Lecture 10 (19 June 2008)

The Brave New World of p-adic Numbers

Equations and Congruences. In this last lecture we return back to our first topic, the solutions of Diophantine equations, and take a look from a somewhat different perspective. We have used congruences to a great effect in showing that a given Diophantine equation has no solutions. This was based to the simple observation:

Observation. If a Diophantine equation $P(x_1, \ldots, x_n) = 0$ has a solution, then the congruence $P(x_1, \ldots, x_n) \equiv 0 \pmod{m}$ has a solution for each $m \in \mathbb{N}$.

So in a lot of examples we were able to show that an equation has no solutions by exhibiting a modulus for which the congruence has no solutions. For example, there are no $x, y, k \in \mathbb{Z}$ such that $x^2 + y^2 = 4k + 3$, since the congruence $x^2 + y^2 \equiv 4k + 3 \pmod{4}$ has no solutions. The difficult part here is guessing the modulus m for which the congruence will have no solutions. For a particular $m \in \mathbb{N}$ it is simple to figure out whether a congruence has a solution or not: there are only finitely many possibilities to try, and one could readily check them all.

One may ask, in the cases where we were unable to find a modulus m to do the work, was it that we haven't tried hard enough? Or, to put it in another way:

Question. If a Diophantine equation $P(x_1, \ldots, x_n) = 0$ has no solutions, is there a modulus m, for which the congruence $P(x_1, \ldots, x_n) \equiv 0 \pmod{m}$ has no solutions?

This the question that we will investigate in this section. We will first look at the one variable case, and try to find a polynomial $P(x)$, for which the equation $P(x) = 0$ has no solutions, but the congruences $P(x) \equiv 0 \pmod{m}$ has a solution modulo every given $m \in \mathbb{N}$.

We start by observing that it is enough to show solutions for modules m that are powers of primes. Indeed, imagine that we have shown that the congruence $P(x) \equiv 0 \pmod{p^N}$ has solution $x_{p,N}$ for every prime p and every exponent $N \in \mathbb{N}$. Let $m \in \mathbb{N}$ be arbitrary. We could factor it as $m = p_1^{e_1} \ldots p_k^{e_k}$. By the Chinese Remainder Theorem, we could choose an $x \in \mathbb{N}$ which satisfies the k congruences $x \equiv x_{p_i, e_i} \pmod{{p_i}^{e_i}}$, $1 \leq i \leq k$. By its choice then x will satisfy the k congruences $P(x) \equiv 0 \pmod{{p_i}^{e_i}}$, and therefore $P(x) \equiv 0 \pmod{m}$.

Before considering modules of the type p^N, we look simply at primes. Linear equations that are solvable modulo every prime are also solvable in integers by the criterion for solvability of Linear Diophantine equations, so we look at the next simplest case, that of quadratic equations. The equation $x^2 + 1 = 0$ has no integral solutions, but we know that the congruence $x^2 + 1 \equiv 0 \pmod{p}$ is solvable for each prime $p \equiv 1 \pmod{4}$ by the first part of the Law of Quadratic Reciprocity, which says $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$. The congruence also has a solution $x = 1$ modulo $p = 2$. So if we could find an integer a, such that $\left(\frac{a}{p}\right) = 1$

for primes $p \equiv 3 \pmod 4$, then the congruence $(x^2+1)(x^2-a) \equiv 0 \pmod p$ will have a solution modulo every prime number p. There is no such a which is not a perfect square; however, we could go a step further and notice that the primes $p \equiv 3 \pmod 4$ are in one of the two categories: $p \equiv 3 \pmod 8$ or $p \equiv 7 \pmod 8$. Let p be a prime in the second of the above categories. Then we know that $\left(\frac{2}{p}\right) = 1$, so the congruence $x^2 - 2 \equiv 0 \pmod p$ is solvable. For a prime in the first category, both $\left(\frac{2}{p}\right) = -1$, and $\left(\frac{-1}{p}\right) = -1$, so $\left(\frac{-2}{p}\right) = 1$, so the congruence $x^2 + 2 \equiv 0 \pmod p$ is solvable for such primes. Putting it all together, we see that the congruence

$$(x^2+1)(x^2-2)(x^2+2) \equiv 0 \pmod p$$

has a solution for every prime number p. The respective equation has no integral solutions, since none of $\sqrt{-1}, \sqrt{2}, \sqrt{-2}$ is an integer.
Next, we go from a prime module p to a power p^N. We do this for a numerical example first. Take the prime $p = 7$. Then, the middle factor is the one that has a solution, for $x^2 \equiv 2 \pmod 7$ we could take $x = 3$ or $x = -3$. Let a_1 be one of these choices, and to be specific, let $a_1 = 3$. We show that there are is an infinite sequence, $a_1, a_2, a_3, \ldots$, such that $a_N^2 \equiv 2 \pmod{p^N}$ for any $N \geq 2$, and moreover for that sequence $a_N \equiv a_{N-1} \pmod{p^{N-1}}$. The other choice for a_1 will lead to a second sequence with the same properties.
Let us look at $x^2 \equiv 2 \pmod{7^2}$, and assume it has a solution a_2. Then $a_2^2 \equiv 2 \pmod{7^2}$ implies $a_2^2 \equiv 2 \pmod 7$, so $a_2 \equiv \pm 3 \pmod 7$, and we could choose $a_2 \equiv a_1 \equiv 3 \pmod 7$. Then $a_2 = 3 + 7t_2$ for some $t \in \mathbb{N}$, and the congruence for a_2 simplifies to

$$a_2^2 - 2 \equiv (3+7t_2)^2 - 2 \equiv 9 + 42t_2 + 49t_2^2 - 2 \equiv 7 + 42t_2 \pmod{49}.$$

There are two things to notice: first, this is not anymore a quadratic congruence for t_2, but linear, and second, it is now, after the possible division by 7, a congruence modulo $p = 7$. Solving it, we find $t_2 \equiv 1 \pmod 7$ which gives $a_2 = a_1 + 7 * 1 = 10$.
We go the to the next step, and look for a_3, such that $a_3^2 \equiv 2 \pmod{7^3}$ and $a_3 \equiv a_2 \pmod{7^2}$.
Then $a_3 = a_2 + 49t_3$ and hence

$$a_3^2 - 2 \equiv (10+49t_2)^2 - 2 \equiv 100 + 2*10*49t_3 + 7^4 t_3^2 - 2 \equiv 98 + 2*10*49*t_2 \pmod{7^3}.$$

Again, we get a linear congruence for t_3, which is solvable, because of the choice of a_3, $49 | a^2 - 2 = 98$ and the congruence simplifies to the congruence $2 + 20t_3^2 \equiv 0 \pmod 7$, for which $t_3 = 2$ is a solution. So we get

$$a_3 = a_2 + 49 * 2 = 3 + 1 * 7 + 2 * 7^2 = 108.$$

and $108^2 - 2 = 11662 = 34 * 343$ so $a_3^2 \equiv 2 \pmod{7^3}$, as expected.
We could keep on in the same fashion, and get

$$a_4 = a_3 + 7^3 * 6 = 3 + 1*7 + 2*7^2 + 6*7^3,\ a_5 = a_4 + 7^4 = 3 + 1*7 + 2*7^2 + 6*7^3 + 1*7^4$$

and so on, where each a_N satisfies $a_N \equiv a_{N-1} \pmod{7^{N-1}}$ and $a_N^2 \equiv 2 \pmod{7^N}$. This procedure, which allows us starting from a solution modulo a prime number, to build solutions modulo arbitrary powers of this prime, will work for primes other than 7, as well, as follows from the following statement, which is a special case of an important theorem, known as *Hensel's Lemma:*

Proposition. Let $x^2 \equiv a \pmod{p}$ has a solution a_1 modulo the odd prime number p. Then there exists a sequence of integers $a_2, a_3, \ldots$ such that for each $i \in \mathbb{N}$ the following two properties hold:

i) $a_{i+1} \equiv a_i \pmod{p^i}$;

ii)$a_i^2 \equiv a \pmod{p^i}$.

Applying this propositions gives us what we want, or at least almost: The congruence

$$(x^2+1)(x^2-2)(x^2+2) \equiv 0 \pmod{p^N}$$

is solvable for every odd prime number p and every exponent N. The piece that is missing is solvability modulo high powers of 2. The given congruence is not solvable modulo 8. But we could deal with by adding one more multiplier: we let the reader check that $x^2 + 7 \equiv 0 \pmod{2^N}$ has a solution for every $N \geq 1$, so we could claim that the congruence

$$(x^2+1)(x^2-2)(x^2+2)(x^2+7) \equiv 0 \pmod{m}$$

has a solution for every $m \in \mathbb{N}$, while the Diophantine equation $(x^2+1)(x^2-2)(x^2+2)(x^2+7) = 0$ clearly has no solutions in integers.

Nevertheless, the statement "$P \equiv 0 \pmod{m}$ has solutions m implies the equation $P = 0$ has integral solution" is not totally lost. In fact there are large classes of multi-variable polynomials P, for which such a statement is true, when one asks in addition to the solvability of the congruences that that $P = 0$ has also real solutions. Such types of statements are known as *Minkowski-Hasse local-to-global principles.*

p-adic numbers. The German mathematician Kurt Hensel, based on the lemma we referred to above, invented a new kind of numbers.

Definition. Given a prime p, a p-adic integer is an infinite sequence of integers $a_1, a_2, \ldots$, such that for each $N \in \mathbb{N}$, $a_{N+1} \equiv a_N \pmod{p^N}$.

We recognize that the sequence $3, 10, 108, \ldots$ from the example in the previous section is a 7-adic number.

It might seem strange and first to think about number as being a sequence, but than this is exactly how we define also real numbers - as sequences of decimal approximations. To make this analogy even more visible: a real number has a decimal expansion, say

$$\sqrt{2} = 1.41421\cdots = 1 + 4 * \frac{1}{10} + 1 * \frac{1}{100} + 4 * \frac{1}{1000} + \ldots$$

and a p-adic number has a p-adic expansion

$$\sqrt{2}_7 = 3 + 1 * 7 + 2 * 7^2 + 6 * 7^3 + 7^4 + \ldots$$

so we could give a new, equivalent definition:

Definition. Given a prime p, a p-adic integer is a formal sum
$\alpha = d_0 + d_1 * p + d_2 * p^2 + d_3 * p^3 + \ldots,$
such that $0 \leq d_{i-1} \leq p - 1$ for each $i \geq 0$.

If one wants to use the the language of mathematical analysis, that one could say that in the same way that the set of real numbers is a completion of the rational numbers with respect to the standard, Euclidean metric, the p-adic numbers are a completion of the rational numbers with respect to the unique metric on the rational numbers for which to numbers are close when their difference is divisible to a high power of the prime p.
The p-adic integers could be added and multiplied together, so they provides us with another example of a ring. Every "usual" integer is also a p-adic integer, for any prime p; it has the property that the sequence that defines it is constant from a point onward, or equivalently, that the formal sum that correspond to them has only zero digits after some point.
The definition of p-adic numbers make the following proposition a tautology

Proposition. Let p be a fixed prime. The congruence $P(x) \equiv 0 \pmod{p^N}$ has a solution for every exponent N if and only if the equation $P(x)$ has a solution in p-adic numbers.