Mathematics 437/537 – Homework #2

due Monday, October 2, 2006 at the beginning of class

1. Which integers satisfy all of the congruences $x \equiv 3 \pmod{14}$, $x \equiv 5 \pmod{15}$ and $x \equiv 7 \pmod{17}$ simultaneously?

2. Find the smallest positive integer n such that $2n \equiv 3 \pmod 5$, $3n \equiv 4 \pmod 7$, and $5n \equiv 6 \pmod{11}$. (Hint: there is a painless way.)

3. (based on NZM 1.3 – 42 & 44) Let a and k be integers greater than 1.
   (a) Suppose that $a^k - 1$ is prime. Prove that $a = 2$ and that k is prime (these are the *Mersenne* primes).
   (b) Suppose that $a^k + 1$ is prime. Prove that a is even and that k is a power of 2 (these are the *Fermat* primes).

4. (NZM 2.5 – 4 & 5)
   (a) Suppose that m is square-free and that d,e are positive integers with $de \equiv 1 \pmod{\phi(m)}$. Show that $a^{de} \equiv a \pmod m$ for all integers a.
   (b) Suppose that m is not square-free. Show that there are integers a_1 and a_2 with $a_1 \not\equiv a_2 \pmod m$ but $a_1^e \equiv a_2^e \pmod m$ for all integers $e > 1$.

5. (NZM 2.6 – 9) Suppose that $f(a) \equiv 0 \pmod{p^j}$ and that $f'(a) \not\equiv 0 \pmod p$. Let $\overline{f'(a)}$ be an integer chosen so that $f'(a)\overline{f'(a)} \equiv 1 \pmod{p^j}$ and put $b = a - f(a)\overline{f'(a)}$. Show that $f(b) \equiv 0 \pmod{p^{2j}}$.

6. How many solutions are there to the congruence
$$x^4 - x^3 + x^2 - x + 1 \equiv 0 \pmod{2269355}?$$

7. (NZM 2.7 – 10). Let $p \geq 5$ be a prime. Write $1/1 + 1/2 + \ldots + 1/(p-1) = a/b$ with $(a, b) = 1$. Show that $p^2|a$.

8. Let a, b and m be integers with $m \neq 0$ and $(a, m) = (b, m) = 1$. Let h, k, ℓ denote the orders modulo m of a, b, ab, respectively. Prove that
$$\frac{hk}{(h,k)^2} \mid \ell \quad \text{and} \quad \ell \mid \frac{hk}{(h,k)}.$$

9. (NZM 2.8 – *24) Let a and $n > 1$ be any integers such that $a^{n-1} \equiv 1 \pmod n$ but $a^d \not\equiv 1 \pmod n$ for every proper divisor d of $n - 1$. Prove that n is a prime.

10. (NZM 2.8 – *31) Show that the decimal expansion of $1/p$ has period $p - 1$ if and only if 10 is a primitive root of p.