Exercises on GCD

These exercises deal with the GCD of several non-zero integers.

1. First we recast the Euclidean algorithm for the gcd of two integers in matrix form.

(a) With the notation from the discussion of the gcd in text, show that for each i, there is an invertible 2-by-2 matrix Q_i with integer entries, such that Q_i^{-1} also has integer entries, and $(n_{i-2}, n_{i-1})Q_i = (n_{i-1}, n_i)$.

(b) Suppose $n_r \neq 0$ but $n_{r+1} = 0$. Conclude that there is an invertible 2-by-2 matrix Q with integer entries, such that Q_i^{-1} also has integer entries, and $(n_r, 0) = (m, n)Q$.

(c) Conclude from this that n_r is an integer linear combination of m and n, and that n_r divides both m, and n. It follows that n_r is the gcd of m and n.

Definition: The greatest common divisor of a collection $\{a_1, \ldots, a_n\}$ of non-zero integers is a natural number β such that β divides each of the a_i and whenever α is a natural number that divides each of the a_i, then α divides β. The gcd of $\{a_1, \ldots, a_n\}$ is unique if it exists.

2. Using Exercise 1, show that given $(a_1, a_2, \ldots, a_n)$, there exists an n-by-n invertible matrix P with integer entries, such that P^{-1} also has integer entries, and there exists a natural number d such that $(d, 0, \ldots, 0) = (a_1, a_2, \ldots, a_n)P$.

3. Using Exercise 2, show that d is an integer linear combination of $a_1, a_2, \ldots, a_n$, and that d divides each of $a_1, a_2, \ldots, a_n$. Conclude that d is the gcd of $\{a_1, \ldots, a_n\}$.

4. Show that d is the smallest natural number in

$$I(a_1, a_2, \ldots, a_n) = \{s_1 a_1 + s_2 a_2, + \cdots + s_n a_n : s_1, s_2, \ldots, s_n \in \mathbb{Z}\}.$$