Homework 5

1. *Without the aid of a computer program, determine the prime factorization of 16,141,806,000. Show your work.*

First let’s take out the factors of 10

Looking at the sum of the digits of , we see that it is , a multiple of , and since the number is also even, we can take out a factor of

Sadly, using the divisibility trick for doesn’t yield satisfactory results, as , which is not a multiple of . Similarly, the divisibility trick for yields , which is not divisible by . (The trick involves taking the last digit of , and performing ), a proof is on the last page if needed for to utilize this trick\*).

The next prime I decided to check the divisibility rule is for , This also involves a similar trick as , where we check , using

As we can see this sum is divisible by , so that means the original number is also a multiple of . Dividing out:

Checking again:

This number has a remainder of when divided by as well, so is a factor again.

Here I was able to see that , and the fact that So is also a prime factor.

Writing this in just prime notation:

1. *What is φ(16,141,806,000)?*

Since we got the prime factorization for this number earlier, we can use the properties of the Euler Phi function by splitting up the primes

1. *Use Fermat’s Theorem to calculate the remainder when is divided by 983*

Looking at , we should first determine if it is prime. Since , we only need to observe primes up to . Quick observation shows that is not divisible by . Looking at , , so is not divisible by , Similarly looking at other multiples, we can see that is not divisible by . Therefore, is prime. In addition, since is prime, is relatively prime to .

Looking at the question in modular arithmetic:

We can split this up into parts

Since is relatively prime to , By Fermat’s theorem,

We saw from Fermat’s theorem that , so from this:

Therefore, the remainder is:

1. *Use Euler’s Theorem to calculate the remainder when is divided by 10829?*

First, it is probably a good idea to find out what is. We need to get the prime factorization of . Obviously, this number is not divisible by . Checking the divisibility trick for

We see that this sum is divisible by , so is a multiple of

This is also divisible by again since

Finishing the prime factorization:

Therefore,

We can apply a similar trick we did for Number 3 on this problem, namely, splitting the exponent (Also, in case I need to mention it, since is relatively prime to since it does not share a factor of or with due to the prime factorization)

By Euler’s Theorem, , since .

Since

Therefore, the value of the remainder is:

1. *Show the steps of running the Miller-Rabin algorithm, testing for primality  
   with the randomly chosen value of .*

The first step is to write out the equation

Where is an odd integer. We know that , by observing its divisibility with

We can stop here since is odd. Now we use our value of that was given in the problem, and compute . I’ll use the fast modular exponent function I wrote for for my calculations (I did not do these questions in order).

Since this value is not , we need to do more testing. Now we perform the for loop part of the algorithm, from

Step 1, , so we perform the else statement block,

Step 2, , perform else block,

Step 3, Else block,

**We have gone through all the values, and never reached a point where mod , Therefore, we can state that, is Composite.**

1. *Trace through the Fermat Factoring algorithm to factor 245,239 as the product of two  
   prime numbers.*

For Fermat Factoring, we want to start at the “midpoint” of where the multiplications can occur, namely,

We can start our algorithm at the ceiling of this, . Since we can represent as , with starting at and working our way up and solving for each time until is a perfect square.

(not perfect square)

(not perfect square)

(not perfect square)

(not perfect square)

(This is , so we can stop)

Rewriting this,

Therefore, our two prime numbers are:

As a side note, we could have done the algorithmic step by adding where is our current value from step 1, for example and .

1. *A primitive root, α, of a prime, p, is a value such that when you calculate the remainders of , when divided by p, each number from the set {1, 2, 3, ..., p-1} shows up exactly once. Prove that a prime p has exactly φ(p-1) primitive roots.*

My first thought process was to apply something similar to the proof of Fermat’s theorem. First, I decided to observe that if a primitive root exists, and it forms the set then we could potentially look at the sum of these remainders:

If is not a primitive root, then this will be violated. A good example is by looking at under the prime

By the nature of mod, this pattern gets repeated for powers , meaning that the sum in this case is whereas a primitive root of should give us a sum of . However, this didn’t amount to anything significant and I couldn’t go forward with this anywhere.

Naturally, I decided to observe multiplication next, thinking it may shine a new light on this problem. Instead of multiplying the remainders, I looked at multiplying all the powers of under mod

If is a primitive root, these multiplications should be equivalent to under mod . This is because under mod , each term becomes a member of the set

We can simplify this further by recognizing that every integer besides in the set has a modular inverse in that is unique from the other integers,

Proof of this is as follows; Assume there are two integers that share a modular inverse, , mod , we have the following relation

This means that divides evenly into , or divides evenly into . It is obvious that cannot divide evenly into since , and since , there is no way for this statement to be true assuming and share a modular inverse.

Therefore, every element in the set has a unique modular inverse mod by contradiction.

Now we can do some simplification, there are an even number of numbers from , since , So we can multiply the values from together such that the terms that multiply are modular inverses of each other. The only remaining terms are and since their modular inverses are themselves. :

So, if is a primitive root of , then the following relation holds under mod . The next step is to validate how many integers satisfy this relation in the set . What this also implies, is that for any integer , if there is a cycle in the remainders when divided by , it will show in this relation.

This is good, but we can simplify this result to help specify what we are looking at.

We can say that the value of , this is due to Fermat’s theorem of

What this means is, at the “middle” of our residues, the value should be . We can visualize this with this chart I made for the Residues , starting from to .

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| 2 | 4 | 8 | 5 | 10 | 9 | 7 | 3 | 6 | 1 |
| 3 | 9 | 5 | 4 | 1 | 3 | 9 | 5 | 4 | 1 |
| 4 | 5 | 9 | 3 | 1 | 4 | 5 | 9 | 3 | 1 |
| 5 | 3 | 4 | 9 | 1 | 5 | 3 | 4 | 9 | 1 |
| 6 | 3 | 7 | 9 | 10 | 5 | 8 | 4 | 2 | 1 |
| 7 | 5 | 2 | 3 | 10 | 4 | 6 | 9 | 8 | 1 |
| 8 | 9 | 6 | 4 | 10 | 3 | 2 | 5 | 7 | 1 |
| 9 | 4 | 3 | 5 | 1 | 9 | 4 | 3 | 5 | 1 |
| 10 | 1 | 10 | 1 | 10 | 1 | 10 | 1 | 10 | 1 |

We can see that at position , in this case . The value of for primitive roots is . Whereas it is a otherwise. Sadly, there are exceptions, such as when , as the cycle length is not a common factor of , meaning we also must check all the prime factors of for

Sadly, despite all these really cool findings, I was still stuck on figuring out how to count all the primitive roots. I began to start getting mentally lost on the table I created looking for some other observations I may have missed.

One thing that began standing out to me was the specific remainders at certain indexes on the table, for reference here it is again for residues under mod :

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| 2 | 4 | 8 | 5 | 10 | 9 | 7 | 3 | 6 | 1 |
| 3 | 9 | 5 | 4 | 1 | 3 | 9 | 5 | 4 | 1 |
| 4 | 5 | 9 | 3 | 1 | 4 | 5 | 9 | 3 | 1 |
| 5 | 3 | 4 | 9 | 1 | 5 | 3 | 4 | 9 | 1 |
| 6 | 3 | 7 | 9 | 10 | 5 | 8 | 4 | 2 | 1 |
| 7 | 5 | 2 | 3 | 10 | 4 | 6 | 9 | 8 | 1 |
| 8 | 9 | 6 | 4 | 10 | 3 | 2 | 5 | 7 | 1 |
| 9 | 4 | 3 | 5 | 1 | 9 | 4 | 3 | 5 | 1 |
| 10 | 1 | 10 | 1 | 10 | 1 | 10 | 1 | 10 | 1 |

When we look at the value , a primitive root of , at indexes , we get the values .

When we look at another primitive root, , at these same indexes, we get . Looking at all the primitive roots, at these indexes (or their powers), we get the *other* primitive roots! The significance of the original indexes is the values and are all relatively prime to .

If this is the case, then since for a primitive root every power of leaves a unique residue mod , then the number of primitive roots should be equal to .

However, this may have been a coincidence, so let’s try to generalize this finding

Let be a primitive root of , our claim is that if some integer such that , then where is another primitive root of . This means when we look at the residues of the powers of , they are , under mod this forms the set . Let us say two elements of the set are equivalent to each other, breaking the property of a primitive root, therefore for integers

If and share a factor, meaning such that . We can construct two integer values for and . The first value being , and the second value being .

This fraction is a valid integer since both and are divisible by their GCD. Looking at our relation:

If is some integer , that means that there are two valid integers two create this statement, this means the primitive root property is broken! HOWEVER, if the value of is , then both and are equal to each other! This is illegal in our definition from before, . So, if is relatively prime to , then the statement:

Is a contradiction since . Therefore when is relatively prime to , the set must form the set for some existing primitive root .

A good example to see this is with

Here, our values of and are and respectively. With two different values, we get two same remainders, meaning the powers of do not form the set .

However, with

Here, and , which brings a contradiction that there are elements in that share a remainder modulo . Therefore, if is relatively prime to , this set forms .

**Since our proof initially starts with the fact that exists, this means there are such values for that forms a different primitive root of .**

(Thank you for this question, it was so interesting to think about! I wanted to include all my thought process which is why I include some technically useless information to the proof. Hopefully I did not make any errors ^\_^)

(I will say, after finishing this problem and realizing a set of discrete log notes exists on the course page, that set of notes definitely takes away a sizeable portion of the difficulty in discovering a pattern, so I’m glad I waited on reading those)

1. *In class, we made a chart, for , of the different lengths of cycles produced by exponentiating each of the possible non-zero mod values, mod . We found that two of the values have a cycle length of , two of the values have a cycle length of , 1 value has a cycle length of , and 1 value has a cycle length of . Based on this example, give a counting/logical argument proving the sum below, for prime numbers, :*

Seeing as how on the last problem I was able to make a good discovery with a chart, I decided to start the problem of by drawing a chart of all the integer factors of , and what integers are relatively prime to those.

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 10: | - | 9 | - | 7 | - | - | - | 3 | - | 1 |
| 5: | - | - | - | - | - | - | 4 | 3 | 2 | 1 |
| 2: | - | - | - | - | - | - | - | - | - | 1 |
| 1: | - | - | - | - | - | - | - | - | - | 1 |

As we can see, adding up the number of numbers does show we have a total of , showcasing the summation above. However, besides this, there is not anything immediately obvious.

One thing that did stand out to me was the missing gaps for each number, and how I could potentially “fill” them in to create a pattern. I decided to try multiplying each integers in the chart with the value where the number on the row (e.g. for the row with , I multiplied all the relatively prime integers by ). I then scaled the chart appropriately.

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 10: | - | 9 | - | 7 | - | - | - | 3 | - | 1 |
| 5: | - | - | 8 | - | 6 | - | 4 | - | 2 | - |
| 2: | - | - | - | - | - | 5 | - | - | - | - |
| 1: | 10 | - | - | - | - | - | - | - | - | - |

This actually fills the rest of the gaps we would need to have the integers , which is a much better way of showcasing the summation for the question.

Sadly, for this to go anywhere, I would have to both prove that no set generated by doing this contains a duplicate, and that all the sets combined contain the integers . This seems like a lot of work, so I decided to look at a different approach. Instead, I came back to my *original* chart I made for number

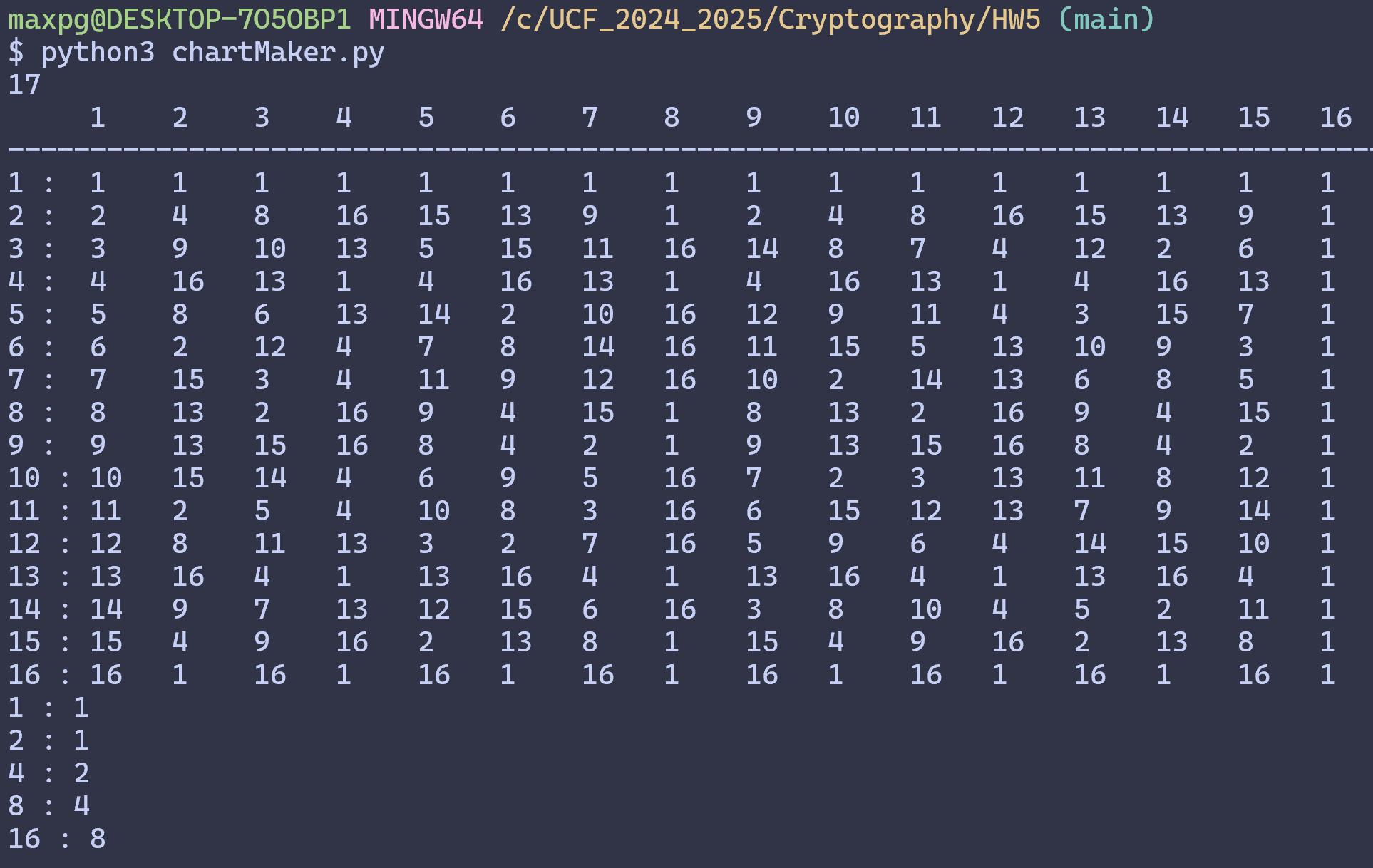
|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| 2 | 4 | 8 | 5 | 10 | 9 | 7 | 3 | 6 | 1 |
| 3 | 9 | 5 | 4 | 1 | 3 | 9 | 5 | 4 | 1 |
| 4 | 5 | 9 | 3 | 1 | 4 | 5 | 9 | 3 | 1 |
| 5 | 3 | 4 | 9 | 1 | 5 | 3 | 4 | 9 | 1 |
| 6 | 3 | 7 | 9 | 10 | 5 | 8 | 4 | 2 | 1 |
| 7 | 5 | 2 | 3 | 10 | 4 | 6 | 9 | 8 | 1 |
| 8 | 9 | 6 | 4 | 10 | 3 | 2 | 5 | 7 | 1 |
| 9 | 4 | 3 | 5 | 1 | 9 | 4 | 3 | 5 | 1 |
| 10 | 1 | 10 | 1 | 10 | 1 | 10 | 1 | 10 | 1 |

Looking at this from a different angle, (also since the problem statement counts the amount of a certain cycle length for 7), I decided to do the same

From this chart we see that (excluding since I was too lazy to write it):

Now of course, these add up to , but a more interesting observation is that the cycle length is actually the amount of relatively prime integers to that value, so for each factor of

Showcasing this for (Screenshot taken from a script’s terminal output that I made)



We can see here that for the factors of , the number of integers with that cycle length is .

Another extremely interesting observation is to look at which numbers actually have the cycle. When we look at which numbers have a cycle of , we see that and have it.

If we raise and to the powers in the set of integers that are relatively prime to We get

It seems that this is generating the set of integers that have a cycle length of , very similar to how worked. If we look at the other cycles, we see a very similar pattern. We can do a proof that no two elements of the set can be equal for some integer with cycle .

Assume we have some integer that has a cycle length of . My claim is that by doing where , then is a new value with a cycle length of . For this to be true, there cannot be any two elements that equal each other, since this means the cycle has changed.

Let us take a generic integer Looking at the set for with cycle length , all of these values must be unique if generates an integer with cycle as well. We can prove this very similarly to how I proved .

Let us assume that two elements *are* equal, we can once again construct two integer values for and in the range . Let and

Once again, . For this statement to be true, . This allows us to satisfy the equation with two unique integer values. So, we can state that the above statement is upheld if and only if . However, if the statement is upheld, that means we break the property of having cycle length . Two elements in the set will be the same if . Therefore, the only values that will fail this condition are .

To illustrate this, let us take a look at some values,

Once again, we want to show that different values for the exponent produce the equation above for . We see that this equation is only true for unique exponents if the .

Therefore, the number of values of that ensure that the equation fails are , where is a divisor of.

**Now for the final part. Every value in the chart will obviously have a cycle. Therefore, the sum of all such where is a divisor of will equal the total amount of numbers from . With this we have proved that**

**For any prime .**

\*Note for number 1

Proof of trick (similar to :

Let be some integer that is **divisible** by , I split into this notation . Now we must look at “dividing” some number by . I am going to factor out a from every term except the ones digit. All operations are under modulus

We say that

By the definition of the floor function, , also, we can observe that is the units digit of , which is essentially

Therefore, we have proved that if , the trick used works for (but not for the problem at hand)