MATH 115, SUMMER 2012
LECTURE 10

JAMES MCIVOR

- MAIN THEME of the course: if $f(x)$ is an integer polynomial, how can we solve the congruence $f(x) \equiv 0 \mod m$?

The Chinese Remainder Theorem is a powerful tool for this. We saw in the previous theorem that it allows us to reduce the task of solving

$$f(x) \equiv 0 \mod m$$

to that of solving

$$f(x) \equiv 0 \mod p^r$$

for the various primes p and their powers r occurring in the factorization of m.

– go over how to do this –

Example 0.1. Solve $f(x) = 64x^7 + 15x^4 + 5x^2 + x + 1 \equiv 0 \mod 288$.

First factor $288 = 32 \cdot 9 = 2^5 \cdot 3^2$.

Since 32 and 9 are coprime, if we have a solution a mod 32 and a solution b mod 9, we can find a solution mod 288 by solving the system

$$x \equiv a \mod 32$$
$$x \equiv b \mod 9$$

But how do we get solutions mod 32 and 9? We figure out how today.

Notice here it's easy to get solns mod 2 and 3:

- mod 2 we have $f(x) \equiv x^4 + x^2 + x + 1 \equiv x + x + x + 1 \equiv x + 1$. There are only two choices for x mod 2, and only $x = 1$ works.

- mod 3 we have $f(x) \equiv x^7 + 2x^2 + x + 1 \equiv x + 2 + x + 1 \equiv 2x$, so $x = 0$ is the only solution.

- this only works because the primes are small,

- how to get from solutions mod p to solutions mod p^k, eg, from mod 2 to mod 32? This is what Hensel's lemma does.

1. Hensel's Lemma

Theorem 1 (Hensel's Lemma)**.** *Let $f(x)$ be a polynomial with integer coefficients, p be a prime, and suppose a is a solution of the congruence $f(x) \equiv 0 \mod p^j$ such that $f'(a) \not\equiv 0 \mod p$. Then there exists an integer t (which is unique mod p) such that $a + tp^j$ is a solution to the congruence $f(x) \equiv 0 \mod p^{j+1}$.*

In English, it say that if we have a solution mod p, we get a unique solution mod p^2; if we have a solution mod p^2, we get a solution mod p^3, etc. So all we need to do is find a solution mod p and let Hensel's lemma do the rest!

It's important to understand this proof, since then you can mimic the argument to do some actual computations. We'll just do the simple case when $j = 1$. In general, the argument is the same.

Proof. - Assume a is a soln mod p.

- Write out Taylor series for $f(a+tp)$, then reduce it mod p^2.

- Prove that all terms except the first two drop out. Reason: $f^{(k)}(a)/k!$ is an integer for each $1 < k \leq n$.

- So now we have

$$f(a+tp) \equiv f(a) + tpf'(a) \mod p^2$$

and we set this congruent to zero and try to solve for t.

- $f(a) \equiv 0 \mod p$ implies $p|f(a)$

- So divide the congruence (and the modulus!) by p.

- Get

$$\frac{f(a)}{p} + tf'(a) \equiv 0 \mod p$$

- $f'(a) \neq 0$, so it's a unit. Write its inverse $f'(a)^{-1}$ (this is a number mod p).

- Put this back into our original set-up. The root a_2 mod p^2 which we wanted has the form

$$a_2 = a + tp = a - f(a)f'(a)^{-1}$$

In general, we will start with a root $a_1 = a$ (I use the subscript 1 for consistency of notation). This gives a root $a_2 = a_1 - f(a_1)f'(a)^{-1} \mod p^2$, this gives a root $a_3 = a_2 - f(a_2)f'(a)^{-1}$, etc. The recursive formula for the root a_n mod p^n is

$$a_n = a_{n-1} - f(a_{n-1})f'(a)^{-1}$$

Notice that the term $f'(a)^{-1}$ is always the same. □

2. Algebraic Interpretation

Recall that there is a homomorphism $\mathbb{Z}/p^2 \to \mathbb{Z}/p$, given by reducing mod p. For example, if $p = 2$, we can consider $\mathbb{Z}/4 \to \mathbb{Z}/2$. It sends 0 to 0, 1 to 1, 2 to 0, and 3 to 1.

Similarly, there are maps $\mathbb{Z}/p^j \to \mathbb{Z}/p^{j-1}$ for each $j > 1$. So we have a chain of homomorphisms

$$\begin{array}{c} \vdots \\ \mathbb{Z}/p^3 \\ \downarrow \\ \mathbb{Z}/p^2 \\ \downarrow \\ \mathbb{Z}/p \end{array}$$

If we look at an element $a \in \mathbb{Z}/p$, we can ask how many things in $\mathbb{Z}/p^2$ get sent to a under this map? In other words, how many preimages does it have? The answer is p. If we have an element b in $\mathbb{Z}/p^2$ which reduces to a mod p, we say b **lies above** a - that's the reason I wrote the maps vertically. Some people also say that we can **lift** a to b.

Some more terminology: Let a be a root of f mod p^j, i.e., $f(a) \equiv 0 \mod p^j$. We call a a **nonsingular** root if $f'(a) \not\equiv 0 \mod p$ (note the modulus for the derivative is p, but the modulus for the root may be a higher power of p). Otherwise it's called a singular root.

Now we can state Hensel's lemma concisely:

Theorem 2 (Hensel's Lemma, Concise Version)**.** *Nonsingular roots lift uniquely.*

3. Using Hensel

Example 3.1. Find all solutions to the congruence $5x^3 + x^2 - 1 \equiv 0 \mod 125$.

(1) Note that $125 = 5^3$ is a prime power, and that the cubic term drops out mod 5 (good news!)
(2) Solve it mod 5 - two roots, 1 and 4
(3) Check for nonsingulartiy. $f'(x) = 2x \mod 5$, so both are nonsingular.
(4) lift the first root, $a = 1$. The first step is to find the inverse to $f'(a)$ mod 5. For $a = 1$, $f'(a) = 2$, whose inverse mod 5 is 3. We call the root a mod 5 a_1, which is considered mod 5, and first lift to a_2, a number mod 5^2:

$$a_2 = a_1 - f(a_1)f'(a)^{-1} = 1 - 5 \cdot 3 = -14 \equiv 11 \mod 25$$

We lift again:

$$a_3 = a_2 - f(a_2)f'(a)^{-1} = 11 - (5 \cdot 1331 + 121 - 1) \cdot 3 = 11 - 6775 \cdot 3 = -20314 \mod 125$$

This number is very large, but we can replace it by something smaller mod 125 by using long division: $-20314 = -162 \cdot 125 - 64 \equiv -64 \equiv 61 \mod 125$, so our desired root mod 125 is 61.