B.Sc. (H) Mathematics semester VI

Paper: Number Theory [20/04/2020 – 24/04/2020]

Book: David M. Burton, "Elementary Number Theory"

Section 4.2

Def^n Let n be a fixed positive integer. Two integers a and b are said to be congruent modulo n, symbolized by

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

if n divides the difference $a-b$;

that is, provided that $a-b = kn$ for some integer k.

Theorem 4.1 :- For arbitrary integers a and b, $a \equiv b \pmod{n}$ if and only if a and b leave the same nonnegative remainder when divided by n.

Proof: Let $a \equiv b \pmod{n}$

then $a = b + kn$ for some integer k.

By Euclidean algorithm, $b = qn + r$ where $0 \le r < n$.

Therefore,

$$a = b + kn = (qn + r) + kn$$

$$a = (q + k)n + r$$

which implies that a has the same remainder as b.

Conversely, suppose a & b leave the same nonnegative remainder when divided by n.

$a = q_1 n + r$ and $b = q_2 n + r$, with some remainder r $(0 \le r < n)$ (1)

Then $a-b = (q_1 n + r) - (q_2 n + r)$

$a-b = (q_1 - q_2) n$

whence $n \mid a-b$.

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

Theorem 4.2 Let $n>1$ be fixed and a, b, c, d be arbitrary integers. Then the following properties hold:

(a) $a \equiv a \pmod{n}$

(b) If $a \equiv b \pmod{n}$, then $b \equiv a \pmod{n}$

(c) If $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then $a \equiv c \pmod{n}$

(d) If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$ then $a+c \equiv b+d \pmod{n}$ and $ac \equiv bd \pmod{n}$

(e) If $a \equiv b \pmod{n}$, then $a+c \equiv b+d \pmod{n}$ and $ac \equiv bc \pmod{n}$

(f) If $a \equiv b \pmod{n}$, then $a^k \equiv b^k \pmod{n}$ for any positive integer k.

Proof: (a) For any integer a, we have $a-a=0 \cdot n$ so that $a \equiv a \pmod{n}$

(b) If $a \equiv b \pmod{n}$ then $a-b = kn$ for some integer k.

Hence $b-a = -(kn) = (-k)n$

and because $-k$ is an integer.

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

(c) Suppose $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$

then there exists integers h and k such that

$a-b = hn$ and $b-c = kn$

$$a-c = (a-b) + (b-c)$$

$$= hn + kn$$

$$a-c = (h+k)n$$

$\Rightarrow a \equiv c \pmod{n}$

(d) If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$

then

$a-b = k_1 n$ and $c-d = k_2 n$ for some k_1 & k_2.

$$(a+c) - (b+d) = (a-b) + (c-d)$$

$$= k_1 n + k_2 n$$

$$= (k_1 + k_2)n$$

$\Rightarrow$ $\boxed{a+c \equiv b+c \pmod{n}}$

$$ac = (b+k_1 n)(d+k_2 n)$$

$$= bd + (bk_2 + dk_1 + k_1 k_2 n)n$$

Because $bk_2 + dk_1 + k_1 k_2 n$ is an integer.

This implies $ac - bd$ is divisible by n.

Hence $\boxed{ac \equiv bd \pmod{n}}$

(e) Apply part (d) on $a \equiv b \pmod{n}$ and $c \equiv c \pmod{n}$

(f) The result is true for $k=1$

because $a \equiv b \pmod{n}$.

Assume that statement is true for k

i.e. $a^k \equiv b^k \pmod{n}$

Together imply that $aa^k \equiv bb^k \pmod{n}$

or $a^{k+1} \equiv b^{k+1} \pmod{n}$

so by induction, the result is true for every k.

Example Show that 41 divides $2^{20} - 1$.

Soln:- Since $2^5 \equiv -9 \pmod{41}$

$$(2^5)^4 \equiv (-9)^4 \pmod{41}$$

$$2^{20} \equiv 81 \cdot 81 \pmod{41}$$

But $81 \equiv -1 \pmod{41}$

so $81 \cdot 81 \equiv 1 \pmod{41}$

$$\Rightarrow 2^{20} - 1 \equiv 81 \cdot 84 \equiv 1 - 1$$

$$2^{20} - 1 \equiv 0 \pmod{41}$$

Thus $41 \mid 2^{20}-1$.

Example: Find the remainder obtain upon dividing the sum

$1! + 2! + 3! + 4! + \cdots + 99! + 100!$ by 12.

Soln:-

Observe that $4! = 24 \equiv 0 \pmod{12}$

for $k \geq 4$

$$k! \equiv 4! \cdot 5 \cdot 6 \cdots k \equiv 0 \cdot 5 \cdot 6 \cdots k$$

$$\equiv 0 \pmod{12}$$

In this way, we find that

$$1! + 2! + 3! + 4! + \cdots + 100!$$

$$\equiv 1! + 2! + 3! + 0 + \cdots + 0$$

$$\equiv 9 \pmod{12}$$

Thus, the sum leaves a remainder of 9 when divided by 12.

Theorem 4.3 If $ca \equiv cb \pmod{n}$, then $a \equiv b \pmod{n/d}$ where $d = \gcd(c, n)$

Corollary If $ca \equiv cb \pmod{n}$ and $\gcd(c, n) = 1$, then $a \equiv b \pmod{n}$.

Exercise - 4.2

1. Prove each of the following assertions:

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

(b) If $a \equiv b \pmod{n}$ and $c > 0$ then $ca \equiv cb \pmod{cn}$

(c) If $a \equiv b \pmod{n}$ and the integers a, b, n are divisible by $d > 0$ then $a/d \equiv b/d \pmod{n/d}$

Proof: (a) $a \equiv b \pmod{n} \Rightarrow a - b = kn$ for some k.

$m \mid n \Rightarrow n = rm$ for some r.

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

(b) If $a \equiv b \pmod{n}$

$a - b = kn$ some k

$ca - cb = kcn$

$\Rightarrow ca \equiv cb \pmod{cn}$

(c) If $a \equiv b \pmod{n}$ and a, b, d all divisible by $d > 0$,

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

$a - b = kn$ for some k.

By assumption

$a = k_1 d \Rightarrow a/d = k_1$

$b = k_2 d \Rightarrow b/d = k_2$

$n = k_3 d \Rightarrow n/d = k_3$

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

$\therefore k_1 - k_2 = k k_3$

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

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

Q-4

Question-4 (a) Find the remainders when 2^{50} and 41^{65} are divided by 7.

Sol:

$$2^{50} = (2^5)^{10}$$

and $2^5 = 4.7 + 4$

so $2^5 \equiv 4 \pmod 7$

$\Rightarrow (2^5)^{10} \equiv 4^{10} \pmod 7$

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

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

and $2^5 \equiv 4 \pmod 7$

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

But $4^4 \equiv 4 \pmod 7$

so $4^4 - 4 \equiv 0 \pmod 7$

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

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

$\Rightarrow$ remainder will be 4.

Questions to be done 4, 5, 6, 10, 11, 12

Assignment