(Chapter 5. P 30 – 34)

Let m, n be two integer with $m \neq 0$.

<u>Definition</u>: We say that m <u>divides</u> n if we can find an integer k such that $n = mk$.

Notation: $m \mid n$ read "m divides n"

If we can not find such an integer, we write $m \nmid n$.

Example: $3 \mid 6$ since $6 = (3)(2)$

$4 \mid 12$ since $12 = (4)(3)$

$5 \nmid 13$.

<u>Definition</u>: A number that divides n is called a <u>divisor</u> of n.

Example: $3 \mid 6$ and hence 3 is a divisor of 6.

$4 \mid 12$ and hence 4 is a divisor of 12.

Example: List all the (positive) divisors for 6.

(Observation; if n is a divior of 6, then $0 < n \leq 6$)

$n=1$	$6=1\cdot 6$	1 is a divisor
$n=2$	$6=2\cdot 3$	2 is a divisor
$n=3$	$6=3\cdot 2$	3 is a divisor
$n=4$	$4\nmid 6$	4 is not a divisor
$n=5$	$5\nmid 6$	5 is not a divisor.
$n=6$.	$6=6\cdot 1$	6 is a divisor.

All the (positive) divisor of 6 are 1, 2, 3, 6.

Definition: A positive number is prime if it only has two divisors.
(In this case, the divisors can only be 1 and itself.)

Otherwise, it is called a composite number

Remark: When we define prime/composite numbers, we exclude 1 since we consider it to be neither prime nor composite.

Example:

	prime or not	divisors
2	✓	1, 2.
3	✓	1, 3
4	×	1, 2, 4
5	✓	1, 5

6	$\times$	1, 2, 3, 6.
...	...	- - -

<u>Proposition</u>: Let m, n be two integers. Let x be another integer such that $x \mid m$ and $x \mid n$ then for any integer r, s, $x \mid (rm + sn)$

Proof: $x \mid m$, there exists an integer a such that $m = ax$. This implies $rm = rax$

$x \mid n$, there exists an integer b such that $n = bx$ This implies $sn = sbx$

Then $rm + sn = rax + sbx = (ra + sb)x$

This shows: $x \mid (rm + sn)$ $\square$

Given two integers m and n.

<u>Definition</u>: A <u>common divisor</u> of m and n is a number that divides both m and n.

Example: $m = 4$, $n = 6$

We can show: $2 \mid 4$ and $2 \mid 6$

This implies: 2 is a common divisor for 4 and 6.

Example : $m=12$, $n=18$

We can show : $3 \mid 12$ and $3 \mid 18$

This implies: 3 is a common divisor for 12 and 18.

Definition: The greatest common divisor of m and n is the largest number that divides both m and n.

Notation : $\gcd(m,n)$

Example: $\gcd(4,6)=2$.

$\gcd(12,18)=6$.

In the left of the class, we introduce an effective way to calculate $\gcd(m,n)$ called Euclidean algorithm.

Before the general method, we can look at one example:

Find $\gcd(132, 36)$.

Step I: divide 132 by 36

$132 = 3 \cdot \underline{36} + \underline{24}$

Step II: divide 36 by 24

$$36 = 1 \cdot \underline{24} + \underline{12}$$

Step III: divide 24 by 12

$$24 = 2 \cdot 12 + 0$$

Step IV: when we find a "0," the previous remainder is the gcd.

In our case, this is 12

Therefore $\gcd(132, 36) = 12$.

The general method:

<u>Theorem 5.1</u> (Euclidean Alogorithm) Let a, b be two integers. We compute the successive quotients and remainders:

$$a = q_1 b + r_1$$

$$b = q_2 r_1 + r_2$$

$$r_1 = q_3 r_2 + r_3$$

$$\vdots$$

$$r_{n-2} = q_n r_{n-1} + r_n$$

$$r_{n-1} = q_{n+1} r_n + 0.$$

Then $\gcd(a,b) = r_n$.

Remark: Why this algorithm will end in finite steps?

Ans: We can show: (we can assume $a > b$)

$$a > b > r_2 > r_3 > \cdots r_n$$

After finitely many steps, we will reach 0.

This idea is called "infinite descent" and we will use this later.