Math 418/818

Assignment 1 - Solutions

1. We apply the table method algorithm from class to \( n = 213 \):

\[
\begin{array}{c|cccccccc}
 i & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\
 q_i & 213 & 106 & 53 & 26 & 13 & 6 & 3 & 1 & 0 \\
r_i & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 \\
\end{array}
\]

Thus, \( 213 = (r_8, \ldots, r_1)_2 = (1, 1, 0, 1, 0, 1, 0, 1)_2 \) or 11010101.

2. (a) Since \( m \) has \( k \) bits and \( n \) has \( \ell \) bits, we have

\[
2^{k-1} \leq m < 2^k \quad \text{and} \quad 2^{\ell-1} \leq n < 2^\ell.
\]

Multiplying these inequalities yields \( 2^{k+\ell-2} \leq mn < 2^{k+\ell} \). Thus, if \( mn < 2^{k+\ell-1} \), then \( mn \) has \( k + \ell - 1 \) bits because \( 2^{k+\ell-2} \leq mn < 2^{k+\ell-1} \), whereas otherwise \( mn \) has \( k + \ell \) bits because \( 2^{k+\ell-1} \leq mn < 2^{k+\ell} \).

2* (b) From (1) we see that \( 2^{-\ell} \leq n^{-1} < 2^{1-\ell} \), so \( 2^{k-\ell} < \frac{m}{n} < 2^{k-\ell+1} \), and hence

\[
2^{k-\ell-1} \leq \frac{mn}{k} < 2^{k-\ell+1}.
\]

This means that \( \lfloor \frac{m}{n} \rfloor \) has either \( k - \ell \) bits (if \( \lfloor \frac{m}{n} \rfloor < 2^{k-\ell} \)) or \( k - \ell + 1 \) bits (if \( \lfloor \frac{m}{n} \rfloor \geq 2^{k-\ell} \)), as claimed.

3. (a) The Euclidean algorithm yields

\[
\begin{align*}
952 &= 2 \cdot 343 + 266 \\
343 &= 1 \cdot 266 + 77 \\
266 &= 3 \cdot 77 + 35 \\
77 &= 2 \cdot 35 + 7 \\
35 &= 5 \cdot 7 + 0
\end{align*}
\]

Thus, \( \gcd(952, 343) = 7 \). By back-substitution we obtain

\[
\begin{align*}
7 &= 1 \cdot 77 - 2 \cdot 35 \\
&= 1 \cdot 77 - 2(266 - 3 \cdot 77) \\
&= 7(343 - 266) - 2 \cdot 266 \\
&= 7 \cdot 343 - 9(266 - 2 \cdot 343) \\
&= 7 \cdot 343 - 9(952 - 2 \cdot 343)
\end{align*}
\]

and so \( x = -9 \) and \( y = 25 \) satisfy the equation \( 952x + 343y = 7 \). The matrix method yields

\[
\begin{pmatrix}
1 & 0 & 952 \\
0 & 1 & 343
\end{pmatrix}
\stackrel{2}{\rightarrow}
\begin{pmatrix}
0 & 1 & 343 \\
1 & -2 & 266
\end{pmatrix}
\stackrel{1}{\rightarrow}
\begin{pmatrix}
1 & -2 & 266 \\
-1 & 3 & 77
\end{pmatrix}
\stackrel{3}{\rightarrow}
\begin{pmatrix}
-1 & 3 & 77 \\
4 & -11 & 35
\end{pmatrix}
\stackrel{5}{\rightarrow}
\begin{pmatrix}
-9 & 25 & 7 \\
49 & -136 & 0
\end{pmatrix},
\]

where the number above each arrow denotes the quotient of the last column of the previous matrix. From the first row of the last matrix we see again that \( x = -9 \) and \( y = 25 \) satisfy the equation \( 852x + 343y = 7 \).

3* (b) By part (a) we know that \( \gcd(952, 343) = 7 \) and that \( x_0 = -9 \) and \( y_0 = 25 \) solves \( 952x_0 + 343y_0 = 7 \). Since \( 7 \mid 70 \), the given Diophantine equation has a solution. By the formula of Theorem 4(b) from class, the general solution is given by:

\[
\begin{align*}
x &= \frac{\frac{70}{7}(-9) + \frac{343}{7}t}{9} = -90 + 49t \\
y &= \frac{\frac{70}{7}(25) - \frac{952}{7}t}{9} = 250 - 136t
\end{align*}
\]

where \( t \in \mathbb{Z} \).

4. (See the MAPLE solution on the course web-site.)

Comment: Please read the instructions to each question carefully.

In Q2, you were asked to use inequalities in your proof.
In Q3, you were supposed to present two ways of computing the extended Euclidean algorithm.
In Q4(a) you were asked to compare and to interpret the two answers.
In Q4(b) you were supposed to calculate (not to display) a list (not a sequence).