COL 202

TUTORIAL SHEET 7

1. Show with the help of Fermat's little theorem that if n is a positive integer, then 42 divides $n^7 - n$.

2. Show that the system of congruences $x \equiv a_1 (\texttt{mod}\ m_1)$ and $x = a_2 (\texttt{mod}\ m_2)$ where a_1, a_2, m_1 and m_2 are integers with $m_1, m_2 > 0$ has a solution if and only if $a_1 - a_2$ divides $\texttt{gcd}(m_1, m_2)$.

3. Use the Chinese remainder theorem to show that an integer a, with $0 \leq a < m = m_1 m_2 \ldots m_n$, where the positive integers $m_1, \ldots, m_n$ are pair-wise relatively prime, can be represented uniquely by the n-tuple $(a \texttt{ mod } m_1, a \texttt{ mod } m_2, \ldots, a \texttt{ mod } m_n)$.

4. Show that if $ac \equiv bd (\texttt{mod}\ m)$ then $a \equiv b (\texttt{mod}\ (m/d))$, where $d = \texttt{gcd}(a, b)$.

5. Show that if a and b are positive irrational numbers such that $1/a + 1/b = 1$, then every positive integer can be uniquely expressed as either $\lfloor ka \rfloor$ or $\lfloor kb \rfloor$ for some positive integer k.

6. Show that every integer greater than 11 can be written as sum of two composite integers. Recall that a composite integer is a positive integer which is not prime and is larger than 1.

7. Prove that if $f(x)$ is a nonconstant polynomial with integer coefficients, then there is an integer y such that $f(y)$ is composite.

8. A routing transit number (RTN) is a bank code used in the United States which appears on the bottom of checks. The most common form of an RTN has nine digits, where the last digit is a check digit. If $d_1 d_2 ... d_9$ is a valid RTN, then it must be the case that

$$3(d_1 + d_4 + d_7) + 7(d_2 + d_5 + d_8) + (d_3 + d_6 + d_9) = 0 (\texttt{mod}\ 10).$$

   - Show that if $d_1 d_2 ... d_9$ is a valid RTN, then $d_9 = 7(d_1 + d_4 + d_7) + 3(d_2 + d_5 + d_8) + 9(d_3 + d_6) \texttt{mod}\ 10$.
   - Show that the check digit of an RTN can detect all single errors, and determine which transposition errors an RTN check digit can detect and which ones it cannot detect.