Collected Homework Week 9

MATH 278: Number Theory — Name (Print): _____
Due: March 23, 2015 at 4:00pm — Extension: March 25, 2015 at 10:00am

Note you may use the following Theorems where helpful. Feel free to go ahead and prove them! (No need to turn them in for this homework though!)

Modulo 3 Theorem 0: If r_1, r_2,..., r_m are natural numbers and each one is congruent to 0 modulo 3, then the product $r_1 r_2 \cdots r_m$ is also congruent to 0 modulo 3.

Modulo 3 Theorem 1: If r_1, r_2,..., r_m are natural numbers and each one is congruent to 1 modulo 3, then the product $r_1 r_2 \cdots r_m$ is also congruent to 1 modulo 3.

Modulo 6 Theorem 1: If r_1, r_2,..., r_m are natural numbers and each one is congruent to 1 modulo 6, then the product $r_1 r_2 \cdots r_m$ is also congruent to 1 modulo 6.

1. Prove the following statements:

   (a) Any prime of the form $3n + 1$ is also of the form $6m + 1$ where m, $n \in \mathbb{Z}$.

   (b) Each integer of the form $3n + 2$ has a prime factor of this form.

   (c) The only prime of the form $n^3 - 1$ is 7. (Hint: Think about factoring.)

   (d) The only prime p for which $3p + 1$ is a perfect square is 5.

2. Our proof of Theorem 3.28, the fact that there are infinitely many primes congruent to 3 modulo 4, gave us an idea of how to construct such a list, building from other primes congruent to 3 modulo 4. The first two primes congruent to 3 modulo 4 are 3 and 7. So let $p_1 = 7$ and construct a list of 6 primes (the two already given plus four more) using the technique from the proof. Be careful! You don't always have one of these primes immediately. Be sure to show and briefly explain your work.

3. Finish the exercises we were working on in class. We showed that if $d|n$, then $2^d - 1|2^n - 1$. Now do the following, explaining your work for each.

   (a) Use the result to find a complete prime factorization of $2^{20} - 1$. (Hint: Use as many different values for d as you can!)

   (b) One of the prime factors of $2^{35} - 1$ is 122921. Find a complete prime factorization of $2^{35} - 1$.

4. If we have found a prime, how far do we have to go before we find another prime? Bertrand proved that for any natural number n, there is at least one prime lying between n and $2n$. Thus we don't have to go any further than we have already come. However, this is very difficult to prove. We can prove a much larger bound with much less difficulty. Prove the following: Let p_n represent the nth prime. Then $p_{n+1} \leq 2^{2^n}$. (Hint: You may have proved before that $\sum_{i=0}^{n-1} 2^i = 2^n - 1$. If you haven't, try doing so, but no need to turn it in for this homework.)

Notebook Problems Week 9

(1) Prove that there are infinitely many primes congruent to 5 modulo 6.

(2) Try to use the same idea we used to prove that there are infinitely many primes congruent to 3 modulo 4 to show that there are infinitely many primes congruent to 4 modulo 5. What goes wrong? In particular, what happens if you start with $p_1 = 19$ and try to make a longer list?