## Polynomial Congruences

We have discussed how to solve the general linear congruence $ax \equiv b \pmod{m}$. From here, it is not far to a consideration of the solution to the general polynomial congruence $f(x) \equiv 0 \pmod{m}$ where

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$

has integer coefficients $a_i$, $i = 0, \ldots, n$.

The first stage of the process is to consider the prime factorization of $m$: say that $m = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$. Then observe that, by the CRT, solving $f(x) \equiv 0 \pmod{m}$ is equivalent to solving the system of congruences

$$\begin{aligned} f(x) &\equiv 0 \pmod{p_1^{e_1}} \\ f(x) &\equiv 0 \pmod{p_2^{e_2}} \\ &\vdots \\ f(x) &\equiv 0 \pmod{p_k^{e_k}} \end{aligned}$$

That is, by means of the CRT, we can reduce our problem to the case where the modulus is a prime power.

The second stage of the process, then, is to deal with polynomial congruences of the form $f(x) \equiv 0 \pmod{p^e}$ where $p$ is prime. For this we use a powerful result, known as

**The Lifting Theorem** Suppose $x \equiv a \pmod{p^e}$ is a solution to the polynomial congruence $f(x) \equiv 0 \pmod{p^e}$. Then, where $f'(x)$ is the derivative of the polynomial, this solution lifts to a solution to the congruence $f(x) \equiv 0 \pmod{p^{e+1}}$ depending on whether $p \mid f'(a)$ and $p^{e+1} \mid f(a)$:

- if $p \nmid f'(a)$, then $f(x) \equiv 0 \pmod{p^{e+1}}$ has the unique solution $x \equiv a + p^e t \pmod{p^{e+1}}$ where $t$ is the unique solution to the linear congruence
$$f'(a)t \equiv -\frac{f(a)}{p^e} \pmod{p};$$
- if $p \mid f'(a)$ and $p^{e+1} \mid f(a)$, then $f(x) \equiv 0 \pmod{p^{e+1}}$ has $p$ distinct solutions of the form $x \equiv a + p^e t \pmod{p^{e+1}}$ where $t = 0, 1, \ldots, p-1$;
- if $p \mid f'(a)$ but $p^{e+1} \nmid f(a)$, then $f(x) \equiv 0 \pmod{p^{e+1}}$ has no solutions which reduce to $a \bmod p^e$.

**Proof** Suppose that $x$ is a solution to $f(x) \equiv 0 \pmod{p^{e+1}}$ that is lifted from the solution $x \equiv a \pmod{p^e}$ to $f(x) \equiv 0 \pmod{p^e}$. Then $x = a + p^e t$ for some integer $t$.

Next, since $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$, we have $f'(x) = n a_n x^{n-1} + (n-1) a_{n-1} x^{n-2} + \cdots + 2a_2 x + a_1$. Also, since $x = a + p^e t$, we use the binomial theorem to conclude that

$$
\begin{aligned}
f(x) &= f(a + p^e t) \\
&= a_n (a + p^e t)^n + a_{n-1} (a + p^e t)^{n-1} + \cdots + a_0 \\
&= a_n \left(a^n + \binom{n}{1} a^{n-1} \cdot p^e t + \binom{n}{2} a^{n-1} \cdot p^{2e} t^2 + \cdots\right) + \\
&\quad a_{n-1} \left(a^{n-1} + \binom{n-1}{1} a^{n-2} \cdot p^e t + \binom{n-1}{2} a^{n-3} \cdot p^{2e} t^2 + \cdots\right) + \\
&\quad \cdots + a_0 \\
&= (a_n a^n + a_{n-1} a^{n-1} + \cdots + a_0) \\
&\quad + (n a_n a^{n-1} + (n-1) a_{n-1} a^{n-2} + \cdots + a_1) p^e t \\
&\quad + \text{ terms involving higher powers of } p^e t \\
&= f(a) + f'(a) p^e t + \text{ terms divisible by } (p^e t)^2 \\
&\equiv f(a) + f'(a) p^e t \pmod{p^{e+1}}
\end{aligned}
$$

But our assumption that $f(x) \equiv 0 \pmod{p^{e+1}}$ implies that

(*) $$f(a)+f'(a)p^e t \equiv 0 \pmod{p^{e+1}}.$$

And since $f(a) \equiv 0 \pmod{p^e}$, it follows that $p^e \mid f(a)$ and we can divide through by $p^e$ in (*):

(**) $$f'(a)t \equiv -\frac{f(a)}{p^e} \pmod{p}$$

But this last congruence is linear in $t$, so we can solve for $t$ using the Fundamental Theorem for Linear Congruences:

- if $p \nmid f'(a)$, then (**) has a unique solution for $t$ obtained by multiplying through by the inverse mod $p$ of $f'(a)$;
- if $p \mid f'(a)$ and $p^{e+1} \mid f(a)$, then (**) is equivalent to the congruence $0t \equiv 0 \pmod{p}$, hence any value of $t$ mod $p$ is a solution: $t = 0,1,\ldots, p-1$;
- if $p \mid f'(a)$ but $p^{e+1} \nmid f(a)$, then (**) has no solutions for $t$.

It is readily seen that these conditions are equivalent to those given the statement of the theorem. //

The effect of the lifting theorem is to show that solving the congruence $f(x) \equiv 0 \pmod{p^{e+1}}$ can be accomplished by first solving the congruence $f(x) \equiv 0 \pmod{p^e}$ then lifting the solutions mod $p^e$ to solutions mod $p^{e+1}$.

This means that the solution of polynomial congruences with prime power modulus $p^e$ begin with solving the same congruence mod $p$ then lifting to solutions mod $p^2$, then solutions mod $p^3$, and so on until we find the solutions mod $p^e$.

At the beginning of the procedure, we are still required to solve $f(x) \equiv 0 \pmod{p}$. For this, we have no special techniques. Often our only option is to test each of the values $x \equiv 0, 1, \ldots, p-1 \pmod{p}$ to see which solve $f(x) \equiv 0 \pmod{p}$.

*Example*: Solve $x^3 + 3x^2 - 4 \equiv 0 \pmod{175}$.

As $175 = 5^2 \cdot 7$, the given congruence is equivalent to the system

$$x^3 + 3x^2 - 4 \equiv 0 \pmod{7}$$
$$x^3 + 3x^2 - 4 \equiv 0 \pmod{5^2}$$

To solve the first congruence, we test the values $x \equiv 0, 1, 2, 3, 4, 5, 6 \pmod{7}$; we then find that $x \equiv 1, 5 \pmod{7}$ are the two solutions.

To solve the second congruence, we first tackle $x^3 + 3x^2 - 4 \equiv 0 \pmod{5}$. Again, we simply test the values $x \equiv 0, 1, 2, 3, 4 \pmod{5}$ to find that $x \equiv 1, 3 \pmod{5}$ are the two solutions. Next, we

proceed to lift each of these solutions to a solution mod $5^2$ (noting that if $f(x) = x^3 + 3x^2 - 4$, then $f'(x) = 3x^2 + 6x$):
in the case of $x \equiv 1 \pmod 5$, we have $f(1) = 0,\ f'(1) = 9$; as $5 \nmid f'(1)$, we can lift to a unique solutions by solving $f'(1)t \equiv -\dfrac{f(1)}{5} \pmod 5$, or $9t \equiv 0 \pmod 5$. Clearly, $t \equiv 0 \pmod 5$, leading to the solution $x \equiv 1 + 0 \cdot 5 \equiv 1 \pmod{5^2}$.
in the case of $x \equiv 3 \pmod 5$, we have $f(3) = 50,\ f'(1) = 45$; as $5 \mid f'(3)$ and $5^2 \mid f(3)$, we can lift to 5 distinct solutions $x \equiv 3, 8, 13, 18, 23 \pmod{5^2}$.

Consequently, we have two solutions $x \equiv 1, 5 \pmod 7$ that can each pair with six solutions $x \equiv 1, 3, 8, 13, 18, 23 \pmod{5^2}$ to yield 12 possible solutions mod 175, each computed via the CRT:

| | $x \equiv 1 \pmod 7$ | $x \equiv 5 \pmod 7$ |
|---|---|---|
| $x \equiv 1 \pmod{25}$ | $x \equiv 1 \cdot 7 \cdot 18 + 1 \cdot 25 \cdot 2 \equiv 1$ | $x \equiv 1 \cdot 7 \cdot 18 + 5 \cdot 25 \cdot 2 \equiv 26$ |
| $x \equiv 3 \pmod{25}$ | $x \equiv 3 \cdot 7 \cdot 18 + 1 \cdot 25 \cdot 2 \equiv 78$ | $x \equiv 3 \cdot 7 \cdot 18 + 5 \cdot 25 \cdot 2 \equiv 103$ |
| $x \equiv 8 \pmod{25}$ | $x \equiv 8 \cdot 7 \cdot 18 + 1 \cdot 25 \cdot 2 \equiv 8$ | $x \equiv 8 \cdot 7 \cdot 18 + 5 \cdot 25 \cdot 2 \equiv 33$ |
| $x \equiv 13 \pmod{25}$ | $x \equiv 13 \cdot 7 \cdot 18 + 1 \cdot 25 \cdot 2 \equiv 113$ | $x \equiv 13 \cdot 7 \cdot 18 + 5 \cdot 25 \cdot 2 \equiv 138$ |
| $x \equiv 18 \pmod{25}$ | $x \equiv 18 \cdot 7 \cdot 18 + 1 \cdot 25 \cdot 2 \equiv 43$ | $x \equiv 18 \cdot 7 \cdot 18 + 5 \cdot 25 \cdot 2 \equiv 68$ |
| $x \equiv 23 \pmod{25}$ | $x \equiv 23 \cdot 7 \cdot 18 + 1 \cdot 25 \cdot 2 \equiv 148$ | $x \equiv 23 \cdot 7 \cdot 18 + 5 \cdot 25 \cdot 2 \equiv 173$ |

(Here, we use the facts that the inverse of 7 mod 25 is 18 and that the inverse of 25 mod 7 is 2; all values inside the table are mod 175.)