### 2.3 Linear Diophantine Equations

* **Definition**
  + A Linear Diophantine Equation is an equation in one or more unknowns with integer coefficients, for which integer solutions are sought (i.e. for integers and , when are given integers)
* **Linear Diophantine Equation Theorem**
  + The linear Diophantine equation has a solution if and only if
* **Proposition**
  + If , and is one particular solution, then the complete integer solution is for all .
* **Tip: Steps for solving**
  + Step 1: Find
  + Step 2: See if ; if true, continue. If false, stop and state that the LDE has no solution
  + Step 3: Use solution found in Extended Euclidean Algorithm (or use Back-Substitution) to find a particular solution to
  + Step 4: Multiply equation by to get a particular solution to
  + Step 5: Use for all to express the general form for all solutions to
  + Step 6: Apply Constraints (e.g. non-negativity) to general solution if necessary
* **Example**
  + Find all non-negative integer solutions to
  + Step 1:

|  |  |  |  |
| --- | --- | --- | --- |
| **x** | **y** | **R** | **q** |
| 1 | 0 | 38 | - |
| 0 | 1 | 34 | - |
| 1 | -1 | 4 | 1 |
| -8 | 9 | 2 | 8 |
| 17 | -19 | 0 | 2 |

* + Step 2: Check that ; LDE has a solution
  + Step 3:
  + Step 4:
  + Step 5:
  + Step 6:
* **Example**
  + Find all non-negative integer solutions to
  + Substitute to simplify the problem
  + Step 1:

|  |  |  |  |
| --- | --- | --- | --- |
| **x** | **y** | **r** | **q** |
| 1 | 0 | 14 | - |
| 0 | 1 | 9 | - |
| 1 | -1 | 5 | 1 |
| -1 | 2 | 4 | 1 |
| 2 | -3 | 1 | 1 |
| -9 | 14 | 0 | 4 |

* + Step 2: Check that ; LDE has a solution
  + Step 3:
  + Step 4:
  + Step 5: Remember to substitute back into the equation
  + Step 6:
* **Example**
  + A trucking company has to move 844 refrigerators. It has two types of trucks it can use; one carries 28 refrigerators and the other 34 refrigerators. If it only sends out full trucks and all the trucks return empty, list the possible ways of moving all the refrigerators.
  + Equivalent problem: Find all non-negative solutions to

### Prime Numbers

* **Definitions**
  + A decimal system is a set of numbers that are written in terms of powers of 10.
  + An integer is called a prime if its only positive divisors are and ; otherwise it’s called composite.
  + The least common multiple of two positive integers a and b is the smallest positive integer that is divisible by both a and b. It will be denoted by .
* **Proposition 2.51:**
  + Every integer larger than 1 can be expressed as a product of primes.
* **Euclid Theorem 2.52**
  + The number of primes is infinite.
* **Theorem 2.53** 
  + If is a prime and , then or .
* **Unique Factorization Theorem 2.54**
  + Every integer, greater than 1, can be expressed as a product of primes and, apart from the order of the factors, this expression is unique.
* **Theorem 2.55**
  + An integer is either prime or contains a prime factor
* **Proposition 2.56** 
  + If is the prime factorization of *a* into powers of distinct primes , then the positive divisors of are those integers of the form where for
* **Theorem 2.57** 
  + If and are prime factorizations of the integers *a* and *b*, where some of the exponents may be zero, then where for.
* **Theorem 2.58** 
  + If and are prime factorizations of the integers *a* and *b*, where some of the exponents may be zero, then where for .
* **Theorem 2.59**
  + For any positive integers and ,
* **Tip**
  + When trying to find the prime factorization of a number, calculate the square root of the number in question. No prime factor will exceed the square root of a number.
* **Example**
  + Factor into prime factors and calculate the greatest common divisor and least common multiple or the two numbers. Note that
  + Solution:
* **Example**
  + Prove that the sum of two consecutive odd primes has at least three prime divisors
  + Solution: Let and be consecutive odd primes where . Note that is an even number, and, therefore, has a prime factor of Hence is an integer and . As and are consecutive odd primes, then is either even, or an odd composite number. Therefore, has at least 2 prime factors. Therefore has at least 3 prime factors (2 and the 2 prime factors from k).
* **Example**
  + Prove that
  + Solution: Let , , . Using Proposition 2.57, , where for. Using this definition, and Proposition 2.58 for expressing the lowest common multiple, we can express the exponents of the prime factors of both expressions:

Hence this problem is equivalent to verifying the following statement for all cases of . Notice that and are interchangeable in the expression (e.g. proving for is the same as proving for ).

* + Case 1:
  + Case 2:
  + Case 3:
* **Example**
  + Let , where is a positive integer and and are odd primes. Prove that if and , then or .
  + Solution: Note that . Since , . Hence or , and, since and is an odd prime, can only equal or .

### 3.1 Congruence

* **Definition**
  + Let m be a fixed positive integer. If , we say that “a is congruent tob modulo m” and write whenever . If , we write .
* **Tip**
  + Consider when is divided by using the Division Algorithm, is congruent to the remainder modulo
* **Proposition 3.11:** Let

1. If , then
2. If and , then .

* **Proposition 3.12:** If and , then
* **Proposition 3.13** 
  + if and only if and have the same remainders when divided by .
* **Example**
  + What is the remainder when is divided by 7
  + Rephrased: Solve for in the congruency , where
  + Solution: and . Hence

### 3.2 Tests for Divisibility

* **Theorem 3.21**
  + A number is divisible by 9 if and only if the sum of its digits is divisible by 9.
* **Theorem 3.22**
  + A number is divisible by 3 if and only if the sum of its digits is divisible by 3.
* **Proposition 3.23**
  + A number is divisible by 11 if and only if the alternating sum of its digits is divisible by 11.
* **Example**
  + Determine whether is divisible by
  + Solution:
    - Clearly, is not divisible by (as it does not end in a ) or 5 (as it does end in a or ).
    - As is even, is divisible by .
    - Dividing by gives us , which is even. Hence is divisible by 4. We can also see this by noting that , the number defined by the last two digits of is divisible by .
    - Dividing by gives us , which is odd. Hence is not divisible by .
    - The sum of the digits in is equal to , which is divisible by . Hence is divisible by .
    - a is divisible by 2 and 3 and is, therefore, divisible by 6.
    - The sum of the digits in is equal to , which is not divisible by . Hence is not divisible by .
    - The alternating sum of the digits in is equal to , which is divisible by . Hence is divisible by .

Therefore, is divisible by

### 3.4 Modular Arithmetic

* **Definitions**
  + The congruence class modulo m of the integer a is the set integers
  + The set of congruence classes of integers, under the congruence relation modulo m is called the set of integers modulo m and is denoted by
  + Modular arithmetic is given by addition and multiplication, and are well defined in
* **Fermat’s Little Theorem 3.42**
  + If p is a prime number that doesn’t divide the integer a, then
* **Corollary 3.43**
  + For any integer a and prime p,
* **Example**
  + What is the remainder when is divided by 7?
  + Rephrased: Solve for in the congruency , where . Use Fermat’s Little Theorem since .
  + Solution:
* **Example**
  + Prove that for all integers .
  + Step 1: Prove that
  + Step 2: Prove that

### 3.5 Linear Congruences

* **Definition**
  + A relation of the form is called a linear congruence in the variable x.
* **Linear Congruence Theorem 3.54**
  + The one-variable linear congruence has a solution if and only if .
  + If xo Z is one solution, then the complete solution is where .Hence there are noncongruent solutions modulo .
* **Example**
  + Solve the congruence
  + Equivalent Problem: Find integer solutions to the linear Diophantine equation
  + Step 1

|  |  |  |  |
| --- | --- | --- | --- |
| **x** | **y** | **r** | **Q** |
| 1 | 0 | 1426 | - |
| 0 | 1 | 805 | - |
| 1 | -1 | 621 | 1 |
| -1 | 2 | 184 | 1 |
| 4 | -7 | 69 | 3 |
| -9 | 16 | 46 | 2 |
| 13 | -23 | 23 | 1 |
| -35 | 62 | 0 | 2 |

* + Step 2: ; no solution
* **Example**
  + Determine the number of congruence classes in that are solutions to the equation
  + Solution: This equation is equivalent to the congruence Since and does not divide into , there are no solutions to this congruence and hence there are no solutions to the equation above in .
* **Example**
  + Find the inverse of in
  + Equivalent Problem: Solve or find integer solutions to
  + Step 1

|  |  |  |  |
| --- | --- | --- | --- |
| **y** | **x** | **r** | **Q** |
| 1 | 0 | 41 | - |
| 0 | 1 | 2 | - |
| 1 | -20 | 1 | 20 |
| -2 | 41 | 0 | 2 |

* + Step 2: ; LDE has a solution
  + Step 3:
  + As , [21] is the inverse of [2] in
* **Example**
  + Solve

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|  | 0 | 1 | 4 | 1 | 0 | 1 | 4 | 1 |
|  | 0 | 2 | 4 | 6 | 0 | 2 | 4 | 6 |
|  | 0 | 3 | 0 | 7 | 0 | 3 | 0 | 7 |

### 3.6 The Chinese Remainder Theorem

* **Chinese Remainder Theorem 3.62**
  + If , then for any choice of the integers and, the simultaneous congruences

have a solution. Moreover, if is one integer solution, then the complete solution is

* **Generalized Chinese Remainder Theorem 3.66**
  + Let be positive integers such that if . Then for any integers the simultaneous congruences

always have a solution. Moreover, if is one solution, then the complete solution is .

* **Example**
  + Solve the simultaneous congruences
  + Solution: First check that each individual congruence has a solution: and .

Check that . If this is true, then this set of simultaneous congruences has a solution. First of all, we can reduce the first congruence to . This further reduces to . Another way of stating this is that for some .

Recall that we can solve a linear congruence by modeling it as a linear Diophantine equation. For example, solving will give us a solution to the second congruence. Using the Extended Euclidean Algorithm, I get a particular solution of . Therefore, .

We now substitute the result from the first congruence into the second:

Solving for , we get . We can rewrite this as , for some . Plugging this back in to the original equation for

* **Example**
  + A basket contains a number of eggs and, when the eggs are removed at a time, there are respectively, left over. When the eggs are removed at a time, there are none left over. Assuming none of the eggs broke during the preceding operations, determine the minimum number of eggs there were in the basket.
  + Set up: The question is providing us with a set of simultaneous congruences, the solution of which is also a congruence. We then must determine the smallest positive integer solution to that final congruence. Taking the information from the question:

We see that are all not equal to . Therefore, we must get eliminate some congruences for this to work. Note that whenever (iii) holds, (i) holds, so we have no need for (i). Similarly, whenever (v) holds, (ii) holds. Finally, we can combine (iii) and (v) by inspection, as which is quite small. If (iii) is true, , and if (v) is true, . Overall is the only overlap. Using all these observations, we can rewrite (i)-(vi) as the following:

We can now solve this set of simultaneous congruences using the Chinese Remainder Theorem as we normally would. The end solution is 119 eggs.

Trick: This particular problem has an elegant trick that makes it easy to solve. If we were to add 1 more egg to the basket, the number of eggs would be divisible by 2, 3, 4, 5, 6, and be congruent to 1 modulo 7. In other words, the number of eggs would now be a positive integer divisible by 60 (the smallest positive integer containing 2, 3, 4, 5, and 6 as factors), and congruent to 1 modulo 7. We can quickly come to 120 eggs by inspection, and conclude that there were 119 eggs initially.

### 3.7 Euler-Fermat Theorem

* **Euler-Fermat Theorem 3.71**
  + If is a positive integer and , then , where is the totient of m, the number of positive integers not exceeding m that are co-prime to m

### 7.1 Cryptography

* **Definitions**
  + Cryptography: study of sending message in a secret or hidden form so that only those people authorized to receive the message will be able to read it
  + Plaintext**:** message being sent
  + Ciphertext**:** encrypted message

### 7.2 Private-Key Cryptography

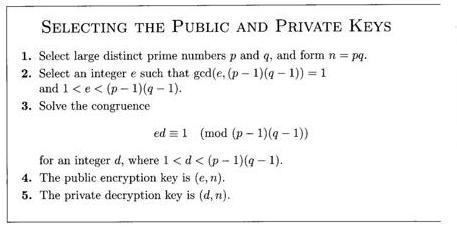
* **Definition**:
* Private-key system: a method for data encryption (and decryption) that requires the parties who communicate to share a common key

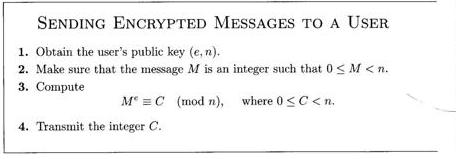
### 7.3 Public-Key Cryptography

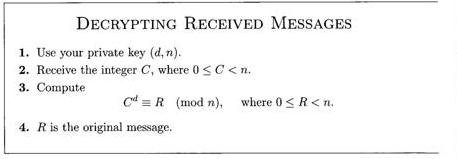
* **Definitions**
  + Public-key cryptosystem: Each user has a pair of cryptographic keys — a public key and a *private* key. The private key is kept secret, whilst the public key may be widely distributed. Messages are encrypted with the recipient's public key and can only be decrypted with the corresponding private key

### 7.4 RSA Scheme

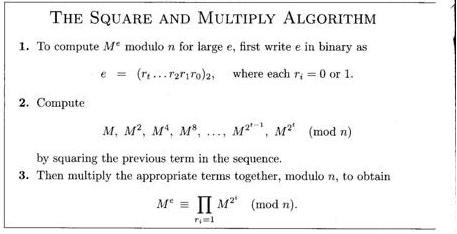
* **RSA Cryptographic Scheme 7.42**







* Reason why RSA works: it is extremely difficult to find the prime factorization of a large (600 digit values used in real life)
* **Square and Multiply Algorithm 7.46**



* **Example**
  + Ron wants to send a message to Hermione after encrypting it using RSA. Hermione’s public key is and her private key is . Using the appropriate key, encrypt the message that Ron wants to send to Hermione.
  + Solution: As we are *encrypting* we must use Hermione’s *public* key. As , is an appropriate message. Encrypting requires us to compute , where .

Using the Square and Multiply Algorithm: As (equivalently, ), can be written as

is the encrypted message.

* **Example**
  + Suppose that and are prime numbers, and Prove that and
  + Solution:
* **Example**
  + Suppose that and . Determine and .
  + Solution: Using statements proved above,

### 8.1 Quadratic Equation

* **Quadratic Formula 8.11**
  + If then the quadratic equation has the solution

### 8.2 Complex Numbers

* **Definition**:
  + Complex number: an expression of the form , where The set of all complex numbers is denoted by
* **Addition and Multiplication of Complex Numbers 8.21**
* **Proposition 8.23**
* **Proposition 8.25**
  + - Let and let and , where .

1. if and only if and ;
2. (associativity of addition)
3. (commutativity of addition)
4. The number is such that (existence of a zero)
5. The number is such that (existence of negatives)
6. (associativity of multiplication)
7. (commutativity of multiplication)
8. The number is such that (existence of a unit).
9. If the elementis the inverse of z and satisfies(existence of inverses)
10. (distributive law)

### 8.3 The Complex Plane

* **Definitions**:
  + Real axis:The real axis is the line in the complex plane corresponding to zero imaginary part
  + Imaginary axis: The axis in the complex plane corresponding to zero real part
  + Complex plane: A one-to-one correspondence between the complex numbers and the plane
  + Modulus/absolute value: The nonnegative real number Ifthen
  + Complex conjugateof is the complex number a complex number multiplied by its conjugate always results in a real number

### 8.4 Properties of Complex Numbers

* **Proposition 8.42:** If z and w are complex numbers, then

1. is twice the real part of
2. is times the imaginary part of z.

* **Corollary 8.42:** If z is a nonzero complex number, then
* **Proposition 8.44:** If z and w are complex numbers, then

1. (the triangle inequality)

* **Example**
  + Write in standard form.
  + Solution: We can ensure there is a real number in the denominator of the fraction by multiplying by the complex conjugate of :
* **Example**
  + If , prove that
  + Solution: Let and
* **Example**
  + Shade the region of the complex plane for which the following expression is real:
  + Solution: Consider . Note that because it would make the denominator zero. We will attempt to write this expression in standard form, and see what conditions make the expression real:

Here we can take a step back and see that this expression is real when (i.e. when ). We, therefore, see that the shaded region in the complex plane will be the unit circle with an open dot at because .

### 8.5 Polar Representation

* **Definition**:
  + The polar form of a complex number is .
* **Convert from Polar to Cartesian Coordinates 8.51**
  + Conversely, a point whose Cartesian coordinates are (x,y) has the polar coordinates whereandis an angle such that
  + We define *cis(* to be cos + i\*sin
* **Theorem 8.53**
  + If andare two complex numbers in polar form, then
* **Example**
  + Convert the numbers and to polar form and multiply them together
  + Solution: Note that lies on the real axis and lies on the complex axis. The arguments of our complex numbers should show this:

Multiplying them together in polar form gives the following:

Now check: is this consistent with regular multiplication? Does ?

### 8.6 De Moivre’s Theorem

* **Complex exponential function**:
* **De Moivre’s Theorem 8.61**: For any real number
* **Corollary 8.62**: If z=r(cos then, for any integer
* **Example**
  + If , express in standard form.
  + Solution: First convert into polar form, then compute :

### 8.7 Roots of Complex Numbers

* **Theorem 8.72**:If is the polar form of a complex number, then all its complex nth roots are equal to

The modulus is the unique real nonnegative root of

* **Example**
  + Find all the solutions to for
  + Solution: Using the quadratic equation:

Switching to polar form and solving for :

Switching to polar form and solving for :

Therefore, ,

### 8.8 Fundamental Theorem of Algebra

* **Fundamental Theorem of Algebra 8.81**
  + Every equation of the form where has at least one solution in the complex numbers.

### Proofs to be memorized:

* **Euclid’s Theorem 2.52**
  + The number of primes is infinite.
  + Proof by Contradiction: Suppose that there is only a finite number of primes, say . We can find a number that can not be generated by multiplying these primes together. Consider . As , is not a prime. On the other hand, is not divisible by any of the primes ; if , then and , a contradiction.
* **Theorem 2.35**
  + If is a prime and , then or .
  + Proof: Suppose that the prime divides but does not divide . Since the only positive divisors of the prime are and , the only positive common divisor of and is ; hence . It now follows from Proposition 2.28 that . Therefore, either or .
* **Proposition 3.12**
  + If and , then
  + Proof: Since and we can write and where . If follows that

Since , the results follow.

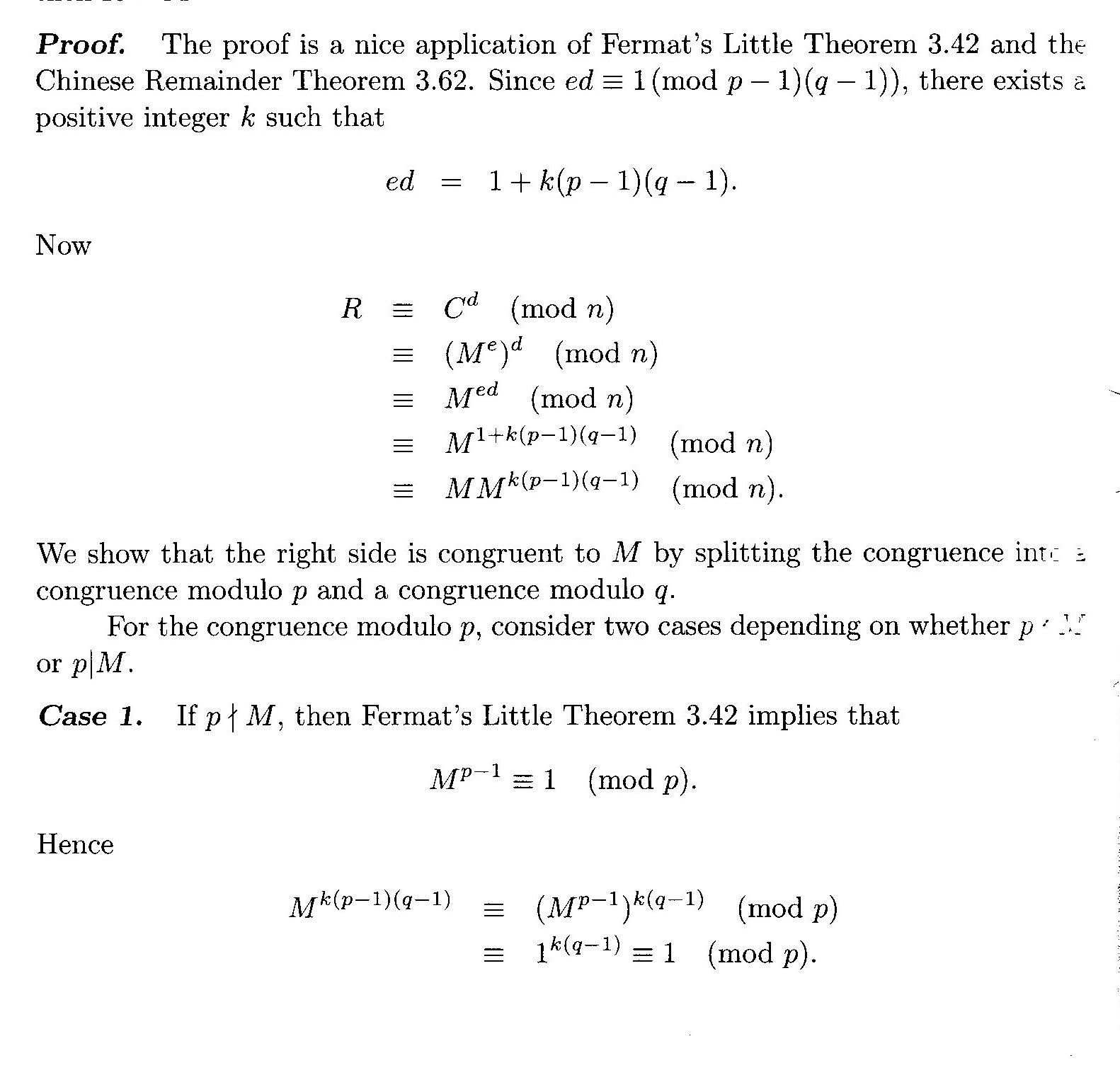
* **Proposition 3.14**
  + if and only if and have the same remainders when divided by .
  + Proof using the division algorithm: and where and . If and have the same remainders when divided by , then and . Conversely, if , then and hence . However, and so
* **Fermat’s Little Theorem 3.42**
  + If is a prime number that does not divide the integer , then
  + Proof:

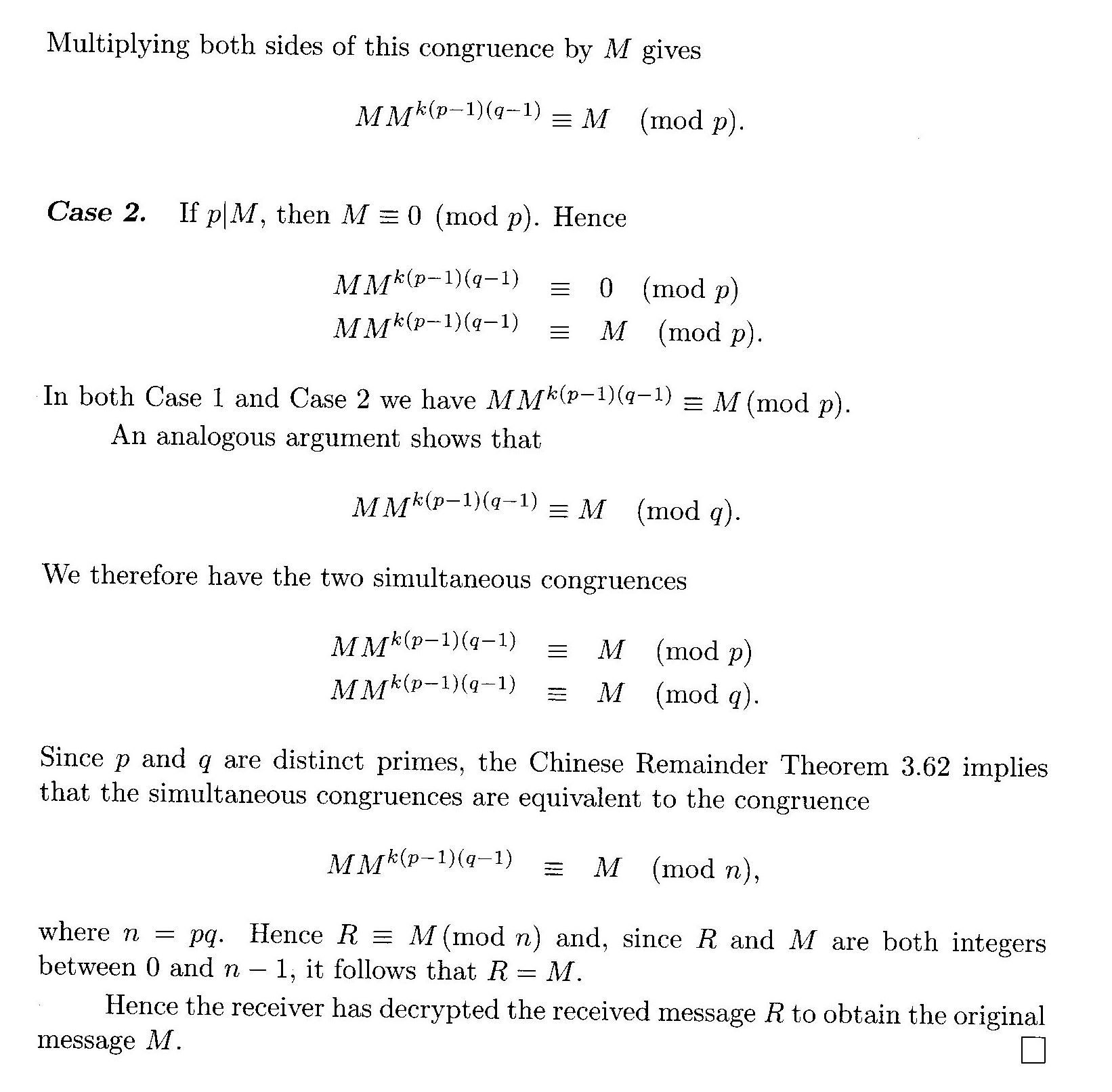
If we shall first show that no two of the numbers are congruent modulo . Suppose that where . By the definition of congruence, this implies and, by Theorem 2.53, . Hence

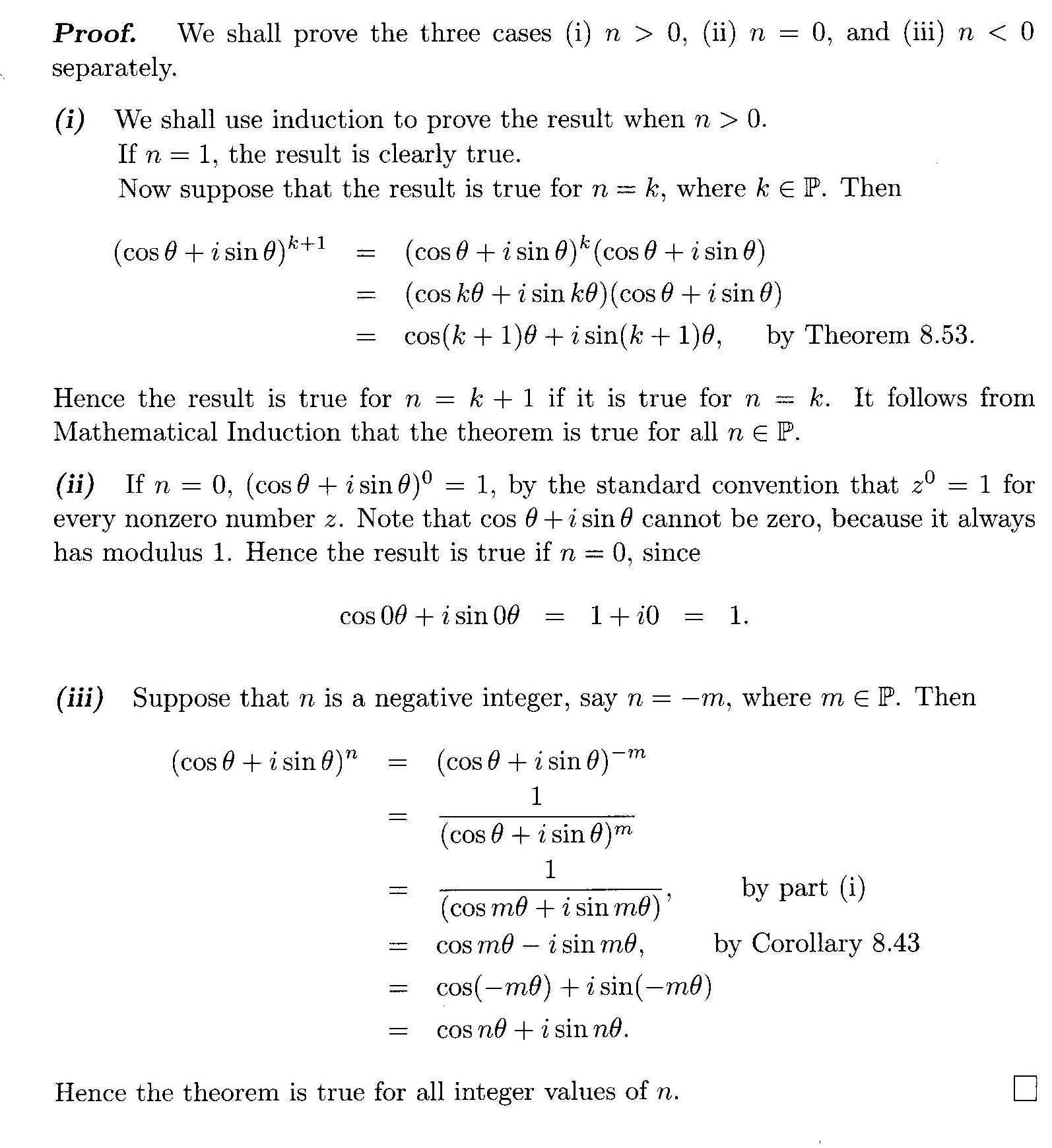
Therefore, the congruence classes are all distinct. But as only contains congruence classes, it follows that }.

Hence the nonzero classes must be a rearrangement of the classes In particular, multiplying them together,

However, because the prime does not divide any of the factors of Hence, by Proposition 3.13, we can cancel and obtain .

* + - Theorem 7.41



* De Moivre’s Theorem 8.61

Materials Covered in Midterm 1&2: Some Examples

* Example 1
  + If are sets, the statement can be expressed as

Express and simplify the negation of this expression, namely , in terms of quantifiers.

* + Solution: Recall that the negation rules for quantifiers always switch the universal quantifier (“for all”) to an existential quantifier (“there exists”). Once we have this in mind, reasoning out the problem becomes easy. What we need to express is that there exists an element of both that is not contained in U.
* Example 2
  + Prove that if is a real number such that , then .
  + Solution: Whenever a conditional statement provides numerical ranges, it is always a good check to see if the contrapositive is easier to prove than the original statement.

Contrapositive: “If is a real number such that then .”

Now this statement becomes much easier to prove.

* Example 3
  + Show that the statement is equivalent to the statement .
  + Solution: This problem is simply a matter of creating a truth table for both statements

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |
| T | T | T | F | F | F | T | F | T |
| T | T | F | F | F | T | T | F | T |
| T | F | T | F | T | F | T | F | T |
| T | F | F | F | T | T | T | F | T |
| F | T | T | T | F | F | T | F | T |
| F | T | F | T | F | T | T | F | T |
| F | F | T | T | T | F | T | T | T |
| F | F | F | T | T | T | F | T | F |

* Example 4
  + Show is not a rational number.
  + Solution: Recall that a rational number can always be expressed as a fraction of 2 integers. Consider two positive integers and such that . Rearranging and squaring both sides of the equation, we get We will now consider the prime factorizations of and . In particular, we count the number of times appears as a factor. As both and are being squared, should appear as a factor in and an even number of times. That means that can be divided into an odd number of times. This discrepancy between and mean that they can not possibly be equal, a contradiction. Therefore, can not be written as a fraction and is not a rational number.
* Example 5
  + What is the maximum number of regions that a plane can be divided into by straight lines?
  + Solution: If we want to maximize the number of regions, no two lines can be parallel and no three lines can intersect at the same point. If we draw one line, the plane will be divided into 2 regions; drawing 2 lines will divide the plane into 4 regions. We continue in this fashion yielding the following table for lines and regions (try drawing the lines and regions)

|  |  |
| --- | --- |
|  |  |
| 1 | 2 |
| 2 | 4 |
| 3 | 7 |
| 4 | 11 |
| 5 | 16 |
| 6 | 22 |
| 7 | 29 |

It appears as though when the line is drawn, the plane is divided into more regions (i.e. the 7th line adds 7 regions). Therefore for a plane with lines, the number of regions .

Base Case (: The plane is divided into 2 regions. We must check if our equation holds.

Induction Hypothesis (: Assume when lines are drawn, .

Induction Conclusion (): Consider adding a line. The number of regions prior to adding the line was equal to . Adding the new line will increase the number of regions by .

* Example 6
  + Find an expression for and prove that your expression is correct.
  + Solution: Similarly to how we approached the previous example, we will make a table evaluating different values of the sum. For ease of comparison, a column with will also be included

|  |  |  |
| --- | --- | --- |
|  |  |  |
| 1 | 1 | 1 |
| 2 | -8 | 4 |
| 3 | 17 | 9 |
| 4 | -32 | 16 |
| 5 | 49 | 25 |
| 6 | -72 | 36 |
| 7 | 97 | 49 |

We can see that there is a relationship between and . Whenever is odd, a closed form for the sum seems to be , and whenever is even, a closed form for the sum seems be . Therefore we will try to prove the following expression for the alternating sum of squares of odd integers

Base Case ():

and

and

Induction Hypothesis (): Assume if is odd and if is even.

Induction Conclusion (): We will split this into both cases for .

Case 1 ( is even, is odd):

by our Induction Hypothesis

Case 2 ( is odd, is even):

by our Induction Hypothesis

Therefore,