MTH 505: Number Theory — Spring 2017
Homework 3 — Drew Armstrong

3.1. (Infinitely Many Primes). Prove that there are infinitely many positive prime integers. That is, prove that the sequence

$$p_1 = 2, p_2 = 3, p_3 = 5, p_4 = 7, p_5 = 11, p_6 = 13, \ldots$$

never stops. [Hint: Assume for contradiction that the sequence stops, i.e., assume that the numbers $p_1, p_2, \ldots, p_k$ are **all of the positive prime numbers**. Now consider the number $N := p_1 p_2 \cdots p_k + 1$. We know from class that the number N has a positive prime factor $p|N$. Prove that this prime p is not in our list.]

3.2. (Infinitely Many Primes $\equiv 3$ Mod 4). In this exercise you will show that the sequence

$$3, 7, 11, 15, 19, 23, 27, \ldots$$

contains infinitely many prime numbers.

(a) Consider a positive integer $n \geqslant 1$. If $[n]_4 = [3]_4$, prove that n has a positive prime factor $p|n$ such that $[p]_4 = [3]_4$. [Hint: We know from class that n can be written as a product of positive primes. What if none of them are in the set $[3]_4$?]

(b) Assume for contradiction that there are only finitely many positive primes in $[3]_4$ and call them

$$3 < p_1 < p_2 < \cdots < p_k.$$

Now use part (a) to obtain a contradiction. [Hint: Define the number $N := 4p_1p_2 \cdots p_k + 3$. By part (a) this number has a positive prime factor $p \in [3]_4$. Show that the prime p is not in your list.]

3.3. (Infinitely Many Primes $\equiv 1$ Mod 4). In this exercise you will show that the sequence

$$1, 5, 9, 13, 17, 21, 25, \ldots$$

contains infinitely many prime numbers.

(a) Assume for contradiction that there are only finitely many primes in this list and call them $p_1, p_2, \ldots, p_k$. Now define the numbers

$$x := 2p_1p_2 \cdots p_k,$$
$$N := x^2 + 1.$$

Show that $N \in [1]_4$ and that $N \in [1]_{p_i}$ for all p_i.

(b) If N is **prime**, show that part (a) leads to a contradiction.

(c) If N is **not prime** then there exists a positive prime divisor $q|N$. Use Euclid's Totient Theorem to prove that $q \in [1]_4$ and then show that part (a) still leads to a contradiction. [Hint: Show that 4 is the multiplicative order of x mod q and then use the fact that $\varphi(q) = q - 1$.]

3.4. (Useful Lemma). For all integers $a, b, c \in \mathbb{Z}$ with $\gcd(a, b) = 1$ show that

$$(a|c \wedge b|c) \Rightarrow (ab|c).$$

[Hint: Use the fact that $\gcd(a, b) = 1$ to write $ax + by = 1$ for some $x, y \in \mathbb{Z}$.]

3.5. (Generalization of Euler's Totient Theorem). Consider a positive integer n with prime factorization

$$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}.$$

Now consider any integers $e, f \in \mathbb{Z}$ with the properties

- $e_i \leqslant e$ for all i,
- $\varphi(p_i^{e_i})|f$ for all i.

In this case prove that $[a^{f+e}]_n = [a^e]_n$ for all integers $a \in \mathbb{Z}$. In the special case that $\gcd(a, n) = 1$ we could then multiply both sides by the inverse $[a^{-e}]_n$ to obtain $[a^f]_n = [1]_n$, which is just another way to state Euler's Totient Theorem. [Hint: For all i we have either $p_i|a$ or $p_i \nmid a$. In the former case show that $p_i^{e_i}|a^e$ and in the latter case use Euler's Totient Theorem to show that $p_i^{e_i}|(a^f - 1)$. In either case we have $p_i^{e_i}|a^e(a^f - 1)$. Now use 3.4 to conclude that $n|a^e(a^f - 1)$.]

[The previous result has an application to the Party Trick that we discussed in class. The prime factorization of 100 is $2^2 \cdot 5^2$. Since $e = 2$ is greater than or equal to both exponents and since $\varphi(100) = 40$ is divisible by both $\varphi(2^2) = 2$ and $\varphi(5^2) = 4$ we conclude that $[a^{42}]_{100} = [a^{40+2}]_{100} = [a^2]_{100}$ for all integers $a \in \mathbb{Z}$. Now you can impress your friends by quickly computing the last two digits of the number a^{42}. And that's not all; the result of 3.5 is also good for cryptography.]

3.6. (RSA Cryptosystem). Consider prime numbers $p, q \in \mathbb{Z}$. Since $\varphi(pq) = (p-1)(q-1)$, Euler's Totient Theorem tells us that for all integers $a \in \mathbb{Z}$ with $\gcd(a, pq) = 1$ we have

$$[a^{(p-1)(q-1)}]_{pq} = [1]_{pq},$$

and then multiplying both sides by $[a]_{pq}$ gives

$$\text{(RSA)} \qquad [a^{(p-1)(q-1)+1}]_{pq} = [a]_{pq}.$$

Now use 3.5 to show that the second equation (RSA) **still holds when** $\gcd(a, pq) \neq 1$, even though the first equation does not.