Math 3527 (Number Theory 1)

Lecture #29

Polynomial Congruences:

- Polynomial Congruences Modulo m
- Polynomial Congruences Modulo p^n and Hensel's Lemma

This material represents §5.1 from the course notes.

Overview

The goal of this last segment of the course is to discuss quadratic residues (which are simply squares modulo m) and the law of quadratic reciprocity, which is a stunning and unexpected relation involving quadratic residues modulo primes.

- We begin with some general tools for solving polynomial congruences modulo prime powers, which essentially reduce matters to studying congruences modulo primes.
- Then we study the quadratic residues (and quadratic nonresidues) modulo p, which leads to the Legendre symbol, a tool that provides a convenient way of determining when a residue class a modulo p is a square.
- We then discuss quadratic reciprocity and some of its applications.

Polynomial Congruences, I

In an earlier chapter, we analyzed the problem of solving linear congruences of the form $ax \equiv b \pmod{m}$. We now study the solutions of congruences of higher degree.

- As a first observation, we note that the Chinese Remainder Theorem reduces the problem of solving any polynomial congruence $q(x) \equiv 0 \pmod{m}$ to solving the individual congruences $q(x) \equiv 0 \pmod{p^d}$, where the p^d are the prime-power divisors of m.

Polynomial Congruences, II

Example: Solve the equation $x^3 + x + 2 \equiv 0 \pmod{36}$.

Polynomial Congruences, II

Example: Solve the equation $x^3 + x + 2 \equiv 0 \pmod{36}$.

- By the Chinese remainder theorem, it suffices to solve the two separate equations $x^3 + x + 2 \equiv 0 \pmod{4}$ and $x^3 + x + 2 \equiv 0 \pmod{9}$.
- We can just test all possible residues to see that the only solutions are $x \equiv 2 \pmod{4}$ and $x \equiv 8 \pmod{9}$.
- Therefore, by the Chinese remainder theorem, there is a unique solution; namely, the solution to those simultaneous congruences, which is $x \equiv 26 \pmod{36}$.

Polynomial Congruences, III

Example: Solve the equation $x^2 \equiv 0 \pmod{12}$.

Polynomial Congruences, III

<u>Example</u>: Solve the equation $x^2 \equiv 0 \pmod{12}$.

- By the Chinese remainder theorem, it suffices to solve the two separate equations $x^2 \equiv 0 \pmod{4}$ and $x^2 \equiv 0 \pmod{3}$, and then put the results back together.
- The first equation visibly has the solutions $x \equiv 0, 2 \pmod{4}$ while the second equation has the solution $x \equiv 0 \pmod{3}$.
- Then applying the Chinese remainder theorem to the 2 possible pairs of congruences $x \equiv 0 \pmod{4}$, $x \equiv 0 \pmod{3}$, and $x \equiv 0 \pmod{4}$, $x \equiv 2 \pmod{3}$, yields the solutions $x \equiv 0, 6 \pmod{12}$ to the original equation.

Polynomial Congruences, IV

Example: Solve the equation $x^2 \equiv 1 \pmod{30}$.

Polynomial Congruences, IV

Example: Solve the equation $x^2 \equiv 1 \pmod{30}$.

- By the Chinese remainder theorem, it suffices to solve the three separate equations $x^2 \equiv 1 \pmod{2}$, $x^2 \equiv 1 \pmod{3}$, $x^2 \equiv 1 \pmod{5}$.
- We can just test all possible residues to see that the solutions are $x \equiv 1 \pmod{2}$, $x \equiv 1, 2 \pmod{3}$, and $x \equiv 1, 4 \pmod{5}$.
- Therefore, by applying the Chinese remainder theorem to all $1 \cdot 2 \cdot 2 = 4$ ways to pick a solution from each congruence, we see that there are 4 solutions modulo 30, and they are $x \equiv 1, 11, 19, 29 \pmod{30}$.

Polynomial Congruences, V

We are therefore reduced to solving a polynomial congruence of the form $q(x) \equiv 0 \pmod{p^d}$.

- Observe that any solution modulo p^d "descends" to a solution modulo p, simply by considering it modulo p.
- For example, any solution to $x^3 + x + 3 \equiv 0 \pmod{25}$, such as $x = 6$, is also a solution to $x^3 + x + 3 \equiv 0 \pmod{5}$.
- Our basic idea is that this procedure can also be run in reverse, by first finding all the solutions modulo p and then using them to compute the solutions modulo p^d.
- More explicitly, if we first solve the equation modulo p, we can then try to "lift" each of these solutions to get all of the solutions modulo p^2, then "lift" these to obtain all solutions modulo p^3, and so forth, until we have obtained a full list of solutions modulo p^d.

Polynomial Congruences, VI

Example: Solve the congruence $x^3 + x + 3 \equiv 0 \pmod{25}$.

Polynomial Congruences, VI

Example: Solve the congruence $x^3 + x + 3 \equiv 0 \pmod{25}$.

- Since $25 = 5^2$, we first solve the congruence modulo 5.
- If $q(x) = x^3 + x + 3$, we can just try all residues to see the only solution is $x \equiv 1 \pmod{5}$.
- Now we "lift" to find the solutions to the original congruence, as follows: if $x^3 + x + 3 \equiv 0 \pmod{25}$ then we must have $x \equiv 1 \pmod{5}$.
- Now write $x = 1 + 5a$: plugging in yields $(1 + 5a)^3 + (1 + 5a) + 3 \equiv 0 \pmod{25}$, which, upon expanding and reducing, simplifies to $5 + 20a \equiv 0 \pmod{25}$.
- Cancelling the factor of 5 yields $4a \equiv 4 \pmod{5}$, which has the single solution $a \equiv 1 \pmod{5}$.
- This yields the single solution $x \equiv 6 \pmod{25}$ to our original congruence.

Polynomial Congruences, VII

Example: Solve the congruence $x^3 + 4x \equiv 4 \pmod{343}$.

Polynomial Congruences, VII

Example: Solve the congruence $x^3 + 4x \equiv 4 \pmod{343}$.

- Since $343 = 7^3$, we first solve the congruence modulo 7, then modulo 7^2, and then finally modulo 7^3.
- By trying all the residue classes, we see that $x^3 + 4x \equiv 4 \pmod{7}$ has the single solution $x \equiv 3 \pmod{7}$.
- Next we lift to find the solutions modulo 7^2: any solution must be of the form $x = 3 + 7a$ for some a.
- Plugging in yields $(3 + 7a)^3 + 4(3 + 7a) \equiv 4 \pmod{7^2}$, which eventually simplifies to $21a \equiv 14 \pmod{7^2}$.
- Cancelling the factor of 7 yields $3a \equiv 2 \pmod{7}$, which has the single solution $a \equiv 3 \pmod{7}$.
- This tells us that $x \equiv 24 \pmod{49}$.

Polynomial Congruences, VIII

Example (continued):

- Now that we know that we must have $x \equiv 24 \pmod{49}$, we can lift to find the solutions modulo 7^3 in the same way.
- Explicitly, any solution must be of the form $x = 24 + 49b$ for some b.
- Plugging in yields $(24 + 7^2 b)^3 + 4(24 + 7^2 b) \equiv 4 \pmod{7^3}$, which eventually simplifies to $147b \equiv 147 \pmod{7^3}$.
- Cancelling the factor of 7^2 yields $3b \equiv 3 \pmod{7}$, which has the single solution $b \equiv 1 \pmod{7}$.
- Hence we obtain the unique solution $x \equiv 24 + 49b \equiv 73 \pmod{7^3}$.

Polynomial Congruences, IX

Example: Solve the congruence $x^3 + 4x \equiv 12 \pmod{7^3}$.

Polynomial Congruences, IX

<u>Example</u>: Solve the congruence $x^3 + 4x \equiv 12 \pmod{7^3}$.

- We first solve the congruence modulo 7. By trying all the residue classes, we see that $x^3 + 4x \equiv 5 \pmod 7$ has two solutions, $x \equiv 1 \pmod 7$ and $x \equiv 5 \pmod 7$.
- Next we lift to find the solutions modulo 7^2: any solution must be of the form $x = 1 + 7k$ or $x = 5 + 7k$ for some k.
- If $x = 1 + 7k$, then we get $(1 + 7k)^3 + 4(1 + 7k) \equiv 12 \pmod{7^2}$, which simplifies to $0 \equiv 7 \pmod{7^2}$. This is contradictory so there are no solutions in this case.
- If $x = 5 + 7k$, then we get $(5 + 7k)^3 + 4(5 + 7k) \equiv 12 \pmod{7^2}$, which simplifies to $14k \equiv 14 \pmod{7^2}$. Solving this linear congruence produces $k \equiv 1 \pmod 7$, so we obtain $x \equiv 12 \pmod{49}$.

Polynomial Congruences, X

Example (continued):

- Now we lift to find the solutions modulo 7^3: from the previous slide, any solution must be of the form $x = 12 + 49k$.
- In the same way as before, plugging in yields $(12 + 7^2 k)^3 + 4(12 + 7^2 k) \equiv 4 \pmod{7^3}$, which after expanding and reducing, simplifies to $98k \equiv 294 \pmod{7^3}$. Solving in the same way as before yields $k \equiv 5 \pmod{7}$, whence $x \equiv 12 + 49k \equiv 257 \pmod{7^3}$.
- Hence, there is a unique solution: $x \equiv 257 \pmod{7^3}$.

Polynomial Congruences, XI

Example: Solve the congruence $x^2 \equiv 9 \pmod{16}$.

Polynomial Congruences, XI

Example: Solve the congruence $x^2 \equiv 9 \pmod{16}$.

- Since $16 = 2^4$, we find the solutions mod 2, then work upward.
- It is easy to see that there is a unique solution to $x^2 \equiv 9 \pmod{2}$, namely, $x \equiv 1 \pmod{2}$.
- Next we lift to find the solutions modulo 2^2: any solution must be of the form $x = 1 + 2k$, so we get $(1+2k)^2 \equiv 9 \pmod{2^2}$, which simplifies to $1 \equiv 9 \pmod{2^2}$. This is always true, so we get two possible solutions, $x \equiv 1, 3 \pmod{4}$.
- If $x = 1 + 4k$, then we get $(1+4k)^2 \equiv 9 \pmod{2^3}$, which simplifies to $1 \equiv 9 \pmod{2^3}$, which is again always true.
- If $x = 3 + 4k$, then we get $(3+4k)^2 \equiv 9 \pmod{2^3}$, which simplifies to $9 \equiv 9 \pmod{2^3}$, which is also always true.
- Thus we get the four solutions $x \equiv 1, 3, 5, 7 \pmod{2^3}$.

Polynomial Congruences, XII

Example (continued):

- Finally, we must lift each solution $x \equiv 1, 3, 5, 7 \pmod{2^3}$ to the modulus 2^4.
- If $x = 1 + 8k$ then we get $(1 + 8k)^2 \equiv 9 \pmod{2^4}$, which simplifies to $1 \equiv 9 \pmod{2^4}$, which is contradictory.
- If $x = 3 + 8k$ then we get $(3 + 8k)^2 \equiv 9 \pmod{2^4}$, which simplifies to $9 \equiv 9 \pmod{2^4}$, which is always true, so we get two solutions $x \equiv 3, 11 \pmod{2^4}$.
- If $x = 5 + 8k$ then we get $(5 + 8k)^2 \equiv 9 \pmod{2^4}$, which simplifies to $25 \equiv 9 \pmod{2^4}$, which is always true, so we get two solutions $x \equiv 5, 13 \pmod{2^4}$.
- If $x = 7 + 8k$ then we get $(7 + 8k)^2 \equiv 9 \pmod{2^4}$, which simplifies to $49 \equiv 9 \pmod{2^4}$, which is contradictory.
- Thus, we get four solutions in total: $x \equiv 3, 5, 11, 13 \pmod{2^4}$.

Polynomial Congruences, XIII: Lucky!

The general procedure will work the same way for any prime power modulus p^n:

- We first solve the congruence modulo p. For each solution we obtain, we then try to lift it to a solution mod p^2, then lift each of those to a solution mod p^3, and so forth, until we get the full list of solutions mod p^n.
- In the last few examples we just worked through, we saw a variety of different behaviors.
- Sometimes, when we lift a solution, we obtain exactly one lifted solution. Other times, the lifting might fail, or it might yield more than one possible lifted solution.
- We would like to understand what determines when each of these behaviors will occur.

Hensel's Lemma, I

Rather than building the motivation, we will simply state the result:

Theorem (Hensel's Lemma)

Suppose $q(x)$ is a polynomial with integer coefficients. If $q(a) \equiv 0$ (mod p^d) and $q'(a) \not\equiv 0$ (mod p), then there is a unique k (modulo p) such that $q(a + kp^d) \equiv 0$ (mod q^{d+1}). Explicitly, if u is the inverse of $q'(a)$ modulo p, then $k = -u \cdot \dfrac{q(a)}{p^d}$.

This result (and a number of variations) is traditionally called Hensel's lemma, although for us it is really more of a theorem since the proof is fairly technical. (The full proof is in the notes, but it is just a formalized version of the procedure we were using earlier.)

Hensel's Lemma, II

Example: Show that there is a unique solution to the congruence $x^3 - 2x + 7 \equiv 0 \pmod{3^{2020}}$.

Hensel's Lemma, II

<u>Example</u>: Show that there is a unique solution to the congruence $x^3 - 2x + 7 \equiv 0 \pmod{3^{2020}}$.

- The idea is to use Hensel's lemma to show that the lifting will always yield a unique solution starting from the bottom level.
- First, we solve the congruence modulo 3: testing all 3 possible residues shows that the only solution is $x \equiv 1 \pmod 3$.
- Now we just compute the derivative: if $q(x) = x^3 - 2x + 7$, then $q'(x) = 3x^2 - 2 \equiv 1 \pmod 3$, no matter what x is.
- Therefore, Hensel's lemma guarantees that we will always have a unique solution to this congruence modulo 3^d for any $d \geq 1$. In particular, the solution is unique modulo 3^{2020}.

Hensel's Lemma, III

Example (continued): Solutions of $x^3 - 2x + 7 \equiv 0 \pmod{3^d}$.

Hensel's Lemma, III

Example (continued): Solutions of $x^3 - 2x + 7 \equiv 0 \pmod{3^d}$.

- We can even calculate the various lifts using the formula given in Hensel's lemma. (Our direct technique will yield the same result, since ultimately it is how Hensel's lemma is proven.)
- For example, mod 3^2, since $q'(a) \equiv 1 \pmod 3$ has inverse $u \equiv 1 \pmod 3$, we will obtain the solution $x = 1 + 3k$ where $k = -u \cdot \dfrac{q(a)}{p^d} = -1 \cdot \dfrac{6}{3} = -2$: thus, $x \equiv -5 \equiv 4 \pmod 9$, which indeed works.
- Lifting again yields $x = 4 + 9k$ where $k = -u \cdot \dfrac{q(a)}{p^d} = -1 \cdot \dfrac{63}{9} = -7$, yielding $x \equiv 4 + 9k \equiv 22 \pmod{27}$.
- We can continue in this way and compute the lifts as high as we desire.

Summary

We discussed how to solve polynomial congruences modulo m and modulo prime powers. We discussed how to use Hensel's lemma to calculate solutions to congruences modulo p^d explicitly in many cases.

Next lecture: Quadratic Residues and Legendre Symbols