Mich. 2007 **NUMBERS AND SETS — EXAMPLES 2** PTJ

Important Note These questions are (deliberately) not all equally difficult or equally long. In general, the first ten questions on each sheet are intended to be ones which can be tackled (perhaps with a hint or two from a supervisor) by anyone who has understood the relevant material in the lectures; questions from 11 onwards may be more challenging, and are intended for those who find the standard material easy.

1. Find the highest common factor of 12345 and 54321.

2. Find integers x and y with $76x + 45y = 1$. Do there exist integers x and y with $3528x + 966y = 12$?

3. Let a, b, c be three positive integers. Are the following true or false? Give proofs or counterexamples as appropriate.
(*a*) $(a, b)(a, c) = (a^2, bc)$.
(*b*) If $(a, b) = (a, c) = 1$, then $(a, bc) = 1$.
(*c*) $\{a, (b, c)\} = (\{a, b\}, \{a, c\})$, where $\{p, q\}$ denotes the least common multiple of p and q.

4. Show that a positive integer is a multiple of 9 if and only if the sum of its (decimal) digits is a multiple of 9. Find a similar test for divisibility by 11.

5. The *Fibonacci numbers* $F_1, F_2, F_3, \ldots$ are defined by $F_1 = F_2 = 1$ and $F_n = F_{n-1} + F_{n-2}$ for all $n > 2$ (so that $F_3 = 2, F_4 = 3, F_5 = 5, \ldots$). Is F_{2007} even or odd? Is it a multiple of 3?

6. Solve (i.e., find all solutions of) the following congruences:
(*a*) $7x \equiv 77 \pmod{40}$.
(*b*) $12y \equiv 30 \pmod{54}$.
(*c*) $3z \equiv 2 \pmod{17}$ and $4z \equiv 3 \pmod{19}$.

7. Explain (without using a calculator) why 23 does not divide $10^{881} - 1$.

8. An RSA encryption scheme (n, e) has modulus $n = 187$ and coding exponent $e = 7$. Find $\phi(n)$, and hence find a suitable decoding exponent d. Check your answer with a caculator by first encoding the number 35 and then decoding the result.

9. Let p be a prime of the form $3k + 2$. Show that the only solution of $x^3 \equiv 1 \pmod{p}$ is $x \equiv 1 \pmod{p}$. Deduce, or prove directly, that every element of $\mathbf{Z}_p$ has a cube root.

10. Let p be a prime.
(*a*) Show that if $0 < k < p$ then $\binom{p}{k}$ is a multiple of p.
(*b*) By considering Pascal's triangle (mod p), show that $\binom{n}{k}$ is a multiple of p whenever p divides n but not k, and that $\binom{np}{kp} \equiv \binom{n}{k} \pmod{p}$ for all n and k.

11. (*a*) Let F be a field. Show that a nonzero polynomial of degree d with coefficients in F has at most d roots in F.
(*b*) Now let $F = \mathbf{Z}_p$ be the field of integers mod p, for some prime p, and suppose d divides $p - 1$. Show that the polynomial $x^d - 1$ divides $x^{p-1} - 1$, and deduce that it has exactly d roots in $\mathbf{Z}_p$.
(*c*) Deduce that, for every d dividing $p - 1$, the multiplicative group $\mathbf{Z}_p^*$ contains $\phi(d)$ elements of order exactly d. Conclude in particular that there exists a number g, prime to p, for which the converse of Fermat's little theorem is true — that is, p divides $g^n - 1$ only if $p - 1$ divides n. Find such a g when $p = 13$.

12. An integer $n > 1$ is called a *Carmichael number* if it is not prime, but every integer a satisfies $a^n \equiv a \pmod{n}$. Prove the following facts about a Carmichael number n:
(a) n is odd.
(b) n is not divisible by the square of any prime.
(c) If p is a prime factor of n, then $p-1$ divides $\frac{n}{p} - 1$. [Use the result of the previous question.]
(d) n has at least three prime factors.
Conversely, if n is a product of at least three distinct odd primes such that $p-1$ divides $\frac{n}{p} - 1$ for each prime factor p of n, prove that n is a Carmichael number. Find the prime factors of 1729, and show that it is a Carmichael number.

13. Recall the Fibonacci numbers F_n from question 5.
(a) Prove that $(F_n, F_{n+1}) = 1$ for all n.
(b) Let $m \geq 3$. By considering the Fibonacci sequence mod F_m, prove that F_m divides F_n if and only if m divides n.
(c) Prove that $(F_m, F_n) = F_{(m,n)}$ for all m and n.

14. Let p be a prime other than 7. Show that every integer is a sum of two (not necessarily distinct) cubes mod p. [Method: first note that, by the result of question 9, we need only consider primes of the form $3k+1$. The nonzero cubes mod p then form a subgroup C of index 3 in $\mathbf{Z}_p^*$, by the results of question 11; first show that it is sufficient to find a sum of two cubes in each coset of C. Now, using the fact that $p > 7$, choose $a \in \mathbf{Z}_p$ which is not a root of the polynomial $x(x^3-1)(x^3+1)$, and consider the cosets to which a^3+1 and a^3-1 belong. (The hard case is when one of them belongs to C itself.)]