Math 437/537 Problem set 2 (due 30/9/09)

Primes

1. Let $a, b \in \mathbb{Z}$ be relatively prime. Show that ab is a perfect kth power iff both a and b are.

2. (Sum of divisors) For a positive integer n write $\sigma(n) = \sum_{d|n} d$ for the sum of its positive divisors (for example, $\sigma(6) = 1+2+3+6 = 12$).
   (a) Let p be prime. Show that $\sigma(p^r) = \frac{p^{r+1}-1}{p-1}$.
   (b) Let a, b be relatively prime. Show that $\sigma(ab) = \sigma(a)\sigma(b)$.

3. (Mersenne and Fermat primes)
   (a) Let $2^a - 1$ be prime. Show that a is prime.
   (b) Let $2^b + 1$ be prime. Show that b is a power of 2.

4. A positive integer n is called *deficient, perfect, or abundant* if $\sigma(n) < 2n$, $\sigma(n) = 2n$, or $\sigma(n) > 2n$ (for example, $6 = 3+2+1$ is perfect).
   (a) Show that 2^a is deficient for all $a \geq 1$.
   (b) Let m be odd, $a \geq 1$, and let $n = 2^a m$ be an even perfect number. Show that $2^{a+1} - 1 | m$. *Hint*: Use 2(b).
   (c) Writing $r = \frac{m}{2^{a+1}-1}$ show that $\left(2^{a+1} - 1\right)(m+r) = 2n$. Conclude that the only positive divisors of m are r, m.
   (d) Show that every even perfect number is of the form $2^{p-1}(2^p - 1)$ where p is a prime such that $2^p - 1$ is also a prime.

5. For a prime p and integer n fine the exponent e so that $p^e \| n!$ (read: p^e divides $n!$ *exactly*; that is such that $p^e | n!$ but $p^{e+1} \nmid n!$).

The Chinese Remainder Theorem

6. Call an integer n *squarefree* if it is not divisible by the square of a non-unit, that is if $d^2 | n$ implies $d | 1$.
   (a) Show that n is squarefree iff it is not divisible by the square of any prime.
   (b) Given $r \geq 1$ find $n \geq 1$ so that $\{n + j\}_{j=1}^{r}$ are all not squarefree. Conclude that there are arbitrarily large gaps between square-free numbers.

7. Find the smallest positive integer x such that $x \equiv 5\,(12)$, $x \equiv 2\,(5)$ and $x \equiv 4\,(7)$ all hold simultaneously.

8. Which integers x satisfy $2x \equiv 1\,(3)$, $3x \equiv 2\,(5)$, $4x \equiv 3\,(7)$, $7x \equiv 6\,(13)$ simultaneously? *Hint*: There is a simple solution!

9. For a non-zero integer n set $\phi(n) = |\{1 \leq d \leq |n| \mid (d, n) = 1\}|$ for the number of residue classes $\bmod n$ which are relatively prime to n. Let a, b be relatively prime. Show that $\phi(ab) = \phi(a)\phi(b)$.

Congruences

10. Let $(n,7) = 1$. Show that $7|n^{12} - 1$ directly (without using induction).

11. Let a,b be (separately) relatively prime to 91. Show that $a^{12} \equiv b^{12}\,(91)$.

12. (Divisibility tests I) For an integer n define $S_{k;10}(n)$ by the following procedure:
    - Write n in base 10
    - Divide the sequence of digits into blocks of length k, starting with the least significant digit (the last block may be shorter).
    - $S_{k;10}(n)$ is the sum of the numbers whose decimal representations are the blocks.

    (a) Show $S_{1;10}(n) \equiv n\,(9)$, and explain how to use this to test whether an integer n is divisible by 3.
    (b) Show $S_{6;10}(n) \equiv n\,(7)$, and explain how to use this to test whether an integer n is divisible by 7.

13. (General divisibility test) Given a base $b \geq 2$ and a number d relatively prime to b find k so that $S_{k;b}(n) \equiv n\,(d)$. Obtain a method to test whether numbers written in base b are divisible by d.