CS 70 Discrete Mathematics and Probability Theory
Fall 2022 Satish Rao and Babak Ayazifar

# HW 05

Due: Saturday, 10/1, 4:00 PM
Grace period until Saturday, 10/1, 6:00 PM

## Sundry

Before you start writing your final homework submission, state briefly how you worked on it. Who else did you work with? List names and email addresses. (In case of homework party, you can just describe the group.)

I did not work with anybody on this homework. I went to office hours on Thursday and Friday to ask for clarification on problems 3, 5, and 6, but did not work with anybody there.

## 1 RSA Practice

Consider the following RSA schemes and solve for asked variables.

(a) Assume for an RSA scheme we pick 2 primes $p = 5$ and $q = 11$ with encryption key $e = 9$, what is the decryption key $d$? Calculate the exact value.

**Solution:** If we have $e = 9$, then we need to find the multiplicative inverse of $e$ modulo $4 \cdot 10 = 40$. It turns out that the multiplicative inverse of 9 is itself, since $9 \cdot 9 = 81$, so $d = 9$ in this case.

(b) If the receiver gets 4, what was the original message?

**Solution:** The receiver gets 4, so using our decryption function $D(y) = y^d = 4^9 \pmod{55}$. So we can write:

$$\begin{aligned} 4^9 &\equiv (64)^3 \pmod{55} \\ &\equiv (9)^3 \pmod{55} \\ &= 729 \pmod{55} \end{aligned}$$

We can then compute this by hand, which gives us a remainder of 14, so the original message was 14.

(c) Encode your answer from part (b) to check its correctness.

**Solution:** So we have $x = 14$, so since we have $e^9$, we evaluate $14^9 \pmod{55}$:

$$14^9 \equiv (-41)^9 x \pmod{55}$$

We can then split the mod:

$$\begin{aligned}
14^9 &\equiv (-1)^9 \pmod{5} \\
&\equiv 4 \pmod{5} \\
14^9 &\equiv (3)^9 \pmod{11} \\
&\equiv 3(9)^4 \pmod{11} \\
&\equiv 3(16) \pmod{11} \\
&\equiv 4 \pmod{11}
\end{aligned}$$

And so we know that $14^9 \equiv 4$ both in mod 5 and mod 11, so therefore $14^9 \equiv 4 \pmod{55}$ as well. Thus, our encoding gives us 4, which matches what the reciever got in part (b).

## 2 Tweaking RSA

You are trying to send a message to your friend, and as usual, Eve is trying to decipher what the message is. However, you get lazy, so you use $N = p$, and $p$ is prime. Similar to the original method, for any message $x \in \{0, 1, \ldots, N-1\}$, $E(x) \equiv x^e \pmod{N}$, and $D(y) \equiv y^d \pmod{N}$.

(a) Show how you choose $e$ and $d$ in the encryption and decryption function, respectively. Prove that the message $x$ is recovered after it goes through your new encryption and decryption functions, $E(x)$ and $D(y)$.

**Solution:** We show that $(x^e)^d \equiv x \pmod{p}$. First, since $ed \equiv 1 \pmod{p-1}$ by definition, then we can write $ed = k(p-1)$ for some integer $k$. Therefore, we can rewrite our exponential:

$$x^{ed} = x \cdot x^{k(p-1)}$$

Where $x^{k(p-1)} \equiv \left(x^{p-1}\right)^k \equiv 1 \pmod{p}$ from Fermat's little theorem. Thus, we have:

$$x^{ed} \equiv x \pmod{p}$$

And thus we've recovered $x$, so our encryption scheme works. ■

(b) Can Eve now compute $d$ in the decryption function? If so, by what algorithm?

**Solution:** Since we know that $N = p$, then we know that $e$ is coprime to $p-1$, and from there we can compute $d$ via the Euclidean Algorithm, which isn't difficult to compute on a computer.

(c) Now you wonder if you can modify the RSA encryption method to work with three primes ($N = pqr$ where $p, q, r$ are all prime). Explain how you can do so, and include a proof of correctness showing that $D(E(x)) = x$.

**Solution:** We follow in a very similar fashion to the RSA scheme where $N = pq$. We choose $e$ such that $e$ is coprime to $(p-1)(q-1)(r-1)$, and $d = e^{-1} \pmod{(p-1)(q-1)(r-1)}$. Therefore, by definition, $ed \equiv 1 \pmod{(p-1)(q-1)(r-1)}$. Now to show correctness, we want to show that:

$$x^{ed} \equiv x \pmod{N}$$

Since $ed \equiv 1 \pmod{(p-1)(q-1)(r-1)}$, then we can write $ed = 1 + k(p-1)(q-1)(r-1)$. Therefore,

$$x^{ed} - x = x^{1+k(p-1)(q-1)(r-1)} - x = x\left(x^{k(p-1)(q-1)(r-1)} - 1\right)$$

Now our goal is to show that this last expression is equal to 0 mod $N$ for all $x$. To do this, we show that it is individually divisible by $p$, $q$ and $r$ for any $x$. The same argument is done for all three primes (since the expression is symmetric), so I'll do it for $p$ only.

- If $x$ is divisible by $p$, then $x(x^{k(p-1)(q-1)(r-1)}-1)$ is clearly divislble by $p$, since it contains $x$ as a factor.
- If $x$ is not divisible by $p$, then $x$ is coprime to $p$, so $x^{k(p-1)(q-1)(r-1)}$ can be rearranged to $\left(x^{p-1}\right)^{k(q-1)(r-1)} \equiv 1^{k(q-1)(r-1)} \equiv 1 \pmod{p}$ by FLT. Therefore $x^{k(p-1)(q-1)(r-1)} - 1 \equiv 0 \pmod{p}$, so the entire expression is still divisible by $p$.

As mentioned previously, the same argument holds for primes $q$ and $r$, since we can write $x^{k(p-1)(q-1)(r-1)} = \left(x^{q-1}\right)^{k(p-1)(r-1)} \equiv 1 \pmod{q}$ and $x^{k(p-1)(q-1)(r-1)} = \left(x^{r-1}\right)^{k(p-1)(q-1)} \equiv 1 \pmod{r}$ if $x$ is coprime to either $q$ or $r$, so the expression is always divisible by $p, q$ and $r$.

Because $p, q, r$ are prime, then this expression must be divisible by $p$, $q$, and $r$ simultaneously, for any $x$. Then, since $N = pqr$, it also follows that this expression is always divisible by $N$ for any $x$, so we are done. ■

# 3 Secret Sharing

Suppose the Oral Exam questions are created by 2 TAs and 3 Readers. The answers are all encrypted, and we know that:

- Two TAs together should be able to access the answers
- Three Readers together should be able to access the answers
- One TA and one Reader together should also be able to access the answers

Design a Secret Sharing scheme to make this work.

**Solution:** We generate three polynomials, $P(x)$ with degree 1, $Q(x)$ with degree 2, and $R(x)$ with degree 2. We let $P(0) = Q(0) = R(0) = s$ (the answers). Now we do the following:

- Give one TA $P(1)$, and the other $P(2)$. This way when the TAs come together they can access the answers by solving for $P(x)$.
- Give one reader $Q(1)$, another $Q(2)$ and the last $Q(3)$. This way when the readers come together they can access the answers by solving for $Q(x)$.
- Give one reader $R(1)$, another $R(2)$ and the last $R(3)$. Then, give $R(4), R(5)$ to both TAs. This way, no two readers can come together to solve $R(x)$ but one reader and one TA collectively have 3 distinct points, so they can solve for $R(x)$.

And so with this set of $P(x)$, $Q(x)$ and $R(x)$ and this way of distributing points we guarantee that the conditions given in the problem statement are satisfied. ■

# 4 Trust No One

Gandalf has assembled a fellowship of eight peoples to transport the One Ring to the fires of Mount Doom: four hobbits, two humans, one elf, and one dwarf. The ring has great power that may be of use to the fellowship during their long and dangerous journey. Unfortunately, the use of its immense power will eventually corrupt the user, so it must not be used except in the most dire of circumstances. To safeguard against this possibility, Gandalf wishes to keep the instructions a secret from members of the fellowship. The secret must only be revealed if enough members of the fellowship are present and agree to use it.

Gandalf has hired your services to help him come up with a secret sharing scheme that accomplishes this task, summarized by the following points:

- There is a party of four hobbits, two humans, an elf, and a dwarf, and a secret message that must remain unknown to everyone if not enough members of the party agree.
- A group of people consisting of at least two people from different people classes and at least one people class that is fully represented (i.e., has all members present) can unlock the secret of the ring.

A few examples: only four hobbits agreeing to use the ring is not enough to know the instructions. One human and three hobbits is not enough. However, all four hobbits and one human agreeing is enough. Both humans and the dwarf agreeing is enough.

**Solution:** Construct a polynomial $P(x)$ of degree 4 with $P(0) = s$ (the secret), so that 5 points are required in order to find $s$. Then, we do the following:

- Give $P(1), P(2), P(3), P(4)$ to the elf.
- Give $P(5), P(6), P(7), P(8)$ to the dwarf.
- Give $P(9)$ to the first hobbit, $P(10)$ to the second, $P(11)$ to the third and $P(12)$ to the fourth.
- Give $P(13)$ to one human and $P(14)$ to the other.

In this construction, one elf or one dwarf combined with anybody else has enough information to solve for $P(x)$. Furthermore, 2 humans or 4 hobbits alone cannot solve for $P(x)$, and no combination of them without either including both humans or all 4 hobbits can solve for $P(x)$ either. Thus, to solve for $s$ without the elf or dwarf, either the humans must be fully represented or the hobbits must be fully represented. ■

# 5 Lagrange? More like Lamegrange.

In this problem, we walk you through an alternative to Lagrange interpolation.

(a) Let's say we wanted to interpolate a polynomial through a single point, $(x_0, y_0)$. What would be the polynomial that we would get? (This is not a trick question.)

**Solution:** The polynomial must be defined over all reals, so we can choose $f_0(x) = y_0$.

(b) Call the polynomial from the previous part $f_0(x)$. Now say we wanted to define the polynomial $f_1(x)$ that passes through the points $(x_0, y_0)$ and $(x_1, y_1)$. If we write $f_1(x) = f_0(x) + a_1(x - x_0)$, what value of $a_1$ causes $f_1(x)$ to pass through the desired points?

**Solution:** It's clear that $f_1(x_0) = f_0(x_0) = y_0$, so we check $f_1(x_1)$, and force it to pass through $y_1$:

$$f_1(x_1) = y_1 = y_0 - a_1(x_1 - x_0)$$

So rearranging here, we get that

$$a_1 = \frac{y_1 - y_0}{x_1 - x_0}$$

(c) Now say we want a polynomial $f_2(x)$ that passes through $(x_0, y_0)$, $(x_1, y_1)$, and $(x_2, y_2)$. If we write $f_2(x) = f_1(x) + a_2(x - x_0)(x - x_1)$, what value of $a_2$ gives us the desired polynomial?

**Solution:** We write $f_2(x_2)$:

$$\begin{aligned} f_2(x_2) = y_2 &= f_1(x_2) + a_2(x_2 - x_0)(x_2 - x_1) \\ &= \left( f_0(x_2) + \frac{y_1 - y_0}{x_1 - x_0}(x_2 - x_0) \right) + a_2(x_2 - x_0)(x_2 - x_1) \end{aligned}$$

By rearranging and solvign for $a_2$ (which is pure algebra, so I'm going to skip it), we obtain our result:

$$\therefore a_2 = \frac{y_2 - y_0 - \frac{y_1 - y_0}{x_1 - x_0}(x_2 - x_0)}{(x_2 - x_0)(x_2 - x_1)}$$

(d) Suppose we have a polynomial $f_i(x)$ that passes through the points $(x_0, y_0)$, ..., $(x_i, y_i)$ and we want to find a polynomial $f_{i+1}(x)$ that passes through all those points and also $(x_{i+1}, y_{i+1})$. If we define $f_{i+1}(x) = f_i(x) + a_{i+1} \prod_{j=0}^{i} (x - x_j)$, what value must $a_{i+1}$ take on?

**Solution:** We assume that $f_i(x)$ is known, so we can rearrange:

$$a_{i+1} = \frac{y_{i+1} - f_i(x_{i+1})}{\prod_{j=0}^{i}(x - x_j)}$$

To show that $f_{i+1}(x)$ also passes through points $(x_0, y_0), \ldots, (x_i, y_i)$, notice that notice that whenever $x = x_i$ then then the second term in $f_{i+1}(x)$ goes to zero since there exists a term in that proudct which is $(x_i - x_i) = 0$, so

$$f_{i+1}(x) = f_i(x)$$

And since $f_i(x)$ is already known to pass through $(x_0, y_0), \ldots, (x_i, y_i)$, then $f_{i+1}(x)$ also does since at every $x = x_i$ we have $f_{i+1}(x) = f_i(x)$. ■

# 6 Equivalent Polynomials

This problem is about polynomials with coefficients in GF($q$) for some prime $q \in \mathbb{N}$. We say that two such polynomials $f$ and $g$ are *equivalent* if $f(x) = g(x)$ for every $x \in \text{GF}(q)$.

(a) Use Fermat's Little Theorem to find a polynomial with degree strictly less than 5 that is equivalent to $f(x) = x^5$ over GF(5); then find a polynomial with degree strictly less than 11 that is equivalent to $g(x) = 1 + 3x^{11} + 7x^{13}$ over GF(11).

**Solution:** For $f(x) = x^5 \equiv x \pmod 5$, so $f(x) = x$ is equivalent. For $g(x) = 1 + 3x^1 1 + 7x^1 3$, we can rewrite $3x^1 1 \equiv x \pmod{11}$ and $7x^{13} \equiv 7x^1 1 \cdot x^2 \equiv 7x^3 \pmod{11}$, so $g(x) = 1 + 3x + 7x^3$ is equivalent.

(b) Prove that whenever $f(x)$ has degree $\geq q$, it is equivalent to some polynomial $\tilde{f}(x)$ with degree $< q$.

**Solution:** Assume that we are taking GF($q$). Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$. We know that for all terms which have degree $k \geq q$, then we can rewrite that term as

$$a_k x^k = a_k \left( x^{q-1} \cdot x^{k-q+1} \right)$$

And by FLT we have that $x^{q-1} \equiv 1 \pmod q$, so we get

$$a_k x^k = a_k x^{k-q+1}$$

And since $k - q + 1 < k$ for prime $q \in \mathbb{N}$, we have successfully reduced the degree of the exponent. Now notice that we can repeat this process until we obtain a term with degree less than $q$, since every time we apply this rule we are reducing the exponent. Furthermore, we can apply this to every term in the polynomial, so the resulting polynomial is guaranteed to have all terms with degree $< q$. ■

# 7 The CRT and Lagrange Interpolation

Let $n_1, \ldots n_k$ be pairwise co-prime, i.e. $n_i$ and $n_j$ are co-prime for all $i \neq j$. The Chinese Remainder Theorem (CRT) tells us that there exist solutions to the following system of congruences:

$$x \equiv a_1 \pmod{n_1} \tag{1}$$
$$x \equiv a_2 \pmod{n_2} \tag{2}$$
$$\vdots \tag{$\vdots$}$$
$$x \equiv a_k \pmod{n_k} \tag{$k$}$$

and all solutions are equivalent $\pmod{n_1 n_2 \cdots n_k}$. For this problem, parts (a)-(c) will walk us through a proof of the Chinese Remainder Theorem. We will then use the CRT to revisit Lagrange interpolation.

(a) We start by proving the $k = 2$ case: Prove that we can always find an integer $x_1$ that solves $(1)$ and $(2)$ with $a_1 = 1, a_2 = 0$. Similarly, prove that we can always find an integer $x_2$ that solves $(1)$ and $(2)$ with $a_1 = 0, a_2 = 1$.

**Solution:** Let's look at $x_1$, for which we have the following congruences:

$$x_1 \equiv 1 \pmod{n_1}$$
$$x_2 \equiv 0 \pmod{n_2}$$

Note that this means that $x_2 = kn_2$ for some integer $k$. Now we substitute this into the first equation to get $x_1 \equiv kn_2 \pmod{n_1}$. In order to make the right hand side equal to 1, notice that $n_2$ is coprime to $n_1$, so we can choose $k = n_2^{-1} \pmod{n_1}$ to arrive at a valid solution.

We can do the exact same thing with $x_2$, where we have:

$$x_2 \equiv 0 \pmod{n_1}$$
$$x_2 \equiv 1 \pmod{n_2}$$

which means that we can write $x_2 = kn_1$ from the first equation, then we get that $k = n_1^{-1} \pmod{n_2}$ to satisfy the second equation.

Thus, we've proven that $x_1$ and $x_2$ always exists. ■

(b) Use part (a) to prove that we can always find at least one solution to $(1)$ and $(2)$ for any $a_1, a_2$. Furthermore, prove that all possible solutions are equivalent $\pmod{n_1 n_2}$.

**Solution:** Taking inspiration from part a, let's set up the following congruences:

$$x_1 \equiv 1 \pmod{n_1}$$
$$x_1 \equiv 0 \pmod{n_2}$$

for $x_1$ and the following for $x_2$:

$$\begin{aligned} x_2 &\equiv 0 \pmod{n_1} \\ x_2 &\equiv 1 \pmod{n_2} \end{aligned}$$

From part (a) we know that this set of congruences always has a solution. Now we multiply the first set of congruences by $a_1$ and the second set by $a_2$, so now we get:

$$\begin{aligned} a_1x_1 &\equiv a_1 \pmod{n_1} \\ a_1x_1 &\equiv 0 \pmod{n_2} \end{aligned} \qquad \begin{aligned} a_2x_2 &\equiv 0 \pmod{n_1} \\ a_2x_2 &\equiv a_2 \pmod{n_2} \end{aligned}$$

Now, we can sum the congruences modulo $n_1$ and $n_2$ to get:

$$\begin{aligned} a_1x_1 + a_2x_2 &\equiv a_1 \pmod{n_1} \\ a_1x_1 + a_2x_2 &\equiv a_2 \pmod{n_2} \end{aligned}$$

Now we have the same number on the left hand side! Let's call $a_1x_1 + a_2x_2 = X$. Then, we can rewrite this as:

$$\begin{aligned} X &\equiv a_1 \pmod{n_1} \\ X &\equiv a_2 \pmod{n_2} \end{aligned}$$

And since $x_1$, $x_2$ are guaranteed to exist from part (a), we also know that $X$ always exists, and so this system of congruences must also exist. To prove that this solution is unique mod $n_1n_2$, let's suppose that there exists another $X'$ which also satisfies:

$$\begin{aligned} X' &\equiv a_1 \pmod{n_1} \\ X' &\equiv a_2 \pmod{n_2} \end{aligned}$$

Then we can take the difference of $X - X'$:

$$\begin{aligned} X - X' &\equiv 0 \pmod{n_1} \\ X - X' &\equiv 0 \pmod{n_2} \end{aligned}$$

Now if we use the fact that if $a \equiv 0 \pmod{n_1}$ and $c \equiv 0 \pmod{n_2}$ then $a \equiv 0 \pmod{n_1n_2}$ (provided that $n_1, n_2$ are coprime), so this means that

$$X - X' \equiv 0 \pmod{n_1 n_2}$$

But this last equation also implies that $X \equiv X' \pmod{n_1 n_2}$, so they are actually the same (mod $n_1 n_2$)! Thus, $X$ is unique modulo $n_1 n_2$. ■

(c) Now we can tackle the case of arbitrary $k$: Use part (b) to prove that there exists a solution $x$ to $(1)$-$(k)$ and that this solution is unique $\pmod{n_1 n_2 \cdots n_k}$.

**Solution:** We essentially create a generalization of what we did in the previous part. Suppose that we have the set of congruences:

$$\begin{aligned} x_1 &\equiv 1 \pmod{n_1} \\ &\vdots \\ x_k &\equiv 0 \pmod{n_k} \end{aligned}$$

In other words, we can rewrite this as:

$$x_i \equiv \begin{cases} 1 \pmod{n_j} & i = j \\ 0 \pmod{n_j} & i \neq j \end{cases}$$

For any $x_i$. Again from part (a), we know that this set of congruences always exists. Now, we multiply each set of $x_i$ by $a_i$ to obtain:

$$a_i x_i \equiv \begin{cases} a_i \pmod{n_j} & i = j \\ 0 \pmod{n_j} & i \neq j \end{cases}$$

Now, for each set of congruences mod $n_i$ we can sum them up (just like we did in part (b)), to get:

$$\begin{aligned} a_1 x_1 + a_2 x_2 + \cdots + a_k x_k &\equiv a_1 \pmod{n_1} \\ a_1 x_2 + a_2 x_2 + \cdots + a_k x_k &\equiv a_2 \pmod{n_2} \\ &\vdots \\ a_1 x_2 + a_2 x_2 + \cdots + a_k x_k &\equiv a_k \pmod{n_k} \end{aligned}$$

Again, notice now that we have the same term on the left hand side, call it $X$. And since $x_1, x_2, \ldots, x_k$ are guaranteed to exist (proven from earlier), then $X$ always exists. To prove that $X$ is unique, we follow the exact same steps as part (b): suppose there exists another $X'$ that also satisfies this set of congruences. Then this means:

$$\begin{aligned} X - X' &\equiv 0 \pmod{n_1} \\ X - X' &\equiv 0 \pmod{n_2} \\ &\vdots \\ X - X' &\equiv 0 \pmod{n_k} \end{aligned}$$

And since their congruences are the same, this means that $X - X' \equiv 0 \pmod{n_1 n_2 \cdots n_k}$, so $X \equiv X' \pmod{n_1 n_2 \cdots n_k}$ which is a contradiction, so $X$ must be unique. ■

(d) For polynomials $p_1(x)$, $p_2(x)$ and $q(x)$ we say that $p_1(x) \equiv p_2(x) \bmod q(x)$ if $p_1(x) - p_2(x)$ is of the form $q(x) \times m(x)$ for some polynomial $m(x)$.

Define the polynomials $x-a$ and $x-b$ to be co-prime if they have no common divisor of degree 1. Assuming that the CRT still holds when replacing $x, a_i$ and $n_i$ with polynomials (using the definition of co-prime polynomials just given), show that the system of congruences

$$\begin{aligned} p(x) &\equiv y_1 \pmod{(x-x_1)} && (1') \\ p(x) &\equiv y_2 \pmod{(x-x_2)} && (2') \\ &\vdots && (\vdots) \\ p(x) &\equiv y_k \pmod{(x-x_k)} && (k') \end{aligned}$$

has a unique solution $\pmod{(x-x_1)\cdots(x-x_k)}$ whenever the $x_i$ are pairwise distinct. What is the connection to Lagrange interpolation?

Hint: To show that a unique solution exists, you may use the fact that the CRT has a unique solution when certain properties are satisfied.

**Solution:** First, we show that if $x_1, x_2$ are distinct then they are coprime. Suppose by contradiction that they *do* have a common divisor $m(x) = ax + b$. Therefore, we can write:

$$\begin{aligned} x - x_1 &= (ax+b)q_1(x) \\ x - x_2 &= (ax+b)q_2(x) \end{aligned}$$

We set $r(x) = 0$ for both polynomials, since $ax+b$ is a common divisor. Then, since $x - x_1$ is of degree 1, it's clear that the degree of $q_1(x)$ and $q_2(x)$ must be 0, or in other words a constant. Therefore, we can write:

$$\begin{aligned} x - x_1 &= (ax+b)c_1 = c_1 a + c_1 b \\ x - x_2 &= (ax+b)c_2 = c_2 a + c_2 b \end{aligned}$$

So matching coefficients, we get:

$$c_1 a = 1,\ c_1 b = x_1$$
$$c_2 a = 1,\ c_2 b = x_2$$

From $c_1 a = 1$ and $c_2 a = 1$, we conclude that $c_1 = c_2 = \frac{1}{a}$. If this is true, then this means that $x_1 = x_2 = \frac{b}{a}$, so $x_1 = x_2$! But this cannot be true, since $x_1, x_2$ are distinct, so we've reached a contradiction. Therefore, $ax+b$ does not exist, and so $x-x_1$ and $x-x_2$ must be coprime given distinct $x_1, x_2$.

Building off this, since we know that $x_1, \ldots, x_k$ are distinct, then each of $x-x_1, x-x_2, \ldots, x-x_k$ are also pairwise coprime, so we can now apply CRT, which guarantees a unique solution $\pmod{(x-x_1)\cdots(x-x_k)}$.

This relates to Lagrange interpolation because when we construct $p(x) = \sum y_i \Delta_i(x)$, we write it as:

$$p(x) = \sum_{i=1}^{d+1} y_i \frac{\prod_{j \neq i}(x-x_j)}{\prod_{j \neq i}(x_i - x_j)}$$

Now notice that when we take $p(x) \bmod (x-x_j)$, then we get the following set of congruences:

$$p(x) \equiv \begin{cases} y_i \Delta_i(x_i) \pmod{x-x_j} & i = j \\ 0 & \text{otherwise} \end{cases}$$

Since $(x-x_j)$ exists as a factor everywhere else *except* when $i = j$, where it is equal to $y_i \Delta_i(x_i)$. Furthermore, since $p(x_i) = y_i$ then we get that $\Delta_i(x_i) \equiv 1 \pmod{x-x_j}$. Building off this, this means that we can change our congruences to:

$$p(x) \equiv \begin{cases} y_i \pmod{x-x_j} & i = j \\ 0 & \text{otherwise} \end{cases}$$

which is the same set of congruences that we have at the beginning of the problem. Furthermore, the uniqueness of $p(x)$ is also another way to show that given $d+1$ points there exists only one unique polynomial of degree $d$ which passes through all $d+1$ points. ■