CISC-102
Fall 2016
Week 5

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 $c = a/b$, $b \neq 0$, 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 an integer.

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

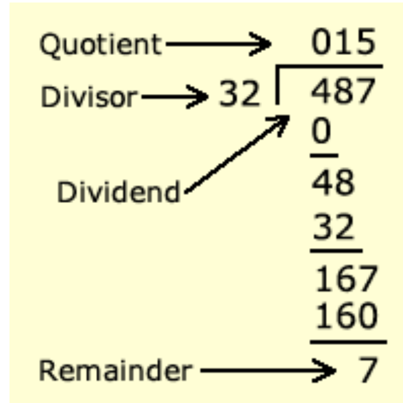
We can also say that ***for all*** integers a,b, $b \neq 0$, we have $c = a/b$ is a rational number.

Divisibility

Let a,b $\in \mathbb{Z}$, a $\neq$ 0.
If $c = \dfrac{b}{a}$ is an integer,
or alternately if c $\in \mathbb{Z}$ such that b = ca
then we say that a <u>*divides*</u> b or equivalently,
b is <u>*divisible*</u> 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 <u>*does not divide*</u> a
or equivalently a is <u>*not divisible*</u> 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 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 $\mid$ b then a $\mid$ bc.

Proof:
Since a $\mid$ 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 $\mid$ ajc ($\frac{ajc}{a}$ = jc is an integer)

so a | bc . □

Divisibility Theorems.

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

Proof:

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

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

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

Obviously $a \mid a(j + k)$ so $a \mid (b + c)$.

Similarly $a \mid a(j - k)$ so $a \mid (b - c)$. □

More Divisibility Theorems.

If $a \mid b$ and $b \neq 0$ 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, $11 \times 13 = 143$

Theorem: Every integer $n > 1$ is either prime or can be written as a product of primes.

For example:

$12 = 2 \times 2 \times 3$.

17 is prime.

$90 = 2 \times 5 \times 3 \times 3$.

$143 = 11 \times 13$.

$147 = 3 \times 7 \times 7$.

$330 = 2 \times 5 \times 3 \times 11$.

Note: If factors are repeated we can use exponents.

$48 = 2^4 \times 3$.

Theorem: Every integer $n > 1$ is either prime or can be written as a product of primes.

Proof:

(1) Suppose there is an integer $k > 1$ that is the largest integer that is the product of primes. This then implies that the integer $k+1$ is not prime or a product of primes.

(2) If $k+1$ is not prime it must be composite and:
$k+1 = ab,\ a,b \in \mathbb{Z},\ a,b \notin \{1,-1, k+1, -(k+1)\}$.

(3) Observe that $|a| < k+1$ and $|b| < k+1$, because $a \mid k+1$ and $b \mid k+1$. We assume that $k+1$ is the smallest positive integer that is not prime or the product of primes, therefore $|a|$ and $|b|$ are prime or a product of primes.

(4) Since $k+1$ is a product of a and b it follows that it too is a product of primes.

(5) Thus we have contradicted the assumption that there is a largest integer that is the product of primes, and we can therefore conclude that every integer $n > 1$ is either prime or written as a product of primes. □

Mathematical Induction (2^{nd} form)

Let P(n) be a proposition defined on a subset of the Natural numbers (b, b+1, b+2, ...) such that:

i) P(b) is true
(Base)
ii) Assume P(j) is true for all j, $b \leq j \leq k$.
(Induction Hypothesis)
iii) Use Induction Hypothesis to show that P(k+1) is true.
(Induction Step)

NOTE: Go back to all of the proofs using mathematical induction that we have seen so far and replace the assumption
(1) Assume P(k) is true for $k \geq b$. (b is the base case value) by
(2) Assume P(j) is true for all j, $b \leq j \leq k$."

and the rest of the proof can remain as is.

Assumption (2) above is stronger than assumption (1). Sometimes this form of induction is called *strong induction.*

NOTE: A stronger assumption makes it easier to prove the result.

Let P(n) be the proposition:

$$\sum_{i=1}^{n} 2^i = 2 + 2^2 + \cdots + 2^n = 2^{n+1} - 2$$

Theorem: P(n) is true for all $n \in \mathbb{N}$.

Proof:

Base: P(1) is $2 = 2^2 - 2$ which is clearly true.

Induction Hypothesis: P(j) is true for j, $1 \leq j \leq k$.

Induction Step:

$$\sum_{i=1}^{k+1} 2^i = 2^{k+1} - 2 + 2^{k+1}$$ (because P(k) is true)

$$= 2(2^{k+1}) - 2$$

$$= 2^{k+2} - 2 \quad \square$$

Theorem: Every integer $n > 1$ is either prime or can be written as a product of primes.

Proof: (Mathematical Induction of the 2nd form) Let P(n) be the proposition that all natural numbers $n \geq 2$ are either prime or the product of primes.

Base: n = 2, P(2) is true because 2 is prime.
Induction Hypothesis:
(1) Assume that P(j) is true, for all j, $2 \leq j \leq k$.
Induction Step: Consider the integer k+1.

(2) Observe that if k+1 is prime P(k+1) is true, so consider the case where k+1 is composite. That is: $k+1 = ab$, $a,b \in \mathbb{Z}$, $a,b \notin \{1,-1, k+1, -(k+1)\}$.
(3) Therefore, $|a| < k+1$ and $|b| < k+1$.
So |a| and |b| are prime or a product of primes.
(4) Since k+1 is a product of a and b it follows that it too is a product of primes.
(5) Therefore, by the 2nd form of mathematical induction we can conclude that P(n) is true for all $n \geq 2$. □

Well-Ordering Principle

In our initial proof that shows that integers greater than 2 are either prime or a product of primes we assumed that if that wasn't true for all integers greater than 2, then there was a smallest integer where the proposition is false. (we called that integer k.) This statement may appear to be obvious, but there is a mathematical property of the positive integers at play that makes this true.

Theorem: Well Ordering Principle: Let S be a non-empty subset of the positive integers. Then S contains a least element, that is, S contains an element $a \leq s$ for all $s \in S$.

- Observe that S could be an infinite set.
- Well ordering does NOT apply to subsets of $\mathbb{Z}$, $\mathbb{Q}$, or $\mathbb{R}$. It is a special property of the positive integers.

NOTE: The Well Ordering Principle can be used to prove both forms of the Principle of Mathematical Induction.

In essence the statement “use the proposition P(k) to show that P(k+1) is true” uses an underlying assumption:

“Should there be a value of *n* where the proposition is false then there must be a smallest value of *n* where the proposition is false”

In all of our induction proofs so far the value $k+1$ plays the role of that smallest value of *n* where the proposition may be false. For all other values j, $b \leq j \leq k$, we can assume that P(j) is true. In the induction step we show that P(k+1) is also true, in essence showing that there is no smallest value of n where the proposition is false. And by well ordering this implies that the result is true for all values of n.

Theorem: There exists a prime greater than n for all positive integers n. (We could also say that there are infinitely many primes.)

Proof: Consider $y = n!$ and $x = n! + 1$. Let p be a prime divisor of x, such that $p \leq n$. This implies that p is also a divisor of y, because $n!$ is the product of all natural numbers from 1 to n. So we have $p \mid x$ and $p \mid y$. According to one of the divisibility theorems we have
$p \mid x - y$. But $x - y = 1$ and the only divisor of 1 is -1, or 1, both not prime. So there are no prime divisors of x less than n. And since every integer is either prime or a product if primes, we either have $x > n$ is prime, or there exists a prime $p, p > n$ in the prime factorization of x. □

Theorem: There is no largest prime.

(Proof by contradiction.)

Suppose there is a largest prime. So we can write down all of the finitely many primes as: $\{p_1, p_2, \ldots, p_\omega\}$.

Now let n = $p_1 \times p_2 \times \cdots \times p_\omega + 1$.

Observe that n must be larger the p_ω the largest prime. Therefore n is composite and is a product of primes. Let p_k denote a prime factor of n. Thus we have

$p_k \mid n$

And since $p_k \in \{p_1, p_2, \ldots, p_\omega\}$ we also have

$p_k \mid (n\text{-}1)$

We know that $p_k \mid n$ and $p_k \mid (n\text{-}1)$ implies that $p_k \mid$ n - (n-1) or $p_k \mid 1$. But no integer divides 1 except 1, and 1 is not prime, so $p_k \mid 1$ is impossible, and raises a mathematical contradiction. This implies that our assumption that p_ω is the largest prime is false, and so we conclude that there is no largest prime. □