n distinct points on $\mathbb{R}$

$\{x_1, x_2, \ldots, x_n\}$ $x_i \neq x_j$

$P(x)$ – polynomial

Values of polynomial at point $x_i$:

$P(x_i) = y_i$

$P(x) = y_i + (x - x_i) \cdot \ldots$

---

$\bar{P}_1(x), \bar{P}_2(x)$: $\bar{P}_1(x_i) = \bar{P}_2(x_i)$ $(i = 1, \ldots, n)$

$P_1(x_i) - P_2(x_i) = 0$, i. e.

$P_1(x) - P_2(x) = F(x) \underbrace{(x - x_1)(x - x_2) \ldots (x - x_n)}_{Q(x)}$

$Q(x)$ divides $P_1(x) - P_2(x)$

We look for polynomial $P(x)$ such that

$P(x_i) = y_i$

order $P(x) \leq n - 1$.

n distinct primes

$\{p_1, p_2, \ldots, p_n\}$ $p_i \neq p_j$

'Value' of number $\underline{\underline{N}}$ at prime $p_i$

$N(p_i) = a_i = N (\mathrm{mod}\, p_i)$

$N = a_i + p_i \cdot \ldots$

---

Value of N at prime $p_i$ takes values in the field $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_{p_i}$

$N = 104$, $\{p_1, p_2, p_3\} = \{3, 5, 7\}$

$N(p_1) = 2 \in \mathbb{F}_3$, $N(p_2) = 4 \in \mathbb{F}_5$, $N(p_3) = 6 \in \mathbb{F}_7$

---

$N_1, N_2$: $N_1(p_i) = N_2(p_i)$ $(i = 1, \ldots, n)$

$N_1(p_i) - N_2(p_i) = 0$

$N_1 - N_2 = F \underbrace{p_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_n}_{Q}$

$Q = p_1 p_2 \ldots p_n$ divides $N_1 - N_2$

We look for integer $N$ such that

$N(p_i) = a_i$ (~~mod $p_i$~~), i.e. $N = a_i (\mathrm{mod}\, p_i)$

$0 \leq N \leq p_1 p_2 \ldots p_n$

We identify ~~remai~~ remainder with element of field $\mathbb{F}_{p_i}$

$$H_i(x) = \frac{Q(x)}{x - x_i} = \prod_{m \neq i} (x - x_m)$$

$H_1(x) = (x-x_2)\dots(x-x_n)$, $H_2(x) = (x-x_1)(x-x_3)\dots(x-x_n)$

$H_i(x)$: $H_i(x_m) = 0$ if $i \neq m$

$$H_i(x_i) = \left.\frac{Q(x)}{x - x_i}\right|_{x = x_i} = \frac{Q(x) - Q(x_i)}{x - x_i} = Q'(x_i)$$

$$h_i(x) = \frac{H_i(x)}{Q'(x_i)} = \frac{1}{Q'(x_i)} \frac{Q(x)}{x - x_i}$$

$h_i(x)$: $h_i(x_m) = \begin{cases} 0 & \text{if } i \neq m \\ 1 & \text{if } i = m \end{cases}$

$$H_i = \frac{Q}{P_i} = \frac{P_1 \cdot P_2 \cdot \dots \cdot P_n}{P_i} = \prod_{m \neq i} P_m$$

$H_1 = P_2 \cdot \dots \cdot P_n$, $H_2 = P_1 \cdot P_3 \cdot \dots \cdot P_n$, ..

$H_i(P_m) = 0$ if $m \neq i$ $\quad (P_m \mid H_i)$

$$H_i(P_i) = \left(\prod_{m \neq i} P_m\right)(P_i) = H_i(\mathrm{mod}\, P_i) = Q_i'(P_i) \in \mathbb{F}_{P_i}$$

---

Example: $N = 104$ $\quad \{P_1, P_2, P_3\} = \{3, 5, 7\}$

$Q_1'(P_1) = H_1(P_1) = 35(3) = 2 \in \mathbb{F}_3$

$Q_2'(P_2) = H_2(P_2) = 21(5) = 1 \in \mathbb{F}_5$

$Q_3'(P_3) = H_3(P_3) = 15(7) = 1 \in \mathbb{F}_7$

---

$$h_i = \frac{H_i}{Q'(P_i)} = H_i \cdot \left(\frac{1}{H_i(P_i)}\right)$$

$h_i$: $h_i(P_m) = \begin{cases} 0 & \text{if } i \neq m \\ 1 & \text{if } i = m \end{cases}$

---

Ex.

$h_1 = \frac{H_1}{H_1(P_1)} = 35 \cdot \left(\frac{1}{2}\right)_3 = 35 \cdot (2)_3 = 70.$

$h_2 = \frac{H_2}{H_2(P_2)} = 21 \cdot (1)_5 = \qquad = 21$

$h_3 = \frac{H_3}{H_3(P_3)} = 15 \cdot (1)_7 = \qquad = 15$

$$h_i(x), \quad h_i(x_m) = \delta_{im}$$

$$P(x) = \sum_i P(x_i) \cdot h_i(x) = \sum_i y_i \, h_i(x).$$

$$P(x) = \sum_i y_i \frac{Q(x)}{Q'(x_i)(x-x_i)}$$

$$h_i: \quad h_i(p_m) = \delta_{im}$$

$$N = \sum_m N(p_m)\, h_m = \sum a_m h_m$$

$$N = \sum a_m \prod_{k \neq m} p_k \left( \frac{1}{\prod_{k\neq m} p_k} \right)_{p_m}$$

Ex. $\{p_1, p_2, p_3\} = \{3, 5, 7\}$

$\{a_1, a_2, a_3\} = \{2, 3, 4\}$

$$h_1 = 35 \cdot \left(\frac{1}{35}\right)_3 = 35 \cdot \left(\frac{1}{2}\right)_3 = 70.$$

$$h_2 = 21 \cdot \left(\frac{1}{21}\right)_5 = 21,$$

$$h_3 = 15 \cdot \left(\frac{1}{15}\right)_7 = 15.$$

$$N = a_1 h_1 + a_2 h_2 + a_3 h_3 =$$

$$= 3 \cdot 70 + 2 \cdot 21 + 4 \cdot 15$$