NUMBER THEORY: CLASS 10

1. Exercise

1) Show that congruences mod m satisfy *an equivalent relation* :

i) **Reflexive property:** if a is an integer, $a \equiv a \bmod m$.

ii) **Symmetric property:** if a and b are integers such that $a \equiv b \bmod m$ then $b \equiv a \bmod m$.

iii) **Transitive property:** if a, b and c are integers such that $a \equiv b \bmod m$ and $b \equiv c \bmod m$ then $a \equiv c \bmod m$.

2) Find the least positive residue of each of the following

a) $3^{10} \bmod 11$.

b) $2^{12} \bmod 13$.

3) Show that the least positive residue of $b^N \bmod m$ where $b < m$ can be computed in $O((log(m))^2 log(N))$.

4) Find the final digit of $(...((7^7)^7)^{\cdots 7})$

(where the 7th power is taken 1000 times).

5) Solving the quadratic congruence turns out to be much harder than the linear congruence.

Find the solution of

$x^2 \equiv -1 \bmod p$.

for $p = 3, 5, 7, 11, 13, 17, 19$. Can you characterize the prime p of which the above equation has a solution?

Date: Friday, September 26, 2008.