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.]

Proof. Assume for contradiction that there are only finitely many positive primes and denote them by $p_1, p_2, \ldots, p_k$. Now consider the number

$$N := p_1 p_2 \cdots p_k + 1.$$

Since $N \geqslant 2$ we know from class that N has a positive prime factor, say $p|N$. By the assumption that $p_1, p_2, \ldots, p_k$ are all of the primes we must have $p_i = p$ for some i. But since $p|N$ we know that $[N]_p = [0]_p$ and from the definition of N we have $[N]_{p_i} = [1]_{p_i}$ for all i. Thus if $p = p_i$ for some i then we obtain the equation

$$[0]_p = [N]_p = [1]_p,$$

which contradicts the uniqueness of remainders. □

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.]

Proof. (a): Let $n \geqslant 1$ and suppose that $[n]_4 = [3]_4$. We know from class that n can be written as a finite product of positive primes, say $n = p_1 p_2 \cdots p_k$. The assumption $[n]_4 = [3]_4$ implies that n is **odd** so all of the primes p_i must also we odd. In other words, for each i we have either $[p_i]_4 = [1]_4$ or $[p_i]_4 = [3]$. Finally, we assume for contradiction that $[p_i]_4 = [1]_4$ for all i. Then we obtain

$$\begin{aligned}
[n]_4 &= [p_1 p_2 \cdots p_k]_4 \\
&= [p_1]_4 \cdot [p_2]_4 \cdots [p_k]_4 \\
&= [1]_4 \cdot [1]_4 \cdots [1]_4 \\
&= [1]_4,
\end{aligned}$$

which contradicts the fact that $[n]_4 = [3]_4$. We conclude that there exists some i such that $[p_i]_4 = [3]_4$ as desired.

(b): Assume for contradiction that there are finitely many positive primes in the set $[3]_4$ and denote them by

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

Now consider the number $N := 4p_1p_2 \cdots p_k + 3$. Since $[N]_4 = [3]_4$ we know from part (a) that there exists a positive prime factor $p|N$ such that $[p]_4 = [3]_4$. I claim that $p \neq 3$. Indeed, if $3|N$ then we would also have $3|4p_1p_2 \cdots p_k$ and by Euclid's Lemma this would imply that $3|p_i$ for some i. But since p_i is prime and $p_i > 3$ this is a contradiction. Now since $p \neq 3$ is a positive prime in the set $[3]_4$ we must have $p = p_i$ for some i. But since $p|N$ we know that $[N]_p = [0]_p$ and from the definition of N we have $[N]_{p_i} = [3]_{p_i}$ for all i. Thus if $p = p_i$ for some i then we obtain the equation

$$[0]_p = [N]_p = [3]_p,$$

which contradicts the uniqueness of remainders because $p > 3$. □

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

$$\begin{aligned}
x &:= 2p_1p_2 \cdots p_k, \\
N &:= x^2 + 1.
\end{aligned}$$

Show that $N \in [1]_4$ and that $N \in [1]_{p_i}$ for all 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 Euclids 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 $\varphi(q) = q - 1$.]

Proof. (a): Note that $2|x$. From Euclid's Lemma (or unique factorization) this implies that $4|x^2$ and hence $[x^2]_4 = [0]_4$. Then we find that

$$[N]_4 = [x^2 + 1]_4 = [x^2]_4 + [1]_4 = [0]_4 + [1]_4 = [1]_4$$

as desired. Note also that $p_i|x$ for each i, so that $p_i|x^2$ and hence $[x^2]_{p_i} = [0]_{p_i}$. Then a similar argument gives $[N]_{p_i} = [1]_{p_i}$.

(b): Suppose that N is **prime**. By part (a) we know that $[N]_4 = [1]_4$ which implies that we must have $N = p_i$ for some i. But then we would also have from part (a) that

$$[1]_N = [1]_{p_i} = [N]_{p_i} = [N]_N = [0]_N,$$

which contradicts the uniqueness of remainders.

(c): If N is **not prime** then we still know that N has a prime factor, say $q|N$, and since N is odd we can assume that $q > 2$. In this case I claim that x has multiplicative order 4 mod q. Indeed, we can reduce the equation $x^2 + 1 = N$ mod q to obtain

$$\begin{aligned}
[x^2+1]_q &= [N]_q \\
[x^2]_q + [1]_q &= [0]_q \\
[x^2]_q &= [-1]_q \\
([x^2]_q)^2 &= ([-1]_q)^2 \\
[x^4]_q &= [1]_q.
\end{aligned}$$

This implies that the multiplicative order $o_q(x)$ **divides** 4. But we also know that $[x]_q \neq [1]_q$ since otherwise we would have

$$[q-1]_q = [-1]_q = [x^2]_q = ([x]_q)^2 = ([1]_q)^2 = [1]_q,$$

which contradicts the uniqueness of remainders because $q > 2$. We conclude that $o_q(x) = 4$.

In general, Euler's Totient Theorem says that the multiplicative order $o_q(x)$ divides the value of the totient function $\varphi(q)$. Since q is prime this means that 4 divides $\varphi(q) = q-1$, and hence $[q]_4 = [1]_4$. Since the list $p_1, p_2, \ldots, p_k$ contains **all** positive primes of the form $[1]_4$ we must have $q = p_i$ for some p_i. But then from part (a) we would have $[N]_q = [1]_q$ which contradicts the fact that q divides N. □

[We have seen that there are infinitely many positive primes in the sets $[1]_2$, $[1]_4$ and $[3]_4$. More generally, it is a theorem of Dirichlet (1837) that there exist infinitely many primes in the set $[a]_n$ for any coprime integers $\gcd(a,n) = 1$. It turns out that this theorem is very difficult to prove; Dirichlet's proof used complex analysis and gave birth to the subject of "analytic number theory". We can rephrase the result by saying that for integers $\gcd(a,n) = 1$, the linear polynomial $f(x) = nx + a$ takes infinitely many prime values. For quadratic polynomials the problem is even harder. Landau's 4th Problem (1914) asks whether there are infinitely many primes of the form $x^2 + 1$. It is still open.]

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

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

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

Proof. Consider integers $a, b, c \in \mathbb{Z}$ with $\gcd(a,b) = 1$ and assume that we have $a|c$ and $b|c$, say $c = ac'$ and $c = bc''$. Since $\gcd(a,b) = 1$ the Euclidean Algorithm says that there exist integers $x, y \in \mathbb{Z}$ such that $ax + by + 1$. Then multiplying this equation by c gives

$$\begin{aligned}
1 &= ax + by \\
c &= c(ax + by) \\
c &= cax + cby \\
c &= (bc'')(ax) + (ac')(by) \\
c &= (ab)(c''x) + (ab)(c'y) \\
c &= (ab)(c''x + c'y),
\end{aligned}$$

which implies that $(ab)|c$ as desired. $\square$

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

$$n = p_1^{e_1} p_2^{e_2} p_3^{e_3} \cdots .$$

Now consider any non-negative integers $e, f \in \mathbb{N}$ 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 $n|a^e(a^f - 1)$.]

Proof. Consider the factor $p_i^{e_i}$ of n. Assuming that $e_i \leqslant e$ and $\varphi(p_i^{e_i})|f$, our goal is to show that $p_i^{e_i}|a^e(a^f - 1)$ for **all** integers $a \in \mathbb{Z}$. Then since the factors $p_i^{e_i}$ and $p_j^{e_j}$ are coprime for $i \neq j$ we can use the result of Problem 3.4 to conclude that $n|a^e(a^f - 1) = (a^{f+e} - a^e)$ and hence

$$[a^{f+e}]_n = [a^e]_n$$

for all integers $a \in \mathbb{Z}$.

There are two cases: (1) If $p_i|a$ then by Euclid's Lemma (or unique factorization) we must have $p_i^{e_i}|a^{e_i}$, and since $e_i \leqslant e$ we must have $a^{e_i}|a^e$. Putting the two together gives $p_i^{e_i}|a^e$ and hence $p_i^{e_i}|a^e(a^f - 1)$. (2) If $p_i \nmid a$ then since p_i is prime we must have $\gcd(a, p_i^{e_i}) = 1$. In this case Euler's Totient Theorem says that the multiplicative order $o_i(a)$ of a mod $p_i^{e_i}$ divides $\varphi(p_i^{e_i})$. Now the assumption $\varphi(p_i^{e_i})|f$ implies that we have $f = o_i(a) \cdot k$ for some $k \in \mathbb{N}$ and hence

$$[a^f]_{p_i^{e_i}} = [a^{o_i(a)\cdot k}]_{p_i^{e_i}} = \left([a^{o_i(a)}]_{p_i^{e_i}}\right)^k = \left([1]_{p_i^{e_i}}\right)^k = [1]_{p_i^{e_i}}.$$

In other words, we have $p_i^{e_i}|(a^f - 1)$, which implies that $p_i^{e_i}|a^e(a^f - 1)$ as desired. $\square$

[We proved in class that $\varphi(n) = \prod_i \varphi(p_i^{e_i})$, hence for any non-negative integer $k \geqslant 0$, the integer $f = \varphi(n)k$ satisfies the assumption of Problem 3.5. (This motivates our use of the letter "f".) Then the result of 3.5 implies that we have

$$[a^{\varphi(n)k+e}]_n = [a^e]_n$$

for all integers $a \in \mathbb{Z}$ and for all non-negative integers $k, e \in \mathbb{N}$ such that $e_i \leqslant e$ for all i.]

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 with $\gcd(a, pq) = 1$ we have

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

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

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

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.

Proof. There is not much to do here. Let a be **any integer** and let $n = p^1 q^1$. Then the result of 3.5 implies that for any non-negative integers $e, f \in \mathbb{N}$ such that $1 \leqslant e$ and $(p-1)(q-1) = \varphi(n)|f$ we have $[a^{f+e}]_n = [a^e]_n$. In other words, for all integers $a \in \mathbb{Z}$ and for all $e \geqslant 1$ and $k \geqslant 0$ we have

$$[a^{(p-1)(q-1)k+e}]_{pq} = [a^e]_{pq}.$$

$\square$

[We will see in class what this equation is good for; the title of Problem 3.6 is a hint.]