05 Elementary Number Theory

05_01 Divisibility

Division Algorithm. If a is an integer and d is a positive integer, then there are unique integers q and r, with $0 \le r < d$, such that $a = d*q + r$. where

d is called the divisor.

a is called the dividend.

q is called the quotient, denoted a div d.

r is called the remainder, denoted a mod d.

Example. Find the quotient and remainder when 174 is divided by 5.

Notice that $174 = 5*34 + 4$. Thus

The quotient is 34 and the remainder is 4.

Example. Find the quotient and remainder when 63 is divided by 7.

Notice that $63 = 7*9 + 0$. Thus

The quotient is 9 and the remainder is 0.

Example. Find the quotient and remainder when 17 is divided by 34.

Notice that $17 = 34*0 + 17$. Thus

The quotient is 0 and the remainder is 17.

Definition. If a and b are two integers with $a \neq 0$, then a divides b, denoted a | b, is defined as if there exists an integer c such that b = a*c. When a divides b, we say that a is a factor or divisor of b. We also say that b is a multiple of a. Clearly, if a | b, then $b \div a = b/a$ is an integer. We use $a \nmid b$ to denote that a does not divide b.

Example. If a = 7 and b = 63, then there exists an integer c = 9 such that 63 = 7*c. Then we have 7 | 63. We can say that 7 divides 63, 63 is divisible by 7, 7 is a factor or divisor of 63, and 63 is a multiple of 9.

Example. If a = 17 and b = 88, then, for any an integer c, b = a*c is not true. Then we have $a \nmid b$. We can say that 17 doesn't divide 88, 88 is not divisible by 17, 17 is not a factor and not a divisor of 63, and 63 is not a multiple of 9.

Example. If n is any integer which is not equal to 0. Then 0 = n*0. Then we have n | 0. We can say that n divides 0, 0 is divisible by n, n is a factor or divisor of 0, and 0 is a multiple of n.

Example. If n is any integer which is not equal to 0. Then n = n*1. Then we have n | n. We can say that n divides n, n is divisible by n, n is a factor or divisor of n, and n is a multiple of n.

Example. If n is any integer. Then $n = n*1$. Then we have $1 \mid n$. We can say that 1 divides n, n is divisible by 1, 1 is a factor or divisor of n, and n is a multiple of 1.

Theorem 1. Suppose a, b, and c are integers with $a \neq 0$.

(1) If $a \mid b$ and $a \mid c$, then $a \mid (b + c)$ and $a \mid (b - c)$;

(2) If $a \mid b$, then $a \mid (b*c)$ for all integers c;

(3) If $b \neq 0$, $a \mid b$, and $b \mid c$, then $a \mid c$.

[Proof of (1) in Theorem 1] Since $a \mid b$ and $a \mid c$, there are two integers i and j such that $b = a*i$ and $c = a*j$. Hence $b + c = a*i + a*j = a*(i + j)$ and $b - c = a*i - a*j = a*(i - j)$. So $a \mid (b + c)$ and $a \mid (b - c)$.

[Proof of (2) in Theorem 1] Since $a \mid b$, there is an integer i such that $b = a*i$. Therefore $b*c = a*i*c = a*(i*c)$. So $a \mid (b*c)$.

[Proof of (3) in Theorem 1] Since $a \mid b$ and $b \mid c$, there are two integers i and j such that $b = a*i$ and $c = b*j$. Hence $c = b*j = a*i *j = a*(i*j)$. So $a \mid c$.