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 $\Longleftrightarrow$ given any integer z, there is an $a_i \in A$ s.t. $a_i - z = kn$ 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. $a_j - z = qn + r$.

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: $A = \{a_1, a_2, \ldots, a_n\}$ is a complete set of residues modulo n $\Longleftrightarrow$ 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 $a_i \equiv a_j \pmod{n}$

$\therefore$ $a_i - a_j = Kn$, 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.

$\therefore$ $z - a_i = sn$, 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. $\therefore a_i \not\equiv a_k \pmod n$

(2) Suppose $a_i \not\equiv a_j \pmod n$ for $a_i, a_j \in A$, $a_i \neq a_j$

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 $a_i - a_j = (q_i - q_j)n$, 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 $\{0, 1, \ldots, n-1\}$, 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]
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 [1]

$a_i + (q-k)n - a_j = sn$, $a_i - a_j = (s-q+k)n$,
$\therefore a_i \equiv a_j \pmod{n}$, a contradiction.

$\therefore z$ is $\equiv$ to one and only one of
$a_i \in A$, mod n

Theorem 2: if $ab \equiv 0 \pmod{p}$, 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

$ab = qpb + rb$, $kp = qpb + rb$,

$p(k - qb) = rb$. $\therefore$ 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 $z \equiv a \pmod{n}$

$\therefore\ z - a = kn$, some k

$\therefore\ z + cn - (a + dn) = z - a + cn - dn$

$= kn + (c-d)n$

$= (k + c - d)n$

$\therefore\ z + cn \equiv a + dn \pmod{n}$

(2) Suppose $z + cn \equiv a + dn \pmod{n}$

$\therefore\ z + cn - (a + dn) = kn$, some k

$\therefore\ z - a = -cn + dn + kn$

$= (k - c + d)n$

$\therefore\ z \equiv a \pmod{n}$

Problems 4.2

1. (a). If $a \equiv b \pmod{n}$ and $m | n$, then $a \equiv b \pmod{m}$

Pf: $a \equiv b \pmod{n} \Rightarrow a - b = kn$, some k.

$m | n \Rightarrow n = rm$, some r.

$\therefore\ a - b = krm \Rightarrow a \equiv b \pmod{m}$

(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,

$$\begin{aligned} a &= k_1 d & \therefore\ a/d &= k_1 \\ b &= k_2 d & b/d &= k_2 \\ n &= k_3 d & n/d &= k_3 \end{aligned}$$

$$\therefore k_1 d - k_2 d = k(k_3 d)$$

$$\therefore k_1 - k_2 = k k_3 \Rightarrow \frac{a}{d} - \frac{b}{d} = k\left(\frac{n}{d}\right)$$

$$\therefore a/d \equiv b/d \pmod{n/d}$$

2. $a^2 \equiv b^2 \pmod{n} \not\Rightarrow a \equiv b \pmod{n}$

$5^2 \equiv 4^2 \pmod{3}$ since $25 - 16 = 3 \cdot 3$
But $5 \not\equiv 4 \pmod{3}$.

3. If $a \equiv b \pmod{n}$, Then $\gcd(a,n) = \gcd(b,n)$

Pf: $a - b = kn$, some k. Let $d = \gcd(a,n)$

$\therefore a = dr, n = ds$, some r, s.

$\therefore dr - b = kds$, $b = d(r - ks)$, $\therefore d \mid b$.

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 $2^{50} \div 7$, $41^{65} \div 7$

$2^{50} \div 7$: $2^{50} = (2^5)^{10}$, $2^5 = 4 \cdot 7 + 4$

$\therefore 2^5 \equiv 4 \pmod{7}$

$\therefore 2^{50} \equiv 4^{10} \pmod{7}$

But $4^{10} = 2^{20} = (2^5)^4$

From above, $2^5 \equiv 4 \mod 7$

$\therefore 2^{20} \equiv 4^4 \pmod{7}$

But $4^4 = 256 = 36 \cdot 7 + 4$

$\therefore 4^4 \equiv 4 \mod 7$, $\therefore 4^4 - 4 \equiv 0 \pmod{7}$

$\therefore 2^{50} - 4 \equiv 4^{10} - 4 \equiv 2^{20} - 4 \equiv 4^4 - 4 \equiv 0 \pmod{7}$

$\therefore 2^{50} \equiv 4 \pmod 7$, so

$2^{50} \div 7$ has remainder $\underline{\underline{4}}$

$41^{65} \div 7$: $41^{65} = (41^5)^{13}$, $41 = 5 \cdot 7 + 6$

$\therefore 41 \equiv 6 \pmod 7$

$\therefore 41^5 \equiv 6^5 \pmod 7$

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 $\underline{\underline{6}}$

(b) What is remainder when $1^2 + 2^5 + \dots + 100^5 \div 4$?

Since $1^5 \equiv 1 \bmod 4$, and since $1 \equiv 5 \equiv 9 \dots \bmod 4$

$32 = 2^5 \equiv 0 \bmod 4$ $2 \equiv 6 \equiv 10 \dots \bmod 4$

$243 = 3^5 \equiv 3 \bmod 4$ $3 \equiv 7 \equiv 11 \dots \bmod 4$

$4^5 \equiv 0 \bmod 4$ $4 \equiv 8 \equiv 12 \dots \bmod 4$

Each block of 4 numbers will have same remainder sum.

Since $1^5+2^5+3^5+4^5 \equiv 1+0+3+0 \equiv 4 \equiv 0 \mod 4$, Then the 25 blocks will all have remainder 0.
$\therefore$ Entire remainder is $\underline{0}$.

5. Prove $53^{103} + 103^{53} \equiv 0 \pmod{39}$
$111^{333} + 333^{111} \equiv 0 \pmod{7}$

Pf: $53^{103} + 103^{53} \equiv 0 \pmod{39}$

$39 = 3 \cdot 13$. $\quad 53 = 3 \cdot 17 + 2 = 3 \cdot 18 - 1$
$103 = 34 \cdot 3 + 1$
$\therefore\ 53 \equiv -1 \pmod{3} \qquad 103 \equiv 1 \pmod{3}$
$\therefore\ 53^{103} \equiv (-1)^{103} \pmod{3} \quad 103^{53} \equiv 1^{53} \pmod{3}$

$53 \equiv 1 \pmod{13} \quad 103 \equiv -1 \pmod{13}$
$\therefore\ 53^{103} \equiv 1 \pmod{13} \quad 103^{53} \equiv -1 \pmod{13}$

$\therefore\ 53^{103} + 103^{53} \equiv -1+1 \equiv 0 \pmod{3}$
$53^{103} + 103^{53} \equiv -1+1 \equiv 0 \pmod{13}$

$\therefore$ Both 3 and 13 divide sum, and $\gcd(3,13)=1$, so by Corollary 2, p. 24,

$3 \cdot 13 = 39$ divides sum.

$\therefore 53^{103} + 103^{53} \equiv 0 \pmod{39}$

$111^{333} + 333^{111} \equiv 0 \pmod 7$

$111 = 7 \cdot 15 + 6$, $\therefore 111 = 16 \cdot 7 + -1$, $\therefore 111 \equiv -1 \pmod 7$

$\therefore 111^{333} \equiv (-1)^{333} \pmod 7$, or $111^{333} \equiv (-1) \pmod 7$

$333 = 47 \cdot 7 + 4$, $\therefore 333 \equiv 4 \pmod 7$, $333 \equiv 2^2 \pmod 7$

$\therefore 333^{111} \equiv 2^{222} \pmod 7$

$2^6 = 64 = 9 \cdot 7 + 1$. $\therefore 2^6 \equiv 1 \pmod 7$

and $222 = 6 \cdot 17$. $\therefore (2^6)^{17} = 2^{222}$

$\therefore 2^{222} \equiv 1^{17} \pmod 7$, or $2^{222} \equiv 1 \pmod 7$

$\therefore 333^{111} \equiv 1 \pmod 7$

$\therefore 111^{333} + 333^{111} \equiv (-1+1) \pmod 7$, or

$111^{333} + 333^{111} \equiv 0 \bmod 7$

6. (a) $7 \mid (5^{2n} + 3 \cdot 2^{5n-2})$, $n \geq 1$

Pf: $n=1$: $5^{2n} + 3 \cdot 2^{5n-2} = 25 + 3 \cdot 8 = 49 = 7^2$

$n+1$: $5^{2(n+1)} + 3 \cdot 2^{5(n+1)-2}$

$= 5^{2n} \cdot 5^2 + 3 \cdot 2^{5n-2} \cdot 2^5$

$= 5^{2n}(3\cdot 7+4) + 3\cdot 2^{5n-2}\cdot(4\cdot 7+4)$

$= 3\cdot 7\cdot 5^{2n} + 4\cdot 7\cdot 3\cdot 2^{5n-2}$

$\quad + 4(5^{2n} + 3\cdot 2^{5n-2})$ [1]

$= 3\cdot 7\cdot 5^{2n} + 4\cdot 7\cdot 3\cdot 2^{5n-2} + 4\cdot 7x$

$= 7(3\cdot 5^{2n} + 4\cdot 3\cdot 2^{5n-2} + 4\cdot x)$

where x is some integer since it was assumed that for n,

$5^{2n} + 3\cdot 2^{5n-2} = 7x$ as in [1].

$\therefore$ For $n+1$, number is divisible by 7.

$\therefore$ true for all $n \geq 1$.

=

or, $5^2 = 25 \equiv 4 \pmod 7$ $\quad\therefore\ 5^{2n} \equiv 4^n \pmod 7$

$2^5 \equiv 4 \pmod 7$ $\quad 2^{5n} \equiv 4^n \pmod 7$

For $n \geq 1$, $2^{5n}\cdot 4^{-1} \equiv 4^n\cdot 4^{-1} \pmod 7$

$\therefore\ 2^{5n-2} \equiv 4^{n-1} \pmod 7$

$\therefore\ 3\cdot 2^{5n-2} \equiv 3\cdot 4^{n-1} \pmod 7$

But $4^n + 3\cdot 4^{n-1} = 4\cdot 4^{n-1} + 3\cdot 4^{n-1}$

$= 7\cdot 4^{n-1}$

$\therefore\ 5^{2n} + 3\cdot 2^{5n-2} \equiv 7\cdot 4^{n-1} \equiv 0 \pmod 7$

(b) $13 \mid (3^{n+2} + 4^{2n+1})$

Pf: $3 \equiv 16 \pmod{13}$, $3 \equiv 4^2 \pmod{13}$

$\therefore 3^n \equiv 4^{2n} \pmod{13}$

$3^n \cdot 9 \equiv 4^{2n} \cdot 9 \pmod{13}$, $3^{n+2} \equiv 4^{2n} \cdot 9 \pmod{13}$

$$\begin{aligned} \therefore 3^{n+2} + 4^{2n+1} &\equiv 4^{2n} \cdot 9 + 4^{2n+1} \pmod{13} \\ &\equiv 4^{2n}(9+4) \pmod{13} \\ &\equiv 4^{2n} \cdot 13 \pmod{13} \\ &\equiv 0 \pmod{13} \end{aligned}$$

(c) $27 \mid (2^{5n+1} + 5^{n+2})$

Pf: $32 \equiv 5 \pmod{27}$, $\therefore 2^5 \equiv 5 \pmod{27}$

$\therefore 2^{5n} \equiv 5^n \pmod{27}$

$2^{5n} \cdot 2 \equiv 2 \cdot 5^n \pmod{27}$

$$\begin{aligned} \therefore 2^{5n+1} + 5^{n+2} &\equiv 2 \cdot 5^n + 5^{n+2} \pmod{27} \\ &\equiv 5^n(2+25) \pmod{27} \\ &\equiv 5^n \cdot 27 \pmod{27} \\ &\equiv 0 \pmod{27} \end{aligned}$$

(d) $43 \mid (6^{n+2} + 7^{2n+1})$

Pf: $6 \equiv 49 \pmod{48}$, $6 \equiv 7^2 \pmod{48}$

$\therefore 6^n \equiv 7^{2n} \pmod{48}$

$6^n \cdot 36 \equiv 7^{2n} \cdot 36 \pmod{43}$

$6^{n+2} + 7^{2n+1} \equiv 7^{2n} \cdot 36 + 7^{2n+1} \pmod{43}$

$\equiv 7^{2n}(36 + 7) \pmod{48}$

$\equiv 0$

7. For $n \geq 1$, $(-13)^{n+1} \equiv (-13)^n + (-13)^{n-1} \pmod{181}$

Pf: $n=1$. $(-13)^2 = 169$, $169 + 13 = 182$

$\therefore 169 \equiv (-13) + 1 \pmod{181}$

$K \Rightarrow K+1$: Suppose $(-13)^{K+1} \equiv (-13)^K + (-13)^{K-1} \pmod{181}$

$\therefore (-13)^{K+1} \cdot (-13) \equiv (-13)^K \cdot (-13) + (-13)^{K-1}(-13) \pmod{181}$

$\therefore (-13)^{K+2} \equiv (-13)^{K+1} + (-13)^K \pmod{181}$

$\therefore$ True for all $n \geq 1$

8. (a) If a 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.

$\therefore a^2 = 16k^2 + 8k + 1$ or $a^2 = 16k^2 + 24k + 9$

$\therefore a^2 - 1 = 8(2k^2 + k)$ or $a^2 - 1 = 8(2k^2 + 3k + 1)$

$\therefore a^2 \equiv 1 \pmod 8$

(b) For any a, $a^3 \equiv 0, 1,$ or $6 \pmod 7$

Pf: By Div. Alg, $a = 7k + r$, $0 \le r < 7$

$a = 7k$: $a^3 = (7k)^3$, $\therefore a^3 = 7 \cdot 7^2 k^3$, $a^3 \equiv 0 \pmod 7$

$a = 7k+1$: $a^3 = (7k+1)^3 = 7^3k^3 + (\ )7^2k^2 + (\ )7k + 1$

$\therefore a^3 - 1 = 7[\quad]$, $\therefore a^3 \equiv 1 \pmod 7$

$a = 7k+2$: $a^3 = 7^3k^3 + (\ )7^2k^2 \cdot 2 + (\ )7k2^2 + 2^3$

$\therefore a^3 - 1 = 7[7^2k^3 + \dots + 1]$

$\therefore a^3 \equiv 1 \pmod 7$

$a = 7k+3$: $a^3 = 7^3k^3 + (\ )7^2k^2 \cdot 3 + (\ )7k \cdot 3^2 + 27$

$a^3 - 6 = 7[7^2k^3 + \dots + 3]$

$\therefore a^3 \equiv 6 \pmod 7$

$a = 7k+4$: $a^3 = 7^3k^3 + \dots + 64$

$a^3 - 1 = 7^3k^3 + \dots + 63 = 7[7^2k^3 + \dots + 9]$

$\therefore a^3 \equiv 1 \pmod 7$

$a=7k+5$: $a^3=7^3k^3+\dots+125=7^3k^3+119+6$
$\therefore a^3-6=7[7^2k^3+\dots+17]$
$\therefore a^3\equiv 6 \pmod 7$

$a=7k+6$: $a^3=7^3k^3+\dots+218=7^3k^3+\dots 31\cdot 7+1$
$a^3-1=7[7^2k^3+\dots+31]$
$\therefore a^3\equiv 1 \pmod 7$

(c) For any a, $a^4\equiv 0$ or $1 \pmod 5$

Pf: By Div. Alg., $a=5k+r$, $0\le r<5$

$a=5k$: $a^4=5\cdot 5^3k^4$, $\therefore a^4\equiv 0 \pmod 5$

$a=5k+1$: $a^4=5^4k^4+(\ )5^3k^3+(\ )5^2k^2+(\ )5k+1$
$\therefore a^4-1=5[\quad]$
$\therefore a^4\equiv 1 \pmod 5$

$a=5k+2$: $a^4=5^4k^4+\dots+16=5^4k^4+\dots+15+1$
$a^4-1=5[5^3k^4+\dots 3]$
$a^4\equiv 1 \pmod 5$

$a=5k+3$: $a^4=5^4k^4+\dots+3^4=5^4k^4+5\cdot 16+1$
$\therefore a^4\equiv 1 \pmod 5$

$a = 5k+4$: $a^4 = 5^4k^4 + \dots + 4^4 = 5^4k^4 + \dots 255 + 1$

$\therefore a^4 \equiv 1 \pmod 5$

(d) If a is not divisible by 2 or 3, Then $a^2 \equiv 1 \pmod{24}$

Pf: By Div. Alg., $a = 24k + r$, $0 \le r < 24$

Since a is not divisible by 2, r must be odd.

Since a is not divisible by 3, $r = 1, 5, 7, 11, 13, 17, 19$

$\therefore a^2 = (24k+r)^2 = 24^2k^2 + 48kr + r^2$

$r = 1$: $r^2 = 1$, $\therefore$ Let $c = 0$

$r = 5$: $r^2 = 25 = 24 + 1$. $\therefore$ Let $c = 1$

$r = 7$: $r^2 = 49 = 2 \cdot 24 + 1$ $\therefore$ Let $c = 2$

$r = 11$: $r^2 = 121 = 5 \cdot 24 + 1$ $\therefore$ Let $c = 5$

$r = 13$: $r^2 = 169 = 7 \cdot 24 + 1$ $\therefore$ Let $c = 7$

$r = 17$: $r^2 = 289 = 12 \cdot 24 + 1$ $\therefore$ Let $c = 12$

$r = 19$: $r^2 = 361 = 15 \cdot 24 + 1$ $\therefore$ Let $c = 15$

$\therefore a^2 = 24^2k^2 + 48kr + 24 \cdot c + 1$

$= 24[24k^2 + 2kr + c] + 1$

$\therefore a^2 \equiv 1 \pmod{24}$

9. If p is prime s.t. $n < p < 2n$, then

$$\binom{2n}{n} \equiv 0 \pmod{p}$$

Pf: $\binom{2n}{n} = \dfrac{1 \cdot 2 \cdot 3 \cdot \cdots n\,(n+1) \cdots (2n)}{n!\,n!} = \dfrac{(n+1) \cdots (2n)}{n!}$

$\therefore n! \binom{2n}{n} = (n+1) \cdots (2n)$

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 $\{a_1, \dots, a_n\}$ is a complete set of residues mod n and $\gcd(a, n) = 1$, Then $\{aa_1, \dots, aa_n\}$ is a complete set of residues mod n.

Pf: Consider aa_i and aa_j, $i \neq j$, $1 \le i, j \le n$

If aa_i and aa_j are congruent mod n, Then $aa_i - aa_j \stackrel{\cdot}{=} Kn$, some K. $\therefore a(a_i - a_j) = Kn$

Since $\gcd(a, n) = 1$, Then by Euclid's lemma, $n \mid (a_i - a_j)$, contradicting That $a_i \not\equiv a_j$.

$\therefore aa_i \not\equiv aa_j$

By Theorem 1 at top, $\{aa_1, \dots, aa_n\}$ 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 $0 \le n \le 9$, Then $2^n \not\equiv 0 \bmod 11$ for $0 \le n \le 9$.
$\therefore$ Consider 2^r and 2^s, $1 \le r, s \le 9$, $r \neq s$.
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 $0 \le s-r \le 8$, Then There is no $k>1$ s.t. $2^s - 2^r = 11k$. $\therefore 2^s \not\equiv 2^r \bmod 11$

$\therefore 0, 1, 2^1, 2^2, \ldots, 2^9$ is a complete set of residues mod 11.

Another proof (more obvious).

Look at remainders from Div. Alg.

$0 : r = 0$	$2^4 : 5$	$2^8 : 3$
$1 : r = 1$	$2^5 : 10$	$2^9 : 6$
$2 : r = 2$	$2^6 : 9$	
$2^2 : r = 4$	$2^7 : 7$	
$2^3 : r = 8$		

$\therefore$ Remainders are in 1-to-1 correspondence to $\{0, 1, \ldots, 9, 10\}$, and Therefore constitute a complete set of residues mod 11.

$0 : 0$	$4^2 : 5$	$8^2 : 9$
$1^2 : 1$	$5^2 : 3$	$9^2 : 4$
$2^2 : 4$	$6^2 : 3$	$10^2 : 1$
$3^2 : 9$	$7^2 : 5$	

$\therefore$ not a 1-to-1 correspondence $\therefore$ not a complete set of residues (Lemma at to of this exercise set).

12. (a) If $\gcd(a,n)=1$, Then

$c, c+a, c+2a, \ldots, c+(n-1)a$ 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. $(s-r)a = nk$.
$\therefore$ $c+sa \not\equiv c+ra$, 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
$c, c+1, c+2, \ldots, c+(n-1)$

(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 $n = \operatorname{lcm}(n_1, n_2)$

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, $1 = \frac{n_1}{dr}$

$$\therefore a - b = K_2 n_2 = K_2 n_2 \left(\frac{n_1}{dr}\right) = \frac{K_2}{r} \cdot \frac{n_1 n_2}{d}$$

But $\frac{n_1 n_2}{d} = \operatorname{lcm}(n_1, n_2)$ (Th 2.8, p. 30)

$$\therefore a - b = \frac{K_2}{r} \cdot \operatorname{lcm}(n_1, n_2)$$

Is $\frac{K_2}{r}$ an integer?

Let s be 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, $r \mid K_2$, 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 $4 \equiv 9 \bmod 5$

$2 \equiv 7 \pmod{5}$

$2^7 \equiv 3^7 \pmod{5}$?

$2^7 = 128$, $3^7 = 2187$, $2187 - 128 = 2059$,

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

$a^2 - 1 = 16r^2 + 24r + 8 = 8(2r^2 + 3r + 1)$

$\therefore \quad a^2 \equiv 1 \pmod 8$

$K \Rightarrow K+1$: Suppose $a^{2^K} \equiv 1 \pmod{2^{K+2}}$

$\therefore \quad a^{2^K} - 1 = (2^{K+2})r$, 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 $89 \mid 2^{44} - 1$

Idea: Look at multiple of 89 to see if close or off by 1 from powers of 2

$2^8 \equiv (-11) \bmod 89$
$2^3 \equiv 2^3 \cdot (-11) \equiv 1 \bmod 89$

$2^5 = 32$ $\quad 2^8 = 256$ $\quad 3 \cdot 89 = 267$
$2^6 = 64$ $\quad 2^9 = 512$ $\quad 6 \cdot 89 = 534$
$2^7 = 128$ $\quad 2^{10} = 1024$ $\quad 11 \cdot 89 = 979$
$2^{11} = 2048$ $\quad 12 \cdot 89 = 1068$
$23 \cdot 89 = 2047$

$\therefore 2^{11} \equiv 1 \pmod{89}$
$\therefore 2^{44} \equiv 1^4 \pmod{89}$

Anoter way: $2^8 \equiv (-11) \pmod{89}$ $\quad (3 \cdot 89 = 267)$
$\therefore 2^3 \cdot 2^8 \equiv 2^3 \cdot (-11) \pmod{89}$, and $2^3(-11) \equiv 1 \pmod{89}$
$\therefore 2^{11} \equiv 1 \pmod{89}$, $\therefore 2^{44} \equiv 1 \pmod{89}$

(6) $97 \mid 2^{48} - 1$

97 is close to 100, so look at powers of 2 Close to 100's. We find That $21 \cdot 97 = 2037$
$\therefore 2^{11} = 2048 \equiv 11 \pmod{97}$
$\therefore 2^{12} = 4096 \equiv 2 \cdot 11 \pmod{97}$
$\therefore 2^{48} \equiv 2^4 \cdot 11^4 \pmod{97}$
But $2^4 \cdot 11^4 = (4 \cdot 121)^2 = (484)^2$, 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

$b - d = sn$, 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. 68, $a \equiv c \pmod{n}$.

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. $\therefore a - b = k_1 r n$

$\therefore a \equiv b \pmod{n}$

Similarly, since $n | n_2$ Then $a \equiv c \pmod{n}$

$\therefore$ By Theorem 4.2 (c), $b \equiv c \pmod{n}$.