Math 17
Winter 2015
Notes from January 5

In class on Monday, January 5, we talked about Diophantine equations, decision problems and computation problems, and reducing one problem to another.

Here is the example of reducing one problem to another that I gave in class, written up in more or less the level of detail I would expect in a homework assignment:

Problem A: Given a polynomial of the form $P(x) = ax^2 + bx + c$, determine whether $P(x)$ has rational roots.

Problem B: Given an integer n, determine whether n is a perfect square.

Each of these is a decision problem, because it consists of an infinite collection of subproblems, each specified by finitely much information, and requires an answer of YES or NO. For Problem A, the information required to specify a subproblem is the polynomial $ax^2 + bx + c$ (or the three integers a, b, and c), and for Problem B, it is the integer n.

Problem A can be reduced to Problem B. Here is an algorithm to solve Problem A, assuming there is an algorithm (which I will call Algorithm B) to solve Problem B:

1. Input $P(x) = ax^2 + bx + c$.
2. Compute the discriminant $d = b^2 - 4ac$.
3. Use Algorithm B to determine whether d is a perfect square.
4. If d is a perfect square, then answer YES, $P(x)$ has rational roots. If d is not a perfect square, then answer NO, $P(x)$ does not have rational roots.

Proof that this works: The quadratic formula tells us that the roots of $P(x)$ are given by $\dfrac{-b \pm \sqrt{d}}{2a}$, where d is the discriminant, $b^2 - 4ac$. Because $-b$ and $2a$ are integers, the roots are rational iff[1] the quantity $\sqrt{d}$ is rational. And, since d is an integer, $\sqrt{d}$ is rational iff d is a perfect square.

ADDITIONAL NOTES:

Exercise 1 of the homework assignment said you do not have to give a solution to your problems, just explain how one can be reduced to the other. However, in this example, it's not hard to give a solution to Problem B. Since we have already shown how to reduce Problem A to Problem B, that will also give a solution to Problem A.

Here is an algorithm to solve Problem B (written up in a different, but also acceptable, style):

[1] *Iff* means "if and only if." That is "A iff B" means "A if and only if B." Another way to say this is, "if A then B, and if B then A."

> Given an integer n, if $n < 0$ then answer NO, n is not a perfect square, and if $n = 0$, answer YES, n is a perfect square. If $n > 0$, compute the squares of the natural numbers, 0^2, 1^2, 2^2, 3^2, $\ldots$, until you reach a natural number k such that either $k^2 = n$ or $(k-1)^2 < n < k^2$. If $k^2 = n$, answer YES, n is a perfect square, and if $(k-1)^2 < n < k^2$, answer NO, n is not a perfect square.

The proof that the reduction of Problem A to Problem B is correct used a fact from number theory: If d is an integer that is not a perfect square, then $\sqrt{d}$ is not rational. Since we're going to be doing some number theory in this class, let's see how to prove this. We will use basic facts about writing natural numbers as products of primes.

To show that if d is not a perfect square then $\sqrt{d}$ is not rational, we can instead assume that $\sqrt{d}$ is rational and show that d must be a perfect square.[2] Suppose, then, that

$$\sqrt{d} = \frac{a}{b},$$

where a and b are integers.

Note that we must have $b \neq 0$, and if $a = 0$, then $d = 0$, so d is a perfect square and we have nothing more to prove. Therefore we can assume $a \neq 0$ as well. Because $\left(\frac{\pm a}{\pm b}\right)^2 = \left(\frac{a}{b}\right)^2$, if either a or b is negative, we can replace it with a positive number. Therefore, we can assume a and b are both positive.

Further, we can assume the fraction $\frac{a}{b}$ is written in lowest terms, so a and b have no prime factors in common.

Squaring each side of the equation $\sqrt{d} = \frac{a}{b}$, and multiplying each side by b^2, we get

$$db^2 = a^2.$$

Now, every prime factor of db^2 must also be a prime factor of a^2, so it must be a prime factor of a. If p were a prime factor of b, then it would be a prime factor of db^2, and therefore also a prime factor of a. But we wrote our fraction in lowest terms, so p cannot be a prime factor of both a and b. This means that p could not have been a prime factor of b after all.

Therefore, b has no prime factors. The only positive natural number with no prime factors is 1. Therefore, the equation $db^2 = a^2$ becomes $d = a^2$. That is, d is a perfect square, which is what we needed to prove.

[2] This is called *showing the contrapositive*. The contrapositive of "if A then B" is "if not B then not A." The statement "if A then B" and its contrapositive "if not B then not A" must either both be true or both be false; therefore, to prove the original statement, it suffices to prove the contrapositive.