Workshop 5

3CC: Codes and Ciphers (530.334)

6th October, 2005

1. In case you’ve forgotten (or never learned it), the Euclidean Algorithm is an algorithm for finding the greatest common divisor of two integers \( m \) and \( n \). It also gives a way of finding integers \( c \) and \( d \) such that \( \gcd(m, n) = mc + nd \). To find \( \gcd(m, n) \) (supposing \( m > n \)):

   - Divide \( n \) into \( m \) giving quotient \( q_1 \) and remainder \( r_1 < n \);
   - divide \( r_1 \) into \( n \) giving quotient \( q_2 \) and remainder \( r_2 < r_1 \);
   - divide \( r_2 \) into \( r_1 \) giving quotient \( q_3 \) remainder \( r_3 < r_2 \);
   - divide \( r_3 \) into \( r_2 \) giving quotient \( q_4 \) remainder \( r_4 < r_3 \);
   - and so on...
   - until the remainder is 0.

Then \( \gcd(m, n) \) is the last non-zero remainder and \( c, d \) are found by back-substitution. The question below gives an example.

(a) The following application of the Euclidean Algorithm to the integers \( m = 81 \) and \( n = 74 \) shows that \( \gcd(81, 74) = 1 \) (since the last non-zero remainder \( r_4 \) is 1).

\[
\begin{align*}
81 & = 74 \cdot 1 + 7 \\
74 & = 4 \cdot 10 + 4 \\
7 & = 4 \cdot 1 + 3 \\
4 & = 3 \cdot 1 + 1 \\
3 & = 1 \cdot 3 + 0 \\
\end{align*}
\]

\[
\begin{align*}
m & = n \cdot q_1 + r_1 \\
n & = r_1 \cdot q_2 + r_2 \\
r_1 & = r_2 \cdot q_3 + r_3 \\
r_2 & = r_3 \cdot q_4 + r_4 \\
r_3 & = r_4 \cdot q_5 + r_5 \\
\end{align*}
\]

Use back-substitution to find integers \( c, d \) such that \( \gcd(m, n) = 1 = 81c + 74d \). Show that the integer \( d \) satisfies \( 74d \equiv 1 \pmod{81} \) (this will be important for the RSA cryptosystem).

(b) Use the Euclidean Algorithm to show that \( \gcd(98, 25) = 1 \), and hence find an integer \( d \) such that \( 25d \equiv 1 \pmod{98} \).

2. Try to think of a mathematical function which might be a ‘one-way function’ (not necessarily using the above questions).
3. Let $C$ be a linear $(n, k)$ $q$-ary code with alphabet $A$ and standard array $M$. Show that

(a) Every word in $A^n$ appears exactly once in $M$.
(b) The number of rows in $M$ is $q^{n-k}$.
(c) Two words $x$ and $y$ in $A^n$ lie in the same coset (row) of $M$ if and only if their difference $x - y$ is a codeword (i.e., is in $C$).

4. Let $C$ be the binary linear code with parity check matrix $H = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \end{pmatrix}$.

(a) Construct a standard array for $C$.
(b) Give a table of coset leaders and their syndromes for $C$.
(c) Use syndrome decoding to decode
   
   i. 11111
   ii. 00000
   iii. 01000