}) &= 2^{(k+1)-2} = 2^{k-1} \\ &= 2 \cdot 2^{k-2} = 2 \lambda(2^k) \end{aligned}$$

for  $k \geq 3$ .

$\therefore$  Using induction, have proved true  
for  $k=1, 2$ .

Assume true for  $K=3$

$$\therefore a^{\lambda(2^k)} \equiv 1 \pmod{2^k}$$

$$\therefore a^{\lambda(2^k)} = 1 + r2^k$$

$$\therefore a^{2\lambda(2^k)} = (1 + r2^k)^2$$

$$\therefore a^{\lambda(2^{k+1})} = 1 + 2r2^k + r^22^{2k}$$

$$= 1 + r2^{k+1} + r^22^{k-1} \cdot 2^{k+1}$$

$$= 1 + (r + r^2 \cdot 2^{k-1}) 2^{k+1}$$

$$\therefore a^{\lambda(2^{k+1})} \equiv 1 \pmod{2^{k+1}}$$

$\therefore$  true for all  $k$ .

(c) IF  $\gcd(a, n) = 1$ , Then  $a^{\lambda(n)} \equiv 1 \pmod{n}$

Pf: Let  $n = p^k$ ,  $p$  odd.  $\therefore \lambda(n) = \phi(n)$  by (a).

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

Note that by corollary 2,  $p_1, p_2$  prime,  
if  $c \equiv 0 \pmod{p_1} \quad \text{and} \quad c \equiv 0 \pmod{p_2}$ , then  $c \equiv 0 \pmod{p_1 p_2}$ ,  
 $c \equiv 0 \pmod{p_1} \quad \text{and} \quad c \equiv 0 \pmod{p_2}$  where  $\gcd(p_1, p_2) = 1$ .

$\therefore$  if  $n = 2^{k_0} p_1^{k_1} \cdots p_r^{k_r}$ , Then by (6) & (c),

$$a^{\lambda(2^{k_0})} \equiv 1 \pmod{2^{k_0}}$$

$$\therefore a^{\text{lcm}[\lambda(2^{k_0}), \phi(p_1^{k_1}), \dots, \phi(p_r^{k_r})]} \equiv 1 \pmod{2^{k_0}}$$

$$\text{since } \lambda(2^{k_0}) \mid \text{lcm}[\lambda(2^{k_0}), \phi(p_1^{k_1}), \dots, \phi(p_r^{k_r})]$$

$$\therefore a^{\lambda(n)} \equiv 1 \pmod{2^{k_0}} \quad [1]$$

(or  $a^{\lambda(n)-1} \equiv 0 \pmod{2^{k_0}}$ )

$$a^{\lambda(p_i^{k_i})} \equiv 1 \pmod{p_i^{k_i}}$$

$$\therefore a^{\text{lcm}[\lambda(2^{k_0}), \phi(p_1^{k_1}), \dots, \phi(p_r^{k_r})]} \equiv 1 \pmod{p_i^{k_i}}$$

$$\text{since } \lambda(p_i^{k_i}) \mid \text{lcm}[\lambda(2^{k_0}), \phi(p_1^{k_1}), \dots, \phi(p_r^{k_r})]$$

$$\text{as } \lambda(p_i^{k_i}) = \phi(p_i^{k_i}) \text{ by (a)}$$

$$\therefore a^{\lambda(n)} \equiv 1 \pmod{p_i^{k_i}} \quad [2]$$

(or,  $a^{\lambda(n)-1} \equiv 0 \pmod{p_i^{k_i}}$ )

$$\therefore \text{By [1] \& [2], } a^{\lambda(n)} \equiv 1 \pmod{n}$$

9. Verify that, for  $5040 = 2^4 \cdot 3^2 \cdot 5 \cdot 7$ ,  $\lambda(5040) = 12$  and  $\phi(5040) = \underline{1152}$ .

$$\begin{aligned} \text{By def. in #8, } \lambda(5040) &= \text{lcm}(\lambda(2^4), \phi(3^2), \phi(5), \phi(7)) \\ &= \text{lcm}(2^2, 3^2 \cdot 3, 4, 6) \\ &= \text{lcm}(2^2, 2 \cdot 3, 2^2, 2 \cdot 3) = 2^2 \cdot 3 = \underline{12} \end{aligned}$$

$$\begin{aligned} \phi(5040) &= (2^4 - 2^3) \cdot (3^2 - 3) \cdot (4) \cdot (6) \\ &= (8)(6)(4)(6) = \underline{1152} \end{aligned}$$

10. Use Problem 8 to show that if  $n \neq 2, 4, p^k, 2p^k$ , where  $p$  is an odd prime, Then  $n$  has no primitive root.

Pf: Let  $n = 2^{k_0} p_1^{k_1} \cdots p_r^{k_r}$  be the prime factorization

Note from Th. 2.8,  $\gcd(a, b) \cdot \text{lcm}(a, b) = ab$ .  
 $\therefore \text{lcm}(a, b) \mid ab$  and  $\text{lcm}(a, b) \leq ab$ .

If  $k_0 \neq 0$ , Then since  $n \neq 2, 4$ , or  $2p^k$ , Then  
 $k_0 \geq 3$ , so  $\lambda(2^{k_0}) = 2^{k_0-2} < 2^{k_0-1} = \phi(2^{k_0})$   
 $\therefore \lambda(2^{k_0}) = \frac{1}{2} \phi(2^{k_0})$   
 $\therefore \lambda(n) = \text{lcm}(\lambda(2^{k_0}), \phi(p_1^{k_1}), \dots, \phi(p_r^{k_r}))$

$$= \text{lcm}(2^{k_0-2}, \phi(p_1^{k_1}), \dots, \phi(p_r^{k_r}))$$

$$< \text{lcm}(2^{k_0-1}, \phi(p_1^{k_1}), \dots, \phi(p_r^{k_r})), \text{ by prob. #1, section 6.1}$$

$$= \text{lcm}(\phi(2^{k_0}), \phi(p_1^{k_1}), \dots, \phi(p_r^{k_r}))$$

$$\leq \phi(n)$$

$\therefore \lambda(n) < \phi(n)$ , and from 8.(c),

$$a^{\lambda(n)} \equiv 1 \pmod{n}$$

$\therefore n$  has no primitive root for  $k_0 \neq 0$ .

If  $k_0 = 0$ , Then  $\lambda(n) = \text{lcm}(\phi(p_1^{k_1}), \dots, \phi(p_r^{k_r}))$

Each  $\phi(p_i^{k_i})$  is even, and  $r > 1$  (i.e., more than one prime factor).

$\therefore$  If  $\phi(p_i^{k_i}) = 2 \leq$

$$\therefore \text{gcd}(\phi(p_1^{k_1}), \dots, \phi(p_r^{k_r})) = \underset{\geq 2}{\text{gcd}}(2s_1, \dots, 2s_r)$$

$$\therefore \text{lcm}(\phi(p_1^{k_1}), \dots, \phi(p_r^{k_r})) \cdot \text{gcd}(\phi(p_1^{k_1}), \dots, \phi(p_r^{k_r}))$$

$$\geq 2 \text{lcm}(\phi(p_1^{k_1}), \dots, \phi(p_r^{k_r}))$$

$\therefore$  Since  $\gcd(a, b) \cdot \text{lcm}(a, b) = ab$ , then

$$\begin{aligned}\phi(n) &= \phi(p_1^{k_1}) \cdots \phi(p_r^{k_r}) \geq 2 \text{lcm}(\phi(p_1^{k_1}), \dots, \phi(p_r^{k_r})) \\ &> \text{lcm}(\phi(p_1^{k_1}), \dots, \phi(p_r^{k_r})) \\ &= \lambda(n)\end{aligned}$$

$\therefore \lambda(n) < \phi(n)$  for  $k_0 = 0$ , and from 8.(c),

$$a^{\lambda(n)} \equiv 1 \pmod{n}.$$

$\therefore$  for  $n \neq 2, 4, p^k, 2p^k$ ,  $\lambda(n) < \phi(n)$ ,

$$\text{and } a^{\lambda(n)} \equiv 1 \pmod{n}.$$

$\therefore n$  has no primitive root.

11. (a) Prove that if  $\gcd(a, n) = 1$ , then the linear congruence  $ax \equiv b \pmod{n}$  has the solution  $x \equiv b a^{\lambda(n)-1} \pmod{n}$ .

Pf: By 8.(c),  $a^{\lambda(n)} \equiv 1 \pmod{n}$ , so

$$b a^{\lambda(n)} \equiv b \pmod{n}$$

$$\therefore 6 \cdot a \cdot a^{\lambda(n)-1} \equiv 6 \pmod{n}$$

$$\therefore a(6a^{\lambda(n)-1}) \equiv 6 \pmod{n}$$

$\therefore x \equiv 6a^{\lambda(n)-1} \pmod{n}$  is a solution.

(3) Use part (a) to solve  $13x \equiv 2 \pmod{40}$  and  
 $3x \equiv 13 \pmod{77}$

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

$$\therefore \text{By (a)} \quad x \equiv 2 \cdot 13^{\lambda(40)-1}$$

$$\begin{aligned} \text{Since } 40 &= 2^3 \cdot 5, \quad \lambda(40) = \text{lcm}(\lambda(2^3), \phi(5)) \\ &= \text{lcm}(2, 4) = 4. \end{aligned}$$

$$\therefore x \equiv 2 \cdot 13^3 \pmod{40}, \quad 2 \cdot 13^3 = 4394$$
$$4394 \equiv 34 \pmod{40}.$$

$$\therefore x \equiv 2 \cdot 13^3 \equiv 34 \pmod{40}$$

$$3x \equiv 13 \pmod{77}. \text{ Note } \gcd(3, 77) = 1.$$

$$\therefore \text{By (a)}, \quad x \equiv 13^{-3} \lambda(77)-1$$

$$77 = 7 \cdot 11, \text{ so } \lambda(n) = \text{lcm}(\phi(7), \phi(11))$$

$$= \text{cm}(\ell, 10) = 30$$

$$\therefore x \equiv 13 \cdot 3^{29} \pmod{77}$$

$$3^4 \equiv 4, \quad 3^8 \equiv 16, \quad 3^{12} \equiv 64, \quad 3^{24} \equiv 4096 \equiv 15$$

$$3^{28} \equiv 60, \quad 3^{29} \equiv 180 \equiv 26, \quad 13 \cdot 3^{29} \equiv 13 \cdot 26 = 338 \equiv 30$$

$$\therefore x \equiv 13 - 3^{29} \equiv 30 \pmod{77}$$

## 8.4 The Theory of Indices

Note Title

4/3/2006

1. Find The index of 5 relative to each of the primitive roots of 13.

There are  $\phi(\phi(13)) = \phi(12) = 4$  prim. roots of 13. 2 is a primitive root as  $2^{12} \equiv 1 \pmod{13}$  and  $2^1, 2^2, 2^3, 2^4, 2^5, 2^6 \not\equiv 1 \pmod{13}$ .

∴ Other prim. roots are found from  $2^K$ ,  $1 \leq K \leq 12$ , s.t.  $\gcd(K, 12) = 1$ , by Th. 8.3 and 8.4.

$$\gcd(K, 12) = 1 \Rightarrow K = 1, 5, 7, 11.$$

$$2^1 \equiv 2, 2^5 \equiv 6, 2^7 \equiv 11, 2^{11} \equiv 7 \pmod{13}.$$

∴ Prim. roots of 13 are: 2, 6, 7, 11.

Construct powers of roots till get 5.

$$2: 2^1 \equiv 2, 2^2 \equiv 4, 2^3 \equiv 8, 2^4 \equiv 3, 2^5 \equiv 6, 2^6 \equiv 12, 2^7 \equiv 11, 2^8 \equiv 9, \\ \underline{2^9 \equiv 5}$$

$$6: 6^1 \equiv 6, 6^2 \equiv -3 \equiv 10, 6^3 \equiv -18 \equiv 8, 6^4 \equiv 48 \equiv 9, 6^5 \equiv 2, \\ 6^6 \equiv 12 \equiv -1, 6^7 \equiv -6 \equiv 7, 6^8 \equiv -36 \equiv 3, \underline{6^9 \equiv 18 \equiv 5}$$

$$7: 7^1 \equiv 7, 7^2 \equiv 10 \equiv -3, \underline{7^3 \equiv -21 \equiv 5}$$

$$H: 11^1 \equiv 11 \equiv -2, 11^2 \equiv -22 \equiv 4, \underline{11^3 \equiv 44 \equiv 5}$$

$$\therefore \text{ind}_2 5 = 9, \text{ind}_6 5 = 9, \text{ind}_7 5 = 3, \text{ind}_{11} 5 = 3$$

2. Use a table of indices for a prim. root of 11, solve the following congruences:

$$(a) 7x^3 \equiv 3 \pmod{11}$$

$$(b) 3x^4 \equiv 5 \pmod{11}$$

$$(c) x^8 \equiv 10 \pmod{11}$$

By table on p. 166, 2 is a prim. root of 11.

$$2^1 \equiv 2, 2^2 \equiv 4, 2^3 \equiv 8, 2^4 \equiv 5, 2^5 \equiv 10 \equiv -1, 2^6 \equiv -2 \equiv 9 \\ 2^7 \equiv 7, 2^8 \equiv 3, 2^9 \equiv 6, 2^{10} \equiv 1$$

a	1	2	3	4	5	6	7	8	9	10
ind <sub>2</sub> a	10	1	8	2	4	9	7	3	6	5

$$(a) 7x^3 \equiv 3 \pmod{11}$$

gcd(3, 11) = 1, and 11 has a prim. root

$$7x^3 \equiv 3 \pmod{11} \Leftrightarrow \text{ind}_2 7 + 3 \text{ind}_2 x \equiv \text{ind}_2 3 \pmod{10}$$

$$\Leftrightarrow 7 + 3 \text{ind}_2 x \equiv 8 \pmod{10}$$

$$\Leftrightarrow 3 \text{ind}_2 x \equiv 1 \pmod{10}$$

Since  $\gcd(3, 10) = 1$ , and  $1 \mid 1$ ,  
Then by Th. 4.7, There is one incongruent  
solution.

$\text{ind}_2 x \equiv 7 \pmod{10}$  is a solution.

From table,  $x = 7$

$$\therefore \underline{\underline{x \equiv 7 \pmod{11}}}$$

$$(6) 3x^4 \equiv 5 \pmod{11}$$

$\gcd(5, 11) = 1$ , and 11 has a prim. root.

$$3x^4 \equiv 5 \pmod{11} \Leftrightarrow \text{ind}_2 3 + 4\text{ind}_2 x \equiv \text{ind}_2 5 \pmod{10}$$

$$\Leftrightarrow 8 + 4\text{ind}_2 x \equiv 4 \pmod{10}$$

$$\Leftrightarrow 4\text{ind}_2 x \equiv 6 \pmod{10}$$

$\gcd(4, 10) = 2$ , and  $2 \mid 6$ , so  
2 incongruent solutions.

$$4\text{ind}_2 x \equiv 6 \pmod{10} \Rightarrow$$

$$2\text{ind}_2 x \equiv 3 \pmod{5} \Rightarrow$$

$$\text{ind}_2 x = 4, 9$$

$$\therefore x \equiv 5, 6 \pmod{11}$$

$$(c) x^8 \equiv 10 \pmod{11}$$

$\gcd(10, 11) = 1$ , and 11 has a prim. root

$$x^8 \equiv 10 \pmod{11} \Leftrightarrow 8 \text{ind}_2 x \equiv \text{ind}_2 10 \pmod{10}$$

$$\Leftrightarrow 8 \text{ind}_2 x \equiv 5 \pmod{10}$$

But  $\gcd(8, 10) = 2$  and  $2 \nmid 5$   
 $\therefore$  by Th. 4.7, no solution to  $8 \text{ind}_2 x \equiv 5 \pmod{10}$

$\therefore$  no solution to  $x^8 \equiv 10 \pmod{11}$

3. The following is a table of indices for the prime 17 relative to the primitive root 3:

$a$	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$\text{ind}_3 a$	16	14	1	12	5	15	11	10	2	3	7	13	4	9	6	8

With the aid of this table, solve the following congruences:

- (a)  $x^{12} \equiv 13 \pmod{17}$ .
- (b)  $8x^5 \equiv 10 \pmod{17}$ .
- (c)  $9x^8 \equiv 8 \pmod{17}$ .
- (d)  $7^x \equiv 7 \pmod{17}$ .

$$(a) x^{12} \equiv 13 \pmod{17} \quad \gcd(13, 17) = 1$$

$$\therefore 12 \text{ind}_3 x \equiv \text{ind}_3 13 \pmod{16}, \text{ind}_3 13 = 4$$

$$\therefore 12 \text{ind}_3 x \equiv 4 \pmod{16}, \gcd(12, 16) = 4$$

$\therefore$  4 incongruent solutions.

Dividing by 4,

$$3 \text{ind}_3 x \equiv 1 \pmod{4}$$

$$\therefore \text{ind}_3 x = 3, 7, 11, 15$$

$$\therefore x = 10, 11, 7, 6 \text{ from table}$$

$$\therefore x \equiv 6, 7, 10, 11 \pmod{12}$$

$$(5) 8x^5 \equiv 10 \pmod{17} \quad \gcd(10, 17) = 1$$

$$\therefore \text{ind}_3 8 + 5 \text{ind}_3 x \equiv \text{ind}_3 10 \pmod{16}$$

$$\therefore 10 + 5 \text{ind}_3 x \equiv 3 \pmod{16}$$

$$5 \text{ind}_3 x \equiv -7 \pmod{16} \quad \gcd(5, 16) = 1$$

$\therefore$  1 solution

$$\therefore 15 \text{ind}_3 x \equiv -21$$

$$- \text{ind}_3 x \equiv -21$$

$$\text{ind}_3 x \equiv 21 \equiv 5, \therefore x = 5 \text{ (from table).}$$

$$\therefore x \equiv 5 \pmod{17}$$

$$(c) 9x^8 \equiv 8 \pmod{17} \quad \gcd(8, 17) = 1$$

$$\text{ind}_3 9 + 8 \text{ind}_3 x \equiv \text{ind}_3 8 \pmod{16}$$

$$\therefore 2 + 8 \text{ind}_3 x \equiv 10 \pmod{16}$$

$$8 \text{ind}_3 x \equiv 8 \pmod{16} \quad \gcd(8, 16) = 8$$

$\therefore 8$  incongruent solutions

$$\therefore \text{ind}_3 x \equiv 1 \pmod{2}$$

$$\therefore \text{ind}_3 x = 1, 3, 5, 7, 9, 11, 13, 15$$

$$\therefore x \equiv 3, 10, 5, 11, 14, 7, 12, 6 \pmod{17}$$

$$(d) 7^x \equiv 7 \pmod{17} \quad \gcd(7, 17) = 1$$

$$\therefore x \text{ind}_3 7 \equiv \text{ind}_3 7 \pmod{16}$$

$$11x \equiv 11 \pmod{16}, \quad \gcd(11, 16) = 1, \text{ so}$$

$$\therefore x \equiv 1 \pmod{16} \quad [\text{just one solution, don't need table at this point}].$$

4. Find the remainder when  $3^{24} \cdot 5^{13}$  is divided by 17.

$$3^{24} \cdot 5^{13} \equiv x \pmod{17}. \quad \gcd(1, 17) = 1, \text{ so just 1 solution}$$

Use 3 as a prim. root of 17, and use table in #3 above.

$$\therefore 24 \text{ind}_3 3 + 13 \text{ind}_3 5 \equiv \text{ind}_3 x \pmod{16}$$

$$\therefore 24(1) + 13(-5) \equiv \text{ind}_3 x \pmod{16}$$

$$89 \equiv 9 \equiv \text{ind}_3 x \pmod{16}, \quad x = 14 \text{ from table}$$

$$\therefore x \equiv 14 \pmod{17}$$

$$\therefore \text{remainder} = \underline{14}$$

5. If  $r$  and  $r'$  are both primitive roots of the odd prime  $p$ , show that for  $\gcd(a, p) = 1$

$$\text{ind}_{r'} a \equiv (\text{ind}_r a)(\text{ind}_{r'} r) \pmod{p-1}$$

This corresponds to the rule for changing the base of logarithms.

Pf: Let  $x = \text{ind}_{r'} a \pmod{p}$

$$y = \text{ind}_r a \pmod{p}$$

$$z = \text{ind}_{r'} r \pmod{p}$$

$\therefore$  By def.,  $(r')^x \equiv a \pmod{p}$ ,

$r^y \equiv a \pmod{p}$ , and

$$(r')^z \equiv r \pmod{p} \Rightarrow (r')^{zy} \equiv r^y \pmod{p}$$

$$\therefore (r')^x \equiv r^y \equiv (r')^{zy} \pmod{p}$$

By Th. 8.2,  $x \equiv zy \pmod{p-1}$

$$\therefore \text{ind}_{r'} a \equiv (\text{ind}_r a)(\text{ind}_r r) \pmod{p-1}$$

6.

(a) Construct a table of indices for the prime 17 with respect to the primitive root 5  
[Hint: By the previous problem,  $\text{ind}_5 a \equiv 13 \text{ ind}_3 a \pmod{16}$ .]

(b) Solve the congruences in Problem 3, using the table in part (a).

$$(a) \text{By } \#5, \text{ind}_5 a = (\text{ind}_6 3)(\text{ind}_3 a) \pmod{16}$$

$$\text{Let } \text{ind}_5 3 = x. \quad \therefore 5^x \equiv 3 \pmod{17}$$

$$\therefore x \text{ ind}_3 5 \equiv \text{ind}_3 3 \equiv 1 \pmod{16}$$

$$\text{From tab/z in } \#3, \text{ind}_3 5 = 5$$

$$\therefore 5x \equiv 1 \pmod{16}, \gcd(5, 16) = 1, \text{ so just one solution } \pmod{16}. \quad \therefore 15x \equiv 3, -x \equiv 3, x \equiv 13$$

$$\therefore \text{ind}_5 3 = 13$$

$$\therefore \text{ind}_5 a \equiv 13 \text{ ind}_3 a \pmod{16}$$

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
ind <sub>3</sub> a	16	14	1	12	5	15	11	10	2	3	7	13	4	9	6	8
13 ind <sub>3</sub> a	208	182	13	156	65	195	143	130	26	39	91	169	52	117	78	104
ind <sub>5</sub> a	16	6	13	12	1	3	15	2	10	7	11	9	4	5	14	8

$$(6) \quad x^{12} \equiv 13 \pmod{17}$$

$$12 \text{ ind}_5 x \equiv \text{ind}_5 13 \pmod{16},$$

$$12 \text{ ind}_5 x \equiv 4 \pmod{16}, \quad \text{gcd}(12, 16) = 4 \text{ solutions}$$

$$3 \text{ ind}_5 x \equiv 1 \pmod{4}, \quad \text{ind}_5 x = 3, 7, 11, 15$$

$$\therefore x \equiv 6, 10, 11, 7 \pmod{17} \text{ as in } \#3$$

$$8x^5 \equiv 10 \pmod{17}$$

$$\text{ind}_5 8 + 5 \text{ ind}_5 x \equiv \text{ind}_5 10 \pmod{16}$$

$$2 + 5 \text{ ind}_5 x \equiv 7$$

$$5 \text{ ind}_5 x \equiv 5 \pmod{16} \quad \text{gcd}(5, 16) = 1 \text{ solution}$$

$$\therefore \text{ind}_5 x \equiv 1 \pmod{16}$$

$$x \equiv 5 \pmod{17}, \text{ as in } \#3$$

$$9x^8 \equiv 8 \pmod{17}$$

$$\text{ind}_5 9 + 8 \text{ ind}_5 x \equiv \text{ind}_5 8 \pmod{16}$$

$$10 + 8 \text{ ind}_5 x \equiv 2 \pmod{16}$$

$$8 \text{ ind}_5 x \equiv -8 \equiv 8 \pmod{16} \quad \gcd(8, 16) = 8 \text{ solutions}$$

$$\text{ind}_5 x \equiv 1 \pmod{2}$$

$$\text{ind}_5 x = 1, 3, 5, 7, 9, 11, 13, 15$$

$$\therefore x \equiv 5, 6, 14, 10, 12, 11, 3, 7 \pmod{16}, \text{as in } \#3$$

$$7^x \equiv 7 \pmod{16}$$

$$x \text{ ind}_5 7 \equiv \text{ind}_5 7 \pmod{16}$$

$$15x \equiv 15 \pmod{16}, \quad \gcd(15, 16) = 1 \text{ solution}$$

$$x \equiv 1 \pmod{16}, \quad \text{same as in } \#3$$

7. If  $r$  is a primitive root of the odd prime  $p$ , verify that

$$\text{ind}_r(-1) = \text{ind}_r(p-1) = \frac{1}{2}(p-1)$$

Pf: Since  $-1 \equiv p-1 \pmod{p}$ , Then

$$\underline{\text{ind}_r(-1)} = \underline{\text{ind}_r(p-1)}$$

(5) Let  $x = \text{ind}_r(p-1)$ . Then  $r^x \equiv p-1 \pmod{p}$

As  $p$  is odd,  $p-1$  is even and  $\therefore \frac{p-1}{2}$  exists

$$\therefore r^{p-1} \equiv 1 \equiv p^2 - 2p + 1 = (p-1)^2 \pmod{p}$$

$$\therefore r^{p-1} \equiv (p-1)^2 \pmod{p}$$

$$\therefore r^{\frac{p-1}{2}} \equiv p-1 \text{ or } -(p-1) = -p+1$$

If  $r^{\frac{p-1}{2}} \equiv -p+1 \equiv 1 \pmod{p}$ , Then since  $\frac{p-1}{2} < p-1$ ,  $r$  wouldn't have order  $p-1$ .

$$\therefore r^{\frac{p-1}{2}} \not\equiv -p+1$$

$$\therefore r^{\frac{p-1}{2}} \equiv p-1 \pmod{p}$$

$$\therefore \text{By def., } \underline{\text{ind}_r(p-1)} = \frac{p-1}{2}$$

8. (a) Determine the integers  $a$  ( $1 \leq a \leq 12$ ) s.t. the congruence  $ax^4 \equiv 6 \pmod{13}$  has a solution for  $b = 2, 5, 6$ .

Note That  $\gcd(5, 13) = 1$

$$\therefore \text{ind } a + 4 \text{ ind } x \equiv \text{ind } 5 \pmod{12}$$

$$\therefore 4 \text{ ind } x \equiv \text{ind } 5 - \text{ind } a \pmod{12}$$

$\gcd(4, 12) = 4$ , so for a solution to exist,

$$4 \mid (\text{ind } 5 - \text{ind } a)$$

$$\therefore \text{ind } b - \text{ind } a = 0, 4(\text{or } -4), 8(\text{or } -8)$$

$$(1) \text{ind } b - \text{ind } a = 0, \therefore \text{ind } b = \text{ind } a$$

$\because b \equiv a$ , and with  $1 \leq a \leq 12, \therefore b = a$

$\therefore a = 2, 5, 6$  when  $b = 2, 5, 6$ , respectively

$$(2) \text{ind } b - \text{ind } a = 4(\text{or } -4)$$

Using table of indices for prim. root 2 of 13  
(p. 175),  $\text{ind}_2 2 = 1, \text{ind}_2 5 = 9, \text{ind}_2 6 = 5$

$$\therefore 1 - \text{ind}_2 a = -4 \Rightarrow \text{ind}_2 a = 5 \Rightarrow a = 6$$

$$9 - \text{ind}_2 a = 4 \Rightarrow \text{ind}_2 a = 5 \Rightarrow a = 6$$

$$5 - \text{ind}_2 a = 4, -4 \Rightarrow \text{ind}_2 a = 1, 9 \Rightarrow a = 2, 5$$

$$\therefore b = 2 : a = 6$$

$$b = 5 : a = 6$$

$$b = 6 : a = 2 \text{ or } 5$$

$$(3) \text{ind } b - \text{ind } a = 8(\text{or } -8)$$

Using table as in (2) above,

$$1 - \text{ind}_2 a = -8, \text{ind}_2 a = 9 \Rightarrow a = 5$$

$$9 - \text{ind}_2 a = 8, \text{ind}_2 a = 1 \Rightarrow a = 2$$

$$5 - \text{ind}_2 a = -8, \text{ind}_2 a = 13 \Rightarrow \text{no solution}$$

$\therefore$  When  $b = 2$ ,  $a = 2, 6, \text{ or } 5$   
 $b = 5$ ,  $a = 5, 6, \text{ or } 2$   
 $b = 6$ ,  $a = 6, 2, \text{ or } 5$

(6) Determine the integers  $a$  ( $1 \leq a \leq p-1$ ) s.t. The congruence  $x^4 \equiv a \pmod{p}$  has a solution for  $p = 7, 11, 13$ .

Construct table of indices for 7, 11  
 3 is a prim. root of 7, 2 is a prim. root of 11.

$$3^1 \equiv 3, 3^2 \equiv 2, 3^3 \equiv 6, 3^4 \equiv 4, 3^5 \equiv 5, 3^6 \equiv 1 \pmod{7}$$

$$\begin{aligned} 2^1 &\equiv 2, 2^2 \equiv 4, 2^3 \equiv 8, 2^4 \equiv 6, 2^5 \equiv 10, 2^6 \equiv 9, 2^7 \equiv 7, 2^8 \equiv 5, \\ 2^9 &\equiv 3, 2^{10} \equiv 1 \pmod{11} \end{aligned}$$

$$\begin{array}{ccccccc} a & 1 & 2 & 3 & 4 & 5 & 6 \\ \text{ind}_3 a & 6 & 2 & 1 & 4 & 5 & 3 \end{array}$$

$$\begin{array}{cccccccccc} a & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ \text{ind}_2 a & 10 & 1 & 8 & 2 & 4 & 9 & 7 & 3 & 6 & 5 \end{array}$$

$$p=7: x^4 \equiv a \pmod{7}$$

$$4 \text{ ind } x \equiv \text{ind } a \pmod{6}, \gcd(4, 6) = 2$$

$$\therefore 2 | \text{ind } a \Rightarrow \text{ind } a = 2, 4, 6$$

$$\therefore \underline{a \equiv 2, 4, 1}$$

$$p=11: x^4 \equiv a \pmod{11}$$

Find  $x \equiv \text{ind } a \pmod{10}$ ,  $\gcd(4, 10) = 2$   
 $\therefore 2 \mid \text{ind } a, \therefore \text{ind } a = 2, 4, 6, 8, 10$

$$\therefore \underline{a \equiv 4, 5, 9, 3, 1}$$

$$p=13: x^4 \equiv a \pmod{13}$$

Find  $x \equiv \text{ind } a \pmod{12}$ ,  $\gcd(4, 12) = 4$   
 $\therefore 4 \mid \text{ind } a \Rightarrow \text{ind } a = 4, 8, 12$

Use table on p. 175

$$\therefore \underline{a \equiv 3, 9, 1}$$

9. Employ the corollary to Th. 8.12 to establish that if  $p$  is an odd prime, then

$$(a) x^2 \equiv -1 \pmod{p} \text{ is solvable} \Leftrightarrow p \equiv 1 \pmod{4}$$

Since  $-1 \equiv p-1 \pmod{p}$ , and  $\gcd(p-1, p) = 1$ , Then  
 $\gcd(-1, p) = 1$ .

Using corollary to Th. 8.12,  $x^2 \equiv -1 \pmod{p}$  is

solvable  $\Leftrightarrow (-1)^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ , as  
 $z = \gcd(2, p-1)$  since  $p$  is odd.

$$(-1)^{\frac{p-1}{2}} = 1 \text{ if } \frac{p-1}{2} \text{ is even}$$

$$-1 \text{ if } \frac{p-1}{2} \text{ is odd}$$

$$\text{So, } (-1)^{\frac{p-1}{2}} \equiv 1 \Leftrightarrow (-1)^{\frac{p-1}{2}} = 1 \Leftrightarrow \frac{p-1}{2} \text{ is even}$$

$$\therefore \frac{p-1}{2} = 2k, \text{ some } k, \text{ so } p = 1 + 4k, \text{ or}$$

$$p \equiv 1 \pmod{4}$$

$$\therefore x^2 \equiv 1 \pmod{p} \text{ solvable} \Leftrightarrow p \equiv 1 \pmod{4}$$

$$(b) x^4 \equiv -1 \pmod{p} \text{ is solvable} \Leftrightarrow p \equiv 1 \pmod{8}$$

As in (a),  $\gcd(-1, p) = 1$ . Using corollary to Th. 8.12,

$$x^4 \equiv -1 \pmod{p} \text{ solvable} \Leftrightarrow (-1)^{\frac{p-1}{d}} \equiv 1 \pmod{p},$$

where  $d = \gcd(4, p-1)$

If  $d = 2$ , Then as in (a),  $p = 1 + 4k$ , some  $k$ ,  
 $\therefore p \equiv 1 \pmod{4}$  and  $\therefore p \equiv 1 \pmod{8}$

If  $d = 4$ , Then  $\frac{p-1}{4} = 2k$ ,  $p = 1 + 8k$ , some  $k$ ,  
 $\therefore p \equiv 1 \pmod{8}$

$\therefore$  if  $(-1)^{\frac{p-1}{d}} \equiv 1 \pmod{p}$  Then  $p \equiv 1 \pmod{8}$

But if  $p \equiv 1 \pmod{8}$ , Then  $p-1 = 8k$ , some  $k$ ,

$$\text{so } (-1)^{\frac{p-1}{d}} = (-1)^{\frac{8k}{d}} = 1 \text{ whether } d=2 \text{ or } 4,$$

so  $(-1)^{\frac{p-1}{d}} \equiv 1 \pmod{p}$ , so  $x^4 \equiv -1 \pmod{p}$  is solvable.

$\therefore x^4 \equiv -1 \pmod{p}$  solvable  $\Leftrightarrow p \equiv 1 \pmod{8}$

10. Given the congruence  $x^3 \equiv a \pmod{p}$ , where  $p \geq 5$  is a prime and  $\gcd(a, p) = 1$ , prove the following:

(a) If  $p \equiv 1 \pmod{6}$ , Then the congruence has either no solutions or 3 incongruent solutions mod  $p$ .

Pf: If  $p \equiv 1 \pmod{6}$ , Then  $p-1 = 6k$ , some  $k$ .  
 $\therefore \gcd(3, 6k) = 3$ .

Since  $p$  is prime, it has a prim. root,  
 so

$$x^3 \equiv a \pmod{p} \Leftrightarrow 3 \text{ ind } x \equiv \text{ind } a \pmod{6k}$$

By Th. 4.7, if  $3 \nmid \text{ind}_a$ , there is no solution. If  $3 \mid \text{ind}_a$ , then there are 3 incongruent solutions.

(6) If  $p \equiv 5 \pmod{6}$ , then the congruence has a unique solution mod  $p$ .

Pf: If  $p \equiv 5 \pmod{6}$ , then  $p-5 = 6k$ , some  $k$ .  
 $\therefore p-1 = 6k+4 = 2(3k+2)$

$$\therefore \gcd(3, p-1) = \gcd(3, 2(3k+2)) = 1. \\ \text{since } \gcd(3, 3k+2) = 1 \text{ for all } k.$$

$$\therefore x^3 \equiv a \pmod{p} \Leftrightarrow 3 \text{ind} x \equiv \text{ind} a \pmod{p-1} \\ \Leftrightarrow 3 \text{ind} x \equiv \text{ind} a \pmod{2(3k+2)}$$

Since  $1 \mid \text{ind} a$ , by Th. 4.7, the latter congruence has a unique solution mod  $p-1$ , and so  $x^3 \equiv a \pmod{p}$  has a unique solution mod  $p$ .

11. Show that the congruence  $x^3 \equiv 3 \pmod{19}$  has no solutions, whereas  $x^3 \equiv 11 \pmod{19}$  has three incongruent solutions.

$$(1) x^3 \equiv 3 \pmod{19}, \gcd(3, 19) = 1$$

Since  $\gcd(3, \phi(19)) = \gcd(3, 18) = 3$ , by Th. 8.12,

$$\text{since } 3^{\frac{18}{3}} = 3^6 = 3^3 \cdot 3^3 \equiv 8 \cdot 8 \equiv 7 \not\equiv 1 \pmod{19},$$

Then  $x^3 \equiv 3 \pmod{19}$  has no solutions.

$$(2) x^3 \equiv 11 \pmod{19}, \gcd(11, 19) = 1$$

Since  $\gcd(3, \phi(19)) = 3$ , by Th. 8.12, since

$$11^{\frac{18}{3}} = 11^6 \equiv (-8)^6 = (64)^3 \equiv 7^3 \equiv 49 \cdot 7 \equiv 11 \cdot 7 \equiv 1 \pmod{19},$$

Then there are  $3 = \gcd(3, \phi(19))$  incongruent solutions.

12. Determine whether the two congruences  $x^5 \equiv 13 \pmod{23}$  and  $x^7 \equiv 15 \pmod{29}$  are solvable.

$$(1) x^5 \equiv 13 \pmod{23}$$

Using Th. 8.12,  $\gcd(13, 23) = 1$ , and  $\gcd(5, 22) = 1$   
 $\therefore$  solvable  $\Leftrightarrow 13^{22} \equiv 1 \pmod{23}$

$$13^2 \equiv 169 \equiv 8, 13^4 \equiv 64 \equiv -5, 13^8 \equiv 25 \equiv 2,$$

$$13^{16} \equiv 4, 13^{20} \equiv -20 \equiv 3, 13^{22} \equiv 8 \cdot 3 = 24 \equiv 1$$

$\therefore 13^{22} \equiv 1 \pmod{23}$ , and so  $x^5 \equiv 13 \pmod{23}$   
is solvable.

(2)  $x^7 \equiv 15 \pmod{29}$

$\gcd(15, 29) = 1$ ,  $\gcd(7, 28) = 7$ .  
 $\therefore$  By Th. 8-12, solvable  $\Leftrightarrow 15^{\frac{28}{7}} \equiv 1 \pmod{29}$

$$15^2 = 225 \equiv 22, 15^4 = 22^2 = 484 \equiv 20 \not\equiv 1 \pmod{29}$$

$\therefore$  not solvable.

13. If  $p$  is a prime and  $\gcd(k, p-1) = 1$ , prove that the integers  $1^k, 2^k, 3^k, \dots, (p-1)^k$  form a reduced set of residues mod  $p$ .

Pf:  $1, 2, \dots, p-1$  form a reduced set of residues mod  $p$ .

Thus, each of  $1^k, 2^k, \dots, (p-1)^k$  must be congruent to one of  $1, 2, \dots, p-1$ .

Let  $1 \leq a \leq p-1$ ,  $1 \leq b \leq p-1$ , and  $a \neq b$ .

Suppose  $a^k \equiv b^k \pmod{p}$ .

$\therefore \text{ind } a^k = \text{ind } b^k$ , so

$$k(\text{ind } a) \equiv k(\text{ind } b) \pmod{p-1}$$

Since  $\gcd(k, p-1) = 1$ , Then

$$\text{ind } a \equiv \text{ind } b \pmod{p-1}$$

By def.,  $1 \leq \text{ind } a \leq p-1$ ,  $1 \leq \text{ind } b \leq p-1$ .  
 $\therefore \text{ind } a = \text{ind } b$

If  $r$  is a prim. root of  $p$ , Then  
 $r^{\text{ind } a} = r^{\text{ind } b}$ . But by def.,

$$a \equiv r^{\text{ind } a} \pmod{p}, b \equiv r^{\text{ind } b} \pmod{p}$$

$$\therefore a \equiv b \pmod{p} \Rightarrow a = b \text{ a}$$

contradiction.

$\therefore a \not\equiv b \pmod{p}$ , so each of the  $p-1$  integers

$1^k, 2^k, \dots, (p-1)^k$  is incongruent to  
the other mod  $p$ .

$\therefore 1^k, 2^k, \dots, (p-1)^k$  form a complete set  
of residues mod  $p$ .

Now need to prove  $\gcd(a^k, p-1) = 1$   
for  $1 \leq a \leq p-1$ .

Consider  $x^k \equiv a \pmod{p}$ .

Clearly  $\gcd(a, p) = 1$ .

Since  $\gcd(k, p-1) = 1$ , Then by  
Th. 8.12, since  $a^{p-1} \equiv 1 \pmod{p}$

by Fermat's Th., Then  $x^k \equiv a \pmod{p}$   
has exactly  $\gcd(x, p-1) = 1$

solution mod  $p$ .

$\therefore$  The solution  $x$  must be among  $1, 2, \dots, p-1$  since the solution is mod  $p$ .

$\therefore$  since  $\gcd(a, p) = 1$ , then  $\gcd(x^k, p) = 1$  as  $x^k \equiv a$  (and using prob. #3, sec. 4.2).

$\therefore$  each of  $1^k, 2^k, \dots, (p-1)^k$  is relatively prime to  $p$ .

$\therefore 1^k, 2^k, \dots, (p-1)^k$  forms a reduced set of residues mod  $p$ .

14. Let  $r$  be a prim. root of the odd prime  $p$ , and let  $d = \gcd(k, p-1)$ . Prove that the values of  $a$  for which the congruence  $x^k \equiv a \pmod{p}$  is solvable are  $r^d, r^{2d}, \dots, r^{\lfloor (p-1)/d \rfloor d}$ .

Pf: (1) Let  $s = 1, 2, \dots, \frac{p-1}{d}$ , let  $a = r^{sd}$

Since  $(r^{sd})^{\frac{\phi(p)}{d}} = (r^{\phi(p)})^s \equiv 1^s = 1 \pmod{p}$ ,

as  $r$  is a prim. root, Then by

Th. 8.12,  $x^k \equiv a \pmod{p}$  has a solution when  $a = r^d, r^{2d}, \dots, r^{\lfloor (p-1)/d \rfloor d}$ , or  $a = r^d, r^{2d}, \dots, r^{p-1}$

(2) If  $x^k \equiv a \pmod{p}$  has a solution, Then, if  $r$  is a prim. root of  $p$ ,

$$\text{ind}_r x^k = \text{ind}_r a, \text{ so } k \text{ ind}_r x \equiv \text{ind}_r a \pmod{p-1}$$

Let  $d = \gcd(k, p-1)$ . Note  $1 \leq d \leq p-1$

$\therefore$  By Th. 4.7,  $d \mid \text{ind}_r a$ . By def.,  $1 \leq \text{ind}_r a \leq p-1$

Let  $m \in \mathbb{Z}$  s.t.  $dm = \text{ind}_r a$ . By def.,  
 $r^{dm} \equiv a \pmod{p}$

Since  $1 \leq d \leq p-1$  and  $1 \leq \text{ind}_r a \leq p-1$ , Then  
it must be true that  $1 \leq m \leq p-1$ .

$\therefore$  (1) shows That when  $a = r^d, r^{2d}, \dots, r^{p-1}$ , Then  
 $x^k \equiv a \pmod{p}$  is solvable, and

(2) shows That if  $x^k \equiv a \pmod{p}$  is solvable,  
a must be congruent mod  $p$  to  $r^{dm}$ ,  
where  $m = 1, 2, \dots, p-1$ .

$\therefore a = r^d, r^{2d}, \dots, r^{p-1}$  are all the values  
 $\pmod{p}$ , for which  $x^k \equiv a \pmod{p}$  is solvable.

15. If  $r$  is a prim. root of the odd prime  $p$ , show that

$$\text{ind}_r(p-a) \equiv \text{ind}_r a + \frac{(p-1)}{2} \pmod{p-1}$$

and consequently, That only half of an index table need be calculated to complete the table.

Pf: By def.,  $r^{\text{ind}_r(p-a)} \equiv p-a \equiv (-a) \pmod{p}$

$$\therefore \text{ind}_r r^{\text{ind}_r(p-a)} = \text{ind}_r (-a). \text{ Since } \text{ind}_r r = 1,$$

$$\begin{aligned} \text{ind}_r(p-a) &\equiv \text{ind}_r(-a) \\ &\equiv \text{ind}_r(-1) + \text{ind}_r(a) \pmod{p-1} \end{aligned}$$

By prob. #7,  $\text{ind}_r(-1) = \frac{1}{2}(p-1)$ .

$$\therefore \text{ind}_r(p-a) = \frac{1}{2}(p-1) + \text{ind}_r a \pmod{p-1}$$

16.(a) Let  $r$  be a prim. root of the odd prime  $p$ .

Establish that the exponential congruence

$$a^x \equiv b \pmod{p} \text{ has a solution} \iff$$

$d \mid \text{ind}_r b$ , where  $d = \gcd(\text{ind}_r a, p-1)$ ; in this case, There are  $d$  incongruent solutions mod  $p-1$ .

Pf:  $a^x \equiv b \pmod{p} \Leftrightarrow$

$$x \text{ ind}_p a \equiv \text{ind}_p b \pmod{p-1} \quad [1]$$

By Th. 4.7, [1] has a solution  $\Leftrightarrow$

$$\gcd(\text{ind}_p a, p-1) = d \mid \text{ind}_p b, \text{ in which}$$

case There are  $d$  incongruent solutions,  
 $\pmod{p-1}$ .

(5) Solve the exponential congruences

$$4^x \equiv 13 \pmod{17} \text{ and } 5^x \equiv 4 \pmod{19}$$

(1)  $4^x \equiv 13 \pmod{17}$  3 is a prim. root of 17

$$x \text{ ind}_3 4 \equiv \text{ind}_3 13 \pmod{16}$$

From table in prob. #3,  $\text{ind}_3 4 = 12$ ,  
 $\text{ind}_3 13 = 4$

$$\therefore 12x \equiv 4 \pmod{16} \quad \gcd(12, 16) = 4$$

4/4, so 4 incongruent solutions mod 16

$$\therefore 3x \equiv 1 \pmod{4}, 9x \equiv 3, x \equiv 3 \pmod{4}$$

$$\therefore \underline{x \equiv 3, 7, 11, 15 \pmod{16}}$$

(2)  $5^x \equiv 4 \pmod{19}$  2 is a prim. root of 19

$$\therefore x \text{ ind}_2 5 \equiv \text{ind}_2 4 \pmod{18}$$

Develop table of indices for 19 relative to 2

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
$\text{ind}_2 a$	18	1	13	2	16	14	6	3	8	17	12	15	5	7	11	4	10	9

$$\therefore \text{ind}_2 5 = 16, \text{ind}_2 4 = 2$$

$$\therefore 16x \equiv 2 \pmod{18}, \gcd(16, 18) = 2$$

$\therefore$  2 incongruent solutions mod 18

$$\therefore 8x \equiv 1 \pmod{9}, -8x \equiv -1, x \equiv -1 \equiv 8$$

$$\therefore \underline{x \equiv 8, 17 \pmod{18}}$$

17. For which values of b is the exponential congruence  $9^x \equiv b \pmod{13}$  solvable.

2 is a prim. root of 13. Use table on p. 175

$$\therefore x \text{ ind}_2 9 \equiv \text{ind}_2 5 \pmod{12}$$

$$\text{ind}_2 g = 8.$$

$$\therefore 8x \equiv \text{ind}_2 6 \pmod{12} \quad \gcd(8, 12) = 4$$

$$\therefore 4 \mid \text{ind}_2 6, \text{ so } \text{ind}_2 6 = 4, 8, 12$$

$$\therefore \delta (\text{using } \text{factc}) = 3, 9, 1$$

$$\therefore 6 \equiv 1, 3, 9 \pmod{13}$$

## 9.1 Euler's Criterion

Note Title

5/10/2006

1. Solve the following quadratic congruences.

$$(a) x^2 + 7x + 10 \equiv 0 \pmod{11}$$

$$\text{Let } y = 2ax + b = 2x + 7, d = b^2 - 4ac = 9$$

$$\therefore y^2 \equiv 9 \pmod{11}, \therefore y \equiv 3, 8 (= 11-3)$$

$$\therefore 2x + 7 \equiv 3 \pmod{11} \quad 2x + 7 \equiv 8 \pmod{11}$$

$$2x \equiv -4$$

$$2x \equiv 1, 10x \equiv 5$$

$$x \equiv -2 \equiv 9$$

$$-x \equiv 5, x \equiv -5 \equiv 6$$

$$\therefore x \equiv 6, 9 \pmod{11}$$

$$(b) 3x^2 + 9x + 7 \equiv 0 \pmod{13}$$

$$y = 2ax + b = 6x + 9, d = b^2 - 4ac = -3$$

$$\therefore y^2 \equiv -3 \equiv 10 \equiv 10 + 2 \cdot 13 = 36 \pmod{13}$$

$$\therefore y \equiv 6, 7 (= 13-6)$$

$$\therefore 6x + 9 \equiv 6 \pmod{13}$$

$$6x + 9 \equiv 7 \pmod{13}$$

$$6x \equiv -3 \equiv 36$$

$$6x \equiv -2, 12x \equiv -4$$

$$x \equiv 6$$

$$-x \equiv -4, x \equiv 4$$

$$\therefore x \equiv 4, 6 \pmod{13}$$

$$(c) 5x^2 + 6x + 1 \equiv 0 \pmod{23}$$

$$y = 2ax + b = 10x + 6, d = b^2 - 4ac = 16$$

$$\therefore y^2 \equiv 16 \pmod{23}, y \equiv 4, 19 (= 23 - 4)$$

$$\therefore 10x + 6 \equiv 4 \pmod{23}$$

$$10x \equiv -2, 20x \equiv -4$$

$$-3x \equiv -4, -24x \equiv -32$$

$$-x \equiv -32, x \equiv 9$$

$$10x + 6 \equiv 19 \pmod{23}$$

$$10x \equiv 13, 20x \equiv 26$$

$$-3x \equiv 3, x \equiv -1$$

$$x \equiv 22$$

$$\therefore x \equiv 9, 22 \pmod{23}$$

2. Prove that the quadratic congruence,  
 $6x^2 + 5x + 1 \equiv 0 \pmod{p}$  has a solution for  
every prime  $p$ , even though  $6x^2 + 5x + 1 = 0$   
has no solution in integers.

$$\text{Pf: } 6x^2 + 5x + 1 = 0, \quad \frac{-5 \pm \sqrt{25 - 24}}{12} = \frac{-5 \pm 1}{12}$$

$$\therefore x = -\frac{1}{2}, -\frac{1}{3}$$

$$6x^2 + 5x + 1 = (3x+1)(2x+1) \equiv 0 \pmod{p}$$

$$\therefore 3x+1 \equiv 0 \pmod{p} \text{ or } (2x+1) \equiv 0 \pmod{p}$$

(1) If  $p$  is odd, Then choose  $x$  s.t.  $2x+1=p$

$$\therefore 2x+1 \equiv 0 \pmod{p} \Rightarrow 6x^2+5x+1 \equiv 0 \pmod{p}$$

(2) If  $p=2$ , then  $3x+1 \equiv 0 \pmod{2}$

$$3x \equiv -1 \equiv 1, \quad x \equiv 1$$

$$\begin{aligned} \therefore x \equiv 1 \pmod{2} &\Rightarrow 3x \equiv 3, \quad 3x+1 \equiv 4 \equiv 0 \pmod{2} \\ &\Rightarrow 6x^2+5x+1 \equiv 0 \pmod{2} \end{aligned}$$

$\therefore$  There is a solution to  $6x^2+5x+1 \equiv 0 \pmod{p}$  for all prime  $p$ .

3. (a) For an odd prime  $p$ , prove that the quadratic residues of  $p$  are congruent mod  $p$  to the integers  $1^2, 2^2, \dots, \left(\frac{p-1}{2}\right)^2$

Proof: (1) For  $a = 1^2, 2^2, \dots, \left(\frac{p-1}{2}\right)^2$ ,

$$a^{\frac{p-1}{2}} = 1^{\frac{p-1}{2}}, 2^{\frac{p-1}{2}}, \dots, \left(\frac{p-1}{2}\right)^{\frac{p-1}{2}}$$

But for  $b = 1, 2, \dots, \frac{p-1}{2}$ ,  $\gcd(b, p) = 1$  as  $1 \leq b < p-1$  and  $p$  is prime.

By Fermat's Th.,  $b^{p-1} \equiv 1 \pmod{p}$

$$\therefore a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$$

$\therefore$  By Euler's Criterion,  $1^2, 2^2, \dots, \left(\frac{p-1}{2}\right)^2$  are quadratic residues of  $p$ .

(2)  $1^2, 2^2, \dots, \left(\frac{p-1}{2}\right)^2$  are incongruent mod  $p$

For if  $a^2 \equiv b^2 \pmod{p}$ ,  $1 \leq a, b \leq \frac{p-1}{2}, a \neq b$ ,

Then  $a^2 - b^2 \equiv 0 \Leftrightarrow (a-b)(a+b) \equiv 0 \pmod{p}$

But  $a+b \leq \frac{p-1}{2} + \frac{p-1}{2} = p-1$

$\therefore \gcd(a+b, p) = 1$ , so can divide by  $a+b$ .

$\therefore a-b \equiv 0 \pmod{p} \Rightarrow a \equiv b \Rightarrow a = b$ ,  
a contradiction.

(3) Let  $a$  be any quadratic residue of  $p$ .

$\therefore x^2 \equiv a \pmod{p}$  has a solution.

Let it be  $x_0$ . S.t.  $1 \leq x_0 \leq p-1$ .

$\therefore p-x_0$  is also a solution.

One of  $x_0, p-x_0$  must be  $\leq \frac{p-1}{2}$ .

For if  $x_0 > \frac{p-1}{2}$ , then  $-x_0 < -\frac{p-1}{2}$ ,

$$\text{so } p-x_0 < p - \frac{p-1}{2} = \frac{p-1}{2}$$

$\therefore$  One of  $x_0^2$  or  $(p-x_0)^2$  is equal  
to  $1^2, 2^2, \dots, \left(\frac{p-1}{2}\right)^2$

Since  $x_0^2 \equiv (p-x_0)^2 \equiv a$ , Then  $a$  must be

congruent to one of  $1^2, 2^2, \dots, \left(\frac{p-1}{2}\right)^2$

(6) Verify That The quadratic residues of 17  
are  $1, 2, 4, 8, 9, 13, 15, 16$ .

$$\text{By 6), } \begin{array}{ll} 1^2 \equiv 1 & 5^2 \equiv 25 \equiv 8 \\ 2^2 \equiv 4 & 6^2 \equiv 36 \equiv 2 \\ 3^2 \equiv 9 & 7^2 \equiv 49 \equiv 15 \\ 4^2 \equiv 16 & 8^2 \equiv 64 \equiv 13 \end{array}$$

4. Show That 3 is a quadratic residue of 23,  
but a nonresidue of 31.

$$\begin{aligned} 3^{\frac{23-1}{2}} &= 3^{11} = 3^2 (3^3)^3 = 9 (27)^3 \equiv 9 \cdot (4)^3 \pmod{23} \\ &\equiv 9 \cdot 64 \equiv 9(-5) \equiv -45 + 46 \equiv 1. \end{aligned}$$

$\therefore 3^{\frac{23-1}{2}} \equiv 1 \pmod{23} \Rightarrow 3 \text{ a quadratic residue of 23}$

$$\begin{aligned} 3^{\frac{31-1}{2}} &= 3^{15} = (3^3)^5 = 27^5 \equiv (-4)^5 \pmod{31} \\ &\equiv -4^3 \cdot 4^2 \equiv (-64)(16) \equiv (-64 + 62)(16) \equiv -32 \equiv -1 \end{aligned}$$

$\therefore 3^{\frac{31-1}{2}} \equiv -1 \pmod{31} \Rightarrow 3 \text{ a quadratic nonresidue of 31.}$

5. Given that  $a$  is a quadratic residue of odd prime  $p$ , prove the following

(a)  $a$  is not a primitive root of  $p$

Pf: If  $a$  were a primitive root of  $p$ , then  $a^n \not\equiv 1 \pmod{p}$  for  $1 \leq n < p-1$ , by def.

But by Euler's criterion,  $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$   
 $p$  is odd so  $\frac{p-1}{2}$  is an integer, and  
 $1 \leq \frac{p-1}{2} < p-1$ , which contradicts the above.

(b) The integer  $p-a$  is a quadratic residue or nonresidue of  $p$  according as  $p \equiv 1 \pmod{4}$  or  $p \equiv 3 \pmod{4}$

Pf: Consider  $x^2 \equiv p-a \pmod{p}$ . This is equivalent to  $x^2 \equiv -a \pmod{p}$ .

$\therefore -a$  (or  $p-a$ ) is a quadratic residue or nonresidue according to whether

$(-a)^{\frac{p-1}{2}} \equiv 1 \pmod{p}$  or  $(-a)^{\frac{p-1}{2}} \equiv -1 \pmod{p}$ ,

Since  $a$  is a quadratic residue,

Then  $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ .

$$\text{But } (-a)^{\frac{p-1}{2}} = (-1)^{\frac{p-1}{2}} a^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} \pmod{p}.$$

$\therefore p-a$  is a quadratic residue or nonresidue according to whether  $(-1)^{\frac{p-1}{2}}$  is 1 or -1, and this according to whether  $\frac{p-1}{2}$  is even or odd.

$$\frac{p-1}{2} \text{ is even} \Leftrightarrow \frac{p-1}{2} = 2k, \text{ some } k,$$

$$\Leftrightarrow p-1 = 4k$$

$$\Leftrightarrow p \equiv 1 \pmod{4}$$

$$\frac{p-1}{2} \text{ is odd} \Leftrightarrow \frac{p-1}{2} = 2k+1, \text{ some } k$$

$$\Leftrightarrow p-1 = 4k+2$$

$$\Leftrightarrow p = 3 + 4k$$

$$\Leftrightarrow p \equiv 3 \pmod{4}$$

$\therefore p-a$  is a quadratic residue or nonresidue according to whether  $p \equiv 1 \pmod{4}$  or  $p \equiv 3 \pmod{4}$

(c) If  $p \equiv 3 \pmod{4}$ , Then  $x \equiv \pm a^{\frac{p+1}{4}} \pmod{p}$  are the solutions of the congruence  $x^2 \equiv a \pmod{p}$ .

$$\text{Pf: } x \equiv \pm a^{\frac{p+1}{4}} \Rightarrow x^2 \equiv a^{\frac{p+1}{2}} = a^{\frac{p-1+2}{2}} = a^{\frac{p-1}{2}} \cdot a$$

Since  $a$  is a quadratic residue,  $a^{\frac{p-1}{2}} \equiv 1$

$$\therefore a^{\frac{p-1}{2}} \cdot a \equiv a.$$

$\therefore x^2 \equiv a \pmod{p}$  when  $x \equiv \pm a^{\frac{p+1}{4}}$

$\frac{p+1}{4}$  is an integer when  $\frac{p+1}{4} = k$ , some  $k$ ,  
 $\therefore p+1 = 4k$ ,  $p = -1 + 4k$ ,  $p \equiv -1 \pmod{4}$ ,  
or  $p \equiv 3 \pmod{4}$ .

Also, by Lagrange's Th. (Th. 8.5),  
there are at most 2 solutions, so

$x \equiv \pm a^{\frac{p+1}{4}}$  are the exact solutions.

6. Let  $p$  be an odd prime and  $\gcd(a, p) = 1$ . Establish  
that the quadratic congruence  $ax^2 + bx + c \equiv 0 \pmod{p}$   
is solvable  $\Leftrightarrow b^2 - 4ac$  is zero or a quadratic  
residue of  $p$ .

Pf: Since  $\gcd(a, p) = 1$  and  $p$  is an odd prime,  
 $\gcd(4a, p) = 1$ .

$\therefore$  Solutions to

$$4a(ax^2 + bx + c) \equiv 0 \pmod{p} \quad [1]$$

are equivalent to

$$ax^2 + bx + c \equiv 0 \pmod{p} \quad [2]$$

since you can divide [1] by  $4a$  to  
get [2]

$$\begin{aligned} \text{But } 4a(ax^2 + bx + c) &= 4a^2x^2 + 4abx + 4ac \\ &= (2ax + b)^2 - b^2 + 4ac \\ &= (2ax + b)^2 - (b^2 - 4ac) \end{aligned}$$

$\therefore$  Solutions to

$$ax^2 + bx + c \equiv 0 \pmod{p} \quad [2]$$

are equivalent to

$$(2ax + b)^2 \equiv b^2 - 4ac \pmod{p} \quad [3]$$

(a) Suppose  $b^2 - 4ac \equiv 0 \pmod{p}$

$\therefore$  Solutions to [2] are equivalent to

$$(2ax + b)^2 \equiv 0 \pmod{p}$$

which is equivalent to

$$2ax \equiv -b \pmod{p}$$

Since  $\gcd(2a, p) = 1$ , this has a unique solution mod  $p$  (Th. 4?).

$$\begin{aligned} \therefore ax^2 + bx + c \equiv 0 \pmod{p} \text{ is solvable} &\Leftrightarrow \\ b^2 - 4ac \equiv 0 \pmod{p} \end{aligned}$$

(5)  $b^2 - 4ac \not\equiv 0 \pmod{p}$  and is a quadratic residue of  $p$ .

$\therefore y^2 \equiv b^2 - 4ac \pmod{p}$  has a solution by definition.

Let  $y_1$  be s.t.  $y_1^2 \equiv b^2 - 4ac \pmod{p}$ ,  $1 \leq y_1 \leq p-1$ .

$\therefore p-y_1$  is also a solution.

By Lagrange Th., these are the only solutions. They are also incongruent.

For if  $y_1 \equiv p-y_1 \pmod{p}$ , then

$2y_1 \equiv p \equiv 0 \pmod{p} \Leftrightarrow y_1 \equiv 0 \pmod{p}$  as  $\gcd(p, 2) = 1$ .  $\therefore b^2 - 4ac \equiv 0$ , a contradiction

Letting  $y_1 = 2ax+b$ , then

$y^2 \equiv b^2 - 4ac \pmod{p}$  is equivalent to

$2ax+b \equiv b^2 - 4ac \pmod{p}$  and  
 $p - (2ax+b) \equiv b^2 - 4ac \pmod{p}$ , or

$$2ax \equiv b^2 - 4ac - b \pmod{p} \quad [4]$$

and

$$2ax \equiv 4ac - b^2 - b \pmod{p} \quad [5]$$

Since  $\gcd(2a, p) = 1$ , by Th. 4.7,  
 [4] and [5] have unique solutions.

$\therefore$  Assuming  $b^2 - 4ac \not\equiv 0 \pmod{p}$ ,

$b^2 - 4ac$  a quadratic residue of  $p$

$\Leftrightarrow (2ax + b)^2 \equiv b^2 - 4ac \pmod{p}$  is solvable,

$\Leftrightarrow ax^2 + bx + c \equiv 0 \pmod{p}$  is solvable.

7. If  $p = 2^k + 1$  is prime, verify that every quadratic nonresidue of  $p$  is a primitive root of  $p$ .

Pf: Let  $a$  be a quadratic nonresidue of  $p$ .

$\therefore$  By Euler's criterion,  $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$

Since  $2^k + 1$  is prime,  $k \geq 1$ .  $p-1 = 2^k$ ,  
 $\therefore \frac{p-1}{2} = 2^{k-1}$

$\therefore a^{2^{k-1}} \equiv -1 \pmod{p}$ . [1]

$$\therefore (a^{2^{k-1}})^2 = a^{2^k} \equiv 1 \pmod{p}, \text{ and}$$

$$\phi(p) = p-1 = 2^k.$$

Let  $n$  be order of  $a \pmod{p}$ .  $\therefore n \mid 2^k$   
By Th. 8.1.

$\therefore$  if  $n \neq 2^k$ , Then  $n = 2^r$ ,  $r < k$

$$\therefore a^{2^r} \equiv 1 \pmod{p} \quad [2]$$

If  $r = k-1$ , Then a contradiction is reached by  $\Sigma 1$ .

If  $r < k-1$ , Then square  $\Sigma 2$   
 $k-1-r$  times.

$$\therefore (a^{2^r})^2 = a^{2 \cdot 2^r} = a^{2^{r+1}} \equiv 1 \pmod{p}$$

$$(a^{2^{r+1}})^2 = a^{2 \cdot 2^{r+1}} = a^{2^{r+2}} \equiv 1 \pmod{p}$$

$$\vdots$$

$$(a^{2^{k-2}})^2 = a^{2 \cdot 2^{k-2}} = a^{2^{k-1}} \equiv 1 \pmod{p}$$

$\therefore$  again, a contradiction is reached  
by  $\Sigma 1$

$\therefore n = 2^k$ , so order of  $a$  is  $p-1 = \phi(p)$

8. Assume  $r$  is a primitive root of prime  $p$ , where  $p \equiv 1 \pmod{8}$ .

(a) Show that the solutions of the quadratic congruence  $x^2 \equiv 2 \pmod{p}$  are given by

$$x \equiv \pm (r^{7(p-1)/8} + r^{(p-1)/8}) \pmod{p}$$

Pf: Since  $r$  is a prim. root of  $p$ ,  $r^{p-1} \equiv 1 \pmod{p}$   
 But  $p-1 = 8k$ , some  $k$ , or  $\frac{p-1}{8} = k$ , an integer.

$$\text{Let } x \equiv \pm (r^{7(p-1)/8} + r^{(p-1)/8}) \pmod{p}$$

$$\therefore x^2 \equiv (r^{7(p-1)/8} + r^{(p-1)/8})^2 \pmod{p}$$

$$= r^{14(p-1)/8} + r^{2(p-1)/8} + 2r^{p-1}$$

$$\equiv r^{14(p-1)/8} + r^{2(p-1)/8} + 2 \pmod{p}$$

$\therefore$  Need to show  $r^{14(p-1)/8} + r^{2(p-1)/8} \equiv 0 \pmod{p}$   
 to show  $x^2 \equiv 2 \pmod{p}$ .

$$r^{14(p-1)/8} + r^{2(p-1)/8} = r^{2(p-1)/8}(r^{12(p-1)/8} + 1)$$

But  $\gcd(r, p) = 1$ , so  $\gcd(r^{2(p-1)/8}, p) = 1$

$\therefore$  If can show  $r^{12(\rho-1)/8} \equiv -1 \pmod{\rho}$ ,

Then  $x^2 \equiv 2 \pmod{\rho}$ .

$$r^{12(\rho-1)/8} = r^{8(\rho-1)/8} \cdot r^{4(\rho-1)/8}$$

$$= r^{\rho-1} \cdot r^{4(\rho-1)/8}$$

$$\equiv r^{4(\rho-1)/8} = r^{\frac{\rho-1}{2}}$$

Since  $(r^{\frac{\rho-1}{2}} + 1)(r^{\frac{\rho-1}{2}} - 1) = r^{\rho-1} - 1 \equiv 0 \pmod{\rho}$

Then  $r^{\frac{\rho-1}{2}} \equiv -1$  or  $r^{\frac{\rho-1}{2}} \equiv 1 \pmod{\rho}$ , but  
not both, since otherwise  $-1 \equiv 1 \pmod{\rho}$ ,  
so  $\rho \equiv 2$ , a contradiction to  
 $\rho \equiv 1 \pmod{8}$ .

But  $r^{\frac{\rho-1}{2}} \neq 1$  since  $r$  is a  
primitive root (order of  $r = \rho-1$ ).

$\therefore r^{\frac{\rho-1}{2}} \equiv -1 \pmod{\rho}$

$\therefore r^{12(\rho-1)/8} \equiv -1 \pmod{\rho}$

$\therefore$  if  $x \equiv \pm(r^{7(\rho-1)/8} + r^{(\rho-1)/8}) \pmod{\rho}$ ,

Then  $x^2 \equiv 2 \pmod{p}$ , and  
 Lagrange's Th. shows there are no  
 more solutions.

(6) Use part (a) to find all solutions to the  
 two congruences  $x^2 \equiv 2 \pmod{17}$  and  
 $x^2 \equiv 2 \pmod{41}$

$$(1) \quad x^2 \equiv 2 \pmod{17}$$

3 is a primitive root of 17

$$\therefore x \equiv \pm (3^{7(17-1)/8} + 3^{(17-1)/8}) \pmod{17}$$

$$= \pm (3^{14} + 3^2) \pmod{17}$$

$$= \pm 3^2(3^{12} + 1) = \pm 9(3^{12} + 1)$$

$$3^2 \equiv 9, \quad 3^4 \equiv -4, \quad 3^8 \equiv 16 \equiv -1, \quad 3^{12} \equiv 4$$

$$\therefore x \equiv \pm 9(4+1) = \pm 45 \equiv 6, \underline{11} \pmod{17}$$

$$(2) \quad x^2 \equiv 2 \pmod{41}$$

6 is a prim. root of 41 (table p. 166)

$$\therefore x \equiv \pm (6^{(41-1)/8} + 6^{(41-1)/8}) \pmod{41}$$

$$= \pm (6^{35} + 6^5) = \pm 6^5 (6^{30} + 1)$$

$$\begin{aligned} 6^2 &= 36 \equiv -5, \quad 6^3 = -30 \equiv 11, \quad 6^4 \equiv 66 \equiv 25 \equiv -16 \\ 6^5 &\equiv -96 \equiv -14, \quad 6^6 \equiv -84 \equiv -2 \\ \therefore 6^{30} &\equiv (-2)^5 \equiv -32 \equiv 9 \end{aligned}$$

$$\therefore x \equiv \pm 14(9+1) = \pm 140 \equiv \pm 17 = 17, 24$$

$$\therefore x \equiv 17, 24 \pmod{41}$$

9. (a) If  $ab \equiv r \pmod{p}$ , where  $r$  is a quadratic residue of the odd prime  $p$ , prove that  $a$  and  $b$  are both quadratic residues of  $p$  or both nonresidues of  $p$ .

Pf: Since  $\gcd(r, p) = 1$ , Then  $\gcd(ab, p) = 1$ ,  
 $\therefore \gcd(a, p) = 1$  and  $\gcd(b, p) = 1$ .

Suppose  $a$  is a quadratic residue and  $b$  a nonresidue.

$$\therefore a^{\frac{p-1}{2}} \equiv 1, \quad b^{\frac{p-1}{2}} \equiv -1 \pmod{p}$$

$$\therefore r^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} \cdot b^{\frac{p-1}{2}} \equiv -1 \pmod{p},$$

which makes  $r$  a nonresidue by corollary to Euler's criterion.

$$\therefore a^{\frac{p-1}{2}} \equiv b^{\frac{p-1}{2}} \equiv 1 \text{ or } a^{\frac{p-1}{2}} \equiv b^{\frac{p-1}{2}} \equiv -1 \pmod{p}$$

(6) If  $a$  and  $b$  are both quadratic residues of the odd prime  $p$  or both nonresidues of  $p$ , show that the congruence  $ax^2 \equiv b \pmod{p}$  has a solution.

Pf: Assume  $\gcd(a, p) = \gcd(b, p) = 1$ .

$\therefore ax^2 \equiv b \pmod{p}$   
is equivalent to,

$$a^2x^2 \equiv ab \pmod{p}, \text{ or}$$

$$(ax)^2 \equiv ab \pmod{p}.$$

$\therefore ax^2 \equiv b \pmod{p}$  has a solution  $\Leftrightarrow$   
 $ab$  is a quadratic residue.

By (a)  $ab$  is a quadratic residue  $\Leftrightarrow$   
 $a, b$  are both quadratic residues or

both nonresidues.

$\therefore ax^2 \equiv b \pmod{p}$  has a solution  $\Leftrightarrow$   
 $a, b$  are both quadratic residues or  
both nonresidues.

10. Let  $p$  be an odd prime and  $\gcd(a, p) = \gcd(b, p) = 1$ .  
Prove that either all three of the quadratic congruences  $x^2 \equiv a \pmod{p}$ ,  $x^2 \equiv b \pmod{p}$ ,  $x^2 \equiv ab \pmod{p}$  are solvable or exactly one of them admits a solution.

Pf: Suppose more than one congruence admits a solution.

(1) Assume  $x^2 \equiv a \pmod{p}$ ,  $x^2 \equiv b \pmod{p}$  are solvable.  
By Euler's criterion,  $a^{\frac{p-1}{2}} \equiv b^{\frac{p-1}{2}} \equiv 1 \pmod{p}$   
 $\therefore a^{\frac{p-1}{2}} \cdot b^{\frac{p-1}{2}} \equiv (ab)^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ ,  
and so  $x^2 \equiv ab \pmod{p}$  is solvable.

(2) Assume  $x^2 \equiv a \pmod{p}$ ,  $x^2 \equiv ab \pmod{p}$  are solvable (case of  $x^2 \equiv b$  and  $x^2 \equiv ab$  is analogous).

$\therefore$  By Euler's criterion,  $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$

and  $(ab)^{\frac{p-1}{2}} = a^{\frac{p-1}{2}} \cdot b^{\frac{p-1}{2}} \equiv 1 \pmod{p}$  [1]

Since  $\gcd(a, p) = 1$ , Then  $\gcd(a^{\frac{p-1}{2}}, p) = 1$

$\therefore$  Dividing by [1] by  $a^{\frac{p-1}{2}}$ , we get

$$b^{\frac{p-1}{2}} \equiv 1 \pmod{p}.$$

$\therefore$  By Euler's criterion,  $x^2 \equiv 5 \pmod{p}$  is solvable.

11. (a) Knowing 2 is a primitive root of 19, find all the quadratic residues of 19.

Proof to Th. 9.1 shows that if a is a quadratic residue, Then if r is a prim. root of 19, Then  $r^k \equiv a \pmod{p}$ ,  $1 \leq k \leq p-1$ , and k is even.

$\therefore$  Look at all  $2^k$  for k even and  $1 \leq k \leq 18$

$$\therefore 2^2 \equiv 4 \quad 2^8 \equiv 4 \cdot 7 \equiv 9 \quad 2^{14} \equiv -32 \equiv 6$$

$$2^4 \equiv 16 \quad 2^{10} \equiv 4 \cdot 9 \equiv -2 \equiv 17 \quad 2^{16} \equiv 24 \equiv 5$$

$$2^6 \equiv 64 \equiv 7 \quad 2^{12} \equiv -8 \equiv 11 \quad 2^{18} \equiv 20 \equiv 1$$

$$\therefore 1, 4, 5, 6, 7, 9, 11, 16, 17$$

(b) Find the quadratic residues of 29 and 31

Can use method in (a), or easier, method in Example 8.1

$$\begin{array}{ll}
 29: & \begin{array}{l} 1^2 \equiv 28^2 \equiv 1 \\ 2^2 \equiv 27^2 \equiv 4 \\ 3^2 \equiv 26^2 \equiv 9 \\ 4^2 \equiv 25^2 \equiv 16 \\ 5^2 \equiv 24^2 \equiv 25 \\ 6^2 \equiv 23^2 \equiv 7 \\ 7^2 \equiv 22^2 \equiv 20 \end{array} & \begin{array}{l} 8^2 \equiv 21^2 \equiv 64 \equiv 6 \\ 9^2 \equiv 20^2 \equiv 81 \equiv 23 \\ 10^2 \equiv 19^2 \equiv 13 \\ 11^2 \equiv 18^2 \equiv 121 \equiv 5 \\ 12^2 \equiv 17^2 \equiv 144 \equiv -1 \equiv 28 \\ 13^2 \equiv 16^2 \equiv 169 \equiv 24 \\ 14^2 \equiv 15^2 \equiv 196 \equiv 51 \equiv -7 \equiv 22 \end{array}
 \end{array}$$

$$\therefore 1, 4, 5, 6, 7, 9, 13, 16, 20, 22, 23, 24, 25, 28$$

$$\begin{array}{ll}
 31: & \begin{array}{l} 1^2 \equiv 30^2 \equiv 1 \\ 2^2 \equiv 29^2 \equiv 4 \\ 3^2 \equiv 28^2 \equiv 9 \\ 4^2 \equiv 27^2 \equiv 16 \\ 5^2 \equiv 26^2 \equiv 25 \\ 6^2 \equiv 25^2 \equiv 5 \\ 7^2 \equiv 24^2 \equiv 18 \\ 8^2 \equiv 23^2 \equiv 2 \end{array} & \begin{array}{l} 9^2 \equiv 22^2 \equiv 81 \equiv 19 \\ 10^2 \equiv 21^2 \equiv 7 \\ 11^2 \equiv 20^2 \equiv -3 \equiv 28 \\ 12^2 \equiv 19^2 \equiv 20 \\ 13^2 \equiv 18^2 \equiv 169 \equiv 45 \equiv 14 \\ 14^2 \equiv 17^2 \equiv 196 \equiv 10 \\ 15^2 \equiv 16^2 \equiv 225 \equiv 8 \end{array}
 \end{array}$$

$$\therefore 1, 2, 4, 5, 7, 8, 9, 10, 14, 16, 18, 19, 20, 25, 28$$

12. If  $n > 2$  and  $\gcd(a, n) = 1$ , Then  $a$  is called a quadratic residue of  $n$  whenever There exists an integer  $x$  s.t.  $x^2 \equiv a \pmod{n}$ . Prove that if  $a$  is a quadratic residue of  $n > 2$ , Then  $a^{\phi(n)/2} \equiv 1 \pmod{n}$ .

Pf: Since  $\gcd(a, n) = 1$  and  $x^2 \equiv a \pmod{n}$ , then  $\gcd(x^2, n) = 1$ , and so  $\gcd(x, n) = 1$  (if  $x$  and  $n$  had a common divisor,  $d \geq 1$ , Then  $d|x \Rightarrow d|x^2$ ).

By Euler's Th.,  $x^{\phi(n)} \equiv 1 \pmod{n}$

$$\therefore a^{\phi(n)/2} \equiv (x^2)^{\phi(n)/2} = x^{\phi(n)} \equiv 1 \pmod{n}$$

13. Show that The result of The previous problem does not provide a sufficient condition for the existence of a quadratic residue of  $n$ ; i.e., find relatively prime integers  $a$  and  $n$ , with  $a^{\phi(n)/2} \equiv 1 \pmod{n}$ , for which The congruence  $x^2 \equiv a \pmod{n}$  is not solvable.

Intuition suggests, from section 8.3, that

if  $n$  is composite and doesn't have a prim. root,  
Then finding such an  $a$  will be easier.

$$\therefore \text{Let } n = 6 \pmod{6}, \begin{array}{ll} 1^2 \equiv 1 & 4^2 \equiv 4 \\ 2^2 \equiv 4 & 5^2 \equiv 1 \\ 3^2 \equiv 3 & \end{array}$$

$\therefore x^2 \equiv 5 \pmod{6}$  is not solvable  
 $\phi(6) = 2$ , however  $5 \not\equiv 1 \pmod{6}$

$$\text{Try } n = 8 \pmod{8}, \begin{array}{ll} 1^2 \equiv 1 & 4^2 \equiv 0 \\ 2^2 \equiv 4 & 5^2 \equiv 1 \\ 3^2 \equiv 1 & 6^2 \equiv 4 \end{array}$$

$\therefore x^2 \equiv 9 \pmod{8}$  not solvable if  $a = 3, 5, 7$

$$\phi(8) = 4 \quad \therefore \phi(8)/2 = 2$$

And,  $3^2 \equiv 5^2 \equiv 7^2 \equiv 1 \pmod{8}$ .

$\therefore \text{Let } n = 8, \underline{a = 3, 5, \text{ or } 7}$ .

## 9.1 The Legendre Symbol and Its Properties

Note Title

5/31/2006

1. Find the value of the following Legendre symbols:
- (a)  $(19/23)$

$$19 \equiv -4 \pmod{23}.$$

$$\begin{aligned}\therefore (19/23) &= (-4/23) = (-1 \cdot 2^2/23) = (-1/23) \\ &= (-1)^{(23-1)/2} = \underline{-1}\end{aligned}$$

(b)  $(-23/59)$

$$\begin{aligned}-23 &\equiv -23 + 59 \pmod{59} = 36 = 6^2 \\ \therefore (-23/59) &= (6^2/59) = \underline{1}\end{aligned}$$

(c)  $(20/31) = (2^2 \cdot 5/31) = (5/31)$   
 $5 \equiv 36 \pmod{31}$

$$\therefore (20/31) = (36/31) = (6^2/31) = \underline{1}$$

(d)  $(18/43) = (2 \cdot 3^2/43) = (2/43)$

$$43 = 5 \cdot 8 + 3, \text{ so by Th. 9.6, } (2/43) = \underline{-1}$$

(e)  $(-72/131) = (-3^2 \cdot 2^2 \cdot 2/131) = (-1/131)(2/131)$

$$(-1/131) = (-1)^{(131-1)/2} = -1 \quad . \quad \therefore (-72/131) = - (2/131)$$

$$131 = (16) \cdot 8 + 3, \text{ so by Th. 9.6, } (2/131) = -1$$

$$\therefore (-72/131) = (-1)(-1) = \underline{1}$$

2. Use Gauss' lemma to compute each of the Legendre symbols below (that is, in each case obtain the integer  $n$  for which  $(a/p) = (-1)^n$ ):

$$(a) (8/11)$$

$$(\rho-1)/2 = 5, \quad \rho/2 = 5.5$$

$$\therefore S = \{8, 16, 24, 32, 40\} = \{1 \cdot 8, 2 \cdot 8, \dots, 5 \cdot 8\} \\ \equiv \{8, 5, 2, 9, 7\} \pmod{11}$$

$$\therefore 8, 9, 7 > \rho/2, \text{ so } n = 3$$

$$\therefore (8/11) = (-1)^3 = -1$$

$$(b) (7/13) \quad (\rho-1)/2 = 6, \quad \rho/2 = 6.5$$

$$\therefore S = \{7, 14, 21, 28, 35, 42\}$$

$$\equiv \{7, 1, 8, 2, 9, 3\} \pmod{13}$$

$$\therefore 7, 8, 9 > \rho/2, \text{ so } n=3$$

$$\therefore (8/13) = (-1)^3 = -1$$

$$(c) (5/19) \quad (\rho-1)/2 = 9, \quad \rho/2 = 9.5$$

$$\therefore S = \{5, 10, 15, 20, 25, 30, 35, 40, 45\}$$

$$= \{5, 10, 15, 1, 6, 11, 16, 2, 7\} \pmod{19}$$

$$\therefore 10, 15, 11, 16 > 9.5, \text{ so } n=4$$

$$\therefore (-1)^4 = 1$$

$$(d) (11/23) \quad (\rho-1)/2 = 11, \quad \rho/2 = 11.5$$

$$\therefore S = \{11, 22, 33, 44, 55, 66, 77, 88, 99, 110, 121\}$$

$$= \{11, 22, 10, 21, 9, 20, 8, 19, 7, 18, 6\}$$

$$\therefore 22, 21, 20, 19, 18 > 11.5, \text{ so } n=5$$

$$\therefore (-1)^5 = -1$$

$$(e) (\mathbb{Z}, 31) \quad (\rho-1)/2 = 15, \quad \rho/2 = 15.5$$

$$\therefore S = \{6, 12, 18, 24, 30, 36, 42, 48, 54, 60, 66, 72, 78, 84, 90\}$$

$$= \{6, 12, 18, 24, 30, 5, 11, 17, 23, 29, 4, 10, 16, 22, 28\} \pmod{31}$$

$$\therefore 18, 24, 30, 17, 23, 29, 16, 22, 28 > 15.5, \text{ so } n = 9$$

$$\therefore (-1)^9 = -1$$

3. For an odd prime  $\rho$ , prove there are  $\frac{\rho-1}{2} - \phi(\rho-1)$  quadratic non-residues of  $\rho$  that are not primitive roots of  $\rho$ .

Pf: By Th. 9.4, There are  $\frac{\rho-1}{2}$  quadratic residues of  $\rho$  and  $\frac{\rho-1}{2}$  quadratic nonresidues of  $\rho$ .

If  $a$  is a quadratic residue of  $\rho$ , it cannot be a primitive root, because  $a^{(\rho-1)/2} \equiv 1 \pmod{\rho}$  by Th. 9.1, and  $\frac{\rho-1}{2} < \rho-1 = \phi(\rho)$ .

$\therefore$  if  $r$  is a primitive root of  $\rho$ , it must be congruent to a quadratic nonresidue of  $\rho$ .

Let  $S$  be the set of quadratic nonresidues of  $p$ . There are thus  $\frac{p-1}{2}$  elements of  $S$ .

$\therefore$  All the primitive roots of  $p$  are congruent to some of the  $\frac{p-1}{2}$  elements of  $S$ .

By the corollary to Th. 8.6 (p. 165), there are  $\phi(p-1)$  primitive roots of  $p$ , and so  $\phi(p-1)$  elements of  $S$  are primitive roots.

$\therefore \frac{p-1}{2} - \phi(p-1)$  elements of  $S$  are not primitive roots of  $p$ .

4. (a) Let  $p$  be an odd prime. Show that the Diophantine equation  $x^2 + py + a = 0$ ,  $\gcd(a, p) = 1$ , has an integral solution if and only if  $(-a/p) = 1$ .

(1) If  $x^2 + py + a = 0$  has a solution, then  $x^2 + a \equiv -y \pmod{p} \Rightarrow x^2 + a \equiv 0 \pmod{p} \Rightarrow x^2 \equiv -a \pmod{p} \Rightarrow (-a) \text{ is a quadratic residue of } p \Rightarrow (-a/p) = 1$ .

(2) If  $(-a/p) = 1$ , then  $(-a)$  is a quadratic residue of  $p \Rightarrow x^2 \equiv -a \pmod{p}$  has a

solution in  $x \Rightarrow$  There is an integer  $k$   
 s.t.  $x^2 = -a + kp$ , or  $x^2 + a - kp = 0$ , or  
 letting  $y = -k$ ,  $x^2 + py + a = 0$

(b) Determine whether  $x^2 + 7y - 2 = 0$  has a solution in integers.

$\gcd(-2, 7) = 1$ . By (a), since  $(2/7) = 1$  by Th. 9.6, Then there is a solution.

5. Prove that 2 is not a primitive root of any prime of the form  $p = 3 \cdot 2^n + 1$ , except when  $p = 13$ .

Pf: Strategy: show 2 is a quadratic residue of  $p$ , and so cannot be a primitive root.

For  $p-1 = 3 \cdot 2^n$ ,  $p-1 \equiv 0 \pmod{8}$  when  $n \geq 3$

$\therefore$  For  $n \geq 3$ ,  $p \equiv 1 \pmod{8}$ , so by Th. 9.6,  $(2/p) = 1$

$\therefore$  For  $n \geq 3$ , 2 is a quadratic residue

and  $\therefore$  not a primitive root.

$\therefore$  Consider  $n=1, 2$

$$n=1: p = 3 \cdot 2 + 1 = 7. \therefore p \equiv 7 \pmod{8}$$

$\therefore$  By Th. 9.6,  $(2/p) = 1$ , so 2 is a

quad. residue, and so 2 is not a  
prim. root.

$$n=2: p = 3 \cdot 2^2 + 1 = 13. \therefore p \equiv 5 \pmod{8}$$

$\therefore (2/p) = -1$ , so 2 is a  
quad. nonresidue, and 2 is a  
know primitive root of 13.

$\therefore$  For  $n \geq 1, n \neq 2$ , if  $p = 3 \cdot 2^n + 1$  is prim,  
Then 2 is not a primitive root of  $p$ .

C. (a) If  $p$  is an odd prime, and  $\gcd(ab, p) = 1$ , prove  
That at least one of  $a, b$ , or  $ab$  is a  
quadratic residue of  $p$ .

$$\text{Pf: } (ab/p) = (a/p)(b/p)$$

$(ab/p)$ ,  $(a/p)$ , and  $(b/p)$  are each equal to 1 or -1.

$\therefore$  if  $(ab/p) = 1$ , by def.,  $ab$  is a quadratic residue of  $p$ .

$\therefore$  Suppose  $(ab/p) = -1$ .

$$\therefore (a/p)(b/p) = -1.$$

$(a/p)$  and  $(b/p)$  cannot both be -1, since  $(-1) \cdot (-1) \neq -1$ .

$\therefore$  Either  $(a/p) = 1$  or  $(b/p) = 1$ .

$\therefore$  either  $a$  or  $b$  is a quadratic residue of  $p$ .

(5) Given a prime  $p$ , show that for some choice of  $n > 0$ ,  $p$  divides  $(n^2 - 2)(n^2 - 3)(n^2 - 6)$

$$\text{Pf: } p=2: \text{ Let } n=3. \text{ Then } (n^2 - 2)(n^2 - 3)(n^2 - 6) = (9-2)(9-3)(9-6) =$$

$$7 \cdot 6 \cdot 3$$

$$\therefore p | 7 \cdot 6 \cdot 3$$

$p = 3$ : Let  $n=3$ , as above,  $p \mid 7 \cdot 6 \cdot 3$

$p > 3$ :  $\therefore \gcd(2 \cdot 3, p) = 1$

$\therefore$  By (a), one of  $2, 3$ , or  $2 \cdot 3$  is a quadratic residue of  $p$ .

$\therefore$  By def., There must be an  $n$  s.t.  $n^2 \equiv 2 \pmod{p}$ , or  $n^2 \equiv 3 \pmod{p}$ , or  $n^2 \equiv 6 \pmod{p}$ .

$\therefore n^2 - 2 \equiv 0 \pmod{p}$ , or  $n^2 - 3 \equiv 0 \pmod{p}$ , or  $n^2 - 6 \equiv 0 \pmod{p}$ .

$\therefore (n^2 - 2)(n^2 - 3)(n^2 - 6) \equiv 0 \pmod{p}$ .

$\therefore$  There is an  $n$  s.t.  $p \mid (n^2 - 2)(n^2 - 3)(n^2 - 6)$

7. If  $p$  is an odd prime, show that

$$\sum_{a=1}^{p-2} (a(a+1)/p) = -1 \quad [(\ ) \text{ is Legendre symbol}]$$

Pf: Use the hint. Let  $a'$  be defined by

$aa' \equiv 1 \pmod{p}$ . Note that since  $\gcd(a, p) = 1$ ,  
 Then  $a'$  exists, by Th. 4.7, for each  $1 \leq a \leq p-2$ .

Note that as  $a$  runs from 1 to  $p-2$ ,  
 $a'$  also runs from 1 to  $p-2$  (not  $p-1$ , for  
 if  $a' = p-1$ , then  $a(p-1) \equiv 1$ ,  $ap-a \equiv 1$ ,  $-a \equiv 1$ ,  
 $0 \equiv 1+a$ ,  $p \equiv 1+a$ ,  $p-1 \equiv a \Rightarrow p-1 \equiv a$ , a  
 contradiction). Also, if  $a, a' \equiv 1$  and  
 $a_2 a' \equiv 1$ , then  $a, a' \equiv a_2 a' \Rightarrow a_1 \equiv a_2 \Rightarrow a_1 = a_2$ .  
 $\therefore$  As  $a$  runs through 1 to  $p-2$ , each  $a'$   
 from 1 to  $p-2$  is represented only once.

$\therefore$  as  $a$  runs through 1 to  $p-2$ ,  $1+a'$  runs  
 through 2 to  $p-1$ .

$$\begin{aligned}\therefore aa' &\equiv 1 \pmod{p} \Rightarrow a+a'a' \equiv a+1 \\ &\Rightarrow a(1+a') \equiv a+1\end{aligned}$$

$$\therefore a(a+1) \equiv a^2(1+a') \pmod{p}$$

$$\therefore (a(a+1)/p) = (a^2(1+a')/p) = ((1+a')/p)$$

$$\therefore \sum_{a=1}^{p-2} (a(a+1)/p) = \sum_{1+a'=2}^{p-1} ((1+a')/p)$$

$$= \sum_{a'=2}^{p-1} (a'/p) = \sum_{a=2}^{p-1} (a/p)$$

$$= \sum_{a=1}^{p-1} (a/p) - (1/p)$$

But by Th. 9.4,  $\sum_{a=1}^{p-1} (a/p) = 0$

and  $(1/p) = 1$ .

$$\therefore \sum_{a=1}^{p-2} (a(a+1)/p) = -1$$

Q. Prove the statements below:

(a) If  $p$  and  $q = 2p+1$  are both odd primes, Then  
 $-4$  is a primitive root of  $q$ .

Pf: Since  $-4 = -2^2$  and  $\gcd(2, q) = 1$ , Then  $\gcd(-4, q) = 1$ .  
Since  $\phi(q) = q-1 = 2p$ , Then order of  
 $-4$  must be  $1, 2, p$ , or  $2p$  by Th. 8.1.

(1) If  $-4 \equiv 1 \pmod{q}$ , Then  $5 \equiv 0 \pmod{q} \Rightarrow$   
 $q | 5$ . But  $q > 5$  since  $p$  is odd.  
 $\therefore$  order of  $-4$  mod  $q$  is not 1.

(2) If  $(-4)^2 \equiv 1 \pmod{q}$ , Then  $15 \equiv 0 \pmod{q}$ ,  
or  $q | 15 \Rightarrow q = 3$  or  $5$ , again  
contradicting  $q > 5$ .  
 $\therefore$  order of  $-4$  mod  $q$  is not 2.

(3) Suppose  $(-4)^p \equiv 1 \pmod{q}$

Since  $(-4)^p = (-4)^{\frac{q-1}{2}}$ , Then  $(-4)^{\frac{q-1}{2}} \equiv 1 \pmod{q}$

But  $(-4/q) = (-4)^{\frac{q-1}{2}} \pmod{q}$

$\therefore (-4/q) = 1 \pmod{q} \Rightarrow (-4/q) = 1 \quad [1]$

However,  $(-4/q) = (-1/q)(2/q)(2/q)$

$(-1/q) = (-1)^{\frac{q-1}{2}} = (-1)^{\frac{2p}{2}} = (-1)^p = -1$  as  $p$  is odd

$(2/q) \equiv 2^{\frac{q-1}{2}} = 2^p \pmod{q}$

If  $p \equiv 1 \pmod{4}$ , Then  $p = 1 + 4k$ ,

some  $k$ , so  $q = 2p + 1 = 3 + 8k$ ,

so  $q \equiv 3 \pmod{8}$ , so by Th. 9.6,

$(2/q) = 1$ .

$\therefore (-4/q) = (-1)(1)(1) = -1$

This contradicts [1].

If  $p \equiv 3 \pmod{4}$  Then, as above,

$q \equiv 7 \pmod{8}$ , so by Th. 9.6,

$(2/q) = 1$

$\therefore (-4/q) = (-1)(1)(1) = -1$ ,

contradicting [1].

$\therefore (-4)^p \not\equiv 1 \pmod{q}$ , so order  
of  $-4 \pmod{q}$  is not  $p$ .

(1), (2), (3)  $\Rightarrow$  order of  $(-4) \pmod{q}$  is  
 $2p = q-1 = \phi(q)$ .

$\therefore -4$  is a primitive root of  $q = 2p+1$ .

(6) If  $p \equiv 1 \pmod{4}$  is a prime, Then  $-4$  and  
 $(p-1)/4$  are quadratic residues of  $p$ .

$$\text{Pf: (i)} (-4/p) = (-1/p)(2/p)(2/p)$$

By corollary to Th. 9-2 (p. 187),  $(-1/p) = 1$   
 $(2/p) = \pm 1$ , so  $(2/p)(2/p) = 1$ .

$\therefore (-4/p) = 1 \Rightarrow -4$  is a quadratic  
residue of  $p$

(ii) Since  $\gcd(4, p) = 1$ , Then

$$\begin{aligned} x^2 \equiv \frac{p-1}{4} \pmod{p} &\iff 4x^2 \equiv p-1 \pmod{p} \\ &\iff 4x^2 \equiv -1 \pmod{p} \\ &\iff (2x)^2 \equiv -1 \pmod{p} \end{aligned}$$

Let  $y = 2x$ .

$\therefore y^2 \equiv -1 \pmod{p}$  has a solution

by corollary to Th. 9.2 (p. 187)  
since  $p \equiv 1 \pmod{4}$

$\therefore x^2 \equiv \frac{p-1}{4} \pmod{p}$  has a solution,

and so  $\frac{p-1}{4}$  is a quadratic residue of  $p$ .

9. For a prime  $p \equiv 7 \pmod{8}$ , show that  $p \mid 2^{\frac{p-1}{2}} - 1$

Pf: By Th. 9.2,  $(2/p) \equiv 2^{\frac{p-1}{2}} \pmod{p}$

By Th. 9.6,  $(2/p) = 1$  since  $p \equiv 7 \pmod{8}$ .

$\therefore 1 \equiv 2^{\frac{p-1}{2}} \pmod{p} \Rightarrow 2^{\frac{p-1}{2}} - 1 \equiv 0 \pmod{p}$

$\Rightarrow p \mid 2^{\frac{p-1}{2}} - 1$

10. Use Problem 9 to confirm that the numbers  $2^n - 1$  are composite for  $n = 11, 23, 83, 131, 179, 183, 239, 281$ .

Need to show  $n = \frac{p-1}{2}$  for  $p$  of form  $7+8k$ .

Then, by #9,  $p | 2^n - 1$ , so  $2^n - 1$  is composite.

$$11: 11 = \frac{p-1}{2}, p = 23 = 7 + (2)8$$

$$23: 23 = \frac{p-1}{2}, p = 47 = 7 + (5)8$$

$$83: 83 = \frac{p-1}{2}, p = 167 = 7 + (20)8$$

$$131: 131 = \frac{p-1}{2}, p = 263 = 7 + (32)8$$

$$179: 179 = \frac{p-1}{2}, p = 359 = 7 + (44)8$$

$$183: 183 = \frac{p-1}{2}, p = 367 = 7 + (45)8$$

$$239: 239 = \frac{p-1}{2}, p = 463 = 7 + 456 = 7 + (57)8$$

$$251: 251 = \frac{p-1}{2}, p = 503 = 7 + 496 = 7 + (62)8$$

All the "p" numbers above are prime.

11. Given that  $p$  and  $q = 4p + 1$  are both prime, prove the following:

(a) Any quadratic nonresidue of  $q$  is either a primitive root of  $q$  or has order  $4 \pmod{q}$ .

Pf: Let  $a$  be a quadratic non-residue of  $q$ .  
It is assumed that  $\gcd(a, q) = 1$ .

$$\therefore -1 = (a/q) \equiv a^{(q-1)/2} = a^{4p/2} = a^{2p} \pmod{q}$$

$$\therefore a^{4p} \equiv 1 \pmod{q}$$

$\therefore$  order of  $a \pmod{q}$  is  $1, 2, 4, p, 2p$ , or  $4p$

(1) If order of  $a \pmod{q}$  is  $4p = \phi(q)$ , Then  
 $a$  is a primitive root of  $q$ !

(2)  $\therefore$  Assume order of  $a \pmod{q}$  is not  $4p$ .

1: Order of  $a \neq 1$ , for if  $a^1 \equiv 1 \pmod{q}$ , Then  
 $x^2 \equiv a \equiv 1 \pmod{q}$  would have a solution  
( $x=1$ ), which contradicts  $a$  as a  
quadratic non-residue.

2: If  $a^2 \equiv 1 \pmod{q}$ , Then  $a^{2p} \equiv 1 \pmod{q}$   
But  $-1 \equiv a^{2p} \pmod{q} \Rightarrow -1 \equiv 1$ , or  
 $q/2$ , an impossibility.  $\therefore$  order of

$a \pmod{q}$  is not 2

p: Suppose  $a^p \equiv 1 \pmod{q}$ .  $\therefore a^{2p} \equiv 1 \pmod{q}$ ,  
and since  $a^{2p} \equiv -1 \pmod{q}$ , then  
 $(\equiv -1 \pmod{q}) \Rightarrow q \mid 2$ , an impossibility.  
 $\therefore$  order of  $a$  is not  $p$ .

2p: As above  $a^{2p} \equiv 1 \pmod{q}$  contradicts  
 $a^{2p} \equiv -1 \pmod{q}$ , so order of  $a$   
can't be  $2p$ .

$\therefore$  Since order can't be  $1, 2, p, 2p, 4p$ ,  
order of  $a \pmod{q}$  must be  $4$ .

$\therefore (1) + (2) \Rightarrow$  order of  $a \pmod{q}$  is either  
 $4p$  or  $4$ . If  $4p = \phi(q)$ , then  $a$  is a  
primitive root of  $q$ .

(6) The integer 2 is a primitive root of  $q$ ;  
in particular, 2 is a prim. root of the primes  
 $13, 29, 53$ , and  $173$ .

Pf:  $\phi(q) = q-1 = 4p+1-1 = 4p$ .

$\therefore$  Need to show  $2^{4p} \equiv 1 \pmod{q}$ , and

order of  $2 \pmod{q}$  can't be  $1, 2, 4, p, 2p$ .

Note  $p \equiv 1 \pmod{4} \Rightarrow p = 1 + 4k$ , so

$$q = 4p + 1 = 4 + 16k + 1 = 5 + 16k = 5 + 8(2k)$$

$$\therefore p \equiv 1 \pmod{4} \Rightarrow q \equiv 5 \pmod{8}$$

$$p \equiv 3 \pmod{4} \Rightarrow p = 3 + 4k, \text{ so}$$

$$q = 12 + 16k + 1 = 13 + 16k = 5 + 8(1 + 2k)$$

$$\therefore p \equiv 3 \pmod{4} \Rightarrow q \equiv 5 \pmod{8}.$$

$\therefore p$  prime and  $q = 4p + 1$  prime  $\Rightarrow$   
 $q \equiv 5 \pmod{8}$ .

$$\therefore (2/q) = -1 \text{ by Th. 9.6}$$

$$\therefore -1 = (2/q) = 2^{\frac{(q-1)}{2}} \pmod{q} = 2^{2p} \pmod{q}$$

$$\therefore 2^{2p} \equiv -1 \pmod{q} \quad [1]$$

(a) Squaring [1],  $2^{4p} \equiv 1 \pmod{q}$

(b)  $\exists p$ : Order of  $2$  can't be  $2p$  by [1], for  
 $2^{2p} \equiv 1 \Rightarrow 1 \equiv -1 \pmod{q} \Rightarrow q \mid 2$ .

$\therefore$  Order of  $2$  can't be  $p$ , for  $2^p \equiv 1 \Rightarrow$

$2^{2p} \equiv 1 \pmod{q}$  by squaring [1].

1:  $2^1 \equiv 1 \pmod{q} \Rightarrow 1 \equiv 0 \Rightarrow q | 1$ , so  
order can't be 1.

2:  $2^2 \equiv 1 \pmod{q} \Rightarrow 3 \equiv 0 \Rightarrow q | 3$ ,  
and impossibility since  $q = 4p + 1$ .

4:  $2^4 \equiv 1 \pmod{q} \Rightarrow 15 \equiv 0 \Rightarrow q | 15 \Rightarrow$   
 $q = 3, 5$ , or  $15$  also an impossibility  
since  $q = 4p + 1$  and  $p$  is prime.

$\therefore$  Order of 2 mod  $q$  is not 1, 2, 4,  $p$ ,  $2p$   
and so must be  $4p$ .

$\therefore (a) \& (b) \Rightarrow 2$  is a primitive root of  $q$

$$13 = 1 + 4(3)$$

$$29 = 1 + 4(7)$$

$$53 = 1 + 4(13)$$

$$173 = 1 + 4(43)$$

$\therefore 13, 29, 53$ , and  $173$  satisfy condition  
and so 2 is a prim. root for each.

12. If  $r$  is a primitive root of the odd prime  $p$ , prove that the product of the quadratic residues of  $p$  is congruent mod  $p$  to  $r^{(p^2-1)/4}$  and the product of the nonresidues of  $p$  is congruent mod  $p$  to  $r^{(p-1)^2/4}$ .

PF: (a) Product of quadratic residues is congruent to  $r^{(p^2-1)/4}$

The quadratic residues are congruent to the even powers of  $r$  (corollary to Th. 9.4).

Let  $a_1, a_2, \dots, a_{\frac{p-1}{2}}$  be the  $(p-1)/2$

quadratic residues of  $p$ .

$$\begin{aligned} a_1 a_2 \cdots a_{\frac{p-1}{2}} &\equiv r^2 \cdot r^4 \cdots r^{p-1} \pmod{p} \\ &= (r^1)^2 \cdot (r^2)^2 \cdots (r^{\frac{p-1}{2}})^2 \pmod{p} \\ &= [r^1 \cdot r^2 \cdots r^{\frac{p-1}{2}}]^2 \pmod{p} \\ &= (r^{1+2+\dots+\frac{p-1}{2}})^2 \pmod{p} \end{aligned}$$

$$\text{But } 1+2+\dots+\frac{p-1}{2} = \frac{p-1}{2} \left[ \frac{p-1}{2} + 1 \right] / 2$$

$$= \frac{p-1}{2} \left( \frac{p+1}{2} \right) / 2 = \left( \frac{p^2-1}{4} \right) / 2$$

$$\begin{aligned}\therefore a_1 a_2 \dots a_{\frac{p-1}{2}} &\equiv (r^{1+2+\dots+\frac{p-1}{2}})^2 \pmod{p} \\ &= \left[ r^{\frac{p^2-1}{4}} \right]^2 \pmod{p} \\ &= r^{\frac{p^2-1}{4}} \pmod{p}\end{aligned}$$

$\therefore$  product of quadratic residues is congruent mod  $p$  to  $r^{\frac{(p^2-1)}{4}}$ .

(6) product of quadratic nonresidues is congruent to  $r^{\frac{(p-1)^2}{4}}$

The quadratic nonresidues are congruent to the odd powers of  $r$  (corollary p. 188)

$\therefore$  Let  $a_1, a_2, \dots, a_{\frac{p-1}{2}}$  be the quadratic nonresidues

$$\begin{aligned}\therefore a_1 \cdot a_2 \dots a_{\frac{p-1}{2}} &\equiv r^1 \cdot r^3 \dots r^{p-2} \pmod{p} \\ &= r^{1+3+\dots+p-2} \pmod{p}\end{aligned}$$

But  $1+3+\dots+p-2 = \frac{p-1}{2} (p-1)/2$ , as

There are  $\frac{p-1}{2}$  terms.

$$\therefore 1 + 3 + \dots + p-2 = \frac{(p-1)^2}{4}.$$

$$\therefore a_1 \cdot a_2 \cdots a_{\frac{p-1}{2}} \equiv r^{\frac{(p-1)^2}{4}} \pmod{p}.$$

13. Establish that the product of the quadratic residues of the odd prime  $p$  is congruent mod  $p$  to 1 or -1 according as  $p \equiv 3 \pmod{4}$  or  $p \equiv 1 \pmod{4}$ .

Pf: Let  $r$  be a primitive root of  $p$ .

Since  $r^{p-1} \equiv 1 \pmod{p}$ , then

$$r^{p-1} - 1 = (r^{\frac{p-1}{2}} + 1)(r^{\frac{p-1}{2}} - 1) \equiv 0 \pmod{p}$$

As  $r$  is a prim. root of  $p$ ,  $r^{\frac{p-1}{2}} - 1 \not\equiv 0 \pmod{p}$

$$\therefore r^{\frac{p-1}{2}} + 1 \equiv 0 \pmod{p} \Rightarrow$$

$$r^{\frac{p-1}{2}} \equiv -1 \pmod{p}. [1]$$

Let  $a_1, a_2, \dots, a_{\frac{p-1}{2}}$  be the quadratic residues of  $p$ .

$\therefore$  By prob. #12 above,

$$a_1 \cdot a_2 \cdots a_{\frac{p-1}{2}} \equiv r^{(\frac{p^2-1}{4})/4} \pmod{p}.$$

$$= \left(r^{\frac{p-1}{2}}\right)^{(\frac{p+1}{2})} \pmod{p}$$

$$= (-1)^{\frac{p+1}{2}} \pmod{p} \text{ by } [1]$$

If  $p \equiv 1 \pmod{4}$ , then  $p = 1 + 4k$ , some  $k$ ,  
so  $\frac{p+1}{2} = \frac{1+4k}{2} = 1+2k$ , an odd integer.

$$\therefore (-1)^{\frac{p+1}{2}} = -1.$$

$$\therefore p \equiv 1 \pmod{4} \Rightarrow a_1 \cdot a_2 \cdots a_{\frac{p-1}{2}} \equiv -1 \pmod{p}$$

If  $p \equiv 3 \pmod{4}$ , then  $p = 3 + 4k$ , some  $k$ ,

$$\text{so } \frac{p+1}{2} = \frac{3+4k}{2} = 2+2k, \text{ an even integer.}$$

$$\therefore (-1)^{\frac{p+1}{2}} = 1.$$

$$\therefore p \equiv 3 \pmod{4} \Rightarrow a_1 \cdot a_2 \cdots a_{\frac{p-1}{2}} \equiv 1 \pmod{p}.$$

14. (a) If the prime  $p > 3$ , show that  $p$  divides the sum of its quadratic residues.

Pf: Let  $r$  be a primitive root of  $p$ .

Let  $a_1, a_2, \dots, a_{\frac{p-1}{2}}$  be the quadratic residues of  $p$ .

By corollary to Th. 9.4 (p. 188),  $r^2, r^4, \dots, r^{p-1}$  are congruent to the quadratic residues of  $p$ .

$$\therefore a_1 + a_2 + \dots + a_{\frac{p-1}{2}} \equiv r^2 + r^4 + \dots + r^{p-1} \pmod{p}$$

$$\text{But } r^2 + r^4 + \dots + r^{p-1} = r^2(1 + r^2 + \dots + r^{p-3}), \\ \text{for } p > 3.$$

$$\therefore a_1 + a_2 + \dots + a_{\frac{p-1}{2}} \equiv r^2(1 + r^2 + \dots + r^{p-3}) \pmod{p}, [1] \\ \text{for } p > 3.$$

But  $r^{p-1} \equiv 1 \pmod{p}$ , as  $r$  is a prim. root.

$$\therefore r^2 + r^4 + \dots + r^{p-1} \equiv 1 + r^2 + r^4 + \dots + r^{p-3} \pmod{p}, \\ \text{for } p > 3.$$

$$\therefore a_1 + a_2 + \dots + a_{\frac{p-1}{2}} \equiv 1 + r^2 + r^4 + \dots + r^{p-3} \pmod{p}, [2] \\ \text{for } p > 3$$

Equating [1] and [2], for  $p > 3$ ,

$$r^2(1+r^2+\dots+r^{p-3}) \equiv (1+r^2+\dots+r^{p-3}) \pmod{p} \quad [3]$$

But  $p$  must divide  $(1+r^2+\dots+r^{p-3})$ , for if not, then we cancel it on both sides of [3], and obtain  $r^2 \equiv 1 \pmod{p}$ . This is a contradiction since  $r$  is a primitive root of  $p > 3$ , so that  $p-1 > 2$  and  $r^{p-1} \equiv 1 \pmod{p}$ .

Since  $p \mid (1+r^2+\dots+r^{p-3})$ , then from [1] or  $\sum_{i=1}^{p-1} a_i$ ,  $p \mid (a_1+a_2+\dots+a_{\frac{p-1}{2}})$

Note: Since  $1+2+\dots+p-1 = \binom{p-1}{2}p$ , then  $p \mid (1+2+\dots+p-1)$ .

$\therefore p$  also divides the sum of the quadratic nonresidues of  $p$ , for  $p > 3$ .

(b) If the prime  $p > 5$ , show that  $p$  divides the sum of the squares of its quadratic nonresidues.

Pf: Let  $r$  be a prim. root of  $p$ , and let  $a_1, a_2, \dots, a_{\frac{p-1}{2}}$  be the quadratic

nonresidues of  $p$ .

By corollary to Th. 9.4 (p. 188),  $r, r^3, \dots, r^{p-2}$  are congruent to the quadratic nonresidues of  $p$ .

$$\therefore a_1^2 + a_2^2 + \dots + (a_{\frac{p-1}{2}})^2 \equiv r^2 + r^6 + \dots + r^{2(p-2)} \pmod{p} \quad [1]$$

Each term on the right side of [1] is described by  $r^{4k-2}$ ,  $1 \leq k \leq \frac{p-1}{2}$

And all terms on the right of [1] are incongruent mod  $p$ .

For if  $r^{4k_1-2} \equiv r^{4k_2-2} \pmod{p}$ , then

by Th. 8.2,  $4k_1 - 2 \equiv 4k_2 - 2 \pmod{p-1} \Leftrightarrow$

$$4k_1 \equiv 4k_2 \pmod{p-1} \Leftrightarrow$$

$$k_1 \equiv k_2 \pmod{p-1}$$

since  $p > 5$ ,  $p-1 > 4$ ,  $\therefore \gcd(4, p-1) = 1$ .

But  $1 \leq k_1, k_2 \leq \frac{p-1}{2}$ , so that  $k_1, k_2 < p-1$ .

$$\therefore k_1 = k_2$$

$$\therefore r^{4k_1-2} \equiv r^{4k_2-2} \pmod{p} \Leftrightarrow k_1 = k_2, \text{ so}$$

all terms on right side of [1] are incongruent mod  $p$ .

All the terms on the right side of [1]

are even, and there are  $\frac{p-1}{2}$  such terms.  
 Since they are incongruent, then the terms are congruent to  $r^2, r^4, \dots, r^{p-1}$ , in some order.

$$\therefore r^2 + r^4 + \dots + r^{2(p-2)} \equiv r^2 + r^4 + \dots + r^{p-1} \pmod{p} \quad [2]$$

By (a), the right side of L23 is divisible by  $p$ , and  $\therefore$  so is the left side of L23, and  $\therefore$  so is the left side of L13.

15. Prove that for any prime  $p > 5$  there exist integers  $1 \leq a, b \leq p-1$  for which  $(a/p) = (a+1/p) = 1$  and  $(b/p) = (b+1/p) = -1$

That is, there are consecutive quadratic residues of  $p$  and consecutive nonresidues.

Pf: Since  $x^2 \equiv 1$ ,  $x^2 \equiv 4$ , and  $x^2 \equiv 9$  have solutions for all  $p > 5$ , then consider  $x^2 \equiv 2$ ,  $x^2 \equiv 5$ ,  $x^2 \equiv 10$ .

Now use G(a).

For  $p > 5$ :  $\gcd(2, p) = 1$ ,  $\gcd(5, p) = 1$ , so  $\gcd(10, p) = 1$ . By G(a) one of 2, 5, or 10 must be a quadratic residue of  $p$ .

If  $(2/p) = 1$ , then 1, 2 are consecutive

residues

If  $(5/p) = 1$ , Then 4 and 5 are consecutive residues

If  $(10/p) = 1$ , Then 9 and 10 are consecutive residues.

Since the above showed at least one pair of consecutive residues for  $p \geq 5$ , then consider the remaining  $p-3$  terms (There are  $p-1$  residues + nonresidues, so subtract out the 2 consecutive residues). Let  $g_k, g_{k+1}$  be the consecutive residues.

∴ Consider the terms:

1, 2, ...,  $g_k, g_{k+1}, \dots, g_{p-1}$

If 2, 3 are consecutive nonresidues, then we're done.

So suppose 2, 3 are not consecutive nonresidues.

∴ Since 1 and 4 are always residues, then in the list, there are at least 3 residues among 1, 2, 3, 4.

Suppose the remaining even number of terms  $5, 6, \dots, p-1$  alternate with

respect to residue/nonresidue.  
 Then in the remaining terms  $5, 6, \dots, p-1$ ,  
 the number of residues = number of  
 nonresidues, and so overall, the  
 number of residues is at least 2  
 greater than the number of nonresidues.

$\therefore$  There must be consecutive nonresidues  
 in the list  $1, 2, \dots, p-1$ .

16. (a) Let  $p$  be an odd prime and  $\gcd(a, p) = \gcd(k, p) = 1$ . Show that if the equation  $x^2 - ay^2 = kp$  admits a solution, then  $(a/p) = 1$  ; for example,  $(2/7) = 1$  because  $6^2 - 2 \cdot 2^2 = 4 \cdot 7$ .

Pf: Suppose  $x, y$  solve  $x^2 - ay^2 = kp$ .

$$(1) \quad \gcd(p, y) = 1$$

For if  $\gcd(p, y) = n > 1$ , then since  $p$  is prime, then  $y = np$ .

$$\therefore x^2 = a(np)^2 + kp = an^2p^2 + kp.$$

$$\therefore p|x, \text{ so } x = mp, \text{ some } m \geq 1.$$

$$\therefore m^2 p^2 = a n^2 p^2 + kp, \text{ or}$$

$$m^2 p - a n^2 p = p(m^2 - a n^2) = k \Rightarrow p \mid k$$

But  $\gcd(k, p) = 1$ .  $\therefore \gcd(p, y) = 1$

(2) By (1),  $y^{p-1} \equiv 1 \pmod{p}$  by Euler's Th.

$$\therefore x^2 - a y^2 = kp \Leftrightarrow x^2 \equiv a y^2 \pmod{p}$$

$$\therefore x^2 y^{p-1} \equiv a y^2 \pmod{p}.$$

$p$  is odd, so  $p-1 \geq 2$ , so  $y^{p-1} \geq y^2$ .  
Using (1) again to divide by  $y^2$ ,

$$x^2 y^{p-3} \equiv a \pmod{p}$$

$$\therefore x^2 y^{p-3} \cdot y^{p-1} \equiv a \pmod{p}$$

$$x^2 y^{2p-4} = (x y^{p-2})^2 \equiv a \pmod{p}$$

$\therefore$  Let  $z = x y^{p-2}$ , so  $z^2 \equiv a \pmod{p}$

$$\therefore (a/p) = 1$$

$\equiv$

Incidentally,  $\gcd(x, p) = 1$

For if  $x = np$ , then  $(np)^2 - ay^2 = kp$ , or

$$n^2p^2 - kp = ay^2, \quad p(np - k) = ay^2.$$

$\therefore p | a$  or  $p | y$ . This contradicts (1) and  $\gcd(a, p) = 1$ .

(b) By considering the equation  $x^2 + 5y^2 = 7$ , demonstrate that the converse of the result in part (a) need not hold.

$$(-5/7) = 1, \text{ for } (-5)^{(7-1)/2} = -5^3 = -125 = -7 \cdot 18 + 1 \\ \text{so } (-5)^{(7-1)/2} \equiv 1 \pmod{7}$$

But there is no integer solution to  $x^2 + 5y^2 = 7$ .

Only possibilities are  $x = 0, 1, 2$ ,  $y = 0, 1$  and these don't work.

(c) Show that for any prime  $p \equiv \pm 3 \pmod{8}$ , the equation  $x^2 - 2y^2 = p$  has no solution.

Pf: Suppose  $x^2 - 2y^2 = p$  has a solution.

Since  $p$  is odd,  $\gcd(2, p) = 1$  and  
clearly  $\gcd(1, p) = 1$ .

$\therefore$  By (a),  $(2/p) = 1$ .

But  $p \equiv \pm 3 \pmod{8} \Leftrightarrow$   
 $p \equiv 3 \pmod{8}$  or  $p \equiv 5 \pmod{8}$ ,

and by Th. 9.6,  $(2/p) = -1$ .

$\therefore x^2 - 2y^2 = p$  can't have a solution.

17. Prove That The odd prime divisors  $p$  of The integers  $q^n + 1$  are of The form  $p \equiv 1 \pmod{4}$

Pf: Let  $p$  be an odd prime divisor of  $q^n + 1$

$\therefore q^n + 1 \equiv 0 \pmod{p}$ , or

$(3^2)^n + 1 \equiv 0 \pmod{p}$ , or  $(3^n)^2 \equiv -1 \pmod{p}$

Since  $p$  is odd, either  $p \equiv 1 \pmod{4}$  or  
 $p \equiv 3 \pmod{4}$ .

By corollary to Th. 9.2 (p. 187) if  $p \equiv 3 \pmod{4}$ ,  
 There can be no solution to  $x^2 \equiv -1 \pmod{p}$ ,  
 so that there is no  $n$  s.t.  $(3^n)^2 \equiv -1 \pmod{p}$

$\therefore$  If  $p$  is to be a divisor of  $9^n + 1$ , it  
 must be of the form  $p \equiv 1 \pmod{4}$ .

18. For a prime  $p \equiv 1 \pmod{4}$ , verify that the sum  
 of the quadratic residues of  $p$  is equal to  
 $p(p-1)/4$

Pf: (1) If  $(a/p) = 1$ , then  $(p-a/p) = 1$

For since  $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ , and

$$(p-a)^n = p^n + \dots + (-a)^n = p^n + \dots + (-1)^n a^n,$$

$$\text{Then } (p-a)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} a^{\frac{p-1}{2}} \pmod{p}$$

For  $p \equiv 1 \pmod{4}$ ,  $p-1=4k$ , some  $k$ ,  
 so  $(-1)^{\frac{p-1}{2}} = (-1)^{2k} = 1$ .

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

$\therefore$  for  $p \equiv 1 \pmod{4}$ ,  $p-a$  is also a quad. residue.

(2) Let  $a_1, \dots, a_r$  be the quadratic residues of  $p$  less than  $p/2$ .

$\because p-a_1, \dots, p-a_r$  are quadratic residues of  $p$ , all less than  $p$ , and  $p-a_i > p/2$  (since  $a_i < p/2$ ,

Then  $-a_i > -p/2$ ,  $p-a_i > p-p/2 = p/2$ .

Since all these residues are less than  $p$ ,  
they are all incongruent.

(3) The  $a_i$  and  $p-a_i$  are all the quadratic residues of  $p$ .

For if  $a_x$  is a quadratic residue of  $p$  s.t.  $p/2 < a_x < p$ , Then  $p-a_x$  is a residue by (2), and  $0 < p-a_x < p/2$ , so  $p-a_x$  must be one of the  $a_i$ , since that set consisted of all residues less than  $p/2$ .

$\therefore p-(p-a_x)$  must be one of the  $p-a_i$ . But  $p-(p-a_x) = a_x$ , so  $a_x$  is one of  $a_i$ .

(4) Since there are a total of  $\frac{p-1}{2}$  quadratic

residues (Th. 9.4), (3)  $\Rightarrow$  There are  $\frac{p-1}{4}$  residues  $< p/2$  and  $\frac{p-1}{4}$  residues  $> p/2$ .

$\therefore r = \frac{p-1}{4}$  in the sequence  $a_1, \dots, a_r$ .

$$(5) \therefore \text{Sum} = (a_1 + \dots + a_r) + [(p-a_1) + \dots + (p-a_r)]$$

$$= p + \dots + p = rp = \left(\frac{p-1}{4}\right)p$$

Note That from (1), for  $p \equiv 3 \pmod{4}$ ,

$$(p-a)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} a^{\frac{p-1}{2}} \equiv -a^{\frac{p-1}{2}} \equiv -1 \pmod{p},$$

so if  $a$  is a quadratic residue of  $p$ ,  
 $p-a$  is a quadratic nonresidue.

### 9.3 Quadratic Reciprocity

Note Title

7/17/2006

1. Evaluate the following Legendre symbols:

(a)  $(71/73)$

$$71 \equiv -1 \pmod{4}, 73 \equiv 1 \pmod{4} \therefore (71/73) = (73/71)$$

$$(73/71) = (71+2/71) = (2/71)$$

$$71 = 7 + 8(8) \Rightarrow 71 \equiv 7 \pmod{8}, \text{ so } (2/71) = 1$$

$$\therefore (71/73) = 1$$

(b)  $(-219/383)$

$$219 = 3 \cdot 73 \quad 383 \equiv 3 \pmod{4}$$

$$\therefore (-219/383) = (-1/383)(3/383)(73/383)$$

$$= (-1)[-(383/3)](383/73)$$

$$= (2/3)(18/73)$$

$$= (-1)(2 \cdot 3^2/73) = -(2/73)$$

$$= -1 \quad \text{as } 73 \equiv 1 \pmod{4}$$

$$\therefore (-219/383) = -1$$

$$(c) (461/773)$$

$$461 \equiv 1 \pmod{4}$$

$$\begin{aligned}\therefore (461/773) &= (773/461) \\&= (312/461) = (2^3 \cdot 3 \cdot 13/461) \\&= (2 \cdot 3 \cdot 13/461) \\&= (2/461)(3/461)(13/461) \\&= (-1)(461/3)(461/13) \\&= (-1)(2/3)(6/13) \\&= (-1)(-1)(2/13)(3/13) \\&= (-1)(3/13) = (-1)(13/3), \text{ as } 13 \equiv 1 \pmod{4} \\&= (-1)(1/3) \\&= -1\end{aligned}$$

$$\therefore (461/773) = -1$$

$$(d) (1234/4567) \quad 1234 = 2 \cdot 617$$

$$4567 \equiv 3 \pmod{4} \quad 617 \equiv 1 \pmod{4}$$

$$\begin{aligned}\therefore (1234/4567) &= (2/4567)(617/4567) \\&= (1)(4567/617) \text{ as } 4567 \equiv 3 \pmod{8} \\&= (248/617)\end{aligned}$$

$$\begin{aligned}
 &= (2^3 \cdot 31 / 617) = (2/617)(31/617) \\
 &= (1)(31/617) \quad \text{as } 617 \equiv 1 \pmod{8} \\
 &= (617/31) = (28/31) \\
 &= (4 \cdot 7/31) = (7/31) \\
 &= -(31/7) \quad \text{as } 2 \equiv 3 \pmod{4}, 31 \equiv 3 \pmod{4} \\
 &= -(3/7) = (7/3) = (1/3) = 1
 \end{aligned}$$

$$\therefore (1234/4567) = 1$$

$$(c) (3658/12703) \quad 3658 = 2 \cdot 31 \cdot 59$$

$$12703 \equiv 7 \pmod{8} \quad \therefore (2/12703) = 1$$

$$\therefore (2/12703)(31/12703)(59/12703)$$

$$= (31/12703)(59/12703) \quad 12703 \equiv 3 \pmod{4}$$

$$= (12703/81)(12703/59) \quad 31 \equiv 3 \pmod{4}$$

$$= (24/81)(18/59)$$

$$= (6/31)(2/59) = -(6/81) \quad \text{as } 59 \equiv 3 \pmod{8}$$

$$= -(2/81)(3/31) = -(3/81) \quad \text{as } (2/31) = 1$$

$$= (31/3) = (1/3) = 1$$

$$\therefore (3658/12703) = 1$$

2. Prove that 3 is a quadratic nonresidue of all primes of the form  $2^{2n} + 1$ , and all primes of the form  $2^p - 1$ , where  $p$  is an odd prime.

Pf: (1) For all  $n$ ,  $4^n \equiv 4 \pmod{12}$

Clearly true for  $n=1$

Assume true for  $n$ .

Then  $4^{n+1} = 4^n \cdot 4 \equiv 4 \cdot 4 = 16 \equiv 4 \pmod{12}$

$$(2) \therefore 2^{2n} = 4^n \equiv 4 \pmod{12}$$

$$\therefore 2^{2n} + 1 \equiv 5 \pmod{12}$$

(3) Let  $p$  be a prime of form  $2^{2n} + 1$ .

$\therefore$  By Th. 9.10 and (2) above,  $(3/p) = -1$ , and so 3 is a quadratic nonresidue of prime  $2^{2n} + 1$ !

(4) If  $p$  is an odd prime,  $p = 2n + 1$ , some  $n$ .

$$\therefore 2^p - 1 = 2^{2n+1} - 1 = 4^n \cdot 2 - 1$$

$$\begin{aligned} \text{By (1), } 4^n \cdot 2 - 1 &\equiv 4 \cdot 2 - 1 \pmod{12} \\ &\equiv 7 \pmod{12} \end{aligned}$$

$$\equiv -5 \pmod{12}$$

$$\therefore 2^p - 1 \equiv -5 \pmod{12}$$

$$\therefore \text{By Th. 9.10, } (3/(2^p - 1)) = -1, \text{ so}$$

3 is a quadratic nonresidue of prime  $2^p - 1$ .

3. Determine whether the following quadratic congruences are solvable:

$$(a) x^2 \equiv 219 \pmod{419}$$

419 is prime.  $\therefore$  Consider  $(219/419)$

$$219 = 3 \cdot 73 \quad 419 \equiv 3 \pmod{4}, \quad 73 \equiv 1 \pmod{4}$$

$$\therefore (219/419) = (3/419) \cdot (73/419)$$

$$(3/419) = -(419/3) = -(2/3) = -(-1) = 1$$

$$(73/419) = (419/73) = (5 \cdot 73 + 54/73)$$

$$= (54/73) = (2 \cdot 3^3/73) = (2 \cdot 3/73)$$

$$= (2/73) \cdot (3/73) = 1 \cdot (3/73)$$

$$= (73/3) = (1/3) = 1$$

$$\therefore (219/419) = 1, \text{ so } \underline{\text{solvable}}$$

$$(b) 3x^2 + 6x + 5 \equiv 0 \pmod{89} \quad [13]$$

$$\gcd(4, 89) = 1, \quad \gcd(3, 89) = 1.$$

$$\therefore [1] \Leftrightarrow 12(3x^2 + 6x + 5) \equiv 0 \pmod{89}$$

$$\Leftrightarrow 36x^2 + 72x + 60 \equiv 0 \pmod{89}$$

$$\Leftrightarrow (6x+6)^2 + 24 \equiv 0 \pmod{89}$$

$$\Leftrightarrow (6x+6)^2 \equiv 65 \pmod{89}$$

$$\text{Let } y = 6x+6. \therefore [1] \Leftrightarrow y^2 \equiv 65 \pmod{89}$$

$$\therefore \text{Consider } (65/89) = (13/89)(5/89)$$

$$(3 \equiv 1 \pmod{4}), (5 \equiv 1 \pmod{4}), (89 \equiv 1 \pmod{89})$$

$$\begin{aligned} \therefore (13/89) &= (89/13) = (11/13) = (13/11) \\ &= (2/11) = -1 \quad \text{as } 11 \equiv 3 \pmod{8} \end{aligned}$$

$$(5/89) = (89/5) = (4/5) = (2^2/5) = 1$$

$$\therefore (65/89) = -1$$

$\therefore [1]$  is not solvable.

$$(C) 2x^2 + 5x - 8 \equiv 0 \pmod{101} \quad [1]$$

As in (a) Let  $y = 2ax + b$ ,  $d = b^2 - 4ac$ ,  
so  $[1] \Leftrightarrow y^2 \equiv d \equiv 97 \pmod{101}$

$\therefore$  Consider  $(97/101)$ . 97 is prime  
 $97 \equiv 1 \pmod{4}$ ,  $101 \equiv 1 \pmod{4}$

$$\therefore (97/101) = (101/97) = (4/97) = (2^2/97) = 1$$

$\therefore \{1\}$  is solvable.

4. Verify That if  $p$  is an odd prime, Then

$$(-2/p) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod{8} \text{ or } p \equiv 3 \pmod{8} \\ -1 & \text{if } p \equiv 5 \pmod{8} \text{ or } p \equiv 7 \pmod{8} \end{cases}$$

$$\text{Pf: } (-2/p) = (-1/p)(2/p)$$

$$(-1/p) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod{4} \\ -1 & \text{if } p \equiv 3 \pmod{4} \end{cases} \quad \begin{matrix} \text{Corollary to Th. 9.2} \\ p \cdot 187 \end{matrix}$$

$$(2/p) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod{8} \text{ or } p \equiv 7 \pmod{8} \\ -1 & \text{if } p \equiv 3 \pmod{8} \text{ or } p \equiv 5 \pmod{8} \end{cases} \quad \text{Th. 9.1}$$

$$\therefore \text{if } p \equiv 1 \pmod{8}, \text{ Then } p \equiv 1 \pmod{4}, \text{ so} \\ (-2/p) = (-1/p)(2/p) = 1 \cdot 1 = 1 \quad [1]$$

$$\text{if } p \equiv 3 \pmod{8}, \text{ Then } p \equiv 3 \pmod{4}, \text{ so} \\ (-2/p) = (-1/p)(2/p) = -1 \cdot -1 = 1 \quad [2]$$

$$\text{if } p \equiv 5 \pmod{8}, \text{ Then } p \equiv 5 \pmod{4} \equiv 1 \pmod{4}.$$

$$(-2/p) = (-1/p)(2/p) = 1 \cdot -1 = -1 \quad [3]$$

$$\text{if } p \equiv 1 \pmod{8}, \text{ Then } p \equiv 7 \pmod{4} \equiv 3 \pmod{4}$$

$$(-2/p) = (-1/p)(2/p) = -1 \cdot 1 = -1 \quad [4]$$

$$\therefore (-2/p) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod{8} \text{ or } p \equiv 3 \pmod{8} \\ -1 & \text{if } p \equiv 5 \pmod{8} \text{ or } p \equiv 7 \pmod{8} \end{cases} \quad [13, 12] \\ [33, 24]$$

5. (a) Prove that if  $p > 3$  is an odd prime, then

$$(-3/p) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod{6} \\ -1 & \text{if } p \equiv 5 \pmod{6} \end{cases}$$

$$\text{Pf: } (-3/p) = (-1/p) \cdot (3/p)$$

(i) Suppose  $p \equiv 1 \pmod{6}$ . Then  $p-1=6K$ , some  $K$ .

(a) If  $K$  is even, Then  $k=2k'$ , so

$$p-1=12k', \text{ or } p \equiv 1 \pmod{12}$$

$$\therefore (-1/p) = (-1)^{\frac{p-1}{2}} = (-1)^{\frac{12k'}{2}} = (-1)^{6k'} = 1$$

$$(3/p) = 1, \text{ by Th. 9.10}$$

$$\therefore (-3/p) = 1 \cdot 1 = 1$$

(b) If  $K$  is odd, Then  $k=2k'+1$ , so

$$p-1=6(2k'+1)=6+12k', \text{ or}$$

$$p \equiv 7 \pmod{12} \Leftrightarrow p \equiv -5 \pmod{12}$$

$$\therefore (-1/p) = (-1)^{\frac{p-1}{2}} = (-1)^{3+6k'} = -1$$

$(3/p) = -1$ , by Th. 9.10

$$\therefore (-3/p) = -1 \cdot -1 = 1$$

$$\therefore p \equiv 1 \pmod{6} \Rightarrow (-3/p) = 1$$

(2) Suppose  $p \equiv 5 \pmod{6}$ . Then  $p-5=6k$ , some  $k$

(a) If  $k$  is even,  $k=2k'$ , some  $k'$ , so  
 $p-5=12k'$ , or  $p \equiv 5 \pmod{12}$

$$\therefore (-1/p) = (-1)^{\frac{p-1}{2}} = (-1)^{4+12k'} = 1$$

$(3/p) = -1$ , by Th. 9.10

$$\therefore (-3/p) = 1 \cdot -1 = -1$$

(b) If  $k$  is odd,  $k=2k'+1$ , so

$$p-5=12k'+6, \text{ or } p \equiv 11 \pmod{12} \Leftrightarrow p \equiv -1 \pmod{12}$$

$$\therefore (-1/p) = (-1)^{\frac{p-1}{2}} = (-1)^{5+6k'} = -1$$

$(3/p) = 1$ , by Th. 9.10

$$\therefore (-3/p) = -1 \cdot 1 = -1$$

$$= \therefore p \equiv 5 \pmod{6} \Rightarrow (-3/p) = -1$$

Note:  $p \not\equiv 3 \pmod{6}$ , for if so, then  
 $p-3 = k \cdot 3 \cdot 2$ , so  $3 | p-3 \Rightarrow 3 | p$   
 similarly for Th. 9.10

(6) Using part (a), show that there are infinitely many primes of the form  $6K+1$ .

Pf: Assume there are a finite number of primes of form  $6K+1$ , say,  $p_1, \dots, p_r$ .

$$\text{Consider } N = (2p_1p_2 \cdots p_r)^2 + 3$$

$3 \nmid N$ , for if  $3 | N$ , then  $3 | (2p_1 \cdots p_r)^2$ ,  
 so 3 must be one of  $p_i$ , but 3 is not of form  $6K+1$ .

$\therefore$  There must be some odd prime divisor,  $p > 3$ , of  $N$ .

And  $p \neq p_i$ , for if  $p = p_i$ , some  $i$ ,  
 then  $p | N \Rightarrow p | 3$ , a contradiction.

$\therefore N \equiv 0 \pmod{p}$ , or equivalently,  
 $(2p_1 p_2 \cdots p_r)^2 \equiv -3 \pmod{p}$

$$\therefore (-3/p) = 1$$

$\therefore$  by (a),  $p \equiv 1 \pmod{6}$ , for if  
 $p \equiv 5 \pmod{6}$ , then  $(-3/p) = -1$ , and  
 $p \not\equiv 3 \pmod{6}$  as shown above.

$\therefore p$  is of form  $6k+1$ , contradicting  $p \neq p_1$ .

$\therefore$  infinitely many primes of form  $6k+1$ .

6. Use Theorem 9.2 and problems 4 and 5 to determine which primes can divide integers of the forms  $n^2+1$ ,  $n^2+2$ , or  $n^2+3$  for some value of  $n$ .

(a)  $p | n^2+1 \Leftrightarrow n^2 \equiv -1 \pmod{p}$

For  $p$  odd,  $(-1/p) = (-1)^{\frac{p-1}{2}}$ , so  $(-1/p) = 1 \Leftrightarrow \frac{p-1}{2}$  is even

$\therefore p \geq 3$ ,  $p = 2k+1$ , so  $\frac{(2k+1)-1}{2}$  is even,

so  $\frac{2k}{2} = k$  is even, so  $k = 2k'$ ,  $\therefore$

$$p = 2(2k') + 1 = 4k' + 1$$

$\therefore$  for  $p$  odd,  $p \equiv 1 \pmod{4}$

if  $p=2$ ,  $n^2+1$  must be even.

$\therefore p \mid n^2+1 \left\{ \begin{array}{l} \text{if } n \text{ is odd, } p=2 \text{ or } p \equiv 1 \pmod{4} \\ \text{if } n \text{ is even, } p \equiv 1 \pmod{4} \end{array} \right.$

(6)  $p \mid n^2+2 \Leftrightarrow n^2 \equiv -2 \pmod{p}$

If  $n$  is even,  $2 \mid n^2+2$ .

If  $n$  is odd,  $n^2+2$  is odd,  $2 \nmid n^2+2$

For  $p$  odd,  $n^2 \equiv -2 \pmod{p}$  is solvable  $\Leftrightarrow$   
 $(-2/p) = 1$ .

By prob. (4) above,  $(-2/p) = 1$  if  $p \equiv 1 \pmod{8}$   
or  $p \equiv 3 \pmod{8}$

$\therefore p \mid n^2+2 \left\{ \begin{array}{l} \text{if } n \text{ is even, } p=2 \text{ or } p \equiv 1 \pmod{8} \text{ or} \\ \qquad \qquad \qquad p \equiv 3 \pmod{8} \\ \text{if } n \text{ is odd, } p \equiv 1 \pmod{8} \text{ or} \\ \qquad \qquad \qquad p \equiv 3 \pmod{8} \end{array} \right.$

((7))  $p \mid n^2+3 \Leftrightarrow n^2 \equiv -3 \pmod{p}$

Problem (5) above addresses  $p > 3$ , in

which case  $(-3/p) = 1$  if  $p \equiv 1 \pmod{6}$ .

For  $p=2$ ,

If  $n$  is even,  $n^2+3$  is odd,  $2 \nmid n^2+3$   
If  $n$  is odd,  $n^2+3$  is even, so  $2 \mid n^2+3$

For  $p=3$ ,  $n^2+3 \equiv 0 \pmod{3} \Leftrightarrow n^2 \equiv 0 \pmod{3}$   
 $\Leftrightarrow 3 \mid n$

$\therefore p \mid n^2+3$   $\begin{cases} \text{if } n \text{ is even, and } p \equiv 1 \pmod{6} \\ \text{if also } 3 \mid n, p = 3 \\ \text{if } n \text{ is odd, } p = 2 \text{ or } p \equiv 1 \pmod{6} \\ \text{if also } 3 \mid n, p = 3 \end{cases}$

7. Prove There exist infinitely many primes of form  $8k+3$ .

Pf: Use prob. (4) above since it has conditions for  $(-2/p)$  using  $\pmod{8}$ .

$\therefore$  Assume finitely many primes of form  $8k+3$ , which is odd, say  $p_1, p_2, \dots, p_n$ .

Consider  $N = (p_1 p_2 \dots p_n)^2 + 2$  ( $N$  is odd).  
 $N$  must contain an odd prime divisor

$\rho$  s.t.  $\rho \neq p_i$ , for if  $\rho = p_i$ , some  $i$ , then  
 $p|N$  and  $p|(p_1 \cdots p_r)^2 \Rightarrow p|2$ .

$$\therefore N \equiv 0 \pmod{\rho} \text{ or } (p_1 \cdots p_r)^2 \equiv -2 \pmod{\rho}$$

$$\therefore \text{By prob. (4) above, } \rho \equiv 1 \pmod{8} \text{ or } \\ \rho \equiv 3 \pmod{8}$$

Suppose  $N = q_1^{k_1} \cdots q_s^{k_s}$  and all  $q_i$  are  
 s.t.  $q_i \equiv 1 \pmod{8}$ .

$$\therefore N = q_1^{k_1} q_2^{k_2} \cdots q_s^{k_s} \equiv 1 \pmod{8} \quad [1]$$

But  $p_i \equiv 3 \pmod{8}$ , so  $p_i^2 \equiv 9 \equiv 1 \pmod{8}$

$$\therefore p_1^2 \cdots p_r^2 \equiv 1 \pmod{8}$$

$$\therefore (p_1 \cdots p_r)^2 \equiv 1 \pmod{8}$$

$\therefore N \equiv 1 \pmod{8}$ , a contradiction  
 to [1].

$\therefore$  All  $q_i$  can't be s.t.  $q_i \equiv 1 \pmod{8}$ ,  
 So there must be some odd prime divisor  $q_i = p$  of  $N$  s.t.  $p \equiv 3 \pmod{8}$ .  
 And This contradicts  $p_i$  above being finite.

8. Find a prime number  $p$  that is simultaneously expressible in the forms  $x^2 + y^2$ ,  $u^2 + 2v^2$ , and  $r^2 + 3s^2$ .

If  $x^2 + y^2 = p$ , Then  $x^2 \equiv -y^2 \pmod{p}$ , or  
 $\frac{x^2}{y^2} \equiv -1 \pmod{p}$ .

Similarly,  $\frac{u^2}{v^2} \equiv -2 \pmod{p}$ ,  $\frac{r^2}{s^2} \equiv -3 \pmod{p}$

where  $(\frac{x}{y})^2$ ,  $(\frac{u}{v})^2$ , and  $(\frac{r}{s})^2$  are integers.

$\therefore$  Look at  $(-1/p) = (-2/p) = (-3/p)$  as a minimum condition.

$$(-1/p) = 1, \text{ if } p \equiv 1 \pmod{4}$$

$$(-2/p) = 1, \text{ if } p \equiv 1 \pmod{8} \text{ or } p \equiv 3 \pmod{8} \quad [\text{prob. 4}]$$

$$(-3/p) = 1, \text{ if } p \equiv 1 \pmod{6} \quad [\text{prob. 5}]$$

$\therefore$  if  $p \equiv 1 \pmod{8}$ , Then  $p \equiv 1 \pmod{4}$

if  $p \equiv 1 \pmod{24}$ , Then  $p \equiv 1 \pmod{4}$ ,  $p \equiv 1 \pmod{8}$ , and  $p \equiv 1 \pmod{6}$ .

$\therefore$  Consider  $p = 1 + 24k$ , for  $k=1, 2, 3, \dots$   
 $\therefore$  Look at 25, 49, 73, ...

73 is prime and  $73 \equiv 1 \pmod{4}$ ,  $73 \equiv 1 \pmod{8}$ ,  
and  $73 \equiv 1 \pmod{6}$ .

To clean up,

$$8^2 + 3^2 = 73$$
$$1^2 + 2(6)^2 = 73$$
$$5^2 + 3(4)^2 = 73$$

These were obtained by trial + error, but  
could have chosen different prime  
s.t.  $p = 1 + 24k$  and then chosen  
 $x, y$  s.t.  $(\frac{x}{y})^2$  is an integer, etc.

9. If  $p$  and  $q$  are odd primes satisfying  $p = q + 4a$   
for some  $a$ , establish that  $(a/p) = (a/q)$ , and  
in particular, that  $(6/37) = (6/13)$

Pf: Since  $p = q + 4a$ ,  $(p/q) = (q + 4a/q)$

But  $q + 4a \equiv 4a \pmod{q}$ , so  $(q + 4a/q) = (4a/q)$   
 $= (2^2 a/q) = (a/q)$ .

$\therefore (p/q) = (a/q)$  [13]

$$\text{Similarly, } q = p - 4a, \text{ so } (q/p) = (p-4a/p) = (-a/p)$$

$$\therefore (q/p) = (-a/p) = (-1/p)(a/p) \quad [2]$$

If  $p \equiv 1 \pmod{4}$ , Then  $(-1/p) = 1$ , [2] becomes

$$(q/p) = (a/p) \quad [2']$$

But by corollary 2 to Th. 9.9 (p. 128),  
 $(p/q) = (q/p)$ .

$$\therefore \text{By [1] and [2'], } (a/q) = (a/p)$$

If  $p \equiv 3 \pmod{4}$ , Then  $(-1/p) = -1$ , [2] becomes

$$(q/p) = -(a/p) \quad [2'']$$

Note that  $p \equiv 4a + q \pmod{4} \Rightarrow p \equiv q \pmod{4}$

$$\therefore q \equiv 3 \pmod{4}$$

$\therefore$  By corollary 2 to Th. 9.9,  $(p/q) = -(q/p)$

$$\therefore \text{By [1] and [2''], } (q/q) = (p/q) = -(q/p) = -(-a/p)$$

$$\therefore (a/q) = (q/p).$$

10. Establish each of the following assertions:

(a)  $(5/p) = 1 \iff p \equiv 1, 9, 11, \text{ or } 19 \pmod{20}$

Pf: By def. of  $(5/p)$ ,  $p$  is an odd prime.

(1) If  $p \equiv 1, 9, 11, \text{ or } 19 \pmod{20}$ , Then

$$\begin{aligned} p &\equiv 1, 9, 11, \text{ or } 19 \pmod{5} \Rightarrow \\ p &\equiv 1 \text{ or } 4 \pmod{5} \end{aligned}$$

Since  $5 \equiv 1 \pmod{4}$ , Then  $(5/p) = (p/5)$

$$\therefore (5/p) = (p/5) = (1/5) \text{ or } (4/5) = (1/5)$$

and  $(1/5) = 1$ .

$$\therefore (5/p) = 1.$$

(2) Suppose  $(5/p) = 1$ . Since  $5 \equiv 1 \pmod{4}$ ,

Then  $(5/p) = (p/5) = 1$ .

$$\therefore 1 \equiv p^{\frac{5-1}{2}} \pmod{5}, \text{ or } 1 \equiv p^2 \pmod{5}.$$

$$\therefore p \equiv 1 \text{ or } 4 \pmod{5}.$$

Also, general for any odd number,  
 $p \equiv 1 \text{ or } 3 \pmod{4}$ .

$$\therefore p \equiv 1 \pmod{5} \text{ or } p \equiv 4 \pmod{5}$$

and  $p \equiv 1 \pmod{4} \text{ or } p \equiv 3 \pmod{4}$

$\therefore 4\rho \equiv 4 \pmod{20}$  or  $4\rho \equiv 16 \pmod{20}$   
and  $5\rho \equiv 5 \pmod{20}$  or  $5\rho \equiv 15 \pmod{20}$

Subtracting,  $\rho \equiv 1$  or  $-11 \pmod{20}$   
or  $\rho \equiv 11$  or  $-1 \pmod{20}$

$$\Rightarrow \rho \equiv 1, 9, 11, \text{ or } 19 \pmod{20}$$

$$(6/\rho) = 1 \iff \rho \equiv 1, 5, 19, \text{ or } 23 \pmod{24}$$

Pf: (1) Suppose  $\rho \equiv 1, 5, 19, \text{ or } 23 \pmod{24}$

Let  $\rho \equiv 1 \pmod{24}$

$\because \rho \equiv 1 \pmod{12} \Rightarrow (3/\rho) = 1 \quad (\text{Th. 9.10})$

and  $\rho \equiv 1 \pmod{8} \Rightarrow (2/\rho) = 1 \quad (\text{Th. 9.6})$

$$\therefore (6/\rho) = (3/\rho)(2/\rho) = 1$$

Let  $\rho \equiv 5 \pmod{24}$

$\therefore \rho \equiv 5 \pmod{12} \Rightarrow (3/\rho) = -1 \quad (\text{Th. 9.10})$

$\rho \equiv 5 \pmod{8} \Rightarrow (2/\rho) = -1 \quad (\text{Th. 9.6})$

$$\therefore (6/\rho) = (3/\rho)(2/\rho) = (-1)(-1) = 1$$

Let  $\rho \equiv 19 \pmod{24}$

$$\begin{aligned}\therefore \rho \equiv 19 &\equiv 7 \equiv -5 \pmod{12} \Rightarrow (3/\rho) = -1 \\ \rho \equiv 19 &\equiv 3 \pmod{8} \Rightarrow (2/\rho) = -1\end{aligned}$$

$$\therefore (6/\rho) = (3/\rho)(2/\rho) = (-1)(-1) = 1$$

Let  $\rho \equiv 23 \pmod{24}$

$$\begin{aligned}\therefore \rho \equiv 23 &\equiv 11 \equiv -1 \pmod{12} \Rightarrow (3/\rho) = 1 \\ \rho \equiv 23 &\equiv 7 \pmod{8} \Rightarrow (2/\rho) = 1\end{aligned}$$

$$\therefore (6/\rho) = (3/\rho)(2/\rho) = 1$$

(2) Suppose  $(6/\rho) = 1$

$$\therefore (3/\rho)(2/\rho) = 1 \Rightarrow$$

$$(3/\rho) = 1 \text{ and } (2/\rho) = 1$$

$$\text{or } (3/\rho) = -1 \text{ and } (2/\rho) = -1$$

(a) If  $(3/\rho) = 1$  Then  $\rho \equiv \pm 1 \pmod{12}$

By Th. 9.10, for  $\rho \not\equiv 3 \text{ or } 9 \pmod{12}$ ,  
since Then  $3/\rho$ .

Also,  $(2/\rho) = 1 \Rightarrow \rho \equiv \pm 1 \pmod{8}$

By Th. 9.6

(i)  $\rho \equiv 1 \pmod{12}$  and  $\rho \equiv 1 \pmod{8} \Rightarrow$

$$\begin{cases} 2\rho \equiv 2 \pmod{24} \\ 3\rho \equiv 3 \pmod{24} \end{cases} \Rightarrow \rho \equiv 1 \pmod{24}$$

by subtracting

$$(2) \rho \equiv 1 \pmod{12} \text{ and } \rho \equiv -1 \pmod{8} \Rightarrow$$

$$\begin{cases} 2\rho \equiv 2 \pmod{24} \\ 3\rho \equiv -3 \pmod{24} \end{cases} \Rightarrow \rho \equiv -5 \Rightarrow$$

$\rho \equiv 19 \pmod{24}$

$$(3) \rho \equiv -1 \pmod{12} \text{ and } \rho \equiv 1 \pmod{8} \Rightarrow$$

$$\begin{cases} 2\rho \equiv -2 \pmod{24} \\ 3\rho \equiv 3 \pmod{24} \end{cases} \Rightarrow \rho \equiv 5 \pmod{24}$$

$$(4) \rho \equiv -1 \pmod{12} \text{ and } \rho \equiv -1 \pmod{8} \Rightarrow$$

$$\begin{cases} 2\rho \equiv -2 \pmod{24} \\ 3\rho \equiv -3 \pmod{24} \end{cases} \Rightarrow \rho \equiv -1 \Rightarrow$$

$\rho \equiv 23 \pmod{24}$

$$\therefore (6/\rho) = 1 \Rightarrow \rho = 1, 5, 19, \text{ or } 23 \pmod{24}$$

$$(c) (7/\rho) = 1 \Leftrightarrow \rho \equiv 1, 3, 9, 19, 25, \text{ or } 27 \pmod{28}$$

Pf: (1) Suppose  $(7/\rho) = 1$

(a) If  $\rho \equiv 1 \pmod{4}$ , Then  $(7/\rho) = (\rho/7)$

$$\therefore 1 \equiv \rho^{\frac{7-1}{2}} \equiv \rho^3 \pmod{7}$$

$\therefore$  running through  $\rho \equiv 1, 2, 3, 4, 5, 6$   
and looking at  $\rho^3$ , we get

$$p \equiv 1, 2, \text{ or } 4 \pmod{7}$$

$$\therefore p \equiv 1 \pmod{4} \text{ and } p \equiv 1, 2, \text{ or } 4 \pmod{7}$$

$$(1) \begin{cases} p \equiv 1 \pmod{4} \\ p \equiv 1 \pmod{7} \end{cases} \Rightarrow \begin{cases} 7p \equiv 7 \pmod{28} \\ 4p \equiv 4 \pmod{28} \end{cases} \Rightarrow 8p \equiv 8 \pmod{28} \\ \therefore \underline{\underline{p \equiv 1 \pmod{28}}}$$

$$(2) \begin{cases} p \equiv 1 \pmod{4} \\ p \equiv 2 \pmod{7} \end{cases} \Rightarrow \begin{cases} 7p \equiv 7 \pmod{28} \\ 4p \equiv 8 \pmod{28} \end{cases} \Rightarrow 8p \equiv 16 \pmod{28} \\ \therefore \underline{\underline{p \equiv 9 \pmod{28}}}$$

$$(3) \begin{cases} p \equiv 1 \pmod{4} \\ p \equiv 4 \pmod{7} \end{cases} \Rightarrow \begin{cases} 7p \equiv 7 \pmod{28} \\ 4p \equiv 16 \pmod{28} \end{cases} \Rightarrow 8p \equiv 32 \pmod{28} \\ \therefore \underline{\underline{p \equiv 25 \pmod{28}}}$$

(1) If  $p \equiv 3 \pmod{4}$ , then  $(7/p) = -(\rho/7)$   
since  $7 \equiv 3 \pmod{4}$

$$\therefore -1 \equiv p^{\frac{7-1}{2}} \equiv p^3 \pmod{7}$$

$$\therefore p \equiv 3, 5, \text{ or } 6 \pmod{7} \Rightarrow \begin{cases} 4p \equiv 12, 20, \text{ or } 24 \pmod{28} \\ 8p \equiv 24, 40, \text{ or } 48 \pmod{28} \end{cases}$$

$$p \equiv 3 \pmod{4} \Rightarrow 7p \equiv 21 \pmod{28}$$

$$(1) \begin{cases} 7p \equiv 21 \pmod{28} \\ 8p \equiv 24 \pmod{28} \end{cases} \left\{ \begin{array}{l} p \equiv 3 \pmod{28} \\ p \equiv 1 \pmod{28} \end{array} \right.$$

$$(2) \begin{cases} 7p \equiv 21 \pmod{28} \\ 8p \equiv 40 \pmod{28} \end{cases} \left\{ \begin{array}{l} p \equiv 19 \pmod{28} \\ p \equiv 11 \pmod{28} \end{array} \right.$$

$$(3) \begin{cases} 7p \equiv 21 \pmod{28} \\ 8p \equiv 48 \pmod{28} \end{cases} \left\{ \begin{array}{l} p \equiv 27 \pmod{28} \\ p \equiv 13 \pmod{28} \end{array} \right.$$

$$\therefore (7/p) = 1 \Rightarrow p \equiv 1, 3, 9, 19, 25, \text{ or } 27 \pmod{28}$$

(2) Suppose  $p \equiv 1, 3, 9, 19, 25, \text{ or } 27 \pmod{28}$

By def. of  $(7/p)$ ,  $p$  is an odd prime.

Also, note  $7 \equiv 3 \pmod{4}$

a) If  $p \equiv 3, 19, \text{ or } 27 \pmod{28}$ , Then  
 $p \equiv 3, 19, \text{ or } 27 \pmod{4}$ , so  $p \equiv 3 \pmod{4}$

$$\therefore (7/p) = -(\rho/7) \quad (\text{corollary 1, p. 198})$$

Also,  $p \equiv 3, 19, \text{ or } 27 \pmod{7} \Rightarrow$   
 $p \equiv 3, 5, 6 \pmod{7}$

$$\therefore (\rho/7) = (3/7), (5/7), \text{ or } (6/7)$$

$$(3/7) = -(7/3) = -(1/3) = -1$$

$$(5/7) = (7/5) = (2/5) = -1$$

$$(6/7) = (3/7)(2/7) = (-1)(1) = -1$$

$$\therefore (\rho/7) = -1$$

$$\therefore (7/\rho) = -(\rho/7) = 1$$

(b) If  $\rho \equiv 1, 9, \text{ or } 25 \pmod{28}$ , Then  
 $\rho \equiv 1, 9, \text{ or } 25 \pmod{4}$ , so  $\rho \equiv 1 \pmod{4}$

$$\therefore (7/\rho) = (\rho/7) \quad (\text{corollary 1, p. 198})$$

Also,  $\rho \equiv 1, 9, 25 \pmod{7}$

$$\therefore (\rho/7) = (1/7), (9/7), (25/7)$$

$$= 1, (2/7), (4, 7) \\ = 1, 1, 1$$

$$\therefore (7/\rho) = (\rho/7) = 1.$$

$$\therefore \rho \equiv 1, 3, 9, 19, 25, 27 \pmod{28} \Rightarrow (7/\rho) = 1$$

11. Prove that there are infinitely many primes of the form  $5K-1$ .

Pf: Assume finitely many primes of form  $5K-1$ . Call them  $p_1, p_2, \dots, p_r$ , where  $p_r > p_i, 1 \leq i < r$ .

Consider the integer  $M = 5(n!)^2 - 1$ . For  $n \geq 1$ ,  $M$  is odd, since  $n!$  is even as it contains 2.  $\therefore M$  has an odd prime divisor.

Note that any odd prime divisor  $p$  of  $M$  must be s.t.  $p > n$ ; for if  $p \leq n$ , then  $p | n!$ , so  $p | M$  and  $p | 5(n!)^2 \Rightarrow p | 1$ , a contradiction.

$\therefore$  For  $N = 5(p_r!)^2 - 1$ , let  $p$  be any odd prime divisor.  $\therefore p > p_r$  and  $p$  cannot be of form  $5K-1$ .

$$\therefore 5(p_r!)^2 \equiv 1 \pmod{p} \Leftrightarrow 25(p_r!)^2 \equiv 5 \pmod{p} \quad [1]$$

since  $p > p_r \geq 19 = 5K-1$  for  $k=4$ .

$$\therefore \gcd(5, p) = 1.$$

$$\therefore [1] \Rightarrow (5/p) = 1$$

But from prob. 10(a) above,  $p \equiv 1, 9, 11, \text{ or } 19 \pmod{20}$   
 $\Rightarrow p \equiv 1, 9, 11, 19 \pmod{5} \Rightarrow$   
 $p \equiv 1 \text{ or } 4 \pmod{5}$

if  $p \equiv 4 \pmod{5}$ , Then  $p \equiv -1 \pmod{5} \Rightarrow$   
 $p = 5k-1$ , some  $k$ . This can't be  
since  $p > p_r$  and  $p_r$  is the largest  
prime of form  $5k-1$ .

$\therefore p \equiv 1 \pmod{5}$ , or  $p = 5k+1$

Since  $p$  is any odd prime divisor of  $N$ ,  
Then

$$N = (5k_1 + 1)^{n_1} (5k_2 + 1)^{n_2} \dots (5k_s + 1)^{n_s}$$

But  $(5k_i + 1)^{n_i}$  is of form  $5k'_i + 1$ ,  
so  $N$  is of form  $5k'' + 1$ .

But this contradicts  $N = 5(p_r!)^2 - 1$   
of form  $5k-1$ .

(if  $5k-1 = 5k'' + 1$ , Then  $5(k-k'') = 2 \Rightarrow 5/2$ ).

$\therefore$  Assumption of finite number of primes of  
form  $5k-1$  is false.

12. Verify the following:

(a) The prime divisors  $p \neq 3$  of the integer  $n^2 - n + 1$  are of form  $6k + 1$ .

Pf: First note  $n^2 - n + 1$  is odd for all  $n \geq 1$ .

For if  $n$  is odd,  $n^2$  is odd, so  $n^2 - n$  is even, so  $n^2 - n + 1$  is odd.

If  $n$  is even,  $n^2$  is even,  $n^2 - n$  is even, so  $n^2 - n + 1$  is odd.

- prime divisors  $p$  of  $n^2 - n + 1 \neq 2$ .  
With assumption  $p \neq 3$ , Then  $p \geq 3$ .

If  $p | n^2 - n + 1$ , Then  $p | 4n^2 - 4n + 4$ .

$$(2n-1)^2 = 4n^2 - 4n + 1$$

$$\therefore p | [(2n-1)^2 + 3]$$

$$\therefore (2n-1)^2 \equiv -3 \pmod{p} \Rightarrow (-3/p) = 1$$

$\therefore p \equiv 0, 1, 2, 3, 4, 5 \pmod{6}$ .

If  $p \equiv 0, 2, 4 \pmod{6}$ , Then  $p \equiv 0, 2, 4 \pmod{2}$   
 $\Rightarrow 2 | p$ , which can't be since  $p \geq 3$ .

If  $p \equiv 3 \pmod{6}$ , Then  $p \equiv 3 \pmod{3} \Rightarrow 3 | p$ , which can't be since  $p \geq 3$ .

$\therefore p \equiv 1 \text{ or } 5 \pmod{6}$ . By prob. 5(a) above,  
 $p \equiv 1 \pmod{6}$ ; for  $p \equiv 5 \Rightarrow (-3/p) = -1$ .

$\therefore p \equiv 1 \pmod{6} \Rightarrow p = 1 + 6k, \text{ some } k$ .

(b) The prime divisors  $p \neq 5$  of the integer  $n^2 + n - 1$  are of the form  $10k + 1$  or  $10k + 9$ .

Pf: If  $p \mid n^2 + n - 1$ , Then  $p \mid 4n^2 + 4n - 4$ .

$$(2n+1)^2 - 5 = 4n^2 + 4n - 4.$$

$$\begin{aligned} \therefore p \mid n^2 + n - 1 &\Rightarrow p \mid (2n+1)^2 - 5 \\ &\Rightarrow (2n+1)^2 \equiv 5 \pmod{p}. \end{aligned}$$

If  $p \neq 5$ , Then  $\gcd(p, 5) = 1$ , so  $(5/p)$  is defined.

$\therefore$  If  $p \neq 5$ ,  $p \mid n^2 + n - 1 \Rightarrow (5/p) = 1$

By Prob. 10(a),  $p \equiv 1, 9, 11, 19 \pmod{20}$

$$\Rightarrow p \equiv 1, 9, 11, 19 \pmod{10}$$

$$\Rightarrow p \equiv 1 \text{ or } 9 \pmod{10}$$

$$\Rightarrow p = 1 + 10k \text{ or } p = 9 + 10k, \text{ some } k.$$

(c) The prime divisors  $p$  of the integer  $2n(n+1)+1$  are of the form  $p \equiv 1 \pmod{4}$ .

$$\text{Pf: } 2n(n+1)+1 = 2n^2 + 2n + 1$$

$$\text{If } p \mid 2n(n+1)+1, \text{ Then } p \mid 4n^2 + 4n + 2 \Rightarrow$$

$$p \mid (2n+1)^2 + 1 \Rightarrow (2n+1)^2 \equiv -1 \pmod{p}$$

$$\therefore p \mid 2n(n+1)+1 \Rightarrow (-1/p) = 1$$

$$\Rightarrow p \equiv 1 \pmod{4}$$

by corollary on p. 187.

(d) The prime divisors  $p$  of the integer  $3n(n+1)+1$  are of the form  $p \equiv 1 \pmod{6}$

$$\text{Pf: } 3n(n+1)+1 = 3n^2 + 3n + 1$$

$$\therefore p \mid 3n(n+1)+1 \Rightarrow p \mid 36n^2 + 36n + 12$$

$$\Rightarrow p \mid (6n+3)^2 + 3$$

$$\Rightarrow (6n+3)^2 \equiv -3 \pmod{p} [1]$$

Note that if  $n$  is even or odd,  $n(n+1)$  is even.  $\therefore 3n(n+1) + 1$  is odd, so  $p \neq 2$ .  
 If  $p = 3$ , Then  $p | 3n(n+1) + 1 \Rightarrow p | 1$ .  
 $\therefore p \neq 3$ .

$\therefore p > 3$ , so  $\gcd(-3, p) = 1$ , so

$$\{1\} \Rightarrow (-3/p) = 1.$$

By prob. 5(a),  $p \equiv 1 \pmod{6}$ .

13. (a) Show that if  $p$  is a prime divisor of  $839 = 38^2 - 5 \cdot 11^2$ , Then  $(5/p) = 1$ . Use this fact to conclude that  $839$  is a prime number.

Pf: (1) If  $p | 38^2 - 5 \cdot 11^2$ , Then

$$38^2 - 5 \cdot 11^2 \equiv 0 \pmod{p} \Leftrightarrow 38^2 \equiv 5 \cdot 11^2 \pmod{p}$$

$\therefore 38$  is a solution to  $x^2 \equiv 5 \cdot 11^2 \pmod{p}$ , and so  $(5 \cdot 11^2/p) = 1 \Rightarrow (5/p)(11^2/p) = 1 \Rightarrow (5/p) = 1$ .

(2) Since  $29^2 = 841 > 839$  only need to consider primes  $< 29$  (discussion p. 45).

By prob. 10 (a),  $(5/p) = 1 \Rightarrow$   
 $p \equiv 1, 9, 11, 19 \pmod{20} \Rightarrow$   
 $p \equiv 1, 9, 11, 19 \pmod{10} \Rightarrow$   
 $p \equiv 1, 9 \pmod{10} \Rightarrow p = 11 \text{ or } 19$

If  $19 \mid 38^2 - 5 \cdot 11^2$ , Then  $19 \mid 5 \cdot 11^2$ .

If  $11 \mid 38^2 - 5 \cdot 11^2$ , Then  $11 \mid 38^2$ .

Both of these are false, so there is no prime  $p$  s.t.  $(5/p) = 1$ .

$\therefore (5/p) \neq 1$ , assumption that 839 is divisible by a prime is false  
 $\Rightarrow 839$  is prime.

(b) Prove that both  $397 = 20^2 - 3$  and  $233 = 29^2 - 3 \cdot 6^2$  are primes.

$$(1) 397 = 20^2 - 3$$

Assume there is a prime divisor  $p$  s.t.  $p \mid 397$ .  
Since  $20^2 = 400$ , only consider  $p < 20$ .

$$\therefore 20^2 \equiv 3 \pmod{p} \Rightarrow (3/p) = 1.$$

By Th. 9.10,  $p \equiv \pm 1 \pmod{12}$

$$\therefore p = 11 \text{ or } 13.$$

But  $11 \nmid 397$  and  $13 \nmid 397$ , so there is

no  $p$  s.t.  $p \mid 387 \Rightarrow 387$  is prime.

$$(2) 733 = 29^2 - 3 \cdot 6^2$$

Assume There is a prime  $p$  s.t.  $p \mid 733$ .  
 $28^2 = 784$ , so just consider  $p < 28$ .

$$29^2 \equiv 3 \cdot 6^2 \pmod{p} \Rightarrow (3 \cdot 6^2/p) = 1 \Rightarrow (3/p) = 1$$

$\therefore$  By Th. 9.10,  $p \equiv \pm 1 \pmod{12}$ .

$\therefore p = 11, 13, \text{ or } 23$ .

But  $11 \nmid 733$ ,  $13 \nmid 733$ , and  $23 \nmid 733$ .

$\therefore$  no prime  $p$  s.t.  $p \mid 733 \Rightarrow 733$  is prime.

14. Solve the quadratic congruence  $x^2 \equiv 11 \pmod{35}$

Since  $35 = 5 \cdot 7$ ,  $x$  is a solution  $\Leftrightarrow x$  is a solution to:  $x^2 \equiv 11 \pmod{5}$  and  $x^2 \equiv 11 \pmod{7}$

$$\therefore x^2 \equiv 11 \pmod{5} \Leftrightarrow x^2 \equiv 1 \pmod{5}$$

$$\Leftrightarrow x \equiv \pm 1 \pmod{5}$$

$$x^2 \equiv 11 \pmod{7} \Leftrightarrow x^2 \equiv 4 \pmod{7}$$

$$\Leftrightarrow x \equiv \pm 2 \pmod{7}$$

$$\therefore (a) \quad x \equiv 1 \pmod{5} \text{ and } x \equiv 2 \pmod{7}$$

(b)  $x \equiv 1 \pmod{5}$  and  $x \equiv -2 \pmod{7}$

(c)  $x \equiv -1 \pmod{5}$  and  $x \equiv 2 \pmod{7}$

(d)  $x \equiv -1 \pmod{5}$  and  $x \equiv -2 \pmod{7}$

For all of these,  $n = 5 \cdot 7$ ,  $N_1 = 7$ ,  $N_2 = 5$

$$\therefore 7x_1 \equiv 1 \pmod{5} \quad 5x_2 \equiv 1 \pmod{7}$$

$$2x_1 \equiv 1, \quad 6x_1 \equiv 3$$

$$x_1 \equiv 3$$

$$15x_2 \equiv 3$$

$$x_2 \equiv 3$$

(a)  $x \equiv 1 \pmod{5}$  and  $x \equiv 2 \pmod{7}$

$$\begin{aligned}\therefore x &= 1 \cdot 7 \cdot 3 + 2 \cdot 5 \cdot 3 = 51 \pmod{35} \\ &\equiv \underline{16} \pmod{35}\end{aligned}$$

(b)  $x \equiv 1 \pmod{5}$  and  $x \equiv -2 \pmod{7}$

$$\therefore x = 1 \cdot 7 \cdot 3 + (-2) \cdot 5 \cdot 3 = -9 \equiv \underline{26} \pmod{35}$$

(c)  $x \equiv -1 \pmod{5}$  and  $x \equiv 2 \pmod{7}$

$$\therefore x = (-1) \cdot 7 \cdot 3 + 2 \cdot 5 \cdot 3 = 9 \equiv \underline{9} \pmod{35}$$

(d)  $x \equiv -1 \pmod{5}$  and  $x \equiv -2 \pmod{7}$

$$\therefore x = (-1) \cdot 7 \cdot 3 + (-2) \cdot 5 \cdot 3 = -51 \equiv \underline{19} \pmod{35}$$

$$\therefore x \equiv 9, 16, 19, \text{ or } 26 \pmod{35}$$

15. Establish that 7 is a primitive root of any prime of the form  $2^{4n} + 1$ .

Pf: For  $n=0$ ,  $2^{4n}+1 = 2$ ,  $\phi(2) = 1$ ,  $7^1 = 7$ , and  $7 \equiv 1 \pmod{2}$ , so you could say 7 (and every odd integer) is a primitive root of 2.

So assume  $n > 0$ .  $\therefore 2^{4n}+1$  is odd

By prob. 7 of section 9.1 (p. 184), every quadratic non-residue of prime  $p = 2^k + 1$  is a primitive root of  $p$ .

$2^{4n}+1$  is of form  $2^k+1$ , so just need to show 7 is a quadratic nonresidue of prime  $p = 2^{4n}+1$ . i.e.,  $(7/p) = -1$ .

Note that for  $n=3k$ ,  $2^{4n}+1$  is not prime, for  $2^{4n}+1 = 2^{12k}+1 = (2^{4k})^3+1$  which

can be factored to  $(2^{4k}+1)[(2^{4k})^2 - 2^{4k} + 1]$

$\therefore 2^{4n}+1$  can only be prime if  $n = 3k+1$   
or  $n = 3k+2$ , for  $k = 0, 1, 2, \dots$

Note:  $2^{4n}+1 = 2^{2 \cdot 2n}+1 = 4^{2n}+1 \equiv 1 \pmod{4}$ .

$\therefore (7/p) = (p/7)$ , by corollary 2, p. 198.

$\therefore$  need to show  $(p/7) = -1$  for  $n = 3k+1$   
or  $n = 3k+2$ ,  $k = 0, 1, 2, \dots$ , assuming  $p$  prime

$n = 3k+1$ : Look at  $(2^{4(3k+1)}+1) \pmod{7}$ , and  
note  $8 \equiv 1 \pmod{7}$

$$\begin{aligned} 2^{4(3k+1)}+1 &= 2^{3(3k+1)} \cdot 2^{(3k+1)}+1 \\ &= (8^{3k+1})(8^k \cdot 2)+1 \\ &\equiv (1)(1 \cdot 2)+1 \equiv 3 \pmod{7} \end{aligned}$$

$$\therefore (2^{4(3k+1)}+1/7) = (3/7) = -(7/3) = -(1/3) = -1$$

$$\begin{aligned} n = 3k+2: 2^{4(3k+2)}+1 &= 2^{3(3k+2)} \cdot 2^{3k+2}+1 \\ &= (8^{3k+2})(8^k \cdot 4)+1 \end{aligned}$$

$$\begin{aligned} &\equiv (1)(1 \cdot 4)+1 \equiv 5 \pmod{7} \\ \therefore (2^{4(3k+2)}+1/7) &= (5/7) = (7/5) = (2/5) = -1 \end{aligned}$$

$\therefore$  When  $2^{4^n} + 1$  is prime,  $(p/7) = -1$ , so  $(7/p) = -1$ , so 7 is a quadratic nonresidue, and  $\therefore$  by prob. 7, section 9.1, 7 is a primitive root of  $2^{4^n} + 1$ .

16. Let  $a$  and  $b > 1$  be relatively prime integers, with  $b$  odd. If  $b = p_1 p_2 \cdots p_r$  is the decomposition of  $b$  into odd primes (not necessarily distinct), Then the Jacobi symbol  $(a/b)$  is defined by

$$(a/b) = (a/p_1)(a/p_2) \cdots (a/p_r)$$

where  $(a/p_i)$  is the Legendre symbol.

Evaluate  $(21/221)$ ,  $(215/253)$ ,  $(631/1098)$

$$(a) (21/221) \quad 221 = 13 \cdot 17$$

$$\begin{aligned}\therefore (21/221) &= (21/13)(21/17) \\ &= (3/13)(7/13)(3/17)(7/17) \\ &= (13/3)(13/7)(17/3)(17/7) \\ &= (1/3)(6/7)(2/3)(3/7)\end{aligned}$$

$$\begin{aligned}
 &= (1)(3/7)(2/7)(-1)(3/7) \\
 &= (-1)(3^2/7)(2/7) = (-1)(1)(1) = -1 \\
 \therefore \underline{(21/22)} &= -1
 \end{aligned}$$

(b)  $(215/253)$   $253 = 11 \cdot 23$ ,  $215 = 5 \cdot 43$

$$\begin{aligned}
 \therefore (215/253) &= (215/11)(215/23) \\
 &= (5/11)(43/11)(5/23)(43/23) \\
 &= (11/5)(10/11)(23/5)(20/23) \\
 &= (1/5)(2/11)(5/11)(3/5)(4/23)(5/23) \\
 &= (1)(-1)(1)(5/3)(1)(23/5) \\
 &= (-1)(2/3)(3/5) \\
 &= (-1)(-1)(5/3) = (2/3) = -1
 \end{aligned}$$

$$\therefore \underline{(215/253)} = -1$$

(c)  $(631/1099)$   $1099 = 7 \cdot 157$ ,  $631$  is prime

$$\begin{aligned}
 \therefore (631/1099) &= (631/7)(631/157) \\
 &= (1/7)(3/157) \\
 &= (1)(157/3) = (1/3) = 1
 \end{aligned}$$

$$\therefore \underline{(631/1099)} = 1$$

17. Under the hypothesis of the previous problem, show that if  $a$  is a quadratic residue of  $b$ , then  $(a/b) = 1$ ;

but the converse is false.

PF: (a) Assume  $x^2 \equiv a \pmod{6}$  has a solution.

Let  $b = p_1 p_2 \dots p_r$ , and note  $\gcd(a, b) = 1$

$$\therefore x^2 \equiv a \pmod{p_1}, x^2 \equiv a \pmod{p_2}, \dots, x^2 \equiv a \pmod{p_r}$$

and note  $\gcd(a, p_i) = 1$ .

$$\begin{aligned} \therefore (a/p_i) &= 1, \quad \therefore (a/b) = (a/p_1)(a/p_2) \dots (a/p_r) \\ &= (1)(1) \dots (1) = 1. \end{aligned}$$

(b) Now assume  $(a/b) = 1$  and let  $b = p_1 p_2$

$$\therefore (a/b) = (a/p_1)(a/p_2).$$

$\therefore$  it may be that  $(a/p_1) = (a/p_2) = -1$

$\therefore$  there would not be a solution to  
 $x^2 \equiv a \pmod{b}$ .

As a concrete example,  $(2/3) = -1$  and

$$(2/5) = -1. \quad \therefore (2/15) = 1,$$

but  $x^2 \equiv 2 \pmod{15}$  can't have a solution.

If it did, then so would  $x^2 \equiv 2 \pmod{3}$

18. Prove That The following properties of The Jacobi hold: If  $b$  and  $b'$  are positive odd integers and  $\gcd(aa', bb') = 1$ , Then

(a)  $a \equiv a' \pmod{b}$  implies that  $(a/b) = (a'/b)$

Pf: Let  $b = p_1 p_2 \dots p_r$  be The decomposition of  $b$  into odd primes (not necessarily distinct). Then by def. of  $(a/b)$ , where  $(a/p_i)$  is The Legendre symbol,

$$(a/b) = (a/p_1)(a/p_2) \dots (a/p_r)$$

From  $\gcd(aa', bb') = 1$ , we get  
 $\gcd(a, p_i) = 1$  and  $\gcd(a', p_i) = 1$ .

From  $a \equiv a' \pmod{b}$ , we get  $a \equiv a' \pmod{p_i}$

$\therefore$  from Th. 9.2,  $(a/p_i) = (a'/p_i)$ .

$$\therefore (a/p_1) \dots (a/p_r) = (a'/p_1) \dots (a'/p_r)$$

$$\therefore (a/b) = (a'/b)$$

$$(b) (aa'/b) = (a/b)(a'/b)$$

As in (a) above, let  $b = p_1 p_2 \dots p_r$ .

Note that  $\gcd(aa', bb') = 1 \Rightarrow \gcd(a/b) = 1$  and  $\gcd(a'/b) = 1$ .

Using Th. 9.2,

$$\begin{aligned} (aa'/b) &= (aa'/p_1)(aa'/p_2) \dots (aa'/p_r) \\ &= (a/p_1)(a'/p_1)(a/p_2)(a'/p_2) \dots (a/p_r)(a'/p_r) \\ &= (a/p_1)(a/p_2) \dots (a/p_r) \cdot (a'/p_1)(a'/p_2) \dots (a'/p_r) \\ &= (a/b)(a'/b) \end{aligned}$$

$$(c) (a/bb') = (a/b)(a/b')$$

First note  $\gcd(aa', bb') = 1 \Rightarrow \gcd(a/b) = 1$  and  $\gcd(a/b') = 1$ .

As in (a), let  $b = p_1 p_2 \dots p_r$  and let

$$b' = p'_1 p'_2 \dots p'_r \therefore bb' = p_1 p_2 \dots p_r p'_1 p'_2 \dots p'_r$$

$$\therefore (a/bb') = (a/p_1)(a/p_2) \dots (a/p_r)(a/p'_1)(a/p'_2) \dots (a/p'_r)$$

$$= (a/b)(a/b')$$

$$(d) \quad (a^2/b) = (a/b^2) = 1$$

From (b), letting  $a' = a$ ,

$$\begin{aligned} (a^2/b) &= (a \cdot a/b) = (a/b)(a/b) \\ &= (a/p_1) \cdots (a/p_r)(a/p_1) \cdots (a/p_r) \\ &= (a/p_1)^2 \cdots (a/p_r)^2 = 1 \cdots 1 = 1 \end{aligned}$$

Similarly, letting  $b = b'$  in (c),

$$(a/b^2) = (a/b)(a/b) = 1 \text{ as above.}$$

$$(e) \quad (1/b) = 1$$

This follows from (d) letting  $a = 1$   
so that  $1 = (a^2/b) = (1^2/b) = (1/b)$

$$(f) \quad (-1/b) = (-1)^{(b-1)/2}$$

If  $b = p_1 p_2 \cdots p_r$ , Then by def., and using  
Th. 9.2,

$$(-1/b) = (-1/p_1)(-1/p_2) \cdots (-1/p_r)$$

$$= (-1)^{(p_1-1)/2} (-1)^{(p_2-1)/2} \cdots (-1)^{(p_r-1)/2} [1]$$

Now use the hint: if  $u$  and  $v$  are odd integers,  
Then  $u = 2r+1$ ,  $v = 2s+1$ , some  $r, s$ .

$$\therefore \frac{u-1}{2} = r, \frac{v-1}{2} = s.$$

$$\begin{aligned} \frac{uv-1}{2} &= \frac{(2r+1)(2s+1)-1}{2} = \frac{4rs + 2r + 2s}{2} \\ &= 2rs + r + s \end{aligned}$$

$$\therefore r+s \equiv r+s \pmod{2} \Rightarrow$$

$$r+s \equiv 2rs + r + s \pmod{2} \Rightarrow$$

$$\frac{u-1}{2} + \frac{v-1}{2} \equiv \frac{uv-1}{2} \pmod{2}$$

$\therefore \left[ \frac{u-1}{2} + \frac{v-1}{2} \right]$  and  $\left[ \frac{uv-1}{2} \right]$  must both  
be odd, or both must be even.

$$\therefore (-1)^{\left[ \frac{u-1}{2} + \frac{v-1}{2} \right]} = (-1)^{\left[ \frac{uv-1}{2} \right]}$$

$$\therefore [1] \text{ becomes } (-1)^{\left[ \frac{p_1-1}{2} \right]} (-1)^{\left[ \frac{p_2-1}{2} \right]} \cdots (-1)^{\left[ \frac{p_r-1}{2} \right]}$$

$$= (-1)^{\left[ \frac{p_1 p_2 - 1}{2} \right]} \cdots (-1)^{\left[ \frac{p_r - 1}{2} \right]}$$

$$= (-1)^{\left[ \frac{p_1 p_2 \cdots p_r - 1}{2} \right]} = (-1)^{\frac{b-1}{2}}$$

$$\therefore (-1/6) = (-1)^{(6-1)/2}$$

$$(g) (2/6) = (-1)^{(5^2-1)/8}$$

$$\text{Let } 6 = p_1 \cdots p_r$$

$$\text{By def., } (2/6) = (2/p_1) \cdots (2/p_r)$$

Using corollary to Th. 9.6, p. 191,  $(2/p_i) = (-1)^{(\rho_i^2-1)/8}$

$$\therefore (2/6) = (-1)^{(\rho_1^2-1)/8} (-1)^{(\rho_2^2-1)/8} \cdots (-1)^{(\rho_r^2-1)/8}$$

Now use the hint: if  $u, v$  are odd integers,

Then  $u = 4r+1$  or  $u = 4r+3$ , some  $r$

$v = 4s+1$  or  $v = 4s+3$ , some  $s$

$$(1) u = 4r+1, v = 4s+1$$

$$\therefore u^2 - 1 = 16r^2 + 8r, v^2 - 1 = 16s^2 + 8s$$

$$\therefore \frac{u^2-1}{8} + \frac{v^2-1}{8} = 2r^2 + r + 2s^2 + s$$

$$\therefore \frac{u^2-1}{8} + \frac{v^2-1}{8} \equiv r+s \pmod{2} \quad [1]$$

$$uv = 16rs + 4r + 4s + 1$$

$$\begin{aligned}
 (uv)^2 &= 16^2 r^2 s^2 + 64 r^2 s + 64 r s^2 + 16 r s \\
 &\quad + 64 r^2 s + 16 r^2 + 16 r s + 4 r \\
 &\quad + 64 r s^2 + 16 r s + 16 s^2 + 4 s \\
 &\quad + 16 r s + 4 r + 4 s + 1 \\
 \therefore (uv)^2 - 1 &= 16^2 r^2 s^2 + 128 r^2 s + 128 r s^2 + 64 r s \\
 &\quad + 16 r^2 + 16 s^2 + 8 r + 8 s \\
 \therefore \frac{(uv)^2 - 1}{8} &\equiv r + s \pmod{2} \quad [2]
 \end{aligned}$$

$$\therefore [13, 12] \Rightarrow \frac{u^2 - 1}{8} + \frac{v^2 - 1}{8} \equiv \frac{(uv)^2 - 1}{8} \pmod{2}$$

$$(2) u = 4r + 1, v = 4s + 3$$

$$u^2 - 1 = 16r^2 + 8r, v^2 - 1 = 16s^2 + 24s + 8$$

$$\therefore \frac{u^2 - 1}{8} + \frac{v^2 - 1}{8} = 2r^2 + r + 2s^2 + 3s + 1$$

$$\therefore \frac{u^2 - 1}{8} + \frac{v^2 - 1}{8} \equiv r + s + 1 \pmod{2} \quad [13]$$

$$uv = 16rs + 12r + 4s + 3$$

$$\begin{aligned}
 (uv)^2 &= 16^2 r^2 s^2 + (16)(12)r^2 s + 64 r s^2 + 48 r s \\
 &\quad + (12)(16)r^2 s + 144 r^2 + 48 r s + 36 r \\
 &\quad + 64 r s^2 + 48 r s + 16 s^2 + 12 s \\
 &\quad + 48 r s + 36 r + 12 s + 9
 \end{aligned}$$

$$\therefore (uv)^2 - 1 = 16r^2s^2 + (24)(16)rs + 128rs^2 + \\ (4)(48)rs + 144r^2 + 16s^2 + \\ 72r + 24s + 8$$

$$\therefore \frac{(uv)^2 - 1}{8} \equiv 9r + 3s + 1 \equiv r + s + 1 \pmod{2} [2]$$

$$\therefore [1], [2] \Rightarrow \frac{u^2 - 1}{8} + \frac{v^2 - 1}{8} \equiv \frac{(uv)^2 - 1}{8} \pmod{2}$$

$$(3) u = 4r + 3, v = 4s + 1$$

same as # (2) above, by symmetry.

$$(4) u = 4r + 3, v = 4s + 3$$

$$u^2 - 1 = 16r^2 + 24r + 8, v^2 - 1 = 16s^2 + 24s + 8$$

$$\therefore \frac{u^2 - 1}{8} + \frac{v^2 - 1}{8} = 2r^2 + 3r + 1 + 2s^2 + 3s + 1$$

$$\therefore \frac{u^2 - 1}{8} + \frac{v^2 - 1}{8} \equiv 3r + 3s \equiv r + s \pmod{2} [1]$$

$$uv = 16rs + 12r + 12s + 9$$

$$(uv)^2 - 1 = 16^2r^2s^2 + (16)(12)rs + (16)(12)rs^2 + 144rs \\ + (12)(16)r^2s + 144r^2 + 144rs + (9)(12)r \\ + (12)(16)rs^2 + 144rs + 144s^2 + (9)(12)s \\ + 144rs + (9)(12)r + (9)(12)s + 80$$

$$= 16^2 r^2 s^2 + (24)(16) r^2 s + (24)(16) r s^2 + \\ (4)(144) r s + 144 r^2 + 144 s^2 + \\ (9)(24) r + (9)(24) s + 80$$

$$\therefore \frac{(uv)^2 - 1}{8} \equiv 27r + 27s \equiv r + s \pmod{2} \quad [2]$$

$$\therefore [1], [2] \Rightarrow \frac{u^2 - 1}{8} + \frac{v^2 - 1}{8} \equiv \frac{(uv)^2 - 1}{8} \pmod{2}$$

=

$$\therefore (1), (2), (3), (4) \Rightarrow \frac{u^2 - 1}{8} + \frac{v^2 - 1}{8} \equiv \frac{(uv)^2 - 1}{8} \pmod{2}$$

$$\therefore (2/5) = (-1)^{(\rho_1^2 - 1)/8} (-1)^{(\rho_2^2 - 1)/8} \dots (-1)^{(\rho_r^2 - 1)/8}$$

$$= (-1)^{[(\rho_1 \rho_2)^2 - 1]/8} \dots (-1)^{(\rho_r^2 - 1)/8}$$

$$= (-1)^{[(\rho_1 \rho_2 \dots \rho_r)^2 - 1]/8}$$

$$= (-1)^{[s^2 - 1]/8}$$

19. Derive The Generalized Quadratic Reciprocity Law:  
 If  $a$  and  $b$  are relatively prime positive odd integers, each greater than 1, Then

$$(a/b)(b/a) = (-1)^{\frac{a-1}{2} \cdot \frac{b-1}{2}}$$

Pf: Let  $a = p_1 p_2 \cdots p_r$ ,  $b = q_1 q_2 \cdots q_s$  be the prime decompositions of  $a$  and  $b$ , where, since  $a$  and  $b$  are odd,  $p_i$  and  $q_j$  are odd primes, not necessarily distinct.

Since  $\gcd(a, b) = 1$ , then  $p_i \neq q_j$  for any  $i, j$ .

By def. of  $(a/b)$ , and using Th. 9.2(d),

$$(a/b) = (a/q_1)(a/q_2) \cdots (a/q_s)$$

$$= (p_1 \cdots p_r / q_1) (p_1 \cdots p_r / q_2) \cdots (p_1 \cdots p_r / q_s)$$

$$= (p_1 / q_1) \cdots (p_r / q_1) \cdot$$

$$(p_1 / q_2) \cdots (p_r / q_2) \cdot$$

$$\vdots$$

$$(p_1 / q_s) \cdots (p_r / q_s)$$

$$= (p_1 / q_1) (p_1 / q_2) \cdots (p_1 / q_s) \cdot \quad \begin{matrix} \text{[rearranging} \\ \text{rows + cols} \end{matrix}$$

$$(p_2 / q_1) (p_2 / q_2) \cdots (p_2 / q_s) \cdot \quad \begin{matrix} \text{to get} \\ \text{r rows,} \end{matrix}$$

$$\vdots \quad \begin{matrix} \text{s cols} \end{matrix}$$

$$(p_r / q_1) (p_r / q_2) \cdots (p_r / q_s)$$

Similarly,

$$(b/a) = (q_1/p_1) \cdots (q_s/p_1) \cdot \begin{matrix} & \\ (q_1/p_2) \cdots (q_s/p_2) \cdot \\ & \vdots \\ (q_1/p_r) \cdots (q_s/p_r) \end{matrix}$$

[r rows,  
s cols]

$$\therefore (a/b)(b/a) = \begin{matrix} & \\ \text{[aligning } (a/b) \text{ rows with } \\ (b/a) \text{ rows] } \end{matrix}$$

$$(p_1/q_1)(p_1/q_2) \cdots (p_1/q_s) \cdot (q_1/p_1) \cdots (q_s/p_1) \cdot$$

$$(p_2/q_1)(p_2/q_2) \cdots (p_2/q_s) \cdot (q_1/p_2) \cdots (q_s/p_2) \cdot$$

$$(p_r/q_1)(p_r/q_2) \cdots (p_r/q_s) \cdot (q_1/p_r) \cdots (q_s/p_r)$$

$$= (p_1/q_1)(q_1/p_1) \cdots (p_1/q_s)(q_s/p_1) \cdot$$

$$(p_2/q_1)(q_1/p_2) \cdots (p_2/q_s)(q_s/p_2) \cdot$$

$$(p_r/q_1)(q_1/p_r) \cdots (p_r/q_s)(q_s/p_r)$$

Now using quadratic reciprocity  
on  $(p_i, p_j)$

$$= (-1)^{\frac{p_1-1}{2} \cdot \frac{q_1-1}{2}} \cdots (-1)^{\frac{p_s-1}{2} \cdot \frac{q_s-1}{2}} \cdot$$

$$(-1)^{\frac{p_2-1}{2} \cdot \frac{q_2-1}{2}} \cdots (-1)^{\frac{p_s-1}{2} \cdot \frac{q_s-1}{2}}$$

⋮

$$(-1)^{\frac{p_r-1}{2} \cdot \frac{q_1-1}{2}} \cdots (-1)^{\frac{p_r-1}{2} \cdot \frac{q_s-1}{2}}$$

$$= (-1)^{\left(\frac{p_1-1}{2}\right) \left[ \frac{q_1-1}{2} + \cdots + \frac{q_s-1}{2} \right]} \cdot$$

$$(-1)^{\left(\frac{p_2-1}{2}\right) \left[ \frac{q_1-1}{2} + \cdots + \frac{q_s-1}{2} \right]} \cdot$$

⋮

$$(-1)^{\left(\frac{p_r-1}{2}\right) \left[ \frac{q_1-1}{2} + \cdots + \frac{q_s-1}{2} \right]} \quad [1]$$

By prob. 18(f) above, when  $u, v$  are odd integers,

$$(-1)^{\frac{u-1}{2} + \frac{v-1}{2}} = (-1)^{\frac{uv-1}{2}}$$

$\therefore [1]$  becomes,

$$(a/b)(b/a) = (-1)^{\left(\frac{p_1-1}{2}\right) \left(\frac{q_1 \cdots q_s - 1}{2}\right)} \cdot$$

$$(-1)^{\left(\frac{p_2-1}{2}\right) \left(\frac{q_1 \cdots q_s - 1}{2}\right)} \cdot$$

$$(-1)^{\left(\frac{p_r-1}{2}\right) \left(\frac{q_1 \cdots q_s - 1}{2}\right)}$$

$$\begin{aligned}
&= (-1)^{\left(\frac{p_1-1}{2}\right)\left(\frac{b-1}{2}\right)} \cdot \\
&\quad (-1)^{\left(\frac{p_2-1}{2}\right)\left(\frac{b-1}{2}\right)} \cdot \\
&\quad \vdots \\
&\quad (-1)^{\left(\frac{p_r-1}{2}\right)\left(\frac{b-1}{2}\right)} \\
&= (-1)^{\left[\frac{p_1-1}{2} + \frac{p_2-1}{2} + \dots + \frac{p_r-1}{2}\right]}\left(\frac{b-1}{2}\right) \\
&= (-1)^{\left[\frac{p_1 p_2 \dots p_r - 1}{2}\right]}\left(\frac{b-1}{2}\right) \\
&= (-1)^{\left[\frac{a-1}{2}\right]}\left(\frac{b-1}{2}\right) \\
&\therefore (a/b)(b/a) = (-1)^{\left(\frac{a-1}{2}\right)\left(\frac{b-1}{2}\right)}
\end{aligned}$$

20. Using The Generalized Quadratic Reciprocity Law, determine whether the congruence,  $x^2 \equiv 231 \pmod{1105}$  is solvable.

First, note  $231 = 3 \cdot 7 \cdot 11$ ,  $1105 = 5 \cdot 13 \cdot 17$ .  
 $\therefore \gcd(231, 1105) = 1$ .

By prob. 17 above, if  $231$  is a quadratic residue of  $1105$  (i.e.,  $x^2 \equiv 231 \pmod{1105}$  has a solution), then  $(231/1105) = 1$ . Can't use

converse, but if can show  $(231/1105) = -1$ ,  
 Then can state  $x^2 \equiv 231 \pmod{1105}$  is not  
 solvable.

$$\therefore (231/1105)(1105/231) = (-1)^{\frac{231-1}{2} \cdot \frac{1105-1}{2}} \\ = (-1)^{(115)(552)} = 1$$

$$\therefore (231/1105)(1105/231)(1105/231) = (1105/231)$$

Using prob. 18(d),

$$(231/1105) = (1105/231)$$

$$= (181 + 4 \cdot 231/231) \quad [181 \text{ is prime}]$$

$$= (181/231) \quad [\text{prob. 18(a)}]$$

$$= (181/3)(181/7)(181/11)$$

$$= (1/3)(6/7)(5/11)$$

$$= (2/7)(3/7)(11/5)$$

$$= (1)(-1)(1) = -1$$

$\therefore (231/1105) = -1$ , so

$x^2 \equiv 231 \pmod{1105}$  is not solvable.

## 9.4 Quadratic Congruence With Composite Moduli

Note Title

8/14/2006

1. (a) Show that 7 and 18 are the only incongruent solutions of  $x^2 \equiv -1 \pmod{25}$

By Th. 8.12,  $x^K \equiv -1 \pmod{25}$  has a solution  $\Leftrightarrow (-1)^{\phi(25)/d} \equiv 1 \pmod{25}$ , where  $\phi(25) = 25 - 5 = 20$ ,  $d = \gcd(K, \phi(25))$ . Here  $K=2$ ,  $d = \gcd(2, \phi(25)) = 2$ , and so  $(-1)^{20/2} = (-1)^{10} = 1 \equiv 1 \pmod{25}$ .  $\therefore$  It has a solution, and Th. 8.12 says it has exactly  $d=2$  incongruent solutions.

$7 \not\equiv 18 \pmod{25}$ , and  $7^2 = 49 \equiv -1 \pmod{25}$ , and  $18^2 = 324 \equiv 24 \equiv -1 \pmod{25}$

To derive 7, 18, first solve for  $\phi^{K-1}$  to get  $x_0$  and  $b$

$$\begin{aligned} \because x^2 &\equiv -1 \pmod{5}, \text{ or } x^2 \equiv 4 \pmod{5} \\ \therefore x_0 &\equiv 2 \pmod{5}, \quad x_0^2 = 4 = -1 + (1)5, \\ \text{so } x_0 &= 2, \quad b = 1 \end{aligned}$$

Now solve  $2x_0y \equiv -b \pmod{5}$ , or  
 $4y \equiv -1 \pmod{5}$ ,  $\therefore y_0 \equiv 1 \pmod{5}$

$\therefore x_1 = x_0 + y_0 p^{K-1} = 2 + 1(5) = 7$  is a solution  
 to  $x^2 \equiv -1 \pmod{5^2}$ , and  $\therefore$  so is  $-7 \equiv 18$ .

$$\therefore x \equiv 7, 18 \pmod{5^2}$$

(b) Use part (a) to find the solutions of  $x^2 \equiv -1 \pmod{5^3}$

(1) Solve  $x^2 \equiv -1 \pmod{5^2}$ . From (a),  $x_0 = 7$ .  
 $\therefore x_0^2 = a + b p^2$ , or  $7^2 \equiv (-1) + b(5^2)$ ,  
 or  $49 \equiv (-1) + (2)(5^2)$ ,  $b = 2$ .

(2) Solve  $2x_0y \equiv -b \pmod{p}$ , or

$$14y \equiv -2 \pmod{5}$$

$$14y - 15y \equiv -2$$

$$-y \equiv -2, \text{ or } y \equiv 2 \pmod{5}$$

$$(3) \therefore x_1 \equiv x_0 + y_0 p^2 = 7 + 2(5^2) = 57$$

$$\therefore x \equiv 57, -57 \pmod{5^3} \equiv 57, 68$$

By Th. 8-12,  $d = \gcd(k, \phi(5^3)) = \gcd(2, 100) = 2$ ,  
 so exactly 2 solutions.

2. Solve each of the following quadratic congruences:

(a)  $x^2 \equiv 7 \pmod{3^3}$

(1) First solve  $x^2 \equiv 7 \pmod{3}$ , or  $x^2 \equiv 1 \pmod{3}$

Clearly,  $x = \pm 1$ . Choose  $x = 1$ .

$$\therefore 1^2 = 1 + (-2)3, \text{ so } x_0 = 1, b = -2$$

(2) Solve  $2x_0y \equiv -b \pmod{3}$ , or

$$2y \equiv 2 \pmod{3}, \text{ so } y = 1.$$

(3)  $\therefore$  A solution to  $x^2 \equiv 7 \pmod{3^2}$  is

$$x_0 + y_0 p = 1 + 1(3) = 4 = x_0'$$

(4)  $\therefore 4^2 = 1 + 5 \cdot 3^2, b' = 1.$

(5) Now solve  $2x_0'y' \equiv -b \pmod{p}$ , or

$$8y' \equiv -1 \pmod{3}, \text{ or } 2y' \equiv 2 \pmod{3},$$

$$\text{so } y'_0 = 1$$

(6)  $\therefore$  a solution to  $x^2 \equiv 7 \pmod{3^3}$  is

$$x_0' + y_0' \cdot 3^2 = 4 + 1 \cdot 9 = 13. \text{ Also, } -13.$$

(7)  $\therefore x \equiv 13, -13 \text{ or } x \equiv 13, 14 \pmod{3^3}$

$$(6) x^2 \equiv 14 \pmod{5^3}$$

$$(1) x^2 \equiv 14 \pmod{5}, \text{ or } x^2 \equiv 4 \pmod{5}. \therefore x_0 = 2$$
$$\therefore 2^2 = 14 + 6 \cdot 5, 6 = -2$$

$$(2) \therefore \text{Solve } 2x_0y \equiv -6 \pmod{5}, \text{ or } 4y \equiv 2 \pmod{5},$$
$$2y \equiv 1 \pmod{5}, y = 3$$

$$(3) \therefore \text{a solution to } x^2 \equiv 14 \pmod{5^2} \text{ is}$$
$$x_0 + y_0 p = 2 + 3(5) = 17$$

$$(4) \therefore 17^2 = 14 + 6(5^2), 6 = 11$$

$$(5) \therefore \text{Solve } 2x_0y \equiv -6 \pmod{p}, \text{ or}$$
$$34y \equiv -11 \pmod{5}, \text{ or } 4y \equiv 4 \pmod{5},$$
$$\therefore y = 1.$$

$$(6) \therefore \text{a solution to } x^2 \equiv 14 \pmod{5^3} \text{ is}$$
$$17 + 1(5^2) = 42, \text{ or } -42. 125 - 42 = 83$$

$$\therefore x \equiv \underline{\underline{42, 83}} \pmod{5^3}$$

$$(c) x^2 \equiv 2 \pmod{7^3}$$

$$(1) x^2 \equiv 2 \pmod{7}, \quad x_0 = 3$$

$$3^2 = 2 + 1 \cdot 7, \text{ so } b = 1$$

$$(2) 2(3)y \equiv -1 \pmod{7}, \text{ or } 6y \equiv 6 \pmod{7},$$

$$y = 1.$$

$$(3) \because \text{solution to } x^2 \equiv 2 \pmod{7^2} \text{ is}$$

$$x_0 + y\rho = 3 + (1) \cdot 7 = 10$$

$$10^2 = 2 + 6(7^2), \quad b = 2$$

$$(4) \because \text{solve } 2(10)y \equiv -2 \pmod{7}, \text{ or}$$

$$20y \equiv -2 \pmod{7} \text{ or } -y \equiv -2 \pmod{7},$$

$$y = 2$$

$$(5) \because \text{solution to } x^2 \equiv 2 \pmod{7^3} \text{ is}$$

$$10 + (2)(7^2) = 108, -108. \quad 7^3 - 108 = 343 - 108 = 235$$

$$\therefore x \equiv 108, 235 \pmod{7^3}$$

3. Solve the congruence  $x^2 \equiv 31 \pmod{11^4}$

$$(1) \text{Solve } x^2 \equiv 31 \pmod{11}, \text{ or } x^2 \equiv 9 \pmod{11}. \quad \therefore x \equiv 3$$

$$3^2 = 31 + 6(11), \quad b = -2.$$

$$(2) \therefore 2(3)y \equiv 2 \pmod{11}, 6y \equiv 2 \pmod{11}, y=4$$

$$(3) \because x+y = 3+4(11) = 47 \text{ is a solution}$$

$\downarrow$  to  $x^2 \equiv 31 \pmod{11^2}$

$$\therefore 47^2 = 31 + 6(11^2), 6 = 18$$

$$(4) \because 2x_0y \equiv -6 \pmod{11} \Leftrightarrow 2(47)y \equiv -18 \pmod{11}$$
$$94y \equiv 4 \pmod{11}, \text{ or } 6y \equiv 4 \pmod{11}$$

$\downarrow$  to  $y \equiv 8 \pmod{11}$

$$\therefore y \equiv 8 \pmod{11}$$

$$(5) \because 47+8(11^2) = 1015 \text{ is a solution to}$$
$$x^2 \equiv 31 \pmod{11^3}$$
$$\therefore 1015^2 = 31 + 6(11^3), 6 = 774$$

$$(6) \because \text{Solve } 2x_0y \equiv -6 \pmod{11}, \text{ or}$$
$$2030y \equiv -774 \pmod{11}, \text{ or}$$

$\downarrow$  to  $y \equiv 3 \pmod{11}$

$$\therefore y \equiv 3 \pmod{11}$$

$$(7) \because 1015 + 3(11^3) = 5008 \text{ is a solution to}$$
$$x^2 \equiv 31 \pmod{11^4}, 11^4 - 5008 = 9633$$

$$\therefore x \equiv 5008, 9633 \pmod{11^4}$$

---

4. Find the solutions of  $x^2 + 5x + 6 \equiv 0 \pmod{5^3}$   
 and  $x^2 + x + 3 \equiv 0 \pmod{3^3}$

$$(a) x^2 + 5x + 6 \equiv 0 \pmod{5^3}$$

$$(x+3)(x+2) \equiv 0 \pmod{5^3}, \therefore x \equiv -3, -2, \text{ or } \\ x \equiv 122, 123 \pmod{5^3}$$

$$(b) x^2 + x + 3 \equiv 0 \pmod{3^3}$$

$$\gcd(4, 3^3) = 1, \therefore x^2 + x + 3 \equiv 0 \Leftrightarrow 4x^2 + 4x + 12 \equiv 0 \\ \Leftrightarrow (2x+1)^2 + 11 \equiv 0 \\ \Leftrightarrow (2x+1)^2 \equiv 16 \pmod{3^3}$$

$$\therefore 2x+1 \equiv 4, 2x+1 \equiv -4$$

$$2x \equiv 3 \quad 2x \equiv -5$$

$$28x \equiv 42 \quad 28x \equiv -70 \quad (\gcd(14, 3^3) = 1)$$

$$x \equiv 42$$

$$x \equiv -70$$

$$x \equiv 15$$

$$x \equiv 11$$

$$\therefore x \equiv 11, 15 \pmod{3^3}$$

5. Prove that if the congruence  $x^2 \equiv a \pmod{2^n}$ , where  $a$  is odd and  $n \geq 3$ , has a solution, then

if has exactly four incongruent solutions.

Pf: Note: can't invoke Th. 8.12 since  $2^n$  has no primitive roots for  $n \geq 3$ .

Since  $a$  is odd, if  $x$  is a solution, then  $x$  must be odd. Also,  $-x$  is a solution.

Suppose  $y$  is any other solution.

$\therefore y^2 \equiv a \pmod{2^n}$ , so  $x^2 \equiv y^2 \pmod{2^n}$ ,  $n \geq 3$ .

$$\therefore (x-y)(x+y) \equiv 0 \pmod{2^n}$$

$$\Leftrightarrow \frac{x-y}{2} \cdot \frac{x+y}{2} \equiv 0 \pmod{2^{n-2}}, n \geq 3$$

by Th. 4.3

But note that  $\frac{x-y}{2} + \frac{x+y}{2} = x$ , which is odd.

$\therefore$  Only one of  $\frac{x-y}{2}, \frac{x+y}{2}$  is even.

(1) Suppose  $\frac{x-y}{2}$  is the even factor,  
so  $\frac{x+y}{2}$  is the odd factor

$$\therefore (x-y)\left(\frac{x+y}{2}\right) \equiv 0 \pmod{2^{n-1}} \Rightarrow$$

$$x - y \equiv 0 \pmod{2^{n-1}} \Rightarrow \\ x \equiv y \pmod{2^{n-1}}$$

(2) Suppose  $\frac{x+y}{2}$  is the even factor, so  $\frac{x-y}{2}$  is the odd factor

$$\therefore (x+y)\left(\frac{x-y}{2}\right) \equiv 0 \pmod{2^{n-1}} \Rightarrow$$

$$x+y \equiv 0 \pmod{2^{n-1}} \Rightarrow \\ x \equiv -y \pmod{2^{n-1}}$$

(1), (2)  $\Rightarrow$  if  $y$  is any other solution,

$$y = \pm x + k 2^{n-1}$$

for  $k$  odd,  $k = 2r+1$ , some  $r$ .

$$\therefore y = \pm x + 2^{n-1} + r 2^n$$

$$\therefore y \equiv \pm x + 2^{n-1} \pmod{2^n} \quad [1]$$

for  $k$  even,  $k = 2r$ , some  $r$ .

$$\therefore y = \pm x + r 2^n$$

$$\therefore y \equiv \pm x \pmod{2^n} \quad [2]$$

$\therefore [1], [2] \Rightarrow$  only incongruent solutions,  
 $\text{mod } 2^n$ , are  $x, -x, x + 2^{n-1}, -x + 2^{n-1}$ .

6. From  $23^2 \equiv 17 \pmod{2^7}$ , find three other  
 solutions of the quadratic congruence  
 $x^2 \equiv 17 \pmod{2^7}$

From #5 above, solutions are  $23, -23, 23 + 2^6$ ,  
 and  $-23 + 2^6 \pmod{2^7}$ .

$$2^6 = 64, 2^7 = 128. \therefore -23 + 2^7 = 105$$

$$\therefore \underline{\underline{23, 105, 87, 41 \pmod{2^7}}}$$

7. First determine the values of  $a$  for which  
 the congruences below are solvable, and then  
 find the solutions of these congruences.

$$(a) x^2 \equiv a \pmod{2^4}$$

By Th. 9.12, solvable  $\Leftrightarrow a \equiv 1 \pmod{8}$ .

$$2^4 = 16. \therefore a = \underline{\underline{1 \text{ or } 9}}$$

Now use #5 above.

$$a=1: x = 1, -1, 1+2^3, -1+2^3$$

$$x \equiv 1, -1 + 16, 9, 7$$

$$\therefore x \equiv 1, 7, 9, 15 \pmod{2^4}$$

$$a=9: x = 3, -3, 3+2^3, -3+2^3$$

$$\therefore x = 3, 13, 11, 5$$

$$(6) x^2 \equiv a \pmod{2^5}$$

$$2^5 = 32. \text{ solvable} \Leftrightarrow a \equiv 1 \pmod{8},$$
$$\therefore a = 1, 9, 17, \text{ or } 25$$

$$a=1: x \equiv \pm 1, \pm 1 + 2^4$$
$$\therefore x \equiv 1, 31, 17, 15$$

$$a=9: x \equiv \pm 3, \pm 3 + 2^4$$
$$\therefore x \equiv 3, 29, 19, 13$$

$$a=17: \therefore x^2 \equiv 17 + 32 = 49$$
$$\therefore x \equiv \pm 7, \pm 7 + 2^4$$
$$\therefore x \equiv 7, 25, 23, 9$$

$$a=25: x \equiv \pm 5, \pm 5 + 2^4$$

$$\therefore x = \underline{\underline{5, 27, 21, 11}}$$

$$(c) x^2 \equiv a \pmod{2^6}$$

$$2^6 = 64. \therefore \text{solvable} \Leftrightarrow a \equiv 1 \pmod{8}$$
$$\therefore a = 1, 9, 17, 25, 33, 41, 49, 57$$

$$a = 1 : \pm 1, \pm 1 + 2^5$$
$$\therefore x \equiv 1, 63, 33, 31$$

$$a = 9 : \pm 3, \pm 3 + 2^5$$
$$\therefore x \equiv 3, 61, 35, 29$$

$$a = 17 : 17 + 64 = 81. \therefore \pm 9, \pm 9 + 2^5$$
$$\therefore x \equiv 9, 55, 41, 23$$

$$a = 25 : \pm 5, \pm 5 + 2^5$$
$$\therefore x \equiv 5, 59, 37, 27$$

$$a = 33 : 33 + 64 = 97, 33 + 128 = 161, 33 + 192 = 225$$
$$\therefore \pm 15, \pm 15 + 2^5$$
$$\therefore x \equiv 15, 49, 47, 17$$

$$a = 41 : 41 + 64 = 105, 41 + 128 = 169$$
$$\therefore \pm 13, \pm 13 + 2^5$$

$$\therefore x \equiv 13, 51, 45, 19$$

$$a = 49; \pm 7, \pm 7 + 2^5 \\ \therefore x \equiv 7, 57, 39, 25$$

$$a = 57; 57 + 64 = 121 \\ \therefore \pm 11, \pm 11 + 2^5 \\ \therefore x \equiv 11, 53, 43, 21$$

8. For fixed  $n > 1$ , show that all the solvable congruences  $x^2 \equiv a \pmod{n}$  with  $\gcd(a, n) = 1$  have the same number of solutions.

Pf: Let  $n = 2^{k_0} p_1^{k_1} \dots p_r^{k_r}$ ,  $k_i \geq 0$

For  $p_i^{k_i}$ ,  $k_i \geq 1$ , we can use Th. 8.12 to state that  $x^2 \equiv a \pmod{p_i^{k_i}}$  has exactly 2 solutions.

The actual value of  $a$  doesn't matter, as long as  $\gcd(a, p_i^{k_i}) = 1$ .

For  $x^2 \equiv a \pmod{2^{k_0}}$ ,  $k_0 \geq 1$ , Th. 9.12 states there are just 2 solutions for  $x^2 \equiv a \pmod{2}$  ( $\pm 1, 1, -1$ ), 2 solutions for  $x^2 \equiv a \pmod{4}$  when  $a \equiv 1 \pmod{4}$

(i.e.,  $x=1, 3$ ), and for  $x^2 \equiv a \pmod{2^n}$ ,  
 $n \geq 3$ , when  $a \equiv 1 \pmod{8}$ , problem #5  
 shows there are exactly 4 solutions.

$\therefore$  if  $\gcd(a, n) = 1$ , then there are  $2 \cdot 2^n$   
 possible solutions if  $a \equiv 1 \pmod{4}$  and  
 $a \not\equiv 1 \pmod{8}$ , and  $4 \cdot 2^n$  possible  
 solutions if  $a \equiv 1 \pmod{8}$ .

Label these solutions  $x_{iK_i}$ , so  
 that, for example,  $x_{1K_1}$  and  $x_{2K_1}$

are the solutions to  $x^2 \equiv a \pmod{p_1^{k_1}}$

$\therefore$  consider the  $4 \cdot 2^n$  ( $a \equiv 1 \pmod{8}$ ) or  
 $2 \cdot 2^n$  ( $a \equiv 1 \pmod{4}$ ,  $a \not\equiv 1 \pmod{8}$ ) linear  
 equation systems:

$$x \equiv x_{1K_0} \pmod{2^{k_0}}$$

$$x \equiv x_{2K_0} \pmod{2^{k_0}}$$

$$\vdots$$

$$\vdots$$

$$x \equiv x_{1K_r} \pmod{p_r^{k_r}}$$

$$x \equiv x_{2K_r} \pmod{p_r^{k_r}}$$

$\vdots$

$\cdots$

$$x \equiv x_{2K_0} \pmod{2^{k_0}}$$

$\vdots$

$$x \equiv x_{2K_r} \pmod{p_r^{k_r}}$$

By The Chinese Remainder Th., There is  
 a simultaneous solution unique to  
 $n = 2^{k_0} p_1^{k_1} \dots p_r^{k_r}$  for each system.

Thus, The number of solutions is, for any  
 $a$  with  $\gcd(a, n) = 1$ :

$$2^r, \text{ if } n = p_1^{k_1} \dots p_r^{k_r}$$

$$2 \cdot 2^r, \text{ if } n = 2 p_1^{k_1} \dots p_r^{k_r}$$

$$2 \cdot 2^r, \text{ if } n = 2^2 p_1^{k_1} \dots p_r^{k_r} \text{ and } a \equiv 1 \pmod{4},$$

$$4 \cdot 2^r, \text{ if } n = 2^{k_0} p_1^{k_1} \dots p_r^{k_r}, k_0 \geq 3 \text{ and } a \equiv 1 \pmod{8}$$

9. (a) Without actually finding them, determine  
 the number of solutions of the congruences  
 $x^2 \equiv 3 \pmod{11^2 \cdot 23^2}$  and  $x^2 \equiv 9 \pmod{2^3 \cdot 3 \cdot 5^2}$

$$(1) x^2 \equiv 3 \pmod{11^2 \cdot 23^2}$$

$$x^2 \equiv 3 \pmod{11^2} \text{ and } x^2 \equiv 3 \pmod{23^2}$$

each will have 2 solutions (by Th. 8.12)

so  $2 \cdot 2 = \underline{\underline{4}}$  solutions

$$(2) x^2 \equiv 9 \pmod{2^3 \cdot 3 \cdot 5^2}$$

$x^2 \equiv 9 \pmod{2^3}$  has 4 (by prob. #5)

$x^2 \equiv 9 \pmod{3} \Leftrightarrow x^2 \equiv 0 \pmod{3}$ , so just 1 solution ( $x \equiv 0$ ).

$x^2 \equiv 9 \pmod{5^2}$  has 2 solutions.

$$\therefore 4 \cdot 1 \cdot 2 = \underline{8} \text{ solutions}$$

$$(5) \text{ Solve } x^2 \equiv 9 \pmod{2^3 \cdot 3 \cdot 5^2}$$

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

$x = \pm 3, \pm 3 + 2^2$  by prob. #5,  
 $\therefore x \equiv 3, 5, 7, 1 \pmod{2^3}$

$$x^2 \equiv 9 \pmod{3} \Leftrightarrow x \equiv 0 \pmod{3}$$

$$x^2 \equiv 9 \pmod{5^2}$$

$x = \pm 3, \text{ or } x \equiv 3, 22 \pmod{5^2}$

$$(1) x \equiv 1 \pmod{8}$$

$$n = 600 = 2^3 \cdot 3 \cdot 5^2$$

$$x \equiv 0 \pmod{3}$$

$$N_1 = 75 = 3 \cdot 5^2$$

$$x \equiv 3 \pmod{25}$$

$$N_2 = 200 = 2^3 \cdot 5^2$$

$$\therefore 75x_1 \equiv 1 \pmod{8}$$

$$200x_2 \equiv 1 \pmod{3}$$

$$3x_1 \equiv 1, 9x_1 \equiv 3$$

$$2x_2 \equiv 1, 4x_2 \equiv 2$$

$$x_1 \equiv 3$$

$$x_2 \equiv 2$$

$$24x_3 \equiv 1 \pmod{25}$$

$$-x_3 \equiv 1, x_3 \equiv -1 \equiv 24$$

$$\therefore (1)(75)(3) + 0 \cdot (200)(2) + (3)(24)(-1) = 153$$

$$\therefore x \equiv \underline{153} \pmod{2^3 \cdot 3 \cdot 5^2}$$

$$(2) \quad x \equiv 3 \pmod{8} \quad \text{as above, } N = 2^3 \cdot 3 \cdot 5^2$$

$$x \equiv 0 \pmod{3} \quad N_1 = 75, N_2 = 200, N_3 = 24$$

$$x \equiv 3 \pmod{25} \quad x_1 = 3, x_2 = 2, x_3 = -1$$

$$\therefore x = (3)(75)(3) + 0 + (3)(24)(-1) = 603$$

$$\therefore x \equiv \underline{3} \pmod{2^3 \cdot 3 \cdot 5^2}$$

$$(3) \quad x \equiv 5 \pmod{8} \quad \text{as in (1), } N = 2^3 \cdot 3 \cdot 5^2$$

$$x \equiv 0 \pmod{3} \quad N_1 = 75, N_2 = 200, N_3 = 24$$

$$x \equiv 3 \pmod{25} \quad x_1 = 3, x_2 = 2, x_3 = -1$$

$$\therefore x = (5)(75)(3) + 0 + (3)(24)(-1) = 1053$$

$$\therefore x \equiv \underline{453} \pmod{2^3 \cdot 3 \cdot 5^2}$$

$$(4) \quad x \equiv 7 \pmod{8} \quad \text{as in (1), } N = 2^3 \cdot 3 \cdot 5^2$$

$$x \equiv 0 \pmod{3} \quad N_1 = 75, N_2 = 200, N_3 = 24$$

$$x \equiv 3 \pmod{25} \quad x_1 = 3, x_2 = 2, x_3 = -1$$

$$\therefore x = (7)(75)(3) + 0 + (3)(24)(-1) = 1503$$

$$\therefore x \equiv 303 \pmod{2^3 \cdot 3 \cdot 5^2}$$

(5)  $x \equiv 1 \pmod{8}$  as in (1),  $N = 2^3 \cdot 3 \cdot 5^2 = 600$   
 $x \equiv 0 \pmod{3}$   $N_1 = 75, N_2 = 200, N_3 = 24$   
 $x \equiv 22 \pmod{25}$   $x_1 = 3, x_2 = 2, x_3 = -1$

$$x = (1)(75)(3) + 0 + (22)(24)(-1) = -303$$

$$\therefore x \equiv 297 \pmod{2^3 \cdot 3 \cdot 5^2}$$

(6)  $x \equiv 3 \pmod{8}$  as in (1),  $N = 2^3 \cdot 3 \cdot 5^2 = 600$   
 $x \equiv 0 \pmod{3}$   $N_1 = 75, N_2 = 200, N_3 = 24$   
 $x \equiv 22 \pmod{25}$   $x_1 = 3, x_2 = 2, x_3 = -1$

$$x = (3)(75)(3) + 0 + (22)(24)(-1) = 147$$

$$\therefore x \equiv 147 \pmod{2^3 \cdot 3 \cdot 5^2}$$

(7)  $x \equiv 5 \pmod{8}$  as in (1),  $N = 2^3 \cdot 3 \cdot 5^2 = 600$   
 $x \equiv 0 \pmod{3}$   $N_1 = 75, N_2 = 200, N_3 = 24$   
 $x \equiv 22 \pmod{25}$   $x_1 = 3, x_2 = 2, x_3 = -1$

$$x = (5)(75)(3) + 0 + (22)(24)(-1) = 597$$

$$\therefore x \equiv 597 \pmod{2^3 \cdot 3 \cdot 5^2}$$

$$(8) \begin{aligned} x &\equiv 7 \pmod{8} & \text{as in (1), } N = 2^3 \cdot 3 \cdot 5^2 = 600 \\ x &\equiv 0 \pmod{3} & N_1 = 75, N_2 = 200, N_3 = 24 \\ x &\equiv 22 \pmod{25} & x_1 = 3, x_2 = 2, x_3 = -1 \end{aligned}$$

$$x = (7)(75)(3) + 0 + (22)(24)(-1) = 1047$$

$$\therefore x \equiv 447 \pmod{2^3 \cdot 3 \cdot 5^2}$$

$$\therefore x \equiv 3, 147, 153, 297, 303, 447, 453, 597 \pmod{2^3 \cdot 3 \cdot 5^2}$$

10. (a) For an odd prime  $p$ , prove that the congruence  $2x^2 + 1 \equiv 0 \pmod{p}$  has a solution if and only if  $p \equiv 1$  or  $3 \pmod{8}$ .

Pf: As  $\gcd(8, p) = 1$ ,  $2x^2 + 1 \equiv 0 \pmod{p}$  has a solution  $\Leftrightarrow 8(2x^2 + 1) \equiv 0 \pmod{p}$  has a solution.

$$\therefore \text{Look at } 16x^2 = (4x)^2 \equiv -8 \pmod{p}.$$

Let  $y = 4x$ . Then can solve  $4x \equiv y \pmod{p}$   
 since  $y^2 \equiv -8$ ,  $\gcd(y^2, p) = \gcd(y, p) = 1$ ,  
 so  $4x \equiv y \pmod{p}$  has a unique

solution.

$\therefore y^2 \equiv -8 \pmod{p}$  has a solution

$$\Leftrightarrow (-8/p) = 1$$

$$(-8/p) = (-1/p)(2^3/p) = (-1/p)(2/p)$$

$$\therefore (-1/p) = (2/p)$$

$$(a) (2/p) = -1 \Leftrightarrow p \equiv 3 \pmod{8} \text{ or } p \equiv 5 \pmod{8}$$

$$(-1/p) = (-1)^{\frac{p-1}{2}} = -1 \Leftrightarrow \frac{p-1}{2} \text{ is odd} \\ \Leftrightarrow \frac{p-1}{2} = 2k+1, \text{ some } k$$

$$\Leftrightarrow p-1 = 4k+2$$

$$\Leftrightarrow p = 3 + 4k$$

$$\therefore (2/p) = (-1/p) = -1 \Leftrightarrow p \equiv 3 \pmod{8}$$

$$(b) (2/p) = 1 \Leftrightarrow p \equiv 1 \pmod{8} \text{ or } p \equiv 7 \pmod{8}$$

$$(-1/p) = (-1)^{\frac{p-1}{2}} = 1 \Leftrightarrow \frac{p-1}{2} \text{ is even}$$

$$\Leftrightarrow \frac{p-1}{2} = 2k, \text{ some } k$$

$$\Leftrightarrow p-1 = 4k$$

$$\Leftrightarrow p = 1 + 4k$$

$$\therefore (2/p) = (-1/p) = 1 \Leftrightarrow p \equiv 1 \pmod{8}$$

$\therefore (a)$  &  $(b)$  show  $2x^2 + 1 \equiv 0 \pmod{p} \Leftrightarrow p \equiv 1 \text{ or } 3 \pmod{8}$

(b) Solve the congruence  $2x^2 + 1 \equiv 0 \pmod{11^2}$

$$\text{Let } z = 4x, \therefore z^2 \equiv -8 \pmod{11^2}$$

Use method described in proof to Th. 9.11

First solve  $z^2 \equiv -8 \pmod{11}$

$$\therefore z^2 \equiv 3 \pmod{11}$$

$$z \equiv 5 \pmod{11} \quad \therefore x_0 = 5$$

$$\therefore x_0^2 = -8 + b(11), b = 3$$

Now solve  $2x_0y \equiv -b \pmod{p}$

$$\begin{aligned}\therefore 2(5)y &\equiv -3 \pmod{11} \\ -y &\equiv -3 \pmod{11} \\ y &\equiv 3 \pmod{11} \quad y_0 = 3\end{aligned}$$

$$\therefore x_0 + y_0 p = 5 + 3(11) = 38$$

$$\therefore z = 38 \text{ solves } z^2 \equiv -8 \pmod{11^2}$$

Now convert back using  $z \equiv 4x \pmod{11^2}$

$$\begin{aligned}\therefore 4x &\equiv 38 \pmod{11^2} \\ 2x &\equiv 19 \pmod{121} \\ 122x &\equiv 19(1) = 1159 \pmod{121} \\ x &\equiv 1159 = 70 \pmod{11^2}\end{aligned}$$

$$\therefore x \equiv \pm 70 \pmod{11^2}$$

$$\therefore x \equiv 51, 70 \pmod{11^2}$$