CSL105: Discrete Mathematical Structures
I semester 2008-09
Last updated: November 3, 2008

Tutorial sheet: **Elementary Number Theory**

---

1. Prove that
   (a) the square of any integer is of the form $3k$ or $3k + 1$,
   (b) the cube of an integer has one of the forms $9k$, $9k + 1$ or $9k + 8$,
   (c) the fourth power of any integer is of the form $5k$ or $5k + 1$, and
   (d) for any integer a, $3a^2 - 1$ is never a perfect square.

2. Prove that gcd is also a multiplicative function in a certain sense viz., If $gcd(b, c) = 1$ then
$$gcd(a, bc) = gcd(a, b)gcd(a, c)$$

3. Prove that
   (a) If p and q are odd primes and $q|a^p - 1$, then either $q|a - 1$ or $q = 2kp + 1$ for some integer k
   (b) Fromt he above show that the prime divisors of $2^p - 1$, where p is any odd prime are of the form $2kp + 1$.

4. If p is an odd prime, then prove that there are infinite primes of the form $2kp + 1$. (*Hint:* If b is prime, then $x^a =_b 1$).

5. Prove that, for any number m, there must be a Fibonacci number F_k such that $F_k \equiv_m 0$, and further that, $k \leq m^2$

6. Show that, every possible divisor of the number $2^{2^n} + 1$, $n \geq 5$, has the form
$$d = h.2^{n+2} + 1$$
for some integer h.

7. Define $S(m) = \{a|\phi(a) = m, a > 0\}$. Prove that
   (a) $S(m)$ is finite.
   (b) $S(m) = \emptyset$ whenever $m > 1$ is an odd integer.

8. Assume that p and q are distinct odd primes such that $p - 1|q - 1$. If $gcd(a, pq) = 1$, show that $a^{q-1} =_{pq} 1$

9. Show the more general result of the mulitplicativity of Euler's function, i.e, Show that
$$\phi(ab) = \frac{d\phi(a)\phi(b)}{\phi(d)} \tag{1}$$
where $d = gcd(a, b)$.

10. Prove that, $x^2 \equiv_n x$ has exactly 2^k different solutions, where k is the number of distinct prime divisors of n.

11. Consider numbers written in base 10.
    (a) Prove that $n - n^R$ is divisible by 9 where n^R denotes the number obtained by *reversing* the digits of n.
    (b) n is a *palindrome* if $n = n^R$. Prove that any palindrome with an even number of digits is divisible by 11.