Math 17
Winter 2015
Notes from January 7

A note on "Notes": These notes, not just today's but in general, are not complete transcriptions of everything we did in class. Instead, they are notes on a few things, often examples, the details of which I think it would be useful to see written out.

In class on Wednesday, January 5, we talked about Diophantine sets and Diophantine expressions.

Diophantine expressions:

A *Diophantine expression* is an expression of the form

$$(\exists x_1)(\exists x_2)\cdots(\exists x_n)\,(D(a_1,\ldots,a_k,x_1,\ldots,x_n)=0),$$

where D is a polynomial with unknowns $a_1,\ldots,a_k,x_1,\ldots x_n$ and integer coefficients. (Recall that "$(\exists x)\cdots$" means "there exists a natural number x such that $\cdots$.") Notice that the "$(D(a_1,\ldots,a_k,x_1,\ldots,x_n)=0)$" part is a Diophantine equation.

We might also write a Diophantine expression as

$$(\exists x_1)(\exists x_2)\cdots(\exists x_n)\,(D_L(a_1,\ldots,a_k,x_1,\ldots,x_n)=D_R(a_1,\ldots,a_k,x_1,\ldots,x_n)).$$

This is not the official form, but can easily be rewritten in the official form.

The unknowns in a Diophantine expression are separated into two classes, the $x_1,\ldots,x_n$ that appear in the "there exists…" parts ($\exists$ is called an *existential quantifier* and these are called *quantified variables*), and the $a_1,\ldots a_k$ that do not (which may be called *free variables*, because they are not quantified, or *parameters*[1]).

A Diophantine expression says that the k-tuple $(a_1,\ldots,a_k)$ (that is, the natural numbers $a_1,\ldots,a_k$ considered in that order) has some property. For example, we saw in class that

$$(\exists x)\,(b=a+1+x)$$

is another way to say $a<b$. Of course, this works only because we are restricting the range of our unknowns to natural numbers.

It is important to be clear that the expression $(\exists x)\,(b=a+1+x)$ is saying something about a and b, but *not* about x. Some people call the quantified variables $x_1,\ldots,x_n$ "dummy variables." An analogy is the integral $\int_a^b f(x)\,dx$, which means the same thing as $\int_a^b f(u)\,du$, and is telling us something about a and b (namely, the area under the graph of $f(x)$ above the interval with endpoints $x=a$ and $x=b$); x, or u, is a "dummy variable."

[1] We'll talk in class on Friday about why they are called parameters.

Diophantine sets:

A *Diophantine set* is a subset A of $\mathbb{N}^k$ that is defined by a Diophantine expression; that is, a set of the form

$$A = \{(a_1, \ldots, a_k) \mid (\exists x_1)(\exists x_2) \cdots (\exists x_n)(D(a_1, \ldots, a_k, x_1, \ldots, x_n) = 0)\}.$$

We say the Diophantine expression

$$(\exists x_1)(\exists x_2) \cdots (\exists x_n)(D(a_1, \ldots, a_k, x_1, \ldots, x_n) = 0)$$

defines the set A.

The set $A = \{(a, b) \mid a < b\}$ is Diophantine because it can be defined by the Diophantine expression $(\exists x)\,(b = a + 1 + x)$:

$$A = \{(a, b) \mid (\exists x)\,(b = a + 1 + x)\}.$$

To show the set

$$B = \{a \mid a \text{ is composite}\}$$

is Diophantine, we have to figure out how to say "a is composite" with a Diophantine expression. Since a is composite just in case a can be written as a product of two factors each of which is greater than 1 and less than a, we begin with

$$(\exists x)(\exists y)\,(1 < x < a \;\&\; 1 < y < a \;\&\; xy = a).$$

We then notice that if one factor is strictly between 1 and a ("strictly" means $1 < x < a$ rather than $1 \leq x \leq a$), then the other must be also, so we can simplify a little to get

$$(\exists x)(\exists y)\,(1 < x < a \;\&\; xy = a).$$

This is not yet a Diophantine expression, because $(1 < x < a \;\&\; xy = a)$ is not a Diophantine equation. However, $xy = a$ is a Diophantine equation, and we know how to say $1 < x$ and $x < a$ with Diophantine expressions. We rewrite

$$(\exists x)(\exists y)\,\big(1 < x \;\&\; x < a \;\&\; xy = a\big);$$

$$(\exists x)(\exists y)\,\big((\exists v)(x = 1 + 1 + v) \;\&\; (\exists w)(a = x + 1 + w) \;\&\; (xy = a)\big).$$

It will not change the meaning if we move the "$(\exists v)$" and "$(\exists w)$" outside the large parentheses, and rewrite "$1 + 1$" as "2":

$$(\exists x)(\exists y)(\exists v)(\exists w)\,\big((x = 2 + v) \;\&\; (a = x + 1 + w) \;\&\; (xy = a)\big).$$

This is almost right, except that inside the large parentheses we have, not a single Diophantine equation, but several Diophantine equations, all of which must be true. That is, we have a system of Diophantine equations.

Fortunately, we have already seen how to take a system of Diophantine equations and turn it into a single Diophantine equation with the same solutions. We'll use this method to rewrite our expression.

$$(\exists x)(\exists y)(\exists v)(\exists w)\left((x = 2 + v) \mathbin{\&} (a = x + 1 + w) \mathbin{\&} (xy = a)\right);$$

$$(\exists x)(\exists y)(\exists v)(\exists w)\left((x - (2 + v) = 0) \mathbin{\&} (a - (x + 1 + w) = 0) \mathbin{\&} (xy - a = 0)\right);$$
$$(\exists x)(\exists y)(\exists v)(\exists w)\left((x - (2 + v))^2 + (a - (x + 1 + w))^2 + (xy - a)^2 = 0\right).$$

Now we have a Diophantine expression meaning "a is composite," which proves B is Diophantine:

$$B = \{a \mid a \text{ is composite}\} =$$
$$\{a \mid (\exists x)(\exists y)(\exists v)(\exists w)\left((x - (2 + v))^2 + (a - (x + 1 + w))^2 + (xy - a)^2 = 0\right)\}.$$

There is actually an easier way to say a is composite. A natural number a is composite just in case it can be written as a product of two factors, each of which is greater than or equal to 2. A natural number b is greater than or equal to 2 just in case it can be written in the form $b = 2 + x$. Therefore, we can show B is composite by writing

$$B = \{a \mid a \text{ is composite}\} = \{a \mid (\exists x)(\exists y)\,((2 + x)(2 + y) = a)\}.$$

I chose not to show you this in class, because the way we did it in class illustrates some important techniques.

We are going to prove a general result about rewriting expressions. It will tell us that because we can rewrite "$1 < x$" and "$x < a$" as Diophantine expressions, it automatically follows that we can rewrite

$$(\exists x)(\exists y)\left(1 < x \mathbin{\&} x < a \mathbin{\&} xy = a\right),$$

as a Diophantine expression. This will save us from going through all this rewriting every single time.