Summer HSSP Lecture Notes

Lane Gunderman

July 15, 2014

First Class: proofs and friends

Contents

1 Glossary of symbols **4**

2 Types of numbers **5**
2.1 Breaking it down . . . 5
2.1.1 Number categories . . . 5
2.1.2 Primes . . . 6
2.2 Questions . . . 7

3 Direct Proofs **8**
3.1 Examples . . . 8
3.1.1 Example 1 . . . 8
3.1.2 Example 2 . . . 9
3.2 Questions . . . 9

4 Proof by Counter-example **10**
4.1 Examples . . . 10
4.1.1 Example 1 . . . 10
4.1.2 Example 2 . . . 10
4.2 Questions . . . 11

5 Proof by induction **12**
5.1 A Motivating Example . . . 12
5.2 Sigma Notation . . . 13
5.2.1 Discrete Numbers Only plz . . . 13
5.3 Induction . . . 13
5.3.1 Example 1 . . . 14
5.3.2 Example 2 . . . 15
5.3.3 Possible Notation Help . . . 15
5.3.4 Example 3 . . . 16
5.4 Final Words . . . 16
5.5 Questions . . . 17

6 Proof by contradiction **19**
6.1 Example . . . 19
6.2 Questions . . . 20

7 Proof by pigeon holing **21**
7.1 Examples . . . 21
7.1.1 Example 1 . . . 21
7.1.2 Example 2 . . . 21
7.2 Questions . . . 22

8 Prime numbers visit 2 **23**
8.1 Primes . . . 23
8.2 Prime Factorization . . . 24
8.2.1 Example 1: 420 . . . 25
8.2.2 Example 2: 23 . . . 25
8.3 Mutually Prime Numbers . . . 26
8.3.1 Mutually Prime Number Sets . . . 26
8.4 Division with Remainders . . . 26
8.5 Greatest Common Divisor . . . 27
8.6 Euclidean Algorithm . . . 28
8.6.1 Background . . . 28
8.6.2 Algorithm . . . 30
8.7 Fundamental Theorem of Arithmetic . . . 31
8.7.1 Fundamental Theorem of Arithmetic (FTA) . . . 32
8.8 Questions . . . 33
8.9 Citation . . . 35

Chapter 1

Glossary of symbols

Below is a list of symbols that will be used to varying degrees in this class. We encourage you to feel free to use them, but won't require them. In addition, if some symbol appears that you don't understand, ask immediately for the english meaning– most of the time its just a simple sentence or idea contracted into a single symbol.

$\forall$: for all or for each

$\exists$: there exists

$\in$: is an element of

$\notin$: is not an element of

$\Rightarrow$: implies or leads to

$\subset$: is a subset of

Σ: summation notation (see induction chapter)

Π: similar to Σ except all additions are replaced by multiplications

$\equiv$: congruent to (used in modular operations)

$\rightarrow$: immediate logic flow

$\sharp$: cardinality

Chapter 2

Types of numbers

There are a variety of different ways to categorize numbers, below we set out the principle divisions. Aside from this, a couple of special subsets are pulled out and briefly examined.

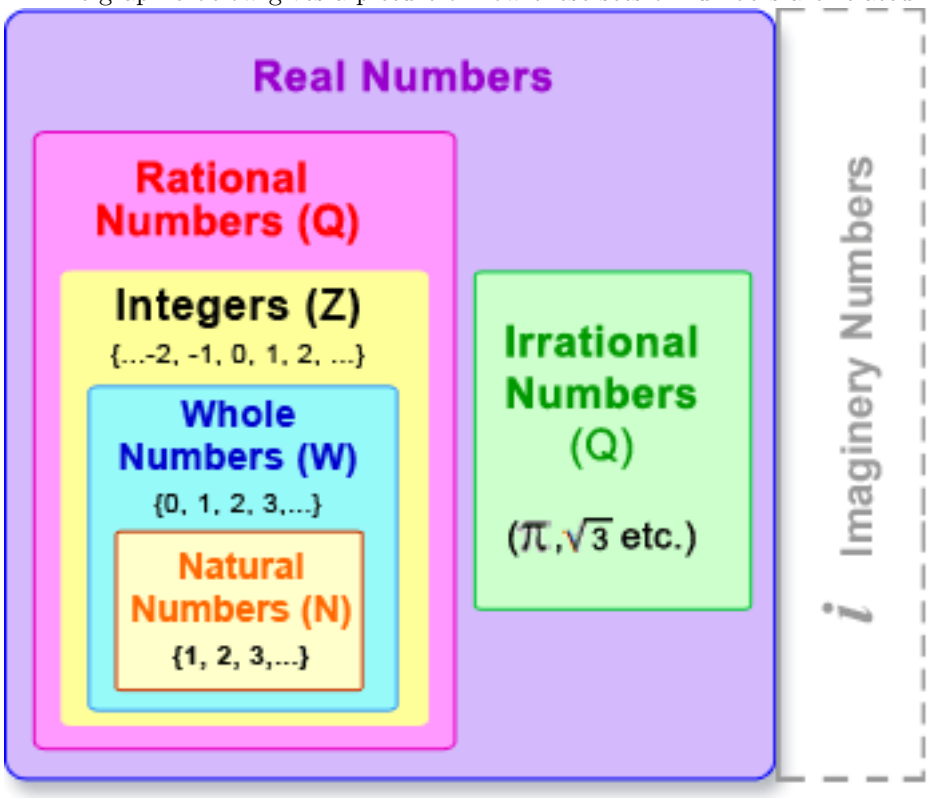
2.1 Breaking it down

All numbers fall into the following simple categorizations:

2.1.1 Number categories

Natural numbers: "Numbers beginning with 1 and 2, where each number is exactly 1 greater than its predecessor."
Whole numbers: "All the natural numbers, and zero"
Integers: "The set of all Whole numbers and their additive inverses"
Rational numbers: "All numbers which can be represented as a ratio $\frac{p}{q}$, where p and q are relatively prime integers"
Real numbers: "All numbers without imaginary components" alternatively: "The set containing all rational and irrational numbers"
Irrational numbers: "All numbers which part are part of the Real numbers but not part of the Rational numbers"

The graphic below gives a picture of how these sets of numbers are related:



2.1.2 Primes

Another often considered categorization of numbers is the set of prime numbers. Primes are the set of natural numbers which have the property that their only two factors are 1 and itself. Please note that 1 is not prime, nor is it composite. Occasionally the additive inverse of primes are also considered primes, however in this course we'll focus on positive primes. If you have not learned about primes, learn this definition well; primes will come up repeatedly!

Relatively Prime Numbers

Two numbers are relatively prime if neither number has a common prime factor with the other, aside from 1. The two numbers are usually both natural numbers.

Don't worry too much about primes at this point, this will be covered more next week and throughout the rest of this course.

2.2 Questions

Categorize the following numbers:
(*)1. $2;\ -1;\ 0;\ \sqrt{2};\ \pi;\ \frac{3}{2}$

(*)2. $\frac{16384}{32};\ 0.\overline{7};\ 11$

(**)3. $\sqrt{2+\sqrt{2+\sqrt{2+\sqrt{2+...}}}}$

(*)4. ∞ (infinity)

Decide which of the following numbers are prime:
(*)5. 2; 5; 8; 0; 51; 1

(**)6. -17; 13689; 52841

(***)7. 89575378759; 852895895231; 3554389342359862463

Decide whether the following pairs of numbers are relatively prime:
(*)8. 2 and 3

(*)9. 21 and 36

(*)10. 216 and 144

(*)11. 121 and 169

(**)12. 40123 and 7433

(**)13. 13 and 13131313131313131313131313...1313131313...131313

Chapter 3

Direct Proofs

Proofs are a way to make a mathematical statement that is without a doubt true. Often times the proof doesn't create a formula or theorem, but rather verify its validity. Here we mention direct proofs. This is the most classical way of proving things.

Directly proving things involves using definitions, postulates, theorems, and other already proven or assumed things, in order to prove that something else is true (either a particular example or a lemma or something of that sort). Those of you who've taken geometry should already be familiar with this method of proving things. Geometry proofs involve using a handful of postulates (assumptions that cannot be proven), for instance, in order to prove something about an angle value in a figure.

Technically, most algebra proofs also involve using postulates, but most are not explicitly mentioned; for instance, when multiplying both sides of an equation, you might state, "Assumption of equality means that all multiples of the equality will also be true", but that seems unnecessary since its a very intuitive fact.

3.1 Examples

Now we give a couple of simple examples. In these examples, the standard set of equality postulates include: addition, subtraction, multiplication, division, substitution, and transitive property.

3.1.1 Example 1

Using the standard set of equality postulates, prove the value of x such that:

$$3x+2=8$$

This can be done in an instant using the algebra we know, x=2. But now we'll prove this answer using the postulates of equality:

3x+2=8, given
3x=6, by subtraction postulate (-2 to both sides)
x=2, by division postulate (division by 3 to both sides)

Although we (likely) applied the exact same steps in finding x quickly, in this case we've shown work and reasoning as to why this value of x is true without a doubt.

3.1.2 Example 2

Again, using the standard set of equality postulates, prove the values of x and y such that:

x+4y=9
2y=4

We can see rather quickly see that y=2, and so x=1. But we need to show how we derived this conclusion using postulates.

2y=4, given
y=2, division postulate (division by 2)
x+4y=9, given
x+4(2)=9, substitution postulate (y=2)
x=1, subtraction postulate (-8 to both sides)

Now we have shown without a doubt that x=1 and y=2. Although there were slightly different ways to prove this, they all lead to the same answer and have no room for ambiguity. The values have been proven.

As might be guessed, there are more challenging proofs than those given above. In addition, often times there will be no limit on the postulates and theorems that can be used to prove something.

3.2 Questions

Prove the values that solve the following using the standard set of equality postulates:

(*)1. 6x+2=3x+5

(*)2. 2x+3y=2 and 2x+4y=4

(**)3. 12x+2y=6 and 15x+3z=9 and 4y+5z=-71

Chapter 4

Proof by Counter-example

We now begin our journey into the land of proofs. The first type of proof we explore is proof by counter-example. This isn't a very utilized proof method, but it is still effective where applicable. The good news is that this proof method is very straight forward.

The idea is as follows: I state the following:

Proposition: X is always true.

I believe that this proposition is always true and that no exceptions exist, so by showing merely a single exception, you will prove that my proposition is false or at least does not hold for all the cases I claimed it did.

That's all there is to a proof by counter-example.

4.1 Examples

Now we show a couple of examples.

4.1.1 Example 1

Proposition: All natural numbers are even.

Dis-proof: Even numbers are divisible by 2. 1 is a natural number, and one is not divisible by 2, therefore that proposition is not always true.

4.1.2 Example 2

Proposition: There exist no triplet primes, where triplet primes are three prime numbers: a,b,c with c-b=b-a=2.

Dat-proof: Consider the three numbers: 3,5,7. All three are prime numbers, and 7-5=5-3=2, which breaks that proposition. This is our counter-example to disprove their proposition.

Hopefully these two examples have given you an idea as to how these proofs are done.

4.2 Questions

Find appropriate counter-examples where possible (not all are possible to find counter-examples for):

(*)1. Proposition: In the interval [0,1) there are more natural numbers than irrational numbers.

(*)2. Proposition: $x^2 + 4x + 5 = 0$ has no real values of x which satisfy the equation.

(*)3. Proposition: Everyone in your immediate family is left-handed.

(**)4. Proposition: There are no other triplet primes than 3,5,7.

(**)5. Proposition: define a perfect number as a number whose sum of all factors (prime and composite) are equal to twice its value. For example, 6 has factors $1, 2, 3, 6$, which sum to 12. We also notice that 28 is a perfect number. I propose that there are no other perfect numbers than 6 and 28.

(*****)6. Proposition: define a perfect number as above. I propose that there are no odd perfect numbers.

Chapter 5

Proof by induction

Here we introduce our first proof method. I kinda lied by saying that last chapter was the first proof method. Proof by counter-example is more of a disproving method than a proof technique. As we begin true proofs, please take careful (careful!) note that these are proof methods, NOT a way to find solutions to questions, but rather a way to verify the validity of a solution. Lastly, throughout these proofs, only ONE side of the proposed formula can be manipulated–you cannot add something to both sides or divide both sides by something, these operations assume equality.

5.1 A Motivating Example

We begin by considering the following challenge of finding the following sum $1+2+3+4+.....+10+11+.....+(n-2)+(n-1)+n = S(n)$, where the ..... indicates that terms have been visually left out, but that the logical terms will fall in place. Also, notice that S is a function of n, the number of terms we are summing together. Clearly one way to approach this is to simply add together numbers manually, but that's not very quick, nor does it give a formula to immediately generate the sum. However, perhaps we can cleverly solve this challenge with some sort of trick. We begin by noting that we can arrange these numbers in any order when adding them up. I figure that perhaps it would be more convenient to consider the sum as the following two orderings:

$S = 1+2+3+4+.....+10+11+.....+(n-3)+(n-2)+(n-1)+n$
$S = n+(n-1)+(n-2)+(n-3)+.....+(n-9)+(n-10)+.....+4+3+2+1$
Adding these together, gives:
$2S = (n+1)+(n+1)+(n+1)+(n+1)+...+(n+1)+(n+1)+...+...(n+1)$
We notice that there are n of these terms. Combining these terms, we have: $2S = n*(n+1)$, or simply $S(n) = \frac{n(n+1)}{2}$.

This is wholly correct, and there is nothing wrong with this answer. How-

ever, later we'll show the validity of this equation not only through the algebra that we did above, but also through our new proof method of induction.

5.2 Sigma Notation

We now introduce a bit of notation. The so-called 'Sigma notation': $\sum_{i=0}^{n} f(i) = f(0) + f(1) + f(2) + f(3) + ... + f(n-1) + f(n)$. The letter Sigma is used because it is the Greek letter S, which is the first letter of Summation, which is what Sigma notation signifies. Take notice that there are multiple parts to the Sigma notation: there is a lower bound for the summation, there is an upper bound for the summation, and lastly there is a function of the increasing index (in this case i).

For example, the first example of 1+2+3+...+n could've been written as: $\sum_{i=1}^{n} i$

5.2.1 Discrete Numbers Only plz

Please take note that everywhere in this, i and n are both Natural or Whole numbers. This means that i and n can only take the values of $0, 1, 2, 3, 4, 5, 6, 7,$ $....., 20, 21, 22, ...$–but no numbers with decimals or negative values. This is what typically distinguishes topics in Discrete Mathematics from other branches of math–you can only have countable values.

Just as a side note, it would be possible to do these summations using negative or even rational numbers, however, those summations will not be covered. To do this, you'd merely either specify the separation of each index or you'd divide each index by some factor so that it'd become a rational number rather than a natural number.

5.3 Induction

Now, we finally introduce induction. A standard explanation of induction is the following. Imagine a row of dominoes. The concept is that if I can find the first domino, and guarantee that each domino has another domino which it will cause to fall down, then I know for certain that I can knock down the entire chain of dominoes. In a mathematical setting, this is rephrased as follows: If I can find the first domino, and show that each n^{th} domino will knock down each $(n+1)^{st}$ domino, then we know that all dominoes following that first domino must also fall. At the moment this is rather unclear, so hopefully the following worked examples will help clarify. As afore mentioned, please note that induction is a tool for proving formulas, not for finding formulas. Induction will (typically) not produce a formula for a question, but rather help to show that the formula that you have must hold true.

The general format is the following:

Inductive Hypothesis: the following formula is true for all n greater than u.

Then we show that the formula (Inductive Hypothesis) is true for some value greater than u.

Now we assume the inductive hypothesis is true for some n, and we ask whether the hypothesis is still true for n+1, given our assumption that its true for some n.

If we can manage to rearrange the n+1 case and substitute in the n case, then it must be true that the formula holds for all n greater than our base case of u.

5.3.1 Example 1

$\sum_{i=0}^{n} 2^i = 2^{n+1} - 1$

Notice that in this example $f(i) = 2^i$. Notice that for each term we're doubling the previous term and adding it on to the current sum.

Before we begin this example, it seems worthwhile to consider some of the importance in this statement. What it literally says is that adding together all the powers of two in a row, will make one short of the next power of two that'll be added. Although a seemingly useless statement, this affirms an absolutely crucial fact in computer science. Computers have been designed to think in binary. Binary uses only 1 and 0 to represent all numbers [I would recommend googling binary or number bases to get a better feel for what this statement says]. A possible concern is that using only 1 and 0, might lead to some gaps in the numbers. However, this example allows you to make certain that using base 2 (binary) counting still accounts for all numbers.

Let us quickly take a look at the n=3 case, before we begin, so that we have a better grasp on this formula:

$\sum_{i=0}^{3} 2^i = 2^0 + 2^1 + 2^2 + 2^3 = 1 + 2 + 4 + 8 = 15 = 16 - 1 = 2^{3+1} - 1$.
Ok, now we know that at n=3, we have the above summation. Now its time to move to the proof.

First we consider the n=0 case:
$LHS = 2^0 = 1 = 2 - 1 = 2^{(0+1)} - 1 = RHS$

Now we supposed that $\sum_{i=0}^{n} 2^i = 2^{n+1} - 1$ is true for some n, and we ask whether it still holds true for n+1.

$\sum_{i=0}^{n+1} 2^i = \sum_{i=0}^{n} 2^i + 2^{n+1}$, notice that we've just spliced off the last term.

Now we apply the Inductive Hypothesis. When applying the inductive hypothe-

sis, we can replace the part of an expression identical to our Inductive Hypothesis with the expression we're trying to prove. $\sum_{i=0}^{n} 2^i + 2^{n+1} = 2^{n+1} - 1 + 2^{n+1} = 2 \cdot 2^{n+1} - 1 = 2^{(n+1)+1} - 1 = RHS$, which completes the proof. Since the formula holds true for n=0, and the n+1 case when true for the n case, the formula will hold true for all n=0 or greater.

This is a very powerful statement as we mentioned before.

5.3.2 Example 2

Now we return to the problem that started this all: $1+2+3+.....+(n-1)+n$. Earlier we showed through algebra that $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$, now let's verify this using our new proof tool of induction.

$\sum_{i=0}^{n} i = \frac{n(n+1)}{2}$

First consider when n=1:
$LHS = 1 = \frac{(1+1)\cdot 1}{2} = RHS$, therefore the formula holds for n=1.

Now we suppose that $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$ is true for some n, and we ask whether it still holds for n+1.

$\sum_{i=1}^{n+1} i = \sum_{i=1}^{n} i + (n+1) = \frac{n(n+1)}{2} + (n+1)$. Notice that again we applied the same technique of taking off the last term, then plugging in our Inductive Hypothesis. Now we simply need to see if we can alter what we have into the n+1 case of our proposed formula. The n+1 case of our formula will be $\sum_{i=1}^{n+1} i = \frac{(n+1)((n+1)+1)}{2}$, which is simply the formula we started with, except with n+1 plugged in for all the n in the original formula.

Now, with our goal in mind, we proceed. $\frac{n(n+1)}{2} + (n+1) = \frac{n(n+1)}{2} + \frac{2\cdot(n+1)}{2}$, expanding the expression we get: $\frac{n^2+n+2n+2}{2} = \frac{n^2+3n+2}{2}$. The numerator is a quadratic that can either be solved using the famed quadratic formula, or by noticing that it can be factored as $(n+1)(n+2)$.

Putting this back in, we have $\frac{(n+1)(n+2)}{2} = \frac{(n+1)((n+1)+1)}{2} = \sum_{i=1}^{n+1} i$. This is exactly what we've hoped for! Since we have shown the formula true for n=1 and true for all n+1 when assumed true for n, the formula will be true for all n=1 or greater.

5.3.3 Possible Notation Help

The following simplification is true, and seemed helpful to some people, for these summation based induction proofs. Let's have $g(n) = \sum_{i=1}^{n} f(i)$. Induction is trying to verify that $g(n+1) = \sum_{i=1}^{n+1} f(i)$, assuming that $g(n) = \sum_{i=1}^{n} f(i)$

(Inductive Hypothesis). Taking off the last term of the summation in the n+1 case, we have: $g(n+1) = \sum_{i=1}^{n} f(i) + \ f(n+1)$, now we apply the Inductive Hypothesis, so that $g(n+1) = g(n) + f(n+1)$. If we can show this, then we know that our supposed formula must be true.

5.3.4 Example 3

This last example is more subtle than the previous ones. Although the other ones were less intuitive, this one requires a bit more care while being proved.

$\sum_{i=1}^{n} k = n \cdot k$

In this example, we notice that $f(i) = k$. This means that the function does not depend on i (the index). We should also take note that this is a fairly intuitive statement: a number added to itself n times, is n times the number.

NOTE: the formula we are trying to prove is often called the Inductive Hypothesis.

We begin with the base case, n=1:
Left-hand side (LHS)=$\sum_{i=1}^{1} k \ = \ k \ = \ 1 \cdot k$=Right-hand side (RHS).

Now we suppose that $\sum_{i=1}^{n} k = n \cdot k$ is true for some n, and we ask whether it is true for n+1.

$\sum_{i=1}^{n+1} k$=$\sum_{i=1}^{n} k \ + k$, which using the Inductive Hypothesis, is also $n \cdot k + k$, which can have the k factored out, making: $(n+1) * k$, which is exactly RHS with n+1. This completes the proof. We have found that the formula holds for 1, and for n+1 when holding for n. This means that it holds for all n=1 or greater.

5.4 Final Words

Before we conclude, we will discuss a little about the uses of induction. Induction is typically used in computer science and or discrete math to prove that certain hypothesized statements are true. Many induction proofs are somewhat similar to the ones seen here, but also there are a number of proofs that involve products of successive terms of a sequence or abstract inductive construction of sets and then using induction on those sets to prove statements about said sets. Needless to say, induction can get a whole ton tougher, but this is supposed to present this material in a somewhat friendly and accessible manner. In addition, it will probably be used a number of times later in this course, so its worthwhile to practice this proof method.

5.5 Questions

Prove the following using induction:
(*)1. $\Sigma 2f(i) = 2\Sigma f(i)$

(*)2. $\sum_{i=0}^{n-1}(2i+1) = n^2$

(**)3. $\sum_{i=0}^{n} i^3 = (\sum_{i=0}^{n} i)^2$

(**)4. $\sum_{i=1}^{n}(\frac{1}{2})^i = 1 - \sum_{n+1}^{\infty}(\frac{1}{2})^i$. This one is a little less formal than one might desire, as ∞ not very well defined, nor is it clear that ∞ is a natural number. This still serves as practice.

(*)5. $\sum_{i=0}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}$

These are somewhat different than the previous examples (in that they are not summation proofs):

(*)6. Prove that $8^n - 3^n$ is divisible by 5, $\forall n \geq 1$

(*)7. Prove that $n^3 - n$ is always divisible by 6, $\forall n \geq 2$. Hint: factoring might help, also it might be useful to show that this is divisible by 2 and by 3, rather than jump straight to 6

(**)8. Prove that $2^{n+2} + 3^{2n+1}$ is divisible by 7, $\forall n \geq 1$

(**)9. Prove that $11^n - 6$ is divisible by 5, $\forall n \geq 1$

(*)10. Prove $\prod_{i=1}^{n} \frac{i}{i+1} = \frac{1}{n+1}$. [n.b.: The symbol Π is like Σ except instead of adding progressive terms, successive terms are multiplied together.]

(****)11. Attempt to prove that:

$$\frac{\sum_i a_i}{n} \geq \sqrt[n]{\prod_i a_i}$$

Where a_i is a set of positive numbers. This is true, but challenging.

(**)12. The following is a "proof" by mathematical induction that everyone has the same birthday. Find the flaw in the proof. Explain.

Property P(n): Every member of a set of n distinct people has the same birthday.

Basis of induction: Since a set of one person has only one birthday, so P(1) is true.

Inductive step: Assume P(k) is true for a positive integer k, we will show that P(k+1) is also true.

For a set $A = \{a_1, a_2, a_3, ...a_{k+1}\}$ of k+1 distinct people, consider two subsets $B = \{a_1, a_2, a_3....a_k\}$ and $C = \{a_2, a_3...a_{k+1}\}$ each with k distinct people,

obtained respectively by removing the last and first person from the set A. By the inductive assumption, every member of set B has the same birthday x, and every member of set C has the same birthday y. Since the two sets B and C have $a_2, a_3....a_k$ in common, the two birthdays x and y must be the same. As a result, every member of the set A has the same birthday and we have shown P(k+1) is true based on the inductive hypothesis that P(k) is true.

Chapter 6

Proof by contradiction

This is another method of proof. Again, please do not try to use this to conjure up a formula, this is only useful for proving validity, although in a different way than proofs by induction.

Consider a proposed theorem (generalized statement in math) that claims that something is true. Proof by contradiction works by assuming that its not true. If, while trying to prove that its not true, you come across something that is mathematically false or contradicts an initial assumption, then your assumption that the theorem is wrong, is itself wrong, so the theorem is right. By going through this, you have disproved the alternative option, and have thus solidified the proposed theorem. You have proven that the statement cannot be false.

6.1 Example

In chapter 1, we asked whether $\sqrt{2}$ was a rational number. Although its reasonable to assume that its not, how would we know for certain? This is an opportunity for proof by contradiction.

We begin by assuming that $\sqrt{2} = \frac{p}{q}$, where p,q are relatively prime natural numbers. We now consider the square of the initial relation:

$$\sqrt{2} = \frac{p}{q}$$
$$2 = \frac{p^2}{q^2}$$
$$p^2 = 2q^2$$

Now we consider this statement. It says that some number is equal to twice another number. This implies that p^2 is an even number. Since p^2 is even, p must be even. This is perfectly fine (for now). Since p is even, we can write it as 2k, where k is a natural number. Now we start over again, except replacing p with 2k. So we have:

$$\sqrt{2} = \frac{2k}{q}$$
$$2 = \frac{(2k)^2}{q^2}$$
$$q^2 = \frac{4k^2}{2}$$
$$q^2 = 2k^2$$

We notice that the right side is again twice a number, which means q^2 is even, which means q is even and can be expressed as 2w. This means that if $\sqrt{2}$ can be expressed as a rational number, then its equal to $\frac{p}{q} = \frac{2k}{2w}$, but this implies that p,q have a common factor of 2, which means that they're not relatively prime as we demanded initially. This is our contradiction, which means that $\sqrt{2}$ cannot be a rational number. This completes the proof.

We only give one example because this is a relatively straight forward proof method that just requires practice and a little intuition.

6.2 Questions

(*)1. Prove $\sqrt{3}$ is irrational

(**)2. Prove the following set of statements:

the product of two positive numbers is positive
the product of two negative numbers is positive
the produce of a positive and a negative number is negative

(**)3. Prove the following statements:

the product of two even numbers is an even number
the product of two odd numbers is an odd number
the product of an even number and an odd number is an even number

(*)4. Prove that the difference between an irrational number and a rational number must be irrational.

(*)5. Prove that if a number m is rational, and the product mn is irrational, then n must be irrational.

Chapter 7

Proof by pigeon holing

Consider your classroom. There are maybe about 30 students in the room. Your mind begins to wander into new domains, and you ask yourself: what're the odds that any two people in this room have the same birthday? Or simpler, what's the maximum number of people needed to guarantee that not everyone in the room has a unique birthday?

Enter pigeon holing. The principle of pigeon holing is that you have a certain number of possible outcomes, but once you have more trials than possible outcomes, then you must have some repetitions. This is a proof of the minimum number of trials needed to ensure a collision or overlap. Its not too useful for verifying formulas, but rather for bounding formulas or expressions.

7.1 Examples

7.1.1 Example 1

Consider the maximum number of coin flips that need to be made before a repeat face is shown.

On the first flip we get either a heads or a tails. Best case we accidentally get the same face twice in a row and that's the end, only one flip. Worst case, on the next flip we land the other face, and now all faces have been shown. On the third flip we get one side and it must be a repeat, which means the most number of flips is a measly three.

7.1.2 Example 2

Consider the birthday problem we began this chapter with. There are only 365 (or 366) days in a year. Each person has some birthday. This means we can apply the same logic as in the previous example, but now we need to repeat it roughly 365 times. This means that the least people we can trap in a room

and know for certain that there is a repeat birthday is 367 people (366 and the certain repeater).

7.2 Questions

(*)1. How many rolls of a 6-sided die are needed to ensure that a repeated roll occurs?

(*)2. How many rolls of an n-sided die are needed to ensure that a repeated roll occurs?

(**)3. How many real numbers do we need to pick between 0 and 1 so that we have an ensured repeat?

Chapter 8

Prime numbers visit 2

Week two at long last! Congrats to those that completed at least part of the homework questions. This weeks reading is shorter and the homework is shorter than last weeks. Enjoy!

This weeks topics include: prime numbers, prime factorization, mutually prime numbers, mutually prime sets of numbers, division with remainders, and the euclidean algorithm.

8.1 Primes

Prime numbers are, as mentioned last week, all numbers such that the only way to multiply natural numbers together to make the number of interest is to use the number itself and one. That's the long-winded version of the simple definition:

A natural number, $p > 1$, is prime if its only factors are 1 and p.

This is the definition of prime numbers that we will use throughout this course. A natural number could, instead of being prime, be composite:

A natural number, c, is composite if there exists at least one other pair of numbers $(a, b) \neq (1, c)$ such that $a \cdot b = c$

From this definition we see that prime numbers are not composite (as was suggested previously), and we are also informed that 1 is not composite, but we also notice that 1 cannot be prime. This means that we must assign 1 as being a special number that is neither prime nor composite.

The take-home message is that all natural numbers greater than 1 can be categorized into either prime numbers or composite numbers.

8.2 Prime Factorization

Here we declare and define a relatively simple concept. All natural numbers can be represented as a product of prime numbers raised to integer powers.

We begin with a couple of quick examples:

First, consider 48. 48 can be written as $2^4 \cdot 3$

Next consider 60. 60 can be written as $2^2 \cdot 3\dot{5}$

Lastly, consider 2035. 2035 can be written as $5 \cdot 11 \cdot 37$

Just for fun, we'll do one more before we move on. Let's do 8893719373. Whether you believe it or not, this can be written as $7^4 \cdot 11^5 \cdot 23$.

Notice that prime numbers, p, can be written in this format as: $p = p^1$. That's the only way to express the prime factorization of a prime number.

Since all primes can be expressed in this way, and all composite numbers, by definition, have at least one prime factor. This leads us to conclude that all natural numbers, N, can be expressed as:

$$N = p_1^{a_1} \cdot p_2^{a_2} \cdot p_3^{a_3} \cdot p_4^{a_4} \cdots$$

Where all p_i are prime numbers and a_i are natural numbers. Although we're assuming this fact for now, later in this lecture this fact will be proven. This set of primes and their exponents can be composed into a set with repeating factors, call it $P_{factors}$. This $P_{factors}$ as a set is called the prime factorization of the number.

Although one could wildly guess at how to decompose a number into its prime factors, there is a relatively efficient algorithm for finding the prime factorization. Consider some presumed composite number C_0. We apply the following algorithm beginning with i=2, and C_i=C_0:

1. Check whether C_i leaves a 0 remainder when divided by i.

2.a. If so: replace C_i by $\frac{C_i}{p}$. Write down this i, as its a factor of our original C_0

2.b. If not: increase i by 1

3. check if i is less than or equal to C_i:

4.a. If so: return to step 1

4.b. If not: stop. The prime factorization is complete.

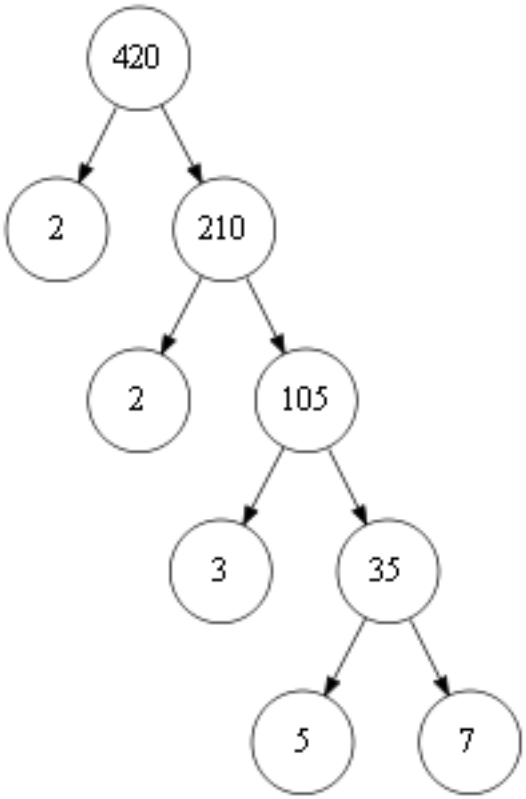
The list of i values give the prime factorization of the number C_0. Some major improvements can be added to this algorithm, but this works effectively and will yield the right answer.

In class we demonstrated a graphical method of doing this, its prettier than

the procedure stated above, but will yield the same result, so its just for aesthetics.

8.2.1 Example 1: 420

We begin by asking whether 420 is divisible by 2. It is, so now we have $C_1 = 210$ and return to step 1. We now ask if 210 is divisible by 2, and get $C_2 = 105$. We now ask if 105 is divisible by 2. Its not. So we try the next number. 105 is divisible by 3, so $C_3 = 35$. We try 3 again, and it fails. Now we try 4, and it fails. Now we try 5 and get $C_4 = 7$. We try 5 and it fails, as does 6. Lastly we try 7 and get $C_5 = 1$. At this point we look at 7 and see that $7 \geq 1$, so we stop the algorithm. Now let's collect all the numbers that worked: 2, 2, 3, 5, 7. Combining like terms gives: $420 = 2^2 \cdot 3 \cdot 5 \cdot 7$ as its prime factorization.



above is a graphical way of looking at this example.

8.2.2 Example 2: 23

We begin by trying 2, it fails. 3 fails, 4 fails, 5 fails, 6 fails..... eventually we try 23 and it succeeds giving $C_1 = 1$, now we have $i \geq C_1$ so we stop. This means that the prime factorization of 23 is 23. This simply means that 23 is prime so

it can't be expressed as a product of any other primes.

In the exercises there are some practice problems, although feel free to play around with this for a while if you haven't done this before.

8.3 Mutually Prime Numbers

Please note that the terms "mutually prime", "relatively prime", and "co-prime" have the same meanings, and will be used interchangeably.

Let us consider two numbers α and β and their corresponding prime factorizations:

$$\alpha = p_1^{a_1} \cdot p_2^{a_2} \cdot p_3^{a_3} \cdot p_4^{a_4} \cdots = \{p_i^{a_i}\}$$
$$\beta = q_1^{b_1} \cdot q_2^{b_2} \cdot q_3^{b_3} \cdot q_4^{b_4} \cdots = \{q_i^{b_i}\}$$

where the thing following the last equality sign is simply saying that we're considering a set of primes raised to powers.

We now make the following definition:

Two numbers α and β are mutually prime if the intersection of their prime factorization sets is the empty set.

What this says in english is that if we compare the prime factorizations of the two numbers and find that there is no common prime divisor, then the two numbers are called mutually prime.

8.3.1 Mutually Prime Number Sets

From this we might generalize to considering more than two numbers. We make the following definition:

A set of numbers $\{N_i\}$ are mutually prime if their is not common factor in all members. The set is pairwise relatively prime if the pairwise intersection of all their prime factorization sets is the empty set.

For instance, the set {2,3,17,35} is a mutually prime set, while {2,3,5,35} is not since 5 and 35 have a common factor of 5 between them.

8.4 Division with Remainders

In the above algorithm we were only interested in the case where the remainder from division was zero. Alternatively the division could have left a remainder. For instance, consider dividing 25 by 7. We can find the remainder by considering that 25 could be written in the form $7 \cdot \gamma + \delta$, usually with $\gamma \geq 1, \delta \geq 0$. This makes sense since 25 is greater than 7, and greater than 14, and 21. So we

could write $25 = 7 \cdot 3 + 4$. This says that the remainder when 25 is divided by 7 is 4. We now generalize:

When a number ν is divided by μ, with $\nu \geq \mu$, we can write $\nu = \mu \cdot \gamma + \delta$, where $\nu > \delta \geq 0$ and $\gamma \geq 1$. δ is the remainder.

If we remove the restrictions on γ and δ, then we have: $\nu = \mu \cdot \gamma + \delta = \mu \cdot (\gamma + \alpha) + (\delta - \mu \cdot \alpha) = \mu \cdot \gamma' + \delta'$. This means that we can vary α and generate a sequence of ways to express ν. The generation of this sequence is called the **Division Algorithm**. An algorithm is another word for a procedure.

8.5 Greatest Common Divisor

In the previous sections we found a way to describe a number as a multiplication of primes. Now we try to find the Greatest Common Divisor (GCD) of a pair of numbers from these values. The GCD is, as the name suggests, the largest number that divides both numbers of interest and leaves no remainder.

Considering a single number, we can gain a simple geometric understanding of the prime factorization set. Imagine using a ruler to represent the number. Each inch is a unit length (1 long) and the total length of the ruler is the same as the number we're considering. Consider trying to put integral length stickers onto the ruler. You clearly don't want to use only half a sticker, so you want to have an integral number of stickers on your ruler. The prime factorization gives you the various lengths of stickers you can use to cover the ruler. For example, consider a ruler of 12 length. 12 has the prime factorization of $2^2 \cdot 3$. This means that you could cover the ruler with 12 stickers of length 1, or 6 stickers of length 2, or 4 stickers of length 3, or 3 stickers of length 4, or 2 stickers of length 6, or 1 sticker of length 12. This is seperating the prime factorization into two parts: one which gives the length of the stickers, the other the number of stickers of that length needed.

Now let's transition to considering a pair of numbers. Each number is a ruler, so let's just consider a two-dimensional ruler, or equivalently a floor with an underlying unit grid. Instead of applying stickers to a floor, we'll tile it instead. Because we're seeking a common factor we need a symmetric integral sized tile, or simply a square. Clearly the only possible choices of square sizes are those which would completely cover the floor without overlap, overhang, or breaking a tile. This means that the squares must have a length that is a divisor of both numbers. We select the largest square size possible and define this to be the GCD, as its the largest number that divides both of the other numbers without any remainder.

This reasoning shows that the GCD is a subset of the prime factorization of both numbers. In fact, its the largest common subset of both numbers, known in set language as the intersection of the two sets*.

(this isn't the classical intersection, but rather the following: for all a_i in both multiple set A and multiple set B, remove a_i once from both sets and place into the intersection set.)

This brings us back to our mutually prime definition quite wonderfully, as this is caused by there being no intersection between the prime factorizations.

8.6 Euclidean Algorithm

Although its true that the GCD can be found by taking the intersection of the prime-factorization sets, it is wasteful to compute these sets then reduce them. Perhaps there is a method that can save us the effort of computing wasteful information. There is! Its called the Euclidean Algorithm.

8.6.1 Background

Alas, before we actually get to the algorithm, we need to build up a set of notations and theorems to help us derive the algorithm. Although its not necessary for understanding the algorithm, without it the algorithm has much less meaning.

The first piece of notation is: $a|b$ which reads: "a divides b (and leaves no remainder)". Using our notation from earlier this chapter, this says that $b = a \cdot \gamma$.

We begin with this list of theorems (one is proved below, some of the others are on the homework assignment):

Theorem of basic divisibility properties

1) $a|b$ implies $a|bc$, where c is an integer
2) $a|b$ and $b|c$ implies $a|c$
3) $a|b$ and $a|c$ implies $a|(bx + cy)$, where x and y are integers
4) $a|b$ and $b|a$ implies $|a| = |b|$
5) $a|b$, $a > 0$, $b > 0$, imply $a \leq b$
6) if $m \neq 0$, $a|b$ implies and is implied by $(ma)|(mb)$

proofs:
All of these follow from the definition of divisibility, and require a similar approach as done below.

1) $a|b$ means that $b = a \cdot r$, and $a|bc$ means $bc = a \cdot q$. multiplying the first re-expression by c gives: $bc = a \cdot (r \cdot c) = a \cdot q$

3) $a|b$ means that $b = a \cdot r$, and likewise $c = a \cdot q$. Multiplying both sides

of each equation by some constants x and y gives: $bx = a \cdot r \cdot x$ and $cy = a \cdot q \cdot y$. Summing gives $bx + cy = a \cdot (rx + qy)$, which is clearly divisible by a.

6) $a|b$ means $b = a \cdot r$, multiplying both sides by m gives $mb = ma \cdot r$, which means $(ma)|(mb)$.

Although before we realized that the GCD is some component of the prime factorization of a pair of numbers, here we begin to think about the GCD as a natural number and not so much as it being a subset of the prime factorizations.

Definition of GCD

Two numbers a and b have some set of natural numbers $C_{div} = \{d_1, d_2, d_3, ...\}$ which divide both a and b, C_{div} is called the set of common divisors. C_{div} is clearly finite since a divisor cannot be greater than the number its dividing. This means that there is a greatest member of this set. We call this greatest member the GCD and denote it (a,b).

Theorem: Bezout's Identity

We can write $g = (b, c) = bx_0 + cy_0$, where x_0 and y_0 are integers.

proof:
We begin by considering bx+cy over all integral x and y. This forms a set $A = \{bx + cy\}$. We choose x_0 and y_0 so that we have the smallest positive integer in A, call that number $\mathbf{L}$.

Next, we prove that $\mathbf{L}|b$ and $\mathbf{L}|c$, please note that not all members of A have this property, only the smallest positive member has this property (or so we're about to prove). Without loss of generality, we consider the first case. After we consider the first case, we could quite easily follow the same logic and draw its corresponding conclusion, so we can examine just the first case and replace all b with c. We suppose for contradiction that its not true that $\mathbf{L}|b$. Then this means that $b = \mathbf{L} \cdot \gamma + \delta$, where $0 < \delta < \mathbf{L}$. Re-arranging we have $\delta = b - \mathbf{L} \cdot \gamma = b - \gamma \cdot (bx_0 + cy_0) = b(1 - \gamma \cdot x_0) + c \cdot (-\gamma \cdot y_0)$, which is in A. But we demanded two things: first $\mathbf{L}$ was the smallest positive element in A, and second that $0 < \delta < \mathbf{L}$, but both of these can't be true, so we have a contradiction. This means that $\mathbf{L}|b$ must be true.

By definition g is the greatest common divisor of b and c, or rephrased, we have b=gB and c=gC. So then $\mathbf{L} = bx_0 + cy_0 = g(Bx_0 + Cy_0)$. This is divisible by g, so $g|\mathbf{L}$, and by part 5 of basic divisibility properties $g \leq \mathbf{L}$, and since g is the greatest common divisor, we cannot have $g < \mathbf{L}$, so $g = \mathbf{L} = bx_0 + cy_0$. This completes the proof.

As a note, this Identity can be generalized into more than just a pair of num-

bers, but rather into a set of numbers. This comes closer to the full Bezout's Identity, but the number sample is sufficient for right here and now.

GCD shift theorem

for all integral x, (a,b)=(a,b+ax).

proof:
Using Bezout's Identity we have $g = (a, b) = ax_0 + by_0 = ax_0 + by_0 + axy_0 - axy_0 = a(x_0 - xy_0) + (b + ax)y_0 = a\chi + (b + ax)y_0 = (a, b + ax)$. The reason this works is because $x_0 - xy_0$ is just a shifted version of the initial x_0 coefficient and so we can increase or decrease x_0 by xy_0 and return to our initial minimal positive value, and allows us to equate the two sides of the equality and prove the theorem.

Example: 2014 and 2020

Before we finally get to the algorithm, well do try to find the gcd of two numbers using the theorems we just derived.

We are tasked to find (2014,2020). Let's apply the gcd shift theorem to this: $(2014, 2020) = (2014, 2020 - 2014 \cdot 1) = (2014, 6) = (2014 - 1800, 6) = (214, 6) = (214 - 180, 6) = (34, 6) = (34 - 30, 6) = (4, 6) = (4, 6 - 4) = (4, 2) = (0, 2) = 2$. 2 is the correct answer, and in fact we could've done this a little quicker as: $(2014, 2020) = (2014, 6) = (4, 6) = (4, 2) = (0, 2) = 2$ by applying the division algorithm to find the smallest positive shifted value for 2014 we can obtain using the gcd shift theorem. Its the same thing either way, but by reducing each number as much as possible at each step it makes the process at least seem quicker.

Using the gcd shift theorem we quickly and easily found the gcd, and we didn't compute excess information. We can formalize and prove the procedure we just applied.

8.6.2 Algorithm

We finally have built up the theorems needed to derive the Euclidean algorithm.

Euclidean Algorithm

Given integers b and c greater than 0, we make a repeated application of the division algorithm, and obtain the following series of equations:

$$b = c \cdot q_1 + r_1,\ 0 < r_1 < c,$$
$$c = r_1 \cdot q_2 + r_2,\ 0 < r_2 < r_1,$$

$$r_1 = r_2 \cdot q_3 + r_3,\ 0 < r_3 < r_2,$$
$$\cdots,\ \cdots$$
$$r_{j-2} = r_{j-1} \cdot q_j + r_j,\ 0 < r_j < r_{j-1}$$
$$r_{j-1} = r_j \cdot q_{j+1}.$$

Then $(b, c) = r_j$. From this we can find the x_0 and y_0 in the equation $(b, c) = bx_0 + cy_0$.

proof:
This set of equations comes about as a repeated application of the GCD shift theorem. Eventually we reach the shifted $(\beta \cdot \alpha, \beta)$, which would next bring $(\beta, 0)$ or $(\beta \cdot \alpha, 0)$ and terminate the chain. Now we examine $(\beta \cdot \alpha, \beta)$ and hope to show that $\beta = (b, c)$.

We begin with the original gcd and work our way along our chain of equations: $(b, c) = (b - cq_1, c) = (r_1, c) = (r_1, c - r_1q_1) = (r_1, r_2) = (r_1 - r_2q_3, r_2) = (r_3, r_2) = ...$ following through the induction gives the conclusion that: $(b, c) = (r_{j-1}, r_j) = (r_j, 0) := r_j$, which shows that the gcd is the last r_i that we obtain in our series of equations.

Example (963,657)

This gives $(963, 657) = (306, 657) = (306, 45) = (36, 45) = (36, 9)$, which means the gcd of 963 and 657 is 9. Its possible to, if keeping careful tabs, generate the x_0 and y_0 so that $(b, c) = bx_0 + cy_0$.

8.7 Fundamental Theorem of Arithmetic

Before we get to prove this big mathematical statement, we need to once again build up some theorems. Luckily the theorems we've already proved can and will be used to help simplify these coming proofs.

Theorem of scaled GCD

For all natural m, a, and b we have: $(ma, mb) = m(a, b)$.

proof:
We start with the left hand side and apply Bezout's Identity: $g = (ma, mb) = m * a * x_0 + m * b * y_0 = m * (a * x_0 + b * y_0) = m * (a, b)$, as desired.

Notice that by variable re-assignment we also have: $\frac{(a,b)}{g} = (\frac{a}{g}, \frac{b}{g})$

This one will also be kept.

Theorem: Euclid's Lemma

If $c|ab$ and $(b, c) = 1$, then $c|a$.

proof:
By our theorem of scaled GCD, $(ab, ac) = a(b, c) = a$. From the statement we have that $c|ab$ and clearly $c|ac$, so $c|a$.

proof 2.0:
We apply Bezout's Identity on (b,c)=1 to get $1 = bx_0 + cy_0$. multiplying both sides by a gives: $a = a \cdot bx_0 + a \cdot cy_0$, the second term is divisible by c since c is a member of the product and the first term is divisible by ab, which by statement is divisible by c, which means that their sum is a, is divisible by c. This completes the proof.

Both of these proofs are valid, the second one though is more clear since it applies Bezout's Identity to highlight the argument.

8.7.1 Fundamental Theorem of Arithmetic (FTA)

Earlier we claimed that it was reasonable to assume that all natural numbers N could be written as $N = p_1^{a_1} * p_2^{a_2} * p_3^{a_3} * p_4^{a_4}...$, however here we provide a proof that this must be true.

FTA: All natural numbers $s > 1$ can be uniquely expressed as $p_1^{a_1} * p_2^{a_2} * p_3^{a_3} * p_4^{a_4}...$, where p_i are primes and a_i are natural number exponents.

proof:
First we show that it must be possible to express s in this way. We make the inductive hypothesis that all numbers between 1 and s can be expressed as a product of primes. Now we consider s+1. If s+1 is prime, we have the trivial case. If s+1 is composite, then $s + 1 = a * b$, where a and b are natural numbers greater than 1, and so each a and b are less than s+1. This means that, by our inductive hypothesis, a and b must both be expressible as a product of primes, and so s+1 must be expressible as a product of these products of primes. This shows the existence of this fact.

Now we show that such a representation is unique. We begin by assuming that it is not. This would mean the following:

$$\begin{aligned} s &= p_1 p_2 p_3 \cdots p_m \\ &= q_1 q_2 q_3 \cdots q_n \end{aligned}$$

And that $m \neq n$. We seek to first show that $m = n$. We first apply Euclid's Lemma be selecting some p_1 and dividing both expressions for n by this prime, so now we have:

$$\frac{s}{p_1} = p_2 * p_3 \cdots p_m$$

$$= q_2 * q_3 \cdots q_n$$

.

Now we inductively repeat until we get:

$$\frac{s}{\prod_i p_i} = \prod_{j=n+1}^{m} q_j$$

which suggests that $m \geq n$. Now we simply repeat the procedure, dividing this time by q_i members. This leaves $n \geq m$. Using these two inequalities we can conclude that $m = n$ and thus the representation is unique.

8.8 Questions

Decide which sets below are relatively prime (and if not, then state which numbers in the set are not relatively prime):

(*)1) {2, 5, 23}

(*)2) {14, 35}

(*)3) {127, 121, 34275}

(*)4) {49, 169, 27}

Write the prime-factorization of the following numbers:

(*)5) 9216

(*)6) 1694

(*)7) 383

(**)8) 977

(**)9) Earlier this chapter we stated an algorithm for finding the prime factorization of a number, N.

(*)a) Define a trial as checking whether the number is evenly divided by a

number. Decide which requires more trials to compute the prime factorization: primes or composites.

(*)b) In this worse case, decide the approximate number of trials needed to find the prime factorization.

(**)c) This is fine but there are a couple of improvements that can easily be made. Perhaps we can stop earlier than once i is greater than C_i. Decide a better place to stop trying numbers, and argue for its correctness. Lastly, state the approximate number of trials needed to find the prime factorization, yet again consider it in the worst case.

(*)d) The last improvement is to re-consider the set of numbers that we need to try. In the initial algorithm we try all natural numbers, suggest a better choice of number type to try.

(**)e) Write out your new algorithm. It might be helpful to simply modify the starting algorithm.

(*)f) Code up both algorithms and show that the new algorithm is quicker. (do and check this for yourself).

Decide the greatest-common-divisor (GCD) of the following number pairs using their prime-factorization:

(*)10) 204 and 726

(*)11) 6336 and 5616

Decide the GCD of the following pairs using the Euclidean algorithm:

(*)12) 720 and 2691

(*)13) 6553 and 7759

(**)14) 2324784 and 1144066

Find a pair of x_0 and y_0 so that $g = (a, b) = ax_0 + by_0$ for each of the following pairs:

(*)15) 24 and 18

(*)16) 720 and 2691

(**)17) 2324784 and 1144066

Find the gcd of the following set of numbers by applying the euclidean algorithm to the numbers pairwise:

(*)18) {504, 3432, 11592}

(*)19) {18375, 38675, 84525}

Find a set of a_i so that $g = (b_1, b_2, ...b_n) = \sum_{i=1}^{n} a_i \cdot b_i$

(*)20) {14, 4, 18}

(**)21) {84, 156, 252}

(****)22) Omitted.

(**)23) Earlier this chapter we stated some basic divisibility theorems. Provide proofs of parts 2 and 4.

(*)24) Applying the gcd shift theorem and scaled gcd theorem find the gcd of the following expressions: $g = (a, b)$. What are the following equal to: $(ga, gb + xa)$ and $(a + bx, b + ay)$ and $(a, 2b)$.

(*)25) Find three natural numbers a,b,c so that they are as a set relatively prime, but pairwise are not relatively prime.

(****)26) Prove that it is always possible to find a set of n numbers where the entire set is relatively prime, but each subset is not relatively prime (taken 2 at a time they are not relatively prime, taken 3 at a time they are not relatively prime, 4 at a time, and so forth up to n-1 at a time).

8.9 Citation

Many parts of this week's lecture notes were aided by the following source: An Introduction to the Theory of Numbers (fifth edition) by Ivan Niven et al.