Lagrange Interpolation & The Chinese Remainder Theorem

Tsz-Wo Sze

2025 · 8 · 12

Abstract

In this article, we generalize Lagrange interpolation to re-construct homogeneous polynomials of two variables. Then, we apply it to solve the puzzle below. Finally, we discuss the similarity between Lagrange interpolation and the Chinese remainder theorem.

$$\begin{aligned}
37\#21 &= 928,\\
77\#44 &= 3993,\\
123\#17 &= 14840,\\
71\#6 &= \quad ?
\end{aligned}$$

1 Lagrange Interpolation

Theorem 1 (Lagrange Interpolation)**.** *For $1 \le i \le n$, let a_i be n numbers and c_i be n numbers. Suppose $a_i \ne a_j$ for any $j \ne i$. Define the Lagrange polynomial*

$$f(x) := \sum_{1\le i\le n} c_i \prod_{1\le j\le n, j\ne i} \frac{x - a_j}{a_i - a_j}.$$

Then, f is a degree d polynomial with $d < n$ and $f(a_i) = c_i$ for all i.

Lagrange interpolation (Theorem 1) re-constructs polynomials of a single variable. We generalize it to re-construct homogeneous polynomials of two variables in Theorem 2 below. When putting $y = b_1 = \cdots = b_n = 1$, Theorem 2 is the same as Theorem 1.

Theorem 2 (Generalized Lagrange Interpolation)**.** *For $1 \le i \le n$, let (a_i, b_i) be n pairs of numbers and c_i be n numbers. Suppose*

$$a_i b_j - a_j b_i \ne 0 \qquad \text{for any } j \ne i. \tag{1.1}$$

Define the homogeneous Lagrange polynomial

$$f(x, y) := \sum_{1\le i\le n} c_i \prod_{1\le j\le n, j\ne i} \frac{x b_j - a_j y}{a_i b_j - a_j b_i}. \tag{1.2}$$

Then, f is a degree d homogeneous polynomial with $d < n$ and $f(a_i, b_i) = c_i$ for all i.

1.1 Solving The Puzzle

We apply Theorem 2 to solve the puzzle mentioned in the abstract. Using the notation $a_i\#b_i = c_i$, let $a_1 = 37, b_1 = 21, c_1 = 928, a_2 = 77, b_2 = 44, c_2 = 3993, a_3 = 123, b_3 = 17, c_3 = 14840$. Then,

$$\begin{aligned}
a_1b_2 - a_2b_1 &= 37\cdot 44 - 77\cdot 21 &&= 11,\\
a_1b_3 - a_3b_1 &= 37\cdot 17 - 123\cdot 21 &&= -1954,\\
a_2b_3 - a_3b_2 &= 77\cdot 17 - 123\cdot 44 &&= -4103;
\end{aligned}$$

$$\begin{aligned}
x\#y &= \frac{c_1(xb_2 - a_2y)(xb_3 - a_3y)}{(a_1b_2 - a_2b_1)(a_1b_3 - a_3b_1)} + \frac{c_2(xb_1 - a_1y)(xb_3 - a_3y)}{(a_2b_1 - a_1b_2)(a_2b_3 - a_3b_2)} + \frac{c_3(xb_1 - a_1y)(xb_2 - a_2y)}{(a_3b_1 - a_1b_3)(a_3b_2 - a_2b_3)}\\
&= 928\frac{(44x - 77y)(17x - 123y)}{(11)(-1954)} + 3993\frac{(21x - 37y)(17x - 123y)}{(-11)(-4103)} + 14840\frac{(21x - 37y)(44x - 77y)}{(1954)(4103)}\\
&= x^2 - y^2.
\end{aligned}$$

Finally, $71\#6 = 71^2 - 6^2 = 5005$.

1.2 The Idea Behind Lagrange Interpolation

Lagrange polynomial (1.2) looks complicated but the idea behind it actually is simple. Given n distinct pairs (a_i, b_i) and n numbers c_i, construct a homogeneous polynomial f satisfying $f(a_i, b_i) = c_i$. For discussion purpose, set $n = 3$. Let

$$f(x, y) := c_1\delta_1(x, y) + c_2\delta_2(x, y) + c_3\delta_3(x, y),$$

where δ_i's are homogeneous polynomials with the following property:

$$\delta_i(x, y) := \begin{cases} 1 & \text{, if } x = a_i \text{ and } y = b_i, \\ 0 & \text{, if } x = a_j \text{ and } y = b_j \text{ for } j \neq i. \end{cases} \tag{1.3}$$

Then, $f(a_i, b_i) = c_i$ for $i = 1, 2, 3$ as desired. The remaining task is to construct δ_i's.

Take δ_1 as an example. Since we want to have $\delta_1(a_2, b_2) = 0$ and $\delta_1(a_3, b_3) = 0$, define it as

$$\delta_1(x, y) := g_2(x, y)g_3(x, y)k_1,$$

where $g_i(x, y) := xb_i - a_iy$ and k_1 is a constant. Note that $g_i(a_i, b_i) = 0$ for all i. Then,

$$\delta_1(x, y) = \begin{cases} g_2(a_1, b_1)g_3(a_1, b_1)k_1 & \text{, if } x = a_1 \text{ and } y = b_1, \\ 0 & \text{, if } x = a_j \text{ and } y = b_j \text{ for } j \neq 1. \end{cases}$$

By assumption (1.1), we have $g_j(a_i, b_i) \neq 0$ for all $j \neq i$. In order to have $\delta_1(a_1, b_1) = 1$, set $k_1 := k_{1,2}k_{1,3}$, where $k_{i,j} := 1/g_j(a_i, b_i)$ for all $j \neq i$. Therefore,

$$\delta_1(x, y) = g_2(x, y)g_3(x, y)k_{1,2}k_{1,3} = \frac{(xb_2 - a_2y)(xb_3 - a_3y)}{(a_1b_2 - a_2b_1)(a_1b_3 - a_3b_1)}$$

satisfies property (1.3). Of course, δ_2 and δ_3 can be constructed similarly.

2 Chinese Remainder Theorem

Theorem 3 (Chinese Remainder Theorem)**.** *Let $a_1, \ldots, a_n > 1$ be n pairwise coprime integers. Let $c_1, \ldots, c_n$ and m be integers such that*

$$m \equiv c_1 \pmod{a_1}, \qquad \cdots, \qquad m \equiv c_n \pmod{a_n}. \tag{2.1}$$

Then,

$$m \equiv \sum_{1 \leq i \leq n} c_i \prod_{1 \leq j \leq n, j \neq i} a_jk_{i,j} \pmod{A}, \tag{2.2}$$

where $A := \prod_{1 \leq i \leq n} a_i$ and $k_{i,j}$'s are integers such that $k_{i,j} \equiv a_j^{-1} \pmod{a_i}$ for $j \neq i$.

2.1 The Idea Behind The Chinese Remainder Theorem

Interestingly, the Chinese remainder theorem equation (2.2) looks similar to the Lagrange polynomial (1.2). Indeed, the ideas behind them are essentially the same. As before, we set $n = 3$ in the following discussion. Let

$$m := c_1\delta_1 + c_2\delta_2 + c_3\delta_3,$$

where δ_i's are integers such that

$$\delta_i \bmod a_j \equiv \begin{cases} 1 & \text{, if } j = i, \\ 0 & \text{, if } j \neq i. \end{cases} \tag{2.3}$$

Then, m satisfies conditions (2.1) as desired. The remaining task is to construct δ_i's.

Take δ_1 as an example. Since we want to have $\delta_1 \equiv 0 \pmod{a_2}$ and $\delta_1 \equiv 0 \pmod{a_3}$, define it as

$$\delta_1 := a_2a_3k_1,$$

for some integer k_1. Then,

$$\delta_1 \bmod a_j \equiv \begin{cases} a_2a_3k_1 & \text{, if } j = 1, \\ 0 & \text{, if } j \neq 1. \end{cases}$$

By the assumption of a_i's being pairwise coprime, the multiplicative inverses of $a_2, a_3 \pmod{a_1}$ exist and they are respectively $k_{1,2}, k_{1,3}$. In order to have $\delta_1 \equiv 1 \pmod{a_1}$, set $k_1 := k_{1,2}k_{1,3}$. Therefore,

$$\delta_1 = a_2a_3k_{1,2}k_{1,3}$$

satisfies property (2.3). Of course, δ_2 and δ_3 can be constructed similarly.