Math 126 Number Theory

Prof. D. Joyce, Clark University

20 Mar 2006

Due Friday. Page 148: 1, 4, and page 151: 3, 7, 11.

Second test. Wednesday, March 8.

Quiz Today.

Last time. Finished the discussion on public-key cryptography and the RSA algorithm.

Next time. We won't finish the notes below today. Next time we'll start where we leave off and perhaps continue on with a detailed analysis of Pythagorean triples.

Today. Begin higher degree Diophantine equations in chapter 5. We've already completed the general theory of linear Diophantine equations. In chapter 5 we'll look at Pythagorean triples—mentioned in the introduction to the course—in more detail. We'll also consider the Fermat/Wiles theorem, at least the statement of it and some low degree cases of it, and discuss the Pell equation.

The statement of the Fermat/Wiles theorem. At our next meeting we'll solve the ancient problem of finding all the Pythagorean triples, the solutions to the Diophantine equation

$$x^2 + y^2 = z^2.$$

Euclid describes these solutions in X.29 of his *Elements*, but they were probably all known to the Greek mathematicians before him. Indeed, they were known to the ancient Babylonians over a millennium before that.

The solution to this Pythagorean triples equation was also included by Diophantus a few centuries after Euclid in Diophantus' *Arithmetic*. This seems to have been the inspiration for Fermat to generalize the problem. He likely began with the analogous equation in three dimensions

$$x^3 + y^3 = z^3.$$

That equation asks what two cubes with integer side lengths x and y have a combined volume equal to that of another cube with integer side length z? It is likely that Fermat had a proof that there were no solutions. (Naturally, he only accepted a solution where all three integers were positive.) Fermat then went on to look at higher powers than 3. He did have a proof for the case $n = 4$, and he concluded that there were no solutions to

$$x^n + y^n = z^n$$

for any $n > 2$. It's unlikely he had a general proof, but he might have had partial proofs that convinced him, and he wrote in the margin of his copy of Diophantus' *Arithmetic* that he could prove it, but the margins were too small to hold his proof.

After Fermat's death, his son published his works and included that statement from the margin. For the next three hundred years, partial progress was made on the proof of Fermat's last theorem, also called Fermat's conjecture, but it wasn't until the 1990s that a complete proof, a proof by Wiles, was constructed.

Preliminary note on the Fermat equation $x^n + y^n = z^n$. In order to prove there are no solutions for all $n > 2$, it's enough just to consider certain of these n. For instance, if we know there are no solutions when $n = 3$, then we can conclude that there are no solutions for $n=6$ because a solution for $x^6+y^6=z^6$ provides one for $n=3$, namely $(x^2)^3+(y^2)^3=(z^2)^3$. Generally speaking, if there are no solutions for n, then there are no solutions for any multiple of n.

That implies that we only need to consider n that are odd primes and $n=4$. On another day, we'll look at Fermat's proof for $n=4$.

Euler's conjecture. Euler stated a conjecture 1778 that generalized Fermat's, namely, for $n>2$ no n^{th} power is the sum of fewer than n n^{th} powers. So, for instance, it takes at least three cubes to sum to a cube, and at least four fourth powers to sum to a fourth power.

Just as Fermat's conjecture was suspected to be true, so was Euler's stronger conjecture. But it turned out to be false. In 1966 Lander and Parkin used a computer search to find a counterexample when $n=5$. They found a solution to

$$v^5+w^5+x^5+y^5=z^5,$$

namely

$$27^5+84^5+110^5+133^5=144^5.$$

In number theory, and in mathematics in general, a statement cannot be accepted as true until it's proved, and the proof must be general. On the other hand, to show that a general statement is false, it is enough to give one counterexample, as Lander and Parkin did for Euler's conjecture.

Diophantine equations and homogeneous equations. By a *Diophantine equation* we mean a polynomial equation in one or more variables where the acceptable solutions are limited to integers, sometimes just to positive integers. On occasion, we'll also accept rational numbers—as Diophantus did—but we can convert the problem of finding rational solutions to an algebraic equation to a problem of finding integral solutions to an associated equation with one more unknown.

For example, suppose we wanted to find all the rational solutions to the equation

$$3x^2+xy=14.$$

If (x,y) is a rational solution, then we could write that solution as $(x,y)=(s/u,t/u)$ where u is a common denominator of the rational numbers x and y. Then the equation becomes

$$3\left(\frac{s}{u}\right)^2+\left(\frac{s}{u}\right)\left(\frac{t}{u}\right)=14.$$

Clearing the denominators simplifies the equation to

$$3s^2+st=14u^2.$$

Now we can see that rational solutions (x,y) to the original equation correspond to integral solutions (s,t,u) of this new equation.

One property of this new equation is that all the terms have the same degree; in the example, that degree is 2. A polynomial equation all of whose terms have the same degree is called a *homogeneous equation.* The process we just went through "homogenizes" the equation. Many of the interesting Diophantine equations are homogeneous equations.

Factoring an equation to solve it. Not all equations factor, but if they can be, then that's one way to solve them. For example, let's find all the positive solutions for the cubic Diophantine equation

$$x^3-y^3=19.$$

Before beginning, we can see that for any positive solution, x has to be greater than y.

You recall that there is a formula to factor the difference of two cubes. It's

$$x^3-y^3=(x-y)(x^2+xy+y^2).$$

We can rewrite our equation as

$$(x-y)(x^2+xy+y^2)=19.$$

Now $x-y$ is positive, so the only two possible values that $x-y$ can have are 1 and 19, because those are the only positive factors of 19.

Case 1: Suppose $x-y=1$. Then

$$x^2+xy+y^2=19.$$

Replacing x by $y+1$, we see $(y+1)^2+(y+1)y+y^2=19$, which simplifies to the equation $3y^2+3y+1=19$, which further simplifies to

$$y^2+y=6.$$

The only positive solution to that equation is $y=2$, in which case, $x=3$.

Case 2: Suppose $x-y=19$. Then $x^2+xy+y^2=1$. But the sum of three positive integers has to be greater than one, so there are no solutions in case 2.

Thus, the only solution to the original equation $x^3-y^3=19$ is $(x,y)=(3,2)$.

Pell equations. These are the quadratic Diophantine equations of the two forms

$$x^2-dy^2=\pm 1$$

where d is a fixed integer. They're misnamed for Pell who didn't work with them. They occurred in the works in ancient Greeks, medieval India, and Fermat also considered them.

They come up in the rational approximation of the square root of d. If you have a solution to one of them, you know

$$|x^2-dy^2|=1.$$

Divide the equation by y^2 and take square roots of both sides. Then

$$\left|\frac{x}{y}-\sqrt{d}\right|=\frac{1}{y}.$$

In other words, x/y is a close approximation to $\sqrt{d}$.

Perhaps the first example

$$x^2-2y^2=\pm 1$$

comes from the ancient Greek approximations for $\sqrt{2}$. See my commentary on proposition II.10 of Euclid's *Elements.*

Using congruences in solving Diophantine equations. Sometimes you can show a Diophantine equation has no solutions using congruences, and sometimes you can use congruences to go partway in finding the solutions. One important theorem for Pell equations uses this technique.

Theorem. The Pell equation

$$x^2-dy^2=-1$$

has no solutions either when 4 divides d or when a prime p divides d where p is congruent to 3 modulo 4.

Proof: Let's first take the case when 4 divides d. Take the equation modulo 4. We get the congruence

$$x^2-dy^2\equiv -1 \pmod 4,$$

but $d\equiv 0 \pmod 4$, and $-1\equiv 3 \pmod 4$, so the congruence simplifies to

$$x^2\equiv 3 \pmod 4.$$

We know that x^2 is always congruent to either 0 or 1 modulo 4, never to 2 or 3, so this congruence is never satisfied. Since the congruence has no solutions, neither does the original equation.

Now let's look at the other case, when some prime p, congruent to 3 modulo 4, divides d. This time, take the equation modulo p. Then

$$x^2-dy^2\equiv -1 \pmod p.$$

Since $d\equiv 0 \pmod p$, that congruence simplifies to

$$x^2\equiv -1 \pmod p.$$

But that congruence doesn't have any solutions, as we'll prove in a moment in a separate theorem.

Thus, in neither case does that Pell equation have a solution. Q.E.D.

Now we need to prove the promised theorem. It should logically come before the theorem we just proved. To keep from making a circular argument we just have to make sure we don't use the preceding theorem in the proof.

Theorem. When a prime p is congruent to 3 modulo 4, then the congruence

$$x^2\equiv -1 \pmod p$$

has no solutions.

Proof: When $p \equiv 3 \pmod 4$, then 4 does not divide $p-1$, but 2 does divide $p-1$. Therefore, the greatest common divisor of $p-1$ and 4 must be 2.

Now suppose that x is a solution to the congruence $x^2 \equiv -1 \pmod p$. Then $x^4 \equiv 1 \pmod p$. From Fermat's theorem, we know that $x^{p-1} \equiv 1 \pmod p$. Since x raised to both the powers 4 and $p-1$ is congruent to 1 modulo p, therefore x raised to their greatest common divisor is also congruent to 1 modulo p. But their GCD is 2. Hence

$$x^2 \equiv 1 \pmod p.$$

That's impossible since $1 \not\equiv -1 \pmod p$. Therefore, there are no solutions to the congruence $x^2 \equiv -1 \pmod p$. Q.E.D.