Math 217
Winter 2015
Friday, January 9

Definitions:

1. A Diophantine expression is an expression of the form

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

where D is a polynomial with integer coefficients. In other words, a Diophantine expression is a Diophantine equation (possibly) preceded by some existential quantifiers.

We may write the Diophantine expression above as $(\exists \vec{x})\, (D(\vec{a}, \vec{x}) = 0)$.

2. A subset A of $\mathbb{N}^k$ is Diophantine if we can write

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

In other words, A is Diophantine if "$(a_1, \ldots, a_k) \in A$" can be rewritten as a Diophantine expression.

3. A property $\varphi(a_1, \ldots, a_k)$ of k-tuples of natural numbers is a Diophantine property if it can be rewritten as a Diophantine expression. If $k > 1$, we may also call this a Diophantine relation.

In particular, A is a Diophantine set iff "$\vec{a} \in A$" is a Diophantine property.

4. A function $f : \mathbb{N} \to N$ is a Diophantine function if "$f(a_1, \ldots a_k) = b$" is a Diophantine property.

5. A collection is *closed* under an operation or function if the result of applying that operation or function to members of the collection is always another member of the collection.

Some Examples:

1. $(\exists x)(ax^2 + bx + c = 0)$ is an example of a Diophantine expression. By replacing the free variables a, b, and c by specific natural numbers, we get a family of subproblems of Hilbert's Tenth Problem. The decision problem for this family is solvable (using the quadratic formula), even though Hilbert's Tenth Problem as a whole is not.

2. We showed in class on Wednesday that $\{(a, b) \mid a < b\}$ is Diophantine, because $a < b$ can be rewritten as $(\exists x)\,(b - (a + 1 + x) = 0)$.

3. Therefore, we showed that $a < b$ is a Diophantine property, or that $<$ is a Diophantine relation.

4. You showed in homework that the function $f : \mathbb{N} \to \mathbb{N}$, defined by setting $f(a)$ to be the remainder when a is divided by 4, is a Diophantine function, because "b is the remainder when a is divided by 4" can be rewritten using a Diophantine expression.

5. $\mathbb{N}$ is closed under the operations addition and multiplication and the functions $f(n) = n^2$ and $g(n, m) = n^m$, but not under the operations subtraction or multiplication or the functions $f(n) = \sqrt{n}$ or $g(n, m) = \text{average}(n, m)$.

Notes:

1. When we separate the unknowns of a Diophantine equation into *parameters* and *variables*, we are determining a *parametrized family* of Diophantine equations, each one obtained by replacing the parameters with specific natural numbers.

   For example, in the Diophantine equation $ax^2 + bx + c = 0$, we may choose to regard a, b, and c as parameters, and x as a variable. This determines the parametrized family of equations of the form $ax^2 + bx + c = 0$, where a, b and c are any natural numbers.

   You have encountered the terminology of parameters before. In Math 8, a *parametric* equation for a line is an equation $\vec{x} = \vec{x}_0 + t\vec{v}$, where $\vec{x}_0$ and $\vec{v}$ are specific vectors. (We think of $\vec{x}$ as representing the position of an object moving at a constant velocity, where t represents time, $\vec{x}_0$ the object's initial position, and $\vec{v}$ the object's velocity.) The unknown t is the parameter. Replacing t in $\vec{x} = \vec{x}_0 + t\vec{v}$ with a specific number gives a specific point on the line, just as replacing a, b and c in $ax^2 + bx + c = 0$ with specific integers gives a specific Diophantine equation in our family.

2. If $A \subseteq \mathbb{N}^k$ the decision problem for A is the problem: Given $(a_1, \ldots, a_k) \in \mathbb{N}^k$, determine whether or not $(a_1, \ldots, a_k) \in A$.

   The decision problem for a Diophantine set is a parametrized family of subproblems of Hilbert's Tenth Problem. Therefore, the decision problem for a Diophantine set A can be reduced to Hilbert's Tenth Problem.

   If we can find any Diophantine set whose decision problem is not solvable, it will follow that Hilbert's Tenth Problem is not solvable.

Proposition: Diophantine properties are closed under conjunction:

Proof:

Suppose $\varphi(\vec{a})$ and $\psi(\vec{a})$ are Diophantine properties of $\vec{a} = (a_1, \ldots, a_k)$. (This does not assume that every a_i is mentioned in both φ and ψ; we can call $a < b$ a property of (a, b, c) if we want to.)

This means we can write

$$\varphi(\vec{a}) \iff (\exists x_1) \cdots (\exists x_n)\, (D_1(\vec{a}, \vec{x}) = 0);$$

$$\psi(\vec{a}) \iff (\exists x_1) \cdots (\exists x_n)\, (D_2(\vec{a}, \vec{x}) = 0);$$

and

$$(\varphi(\vec{a})\ \&\ \psi(\vec{a})) \iff (\exists x_1) \cdots (\exists x_n)\, (D_1(\vec{a}, \vec{x}) = 0)\ \&\ (\exists x_1) \cdots (\exists x_n)\, (D_2(\vec{a}, \vec{x}) = 0)$$

$$\iff (\exists x_1) \cdots (\exists x_n)\, (D_1(\vec{a}, \vec{x}) = 0)\ \&\ (\exists y_1) \cdots (\exists y_n)\, (D_2(\vec{a}, \vec{y}) = 0)$$

$$\iff (\exists x_1) \cdots (\exists x_n)(\exists y_1) \cdots (\exists y_n)\, (D_1(\vec{a}, \vec{x}) = 0)\ \&\ (D_2(\vec{a}, \vec{y} = 0)$$

$$\iff (\exists x_1) \cdots (\exists x_n)(\exists y_1) \cdots (\exists y_n)\, ((D_1(\vec{a}, \vec{x}))^2 + (D_2(\vec{a}, \vec{y}))^2 = 0).$$

This is a Diophantine expression, so this completes the proof.

Note: It was important to change the names of the quantified variables before combining expressions.

$$(\exists x)\, (x \text{ is even})\ \&\ (\exists x)\, (x \text{ is odd})$$

does not mean the same thing as

$$(\exists x)\, (x \text{ is even }\ \&\ x \text{ is odd});$$

the first means that there is an even number and also there is an odd number, while the second means that there is a number that is both even and odd. However,

$$(\exists x)\, (x \text{ is even})\ \&\ (\exists x)\, (x \text{ is odd})$$

does mean the same thing as

$$(\exists x)(\exists y)\, (x \text{ is even }\ \&\ y \text{ is odd}).$$

Exercises:

Work together in class on these exercises. You can (and should) use the facts that Diophantine expressions are closed under conjunction (& or $\wedge$, meaning and), disjunction ($\vee$, meaning inclusive or), and existential quantification ($(\exists x)$, where x is any unknown, meaning there exists a natural number x).

Some relevant definitions are on the next page.

1. We have already shown that $a < b$ is Diophantine. Show that $a = b$, $a \leq b$, and $a \neq b$ are also Diophantine.

2. Show the function $f : \mathbb{N}^2 \to \mathbb{N}$, where $f(a, b)$ is the remainder when a is divided by $b+1$, is Diophantine, by showing that "c is the remainder when a is divided by $b+1$" can be rewritten as a Diophantine expression.

3. Show that the Diophantine functions from $\mathbb{N}^k$ to $\mathbb{N}$ are closed under addition; that is, if f and g are Diophantine functions, then so is $f + g$.

4. Show that the Diophantine functions from $\mathbb{N}$ to $\mathbb{N}$ are closed under composition.

5. Show that if $f : \mathbb{N}^2 \to \mathbb{N}$, $g : \mathbb{N}^3 \to \mathbb{N}$, and $h : \mathbb{N}^3 \to \mathbb{N}$ are Diophantine functions, so is $k : \mathbb{N}^2 \to \mathbb{N}$, where k is defined by

$$k(a, b, c) = f(h(a, b, c),\ g(a, b, c)).$$

6. State a more general form of the preceding exercise. You need not prove it — it should be clear that pretty much the same proof works.

7. Suppose that $\varphi(a, b)$ expresses a Diophantine property of (a, b), and $f : \mathbb{N}^3 \to \mathbb{N}$ is a Diophantine function. Show that $\varphi(a, f(b, c))$ is a Diophantine property of (a, b, c).

8. State the most general form of the above exercise that you can. Again, you need not prove it.