HOMEWORK 9
MATH 308
DUE: 11/20/2018

Throughout, let a, b, and c be non-zero integers.

1. Consider the following statements:
   i. a is divisible by 3;
   ii. a is divisible by 9;
   iii. a is divisible by 12;
   iv. $a = 24$;
   v. a^2 is divisible by 3;
   vi. a is even and divisible by 3.

   Which conditions are necessary for a to be divisible by 6? Which are sufficient? Which are necessary and sufficient?
2. Run the Euclidean algorithm with $a = 30$, $b = 12$.
3. Recall from lecture that executing the Euclidean algorithm for $a = 100$ and $b = 36$ gives the following equations:

$$100 = 36 * 2 + 28, \tag{E1}$$
$$36 = 28 * 1 + 8, \tag{E2}$$
$$28 = 8 * 3 + 4, \tag{E3}$$
$$8 = 4 * 2 + 0. \tag{E4}$$

   (a) Follow these steps to express 4 as an *integer combination* of 100 and 36, i.e., find (possibly negative) integers x and y such that $100x + 36y = 4$:
      (i) Use equation (E3) to express 4 as an integer combination of 8 and 28 (find integers x and y such that $8x + 28y = 4$).
      (ii) Use equation (E2) to express 8 as an integer combination of 28 and 36 .
      (iii) Use equation (E1) to express 28 as an integer combination of 36 and 100.
      (iv) Plug your equation from part (ii) into your equation in part (i), expanding and simplifying, to express 4 as an integer combination of 28 and 36.
      (v) Plug your equation from part (iii) into your equation in part (iv), expanding and simplifying, to express 4 as an integer combination of 36 and 100.

   (b) Make an argument (write an informal proof) justifying the following claim:
   For any positive integers a and b, there exist integers x and y satisfying $\gcd(a, b) = ax + by$.
4. Consider Euclid's Lemma and its proof from Chapter 28 of "How to think…":

   Euclid's Lemma. Suppose that n, a, and b are natural numbers. If $n|ab$ and $\gcd(n, a) = 1$, then $n|b$.

   Proof. Since $\gcd(n, a) = 1$, there exist integers k and ℓ such that $kn + \ell a = 1$. Thus $knb + \ell ab = b$. We obviously have $n|knb$. We also have $n|ab$, so $n|lab$. Thus $n|knb + lab$, i.e. $n|b$. □

   (a) Analyze the theorem statement: give examples, non-examples, assumptions and conclusions, compare to other results, etc. Compare to the statement given in class.

   (b) Identify in the proof (here) where the hypotheses were used.
   (c) What theorems/lemmas/etc. were used in the proof?
   (d) Compare/contrast this proof to the proof from class.
   (e) Analyze what happens when we drop the hypothesis that $\gcd(n, a) = 1$.
5. Prove the following.
   (a) We have $a|b$ if and only if $-a|b$.
   (b) If δ is a common divisor of a and b, then $\delta|\gcd(a, b)$.
   (c) If $a \geq 4$ is not prime, then $a|(a-1)!$.
6. Use strong induction to prove the division algorithm:

   For any $a, b \in \mathbb{Z}$ with $b \neq 0$, there are unique integers q and r satisfying
   $$a = bq + r \qquad \text{and} \qquad 0 \leq r < |b|.$$
   [Recall: We sketched a proof in class. You'll need to do two cases.]
7. An integer ℓ is called a *common multiple* of non-zero integers a and b if $a|\ell$ and $b|\ell$. The smallest positive such ℓ is called the *least common multiple* of a and b, denoted $\operatorname{lcm}(a, b)$. For example, $\operatorname{lcm}(3, 7) = 21$ and $\operatorname{lcm}(12, 66) = 132$.
   (a) Compute $\operatorname{lcm}(12, 8)$, $\operatorname{lcm}(30, 20)$, $\operatorname{lcm}(-10, 22)$, and $\operatorname{lcm}(9, 10)$.
   (b) Prove that if $a|m$ and $b|m$, then $\operatorname{lcm}(a, b)|m$.
   (c) Prove that for any $r\mathbb{Z}$, we have $\operatorname{lcm}(ra, rb) = r \operatorname{lcm}(a, b)$.
   (d) Show that $ab = \gcd(a, b)\operatorname{lcm}(a, b)$.