Spring 2019, Math 320: Problem Set 1
Due: Tuesday, February 5th, 2019
The Division Algorithm and Greatest Common Divisors

Discussion problems. The problems below should be worked on in class.

(D1) *Greatest Common Divisors.* The goal of this problem is to build familiarity and intuition for gcd. Some of the questions are open-ended; you may find it helpful to compute several small(ish) examples to aide in formulating conjectures.

(a) Compare your answers to Preliminary Problem (P1). Agree on a correct definition, and write it at the top of the board for reference.
(b) Find $d = (5, 7)$, and find x and y so that $5x + 7y = d$.
(c) Find $d = (35, 21)$, and find x and y so that $35x + 21y = d$.
(d) For $a, b \in \mathbb{Z}$ positive, how are (a, b), $(-a, b)$ and $(-a, -b)$ related?
(e) If $(a, 0) = 1$, what can a possibly be?
(f) If $a \in \mathbb{Z}$, what are the possible values of $(a, a + 2)$? What about $(a, a + 6)$?
(g) Find a formula for $(a, a + 24)$ in terms of a. Hint: this can be done in significantly fewer than 12 cases!
(h) Prove or disprove: if $a \mid b$ and $b \mid c$, then $a \mid c$.
(i) Prove or disprove: if $(a, b) = 1$ and $(a, c) = 1$, then $(a, b + c) = 1$.
(j) Write proofs (as a group!) of your conjectures above, starting with part (d).

(D2) *The Division Algorithm.* The goal of this problem is to prove the following theorem.

Theorem. *For any $a, b \in \mathbb{Z}$ with $b > 0$, there exist unique integers $q, r \in \mathbb{Z}$ with $0 \le r < b$ so that $a = qb + r$.*

(a) First, we will prove that if $a \ge 0$, then $a = qb + r$ for some $q, r \in \mathbb{Z}$ with $0 \le r < b$. The following proof uses induction on a, but contains some errors. Locate and correct the errors, and write (as a group!) a full, correct proof on the board.

Proof. Denote by $P(a)$ the statement "$a = qb + r$ for some $q, r \in \mathbb{Z}$ with $0 \le r < b$".
Base case: suppose $a < b$. Choosing $q = 0$ and $r = a$, we see $qb + r = a$.
Inductive step: suppose $a \ge b$ and that $P(a - b)$ holds (the *inductive hypothesis*). The inductive hypothesis implies $a - b = q'b + r$ for some $q', r \in \mathbb{Z}$ with $0 \le r < b$. Rearranging yields $a = (q' + 1)b + r$, and choosing $q = q' + 1$ and $r = r' + 1$ completes the proof. □

(b) Next, we will prove that if $a < 0$, then $a = qb + r$ for some $q, r \in \mathbb{Z}$ with $0 \le r < b$. As a group, turn the following "proof sketch" into a formal proof.

Proof. The integer $a + db$ is positive if d is large enough. We can then apply part (a) to write $a + db = q'b + r'$, and rearrange accordingly to find q and r. □

(c) It remains to prove the "uniqueness" part. Fill in the end of the following proof.

Proof. Suppose $q_1, r_1 \in \mathbb{Z}$ with $0 \le r_1 < b$ satisfy $a = q_1b + r_1$, and that $q_2, r_2 \in \mathbb{Z}$ with $0 \le r_2 < b$ satisfy $a = q_2b + r_2$. By way of contradiction, assume $r_1 \ne r_2$. Without loss of generality, we can assume $r_1 < r_2$. Rearranging the equation $a = q_1b + r_1 = q_2b + r_2$, we obtain... □

(d) Try to prove part (c) directly, i.e. *without* proof by contradiction. Start by assuming that $a = q_1b + r_1 = q_2b + r_2$ as before, but *without* assuming $r_1 \ne r_2$, and prove $r_1 = r_2$.

Homework problems. You must submit *all* homework problems in order to receive full credit.

For this assigment only, do *not* use prime factorization in any of your arguments.

(H1) Find $d = (75, 65)$, and find x and y so that $75x + 65y = d$.

(H2) Use the division algorithm to prove that the square of any integer a is either of the form $5k$, $5k + 1$, or $5k + 4$ for some integer k.

(H3) Prove that $(a, b) = 1$ and $(a, c) = 1$ implies $(a, bc) = 1$.

(H4) Let $d = (a, b)$. Prove that if $a \mid c$ and $b \mid c$, then $ab \mid cd$.

(H5) Determine whether each of the following statements is true or false. Prove each true statement, and give a counterexample for each false statement.

(a) If $a \mid c$ and $(a, b) \mid c$, then $b \mid c$.
(b) If $(a, b) > 1$ and $(a, c) > 1$, then $(b, c) > 1$.
(c) If $(a, b) = 1$ and $(a, c) = 1$, then $(a, b - c) = 1$.

Challenge problems. Challenge problems are not required for submission, but bonus points will be awarded for submitting a partial attempt or a complete solution.

(C1) Prove that $((a, b), c) = (a, (b, c))$ for all $a, b, c \in \mathbb{Z}$.