MATH 55 - Worksheet 2 (Friday)

1 Use the construction in the proof of the Chinese remainder theorem to find all solutions to the system of congruences $x \equiv 2 \bmod 3$, $x \equiv 1 \bmod 4$ and $x \equiv 3 \bmod 5$.

2 Use Fermat's little theorem to compute

a $3^{302} \bmod 5$

b $3^{302} \bmod 7$

c $3^{302} \bmod 11$

d Use your results from the previous parts and the Chinese remainder theorem to find $3^{302} \bmod 385$.

3 Using Fermat's little theorem show that if n is a positive integer, then 42 divides $n^7 - n$.

4 **[Wilson's Theorem]** For any prime p, $(p-1)! \equiv -1 \bmod p$

We will prove Wilson's theorem in the following steps:

a Show that the positive integers less than 11, except 1 and 10, can be split into pairs of integers such that each pair consists of integers that are inverses of each other modulo 11.

b Use part **a** to show that $10! \equiv -1 \bmod 11$

c Show that if p is prime, the only solutions of $x^2 \equiv 1 \mod p$ are integers x such that $x \equiv 1 \mod p$ or $x \equiv -1 \bmod p$.

d Using **c**, generalize **a** to a general prime p; that is, show that if p is a prime, the positive integers less than p, except 1 and $p-1$, can be split into $(p-3)/2$ pairs of integers such that each pair consists of integers that are inverse of each other.

e Now prove Wilson's Theorem

f Is it true that $(n-1)! \equiv -1 \bmod n$ for all positive integers n?