Section 4 (Number Theory)

- Suppose that a and b are integers. Then **a divides b** if b = an for some integer n. a is a **factor** or **divisor** of b. b is a **multiple** of a.
- a divides b is also written as a|b
  - **Divisor is always on the left, multiple on the right**
  - Ex. 7|77 is true. 77|7 is false.
  - 7|7 is true because 7= 7(1)
    - a|a will be true because a = a(1)
  - 7|0 is true because 0 = 7(0)
    - b|0 will be true because 0 = b(0)
  - 0|7 is false
    - 0|c will always be false because no 0 times anything will always be 0 and never another value c
  - -3|12 is true because 12 = -3(4)
  - 3|-12 is true because -12 = 3 (-4)
- **An integer p is even when 2|p**
- If c divides **BOTH** a and b, then c is called a **common divisor** of a and b. The largest such is called the gcd or greatest common divisor, gcd(a,b)
- A common multiple of a and b is a number c such that a|c and b|c. The smallest such is the lcm or least common multiple, lcm(a,b)
- $lcm(a,b)=\frac{ab}{\gcd(a,b)}$
- If two integers a and b share **NO COMMON FACTORS,** gcd(a,b) =1 and these numbers are called **relatively prime**
- gcd(k,0) = gcd(0,k) = k
- gcd(0,0) is undefined
- **Division Algorithm:** For any integers a and b, where b is positive, there are unique integers q (quotient) and r (remainder) such that a = bq+r and $0 \leq r < b$
- **Corollary:** Suppose that a and b are integers and b is positive. Let r be the remainder when a is divided by b. Then gcd(a,b) = gcd(b,r)

- **Euclidean Algorithm (for computing gcd):**

```
gcd(a,b: positive integers)
   x := a
   y := b
   while (y > 0)
      begin
      r := remainder(x,y)
      x := y
      y := r
      end
   return x
```

- Two integers are "**congruent mod k**" if they differ by a multiple of k
  - **Definition:** If k is any positive integer, two integers a and b are congruent mod k (written a $\equiv$ b (mod k)) if k|a-b
    - **k|(a-b) = k|(b-a)**
    - eg. 3 $\equiv$ 38 (mod 7) since 38-3 = 35
    - 38 $\equiv$ 3 since 3-38 = -35
    - -29 $\equiv$ -13 (mod 8) since -13 – (-29) = 16
- Example proof:

Claim 24 *For any integers a, b, c, d, and k, k positive, if $a \equiv b \pmod{k}$ and $c \equiv d \pmod{k}$, then $a + c \equiv b + d \pmod{k}$.*

Proof: Let a, b, c, d, and k be integers with k positive. Suppose that $a \equiv b \pmod{k}$ and $c \equiv d \pmod{k}$.

Since $a \equiv b \pmod{k}$, $k \mid (a - b)$, by the definition of congruence mod k. Similarly, $c \equiv d \pmod{k}$, $k \mid (c - d)$.

Since $k \mid (a - b)$ and $k \mid (c - d)$, we know by a lemma about divides (above) that $k \mid (a - b) + (c - d)$. So $k \mid (a + c) - (b + d)$

But then the definition of congruence mod k tells us that $a + c \equiv b + d \pmod{k}$. □

- **Congruence class/equivalence class:** group of congruent integers, written [x]
- **The group [x] is the set of all integers congruent to x mod k, or the set of integers that have remainder x when divided by k**
- If k = 7, [3] = {3, 10, -4, 17, -11…}
    - In the mod 7 system [3] = [-4] = [10]
- **Equivalence class manipulation:**
    - [x] + [y] = [x+y]
    - [x] * [y] = [x*y]
    - eg. For k = 7,
        - [4] + [10] = [14] = [0]
        - [-4] * [10] = [-40] = [2]
- Integers mod k are written as Z_k