SOLUTIONS TO POLYNOMIAL CONGRUENCES (MA2316, FIFTH WEEK)

VLADIMIR DOTSENKO

Last week, we figured out how to solve quadratic equations modulo primes, or at least how to figure out whether a quadratic equation has solutions. Indeed, a general quadratic congruence

$$ax^2 + bx + c \equiv 0 \pmod{p}$$

has solutions if and only if its discriminant $b^2 - 4ac$ is a square modulo p, as the formula for roots of quadratic equations (which makes sense over any field) tells us. (To be completely precise, this formula is not applicable for $p = 2$, since it has 2 in the denominator, but solving equations modulo 2 is easy enough by inspection, since the corresponding field consists of just two elements). We shall now address solutions to polynomial congruences modulo any integer n, and then discuss a topic in number theory which is naturally related to that, the p-adic numbers.

First of all, let us remark that it is sufficient to figure out how to solve congruences modulo prime powers. For if $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ is a prime decomposition of n, then of course for each polynomial $f(t)$ we have (for any x modulo n)

$$f(x) \equiv 0 \pmod{n} \quad \text{if and only if} \quad \begin{cases} f(x) \equiv 0 \pmod{p_1^{a_1}}, \\ f(x) \equiv 0 \pmod{p_2^{a_2}}, \\ \cdots \\ f(x) \equiv 0 \pmod{p_k^{a_k}}. \end{cases}$$

However, if x_i is a solution to $f(t) \equiv 0 \pmod{p_i^{a_i}}$ for each $i = 1, \ldots, k$, then the Chinese Remainder Theorem guarantees that there exists a unique x modulo n such that

$$\begin{cases} x \equiv x_1 \pmod{p_1^{a_1}}, \\ x \equiv x_2 \pmod{p_2^{a_2}}, \\ \cdots \\ x \equiv x_k \pmod{p_k^{a_k}}, \end{cases}$$

and therefore by above congruences $f(x) \equiv 0 \pmod{n}$. We just proved the following

Theorem 1. *If $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$, and $f(t)$ is a polynomial modulo n, then the number of solutions to the congruence $f(t) \equiv 0 \pmod{n}$ is equal to the product of numbers of solutions to congruences $f(t) \equiv 0 \pmod{p_i^{a_i}}$.*

It remains to deal with the case of a prime power p^m. Of course, in order to be able to solve a congruence modulo p^m, one has to be able to solve it modulo p. In the case of quadratic equations, we learned how to do that; in the case of polynomials of higher degrees there are certain methods, although less powerful. We however shall assume that we can handle the case of congruences modulo p, and describe a process of "amelioration", or "lifting" of solutions to solutions modulo higher powers. The key ingredient is the following result, often referred to as "Hensel's Lemma":

Theorem 2. *Let $f(t)$ be a polynomial modulo p^{n+1}. Suppose that for some x modulo p^n we have*

- *$f(x) \equiv 0 \pmod{p^n}$,*
- *for some k such that $0 \leq 2k < n$ we have $f'(x) \equiv 0 \pmod{p^k}$ but $f'(x) \not\equiv 0 \pmod{p^{k+1}}$.*

Then there exists y modulo p^{n+1} such that

- $f(y) \equiv 0 \pmod{p^{n+1}}$,
- $f'(y) \equiv 0 \pmod{p^k}$ *but* $f'(y) \not\equiv 0 \pmod{p^{k+1}}$,
- $y \equiv x \pmod{p^{n-k}}$.

Proof. The proof in fact is suggested by the last requirement that y must satisfy. Let us look for y in the form $y = x + p^{n-k}z$. Taylor's formula for polynomials tells us that

$$f(y) = f(x + p^{n-k}z) = f(x) + p^{n-k}zf'(x) + p^{2n-2k}h \pmod{p^{n+1}}$$

for some h. By our assumption, $f(x) \equiv p^n b \pmod{p^{n+1}}$, and also for some c coprime to p we have $f'(x) \equiv p^k c \pmod{p^{n+1}}$, so

$$f(y) = p^n(b + zc) + p^{n+(n-2k)}h \equiv p^n(b + zc) \pmod{p^{n+1}}$$

because of our assumption on k. Finally, because of our assumptions on c, we can find z modulo p for which $b + zc \equiv 0 \pmod{p}$, and hence

$$f(y) \equiv 0 \pmod{p^{n+1}}.$$

Note also, that Taylor's formula applied for $f'(t)$ gives us

$$f'(y) = f'(x + p^{n-k}c) \equiv f'(x) \pmod{p^{n-k}},$$

so since $n - k > k$ and $f'(x) \equiv p^k c \pmod{p^{n+1}}$, we conclude that $f'(y) \equiv 0 \pmod{p^k}$ but $f'(y) \not\equiv 0 \pmod{p^{k+1}}$, as required. □

Remark. *Note that mnemonically our formula $z = -\frac{b}{c}$ implies that we have $y = x + p^{n-k}z = x - \frac{p^n b}{p^k c} = x - \frac{f(x)}{f'(x)}$, so what is happening here is precisely one iteration of the "Newton's method" for constructing approximate solutions to equations.*

Remark. *As with Newton's method, this result does not make claims about the uniqueness of y, neither does it claim anything for the case where the derivative $f'(x)$ is divisible by high powers of p. However, in many cases it gives a method for solving equations which is powerful enough.*