Math 580/780I Notes 2

Divisibility Basics:

- Definition. Let a and b be integers. Then a divides b (or a is a divisor of b or b is divisible by a) if there is an integer c such that $b = ac$.
- Notation. We write $a|b$ if a divides b, and we write $a \nmid b$ if a does not divide b.
- Definition. An integer p is prime (or is a prime) if it is > 1 and divisible by no other positive integer other than 1 and itself.
- The division algorithm.

Theorem 4. *If $a \neq 0$ and b are any integers, then there exist unique integers q (called the quotient) and r (called the remainder) with $0 \leq r < |a|$ such that $b = qa + r$.*

- **Proof.** Let r be the least non-negative integer in the double sequence

$$\ldots, b - 2a, b - a, b, b + a, b + 2a, \ldots.$$

Let q be such that $b - qa = r$. Since $(b - qa) - |a|$ is in the double sequence and $< b - qa$, we have $(b - qa) - |a| < 0$. Thus, $r < |a|$. Also, $r \geq 0$. This proves the existence of q and r as in the theorem.

For $j \in \{1, 2\}$, suppose q_j and r_j are integers such that $b = q_j a + r_j$ and $0 \leq r_j < |a|$. Then

$$(q_1 - q_2)a - (r_1 - r_2) = 0. \qquad (*)$$

This implies $a|(r_1 - r_2)$. On the other hand, $r_1 - r_2 \in (-|a|, |a|)$. Hence, $r_1 = r_2$. Now, $(*)$ implies $q_1 = q_2$, establishing the uniqueness of q and r as in the theorem. ■

- Definition and Notation. Let n and m be integers with at least one non-zero. The greatest common divisor of n and m is the greatest integer dividing both n and m. We denote it by $\gcd(n, m)$ or (n, m).
- Note that if n is a non-zero integer, then $(0, n) = |n|$.
- **Theorem 5.** *If a and b are integers with at least one non-zero, then there exist integers x_0 and y_0 such that $ax_0 + by_0 = (a, b)$. Moreover,*

$$\{ax + by : x, y \in \mathbb{Z}\} = \{k(a, b) : k \in \mathbb{Z}\}.$$

- **Proof.** Let $S = \{ax + by : x, y \in \mathbb{Z}\}$. Let d denote the smallest positive integer in S. Let x_0 and y_0 be integers for which $d = ax_0 + by_0$. Theorem 5 follows from the following claims.

Claim 1. $\{kd : k \in \mathbb{Z}\} \subseteq S$.

Reason: Clear.

Claim 2. $S \subseteq \{kd : k \in \mathbb{Z}\}$.

Reason: Let $u = ax' + by' \in S$. By Theorem 4, we have integers q and r with $u = dq + r$ and $0 \leq r < d$. On the other hand,

$$r = u - dq = (ax' + by') - (ax_0 + by_0)q = a(x' - x_0 q) + b(y' - y_0 q) \in S.$$

It follows that $r = 0$ and $u = qd$.

Claim 3. $d|a$ and $d|b$.

Reason: Use Claim 2 together with $a \in S$ and $b \in S$.

Claim 4. $d = (a, b)$.

Reason: Since $ax_0 + by_0 = d$, $(a, b)|d$ so that $(a, b) \leq d$. Since $d|a$ and $d|b$, d is a common divisor of a and b. By the definition of greatest common divisor, $d = (a, b)$.

Homework:

(1) What are the divisors of 6? What are the divisors of 12?

(2) What are the divisors of 2^{2010}? How many are there?

(3) Let a, b, c, and d denote positive integers. Explain why each of the following are true.
  (a) If $a|b$ and $b|c$, then $a|c$.
  (b) If $ac|bc$, then $a|b$.
  (c) If $a|b$ and $c|d$, then $ac|bd$.

(4) Let n be an integer. Explain why $n(n + 5)(2n + 11)$ is divisible by 3. In other words, explain why one of n, $n + 5$ and $2n + 11$ must be divisible by 3. (Hint: Use Theorem 4 with $a = 3$ and $b = n$.)

(5) Prove that the product of any 3 consecutive integers is divisible by 6.

Challenge Problem:

Let n be a positive integer. Prove that n divides $(n - 1)!$ unless n is a prime or $n \in \{1, 4\}$. Be careful when handling the case that n is a square.