Number Theory 9

30 January 2024 17:57

Modular Number Theory :-

$a \equiv b \pmod{c}$

$\rightarrow$ $\exists$ a q such that $a = cq + b$
which is also equivalent to
$\exists$ a q' such that $b = cq' + a$

$a = cq + b$
$b = a - cq$
$= cq' + a$

$a \equiv b \pmod{c}$
$\Updownarrow$ Same as
$b \equiv a \pmod{c}$

$3 \equiv 13 \pmod{10}$
$-1 \equiv 7 \pmod{8}$

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

Q> Let a, n be fixed integers. Show that the set of integers b such that $b \equiv a \pmod{n}$ form an arithmatic progression. What is the common difference?

Ans:- $b_1 = nq_1 + a$
$b_2 = nq_2 + a$

$b_2 - b_1 = n(q_2 - q_1) \equiv 0 \pmod{n}$
$\rightarrow b_2 - b_1 =$ common difference $= nK$

$b_2 = b_1 + nk = n(q_1 + k) + a$
⋮
so on

$a \equiv r \pmod{b}$

r is remainder if $0 \leq r < b$

- $a \equiv x \pmod{c}$

  $b \equiv y \pmod{c}$

Then $a+b \equiv x+y \pmod{c}$

$a = ck_1 + x$
$b = ck_2 + y$ $\Rightarrow a+b = c(k_1+k_2) + (x+y)$

- $a \equiv x \pmod{c}$

  $b \equiv y \pmod{c}$

Then $ab \equiv xy \pmod{c}$

$a = ck_1 + x$
$b = ck_2 + y$ $\Rightarrow ab = (ck_1+x)(ck_2+y)$

$= c^2 k_1 k_2 + ck_2 x + ck_1 y + xy$

Q) Find the remainder when 2^{10} is divided by 10

Ans:- $2^{10} \equiv 2^3 \times 2^3 \times 2^3 \times 2 \pmod{10}$

$\equiv \underbrace{8 \times 8} \times \underbrace{8 \times 2} \pmod{10}$

$\equiv \underbrace{4 \times 6} \pmod{10}$

$\equiv 4 \pmod{10}$

---

positive

Q> Show that $a-b \mid a^n - b^n$ for any positive integer n

Ans:— $a^n - b^n = a\,a^{n-1} - a b^{n-1} + a b^{n-1} - b^n$

$$= a(a^{n-1} - b^{n-1}) + b^{n-1}(a-b)$$

$$\equiv a(a^{n-1} - b^{n-1}) \pmod{(a-b)}$$

$\vdots$

So on

$$\equiv a^{n-1}(a-b) \pmod{(a-b)}$$

$$\equiv 0 \pmod{(a-b)}$$

HomeWork

Q> If p is an odd prime and a, b are coprime, show that

$$\gcd\left(\frac{a^p + b^p}{a+b}, a+b\right) \in \{1, p\}$$

HomeWork

Q> Let f be a polynomial with integer coefficients. Show that $(a-b) \mid (f(a) - f(b))$ for any integers a, b which is same as saying $f(a+d) \equiv f(a) \pmod{d}$