Divisibility Theory in the integers

Prepared by
Mr. Raut S.R.
Assit.Prof. and Head,
Dept. of Mathematics,
Mrs.K.S.K.College Beed.

"*Integral numbers are the fountainhead of all mathematics.*"

H. MINKOWSKI

"*Number was born in superstition and reared in mystery, . . . numbers were once made the foundation of religion and philosophy, and the tricks of figures have had a marvellous effect on a credulous people.*"

F. W. PARKER

Plato said, "God is a geometer." Jacobi changed this to, "God is an arithmetician." Then came Kronecker and fashioned the memorable expression, "God created the natural numbers, and all the rest is the work of man."

FELIX KLEIN

WELL-ORDERING PRINCIPLE. *Every nonempty set S of nonnegative integers contains a least element; that is, there is some integer a in S such that $a < b$ for all b belonging to S.*

THEOREM 1-2 (Principle of Finite Induction). *Let S be a set of positive integers with the properties*

(i) *1 belongs to S, and*

(ii) *whenever the integer k is in S, then the next integer $k+1$ must also be in S.*

Then S is the set of all positive integers.

1. Establish the formulas below by mathematical induction:

(a) $1+2+3+\cdots+n=\dfrac{n(n+1)}{2}$ for all $n\geq 1$;

(b) $1+3+5+\cdots+(2n-1)=n^2$ for all $n\geq 1$;

(c) $1\cdot 2+2\cdot 3+3\cdot 4+\cdots+n(n+1)=\dfrac{n(n+1)(n+2)}{3}$ for all $n\geq 1$;

(d) $1^2+3^2+5^2+\cdots+(2n-1)^2=\dfrac{n(4n^2-1)}{3}$ for all $n\geq 1$;

(e) $1^3+2^3+3^3+\cdots+n^3=\left[\dfrac{n(n+1)}{2}\right]^2$ for all $n\geq 1$.

2. If $r\neq 1$, show that

$$a+ar+ar^2+\cdots+ar^n=\frac{a(r^{n+1}-1)}{r-1}$$

for any positive integer n.

3. Use the Second Principle of Finite Induction to establish that

$$a^n-1=(a-1)(a^{n-1}+a^{n-2}+a^{n-3}+\cdots+a+1)$$

THE BINOMIAL THEOREM

the general binomial expansion will take the form

$$(a+b)^n = \binom{n}{0}a^n + \binom{n}{1}a^{n-1}b + \binom{n}{2}a^{n-2}b^2 + \cdots + \binom{n}{n-1}ab^{n-1} + \binom{n}{n}b^n$$

or, written more compactly,

$$(a+b)^n = \sum_{k}^{n} \binom{n}{k} a^{n-k}b^k.$$

In Particular,

$$(a+b)^1 = a+b,$$
$$(a+b)^2 = a^2+2ab+b^2,$$
$$(a+b)^3 = a^3+3a^2b+3ab^2+b^3,$$
$$(a+b)^4 = a^4+4a^3b+6a^2b^2+4ab^3+b^4, \text{ etc.}$$

THEOREM 2-1 (Division Algorithm). *Given integers a and b, with $b > 0$, there exist unique integers q and r satisfying*

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

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

Proof: We begin by proving that the set

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

is nonempty. For this, it suffices to exhibit a value of x making $a - xb$ nonnegative. Since the integer $b \geq 1$, we have $|a|\, b \geq |a|$ and so

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

Hence, for the choice $x = -|a|$, $a - xb$ will lie in S. This paves the way for an application of the Well-Ordering Principle, from which we infer that the set S contains a smallest integer; call it r. By the definition of S, there exists an integer q satisfying

$$r = a - qb, \qquad 0 \leq r.$$

We argue that $r < b$. If this were not the case, then $r \geq b$ and

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

The implication is that the integer $a-(q+1)b$ has the proper form to belong to the set S. But $a-(q+1)b=r-b<r$, leading to a contradiction of the choice of r as the smallest member of S. Hence, $r<b$.

We next turn to the task of showing the uniqueness of q and r. Suppose that a has two representations of the desired form; say

$$a=qb+r=q'b+r',$$

where $0\leq r<b$, $0\leq r'<b$. Then $r'-r=b(q-q')$ and, owing to the fact that the absolute value of a product is equal to the product of the absolute values,

$$|r'-r|=b|q-q'|.$$

Upon adding the two inequalities $-b<-r\leq 0$ and $0\leq r'<b$, we obtain $-b<r'-r<b$ or, in equivalent terms, $|r'-r|<b$. Thus, $b|q-q'|<b$, which yields

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

Since $|q-q'|$ is a nonnegative integer, the only possibility is that $|q-q'|=0$, whence $q=q'$; this in its turn gives $r=r'$, ending the proof.

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

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

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

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

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

To illustrate the Division Algorithm when $b < 0$, let us take $b = -7$. Then, for the choices of $a = 1, -2, 61$, and -59, one gets the expressions

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

We wish to focus attention, not so much on the Division Algorithm, as on its applications. As a first example, note that with $b = 2$ the possible remainders are $r = 0$ and $r = 1$. When $r = 0$, the integer a has the form $a = 2q$ and is called *even*; when $r = 1$, the integer a has the form $a = 2q + 1$ and is 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 to be made is that the square of an integer leaves the remainder 0 or 1 upon division by 4.

PROBLEMS 2.1

1. Prove that if a and b are integers, with $b > 0$, then there exist unique integers q and r satisfying $a = qb + r$, where $2b \leq r < 3b$.
2. Show that any integer of the form $6k + 5$ is also of the form $3k + 2$, but not conversely.
3. Use the Division Algorithm to establish that
   (a) every odd integer is either of the form $4k + 1$ or $4k + 3$;
   (b) the square of any integer is either of the form $3k$ or $3k + 1$;
   (c) the cube of any integer is either of the form $9k$, $9k + 1$, or $9k + 8$.

Divisibility:

DEFINITION 2-1. An integer b is said to be *divisible* by an integer $a \neq 0$, in symbols $a \mid b$, if there exists some integer c such that $b=ac$

We write $a \nmid b$ to indicate that b is not divisible by a.

Thus, for example, -12 is divisible by 4, since $-12 = 4(-3)$. However, 10 is not divisible by 3; for there is no integer c which makes the statement $10 = 3c$ true.

There is other language for expressing the divisibility relation $a \mid b$. One could say that a is a *divisor* of b, that a is a *factor* of b or that b is a *multiple* of a. Notice that, in Definition 2-1, there is a restriction on the divisor a: whenever the notation $a \mid b$ is employed, it is understood that a is different from zero.

If a is a divisor of b, then b is also divisible by $-a$ (indeed, $b = ac$ implies that $b = (-a)(-c)$), so that the divisors of an integer always occur in pairs. In order 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. For this reason, we shall usually limit ourselves to a considcration of positivc divisors.

Basic Properties of Divisibility

THEOREM 2-2. *For integers a, b, c, the following hold:*

(1) $a \mid 0, 1 \mid a, a \mid a$.

(2) $a \mid 1$ *if and only if* $a = \pm 1$.

(3) *If* $a \mid b$ *and* $c \mid d$, *then* $ac \mid bd$.

(4) *If* $a \mid b$ *and* $b \mid c$, *then* $a \mid c$.

(5) $a \mid b$ *and* $b \mid a$ *if and only if* $a = \pm b$.

(6) *If* $a \mid b$ *and* $b \neq 0$, *then* $|a| \leq |b|$.

(7) *If* $a \mid b$ *and* $a \mid c$, *then* $a \mid (bx + cy)$ *for arbitrary integers* x *and* y.

The Greatest Common Divisor:

Common Divisor:

If a and b are arbitrary integers, then an integer d is said to be a *common divisor* of a and b if both $d \mid a$ and $d \mid b$. Since 1 is a divisor of every integer, 1 is a common divisor of a and b; hence, their set of positive common divisors is nonempty. Now every integer divides 0, so that if $a = b = 0$, then every integer serves as a common divisor of a and b.

DEFINITION 2-2. Let a and b be given integers, with at least one of them different from zero. The *greatest common divisor* of a and b, denoted by gcd (a, b), is the positive integer d satisfying

(1) $d \mid a$ and $d \mid b$,
(2) if $c \mid a$ and $c \mid b$, then $c \leq d$.

Examples:

Example 2-1

The positive divisors of -12 are $1, 2, 3, 4, 6, 12$, while those of 30 are $1, 2, 3, 5, 6, 10, 15, 30$; hence, the positive common divisors of -12 and 30 are $1, 2, 3, 6$. Since 6 is the largest of these integers, it follows that $\gcd(-12, 30) = 6$. In the same way, one can show that

$$\gcd(-5, 5) = 5, \quad \gcd(8, 17) = 1, \quad \text{and} \quad \gcd(-8, -36) = 4.$$


Thank
You