

MATH 567 FALL 2008, NUMBER THEORY I, PROBLEMS 4

To be submitted by Tuesday, September 23rd

Easier problems

1. Show that if $f(x)$ is a polynomial with integer coefficients and if $f(a) \equiv k \pmod{m}$, then $f(a + tm) \equiv k \pmod{m}$ for every integer t .
2. Prove that any fourth power must have one of 0, 1, 5, 6 for its unit digit.
3. Show that $61! + 1 \equiv 63! + 1 \equiv 0 \pmod{71}$.
4. Prove that for any integer n
 - (i) $n^7 - n$ is divisible by 42.
 - (ii) $n^{13} - n$ is divisible by 2730.

Harder problems

5. Prove that if $a^p \equiv b^p \pmod{p}$, then $a^p \equiv b^p \pmod{p^2}$.
6. Prove that if m is an odd positive integer, then the sum of any complete set of residues modulo m is $0 \pmod{m}$. If m is any integer with $m > 2$, then prove the analogous result for any reduced system of residues modulo m .
7. The numbers $F_n = 2^{2^n} + 1$ are called Fermat numbers. F_0 through F_4 are prime. Fermat had conjectured that F_n is always prime. Show that $641|F_5$. We now know that F_5, \dots, F_{19} are composite and it is now conjectured that there are no further Fermat primes!
Suppose that p is a prime with $p|F_n$. Let e denote the smallest positive integer such that $2^e \equiv 1 \pmod{p}$.
 - (i) Show that e exists and $e|2^{n+1}$.
 - (ii) Show that $e \nmid 2^n$.
 - (iii) Show that $p \equiv 1 \pmod{2^{n+1}}$.