Mathematics 437/537 – Homework #3

due Monday, October 16, 2006 at the beginning of class

1. (NZM 2.8 – *26) The positive integer m is called a *Carmichael number* if $a^{m-1} \equiv 1 \pmod{m}$ for all a with $(a, m) = 1$. Show that m is a Carmichael number if and only if m is square-freee and $(p-1)|(m-1)$ for all primes $p|m$.
2. Find all Carmichael numbers of the form $3pq$ where p and q are prime.
3. (NZM 2.8 – *29) Show that the sequence $1^1, 2^2, 3^3, \ldots$ considered $(\mathrm{mod}\ p)$ is periodic with least period $p(p-1)$. (As usual p is a prime.)
4. Consider the sequnce $2, 2^2, 2^{2^2}, 2^{2^{2^2}}, \ldots$ defined recursively by $x_1 = 1$ and $x_{k+1} = 2^{x_k}$ for $k \geq 1$. Prove that for any positive integer m, this sequence is eventually constant modulo m.
5. (NZM 2.8 – *37 (H)) Show that if $n > 1$ then $n \nmid 2^n - 1$.
6. Find all non-negative integers m and n for which $2^m = 3^n \pm 1$. (Hint: This question does belong here).
7. Let p be an odd prime, and write $p - 1 = 2^k q$ with q odd and $k \geq 1$. Let a be an integer such that $\left(\frac{a}{p}\right) = -1$. Set $b = a^q$. Prove that b has order exactly 2^k modulo p. Determine the order of $b^{2^j} \pmod{p}$ for every $0 \leq j \leq k$.
8. (NZM 3.1 – *20 (H)) Let p be an odd prime. Prove that if there is an integer x such that
$$p|(x^2+1) \text{ then } p \equiv 1 \pmod{4};$$
$$p|(x^2-2) \text{ then } p \equiv 1 \text{ or } 7 \pmod{8};$$
$$p|(x^2+2) \text{ then } p \equiv 1 \text{ or } 3 \pmod{8};$$
$$p|(x^4+1) \text{ then } p \equiv 1 \pmod{8}.$$
Show that there are infinitely many primes of each of the forms $8n+1, 8n+3, 8n+5, 8n+7$.
9. (NZM 3.2 – 14) Let p and q be *twin primes*, i.e. $q = p + 2$. Prove that there is an integer a such that $p|(a^2 - q)$ if and only if there is an integer b such that $q|(b^2 - p)$.
10. (NZM 3.2 – *16) Show that if $p = 2^{2^n} + 1$ is prime then 3 is a primitive root $(\mathrm{mod}\ p)$ and that 5 and 7 are primitive roots $(\mathrm{mod}\ p)$ provided that $n > 1$.