MATH 371 – Homework assignment 2 – September 6, 2013

1. Suppose $a, b \in \mathbb{N}$ such that $a + b = p$ is a prime number. Prove that $\gcd(a, b) = 1$.

2. It seems that $\varphi(n)$ is even for $n > 2$. Prove this, or find a counterexample.

3. You know that $\varphi(5) = 4$, $\varphi(8) = 4$ and $\varphi(10) = 4$. So $(\mathbb{Z}/5)^*$, $(\mathbb{Z}/8)^*$ and $(\mathbb{Z}/10)^*$ are all (abelian) groups of order 4. There are two abelian groups of order 4 (actually, there are only two groups of order 4, and both are abelian), the cyclic group and the Klein 4-group. To which of these are $(\mathbb{Z}/5)^*$, $(\mathbb{Z}/8)^*$ and $(\mathbb{Z}/10)^*$ isomorphic?

4. (a) Prove that if $2^n + 1$ is a prime number, then n must be a power of 2. (*Hint*: First show that if $n = ab$ where b is odd, then $2^a + 1$ is a factor of $2^n + 1$.) The nth *Fermat number* F_n is defined to be $F_n = 2^{2^n} + 1$.

(b) Show that F_0, F_1, F_2, F_3 and F_4 are prime.

(c) Show that $\prod_{i=0}^{n-1} F_i = F_n - 2$.

(d) Use (c) to show that $\gcd(F_m, F_n) = 1$ if $m \neq n$.

(e) Use (d) to give another proof that there are infinitely many prime numbers.

(f) Show that F_5 is composite. In fact, it is not known whether any of the F_n for $n > 4$ is prime.

5. Let $n \in \mathbb{N}$. Recall that we are writing $\text{div}(n)$ for the set of (positive) divisors of n. Let $d(n)$ be the number of elements in this set, so $d(n)$ is the number of divisors of n.

(a) Show that $d(n)$ is a multiplicative function (i.e., if $\gcd(m, n) = 1$ then $d(mn) = d(m)d(n)$.
(b) Find a formula for $d(n)$ in terms of the prime factorization of n as $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$.

Next, let $\sigma(n)$ be the sum of the (positive) divisors of n.

(c) Show that $\sigma(n)$ is also a multiplicative function.
(d) Find a formula for $\sigma(n)$ in terms of the prime factorization of n.

6. Suppose that $N = pq$ is the product of two diferent (big) prime numbers p and q. Show that p and q are solutions of the quadratic equation

$$x^2 + (\varphi(N) - N - 1)x + N = 0.$$

This shows that finding $\varphi(N)$ is just as hard as factoring N into primes.

7. (a) Using only Fermat's little theorem, show that 899 is composite.
(b) Show that 15 is not a strong pseudoprime relative to 11.
(c) Show that 25 is a strong pseudoprime relative to 7.

8. Show that $x^4 + y^4 = z^4$ has no nontrivial integer solutions (i.e., solutions where neither x nor y is zero).