Fall 2023, Math 320: Week 1 Problem Set
Due: Thursday, September 7th, 2023
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's. Some of the questions are open-ended; you may find it helpful to do several small(ish) examples to aide in formulating conjectures.

(a) Compare your answers to Preliminary Problem (P1). Agree on a correct definition.

(b) Find $d = \gcd(35, 21)$, and find x and y so that $35x + 21y = d$.

(c) For $a, b \in \mathbb{Z}$ positive, how are $\gcd(a, b)$, $\gcd(-a, b)$ and $\gcd(-a, -b)$ related?

(d) Fill in the blanks in the following proof that $\gcd(ca, cb) = c\gcd(a, b)$ for all $a, b, c \in \mathbb{Z}$ with $c > 0$ and a and b not both 0.

Proof. Let $d = \gcd(a, b)$. Then $kd = a$ and $\ell d = b$ for some $k, \ell \in$ ____, and by Bézout's identity, $d = ax + by$ for some $x, y \in$ ____. Multiplying yields the equalities

$$ca = (\_\_)cd, \qquad cb = (\_\_)cd, \qquad \text{and} \qquad cd = (\_\_)ca + (\_\_)cb,$$

meaning $\gcd(ca, cb) =$ ____ by Bézout's identity. □

(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 $a = 7q + r$ for some $q, r \in \mathbb{Z}$ with $0 \le r < 7$ (that is, we are assuming $b = 7$ and $a \ge 0$, and proving only the existence of q and r). The proof below uses induction on a, but contains an error. Locate/correct the error.

Proof. Denote by $P(a)$ the statement "$a = 7q + r$ for some $q, r \in \mathbb{Z}$ with $0 \le r < 7$". Base cases: suppose $a = 0, 1, \ldots, 6$. Choosing $q = 0$ and $r = a$, we see $7q + r = a$. Inductive step: suppose $a \ge 7$ and that $P(a - 7)$ holds (the *inductive hypothesis*). The inductive hypothesis implies

$$a - 7 = 7q' + r'$$

for some $q', r' \in \mathbb{Z}$ with $0 \le r' < 7$. Rearranging yields

$$a = 7(q' + 1) + r',$$

and choosing $q = q' + 1$ and $r = r' + 1$ completes the proof. □

(b) Modify the proof in the previous part (using a different color!) to prove that for any $b > 0$ and $a \ge 0$, there exist $q, r \in \mathbb{Z}$ with $0 \le r < b$ so that $a = qb + r$.

(c) 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, written out fully.

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

(d) 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 $a = q_1 b + r_1$, and that $q_2, r_2 \in \mathbb{Z}$ with $0 \le r_2 < b$ satisfy $a = q_2 b + r_2$. By way of contradiction, assume $r_1 \ne r_2$. Without loss of generality, assume $r_1 < r_2$. Rearranging $a = q_1 b + r_1 = q_2 b + r_2$, we obtain… □

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

Unless otherwise stated, $a, b, c, d, n \in \mathbb{Z}$ are arbitrary.

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

(H1) Find $d = \gcd(75, 65)$, and find $x, y \in \mathbb{Z}$ 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) Let $d = \gcd(a, b)$. Prove that if $a \mid c$ and $b \mid c$, then $ab \mid cd$.

(H4) Prove that if $\gcd(a, b) = 1$, then $\gcd(a, b^n) = 1$ for all $a, b, n \in \mathbb{Z}$ with $n \geq 1$.

Hint: use induction on n.

(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 $\gcd(a, b) = 1$ and $\gcd(a, c) = 1$, then $\gcd(a, b + c) = 1$.

(b) If $\gcd(a, b) = 1$ and $\gcd(a, c) = 1$, then $\gcd(a, bc) = 1$.