**MAS3008 NUMBER THEORY EXERCISE SHEET 2**

**The following questions, or parts of questions, count for assessment: 1(i)(iii)(iv), 2(ii)(iv), 3, 5, 7, 9, 10(i)(iv)(v), 11(ii)(iii). These are marked *. Please hand in your solutions, via the Coursework Box on Level 8 of the Laver Building, by Friday 15th November.**

1. Solve the following congruences (giving the most general solution), or show that no solution exists:
(i)* $3x \equiv 10 \pmod{13}$;
(ii) $12x \equiv 20 \pmod{38}$;
(iii)* $15x \equiv 43 \pmod{99}$;
(iv)* $66x \equiv 102 \pmod{168}$;
(v) $553x \equiv 490 \pmod{1001}$. [**10**]

2. Find all integer solutions (if any exist) to each of the following equations:
(i) $7x - 11y = 4$;
(ii)* $13x + 31y = 2$;
(iii) $15x - 27y = 5$;
(iv)* $12x + 28y = 16$. [**10**]

3*. (i) Show that any natural number $n$ with $n \equiv 3 \pmod 4$ must have at least one prime factor $q \equiv 3 \pmod 4$. [**3**]
(ii) Deduce that there are infinitely many primes $q \equiv 3 \pmod 4$.
[**Hint**: If $p_1, p_2, \ldots, p_r$ is any finite list of primes, what can you say about the prime factors of $N = 4p_1p_2\ldots p_r - 1$?] [**7**]
(iii) Adapt parts (i) and (ii) to show that there are infinitely many primes $q \equiv 5 \pmod 6$. [**5**]
**Total for question: [15]**

4. Show that the property

$$ab = 0 \Rightarrow a = 0 \text{ or } b = 0$$

holds in $\mathbb{Z}_n$ if and only if $n$ is a prime number.

5*. (i) Let $n$ and $k$ be integers $\geq 2$. Show that $(n-1) \mid (n^k - 1)$. [**3**]
(ii) Deduce that if $n^k - 1$ is prime then $n = 2$ and $k$ is prime.
[**Hint**: If $k = ab$ you can apply (i) with $n = 2^a$.] [**7**]
(iii) Which of the numbers $M_p = 2^p - 1$, for $p = 2, 3, 5, 7, 11$, are prime? [**5**]
(iv)Primes of this form are called Mersenne primes. The largest known prime (discovered November 2001) is the Mersenne prime $M_p$ for $p = 13466917$. How many decimal digits does this have? [**5**]
**Total for question: [20]**

6. Show that if $k > 1$ is odd then $(n+1) \mid (n^k+1)$ for every natural number $n$. Show that if $2^k+1$ is prime then $k = 2^m$ for some $m \geq 0$. Verify that the numbers $F_k = 2^{2^k}+1$ are prime for $k = 0, 1, 2, 3, 4$ but that $F_5$ is divisible by 641. (Primes of this form are called Fermat primes.)

7*. (i) Use Fermat's Little Theorem to evaluate
(a) $2^{302} \bmod 7$; (b) $5^{123} \bmod 61$. **[4]**
(ii) Let $a$ be an integer with $\gcd(a, 561) = 1$. Show that $a^{560} \equiv 1 \pmod{p}$ for each of the primes $p = 3,\ 11,\ 17$, and hence that $a^{560} \equiv 1 \pmod{561}$. **[6]**
**Total for question: [10]**

8. Recall that the order of $a$ mod $p$ is the smallest positive integer $k$ with $a^k \equiv 1 \pmod{p}$. Make a table of the orders of all integers $1 \leq a \leq 12$ mod 13. Also, find the inverse in $\mathbb{Z}_{13}$ of each $a$, and compare the order of $a$ mod 13 with the order of its inverse. What do you notice? Can you prove that this holds in general (i.e for any prime $p$ in place of 13)?

9*. Let $p$ be prime, let $a \in \mathbb{Z}$, and let $l$ be any prime which divides $a^{p-1} + a^{p-2} + \ldots + a + 1$. Show that the order of $a$ modulo $l$ is either 1 or $p$. Deduce that either $l = p$ or $l \equiv 1 \pmod{p}$. Hence show that there are infinitely many primes $l$ with $l \equiv 1 \pmod{p}$. **[15]**

10. Solve each of the following systems of simultaneous congruences:
(i)* $x \equiv 6 \pmod{17}$, $x \equiv 5 \pmod{11}$;
(ii) $x \equiv 3 \pmod{9}$, $3x \equiv 10 \pmod{17}$;
(iii) $2x \equiv 1 \pmod{9}$, $3x \equiv 5 \pmod{17}$;
(iv)* $x \equiv 4 \pmod{12}$, $x \equiv 7 \pmod{15}$;
(v)* $x \equiv 1 \pmod{5}$, $x \equiv 3 \pmod{7}$, $x \equiv 2 \pmod{9}$. **[10]**

11. Use the Chinese Remainder Theorem to find all solutions of the following congruences:
(i) $x^2 \equiv 1 \pmod{77}$;
(ii)* $x^2 \equiv -1 \pmod{65}$;
(iii)* $x^2 \equiv 1 \pmod{165}$. **[10]**

Nigel Byott, October 2002