Divisibility Theory in the integers

The Division Algorithm

Theorem 1. Given integers a and b, with $b > 0$, there exist unique integers q and r satisfying

$$a = qb + r, \quad 0 \le r < b.$$

The integers q and r are called, respectively, the quotient and remainder in the division of a and b.

Proof:- Lets begin by proving that the set

$$S = \{a - xb \mid x \text{ an integer} ; a - xb \ge 0\}.$$

is non-empty.

To do this, it suffices to exhibit a value of x making $a - xb$ non-negative.

Since $b \ge 1$, we get -

$$|a| b \ge |a|. \text{ So we have}$$

$$a - (-|a|)b = a + |a|b \ge a + |a| \ge 0.$$

For the choice $x = -|a|$, we get $a - xb \in S$.

Hence by the Well-Ordering Principle, we can say that the set S contains a smallest integer; ~~call~~ let us say r.

By defn of S, there exists an integer q satisfying

$$r = a - qb, \quad 0 \le r.$$

Claim: $r < b$.

On the contrary, let $r \ge b$.

$$a - (q+1)b = (a - qb) - b = r - b \ge 0.$$

This gives $a - (q+1)b \in S$.

But $a - (q+1)b = r - b < r$, which is a contradiction [illegible] smallest member of S.

Hence, $\boxed{r < b}$.

<u>To show the uniqueness of q and r</u>:

Suppose that a has two representations of the desired form, say,

$$a = qb + r \quad \& \quad a = q'b + r';$$

where $0 \le r < b$, $0 \le r' \le b$.

Then, $r' - r = b(q - q')$

$|r' - r| = b|q - q'|$ (taking the absolute values)

Now $-b < -r \le 0$ and $0 \le r' < b$,

Adding, we get —

$$-b \le r' - r < b.$$

or, $|r' - r| < b$.

Thus $b|q - q'| < b$, which gives —

$$0 \le |q - q'| < 1.$$

Since $|q - q'|$ is a non-negative integer, the only possibility is that $|q - q'| = 0$, whence $q = q'$; which in turn gives $r = r'$. $\square$.

~~Corollary: If a~~

<u>Note</u> :- A more general version of the Division ~~Algori~~ Algorithm is obtained on replacing the restriction that b must be positive by the simple requirement that $b \neq 0$.

Corollary- If a and b are integers, with $b \neq 0$, then there exist unique integers q and r such that

$$a = qb + r, \quad 0 \leq r < |b|.$$

Proof: It is enough to consider the case in which b is negative. Then $|b| > 0$, and Theorem 1 produces unique integers q' and r for which

$$a = q'|b| + r, \quad 0 \leq r < |b|.$$

Noting that $|b| = -b$, we may take $q = -q'$ to arrive at $a = qb + r$, with $0 \leq r < |b|$.

To illustrate the DA, when $b \leq 0$, let us take $b = -7$. Then for the choices of $a = 1, -2, 61$ and -59, we get the expressions

$$1 = 0(-7) + 1$$
$$-2 = 1(-7) + 5$$
$$61 = (-8)(-7) + 5$$
$$-59 = 9(-7) + 4.$$

Applications of DA:

With $b = 2$, the possible remainders are $r = 0$ & $r = 1$.

When $r = 0$, the integer a has the form $a = 2q$ and called even &

When $r = 1$, the integer a has the form $a = 2q + 1$ & called odd

Now a^2 is either of the form $(2q)^2 = 4k$ or

$$(2q+1)^2 = 4(q^2+q) + 1 = 4k+1.$$

The point is that the square of an integer leaves the remainder 0 or 1 upon divisible by 4.

We can show, the square of any odd integer is of the form $8k+1$.

By Division Algorithm, any integer is representable as one of the four forms:

$$4q,\ 4q+1,\ 4q+2,\ 4q+3.$$

Only those integers of the form $4q+1$ & $4q+3$ are odd. We find that

$$(4q+1)^2 = 8(2q^2+q)+1 = 8k+1$$

& Similarly,

$$(4q+3)^2 = 8(2q^2+3q+1)+1 = 8k+1.$$

eg odd integer $7^2 = 49 = 8\cdot 6+1$ & $13^2 = 169 = 8\cdot 21+1$.

Ex. Let us show that the expression $\frac{a(a^2+2)}{3}$ is an integer for all $a \geq 1$. According to the DA, every a is of the form $3q$, $3q+1$ or $3q+2$.

Let $a = 3q$, $\frac{a(a^2+2)}{3} = q(9q^2+2) \longrightarrow$ which is an integer.

Similarly, let $a = 3q+1$,

then $$\frac{(3q+1)((3q+1)^2+2)}{3} = \underbrace{(3q+1)(3q^2+2q+1)}_{\text{an integer}}$$

Finally, for $a = 3q+2$;

$$\frac{(3q+2)((3q+2)^2+2)}{3} = \underbrace{(3q+2)(3q^2+4q+2)}_{\text{integer}}.$$

Hence, our result is established in all cases.

The Greatest Common Divisor

Definition: An integer b is said to be divisible by an integer $a \neq 0$, in symbol $a|b$, if there exists some integer c s.t. $b = ac$. We write $a \nmid b$ to indicate that b is not divisible by a.

For eg:- -12 is divisible by 4, because $-12 = 4(-3)$. However, 10 is not divisible by 3; since there is no integer c that makes the statement $10 = 3c$ true.

$a|b$ — a is a divisor of b
— a is a factor of b
— b is a multiple of a.

If a is a divisor of b, then b is also divisible by $-a$. [indeed, $b = ac$ implies $b = (-a)(-c)$], so that the divisors of an integer occur in pairs.

Note:- To find all the divisors of a given integer, it is sufficient to obtain the positive divisors and then adjoin to them the corresponding negative integers.

Thm 2: For integers a, b, c, the following hold

(a) $a|0$, $1|a$, $a|a$
(b) $a|1$ if and only if $a = \pm 1$.
(c) If $a|b$ & $c|d$, then $ac|bd$.
(d) If $a|b$ & $b|c$, then $a|c$.
(e) $a|b$ & $b|a$ if and only if $a = \pm b$
(f) If $a|b$ & $b \neq 0$, then $|a| \leq |b|$.
(g) If $a|b$ & $a|c$, then $a|(bx + cy)$ for arbitrary integers x & y.