

Math 104A, Number Theory, Fall 2002.
Summary of Lecture 15.

Polynomial congruences. Set

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_0.$$

We want to solve

$$(*) \quad f(x) \equiv 0 \pmod{m}.$$

We have already solved the case when $f(x) = ax + b$. The strategy for general polynomials is to find the prime factorization of m and solve (*) when m is replaced by a prime factor of m , then use this to solve (*) when m is replaced by a prime power, and finally to put these solutions together to solve (*) for general m .

When m is a small prime we try all values of x modulo m .

Example. Find the solutions of $x^2 + 2x + 2 \equiv 0 \pmod{5}$.

x	$x^2 + 2x + 2$
0	2
1	0
2	0
3	2
4	2

We find two solutions, 1 and 2.

Example. Find the solutions of $x^2 + 2x + 2 \equiv 0 \pmod{25}$.

If $f(x) \equiv 0 \pmod{25}$ then $f(x) \equiv 0 \pmod{5}$ and so $x \equiv 1$ or $x \equiv 2 \pmod{5}$. First suppose $x \equiv 1 \pmod{5}$. The possible values of x modulo 25 are 1, 6, 11, 16, 21. We would like to compute

$$f(1 + 5k) \pmod{25}.$$

There is a trick.

Lemma.

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_0, \quad f'(x) = n a_n x^{n-1} + (n-1) a_{n-1} x^{n-2} + \dots + a_1.$$

The following congruence holds:

$$f(x_0 + p^k t) \equiv f(x_0) + p^k t f'(x_0) \pmod{p^{k+1}}.$$

Checking this when $f = x^2 + 2x + 2$, with $p = 5$ and $k = 1$, we have

$$\begin{aligned} f(x_0 + 5t) &= (x_0 + 5t)^2 + 2(x_0 + 5t) + 2 \\ &= x_0^2 + 2x_0 + 2 + 2 \cdot 5tx_0 + 2 \cdot 5t + 5^2t^2 = f(x_0) + 5tf'(x_0) + 25t^2. \end{aligned}$$

Hence

$$\begin{aligned} f(1 + 5t) &\equiv f(1) + 5tf'(1) \pmod{25} \\ &\equiv 5 + 5t \cdot 4 \pmod{25}. \end{aligned}$$

Hence

$$\begin{aligned} f(1 + 5t) \equiv 0 \pmod{25} &\Leftrightarrow 5 + 5 \cdot 4t \equiv 0 \pmod{25} \\ \Leftrightarrow 1 + 4t \equiv 0 \pmod{5} &\Leftrightarrow 4t \equiv 4 \pmod{5}. \end{aligned}$$

Since $(4, 5) = 1$ we have the unique solution $t \equiv 1 \pmod{5}$ and $x \equiv 6 \pmod{25}$.

The same argument applied to $x = 2 + 5t$ gives one other solution, $x \equiv 17 \pmod{25}$. We stated Theorem 3.4.6

Example. Using this we can quickly solve $x^2 + 2x + 2 \equiv 0 \pmod{125}$. We have the possibilities $x \equiv 6$ or $x \equiv 17 \pmod{25}$. Now $f'(6) = 14$ and $f'(17) = 36$. Since 5 does not divide either of these, we get precisely two solutions to $f(x) \equiv 0 \pmod{125}$. With a little more work we can evaluate these. For one solution, $x = 6 + 25t$, we find t by solving

$$f(6) + 25tf'(6) \equiv 0 \pmod{125}.$$

We solve this:

$$\begin{aligned} 50 + 25t \cdot 14 \equiv 0 \pmod{125} &\Leftrightarrow 2 + 14t \equiv 0 \pmod{5} \\ &\Leftrightarrow 4t \equiv 3 \pmod{5} \Leftrightarrow t \equiv 2 \pmod{5}. \end{aligned}$$

The solution is $x = 56$. Solving in the same way for a solution $x = 17 + 25t$ we get the solution $x = 67$.

Example. Find all the solutions to $x^2 + 7x + 1 \equiv 0 \pmod{27}$.

Solution: First solve $x^2 + 7x + 1 \equiv 0 \pmod{3}$. We have

x	$x^2 + 7x + 1 \equiv x(x + 1) + 1 \pmod{3}$
0	1
1	0
2	1

There is one solution, $x \equiv 1 \pmod{3}$.

Now solve $x^2 + 7x + 1 \equiv 0 \pmod{9}$. We have $f'(x) = 2x + 7$, so $f'(1) = 9$. Since $3|9$, we are in case (b) or (c) of Theorem 3.4.6 and we must compute $f(1)$. Now $f(1) = 9$ and since $9|9$ the solutions modulo 9 are $x = 1 + 3t$ for all t . This gives 3 solutions, $x = 1, 4, 7$.

Now we solve $x^2 + 7x + 1 \equiv 0 \pmod{27}$.

x	f'	f
1	9	9
4	15	45
7	21	99

In each case, $3|f'(x)$ but $27 \nmid f(x)$, so there are no solutions.