Discrete Mathematics lecture notes 1-2

September 5, 2013

2. More basic number theory (as a vehicle for proving stuff)

We now know what it means for the integer a to divide the integer b: There is some c such that $b = a \cdot c$, and we write $a|b$. We used this last time to define the notion of an integer's being even:

Definition 1. An integer a is *even* if $2|a$.

This is not a new notion, and neither is the next one we'll introduce, though a bit more care must be taken. We want to say what it means for an integer to be *odd*, but there are a number options we have to pick from. For this reason, we will introduce *three* notions of "odd."

Definition 2. Pick $a \in \mathbb{Z}$.

- a is *odd* if a is not even, i.e., $2 \nmid a$.
- a is *odder* if $2|a+1$.
- a is *oddest* if there is some $k \in \mathbb{Z}$ such that $a = 2k + 1$.[1]

Of course, we hope that there's no difference between odd, odder, and oddest, but *a priori* there may well be: This is something we have to *prove*. Before we jump into that, let's look a little closer at the danger of making definitions.

Giving a definition is easy. Giving a useful definition is hard.[2] There's nothing particularly noteworthy in that observation. What is noteworthy is a surprising way that a definition can turn out to be useless: It can be *vacuous*. This isn't saying that the definition is somehow stupid,[3] but that I have defined something that cannot exist. For example:

Definition 3. Pick $a \in \mathbb{Z}$.

- a is *surpassing strange* if a is both even and odd.
- a is *surpassing stranger* if a is both even and odder.
- a is *surpassing strangest* if a is both even and oddest.[4]

It should be fairly clear that there is no surpassing strange integer, as the definition of "odd" was "not even," and the set of integers that are simultaneously even and not even is empty.[5] So, while I can define "surpassing strange," the definition is vacuous, and I probably shouldn't.

However, it is not immediately clear that "surpassing stranger" and "surpassing strangest" are vacuous definitions: Maybe we could have some a such that $2|a$ and there is also a $k \in \mathbb{Z}$ with $a = 2k + 1$. Who's to say there isn't? Of course, once we show that "odd," "odder," and "oddest" are actually the same definition, the vacuity of "surpassing strange" will imply that of the other two as well.[6]

Ok, back on track. Let's see that there really is no difference in our varying degrees of oddicity. We will make use of the following Theorem, whose proof we postpone[7] in the interests of narrative flow:

Theorem 4 (Division in $\mathbb{N}$)**.** *Let $n, m \in \mathbb{N}$ be greater than 0. Then there exist unique $q, r \in \mathbb{N}$ with $0 \leq r < m$ such that*

$$n = mq + r.$$

[1] Of these, only the term "odd" is ever used. I'm just introducing fake definitions to illustrate a point.

[2] E.g., an integer a is *shiny* if $a = 12$ or $a = 97$ or $a = -7^{15} + 1$. Just because I *can* make a definition doesn't mean I *should*.

[3] Cf. "shiny."

[4] Again, I just made up these terms.

[5] This is actually part of the axioms that govern our *logic* or metamathematics: A statement and its negation cannot both be true. In some sense, this axiom is subject to tinkering, just like everything else we've introduced, but in this course we won't toy with the logical foundations of our mathematics. Also, we'll talk more about what I mean by "the set is empty" soon.

[6] Why?

[7] But will get to!

The naming of the natural numbers in the conclusion of this Theorem is meant to be suggestive: q for *quotient* and r for *remainder*. Indeed, this is just the precise version of saying that we can divide natural numbers to get a quotient and remainder.[8]

Let's state our main Theorem in a reasonably fancy way:

Theorem 5. *For $a \in \mathbb{Z}$, the following are equivalent:*

- *(i) a is odd.*
- *(ii) a is odder.*
- *(iii) a is oddest.*

Proof. First, the statement "the following are equivalent" is a fairly common one in the math world, to the extent that it sometimes abbreviated "TFAE." It means that there is no logical difference between the three statements (i), (ii), and (iii): If one of the three is true, so are the other two; conversely, if one is false, all are. We'll cover this point in more detail in the next class, but for now let's just note that it's enough to show that we have the following chain of implications: (i)$\Rightarrow$(ii)$\Rightarrow$(iii)$\Rightarrow$(i).

Assume that $a > 0$. Then, appealing to the Division in $\mathbb{N}$ Theorem (with a playing the role of n and 2 playing the role of m), there exist unique $q, r \in \mathbb{N}$ with $0 \leq r < 2$ such that

$$a = 2q + r.$$

The condition of r means that either $r = 0$ or $r = 1$.

(i)$\Rightarrow$(ii) If a is odd, then $2 \nmid a$, so there is no k such that $2k = a$. If $r = 0$, then setting $k = q$ would show that q is such a k, so we conclude $r = 1$.[9] Thus $a = 2q + 1$.

We want to show that $2|a + 1$. We have $a + 1 = (2q + 1) + 1 = 2q + 2 = 2(q + 1)$. As $q \in \mathbb{N}$, we have $q + 1 \in \mathbb{N}$ as well, which is the defining characteristic of $|$. Thus a is odder.

(ii)$\Rightarrow$(iii) If a is odder, then $2|a + 1 = (2q + r) + 1$. If $r = 0$, we'd have $2|2q + 1$, so there is some $k \in \mathbb{N}$ such that $2k = 2q + 1$. Rearranging, this gives $1 = 2k - 2q = 2(k - q)$. As $k, q \in \mathbb{N}$, we have $k - q \in \mathbb{Z}$. But the only integers with multiplicative inverses[10] are ± 1,[11] and this equation would imply that 2 has a multiplicative inverse in $\mathbb{Z}$, a contradiction. Thus we must have $r = 1$, and setting $k = q$ we conclude that a is oddest.

(iii)$\Rightarrow$(i) If a is oddest, then there is some $k \in \mathbb{Z}$ such that $a = 2k + 1$. We also have $a = 2q + r$, so equating these we get $2k + 1 = 2q + r$. Thus $2k - 2q = 2(k - q) = r - 1$ and $r - 1$ is even. If $r = 0$, then $r - 1 = -1$ is not even[12], so $r = 1$. If a were even, we'd again conclude that 2 has a multiplicative inverse in $\mathbb{Z}$[13], which would again be nonsense, so we conclude that a is not even. This is the definition of odd, and we're done.

□

Exercise. Note that the proof I gave for our main Theorem started with the assumption that $a > 0$. As the hypothesis of the theorem was simply that $a \in \mathbb{Z}$, this is *not* a complete proof: Finish the work.

[8] Explicitly, n divided by m has quotient q and remainder r.

[9] This is actually a mini argument by contradiction, as we'll get to below.

[10] In $\mathbb{Z}$!

[11] We haven't proved this fact yet, but we don't have to take it as an axiom, though it depends on another axiom we haven't discussed yet.

[12] Why? Look at the argument in the previous step.

[13] Fill in the steps here.

3. Proof by contradiction

The Proof of the main Theorem of the previous section was relatively involved for what we've seen so far, but on the macro level it was basically three "direct" proofs linked together. Each of these involved small examples of proofs by contradictions, true, but let us look at one big example to illustrate how this technique works.

Again, that this is a valid method of proof is actually an axiom of our logical system: If I assume a statement A and that implies something we know to be untrue, we must conclude that A is false. Equivalently, to prove that B is *true*, we can define a new statement $A =$"B is false," show that A implies something untrue, and conclude that A is false. But if A is false, "B is false" is false, or B is true.

Let's try to make this explicit with an example.

Definition 6. For $x \in \mathbb{R}$, we say that x is *rational* if there exist[14] integers $a, b \in \mathbb{Z}$ such that $b \neq 0$ and $x = \frac{a}{b}$. Denote the set of all rational numbers by $\mathbb{Q}$.

Conversely, we say that $x \in \mathbb{R}$ is *irrational* if x is not rational.

So clearly the definition "rational" is not vacuous,[15] but it's far from clear that there are any irrational numbers.[16]

Theorem 7. *There is some real number $x > 0$ such that $x^2 = 2$.*

Proof. Consider an isosceles right triangle with sides of length 1 and hypotenuse of length x. By the Pythagorean Theorem, $x^2 = 1^2 + 1^2 = 1 + 1 = 2$.[17] □

Notation 8. Pick some $x \in \mathbb{R}_{\geq 0}$[18] such that $x^2 = 2$, and denote it by $\sqrt{2}$.[19]

I don't feel like giving the same proof that $\sqrt{2} \notin \mathbb{Q}$ as I gave in class. Let's try something different.

Lemma 9. *Let R be the subset of real numbers that can be written $a + b\sqrt{2}$ for $a, b \in \mathbb{Z}$. Then R is closed under addition and multiplication, i.e., if $a + b\sqrt{2}$ and $a' + b'\sqrt{2}$ are two different elements of R, then $(a + b\sqrt{2}) + (a' + b'\sqrt{2}) \in R$ and $(a + b\sqrt{2}) \cdot (a' + b'\sqrt{2}) \in R$.*

Proof. We compute:

$$(a + b\sqrt{2}) + (a' + b'\sqrt{2}) = (a + a') + (b + b')\sqrt{2}$$

and $a + a', b + b' \in \mathbb{Z}$ by assumption that $a, a', b, b' \in \mathbb{Z}$. Similarly, we have

$$(a + b\sqrt{2}) \cdot (a' + b'\sqrt{2}) = (aa' + 2bb') + (ab' + a'b)\sqrt{2}$$

with both $aa' + 2bb'$ and $ab' + a'b$ integers. □

Theorem 10. *$\sqrt{2}$ is irrational.*

Proof. Suppose not, so there are integers $n, m \in \mathbb{Z}$, $m \neq 0$, such that $\sqrt{2} = \frac{n}{m}$. Then every element of R from the previous Lemma is of the form $\frac{a}{m}$ for some $a \in \mathbb{Z}$ by the rules of addition of fractions. In other words, we have that every element of R is rational and can be written with denominator m. In particular, there are only finitely many elements of R that are greater than 0 and less that 1: If $x \in R$ with $0 < x < 1$, then $x \in \left\{\frac{1}{m}, \frac{2}{m}, \ldots, \frac{m-1}{m}\right\}$.

[14] N.b.: We do *not* require uniqueness here.

[15] Why?

[16] According to legend, it was once so unclear that the one who first showed that $\sqrt{2}$ is irrational was drowned for his efforts. Let's follow his lead!

[17] If you're miffed that I'm using facts we haven't proved, don't worry: It's much worse than you think. The actual problem is that the term "real number" is something we haven't defined yet, and is a much more subtle concept than anything we've encountered up until this point. We will probably not get to a formal description of the real numbers in the course, so for now let us go back to antiquity and think of a positive real number as a length of a line segment. From this as our starting point, together with Euclid's Axioms for planar geometry, it is not that big to accept this proof as more or less rigorous.

[18] This is fairly standard notation for the set of real numbers that are greater than or equal to 0.

[19] Of course, there is only one such x, but we haven't proved that yet, have we?

I claim that there is at least one element of R that lives between 0 and 1. Consider: $\sqrt{2} \in R$ is such that $1 < (\sqrt{2})^2 = 2 < 4$. Thus $1 < \sqrt{2} < 2$, so $0 < -1 + \sqrt{2} < 1$, as claimed.[20] Thus, there is a *nonzero*, but *finite* number of elements of R that live between 0 and 1.

Let $x \in R \cap (0,1)$[21] be one such element. Then we have[22]

$$(0 < x < 1) \Rightarrow (0 < x^2 < x) \Rightarrow (0 < x^3 < x^2) \Rightarrow \ldots$$

where each new equality is formed by multiplying the previous by x in all places. Thus we have constructed an *infinite* collection of real numbers

$$1 > x > x^2 > x^3 > \ldots > 0.$$

But $x \in R$, and we saw in the previous Lemma that R is closed under multiplication. Thus $x^2 \in R$. And $x^3 \in R$. And so on.[23] But this means there is an infinite collection of elements of R that live between 0 and 1, contrary to our assumption that $\sqrt{2}$ is rational. □

This is a fairly involved example of proof by contradiction, but at the end of the day, the idea is the same for all of them. Compare the proof above to the one given in class to convince yourself that this is true, and also that there's more than one way to deny the consequent.

[20] We're making use of the *order relation* on $\mathbb{Q}$, which in turn comes from that of $\mathbb{Z}$, which comes from that of $\mathbb{N}$... which we'll talk about more soon enough.

[21] Note the new symbol $\cap$: This is the *intersection*, and just means those elements of R that also live in the interval $(0,1)$.

[22] Again, using the fact that multiplication of positive real numbers respects order.

[23] Induction!