# Homework 2: Due Friday, September 13

**Preamble:** We saw how fast the Euclidean Algorithm ran in class. However, it is not obvious why the algorithm terminates so quickly. In the next problem, we work to understand the theory behind the speed. Let $a, b \in \mathbb{N}$ with $b \neq 0$. Write $a = qb + r$ where $q, r \in \mathbb{N}$ and $0 \leq r < b$. Notice that after one step of the algorithm, the new second argument $r$ may not be much smaller than the original second argument $b$. For example, if $a = 77$ and $b = 26$, then we have $q = 2$ and $r = 25$. However, it turns out that after *two* steps of the Euclidean Algorithm, the new second argument will be at most half the size of the original second argument. This is what we will prove in the next problem. From this fact, it follows that on input $(a, b) \in \mathbb{N}^2$, the algorithm terminates in at most $2 \log_2 b$ many steps.

**Problem 1:** Let $a, b \in \mathbb{N}$ with $b \neq 0$. In the first step of the algorithm, we write $a = qb + r$ where $q, r \in \mathbb{N}$ and $0 < r < b$ (we can assume that $r \neq 0$ because otherwise the algorithm stops at the next step). In the next step of the algorithm, we write $b = pr + s$ where $p, s \in \mathbb{N}$ and $0 \leq s < r$. Show that $s < \frac{b}{2}$.
*Hint:* You may find it useful to break the problem into cases based on how large $r$ is.

**Problem 2:** Let $a, b, c \in \mathbb{Z}$. Using only the material through Section 2.4 (so without using the Fundamental Theorem of Arithmetic), show that the following are equivalent, i.e. prove that (1) implies (2) and also that (2) implies (1):

1. $\gcd(ab, c) = 1$.
2. $\gcd(a, c) = 1$ and $\gcd(b, c) = 1$.

**Problem 3:** Let $p \in \mathbb{N}^+$ be prime. Define a function $ord_p \colon \mathbb{Z}\backslash\{0\} \to \mathbb{N}$ as follows. Given $a \in \mathbb{Z}\backslash\{0\}$, let $ord_p(a)$ be the largest $k \in \mathbb{N}$ such that $p^k \mid a$. For example, we have $ord_3(45) = 2$ and $ord_3(10) = 0$. Without using the Fundamental Theorem of Arithmetic, prove that for all $p, a, b \in \mathbb{Z}\backslash\{0\}$ with $p$ prime, we have $ord_p(ab) = ord_p(a) + ord_p(b)$.

**Problem 4:** Let $S = \{2n : n \in \mathbb{Z}\}$ be the set of even integers. Notice that the sum and product of two elements of $S$ is still an element of $S$. Call an element $a \in S$ *irreducible* if $a > 0$ and there is no way to write $a = bc$ with $b, c \in S$. Notice that 6 is irreducible in $S$ (because there is no way to write 6 as a product of two even numbers) even though it is not prime in $\mathbb{Z}$.
a. Give a characterization of the irreducible elements of $S$.
b. Show that the analogue of Fundamental Theorem of Arithmetic fails in $S$ by finding a positive element of $S$ which does *not* factor uniquely (up to order) into irreducibles.

**Problem 5:** Let $A = \mathbb{N}$ and define $a \sim b$ to mean that there exists $n \in \mathbb{Z}$ with $a = 2^n b$.
a. Show that $\sim$ is an equivalence relation on $A$.
b. Characterize which elements of $\mathbb{N}$ are the smallest elements of their equivalence class. In other words, find a simple characterization of the set $\{a \in \mathbb{N} : a \leq b \text{ for all } b \in \mathbb{N} \text{ with } a \sim b\}$.

**Problem 6:** Let $A, B, C$ be sets and let $f \colon A \to B$ and $g \colon B \to C$ be functions.
a. Show that if $g \circ f$ is injective, then $f$ is injective.
b. Show that if $g \circ f$ is surjective and $g$ is injective, then $f$ is surjective.

**Problem 7:** Let $Q$ and $P$ be defined as in Section 3.5 of the notes. Thus, $Q$ is the set of equivalence classes of the set $\mathbb{Z} \times (\mathbb{Z}\backslash\{0\})$ under the equivalence relation $(a, b) \sim (c, d)$ if $ad = bc$, and $P$ is the set of equivalence classes of the set $\mathbb{R}^2\backslash\{(0, 0)\}$ under the equivalence relation $(x_1, y_1) \sim (x_2, y_2)$ if there exists a real number

$\lambda \neq 0$ with $(x_1, y_1) = (\lambda x_2, \lambda y_2)$. Determine which of the following functions on equivalence classes are well-defined. In each case, either give a proof or a specific counterexample.
a. $f\colon Q \to \mathbb{Z}$ defined by $f(\overline{(a,b)}) = a - b$.
b. $f\colon Q \to Q$ defined by $f(\overline{(a,b)}) = \overline{(a^2 + 3ab + b^2, 5b^2)}$.
c. $f\colon P \to \mathbb{R}$ defined by

$$f(\overline{(x,y)}) = \frac{2xy^3 + 5xy}{x^4 + y^4}$$

d. $f\colon P \to P$ defined by $f(\overline{(x,y)}) = \overline{(x^3 + 5xy^2, y^3)}$.