115 Homework 3 Solutions

Due Friday October 22

Question 1 Show that a matrix with integer entries can have determinant 1 only if the greatest common divisor of every row and column is also 1.

Proof:

Suppose we have an $n \times n$ matrix $\mathbf{A} = [a_{ij}]$ where at least one of the rows or columns has greatest common divisor different than 1.

case i) suppose row i is such that $(a_{i1}, a_{i2}, \ldots, a_{in}) = k \neq 1$ Then we can write $\det \mathbf{A} =$

$$\det \begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ \vdots & \vdots & \ldots & \vdots \\ a_{i1} & a_{i2} & \ldots & a_{in} \\ \vdots & \vdots & \vdots & \ddots \end{pmatrix} = \det \begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ \vdots & \vdots & \ldots & \vdots \\ k(a_{i1}/k) & k(a_{i2}/k) & \ldots & k(a_{in}/k) \\ \vdots & \vdots & \vdots & \ddots \end{pmatrix} =$$

$$\det \left(k \begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ \vdots & \vdots & \ldots & \vdots \\ (a_{i1}/k) & (a_{i2}/k) & \ldots & (a_{in}/k) \\ \vdots & \vdots & \vdots & \ddots \end{pmatrix} \right) = k \det \begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ \vdots & \vdots & \ldots & \vdots \\ (a_{i1}/k) & (a_{i2}/k) & \ldots & (a_{in}/k) \\ \vdots & \vdots & \vdots & \ddots \end{pmatrix}$$

This product is clearly not equal to 1 since k is an integer not equal to 1 and clearly all the entries of the matrix

$$\begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ \vdots & \vdots & \ldots & \vdots \\ (a_{i1}/k) & (a_{i2}/k) & \ldots & (a_{in}/k) \\ \vdots & \vdots & \vdots & \ddots \end{pmatrix}$$

are integers, which ensures its determinant is an integer and thus its determinant multiplied by k is not equal to 1.

case ii) suppose column j is such that $(a_{1j}, a_{2j}, \ldots, a_{nj}) = k \neq 1$ Then we know from linear algebra that $\det \mathbf{A} = \det \mathbf{A}^t$ and we can apply the same argument as in case i). Thus we see by contraposition that a matrix having determinant one implies that the matrix must have rows and columns with greatest common divisor 1.

Question 2 (Rosen 3.2.20) Show that $(a_1, \dots, a_n)$ is the least positive integer linear combination $m_1a_1 + \cdots m_na_n$.

Proof:

We will induct on n. The base case, that (a_1, a_2), is the least positive integer linear combination of a_1 and a_2, is theorem 3.8 (pg.81) in the text. For the inductive step, we use lemma 3.2 (pg.83) in the text. Thus

$$(a_1, \dots, a_n) = (a_1, \dots, (a_{n-1}, a_n)) = m_1a_1 + \cdots m_{n-1}(a_{n-1}, a_n),$$

by the inductive hypothesis. Now

$$m_1a_1 + \cdots m_{n-1}(a_{n-1}, a_n) = m_1a_1 + \cdots m_{n-1}(m'_{n-1}a_{n-1} + m'_na_n) =$$

$$m_1a_1 + \cdots m_{n-1}m'_{n-1}a_{n-1} + m_{n-1}m'_na_n.$$

Thus we see that $(a_1, \dots a_n)$ is the least positive integer linear combination of $a_1, \dots, a_n$.

Question 3 (Rosen 3.3.4a,c) Use the (extended) Euclidean algorithm to compute $(51, 87)$ and $(981, 1234)$ and express your answers as linear combinations.

a.) From exercise 2 we have $(51, 87) = 3$

$$3 = 15 - 2 \cdot 6 = (51 - 36) - 2(36 - 2 \cdot 15) = 51 - 3(87 - 51) + 4(51 - 36) =$$

$$8(51) - 3(87) - 4(87 - 51) = 12(51) - 7(87).$$

b.) From exercise 2 we have $(981, 1234) = 1$

$$1 = 31 - 6 \cdot 5 = (253 - 222) - 6(222 - 7 \cdot 31) = (1234 - 981) - 7(981 - 3 \cdot 253) + 42(253 - 222) =$$

$$1234 - 8(981) + 63(1234 - 981) - 42(981 - 3 \cdot 235) = 64(1234) - 113(981) + 126(1234 - 981) =$$

$$-239(981) + 190(1234).$$

Question 4* (Rosen 3.3.21,22) *The Game of Euclid*
Two players start with a pair of positive integers $\{x, y\}$, $(x \geq y)$. They take turns replacing $\{x, y\} \mapsto \{\max(x - ty, y), \min(x - ty, y)\}$ where $x - ty \geq 0$. The game is won by moving to a pair with one vanishing element. Show:

(i) The game always ends and at $\{(x, y), 0\}$ to boot!

(ii) The player starting can always win if $x = y$ or $x > y(1 + \sqrt{5}/2)$, otherwise the second player can always win.

Proof:

i)Note that $(x, y) = (x - ty, y)$, as any divisor of x and y is also a divisor of $x - ty$. So, every move in the game of Euclid preserves the greatest common divisor of the two numbers. Since $(a, 0) = a$, if the game beginning terminates, then it must do so at $\{(a, b), 0\}$. Since the sum of the two numbers is always decreasing and positive, the game must terminate.

ii) We will first show that if $y < x \leq y(1 + \sqrt{5})/2$, then there is a unique move from $\{x, y\}$ that goes to a pair $\{y, z\}$ with $y > z(1 + sqrt5)/2$. For convenience, let $\phi = (1 + sqrt5)/2$. If $y < x \leq y\phi$, then the move $\{x, y\}$ to $\{y, x - y\}$ is a legal move. But $x - 2y < x - y\phi \leq 0$, so there is only one legal move. In this case, since $\phi^2 = \phi + 1$, we have that $x \leq y\phi \to x\phi \leq y(\phi + 1)$ and hence $(x - y)\phi \leq y$, as desired. Now if $x = y$ the first player wins immediately. Suppose $x > y\phi$. Then let k be defined by $ky < x < (k + 1)y$. If $x - ky < y \leq (x - ky)\phi$, then the first player makes the move $\{y, x - ky\}$ which leaves the second player in the exact situation above: $x - ky < y \leq (x - ky)\phi$. Therefore, the second player has only one move, which puts the player back into the situation with $x > y\phi$ again. If, on the other hand, $(x - ky)\phi < y$, then the first player makes the move $\{y, x - (k - 1)y\}$, in which case, we have $y\phi > (x - ky)\phi^2 = (x - ky)(\phi + 1) = (x - ky)\phi + (x - ky) > y + (x - ky) = x - (k - 1)y$. Therefore, the second player is again put into the same situation above. Hence a player in the position $x > y\phi$ can always force the other player to be in the first situation which is a losing situation.

Question 5 (Rosen 3.4.8) Show that every positive integer is the product of possibly a square and a "square-free" integer (no factor other than 1 appears more than once).

Proof:

Suppose that the primes in the factorization of n that occur to an even power are $p_1, \ldots, p_k$ and let the power of p_i in the factorization be $2b_i$ and suppose that the primes that occur to an odd power are $q_1, \ldots, q_l$ and let the power of q_j in the factorization be $2c_j + 1$. Then

$$n = (p_1^{b_1} p_2^{b_2} \cdots p_k^{b_k} q_1^{c_1} q_2^{c_2} \cdots q_l^{c_l})^2 (q_1 q_2 \cdots q_l).$$

This is the factorization of n into a perfect square and a square-free integer.

Question 6 Develop and prove an algorithm for writing $(a, b) = ma + nb$. Feel free to use Rosen Theorem 3.13.

Proof:

From Rosen Theorem 3.13 we have that $(a, b) = s_n a + t_n b$ where s_n and t_n are the nth terms of the sequences defined recursively by

$$s_0 = 1, t_0 = 0, s_1 = 0, t_1 = 1$$

and

$$s_j = s_{j-2} - q_{j-1} s_{j-1}, t_j = t_{j-2} - q_{j-1} t_{j-1}$$

for $j = 2, 3, ..., n$ where $q_j = [r_{j+1}/r_j]$ from the division algorithm. The proof of this algorithm is the proof of Theorem 3.13.