Ma6 Set 1

Victoria Liu

October 19, 2020

Problem 1

Proof. We have already shown in class that there are infinitely many primes. For $n \pmod 4$, we see that only forms congruent to $1 \pmod 4$ or $3 \pmod 4$ may have infinitely primes, since $0 \pmod 4$ and $2 \pmod 4$ are even. We want to show that there are infinitely many primes of the form $3 \pmod 4$.

We use proof by contradiction. Suppose there are a finite number of primes of the form $3 \pmod 4$, sorted in order from $p_0, p_1, p_2, ...p_n$. This would make $p_0 = 3, p_1 = 7$, and so on. Now, we consider the number $a = p_0 \cdot p_1 \cdot p_2 \cdot ... \cdot p_n + 3$. Note that we are not including $p_0 = 3$, which will be useful later. Since $a > p_n$, under our assumption of finite primes, a must be composite. Now we are interested in finding its factors.

We notice that a is odd, so it cannot have even factors such as $0 \pmod 4$ or $2 \pmod 4$. It must have factors of the forms $1 \pmod 4$ or $3 \pmod 4$. We notice that numbers of the form $4k + 1$ are closed under multiplication, so a must have at least one factor of the form $3 \pmod 4$. However, this is impossible because each $p_1, p_1, p_2, ...p_n$ divides $a - 3$ (i.e. a can be written as $3 \pmod{p_i}$ where $1 \leq i \leq n$. Since $p_i > 3$, we will never get $a = 0 \pmod{p)_i}$, so a actually cannot have any factors of the form $3 \pmod 4$. Now, we've reached a contradiction, since we earlier showed that a must have factors of the form $3 \pmod 4$. Thus, our original premise that there are a finite number of primes of the form $3 \pmod 4$ must be false, and there must actually be an infinite number of primes of form $3 \pmod 4$.

□

Problem 2

2.a

This is not transitive; for example, $2 \sim 3$ and $3 \sim 4$, but this does not imply $2 \sim 4$, since $2|4$.

2.b

This is not transitive; $2020 \sim 2$ and $2 \sim 0$. However, this does not imply $2020 \sim 0$ because $2020 > 0 + 2019$

2.c

This is transitive. If $a^2 \equiv b^2 \pmod{2019}$, then we can find q such that $2019 * q = a^2 - b^2$. Likewise, if $b^2 \equiv c^2 \pmod{2019}$, then we can find s such that $2019 * s = b^2 - c^2$. Now, we write $a^2 - c^2$ as:

$$a^2 - c^2 = (a^2 - b^2) + (b^2 - c^2) = q * 2019 + s * 2019 = 2019 * (r + s) \tag{1}$$

This implies that $2019|a^2 - c^2$, and $a^2 \equiv c^2 \pmod{2019}$, and $a^2 \sim c^2 \pmod{2019}$

2.d

This statement is not transitive; for example, $\gcd(2020, 4082420) = 2020$ and $\gcd(4082420, 2021) = 2020$. This means that $2020 \sim 4082420$ and $4082420 \sim 2021$. However, $\gcd(2020, 2021) = 1$, so the transitive statement $2020 \sim 2021$ does not hold.

Problem 3

Proof. We begin by writing the base ten number $a_n a_{n-1} \cdots a_1 a_0$ as:

$$a_n * 10^n + a_{n-1} * 10^{n-1} + \cdots + a_1 * 10^1 + a_0 * 10^0 \tag{2}$$

We can pull out the value of one a term from each addend as such:

$$[a_n + a_{n-1} + \cdots + a_2 + a_1 + a_0] + [a_n * (10^n - 1) + a_{n-1} * (10^{n-1} - 1) + \cdots + a_2 * 99 + a_1 * 9] \tag{3}$$

Note the two groupings in the boldface brackets. Let's call their respective sums b and c. For clarification:

$$b = a_n + a_{n-1} + \cdots + a_2 + a_1 + a_0 \tag{4}$$

$$c = a_n * (10^n - 1) + a_{n-1} * (10^{n-1} - 1) + \cdots + a_2 * 99 + a_1 * 9 \tag{5}$$

$$a_n a_{n-1} \cdots a_1 a_0 = b + c \tag{6}$$

$9|c$ because each number in this grouping is multiplied by a number divisible by nine. We know this because $10^m - 1 = 9 * n$, where n is an $(m-1)$-digit-long number composed of 1's. We can now see that when b is divisible by 9, then our original number $a_n a_{n-1} \cdots a_1 a_0$ will be divisible by 9 as well. By the same token, if our original number is divisible by 9, then we would be able to write the value of the number in the form of $b + c$, and b must be divisible by 9 since c always is. Note that b is the value of all the digits summed up, and it is exactly what the problem is asking for. So QED!

□

Problem 4

4.a

Proof. Let L_a represent the last digit of the a^{th} Fibonacci number. We first show that a cycle of last digits exists. We note that if we can find a non-zero r in the set $\{r \mid L_r = 0 \wedge L_{r+1} = 1\}$, then a cycle consisting of r Fibonacci last digits exists. This is because the Fibonacci sequence is defined recursively by the previous two elements, so finding consecutive numbers that end in 0 and 1, respectively, will be the same as starting a new cycle. Using Mathematica, we see that F_{60} and F_{61} are the first such numbers ending in 0 and 1, respectively. Thus, a cycle of last digits exists, and this 60-digit cycle can include all numbers of the Fibonacci sequence (i.e., we don't have a sequence like $1, 2, 3, 4, 5, 4, 5, 4, 5...$, where the cycle does not include the first three numbers).

Now, we want to show that there are an infinite number of such cycles of size 60. We will use a proof by contradiction. Suppose instead that we have a finite number $a + 1$ cycles. This means that after $60 * a + 60$ numbers, we no longer have cycles. Let's look at the two numbers immediately before, and they are still in a cycle so $L_{60*a+58} = 9$ and $L_{60*a+59} = 1$. These two numbers then define $L_{60*a+60} = 0$ and $L_{60*a+61} = 1$. Now, $L_{60*a+60}$ and $L_{60*a+61}$ can start a new cycle. This contradicts our assumption that there would be no more cycles after $60 * a + 60)$ numbers. Thus, our original assumption is wrong, and there are an infinite number of such cycles.

□

4.b

Before we get to the actual proof, we use the Remainder Theorem to show that

$$\gcd(F_a, F_{a+1}) = 1 \tag{7}$$

for every natural number a. This will be useful later. Let's first show the base case, where $a = 0$, and we see that $\gcd(F_0, F_1) = 1$. We see that it works for $a = 1$ as well, where $\gcd(F_1, F_2) = 1$. Now, let's assume this is true for all numbers up to k, so $\gcd(F_k, F_{k+1}) = 1$. We notice that the remainder of F_{k+2}/F_{k+1} is F_k. Using the Remainder Theorem, we see that:

$$\gcd(F_{k+2}, F_{k+1}) = \gcd(F_{k+1}, F_k) = 1 \tag{8}$$

By our induction hypothesis, $gcd(F_{k+2}, F_{k+1}) = 1$, thus completing the proof. In other words, consecutive Fibonacci numbers are relatively prime.

Proof. Now, we split the problem set proof into two parts, first proving that the cycles are of length equal or less than $m^2 - 1$, and then proving that there are infinite such cycles. For the first part, let us consider $m > 1$, since the statement does not work for $m = 1$; when $m = 1$, every number is congruent to $0 \pmod 1$, so we have a cycle size of 1, which is greater than $m^2 - 1$.

Our proof will be similar to a pigeon-hole proof. We will do a proof by contradiction, first assuming that there are at least m^2 numbers per cycle. Let us consider any $m^2 + 1$ consecutive Fibonacci numbers $\pmod m$ (i.e. we have exactly m^2 numbers in a cycle, so we would be considering all

numbers of a cycle, plus the first number of the next cycle). Out of these $m^2 + 1$ consecutive numbers, we have m^2 pairings of two consecutive numbers. We are working in $\pmod m$, so there are exactly m^2 possible ways to fill these two consecutive spaces. However, we know that two consecutive numbers cannot both be $0 \pmod m$ because two consecutive Fibonacci numbers are relatively prime. Going back to our m^2 pairings of two consecutive numbers, we now see that there must be a repeat pairing within these $m^2 + 1$ numbers, since $(0, 0)$ is not allowed. Let's say that the repeats happen at $(F_a \pmod m, F_{a+1} \pmod m)$ and $(F_{a+k} \pmod m, F_{a+k+1} \pmod m)$. Since we are only talking about $m^2 + 1$ consecutive numbers, $\mathbf{k \leq m^2 - 1}$. However, notice that by having repeated consecutive number pairs, we are starting the cycle again; this is because the Fibonacci sequence is recursively defined by the two previous numbers. In other words, $F_{a+l} = F_{a+k+l}$ for any $l \in \mathbb{N}$, and the cycle length is k. Our original assumption of having a cycle length of at least m^2 means that $k \geq m^2$. This contradicts the boldface claim above, suggesting that our original assumption is incorrect. In other words, cycles are of length equal or less than $m^2 - 1$.

Now, we show that there are infinite such cycles. Let $c \leq m^2 - 1$ be the number of elements per cycle. Suppose instead that we have a finite number $a + 1$ cycles. This means that after $c * a + c$ numbers, we no longer have cycles. Let's look at the two numbers immediately before, and they are still in a cycle so $L_{c*a+c-2} = L_{c*a-2}$ and $L_{c*a+c-1} = L_{c*a-1}$. These two numbers then define $L_{c*a+c} = L_{c*a}$ and $L_{c*a+c+1} = L_{c*a+1}$. Now, L_{c*a+c} and $L_{c*a+c+1}$ can start a new cycle, since the Fibonacci numbers are defined recursively by two consecutive numbers. This contradicts our assumption that there would be no more cycles after $c * a + c$ numbers. Thus, our original assumption is wrong, and there are an infinite number of such cycles.

□

4.c

Proof. We examine the Fibonacci numbers $\pmod{F_r}$. We know that $F_0 \equiv 0 \pmod{F_r}$, and $F_r \equiv 0 \pmod{F_r}$ as well. Since $F_r \equiv 0 \pmod{F_r}$, then $F_{r+1} \equiv F_{r-1} \pmod{F_r}$, and $F_{r+2} \equiv F_{r-1} \pmod{F_r}$ as well, and we can see that these three numbers congruent to the F_0, F_1, and F_2 multiplied by F_{r-1}, all $\pmod{F_r}$. To explore this cyclical nature more thoroughly, we will use *mod* multiplication rules. We see that $F_{r-1} \equiv F_{r-1} \pmod{F_r}$. Now, we multiply this expression with the expressions for F_0 and F_1 to get the expressions for F_r and F_{r+1}:

$$F_{r-1} * F_0 \pmod{F_r} \equiv F_{r-1} * 0 \pmod{F_r} \equiv F_r \pmod{F_r} \tag{9}$$

$$F_{r-1} * F_1 \pmod{F_r} \equiv F_{r-1} * 1 \pmod{F_r} \equiv F_{r+1} \pmod{F_r} \tag{10}$$

To be clear, the important equations are:

$$F_r \pmod{F_r} \equiv F_{r-1} * F_0 \tag{11}$$

$$F_{r+1} \pmod{F_r} \equiv F_{r-1} * F_1 \tag{12}$$

This gives us a convenient "cycle" every r numbers, where $F_{a*r} \equiv 0 \pmod{F_r}$ for any $a \in \mathbb{N}$; the cycle results because of *mod* addition rules and the recursive nature of the Fibonacci sequence. More generally,

$$F_{a*r+b} \pmod{F_r} \equiv F_{a*r-1} * F_b \tag{13}$$

Since $F_{a*r} \equiv 0 \pmod{F_r}$, this means that for any F_n where $r|n$, we can find k such that $k * F_r = F_n$.

□

Problem 5

The prime factorization of 2881 is $43 * 67$, meaning that $\phi(2881) = 42 * 66 = 2772$. We have our encryption key $e = 5$, and now we want to find d such that $ed \equiv 1 \pmod{2772}$. We write a function called coef_extended_euclid(), which takes in two relatively prime numbers, e and $\phi(n)$, and spits out the coefficients d and a such that $d * e + a * \phi(n) = 1$. Notice that this means $ed \equiv 1 \pmod{\phi(n)}$.

[32]:
```
import numpy as np
def coef_extended_euclid(rprime_1, rprime_2):
    """
    given two relatively prime numbers, spits out the coefficients for
    coef_1 * rprime_1 + coef_2 * rprime_2 = 1. Make sure
    rprime_1 > rprime_2.
    """
    #we create rows of the extended Euclidian matrix
    row_0 = np.asarray([rprime_1, 1, 0])
    row_1 = np.asarray([rprime_2, 0, 1])

    #the multiplicative factor for row_1
    floor_quotient = rprime_1 // rprime_2

    #Extended Euclidian matrix
    while row_1[0] > 1:
        row_2 = row_0 - floor_quotient * row_1
        row_0 = row_1
        row_1 = row_2
        floor_quotient = row_0[0] // row_1[0]

    coef_1 = row_1[1]
    coef_2 = row_1[2]
    return (coef_1, coef_2)

def decryption(e, totient_n):
    """
    e is the encryption number
    d is the decryption number
```

```
    """
    _, d = coef_extended_euclid(totient_n, e)
    return d

d = decryption(5, 2772)
print("decryption d = ", d)
```

```
decryption d =  1109
```

We get $d = 1109$, and we use Mathematica for modular exponentiation.

$$559^{1109} \equiv 301 \pmod{2881} \tag{14}$$

$$752^{1109} \equiv 1220 \pmod{2881} \tag{15}$$

$$915^{1109} \equiv 503 \pmod{2881} \tag{16}$$

$$849^{1109} \equiv 862 \pmod{2881} \tag{17}$$

$$405^{1109} \equiv 119 \pmod{2881} \tag{18}$$

$$2^{1109} \equiv 309 \pmod{2881} \tag{19}$$

$$1702^{1109} \equiv 913 \pmod{2881} \tag{20}$$

$$1373^{1109} \equiv 920 \pmod{2881} \tag{21}$$

$$\tag{22}$$

We find that 0301 1220 0503 0862 0119 0309 0913 0920 corresponds to the message "CALTECH>ASCIIMIT", or just "CALTECH>MIT", since the ASCII special symbol for ">" is 62.