1  Homework 7

**Exercise 16.4:** Let \( c \in D(b, r) \). By definition, this means that \( c|b \) and \( c|r \). But then \( c|bq + r = a \) and therefore \( c \in D(a, b) \).

**Exercise 17.1:** \( 7684 = 4148 + 3536, 4148 = 3536 + 612, 3536 = 5 \cdot 612 + 476, 612 = 476 + 136, 476 = 3 \cdot 136 + 68 \). Now we go back. \( 68 = 476 - 3 \cdot 136 = 476 - 3 \cdot (612 - 476) = 4 \cdot 476 - 3 \cdot 612 = 4 \cdot (3536 - 5 \cdot 612) - 3 \cdot 612 = 4 \cdot 3536 - 23 \cdot 612 = 4 \cdot 3536 - 23 \cdot (4148 - 3536) = 27 \cdot 3536 - 23 \cdot 4148 = 27 \cdot (7684 - 4148) - 23 \cdot 4148 = 27 \cdot 7584 - 50 \cdot 4148 \). So pick \( m = 27 \) and \( n = -50 \).

**Exercise 17.2** By 17.1 above, pick \( m = 27, n = 50 \).

**Exercise 17.6** Since \( \gcd(a_1, b_1) = 1 \), there exist integers \( m, n \) such that \( ma_1 + nb_1 = 1 \). Since \( a_1b_2 = a_2b_1 \) then also \( ma_1b_2 = ma_2b_1 \). But \( ma_1 = 1 - nb_1 \) and therefore, after substituting, we get \( (1 - nb_1)b_2 = ma_2b_1 \) and \( b_2 - nb_1b_2 = ma_2b_1 \). But then \( b_1|b_2 \). By symmetry \( b_2|b_1 \) and therefore \( b_1 = b_2 \) and also \( a_1 = a_2 \) as desired.

**Problem IV.4:** Since \( 98 = 2 \cdot 7^2 \), then 98 is a square of a rational number if and only if 2 is. But we have seen that there is rational number whose square is 2.

**Problem IV.11:** Given a pair of integers \((a, b)\), remember that the sequence \( a_i \) is defined by \( a_0 = a, a_1 = b \) and \( a_{k-1} = q_k a_k + a_{k+1} \), where each step is an Euclidean division. By working our way backwards as in Exercise 17.1, we have unique integers \( m_k \) and \( n_k \) such that \( a_k = am_k + bn_k \). Let’s prove that \( m_k/n_k - m_{k-1}/n_{k-1} = (-1)^k \) by induction on the length \( N \) of the sequence \( a_i \).

The base case is \( N = 1 \). By our definitions, \( a_0 = 1 \cdot a + 0 \cdot b \) and \( m_0 = 1, n_0 = 0 \). Similarly, \( a_1 = b = 0 \cdot a + 1 \cdot b \) and therefore \( m_1 = 0, n_1 = 1 \). By plugging these values, one establishes the base case. Now the inductive step; suppose that there is a sequence of length \( N + 1 \). Let \( a_0 = q_1 a_1 + a_2 \). Call \( a_k', m_k' \) and \( n_k' \) the values that we get by applying the algorithm to the pair \((a_1, a_2)\), which has length \( N \). Let’s determine the relations these have with the \( a_k, m_k \) and \( n_k \). Clearly \( a_k' = a_{k+1} \). Now, by definition of \( m_k \) and \( n_k \) we have that \( a_{k+1} = am_{k+1} + bn_{k+1} \). By definition of \( m_k' \) and \( n_k' \) we have instead that \( a_{k+1} = a_k' = a_1 m_k' + a_2 n_k' = a_1 m_k' + (a_0 - q_1 a_1) \cdot n_k' = a_0 n_k' + (m_k' - q_1 n_k') a_1 \).

By construction, we must have \( m_{k+1} = n_k' \) and \( n_{k+1} = m_k' - q_1 n_k' \) for all \( 0 < k \leq N \). Now, \( m_{k+1}n_k - m_k n_{k+1} = n_k' (m_k' - q_1 n_k') - n_k' (m_k' - q_1 n_k') = n_k' m_{k+1} - n_k' m_k' = -(n_k' m_{k+1} - n_k' m_k') = -(n_k' m_{k+1} - n_k' m_{k+1}) = (-1)^k = (-1)^{k+1} \) for \( 0 < k < N \). The last check we need is \( m_1 n_0 - m_0 n_1 = -1 \), but this is the same reasoning as in the base case.