Math 17

Winter 2015

Written Exercises Assigned January 9

These exercises are due at the beginning of class on Friday, January 16.

This handout also includes solutions to some of the exercises we were working on in class, following the homework exercises.

Exercises:

1. Given two polynomials $D_1(a_1, \dots, a_k, x_1, \dots x_n)$ and $D_2(a_1, \dots, a_k, y_1, \dots y_m)$, show how to produce a single polynomial

$$D(a_1, \dots, a_k, x_1, \dots, x_n, y_1, \dots y_m)$$

   such that $D(a_1, \dots, a_k, x_1, \dots, x_n, y_1, \dots y_m) = 0$ if and only if we have

   $D_1(a_1, \dots, a_k, x_1, \dots x_n) = 0$ or $D_2(a_1, \dots, a_k, y_1, \dots y_m) = 0$ (or possibly both).

   (Hint: Given two numbers, how can you find a number that equals zero just in case at least one of the original two numbers does?)

2. Use the previous exercise to show that Diophantine properties are closed under disjunction (inclusive or; "φ or ψ" can be written "$(\varphi \vee \psi)$").

   Conclude that, for any given k, the Diophantine sets of dimension k are closed under union.

3. Do exercise 2 below.

4. Do exercise 3 below.

5. Do exercise 7 below.

Some Solutions from In-Class Exercises:

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

   Solution: We showed $a < b$ is Diophantine by rewriting it as a Diophantine expression, namely

$$a < b \iff (\exists x)\,(b - (a + 1 + x) = 0).$$

   We can do the same with $a \le b$,

$$a \le b \iff (\exists x)\,(b - (a + x) = 0),$$

and $a = b$ is already a Diophantine expression. For $a \neq b$, we can either rewrite $a \neq b$ explicitly as a Diophantine expression

$$a \neq b \iff (\exists x)\,((a-b)^2 - (x+1) = 0),$$

or we can rewrite it as a combination of things we have already shown to be Diophantine, together with operations under which Diophantine properties are closed; that is, conjunction (and, $\wedge$), disjunction (or, $\vee$), and existential quantification:

$$a \neq b \iff (a < b \ \vee \ b < a).$$

Note: Diophantine properties generally are *not* closed under negation (not, written $\neg$). We will eventually prove this.

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.

   Note: You do not have to do this explicitly; you can combine Diophantine properties using conjunction, disjunction, and existential quantification, as in our second argument that $a \neq b$ is a Diophantine property.

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.

   Solution: By the definition of closed, this means we must show that if f and g are Diophantine functions, so is their composition, $f \circ g$. Recall that $(f \circ g)(a) = f(g(a))$.

   Begin by assuming that f and g are Diophantine functions. That is $f(a) = b$ and $g(a) = b$ are Diophantine properties. We must show that $(f \circ g)(a) = b$, or $f(g(a)) = b$, is a Diophantine property.

   By changing the names of some parameters and using the fact that Diophantine properties are closed under conjunction, we can arrive at the Diophantine property

   $$g(a) = c \ \ \& \ \ f(c) = b.$$

   This is close to what we want — it implies that $f(g(a)) = b$ — but it is not a property of two numbers a and b, it is a property of three numbers a, b, and c.

   We can rewrite $f(g(a)) = b$ as a suitable combination of Diophantine properties by using an existential quantifier:

   $$f(g(a)) = b \iff (\exists x)\,(g(a) = x \;\&\; f(x) = b).$$

   This shows "$f(g(a)) = b$" is a Diophantine property, which shows $f \circ g$ is a Diophantine function, which is what we needed to show.

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 $k : \mathbb{N}^3 \to \mathbb{N}$, where k is defined by

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

   Idea: This is another way of combining Diophantine functions using composition. We can use the same trick as in the previous exercise, using one variable x for the value of $h(a, b, c)$ and a second variable y for the value of $g(a, b, c)$.

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.

   Solution: We want to say, loosely, that whenever we combine Diophantine functions using composition we get another Diophantine function. To be more precise:

   Suppose that $h : \mathbb{N}^k \to \mathbb{N}$ is a Diophantine function, and $g_1 : \mathbb{N}^n \to \mathbb{N}, \dots, g_k : \mathbb{N}^n \to \mathbb{N}$ are Diophantine functions. (We do not assume that the value of g_i depends on all its arguments; for example, in the case $n = 4$, we could have $g_1(a_1, a_2, a_3, a_4) = a_1 + a_3$.)

   Then the composition $h : \mathbb{N}^n \to \mathbb{N}$ defined by

$$h(a_1, \dots, a_n) = f(g_1(a_1, \dots, a_n), g_2(a_1, \dots, a_n), \dots, g_k(a_1, \dots a_n))$$

   is also a Diophantine function.

7. Suppose that $\varphi(a, b)$ expresses a Diophantine property of (a, b), and $f : \mathbb{N}^2 \to \mathbb{N}$ is a Diophantine function. Show that $\varphi(a, f(b, c))$ is a Diophantine property of (a, b, c).

   Note: For example, let $f(a, b)$ be the remainder when a is divided by $b+1$. We know that f is a Diophantine function, and $a \neq b$ is a Diophantine property. This exercise claims that therefore

$$a \neq f(b, c),$$

   or "the remainder when b is divided by $c + 1$ is not a," is also a Diophantine property (of the triple (a, b, c)).

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

   Solution: Suppose $\varphi(a_1, \dots, a_k)$ is a Diophantine property of $a_1, \dots, a_k$, and $f : \mathbb{N}^n \to \mathbb{N}$ is a Diophantine function. Then

$$\varphi(a_1, \dots, a_{i-1}, f(b_1, \dots, b_n), a_{i+1}, \dots a_k)$$

   (where there may be repetitions among the a_j and b_ℓ) is also a Diophantine property.

   That is, if $\varphi(a_1, \dots, a_k)$ expresses a Diophantine property, we can replace any of the free unknowns a_i by an expression for a Diophantine function $f(b_1 \dots, b_n)$ of any unknowns $b_1, \dots, b_n$ (which may include some of the a_j), and the result still expresses a Diophantine property.

Our textbook refers to an expression for a Diophantine function as a "Diophantine term." We could say that Diophantine properties are closed under substitution of Diophantine terms.

Note: By applying this repeatedly, we could replace any number of the a_j with Diophantine terms, and still have a Diophantine property.