Boston University Summer I 2009

MA341 Number Theory Kalin Kostadinov

Workshop 1- Building on the Axioms. The First Proofs

The goal of this workshop was to organize our experience with the common integers and their properties in a concise manner. We started up with a system of axioms for the Ring of Rational Integers, and discussed why one needs such a system and what are its desirable properties.

Then we explored some immediate consequences form these *axioms,* and in this process we wrote our first simple *proofs*.

Here are the (very-slightly edited, there are inaccuracies reflecting the student level of understanding of some of the concepts in the workshop) comments of some of the students about the activity:

Daniela:

Today's workshop, Axiomatic Description of the Integers, involved the use of basic axioms on very simple proofs. Basic axioms include operations such as the associative and commutative properties of addition and multiplication, the distributive law, and the additive inverse, to name a few. It is important to note that in this case we are studying the integers in Z, as some of these axioms may vary depending on the range of numbers. For example, the Well Ordering Principle can't apply to rational numbers. Since there are so many it is nearly impossible to determine which one is really the smallest because they can keep decreasing to a certain limit infinitely. Because of this, it is important to keep track of what set you are really talking about in a proof.

Using these axioms, we came up with a proof for a very simple equation: $0*0=0$. It seems like a very simple, obvious proof, but it did take several steps using the most basic algebraic operations to show that this is actually true. After this proof we defined several terms that could have been useful in the proof. We said that $a > b$ when $a + b' \in N$ (from axiom 4 which says that given $a \in Z$, $\exists\, a' \in Z$ such that $a + a' = 0$). An element, a is called positive if $a > 0$, and it is called negative if a' is positive. Through this we claimed that if a and b are negative, then $a + b$ is negative too, and $a*b$ is positive. The proof for these claims was not fully completed.

****

Jae:

Our first workshop was mainly divided into two categories: Axioms and Proofs.

We began with a worksheet on axioms and discussed in great detail of the concepts of axioms. Some questions that were discussed:

1. (regarding axiom #10) What about repeats in a set?
   {1,2,3} is a set with three elements, however {1,2,2,3,3,3} is still a set with three elements. Repeats and the ordering of numbers do not matter.

2. What are axioms good for?
Axioms are the starting points and properties for proofs.

3. What makes a good system of axioms?
(a) with a good system of axioms you are able to distinguish between two different objects.
(b) they must be true, universal, and you don't want them to be contradictory.
(c) Axioms must be strong, and you gave an example with "twin primes" we have yet to find a strong axiom to prove this idea.

It is interesting to learn what are the basic properties that allow us to prove more complex problems.

PROOFS, concepts of PROOFS:
We did many examples and studied the definition of a>b, a>0 and an element that is negative.
We tried to prove in great detail that (a)(0)=0 and (0)(0)=0
by using the properties and concepts of axioms that we discussed before we were able to solve the proof (0)(0)=0.

To a person on the streets, trying to prove (0)(0)=0 may sound ridiculous and absurd; however it was very surprising to see how hard this proof really is. Since little these basic ideas are just assumed, however once sitting down to prove these ideas is a whole new domain.
It makes you question and wonder about basic equations, for example:
How do I know and prove that 1+1 is really 2.
Answer: I learned that, well, 2=1+1 is infact a definition, and does not require proof.

****

Lorna:

In Tuesday's lecture, on May 26, 2009 we discussed Axiomatic descriptions of Integers. We looked at the different axioms given to us but also discussed what an axiom is and tried to construct some of our own. First we discussed what a set is and when a set is similar to another, as in for example {1, 2,3} is similar to {1,2,2,3,3,3} and {3,2,1}.
Later on we looked at all the axioms given and singled axiom 10 as one of their most important axioms because it is axiom 10 that differentaites this set of axioms as a property of integers rather than rational numbers.
We pointed out four important qualities that defined what an axiom is:
1. an axiom has to distinguish between different objects
2. an axiom has to be as simple as possible(no redundancy)
3. an axiom has to be consistent(it should always work)
4. axioms cannot be contradictory(we should not be able to prove a

statement and its opposite in the same set of axioms.
After this we went on to explain some of the proofs in the axioms and especially concentrated on problem solving skills. We tried to make our own proofs like trying to prove that a*0 = 0 using the axioms given to us and 0*0 = 0

****

Fred:

In this workshop we went over the axiomatic description of the integers. Additionally, we attempted to write two proofs based on these axioms. The first proof was demonstrating that a * 0 = 0. The second proof was a demonstration that the product of two negative numbers is positive. Both of these proofs were left unfinished. This workshop followed studying the properties of congruencies, as well as systems of linear congruencies.

****

Tim:

The workshop about the axiomatic description of the integers was very interesting. It really gave me a new perspective to look at how the theory behind simple equations came about. I never knew that something so simple could be so complex. The workshop made me look back to simple equations that are learned as early as elementary school, and see how the use of axioms assembled them. I was surprised to see how many axioms were created only by only using the addition and multiplication function. Even though the axioms listed are extremely elementary in difficulty, the combination of the axioms listed is very powerful. Properties of axioms were also discussed in class. We came to the conclusion that it is necessary for a list of axioms to be relatively small, to be exclusive to the set being discussed, and for a set of axioms not have contradicting claims.

****

Spencer:

In our workshop on Tuesday we discussed axioms and how they relate to mathematical proof. Axioms are the most basic "principles" of any mathematical class or theory. They are the statements which can appear without any previous justification in a formal proof. For example, we might choose "A = A" as an axiom since it allows us to draw certain conclusions from statements involving the sign "=."

But how do mathematicians choose axioms? Euclid used statements that he considered to be "self-evident" as axioms (for example, that there exists a unique line through any two distinct points) to create what we now know as Euclidean geometry; over a century later, mathematicians discovered the so-called "non-Euclidean" geometries by simply throwing out Euclid's seemingly self-evident Parallel Postulate. This demonstrates that every theory can be identified and distinguished by its set of axioms. For example, by axiomatically describing the set N of integers, we can formally distinguish this set from the sets Q and R of rationals or reals: One axiom of N is that it is well-ordered (ie, every subset of N contains a least element), whereas any open interval of R or Q contains an infinite number of elements and no least element.

A "good" set of axioms is as small as possible by containing no redundancies. (An axiom is called redundant if it can be proved from the other axioms.) It should also be consistent (provide no possible proof of a contradiction), and ideally it should be complete. A set of axioms is called complete if there exists either a proof or counterexample for any statement about the space the axioms describe.

Finally, we practiced using axioms in a rigorous proof by attempting to provide proofs for basic, obvious propositions such as "[a x 0 = 0] for any integer a" and "The additive inverse 0 zero is unique." This ended up being a tricky task, since we are not allowed to assume anything except the axioms. Every statement in the proof must itself be proved from the axioms. In this way a proof can be conceived as a chain of lemmas connecting the axioms and conclusion.

****

Isabelle:

During the workshop on Tuesday, we were introduced to the axioms that define the Ring of Rational Integers, the set Z. Axioms are formal logical expressions used to build mathematical theories about the system they define, in this case, Z. Some axioms may be used to define multiple systems. For example, a+b=b+a holds true for all a and b element of both systems Z and the real numbers, R. However, some axioms describe what is unique about a particular system. For example, the well-ordered principle, says that every non-empty subset of N, the natural numbers, has a least element. This does not hold for all subsets of R. For example, the open set (0,1) has no least element. Thus while systems that are elements of other systems are subject to the same axioms as the larger set(eg. Z element of R), there may be axioms that can define a subset but not the larger set. It is also important that no axioms within a set are contradictory.

After the introduction to axioms, we began to use them in order to prove other theories about the system Z. For instance, in order to prove that 0*0=0, we first noted by 0'=0+0' by axiom 3. Then we said that 0*0=(0+0')*0=0*0 + 0'*0 by axiom 4 and axiom 7. From here we were able to show that, defining x as 0*0, x=0.

****

Susan:

Kalin handed out the list of axioms for the set of integers. Looking at axioms was a new thing for me, I had heard the word before, but no professor had ever taken the time to me explain what they were. After reading through a few of the axioms aloud and all of them by ourselves, we began compiling a set of criteria for a list of axioms. These criteria included ? non-redundant, distinguish working set from all other sets, not contradictory, and strong enough to prove or disprove anything. One of the reasons mathematics is so addictive is that many questions still remain unresolved. Does this mean our set of axioms is not strong enough? Do we need an additional axiom for the integers to solve Fermat?s Last Theorem?

We then went on to begin to prove simple, seemingly obvious statements using the axioms. At first, this was a bit of a challenge. In order to think about solving a*0=0 we needed to simplify it to 0*0=0, which we could prove together with a lot of guidance from Kalin. During this proof, Kalin demonstrated that in order to prove something, sometimes you need to work backwards and forwards and end up meeting in the middle. I had never thought about proofing this way. Hopefully this workshop will come in handy when I begin my semester project, a formal proof.

****

Samantha:

In today's workshop we discussed some of the most basic mathematical statements, which we often believe to be true and use without hesitation. A "good" list of axioms show no redundancy, are universal, distinguish between different groups of numbers, are strong enough to prove or disprove a claim, and do not contradict one another. During class we had the opportunity to study Axioms of the Integers and attempt to prove some of the most fundamental mathematical statements. A proof is formalized to some degree and builds a chain between a plausible argument and conclusion.

Example: Prove that 0 = 0`

1. There exists 0` in the set of integers such that 0 + 0` = 0. By axiom 4, very element *a* in the set of integers has an additive inverse: Given that *a* is in the set of integers, there is an element *a*` in the set of integers such that *a + a` = 0*.
2. 0 + 0` = 0`. By axiom 3, the set of integers contains a special element, denoted with the symbol 0, and called zero, which is neutral for the addition operation: *a + 0 = a* for all elements *a* in

the set of integers.

3. Therefore we can conclude that 0 = 0`.

As we discover more axioms and use these axioms to prove certain statements we are increasing the claims we can use for future proves. Axioms can also be used to construct definitions.

Definition: We say that $a > b$, when the $a + b`$ is an element of the natural numbers.
i.e. $a = -3, b = -5, b`= 5, a + b` = 2.$
i.e. $a = 7, b = 5, b` = -5, a + b` = 2.$
An element a in the set of integers is called positive if $a > 0$.
An element a in the set of integers is called negative is $a`$ is positive.

Once again, the definitions continue to build off one another and are rooted in previous axioms (for instance the Trichotomy principle). I believe that proofs are essential to truly understanding any type of mathematics. By proving these 'simple' concepts we will increase our understanding and enhance our further learning.

****

Sarah:

In the workshop on Tuesday we discussed axioms that applied to the integers. Many of the axioms were obvious, simple properties we learned in middle school such as associativity, additive inverses, distributivity, and commutativity. We learned that the Well Ordering Principle was on the list to exclude the real numbers. The only operations we were given to work with were addition and multiplication. Some very important characteristics that all axioms must follow are consistency and non-contradictory and strong enough that we may use them to prove or disprove a claim.

With the axioms, we were then given the task to prove simple, common knowledge properties. This task turned out to be quite difficult however. Trying to prove that a*0=0 turned out to be quite challenging. So as we learned in our first lesson when given a difficult problem, break it down to something simpler. So we tried proving 0*0=0. By using the axioms of additive inverses, the neutralness of 0 in addition, distribution, associativity, and commutativity we were able to conquer the seemingly easy task of proving 0*0=0. We concluded by defining what it is to be negative and positive. a>b when a+b1 is an element of the natural numbers. a in the integers is positive if a>0 and a is negative if a1 is positive.

Boston University | MA341 Number Theory
Summer I 2008 | Kalin Kostadinov

Workshop 1- Distilling Axioms, Proving Consequences

The goal of this workshop was to organize our experience with the common integers and their properties in a concise manner. We set up to find which properties fully describe the integers, and separate them from the other numerical system.

Then we explored some immediate consequences form these *axioms,* and in this process we wrote our first simple *proofs*.

Here are the (non-edited) comments of some of the students about the activity:

Allan:

Yesterday, at our workshop, we discussed in great detail, the definition of the set of Z. This set contains all the integers {...,-3, -2, -1, 0, 1, 2, 3, ...} .
To properly define Z, we say:
For every integer a in Z, one of the following conditions is true:
a) The integer a is equal to zero.
b) The integer a is in the set of natural numbers, N
c) The negative of a, (-a), is in the set of natural numbers, N.
There are several properties of integers in Z.
1) They have the operations of addition and multiplication, both of which can generate new members of the set of Z.
2) They have additive and multiplicative inverses and identities, which means that the operation can be reversed and neutralized.
3) Every integer can be represented as a product of unique primes.
4) The operations of addition and multiplication are commutative, which means, the order in which it is performed does not matter.
5) The operations of addition and multiplication are together distributive, a * (b + c) = a*b + a*c
6) There are no zero divisors, which means that when a*b = 0, either a = 0 OR b = 0.
7) One integer in Z can be compared to another integer in Z to determine which is greater.
So, if a > b, then a - b is in the set of natural numbers, N.
Additionally, I have read online that the set Z is closed for the operations of addition and multiplication. This means that a+b is inside the set Z, and that a*b is inside the set Z.

Also, I have read online that if one applies the following function to Z, we can show that the number of elements in Z is equal to the number of elements in N. This shows the cardinality of the two sets:
f(x) = 2x + 1, if x >= 0 && |x|, if x < 0

****

Andrew:

During the workshop on 27 May 2008 we attempted to describe the integers. We were able to arrive at approximately 12 properties of the integers. These included the existence of the addition and multiplication operators as well as an additive identity and a multiplicative identity. I found that the most interesting property we derived was that for every a contained in the set of integers, the exists an integer b such that b > a.

We also spent time trying to describe the natural numbers. I found that the most important property of these was the property which defined 'greater than': we say that a > b if and only if a-b exists in the natural number set. Overall I found that the concepts examined in this workshop set the ground work for many interesting results to come later.

****

Brendan:

In Tuesday's workshop we discussed integers, we listed properties and axioms for the set of integers, and we proved some of these axioms.
Here is a summary of the list we created:
There exists operations “+” and “.” on Z (closed under addition and multiplication).
Both of these operations are associative and commutative.
There's an additive identity (0) and a multiplicative identity (1).
The natural numbers is a subset of Z.
Every integer can be uniquely represented as a product of primes.
There's an additive inverse. We proved the uniqueness of the additive inverse using properties of associativity and commutativity.
There are no zero divisors.
And for every a in Z exactly one of the following is true: 1) a=0, 2) a is in N, or 3) -a is in N.
We then proved that square root of 2 is not in Z.
We created this list of axioms in this workshop in order to better our understanding of integers and so that we may use these axioms to prove other theorems and solve other problems involving integers.

****

Cicek:

On Tuesday's workshop, we have discussed properties of integers and worked on related proofs.
We have reminded ourselves the algebraic properties first, such as closure, associativity, commutativity, identity and inverse elements, distributivity, zero divisors, etc.
This workshop impressed me in a way that the things we knew about integers were a lot deeper than I've thought. I found it interesting that such simple cases like uniqueness of an additive inverse would be a proof to enjoy. After attending this workshop and solved related questions from the homework, I have realized that proofs require a lot more thinking than I have expected.
Overall, I think this was a very helpful workshop in terms of expanding my view on numbers.

****

David:

In workshop on Tuesday we characterized the integers by listing their properties; specifically, the ring axioms and the "trichotomy principle," i.e. that each integer is either zero, a natural number, or its inverse is a natural number. We then used these axioms to prove monotonicity for the natural number, i.e. given natural numbers a,b, then ab>=max(a,b), and that 1/2 is not an integer. The trichotomy principle is an important tool because it allows for the use of mathematical induction because it gives a recursive definition for natural numbers, i.e. 1 is in N and for any a in N, a+1 is in N. This lets us prove general statements about the natural numbers by showing that it is true for 1 and that, if it is true for any arbitrary a in N, it is true for a+1. Also, the axioms we listed define the integers, so all other properties of integers (e.g. Unique factorization, etc) can be proven just from the axioms.

****

Joe:

In the workshop, we discussed the general axioms of a commutative ring with identity. Then we constructed the natural numbers by the recursion theorem. After we had the naturals, we created the integers by taking the union of the naturals, the negation of each natural, and 0.

That construction of the integers is the only thing that differentiates our ring from a general commutative ring with identity.

Of course, we decided not to include 0 in the natural numbers, which is a personal pet peeve of mine, but I'm aware that in particular, number theory is where 0 isn't considered a natural number. I'm more used to set theory, where the Von Neumann construction of the natural numbers defines 0 to be the empty set, 1 to be the set containing the empty set, 2 to be the set containing 0 and 1, etc.

I also thought it was weird that we referred to the recursion theorem (the definition of N as the set containing 1, n + 1 for any n in N, and only those elements produced by the previous two rules) as the principal of mathematical induction. I suppose it's possible that the two are equivalent, but haven't thought about it much. Generally we state as an axiom that at least one inductive set exists (the axiom of infinity), after defining PMI and the resulting inductive set. I think it would be lot more difficult to prove that N is a set if we stated the recursion theorem as an axiom instead of a theorem, and then attempted to prove the axiom of infinity as a result.

****

Tina:

I also added an axiom number 11 myself and I wasn't sure if it was correct.
The goal for this workshop was to describe the integers (set Z)
We came up with the following axioms to define the properties of an integer:

0) we could add integers and get a third one (there is an operation "+") on Z
1) There is an additive identity (there is a neutral element with respect to addition)
2) Z is closed under multiplication
3) There exists a multiplicative identity 1

4) There are negative numbers (some of the integers are positive)
4a) 1 is in the set of natural numbers
4b)natural numbers are closed under addition and multiplication
4c)if n is in the natural set of numbers so is n+1
4d)the only numbers in N are the ones obtained from a and c
5) Every integer can be uniquely represented as a product of primes
6) For every a,b,c in Z : a(b+c)= ab+ac
7) "+" and "." are associative
7b) "+" and "." are commutative
8) There is a subtraction. For every a in Z there is an additive inverse
9) There are no zero divisors (ab=0 then either a=0 or b=0)
10) We say that if a>b if and only if a-b is in the set of natural numbers
11) any integer raised to the power of an integer is still an integer
-we mentioned that integers are a countably infinite set
-We also proved that an additive inverse of an integer is unique.
-We also proved that the square root of 2 is not an integer. It was a proof by contradiction. Our Lemma was that if a and b are in the natural set of numbers the a.b is bigger or equal to both a and b.
And then we went on to prove the Lemma that if ab is bigger than a then ab-a is in the natural set of numbers and if ab=a then b must equal one.