Integers & Division - 2

Wednesday, November 4, 2020 8:51 AM

Lemma: If a, b, and c are integers such that $\gcd(a,b)=1$, and $a \mid bc$, then $a \mid c$.

Proof: Because $\gcd(a,b)=1$, by Bézout's theorem, there are integers s and t such that,

$$\boxed{sa + tb = 1.}$$

Multiplying both sides by c we obtain,

$$sac + tbc = c$$

By part (ii) of theorem-1, as $a \mid bc$, then $a \mid tbc$.

By part (i) of theorem-1, as $a \mid sac$ and $a \mid tbc$, we conclude $a \mid sac + tbc$.

Because $sac + tbc = c$, it follows $a \mid c$, completing the proof.

$a_1 \cdot a_2 \cdots a_n$

$a_1 a_2 \cdots a_{n-1}$, a_n

Lemma: If p is a prime and $p \mid a_1 a_2 \ldots a_n$, where each a_i is an integer, then $p \mid a_i$ for some i.

Proof: Since p is a prime, then either $p \mid a_1 a_2 \cdots a_{n-1}$ or $p \mid a_n$.

If $p \mid a_n$, then we get $i = n$, such that $p \mid a_i$

If $p \mid a_1 a_2 \ldots a_{n-1}$, then again p is a prime and either $p \mid a_1 a_2 \ldots a_{n-2}$ or $p \mid a_{n-1}$.

If $p \mid a_{n-1}$, then we get $i = n-1$, s.t. $p \mid a_i$

else $p \mid a_1 a_2 \ldots a_{n-2}$

We apply the same procedure as above and will eventually get some i for which $p \mid a_i$.

<u>Theorem</u>: Prime factorization of a positive integer is unique.

<u>Proof</u>: We will use proof by contradiction. Suppose that a positive integer n can be written as product of primes in two different ways, say

$n = p_1 p_2 \ldots p_s$ and $n = q_1 q_2 \ldots q_t$, each p_i and q_j are primes such that $p_1 \le p_2 \le \ldots \le p_s$ and $q_1 \le q_2 \le \ldots \le q_t$.

When we remove the common primes from the two factorization then we have,

$$\underline{p_{i_1} p_{i_2} \ldots p_{i_u}} = \underline{q_{j_1} q_{j_2} \ldots q_{j_v}}.$$

where no prime occurs on both sides of this equation and u & v are +ve integers.

By Lemma, it follows that $p_{i_1} \mid q_{j_k}$ for some k. Because no prime divides another prime, ~~this is impossible~~. Consequently, there can be at most one factorization of n into primes of non-decreasing order.

Modular Arithmetic:

Theorem-1: Let a and b be integers, and let m be a positive integer. Then $a \equiv b \pmod{m}$ iff $a \bmod m = b \bmod m$.

Proof: Let $a \bmod m = r_1$ and $b \bmod m = r_2$, r_1 and r_2 are positive integers. Suppose k and l are two integers such that

$$a = mk + r_1 \text{ and } b = ml + r_2.$$

If $a \equiv b \pmod{m}$, by the defn. of congruency, we know $m \mid (a-b)$. Therefore,

$$a - b = m(k-l) + (r_1 - r_2).$$

Dividing both sides by m we get,

$$\frac{a-b}{m} = (k-l) + \left(\frac{r_1 - r_2}{m}\right)$$

If $m \mid (a-b)$, then $\left(\frac{r_1 - r_2}{m}\right) = 0$ which follows that $r_1 = r_2$ i.e. $a \bmod m = b \bmod m$, which completes the proof.

Theorem: Let m be a +ve integers. The integers a and b are Congruent modulo m iff there is an integer k s.t. $a = b + km$.

Proof: If $a \equiv b \pmod{m}$, then by defn. of Congruency $m \mid (a-b)$. This means there is an integer K such that $a - b = K.m$, so that $a = b + K.m$.

Conversely, if there is an integer K such that $a = b + Km$, then $Km = a - b$. Hence $m \mid (a-b)$ which ~~foo~~ follows $a \equiv b \pmod{m}$.

Theorem: Let m be a positive integer. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a + c \equiv b + d \pmod{m}$ and $ac \equiv b.d \pmod{m}$.

Because $m \mid a-b$, then $a = b + s.m$ for some integer s.

Because $m \mid c-d$, then $c = d + t.m$ for some integer t.

Why mathematical induction is valid?

* Well-ordering property for a set of non-negative

Integers :- every nonempty subset of non-negative integers has a least element.

Let $P(1)$ is true and that the proposition $P(K) \to P(K+1)$ for all positive integers K.

Assume that there is at least one positive integer for which $P(n)$ is false. Then the set S of positive integers for which $P(n)$ is false is non-empty. Thus, by the well-ordering property, S has a least element, which will be denoted by m. We know that m cannot be 1, because $P(1)$ is already true. Because m is positive and greater than 1, $(m-1)$ is also an integer. Furthermore, as $(m-1)$ is less than m, it is not in S. So $P(m-1)$ is also true. Because the conditional statement $P(m-1) \to P(m)$ is also true (inductive step), it must be the case that $P(m)$ is true. This contradicts the choice of m. Hence $P(n)$ must be true for every positive integer n.

Prob 2: Prove that sum of first n odd integers is n^2.

$\rightarrow$ $P(n): 1+3+5+7+\ldots+(2n-1)=n^2$

Basis step: $P(1) = 1^2 = 1$ (true)

Inductive step: Suppose $P(k)$ is true for an arbitrary integer k.

$$1 + 3 + 5 + \ldots + (2k-1) = k^2$$

We have to show that $P(k+1)$ is true

i.e. $1 + 3 + 5 + \ldots + (2k-1) + (2k+1) = (k+1)^2$

$$\underbrace{1 + 3 + 5 + \ldots + (2k-1)}_{k^2 \text{ (IH)}} + (2k+1)$$

$$\Rightarrow k^2 + 2k + 1 = (k+1)^2.$$