2 The CRT and Lagrange Interpolation

(a) Direct Proof

Proof. We proceed by a direct proof for both statements given $k = 2$. First, we show that: by assumption, n_1, n_2 are coprime, which is equivalent to $\gcd(n_1, n_2) = 1$, so we can write $k_1 n_1 + k_2 n_2 = 1$ for some $k_1, k_2 \in \mathbb{Z}$.

Part 1: Given that $a_1 = 1, a_2 = 0$, so we have that $x_1 \equiv 1 \pmod{n_1}, x_1 \equiv 0 \pmod{n_2}$. Now, consider $x_1 = k_2 n_2$. Since $n_2, k_2 \in \mathbb{Z}$, so $x_1 \in \mathbb{Z}$ and $x_1 \equiv 0 \pmod{n_2}$. Since we also have $x_1 = 1 - k_1 n_1 = (-k_1) \cdot (n_1) + 1$, with $-k_1 \in \mathbb{Z}$, so $x_1 \equiv 1 \pmod{n_1}$, which implies that $x_1 = k_2 n_2$ is a valid solution to the first situation.

Part 2: Given that $a_1 = 0, a_2 = 1$, so we have that $x_2 \equiv 0 \pmod{n_1}, x_2 \equiv 1 \pmod{n_2}$. Now, consider $x_2 = k_1 n_1 \in \mathbb{Z}$. Similarly, we have that $x_2 \equiv 0 \pmod{n_1}$, and with $x_2 = 1 - k_2 n_2 = (-k_2) \cdot (n_2) + 1$, so similar to Part 1 above, $x_2 \equiv 1 \pmod{n_2}$, which gives that $x_2 = k_1 n_1$ is a valid solution to the first situation.

Q.E.D.

(b) Direct Proof

Proof. We proceed by a direct proof for both statements where we still write $k_1 n_1 + k_2 n_2 = 1$ for some $k_1, k_2 \in \mathbb{Z}$.

For any given a_1, a_2, consider $x = a_1 k_2 n_2 + a_2 k_1 n_1$. So, $x = a_1(1 - k_1 n_1) + a_2 k_1 n_1 = a_1 + (-a_1 k_1 + a_2 k_1) n_1$. Since $a_1, k_1, a_2, k_2 \in \mathbb{Z}$, so $-a_1 k_1 + a_2 k_1 \in \mathbb{Z}$, which gives us that $x \equiv a_1 \pmod{n_1}$. Similarly, $x = a_1 k_2 n_2 + a_2 k_1 n_1 = a_1 k_2 n_2 + a_2(1 - k_2 n_2) = a_2 + (a_1 k_2 - a_2 k_2) n_2$ and since $a_1, k_1, a_2, k_2 \in \mathbb{Z}$, so $a_1 k_2 - a_2 k_2 \in \mathbb{Z}$, so we have $x \equiv a_2 \pmod{n_2}$. Thus, there exists at least one solutoin x to (1) and (2) for any a_1, a_2.

For any two solutions x', x^* to (1) and (2) with given a_1, a_2, we have that $x' \equiv x^* \equiv a_1 \pmod{n_1}$ and $x' \equiv x^* \equiv a_2 \pmod{n_2}$. So, $x' - x^* \equiv 0 \pmod{n_1}$ and $x' - x^* \equiv 0 \pmod{n_2}$. Since given that $\gcd(n_1, n_2) = 1$, using previous homework results, we have that $x' - x^* \equiv 0 \pmod{n_1 n_2}$. Thus, $x' \equiv x^* \pmod{n_1 n_2}$, which implies that all possible solutions are equivalent $\pmod{n_1 n_2}$, as desired.

Q.E.D.

(c) Direct Proof

Proof. We proceed by a direct proof for both statements.

Since for all $i \neq j$, it is given that n_i, n_j are coprime, so we can repeat the process we described and proved in part (b) by solving two equations at a time, which will always yield us a solution x. In other words, $\exists$ a solution x to (1)-(k).

Again, we can show that this solution is unique $\pmod{n_1 n_2 \cdots n_k}$ by showing that for any two solutions x', x^* to (1)-(k), we have $x' - x^* \equiv 0 \pmod{n_1 n_2 \cdots n_k}$ by repetitively using the strategy presented in part (b), given that for all $i \neq j$, it is given that n_i, n_j are coprime. Thus, $x' \equiv x^* \pmod{n_1 n_2 \cdots n_k}$, which implies that the solution x is unique $\pmod{n_1 n_2 \cdots n_k}$.

Q.E.D.

(d) Definition see below; $p(1)$

Let $p(x) = k(x) \cdot q(x) + r(x)$ where $k(x), r(x)$ are also polynomials and $0 \leq \deg(r) < \deg(q)$. Mimicing the definition of a mod b for integers, we define polynomial mod, $p(x)$ mod $q(x)$, to be: $q(x) \equiv r(x) \pmod{p(x)}$ where $0 \leq \deg(r) < \deg(q)$.

Then, consider when $x = 1$, we have $p(x) - p(1) = p(1) - p(1) = 0$, which means that $x = 1$ is a root for $p(x) - p(1)$ where $p(1)$ is a constant that can be calculated, which implies that $\deg(p(1)) = 0 < 1 = \deg(x - 1)$. Since we also have that $p(x) - p(1) = 0 \equiv 0 \pmod{x - 1}$, so $p(x) \equiv p(1) \pmod{x - 1}$.

Thus, $p(x) \bmod (x-1)$ is $p(1)$.

(e) Direct Proof; connection to Lagrange interpolation explained below.

Proof. We proceed by a direct proof for both statements. We claim that each of the $x - x_i$ are pairwise coprime given the x_i are pairwise distinct.

We proceed by a proof by contradiction to prove the above claim. Assume that for some two polynomials $x - x_m, x - x_n$ with $x_m \neq x_n$, they have a common divisor of degree 1, $ax + b$ and $a \neq 0$. Let R be the assertion that $x_m \neq x_n$ and let $x - x_m = k_m(ax + b), x - x_n = k_n(ax + b)$ where $k_m, k_n \in \mathbb{R}$. So, $x - x_m = ak_m x + bk_m$ and $x - x_n = ak_n x + bk_n$, which gives us these four equations:

$$\begin{aligned} 1 &= ak_m \\ -x_m &= bk_m \\ 1 &= ak_n \\ -x_n &= bk_n \end{aligned}$$

So, we have $1 = ak_m = ak_n$. With $a \neq 0$, so $k_m = k_n$. Thus, the equations above gives us that $x_m = -bk_m = -bk_n = x_n$, which implies $\neg R$. So, $R \wedge \neg R$ holds, which gives the contradiction.

Thus, our claim is true that each of the $x - x_i$ are pairwise coprime. Then, since we're told that the CRT still holds when replacing x, a_i, n_i with polynomials and using the coprime definition, so the system of congruences given has a unique solution $\pmod{(x - x_1)\cdots(x - x_k)}$ whenever the x_i are pairwise distinct.

Now, this is very similar to our Lagrange interpolation, since the way we write the greatest common divison of the $(x - x_i)$'s corresponds to the first step of finding the polynomials Δ_i, and finding the actual solution $p(x)$ by multiplication corresponds to our step in CRT where we multiply the base solution by y_i for each corresponding factor. Therefore, using the CRT for polynomials to find $p(x)$ is an equivalent method to Lagrange interpolation. Thus, this is also another proof of why Lagrange interpolation works and why there's a unique solution $p(x)$ in the modular setting, correspondingly, $GF(p)$.