MATH 25 CLASS 20 NOTES, NOV 4 2011

Contents

1. Solving polynomial congruences to prime power moduli

Right now we still have no better way to solve $f(x) \equiv 0 \mod p$ than brute force. As a matter of fact there are better methods than this, but no methods are currently known which are vastly better (like the case of the fast exponentiation mod n vs the naive method of brute force multiplication). In this class, we will use brute force to solve this congruence, except when $f(x)$ is linear, for which we already have an algorithm. The last part of this class will be dedicated to solving this congruence in a systematic way when $f(x)$ is quadratic.

Brute force on $f(x) \equiv 0 \mod p$ requires p different trials. What if we want to solve $f(x) \equiv 0 \mod p^e$ instead, for some $e \geq 1$? Brute force will require p^e different trials, which is very large. However, there is a way to solve $f(x) \equiv 0 \mod p^e$ without this many trials. Before describing the general method, let's look at some specific examples.

Examples.

- Show that $x^3 + 2x + 1 \equiv 0 \mod 5^4$ has no solutions. For a problem like this, perhaps we can get lucky and show that $x^3 + 2x + 1 \equiv 0 \mod 5$ has no solutions. After all, if $x^3 + 2x + 1 \equiv 0 \mod 5^4$, then $x^3 + 2x + 1 \equiv 0 \mod 5$ must be true as well.

  Indeed, a brute force check shows that $x^3 + 2x + 1 \equiv 0 \mod 5$ has no solutions. Therefore, the original congruence has no solutions either. It is worthwhile to note that it is possible for $f(x) \equiv 0 \mod p$ to have a solution, but for $f(x) \equiv 0 \mod p^e$ to have no solutions. We will shortly see how to handle this situation.
- Find all solutions to $f(x) = x^3 + 2x^2 + 2 \equiv 0 \mod 27$. We start by solving the congruence $x^3 + 2x^2 + 2 \equiv 0 \mod 3$. There are three cases to check and we quickly find that the only solution is $x \equiv 2 \mod 3$.

  At this point, we look for solutions to $f(x) \equiv 0 \mod 9$. Since we already know that any solution satisfies $x \equiv 2 \mod 3$, we must have $x \equiv 2, 5, 8 \mod 9$. Again, checking each case shows that $x \equiv 2 \mod 9$ is the only solution mod 9. (Even though you might discover that $f(2) \equiv 0 \mod 9$, you still need to check $5, 8 \mod 9$, since in general it is possible for a single solution mod 3 to yield multiple solutions mod 9.)

Finally, we look for solutions to $f(x) \equiv 0 \mod 27$. We know $x \equiv 2 \mod 9$ for any solution, so $x \equiv 2, 11, 20 \mod 27$. One checks that $x \equiv 20 \mod 27$ is the only solution to this congruence. (Notice that if you do these calculations by hand, they are starting to get a bit tedious, even when the modulus is as low as 27!)

The main idea behind these two examples is that if we want to solve $f(x) \equiv 0 \mod p^e$, we can get a lot of information from trying to understand the easier-to-solve congruences $f(x) \equiv 0 \mod p^i$, where $1 \leq i < e$. In particular, sometimes we can get lucky and rule out solutions immediately by considering $f(x) \equiv 0 \mod p$, and if we find solutions, we can try to gradually 'lift' a solution mod p^i to the larger modulus p^{i+1}, until we reach the modulus p^e.

As a procedure to solve $f(x) \equiv 0 \mod p^e$, this works fine, but we might ask whether there are general properties which are true about lifting solutions. For instance, in the second example, we saw that each solution mod p^i lifted to exactly one solution mod p^{i+1}. Is this always true? Or is it possible for a solution to lift to more than one solution? If so, how many solutions mod p^{i+1} might there be? And can we easily distinguish when each case occurs, without resorting to actual trial-and-error?

Fortunately, there is a relatively simple criterion to determine when all these things happen. Suppose we want to solve $f(x) \equiv 0 \mod p^e$, where $f(x)$ is a polynomial with integer coefficients. Furthermore, suppose we know that $x_i \mod p^i$ is a solution to $f(x) \equiv 0 \mod p^i$.

The possible solutions mod p^{i+1} that appear as lifts of a_i are given by $x_i + p^i k_i$, where $0 \leq k_i < p$. (In the second example, we have $a_0 = 2, p = 3, i = 0$, and then possible solutions mod 3^2 are $2, 2+3\cdot 1, 2+3\cdot 2$, for instance.) How might we determine which of these candidate solutions are real solutions to $f(x) \equiv 0 \mod p^{i+1}$? We will plug these candidate solutions into this congruence and see which ones actually solve the equation!

Let $f(x) = \sum_{j=0}^{n} a_j x^j$. Plugging in $x_i + p^i k_i$ in for x into $f(x)$ yields

$$f(x_i + p^i k_i) = \sum_{j=0}^{n} a_j (x_i + p^i k_i)^j.$$

On the surface, this looks like a horrible mess to expand each jth power. However, recall that we are only interested in the value of this expression modulo p^{i+1}. So, for instance, if we expand $(x_i + p^i k_i)^2$, we end up getting $x_i^2 + 2p^i k_i x_i + p^{2i} k_i^2$, and the last term disappears mod p^{i+1} since $i + 1 \leq 2i$.

More generally, we see that when we expand $(x_i + p^i k_i)^j$, any term in which $p^i k_i$ is raised to a second power or higher disappears when considered mod p^{i+1}. With this in mind, we find that

$$f(x_i + p^i k_i) \equiv \sum_{j=0}^{n} (a_j x_i^j + a_j j x_i^{j-1} p^i k_i) \mod p^{i+1}.$$

This doesn't really look much friendlier, but notice that the first part of the sum is just $f(x_i)$. The second part of the sum doesn't look as simple, but a little bit of thought shows that it is equal to $p_i k_i f'(x_i)$. So altogether, we have

$$f(x_i + p^i k_i) \equiv f(x_i) + f'(x_i)p_i k_i \mod p^{i+1}.$$

At this point, we use the fact that $f(x_i) \equiv 0 \mod p^i$. Because this is so, we can write $f(x_i) \equiv p^i q_i \mod p^i$, for some $0 \le q_i < p$.

Therefore, we want to solve the equation

$$p^i q_i + f'(x_i)p^i k_i \equiv 0 \mod p^{i+1}.$$

Since p^i divides every number in sight (both the terms in the sum and the modulus), this is equivalent to solving

$$q_i + f'(x_i)k_i \equiv 0 \mod p. \tag{1}$$

Notice that something amazing happens: this is a linear equation in the single variable k_i! After all, $q_i, f'(x_i)$ are numbers which depend only on $x_i, f(x)$, and we wanted to solve for k_i, which will determine x_{i+1}.

When does this linear equation have a unique solution? Remember that this has a unique solution exactly when $\gcd(p, f'(x_i)) = 1$, or, in other words, when $p \nmid f'(x_i)$. (Notice that the fact that x_i is only unique up to multiples of p^i does not matter, since $f'(x_i)$ has the same value mod p even if we replace x_i by $x_i + p^i k$ for some integer k.) So if $p \nmid f'(x_i)$, then we can solve for k_i, and then $f(x) \equiv 0 \mod p^{i+1}$ will have exactly one solution which is lifted from x_i.

What happens if $p \mid f'(x_i)$? In this case, Equation 1 reduces to

$$q_i \equiv 0 \mod p.$$

Well, either $q_i \equiv 0 \mod p$ or not. If $q_i \equiv 0 \mod p$ (which, given the way we've defined q_i to satisfy $0 \le q_i < p$, means that $q_i = 0$), then this equation is always true, regardless of the value of k_i we choose. On the other hand, if $q_i \not\equiv 0 \mod p$, then it does not matter what value we choose for k_i.

2. Hensel's Lemma

Let's summarize this result:

Theorem 1 (Hensel's Lemma, Example 4.10 in the book)**.** *Let $f(x)$ be a polynomial with integral coefficients. Let p be a prime. Let $x_i \mod p^i$ be a solution to $f(x) \equiv 0 \mod p^i$. Then:*

- *If $p \nmid f'(x_i)$, then there is a unique $x_{i+1} \mod p^{i+1}$ satisfying $x_{i+1} \equiv x_i \mod p^i$ (that is, x_{i+1} is a lift of x_i) and $f(x_{i+1}) \equiv 0 \mod p^{i+1}$. If we write $x_{i+1} = x_i + p^i k_i$ and $f(x_i) = p^i q_i$, where $0 \le k_i, q_i < p$, then k_i is the unique solution to $q_i + f'(x_i)k_i \equiv 0 \mod p$.*
- *If $p \mid f'(x_i)$ and $p^{i+1} \nmid f(x_i)$ (in the terminology of the previous case, $q_i \neq 0$), then there are no $x_{i+1} \mod p^{i+1}$ which solve $f(x) \equiv 0 \mod p^{i+1}$ and satisfy $x_{i+1} \equiv x_i \mod p^i$. (In other words, no lifts of x_i solve $f(x) \equiv 0 \mod p^{i+1}$.)*
- *If $p \mid f'(x_i)$ and $p^{i+1} \mid f(x_i)$, then every $x_{i+1} \mod p^{i+1}$ which satisfies $x_{i+1} \equiv x_i \mod p^i$ is also a solution of $f(x) \equiv 0 \mod p^{i+1}$.*

Examples.

- Let's go back to the example $f(x) = x^3 + 2x^2 + 2 \equiv 0 \mod 3^3$. We saw that $f(2) \equiv 0 \mod 3$ (remember, we still only know the trial-and-error method when solving $f(x) \equiv 0 \mod p$), so $x_1 = 2$ in our language. To determine all lifts of x_1 to solutions mod 9 using Hensel's Lemma, first we calculate $f'(x) = 3x^2 + 4x$. Therefore $f'(x_1) = f'(2) = 12 + 8 = 20$, and evidently $3 \nmid 20$, so we are in the first case of Hensel's Lemma.

  To actually determine the lift, we also need to know the value of $f(x_1)$ mod 9, not just mod 3. We calculate $f(2) = 18 = 3 \cdot 6$. So this tells us that $q_1 = 0$, since $18 \equiv 0 \mod 9$, and $0 = 3 \cdot 0$. (Notice that had we chosen $x_1 = -1$ in all this, we still would have found that $3 \nmid f'(x_i)$, but $f(-1) = 3$ would have yielded a value of $q_1 = 1$. So the actual q_i do depend on your choice of representative for x_i, but does not impact whether $p \mid f'(x_i)$ or not.) To determine k_1, which in turn determines $x_2 = x_1 + 3^1 k_1$, we solve $q_1 + f'(x_1)k_1 \equiv 0 \mod 3$. Plugging in all the numbers we've calculated, this becomes $0 + 2k_1 \equiv 0 \mod 3$, which obviously has unique solution $k_1 \equiv 0$ mod 3. Since we require $0 \le k_1 < 3$, this gives $k_1 = 0$. Therefore the solution $x_1 = 2 \mod 3$ uniquely lifts to the solution $x_2 = 2 \mod 9$ of $f(x) \equiv 0$ mod 9. You can use Hensel's Lemma to lift this solution to a solution mod 27 as an exercise. You might also want to do the calculation of lifting $-1 \mod 3$ to a solution mod 9; you will get the same result but as mentioned, the value of q_1, and hence k_1, changes.
- To see an example of one of the latter two cases happening, consider the old question of solutions to $x^2 - 1 \equiv 0 \mod 8$. We already solved this using brute force, but let's see what happens when we apply Hensel's Lemma to it. First, the congruence $x^2 \equiv 1 \mod 2$ clearly only has solution $x_1 \equiv 1 \mod 2$. Since $f(x) = x^2 - 1, f'(x) = 2x$. However, notice that $2 \mid (2x)$ regardless of the value of x. Therefore, either $x_1 \equiv 1 \mod 2$ lifts to $p = 2$ solutions mod 4, or no solutions mod 4. To check which occurs (of course, we already know which case occurs, but we want to check that Hensel's Lemma works), we check the value of $f(x_1) = f(1) = 0$. Since $2^2 \mid 0$, we are in the last case of Hensel's Lemma, which tells us that every lifting of $1 \mod 2$ to mod 4 (namely, $1, 3$ mod 4) are also solutions to $f(x) \equiv 0 \mod 4$. And then one can check the same thing happens when checking for lifting of both $1, 3 \mod 4$ to mod 8, which gives the solutions $1, 3, 5, 7 \mod 8$, which we already knew.
- Consider $f(x) = 2x^2 + 3x + 2 \equiv 0 \mod 7^2$. When we consider $f(x) \equiv 0$ mod 7, trial and error gives the unique solution $x_1 \equiv 1 \mod 7$. We now test if we can lift this to any solutions mod 49. First, we compute $f'(x) = 4x + 3$. In particular, $7 \mid f'(1)$. Therefore, we need to check whether $49 \mid f(1)$. A quick calculation shows that $f(1) = 7$, so $49 \nmid 7$. Hensel's Lemma therefore tells us that there is no lift of $1 \mod 7$ to a solution of $f(x) \equiv 0 \mod 7^2$, and therefore no solutions to this congruence in general.
- Consider $f(x) = x^2 + 3 \equiv 0 \mod 7^n$, for any positive integer n. Does this have any solutions? Notice that $x_1 = 2$ solves $f(x) \equiv 0 \mod 7$. We compute $f'(x) = 2x$, and $f'(x_1) = 4$. In particular, $7 \nmid 4$, so there is a unique lift of $x_1 \equiv 2 \mod 7$ to mod 49 which solves $f(x) \equiv 0 \mod 49$.

  Instead of computing what this lift, say x_2, actually is, let's think about whether we can lift this to a solution $x_3 \mod 7^3$ of $f(x) \equiv 0 \mod 7^3$. We need to check whether $7 \mid f'(x_2)$ or not. While we don't know what x_2 is, we do know that $x_2 \equiv 2 \mod 7$. Therefore, $f'(x_2) \equiv f'(2) = 4 \mod 7$, so we can conclude that $7 \nmid f'(x_2)$. Therefore $x_2 \mod 7^2$ lifts to a unique solution $x_3 \mod 7^3$ of $f(x) \equiv 0 \mod 7^3$.

This procedure clearly can continue indefinitely; a solution $x_n \mod 7^n$ satisfies $7 \nmid f'(x_n)$ because $x_n \equiv 2 \mod 7$, and therefore lifts to a solution $x_{n+1} \mod 7^{n+1}$ of $f(x) \equiv 0 \mod 7^{n+1}$.

So in the end, we get a sequence of solutions $x_1 = 2, x_2, x_3, \ldots$, where x_i solves $f(x) \equiv 0 \mod 7^i$. Furthermore, these solutions satisfy the 'compatibility' conditions $x_j \equiv x_i \mod 7^i$, if $i \leq j$.