Number Theory 10

03 February 2024 10:56

HomeWork

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

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

Ans:- $\gcd(a^{p-1} - a^{p-2}b + a^{p-3}b^2 - \cdots + b^{p-1}, a+b)$

$\gcd(a,b)=1 \Rightarrow a \nmid (a+b)$ & $b \nmid (a+b)$

$a \mid (a^{p-1} - a^{p-2}b + \cdots - ab^{p-2})$

$b \mid (-a^{p-2}b + \cdots - ab^{p-2} + b^{p-1})$

$\gcd(a, a+b)=1$ $\quad$ $\gcd(b, a+b)=1$

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

$\equiv -b \pmod{a+b}$

in (mod p)

$\gcd((-b)^{p-1} - (-b)^{p-2}b + (-b)^{p-3}b^2 - \cdots + b^{p-1}, a+b)$

$= \gcd(b^{p-1} + b^{p-1} + b^{p-1} + \cdots + b^{p-1}, a+b)$

$= \gcd(pb^{p-1}, a+b)$

$\gcd(b^{p-1}, a+b) = 1 \Rightarrow$ If $p \mid (a+b)$ then $\gcd(pb^{p-1}, a+b) = p$

else $\gcd(pb^{p-1}, a+b) = 1$

Q> Find all primes p and q such that $p+q = (p-q)^3$

Ans:- $q \equiv -q^3 \pmod p \Rightarrow q + q^3 \equiv 0 \pmod p$

$\Rightarrow q(q^2+1) \equiv 0 \pmod p$

$\Rightarrow p \mid q(q^2+1)$

$p \equiv p^3 \pmod q \Rightarrow p - p^3 \equiv 0 \pmod q$

$\Rightarrow q \mid p(1-p^2)$

$\Rightarrow q \mid p(p^2-1)$

$$p+q = (p-q)^3 \Rightarrow (p+q) \mid (p-q)^3 \Rightarrow (p-q)^3 \equiv 0 \pmod{p+q}$$

$$(p-q) \equiv -2q \pmod{p+q}$$

$$(p-q)^3 \equiv -8q^3 \pmod{p+q} \longrightarrow -8q^3 \equiv 0 \pmod{p+q}$$

$$\Rightarrow (p+q) \mid 8q^3$$

$p \neq q$ is must else $p+q = (p-q)^3 = 0$ not possible

$\gcd(p+q, q) = 1 \Rightarrow p+q \nmid q \Rightarrow (p+q) \mid 8q^3$ means $(p+q) \mid 8$

So $(p+q) \in \{1, 2, 4, 8\}$

$q, p \in \{1, 3, 5, 7\}$ so $(p, q) = (5, 3)$

Fermat's Little Theorem :-

Let a be any number coprime to a prime p. Then
$$a^p \equiv a \pmod{p}$$

Q) Let a, b be integers and p be a prime. Then show that $p \mid (ab^p - a^p b)$

Inverse :-

Let p be a prime and a be an integer coprime to p

Let p be a prime and a be an integer coprime to p

Then there always exists an integer x such that,

$$ax \equiv 1 \pmod p$$

This x is called the inverse of a modulo p.

x is also written as a^{-1} or $\frac{1}{a}$.

$$x \equiv \frac{1}{a} \pmod p$$

Examples:-

$$a \equiv 3 \pmod 7$$

$$x \equiv 5 \Rightarrow ax \equiv 1 \pmod 7$$

$$\Rightarrow x \equiv \frac{1}{3} \pmod 7$$

$$x \equiv \frac{y}{z} \pmod p \Rightarrow xz \equiv y \pmod p$$

Lemma:- Let $b, d \not\equiv 0 \pmod p$. Then for any a, c, we get,

$$\frac{a}{b} + \frac{c}{d} \equiv \frac{(ad+bc)}{bd} \pmod p$$

(normal addition of fractions holds)

$$\frac{a}{b} \cdot \frac{c}{d} \equiv \frac{ac}{bd} \pmod p$$

(normal multiplication of fractions holds)

Q> Find the inverse of all $\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$ modulo 11.

Ans:– $1^{-1} = 1$, $2^{-1} = 6$, $3^{-1} = 4$, $5^{-1} = 9$, $6^{-1} = 2$, $7^{-1} = 8$,
$4^{-1} = 3$, $8^{-1} = 7$, $9^{-1} = 5$, $10^{-1} = 10$

$$(p-1)(p-k) = p(p-k) - 1(p-k)$$
$$= p(p-k) - p + k \equiv k \pmod p$$
$$\equiv 1 \pmod p$$

So $k = 1$ as $k \in \{0, \ldots, p-1\}$

So, $(p-1)^{-1} = (p-1)$
for p prime

Q> If $a \not\equiv 0 \pmod p$ then show that $a^{p-2} \equiv a^{-1} \pmod p$

Ans:– $a^{p-1} \equiv 1 \pmod p$
$\Rightarrow a\, a^{p-2} \equiv 1 \pmod p$
$\Rightarrow a^{p-2} \equiv a^{-1} \pmod p$

Q> Show that $(a^{-1})^n \equiv (a^n)^{-1} \pmod p$.

Ans:– $(a^n)^{-1} = \frac{1}{a^n}$ $\quad a^n (a^{-1})^n = a^n \frac{1}{a^n} = 1$

$\Rightarrow$ Proved.

Q> Prove that 7 is only prime of the form $n^3 - 1$.

Ans:– $(n^3-1) = \underset{\rightarrow P_1}{(n-1)}\underset{\rightarrow P_2}{(n^2+n+1)}$ $\quad$ $2k \rightarrow p \in k$'s factor

So n can't be odd
So n must be even
So iff $n-1 = 1$ then n^2+n+1 can be a prime
So $n^3 - 1 = 2^3 - 1 = 7$ is the only prime