CISC-102
Winter 2016
Lecture 9

Properties of the Integers

Let a,b $\in \mathbb{Z}$ then

1. if c = a + b then c $\in \mathbb{Z}$
2. if c = a - b then c $\in \mathbb{Z}$
3. if c = (a)(b) then c $\in \mathbb{Z}$
4. if c = a/b then c $\in \mathbb{Q}$

If a & b are integers the quotient a/b may not be an integer. For example if c = 1/2, then c is not an integer. On the other hand with c = 6/3 then c is n integer.

We can say that *there exists* integers a,b such that c = a/b is not an integer.

We can also say that *for all* integers a,b we have c = a/b is a rational number.

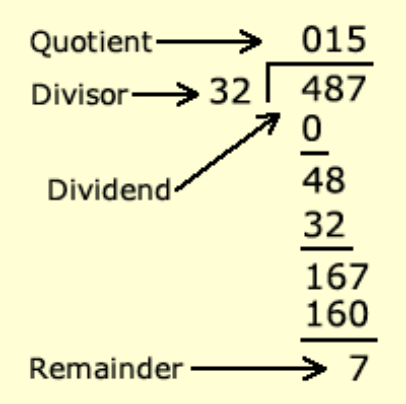
Divisibility

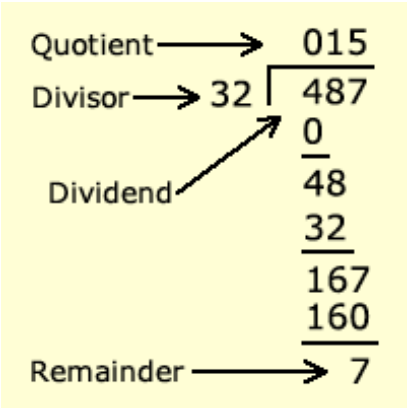
Let a,b $\in \mathbb{Z}$, a $\neq 0$.
If c = $\frac{b}{a}$ is an integer,

or alternately if c $\in \mathbb{Z}$ such that b = ca
then we say that a *divides* b or equivalently,
b is *divisible* by a, and this is written

$$a \mid b$$

NOTE: Recall long division:





Referring to the long division example, b = 32, is the divisor a = 487 is the dividend. The quotient q = 15 and the remainder r = 7.
In this case b *does not divide* a
or equivalently a is *not divisible* by b.

This can be notated as:

$$b \nmid a$$

and we can write $a = bq + r$ or, $487 = (32)(15) + 7$

Division Algorithm Theorem

Let $a,b \in \mathbb{Z}$, $b \neq 0$ there exists $q,r \in \mathbb{Z}$, such that:

$$a = bq + r,\ 0 \leq r < |b|$$

NOTE: The remainder in the Division Algorithm Theorem is always positive.

Notation

The *absolute value* of b denoted by

$$|\, b \,|$$

is defined as:

$$|\, b \,| = b \text{ if } b \geq 0$$

$$\text{and } |\, b \,| = -b \text{ if } b < 0.$$

Therefore for values

a = 22, b = 7, and a = -22, b = -7 we get

$22 = (7)(3) + 1$

but

$-22 = (-7)(4) + 6.$

Divisibility

Suppose on the other hand that we have a = 217 and b = 7. We have 217 = (31) (7) + 0 so we conclude that b ∣ a.

$$
\begin{array}{r}
31 \\
\hline
7 \mid 217 \\
\underline{21} \\
07 \\
\underline{7} \\
0
\end{array}
$$

Divisibility Theorems.

Let $a,b,c \in \mathbb{Z}$. If $a \mid b$ and $b \mid c$ then $a \mid c$.

Proof:

Suppose $a \mid b$ then there exists an integer j such that

(1) $b = aj$

Similarly if $b \mid c$ then there exists an integer k such that

(2) $c = bk$

Replace b in equation (2) with aj to get

(3) $c = ajk$

Thus we have proved that if $a \mid b$ and $b \mid c$ then $a \mid c$. □

Divisibility Theorems.

Let a,b,c $\in \mathbb{Z}$. If a ⁞ b then a ⁞ bc.

Proof:
Since a ⁞ b there exists an integer j such that

b = aj, and bc = ajc for all (any) c $\in \mathbb{Z}$.

It should be obvious that a ⁞ ajc ($\frac{ajc}{a}$ = jc is an integer)

so a | bc . □

Divisibility Theorems.

Let a,b,c $\in \mathbb{Z}$. If a ∣ b and a ∣ c. Then a ∣ (b + c) and a ∣ (b - c).

Proof:

Since a | b there exist a j $\in \mathbb{Z}$ such that b = aj.

Since a | c there exist a k $\in \mathbb{Z}$ such that c = ak.

Therefore b + c = (aj + ak) = a(j + k).

Obviously a | a(j + k) so a ∣ (b + c).

Similarly a | a(j - k) so a ∣ (b - c). □

Notation

The *absolute value* of a denoted by

$$|a|$$

is defined as:

$$|a| = a \text{ if } a \geq 0$$

$$\text{and } |a| = -a \text{ if } a < 0.$$

Divisibility Theorems.

If $a \mid b$ then $|a| \leq |b|$.

If $a \mid b$ and $b \mid a$ then $|a| = |b|$.

If $a \mid 1$ then $|a| = 1$.

Prime Numbers

Definition: A positive integer $p > 1$ is called a *prime number* if its only divisors are 1, -1, and p, -p.

The first 10 prime numbers are:

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, ...

Definition: If an integer $c > 2$ is not prime, then it is *composite*. Every composite number c can be written as a product of two integers a,b such that $a,b \notin \{1,-1, c, -c\}$.

Determining whether a number, n, is prime or composite is difficult computationally. A simple method (which is in essence of the same computational difficulty as more sophisticated methods) checks all integers k, $2 \leq k \leq \sqrt{n}$ to determine divisibility.

Example: Let n = 143

2 does not divide 143
3 does not divide 143
4 does not divide 143
5 does not divide 143
6 does not divide 143
7 does not divide 143
8 does not divide 143
9 does not divide 143
10 does not divide 143
11divides 143, $11 \times 13 = 143$