**Principle of Induction proof outline with blanks.**

Suppose it is not true. Let .

This set is \_\_\_\_\_\_\_\_\_\_\_\_\_ and by \_\_\_\_\_\_\_\_\_\_\_\_\_ has a \_\_\_\_\_\_\_\_\_\_\_\_\_\_ element, .

Explain why is in . (two things to show)

Why does this imply that

What’s the contradiction?

**FT of Pascal’s Triangle proof outline.**

Write out first 3 rows two different ways. (we will call the first row the 0th row)

Let

Is

Assume . Must show that \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

What must be? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

Show it by adding fractions and getting a common denominator.

**Binomial Theorem proof outline:**

Let .

Is

Assume , that \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. (\*)

Must show that \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

Multiply both sides of (\*) by

Combine like terms.

All terms are of what form (in terms of powers of and )

What is the coefficient of ?

Use the result of FT of Pascal’s Triangle to add the sum above.

**Division Algorithm: Will be an online assignment soon.**

**for some and as long as and are not both 0, proof outline**

Let .

Explain why it is nonempty.

It is nonempty so by \_\_\_\_\_\_\_\_\_\_\_ has a \_\_\_\_\_\_\_ element, .

So by definition of our set there are integers and so that

We will show

Using the \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ we can obtain integers so that and .

Solve this for and write as a linear combination of and .

If then it would be in \_\_\_\_\_\_\_\_ but the least element in that set is \_\_\_\_ and from above .

So

Explain why divides .

Reversing the roles of and , we can get divides

So is a \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. We will show it is the greatest!

Let be ANY divisor of and . Then explain why divides .

Thus since any common divisor divides it must be the greatest.

**divides and then divides**

Proof: divides means \_\_\_\_\_\_\_\_ similarly divides means\_\_\_\_\_\_\_\_.

= \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ which is a multiple of \_\_\_\_, i.e., divides

**Euclidean Algorithm Lemma:**

Show any common divisor of and is also a common divisor of and and vice versa.

Since both sets of common divisors are the same, the greatest element of each is the same.

**iff**  **for some and**

From left to right is a special case of previous theorem.

Right to left. Assume for some and . Let . Cleary divides \_\_\_ and also \_\_\_. So by an earlier result it divides \_\_\_\_\_\_\_\_\_\_\_\_\_\_= 1, so .

**Euclid’s Lemma. If divides and then divides**

Write 1 = \_\_\_\_\_\_\_\_\_\_\_\_\_\_. Multiply by to get \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. Explain why the result follows.

**then**

Note that all fractions here are really \_\_\_\_\_\_\_\_\_.

Write = \_\_\_\_\_\_\_\_\_\_\_\_\_\_. Divide both sides by to get \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, so by previous result we are done.

**If has a solution then all solutions are given by and where .**

Let be a solution and suppose is also.

Both \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ and \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ .

So . (\*)

By previous result let and . Note that

So and Sub this into (\*) and divide both sides by , to get \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

Now divides \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (right side of previous) and , so by \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ divides \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

So some . \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

Solve for and in terms of

So and . No matter , is a solution to

Plug in for and show you get .

**There are infinitely many primes of the form**

Show the product of 2 numbers of the form is of the same form.

Assume there are only finitely many of this form,

Consider (write in form ) but this can’t be prime because \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. So that means it factors into a product of at least 2 primes, . At least one of these, say is of the form \_\_\_\_\_\_\_\_\_\_\_\_ other wise is of the form .

Can be one of the ? \_\_\_\_\_\_\_ because it would have to divide \_\_\_\_.

**If divides then it divides at least one of them.**

If divides then we are done. If not then . By \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ divides \_\_\_\_\_.

This extends to products of more than 2 numbers.

**has a solution if divides**

(left to right) assume the left, by definition of , we can write \_\_\_\_\_\_\_,

Subbing in to the left should do it!

(right to left) divides means we can write , but by an earlier theorem that says the gcd can be written as a linear combination we get \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

mulitlplying both sides by the letter 2 blanks ago gives , a solution.

**iff and have the same remainder when divided by**

(left to right) The left means that \_\_\_\_\_\_\_\_\_. Let be the remainder when is divided by , so \_\_\_\_\_\_\_\_\_\_, sub this into the previous bland to get \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

(right to left) Use the DA to write out and , remember they have the same remainder.

Show

**implies where**

Because divides both and , we can write \_\_\_\_ \_\_\_\_,

(By the way a short easy to prove result we are using is )

We know that , sub in for and to get \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

Divide by sides by to get \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

So divides \_\_\_\_\_\_\_\_\_\_\_\_\_\_ but so divides \_\_\_\_\_\_\_\_\_\_\_\_\_\_.

So , but we are done because \_\_\_\_\_\_\_.

Two immediate corollaries are implies if and 2. implies provided is not congruent to modulo .

**The decimal representation of a positive integer is unique!**

First we will show there is a representation, start with . We will use the DA over and over to get with each of the ’s with .

Use the DA to divide by 10, let be the first quotient. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ with \_\_\_\_\_\_.

If we are done. If not divide by 10 to get . \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ with \_\_\_\_\_\_.

Here we have \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. If we are done, if not continue. This process must eventually stop.

When it stops we have the claimed representation with each \_\_\_\_\_.

Now for uniqueness.

Suppose . There could be some 0’s at the front of one of them.

We know that .

Suppose one of the is not 0 and the representations differ, in fact let be the first subscript where this happens.

So (look two lines ahead omit 0’s)

Divide both sides by to get \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

Now . So 10 divides , but the smallest can be is \_\_\_\_ and the largest is \_\_\_\_\_. The only thing 10 divides in this range is \_\_\_. So and we are done.

**has a solution iff divides**

iff \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_(definition) iff \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_(get isolated on right hand side)

From earlier the last blank has a solution iff \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

**If has solutions then it has distinct solutions modulo**

Let be a solution to which is equivalent to .

From earlier all solutions are given by

\_\_\_\_\_\_\_\_\_\_\_\_, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

The values of for are:

Claim: all these are incongruent modulo .

Suppose two are congruent, i.e., \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

Subtract from both sides: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

From an earlier result and knowing \_\_\_\_, we can “divide” both sides by gives \_\_\_\_\_\_\_\_\_\_\_\_\_, i.e., the two solutions are the same.

Claim: any solution is congruent to one of these.

Let be any solution. Use the DA to write where \_\_\_\_\_\_\_\_\_.

\_\_\_\_\_\_\_\_\_\_\_\_\_=\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_(multiply out).

**Chinese Remainder Theorem**

Let be the product of all the moduli, i.e., \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

Let .

What is the GCD of and ?

has \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ call it .

Consider .

Show satisfies all the given congruences.

Suppose is also a solution.

This means for each that \_\_\_\_\_\_\_\_\_\_\_\_\_ i.e., divides \_\_\_\_\_\_\_\_.

But all the ’s are \_\_\_\_\_\_\_\_\_\_ so \_\_\_\_\_\_\_\_\_\_\_ divides \_\_\_\_\_\_\_i.e.,

**and both dividing with implies divides .**

Use the definition of “divides” to write two different ways.

Use a result that says if then you can write 1 as a linear combination of and .

Should be able to get a multiple of .

**Fermat’s Little Theorem**

Write out the first multiples of a:

Are any congruent to 0 modulo ?

Claim: They are all incongruent modulo .

Suppose two are congruent, i.e.,

Dividing both sides by yields \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_meaning the solutions are actually the same.

What is the simpliest way to write numbers all different modulo and not congruent to 0?

These numbers above are the same as in the first blank, although probably in different order. So the products are the same modulo , write this out:

Cancel out stuff on both sides to get the result.

An immediate corollary is . Why immediate?

Is the contrapositive of the theorem true? What is it?

Is the converse of the theorem true? What is it?

**an odd pseudoprime makes a larger pseudoprime.**

larger is obvious.

How can you factor ?

with both bigger than 1 since is not \_\_\_\_\_\_\_\_\_\_\_\_\_.

pseudoprime means that , or \_\_\_\_\_\_\_\_=\_\_\_\_.

So .

We want

(use last blank) (use the factor thing above with ) by using the definition of .

**Wilson’s Theorem**

Show it works for .

Take

Let

How many solutions does have?

Call the one solution , so that

will be iff \_\_\_\_\_\_\_\_\_\_\_\_\_\_, which is the same as \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (factor) which only happens if \_\_\_\_\_\_ or \_\_\_\_\_\_\_\_

So remove those two and look at the set of \_\_\_\_\_\_\_\_\_\_\_ numbers .

These can be paired up in \_\_\_\_\_\_\_\_\_\_ pairs , etc.

So \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Multiply both side by 1 an to get \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Converse of Wilson’s Theorem**

Suppose that is not prime. Then it has a proper divisor \_\_\_\_\_. But it is one of the factors of \_\_\_\_\_\_\_\_\_\_\_.

So divides \_\_\_\_\_\_\_\_\_\_, if the converse is not true then divides \_\_\_\_\_\_\_\_\_\_, but divides , so also divides \_\_\_\_\_\_\_\_\_\_, this yields a contradiction in that divides \_\_\_\_\_\_.

**The divisors of are of where**

We must show any divisor is of that form and anything of that form is a divisor.

Let then showing that anything of that form is a divisor.

Let be any divisor of . Can the prime factorization of have any primes not in the list ?

Can the prime factorization of have any exponents on the primes in the previous list greater than ?

So any divisor must be of the form given.

**.**

Let .

Multiply both sides by .

Add the two equations to get….

Factor out ( from the LHS and divided both sides by this to get the result.

**Let then and .**

From the last result the divisors are \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

How many choices for the exponent on ?\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

Multiplying those together gives the result for .

Consider. Note that when multiplied out every divisor of shows up exactly once.

So the sum of all the divisors is this product.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ and so forth giving the result.

**It is the case that**

Let be any divisor of , so . There will be \_\_\_\_\_\_\_ pairs of the ’s and ’s because there are \_\_\_\_\_\_ divisors of .

Multiplying out the product of all the ’s and writing two ways we can get:

\_\_\_\_\_\_\_\_(a power of ) = \_\_\_\_\_\_\_\_\_\_\_\_\_\_(product of all the divisors of ) \* \_\_\_\_\_\_\_\_\_\_\_\_\_\_(product of all the divisors of ) because if you let be the divisors of (what is the ? subscript?) then what will be?

Rewriting above we get

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_=\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (this side should be a square)

Taking the square root gives the answer!

There is a potential problem here, when is odd?

Note in these cases the left side will be an integer. Why?

**and are multiplicative**

Let and be greater than 1, noting that if either are 1, the result follows. (where do we really need this below?)

Let ,

Write out prime factorizations of each

Is there any common primes in each factorization?

So \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ =

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_(first half)\*\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_(second half) =

\_\_\_\_\_\_\_\_\_\*\_\_\_\_\_\_.

Similary

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ =

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_(first half)\*\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_(second half) =

\_\_\_\_\_\_\_\_\_\*\_\_\_\_\_\_.

**Let then the divisors of are of the form where divides and divides , and these products are all distinct and**

Let , write out the prime factorizations of each.

Are there any common primes to each?

So = \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

Let be an divisor of this, so = \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ with\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ and \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, and this factorization is \_\_\_\_\_\_\_\_\_\_\_\_\_.

We can write , where = \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ and divides and = \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ and divides . So any divisor is of the promised form.

Are there any common primes to and ?

So .

Finally, if for some divisor of , we have with \_\_\_\_\_\_ dividing \_\_\_\_\_\_ and \_\_\_\_\_\_ dividing \_\_\_\_\_, Now divides \_\_\_\_\_ and since ( = \_\_\_\_ since they have no common prime factor. Of course similarly divides \_\_\_\_\_, so they are equal as well as the ’s. So all such products are distinct.

**If is multiplicative then so is**

Let .

Now (use definition of letting the divisors be ) =

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(use previous result with )

We know that \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

Now \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_(use previous 2 blanks).

What is ?

If we multiply out these sums, the terms will be of the form \_\_\_\_\_\_\_\_\_\_\_\_\_ where \_\_\_\_\_\_\_\_\_\_\_\_ and \_\_\_\_\_\_\_\_\_\_\_\_. And it will be all such sums, so it can be written in summation notation as

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

But also = \_\_\_\_\_\_\*\_\_\_\_\_\_\_. So we have

This result can be used as another proof that and are multiplicative. You use and . Show they are first multiplicative. Also recall the summation formulae for and .

**is multiplicative**

Let \_\_\_\_. If either is one show

If either or is zero show

Assume neither nor is zero and neither nor is 1.

\_\_\_\_\_\_\_\_\_\_\_\_, \_\_\_\_\_\_\_\_\_\_\_\_ and no prime is in both products.

Show .

**.**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

is \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ by earlier result.

Result follows.

**Let then (MOBIUS INVERSION FORMULA)**

is true because if runs over all the divisors of , so does .

Sure enough if does divide ? And if does d divide ?

(use the def’n of and dummy variable )

= (you can move the inside the summation)

Turns out that and is equivalent to the same pair of statements with and reversed. By symmetry we will show only one direction. From the two statements is it clear that ? Why?

From the two statements is it clear that ? Why?

= (using the previous paragraph rewrite what the summations are over)

= (factor out

= (what is unless \_\_\_\_ = 1, in which case it is 1, so we can replace the with \_\_\_\_\_\_)

=

=

**If is multiplicative so is**

Let \_\_\_\_.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_(use MIV)

= \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_(recall the divisors of are of the form where \_\_\_\_ divides \_\_\_\_ and \_\_\_\_ divides \_\_\_\_ and .

So \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_(use the fact that and are \_\_\_\_\_\_\_\_\_\_).

Now what is ?

If we multiply out these sums, the terms will be of the form \_\_\_\_\_\_\_\_\_\_\_\_\_ where \_\_\_\_\_\_\_\_\_\_\_\_ and \_\_\_\_\_\_\_\_\_\_\_\_. And it will be all such sums, so it can be written in summation notation as

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

But also is \_\_\_\_\_\_\*\_\_\_\_\_\_, so we are done.

**.**

How many positive integers are there not exceeding ?

How many are NOT relative prime with ?

Subtracting gives the result!

**iff and**

Let , we know we can write 1 as a linear combination as follows.

From this we can write 1 as a linear combination of and as well as and

Suppose , we know we can write as a linear combination as follows.

From this we can write as a linear combination of and as well as and

(in both directions we are recalling what theorem?)

**The Euler Phi-Function is multiplicative.**

Let .

We must show .

Arrange into columns and rows naturally (also explicitly listing the th column)

What about and ? (hint Euclidean Algorithm Lemma we did)

So entry is relatively prime to iff \_\_\_\_ is relatively prime to .

So how many columns have entries that are relatively prime to ?

In those columns how many entries are are relatively prime to ?

Look at the th column.

Show no two are congruent modulo .

How many entries in the th column?

So all entries in the th column modulo are

How many of these are relatively prime with ?

So \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\*\_\_\_\_\_\_\_\_\_\_\_\_\_(how many columns that have all entries relatively prime with )(how many in each column that are relatively prime with ).

**Let , then \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.**

Proof is very straightforward using 2 earlier results.

**Euler’s Theorem:**

Let be positive integers less than that are relatively prime with .

(what is the last subscript?)

Multiply each entry by .

Show that in the list above that all distinct modulo .

Show that each entry in the multiplied by list is relatively prime with .

The list has \_\_\_\_\_\_\_ elements all distinct modulo and relatively prime with , but there are \_\_\_\_\_\_ such elements. So what about the two lists? (the before multiplied by list and the after multiplied by list?

Write out each list multiplied out is congruent modulo .

Divide each side by all the ’s, which is OK because \_\_\_\_\_.

That should give the result!

**The sum of the numbers less than , relatively prime to is**

Trick is to notice . Show this by showing ANY common divisor of and is a common divisor of and and vice versa. (If both list of common divisors are the same, then the GREATEST will be also)

Write out the sum of such numbers twice and use trick.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**.**

Proof:

Look at . What are the possibilities for ?

So since is only 1 number, each of these numbers will be in exactly one of the following sets: Let . .

Show that iff . (L to R done before)

R to L (really NOT L to NOT R)

Suppose , since we are talking about and we must have dividing \_\_\_\_ and \_\_\_\_.

So if then And so \_\_\_\_\_ and \_\_\_\_\_\_.

Use the last to write a linear combination.

Because of what divides, it must also divide \_\_\_. So \_\_\_\_\_\_\_\_\_\_, with \_\_\_\_>1.

So now \_\_\_\_\_ and \_\_\_\_\_\_. And \_\_\_\_\_\_ and \_\_\_\_\_\_\_. So \_\_\_\_\_>1 divides them both a contradiction.

Back to . How many elements? It is the number of positive integers not exceeding \_\_\_\_\_ that have \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. Divide each number in this set by . This set will have the same number of elements. This set will consist of numbers of the form \_\_\_\_\_not exceeding \_\_\_\_\_ that have \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. Could there be other numbers not of this form, say for example, , less than \_\_\_\_\_ that are relatively prime with \_\_\_\_ in this set? Suppose Then \_\_\_\_, because from above if it is NOT \_\_\_ then \_\_\_\_\_\_\_\_\_\_\_ is not 1. So and and so is of the form \_\_\_\_ so the answer to the question is \_\_\_\_.

How many numbers not exceeding are relatively prime with ?

How many numbers in the set ?

How many positive integers are there not exceeding ?

Each is in exactly one of the ’s, from that we get

But as iff since .

So you can replace with \_\_\_\_ and get the result.

**.**

Proof, easy. Use previous result + MIV!

**Suppose the order of modulo is . Then iff**

(R to L) Suppose . Then \_\_\_\_\_\_\_\_\_. The result should come soon!

(L to R) Use the DA with and , noting that if one is bigger then it must be \_\_\_\_.

, but So So since is the least positive such integer, . The result should be apparent.

**Suppose the order of modulo is . iff**

(L to R) Wlog take . Take and cancel out from both sides which is OK becase……

Result should follow from last result.

(R to L)  means \_\_\_\_\_\_\_\_\_\_\_\_\_so .

**are all distinct mod where is the order of mod**

Suppose two are congruent, the last result should give a contradiction.

**The order of modulo is where is the order of mod .**

Let So \_\_\_\_\_ and \_\_\_\_\_\_ and ( , ) = 1.

Show .

An earlier result tells us that \_\_\_\_\_ divides \_\_\_\_\_.(\*\*\*)

Let be the order of modulo . From above \_\_\_\_ divides \_\_\_\_\_\_.

is congruent to \_\_\_\_ modulo . So \_\_\_\_ divides \_\_\_\_\_\_. From this should be able to get the reverse of \*\*\*. So \_\_\_\_\_\_ = \_\_\_\_\_\_\_. So , the order of modulo = \_\_\_\_\_\_.

Note an immediate result is that if is a primitive root modulo then so is provided .

**If a primitive root modulo then the powers (1 through of are congruent to the numbers less than that are relatively prime with .**

so \_\_\_\_\_.

So each is congruent to one of the numbers less than that are relatively prime with .

Each of the ’s are \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ by a previous result.

**If has any primitive roots then it has**

Let be a primitive root. From the last result any primitive root must be in the list

because any primitive root must be relatively prime with .

If any of those in the list are primitive roots then the power must be relatively prime with \_\_\_\_\_ and there are \_\_\_\_\_\_\_\_ of them.

**LaGrange’s Theorem**

For degree , we must show \_\_\_\_\_\_\_\_\_\_\_\_\_ has at most \_\_\_\_ solution modulo .

Since \_\_\_\_\_\_\_\_\_\_\_\_ from an earlier result we have a unique solution, so the theorem is true for degree .

Now let’s assume the theorem holds for degree , that is

Now let’s consider where the degree of is \_\_\_\_.

If there are no solutions, we are done!

So assume there is a solution, ., that is \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

If we divide into there will be some quotient, , and some remainder, , and the remainder will be degree 0 (i.e., a number), and the degree of will be \_\_\_\_\_\_.

So we can write \_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_+\_\_\_\_\_\_.

From this we can find out that \_\_\_\_\_\_\_\_\_\_\_\_\_

So we can improve from 2 lines above to get \_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_.

Suppose is a different (than ) solution to .

Use 2 lines above to get \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Because is not congruent to \_\_\_\_\_ mod , we can divide both sides by it giving

So any solution to different than \_\_\_\_ must satisfy \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

By induction assumption the last blank has at most \_\_\_\_\_\_ solutions.

So has at most \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ solutions.

**If , has exactly solutions.**

implies (if you need a letter not used yet, use )

Consider .

has at \_\_\_\_\_\_\_\_ \_\_\_\_\_ solutions.

What happens if you multiply by Write the biggest exponent without using or .

By \_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_ is always true as long as \_\_\_\_\_\_\_\_, so that means it has exactly \_\_\_\_\_\_\_\_\_\_\_\_\_ solutions.

Consider .

has at \_\_\_\_\_\_\_ \_\_\_\_\_ solutions.

has exactly \_\_\_\_\_\_ solutions, see few lines up. Since has at \_\_\_\_\_\_ \_\_\_ solutions, must have at \_\_\_\_\_\_\_\_\_\_ \_\_\_solutions. Using this and two lines above we get has \_\_\_\_\_\_\_\_\_\_\_ \_\_\_ solutions.

**If then there are exactly incongruent integers having order modulo**

Before the proof, note that an immediate result of this is that primes have primitive roots! (recall a primitive root modulo would have order \_\_\_\_\_\_\_\_, and that divides , in fact there are \_\_\_\_\_\_\_\_ primitive roots!

Let and denote how many integers between 1 and , inclusive, that have order .

The only possible orders are divisors of \_\_\_\_\_\_\_\_, so \_\_\_\_\_\_\_\_\_.

We also know that \_\_\_\_\_\_\_\_\_.

So what about these two sums?

If we could show for each divisor of , then what about and ?

If then is true, so assume So there is an integer, say , of order \_\_\_\_.

What about the powers of from 1 to ? (earlier result)

Show they all satisfy .

has \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ solutions. So is it possible to have another solution to besides the powers of from 1 to ?

How many of these powers will have order ? Note \_\_\_\_\_ of them have a greater order. And from a previous result the power would have to be \_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_ with , and there are \_\_\_\_\_\_\_ of those.

So in this case = \_\_\_\_\_\_, and again is true.

**etc, do NOT have primitive roots**

First we wish to show for and odd. It is done by induction.

Show this is true for the base case, .

Assume that it holds for , we wish to show it holds for \_\_\_\_\_\_\_\_\_\_\_\_, namely that \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

is equivalent to the equation \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ for some .

Squaring both sides of last equation gives \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

From this we see that

Now with this done we note that the integers relatively prime with are the \_\_\_\_\_ integers, and that \_\_\_\_\_\_ and (power of 2) and so and so there are no primitive roots.

**Let with both greater than 2, then has no primitive roots.**

We need to know that the LCM of two numbers times the GCD of the two numbers = the product of the two numbers. This can be proven by prime factorization of each:

The candidates for primitive roots of are those positive integers, , less than \_\_\_\_\_ such that \_\_\_\_\_\_\_ = 1.

If then what about and ?

Let be the LCM of and and be the GCD of those two.

Both and are what kind of numbers? (so is at least \_\_\_\_)

Using the LCD, GCD result we know \_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_(replace with blank in last line).

Euler’s Theorem says \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_(use )

Raise both sides of last line to the power to get \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

Similarly we can get \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ switch the and .

So and why is ?

So every possible candidate for a primitive root modulo has order at most \_\_\_\_\_\_\_ so they are all eliminated from being primitive roots.

This result says that any number that is divisible by two odd numbers cannot have primitive roots as well as any number of the form , and an odd prime. All that is left to check to see if they have primitive roots are numbers of the form powers of odd primes and twice powers of odd primes. (by the way both types always have primitive roots)

**If is an odd prime, the there is a primitive root of such that is not congruent to 1 modulo .**

We know that has a \_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_, call it . If is not congruent to to 1 modulo , we are done. If it is(!!), then look at . Clearly since they are equal mod , \_\_\_\_\_\_ is also a \_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_ modulo \_\_\_.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_(mod (use the binomial theorem, but you only need to worry about the first \_\_\_ terms as the rest all have at least a .

Now \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_(mod (use the assumption (!!) and simplify)

Since there is no common divisor with and , so is not 0 modulo and the result should follow.

Notice that a primitive root modulo implies either or or both are primitive roots modulo . This is true because, the order of modulo is the first exponent that gives \_\_\_ modulo But that also means that \_\_\_ modulo . So is a multiple of

Since \_\_\_\_\_\_\_\_ and we know has order \_\_\_\_\_\_\_\_ or \_\_\_\_\_\_\_\_ modulo (recall it’s a primitive root modulo and the proof says that either \_\_\_\_\_\_\_ or \_\_\_\_\_\_\_\_\_ doesn’t have order \_\_\_\_\_\_.

**Let be an odd prime with primitive root that has the property is not congruent to 1 modulo , then is not congruent to 1 modulo , for**

Proof is by induction. Show the first step, namely

Assume true for some , we must show it is true for \_\_\_\_\_\_\_, namely

What is ?

So (see last question)(modulo (hint by Euler’s Theorem)

So there is some such that \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ where is not a multiple of because why?

Raise both sides of last equation to the power to get

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_( (hint in last blank only need first two terms of binomial expansion)

Result should follow.

**Powers of odd primes have primitive roots.**

Choose a primitive root of that has the property in the last result. Let order of modulo , it must divide \_\_\_\_\_\_\_\_\_\_\_. also implies . So is a multiple of \_\_\_\_\_\_\_.

So must be of the form \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ where . Assume , i.e., is not a primitive root, then would be a multiple of \_\_\_\_, and hence to that power would be \_\_\_\_ modulo . So , i.e., is a primitive root.

**Two times powers of odd primes have primitive roots.**

Choose to be an odd primitive root of , note if is even, simply replace it with

and order of modulo must divide \_\_\_\_\_\_\_\_ = \_\_\_\_\_\_\_\_\_\_\_.(leave all ’s)

implies so is a multiple of \_\_\_\_\_.

From this we see that , and that we have the desired primitive root.

Solving , not 0 modulo . Or in general not , but

Explaining why really only care about , i.e. is a quadratic residue modulo

Show that turns into if , and

(hint you can divide by since we are really taking

**Euler’s Criterion**

Suppose is a quadratic residue, then \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ has a solution, say .

Explain why .

Now \_\_\_\_\_\_\_\_\_\_\_(get in there) \_\_\_\_\_\_\_\_\_\_\_\_(simplify exponets) \_\_\_ (by what theorem?)

Now assume . Let be a primitive root of . (what result are we using here?, is it a big or small result?).

So the powers of will take on all values of modulo , otherwise would \_\_\_\_ be a primitive root of .

So one of those powers, say, , will be . Written out as \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

Find out what is congruent to modulo

From an earlier result the order of , namely \_\_\_\_\_\_\_\_\_(recall it is a primitive root), must divide into , this implies \_\_\_\_\_ is an integer and \_\_\_\_\_ is even, say .

Now find out what is congruent to modulo .

This should show that is a quadratic residue, namely of \_\_\_\_\_ modulo .

Note that because , with odd, you can factor the LHS to get

So either is congruent to \_\_\_\_(namely when \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_) or \_\_\_\_\_(namely when \_\_\_\_\_\_\_\_\_\_\_\_\_)

**Let and be relatively prime to , and odd prime.**

**If then .**

**.**

**.**

**.**

**.**

**.**

All proofs should be quick with possible exception of . Use the rule just prior to it to show

The only possibilities for each side are \_\_\_\_\_ and \_\_\_\_\_\_ if , then one side would be \_\_\_\_ and the other \_\_\_\_ modulo , but they are congruent, that means would have to be \_\_\_, a contradiction.

**Gauss’s Lemma**

Write out the multiples of from 1 to .

Can it be the case that any of these are congruent to each other or 0?

Is it possible to have a remainder of when dividing by ?

Let be the remainders less than , and be the remainders \_\_\_\_\_\_\_\_ than .

Calculate \_\_\_\_\_\_\_.

, are all less than \_\_\_\_.

We wish to show they are all distinct. If any of the ’s or ’s were equal that would violate what was just show above, namely \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

What if there was case where ? Then there would be a couple of multiples of , say and from \_\_ to \_\_\_\_ such that and \_\_\_\_\_\_\_\_. Note that \_\_\_\_\_\_\_\_\_\_\_.

We have \_\_\_\_\_\_\_\_\_\_(use last line) \_\_\_\_\_\_ ()(use 2 lines above), and since \_\_\_\_\_ we can divide by , to get that \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, namely \_\_\_\_\_\_\_\_\_ is a multiple of \_\_\_, which is not possible.

How many numbers in the list , ? (recall they are all distinct mod )

How many numbers in the list ? (which are distinct also)

So what about those last two lists?

What is the product of the numbers in the second list?

Which is congruent modulo to \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (use the first list)

So \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_(mod )

What about modulo the lists and the list of the multiples of from 1 to written at the start of the proof.

So now replacing, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_(mod )

Canceling out , which is OK since it is \_\_\_\_\_\_\_\_ \_\_\_\_\_\_ with gives \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

Multiplying both sides by and recalling Euler’s Criterion should give the result.

Now we can tell when 2 is a quadratic residue or not modulo an odd prime!

**.**

Write out the multiples of 2 up to .

We want to see how many have remainder greater than \_\_\_\_\_ when divided by \_\_\_ (Guass’s Lemma)

They are all less than \_\_\_, so we only have to count how many in the list are greater than \_\_\_\_\_.

We will do this by counting the total – ones NOT greater than \_\_\_\_\_.

Note that is the same as \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_(divide by 2), so the number of multiples is , the greatest integer less than or equal to .

Let how many of the multiples of 2 are greater than \_\_\_\_\_.

\_\_\_\_\_\_\_\_\_(total multiples of 2) - \_\_\_\_\_\_\_\_\_\_(how many multiples less than \_\_\_)

Calculate for each case , , ,, actually only worry about if is even or odd. The result follows from Gauss’s Lemma.

**Another Lemma needed to prove the law of quadratic reciprocity, namely that for odd and an odd prime.**

Just like in Guass’s Lemma write out the multiples of from 1 to .

For each above divide by use the DIV ALG to write \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_(\*) (use ’s for the quotients and ’s for the remainders and note that \_\_\_\_\_ \_\_\_\_\_.

Dividing both sides of the equation(\*) by we get \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

From this we see that \_\_\_\_\_\_\_\_\_\_\_\_ and subbing this into (\*) we get \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_(\*\*).

Just like in the proof of Gauss’s Lemma, if it is one of the ’s and otherwise it is one of the ’s.

Summing up all the (\*\*) equations we get

In the proof of Gauss’s Lemma we found out that , are just what integers in some order?

So

Subtracting the two giant sum formulas gives (hint on first you can factor out the on the LHS)

Rewrite this last line as equivalent modulo 2!

And solve this for

From Gauss’s Lemma \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

**Law of Quadratic Reciprocity**

For this proof we need the picture at the top of page 187 for reference.

We wish to count the total number of dots strictly inside the rectangle in two different ways.

Since we are talking about odd primes count the total number of points by multiplying the vertical and horizontal, to get

Find the equation of their diagonal line.

Multiply both sides by to get

If a dot was on this line, then would have to divide \_\_\_\_\_\_ and since it doesn’t divide \_\_\_\_ (since the primes are distinct), would have to divide \_\_. Since the rectangle’s base is from 0 to , none of the \_\_\_\_’s can be a multiple of . So there are \_\_\_\_\_ dots on this diagonal line inside the rectangle.

So the total number of dots = dots in the upper left + dots in the lower right!

Consider the vertical line in the picture. What is the -coordinate where this vertical line hits the diagonal line?

The number of dots along this vertical line strictly inside the lower right triangle is \_\_\_\_\_\_\_\_\_ (hint use greatest integer function).

If we sum this over all vertical lines from to , we get the total number of dots in the lower right triangle to be

If we were to reverse the roles of and we can get the total number of dots in the upper left triangle to be(switch with \_\_\_\_, with \_\_\_\_, and with )

So the total number of dots strictly inside the rectangle has been counted two ways, we can write down an equation (LHS earlier count = RHS sum of the two sums we just got)

Bringing out the big gun of Guass’s Lemma twice we get

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ = \_\_\_\_\_\_\_\_\_\_\_\_\_\_.

**How many perfect -shuffles to bring a deck of cards back to its original configuration?**

Let’s number the card positions in the deck starting at 0. That way a card in position has \_\_\_\_ cards on top of it?

Arrange the cards into piles as follows the first pile cards 0 to \_\_\_\_, etc. Make sure to include the -th row and the -th column.

The new arrangement of the deck is determined by taking the top cards in order, then the second cards in order, etc.

Consider a card in position . After a shuffle to goes to position \_\_\_\_\_\_(complete rows) + \_\_\_\_\_\_\_(first cards in the incomplete row). So goes to \_\_\_\_\_\_\_.

What is \_\_\_\_\_\_(modulo ). So in other words, modulo card goes to \_\_\_\_\_.

How long does it take card 1 to get back to its original position? The order of \_\_\_\_ modulo \_\_\_.

Show card returns after that many shuffles. (it may return sooner also, but we don’t care)

What about decks, such as

0,1,0,1,… (2-moded out deck)

0,1,2,0,1,2,… (3-moded out deck)

In general (-moded out deck)

Theorem due to Packard says the following.

If fails to divide , then it is the order of modulo .

If does divide , then it is the order of modulo .