1 Polynomial interpolation and its application

Oleg Demchenko, St.Petersburg State University

1.1 Polynomial interpolation

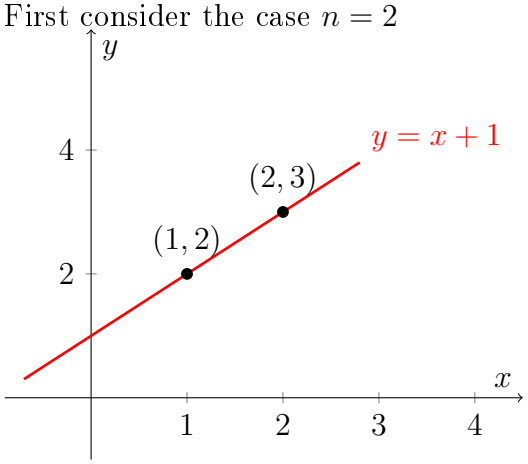
Definition. Interpolation data is given by two sets of n real numbers each, $x_1, \dots, x_n$ (the **nodes**) and $y_1, \dots, y_n$ such that $x_i \neq x_j$ for $i \neq j$.

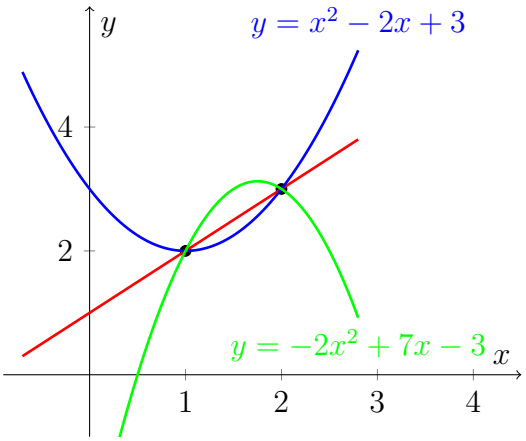
Interpolation data is often represented as a table

x	x_1				x_n
y	y_1				y_n

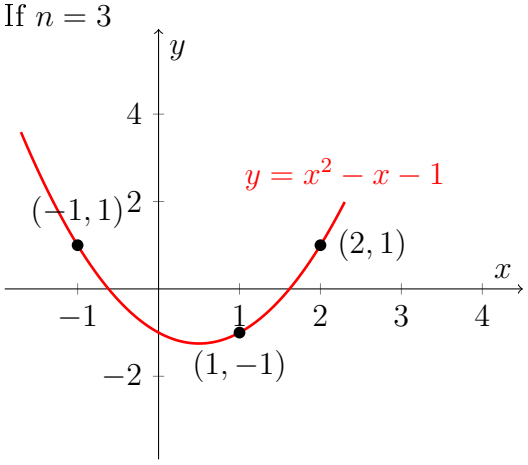
Definition. Interpolation polynomial for interpolation data $x_1, \dots, x_n$; $y_1, \dots, y_n$ is a polynomial $f \in \mathbb{R}[x]$ such that $f(x_i) = y_i$ for $1 \leq i \leq n$.

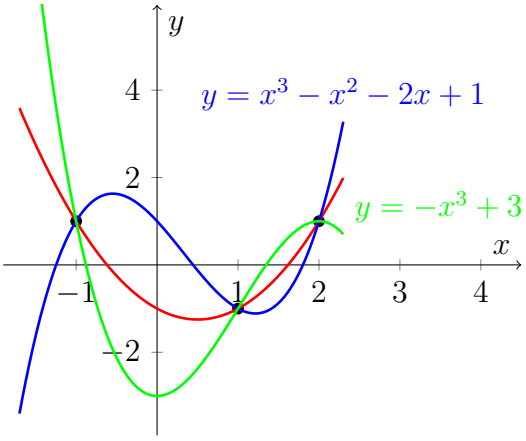
First consider the case $n = 2$





If $n = 3$





Theorem 1.1 (Interpolation theorem). *There exists a unique interpolation polynomial of degree not exceeding $n - 1$ for interpolation data $x_1, \dots, x_n$; $y_1, \dots, y_n$.*

Proof. Denote

$$\varphi_i(x) = (x - x_1) \cdots (x - x_{j-1})(x - x_{j+1}) \cdots (x - x_n).$$

Note that $\deg(\varphi_i) = n-1$, and $x_1, \dots, x_{i-1}, x_{i+1} \dots, x_n$ are its roots with $\varphi_i(x_i) \neq 0$.

Consider the polynomial

$$f(x) = \frac{y_1}{\varphi_1(x_1)}\varphi_1(x) + \dots + \frac{y_i}{\varphi_i(x_i)}\varphi_i(x) + \dots + \frac{y_n}{\varphi_n(x_n)}\varphi_n(x).$$

One can easily see that $f(x_i) = y_i$ for any $1 \leq i \leq n$, i.e., f is an interpolation polynomial. Moreover, $\deg f \leq n-1$, since $\deg \varphi_i = n-1$ for any $1 \leq i \leq n$.

Let $f, g \in \mathbb{R}[x]$ be two interpolation polynomials of degree $< n$. This implies $f(x_i) = y_i = g(x_i)$ for all $i = 1, \dots, n$. Consider the polynomial $h = f - g$; then $h(x_i) = f(x_i) - g(x_i) = 0$ for all i. All x_i are different, thus h has n different roots $x_1, \dots, x_n$. On the other hand, $\deg h \leq \max(\deg f, \deg g) \leq n-1$. By D'Alembert's Theorem, a polynomial of degree $< n$ cannot have n roots unless the polynomial is the zero polynomial. Thus $h = 0$, and $f = g$. □

Definition. The polynomial

$$\boxed{f = \sum_{i=1}^{n} y_i \frac{(x-x_1)\dots(x-x_{i-1})(x-x_{i+1})\dots(x-x_n)}{(x_i-x_1)\dots(x_i-x_{i-1})(x_i-x_{i+1})\dots(x_i-x_n)}}$$

is called the **Lagrange interpolating polynomial**.

Example. Consider interpolation data

x	-1	1	2
y	1	-1	0

The Lagrange interpolating polynomial then equals

$$\begin{aligned} f(x) =& 1 \cdot \frac{(x-1)(x-2)}{(-1-1)(-1-2)} + (-1) \cdot \frac{(x-(-1))(x-2)}{(1-(-1))(1-2)} + 0 \cdot \frac{(x-(-1))(x-1)}{(2-(-1))(2-1)} \\ =& \frac{1}{6}(x^2 - 3x + 2) + \frac{1}{2}(x^2 - x - 2) = \frac{2}{3}x^2 - x - \frac{2}{3} \end{aligned}$$

An alternative approach to polynomial interpolation is obtained if we use linear algebra. If $f(x) = a_{n-1}x^{n-1} + \dots + a_1 x + a_0$ is a required interpolation polynomial then

$$\begin{cases} a_{n-1}x_1^{n-1} + \dots + a_1 x_1 + a_0 = y_1 \\ a_{n-1}x_2^{n-1} + \dots + a_1 x_2 + a_0 = y_2 \\ \qquad\qquad\qquad\qquad \vdots \\ a_{n-1}x_n^{n-1} + \dots + a_1 x_n + a_0 = y_n \end{cases}.$$

It can be considered as a system of linear equations in the variables $a_{n-1}, \dots, a_1, a_0$. The solution of this system can be found by Cramer's rule: $a_i = D_i/D$ for $0 \leq i \leq n-1$, where

$$D = \begin{vmatrix} x_1^{n-1} & \dots & x_1 & 1 \\ x_2^{n-1} & \dots & x_2 & 1 \\ \vdots & & \vdots & \vdots \\ x_n^{n-1} & \dots & x_n & 1 \end{vmatrix}, \qquad D_i = \begin{vmatrix} x_1^{n-1} & \dots & x_1^{i+1} & y_1 & x_1^{i-1} & \dots & x_1 & 1 \\ x_2^{n-1} & \dots & x_2^{i+1} & y_2 & x_2^{i+1} & \dots & x_2 & 1 \\ \vdots & & \vdots & \vdots & \vdots & & \vdots & \vdots \\ x_n^{n-1} & \dots & x_n^{i+1} & y_{n-1} & x_n^{i+1} & \dots & x_n & 1 \end{vmatrix}.$$

Let's find the solution for $n = 3$. Then

$$D = \begin{vmatrix} x_1^2 & x_1 & 1 \\ x_2^2 & x_2 & 1 \\ x_3^2 & x_3 & 1 \end{vmatrix}, \quad D_0 = \begin{vmatrix} x_1^2 & x_1 & y_1 \\ x_2^2 & x_2 & y_2 \\ x_3^2 & x_3 & y_3 \end{vmatrix}, \quad D_1 = \begin{vmatrix} x_1^2 & y_1 & 1 \\ x_2^2 & y_2 & 1 \\ x_3^2 & y_3 & 1 \end{vmatrix}, \quad D_2 = \begin{vmatrix} y_1 & x_1 & 1 \\ y_2 & x_2 & 1 \\ y_3 & x_3 & 1 \end{vmatrix}.$$

One can see that

$$D = x_1^2x_2 + x_1x_3^2 + x_2^2x_3 - x_3^2x_2 - x_1^2x_3 - x_2^2x_1 = (x_2 - x_3)(x_1 - x_3)(x_1 - x_2).$$

Using cofactor expansions along the column (y_1, y_2, y_3) we can calculate the coefficient of the polynomial $a_2x^2 + a_1x + a_0 = (D_2x^2 + D_1x + D_0)/D$ at y_1:

$$\begin{aligned} \frac{1}{D}\left(\begin{vmatrix} x_2 & 1 \\ x_3 & 1 \end{vmatrix} x^2 - \begin{vmatrix} x_2^2 & 1 \\ x_3^2 & 1 \end{vmatrix} x + \begin{vmatrix} x_2^2 & x_2 \\ x_3^2 & x_3 \end{vmatrix}\right) &= \frac{1}{D}(x_2x^2 - x_3x^2 - x_2^2x + x_3^2x + x_2^2x_3 - x_3^2x_2) \\ &= \frac{(x_2 - x_3)(x - x_2)(x - x_3)}{(x_2 - x_3)(x_1 - x_3)(x_1 - x_2)} = \frac{(x - x_2)(x - x_3)}{(x_1 - x_3)(x_1 - x_2)}. \end{aligned}$$

Similar results are valid for the coefficients at y_2 and y_3 which shows that the resulting polynomial is equal to the Lagrange interpolating polynomial.

1.2 Factoring polynomials in $\mathbb{Z}[x]$ in a finite number of steps

Problem: Factor $f \in \mathbb{Z}[x]$ in a finite number of steps

Lemma 1.2. *If $f = gh$, where $f, g, h \in \mathbb{Z}[x]$ and $\deg f = n$ then either $\deg g \le [n/2]$ or $\deg h \le [n/2]$.*

Proof. If $\deg g > [n/2] \ge (n+1)/2$ and $\deg h > [n/2] \ge (n+1)/2$ then $n = \deg f = \deg g + \deg h \ge 2(n+1)/2 = n + 1$, a contradiction. □

Lemma 1.3. *If $f = gh$, where $f, g, h \in \mathbb{Z}[x]$ then the leading coefficient of f is equal to the product of the leading coefficients of g and h, and the constant term of f is equal to the product of the constant terms of g and h.*

Proof. Follows from the multiplication formula

$$(a_nx^n + \cdots + a_1x + a_0)(b_mx^m + \cdots + b_1x + b_0) = a_nb_mx^{n+m} + \cdots + (a_1b_0 + a_0b_1)x + a_0b_0.$$

□

Lemma 1.2 implies that if $\deg f = n$ then one of its factors has a degree $\le [n/2]$. The problem is that there are infinitely many polynomials of degree $\le [n/2]$.

Denote $d = [n/2]$. Let $a_0, \ldots, a_d$ be distinct integers. For each integer $(d+1)$-tuple $\mathbf{c} = (c_0, \ldots, c_d)$ such that $c_i \mid f(a_i)$ for $i = 0, \ldots, d$, we find the unique $g_{\mathbf{c}}(x) \in \mathbb{Q}[x]$ of degree $\le d$ with $g_{\mathbf{c}}(a_i) = c_i$ for all i. Since each $f(a_i)$ has only a finite number of integer divisors c_i, there is only a finite number of possible $\mathbf{c}$ and hence only a finite number of polynomials $g_{\mathbf{c}}(x)$.

It turns out that any divisor g of f in $\mathbb{Z}[x]$ of degree $\le d$ must be an $g_{\mathbf{c}}(x)$ for some $\mathbf{c}$. Indeed, suppose $f = gh$ for some $h \in \mathbb{Z}[x]$. Then $f(a_i) = g(a_i)h(a_i)$ in $\mathbb{Z}$, so $g(a_i) \mid f(a_i)$ for $i = 0, \ldots, d$. Thus the tuple $(g(a_0), \ldots, g(a_d))$ is one of the tuples $g_{\mathbf{c}}$. Lagrange interpolation gives a unique

polynomial $g_{\mathbf{c}}$ of degree $\leq d$ with $g_{\mathbf{c}}(a_i) = g(a_i)$ for $1 \leq i \leq n$. Thus, since $g_{\mathbf{c}}$ and g both have degree $\leq d$ and have the same values on $d+1$ points, they must be equal.

Thus, in order to factor f, we divide it by each of the polynomials $g_{\mathbf{c}}$. Notice that some of these polynomials have non-integer (rational) coefficients and therefore can be excluded. Lemma 1.3 suggests that if the leading coefficient or the constant term of $g_{\mathbf{c}}$ does not divide that of f, such $g_{\mathbf{c}}$ does not have to be tested.

Example. Here is an illustration of how the above factoring method works. Let $f(x) = x^4 + x + 1$. If $g(x)$ factors it must have a factor of degree ≤ 2. Choose the nodes $-1, 0, 1$. Since $g(-1) = 1, g(0) = 1$, $g(1) = 3$, we have $c_0 \mid 1, c_1 \mid 1, c_2 \mid 3$. The corresponding Lagrange polynomial is

$$g(x) = \frac{c_0}{2}x(x-1) - c_1(x-1)(x+1) + \frac{c_2}{2}x(x+1) = \frac{c_0 - 2c_1 + c_2}{2}x^2 + \frac{-c_0 + c_2}{2}x + c_1.$$

It gives the list of all possible factors of f

	$\mathbf{c} = (c_0, c_1, c_2)$	$g_{\mathbf{c}}(x)$
1	$(1, 1, 3)$	$x^2 + x + 1$
2	$(1, 1, 1)$	1
3	$(1, 1, -3)$	$-2x^2 - 2x + 1$
4	$(1, 1, -1)$	$-x^2 - x + 1$
5	$(-1, 1, 3)$	$2x + 1$
6	$(-1, 1, 1)$	$-x^2 + x + 1$
7	$(-1, 1, -3)$	$-3x^2 - x + 1$
8	$(-1, 1, -1)$	$-2x^2 + 1$
9	$(1, -1, 3)$	$3x^2 + x - 1$
10	$(1, -1, 1)$	$2x^2 - 1$
11	$(1, -1, -3)$	$-2x - 1$
12	$(1, -1, -1)$	$x^2 - x - 1$
13	$(-1, -1, 3)$	$2x^2 + 2x - 1$
14	$(-1, -1, 1)$	$x^2 + x - 1$
15	$(-1, -1, -3)$	$-x^2 - x - 1$
16	$(-1, -1, -1)$	-1

Since the leading coefficient of f is 1, the leading coefficients of its factor must be ± 1. Therefore items $3, 5, 7, 8, 9, 10, 11, 13$ cannot be factors. Items 2 and 16 are trivial factors. So only items $1, 4, 6, 12, 14, 15$ must be checked as possible factors of $x^4 + x + 1$:

Since items $1, 4, 6$ are associated to items $15, 14, 12$, respectively, we need only check the first three. Direct division shows that none are factors, therefore f is irreducible.

Remark. Notice that the number of possible factors of f depends on d but, more significantly, also depends on the number of divisors of $f(a_i)$.

Example. Now let $f(x) = 3x^6 + 4x^5 + 6x^4 - 4x^3 - x^2 - 5x + 2$. First, we make a table of the prime decomposition of $f(x_i)$ for integers $-9 \leq x_i \leq 9$.

x	$f(x)$
-9	$5^3 \cdot 17 \cdot 659$
-8	$2 \cdot 229 \cdot 1489$
-7	$3 \cdot 5 \cdot 101 \cdot 199$
-6	$2^2 \cdot 5^4 \cdot 47$
-5	$19^2 \cdot 107$
-4	$2 \cdot 3^3 \cdot 5 \cdot 37$
-3	$23 \cdot 79$
-2	$2^3 \cdot 5^2$
-1	$3 \cdot 5$
0	2
1	5
2	$2^2 \cdot 3 \cdot 31$
3	$5 \cdot 19 \cdot 37$
4	$2 \cdot 5 \cdot 41 \cdot 43$
5	$3^2 \cdot 17 \cdot 409$
6	$2^8 \cdot 5 \cdot 139$
7	$397 \cdot 1091$
8	$2 \cdot 3 \cdot 5 \cdot 17 \cdot 19 \cdot 97$
9	$5 \cdot 19 \cdot 43 \cdot 457$

Since $\deg f = 6$, we need to choose 4 nodes. If $x_0 = -3, x_1 = -1, x_2 = 1, x_3 = 7$, the corresponding Lagrange polynomial is

$$\begin{aligned} g(x) =& c_0 \frac{(x+1)(x-1)(x-7)}{(-3+1)(-3-1)(-3-7)} + c_1 \frac{(x+3)(x-1)(x-7)}{(-1+3)(-1-1)(-1-7)} \\ &+ c_2 \frac{(x+3)(x+1)(x-7)}{(1+3)(1+1)(1-7)} + c_3 \frac{(x+3)(x+1)(x-1)}{(7+3)(7+1)(7-1)} \\ =& \frac{-6c_0 + 15c_1 - 10c_2 + c_3}{480} x^3 + \frac{14c_0 - 25c_1 + 10c_2 + c_3}{160} x^2 \\ &+ \frac{6c_0 - 255c_1 + 250c_2 - c_3}{480} x + \frac{-14c_0 + 105c_1 + 70c_2 - c_3}{160} \end{aligned}$$

Then we have the possible values of c_0, c_1, c_2, c_3

c_0	c_1	c_2	c_3
± 1	± 1	± 1	± 1
± 23	± 3	± 5	± 397
± 79	± 5		± 1091
± 1817	± 15		± 433127

and the following conditions on them

$$-6c_0 + 15c_1 - 10c_2 + c_3 = \pm 480, \pm 3 \cdot 480 \tag{1}$$

$$-14c_0 + 105c_1 + 70c_2 - c_3 = \pm 160, \pm 2 \cdot 160 \tag{2}$$

$$160 \mid (14c_0 - 25c_1 + 10c_2 + c_3) \tag{3}$$

$$480 \mid (6c_0 - 255c_1 + 250c_2 - c_3) \tag{4}$$

Notice that the Lagrange polynomial corresponding to (c_0, c_1, c_2, c_3) is associated to the Lagrange polynomial corresponding to $(-c_0, -c_1, -c_2, -c_3)$. Thus we can assume one of the entries, say c_0, to be positive.

If $c_3 = \pm 433127$ then condition (2) implies

$$433127 = |-14c_0 + 105c_1 + 70c_2 \pm 160| \quad \text{or} \quad 433127 = |-14c_0 + 105c_1 + 70c_2 \pm 320|.$$

The maximum of the former quantity is $14 \cdot 1817 + 105 \cdot 15 + 70 \cdot 5 + 320 < 433127$, therefore $c_3 \neq \pm 433127$.

Then the possible values of c_0, c_1, c_2, c_3 are

c_0	c_1	c_2	c_3
1	± 1	± 1	± 1
23	± 3	± 5	± 397
79	± 5		± 1091
1817	± 15		

If $c_0 = 1817$ then condition (2) implies

$$14 \cdot 1817 = |105c_1 + 70c_2 - c_3 \pm 160| \quad \text{or} \quad 14 \cdot 1817 = |105c_1 + 70c_2 - c_3 \pm 2 \cdot 160|.$$

The maximum of the former quantity is $105 \cdot 15 + 70 \cdot 5 + 1091 + 320 < 14 \cdot 1817$, therefore $c_0 \neq \pm 1817$.

Then the possible values of c_0, c_1, c_2, c_3 are

c_0	c_1	c_2	c_3
1	± 1	± 1	± 1
23	± 3	± 5	± 397
79	± 5		± 1091
	± 15		

Conditions (1) and (3) give

$$160 \mid (-6c_0 + 15c_1 - 10c_2 + c_3)$$
$$160 \mid (14c_0 - 25c_1 + 10c_2 + c_3)$$

and we can conclude that $160 \mid 5(-6c_0 + 15c_1 - 10c_2 + c_3) + 3(14c_0 - 25c_1 + 10c_2 + c_3) = 12c_0 - 20c_2 + 8c_3$, whence $40 \mid 3c_0 - 5c_2 + 2c_3$. Then the corresponding remainders of $3c_0, 5c_2, 2c_3$ modulo 40 are

$3c_0$	$5c_2$	$2c_3$
3	± 5	± 2
29	± 25	± 34
37		± 22

The above table implies that there are 5 possible combination of the remainders of $3c_0, 5c_2, 2c_3$ modulo 40:

	$3c_0$	$5c_2$	$2c_3$
1	3	5	2
2	37	-5	-2
3	29	-5	-34
4	3	25	22
5	37	-25	-22

which correspond to the following values of c_0, c_2, c_3

	c_0	c_2	c_3
1	1	1	1
2	79	-1	-1
3	23	-1	-397
4	1	5	1091
5	79	-5	-1091

Conditions (1) and (2) give

$$160 \mid (-6c_0 + 15c_1 - 10c_2 + c_3)$$
$$160 \mid (-14c_0 + 105c_1 + 70c_2 - c_3)$$

and we can conclude that $160 \mid (-6c_0 + 15c_1 - 10c_2 + c_3) + (-14c_0 + 105c_1 + 70c_2 - c_3) = -20c_0 + 120c_1 + 60c_2$, whence $8 \mid -c_0 + 6c_1 + 3c_2$. Then the corresponding remainders of $c_0, 6c_1, 3c_2$ modulo 8 are

c_0	$6c_1$	$3c_2$
1	± 6	± 3
7	± 2	± 7
7	± 6	
	± 2	

The above table implies that there are 6 possible combination of the remainders of $c_0, 6c_1, 3c_2$ modulo 8:

	c_0	$6c_1$	$3c_2$
1	1	-6	7
2	1	6	3
3	1	-2	3
4	7	6	-7
5	7	-6	-3
6	7	2	-3

which correspond to the following values of c_0, c_1, c_2

	c_0	c_1	c_2
1	1	-1	5
2	1	-5	5
3	1	1	1
4	1	5	1
5	1	-3	1
6	1	-15	1
7	23	1	-5
8	23	5	-5
9	23	-1	-1
10	23	-5	-1
11	23	3	-1
12	23	15	-1
13	79	1	-5
14	79	5	-5
15	79	-1	-1
16	79	-5	-1
17	79	3	-1
18	79	15	-1

Now we match this table with the table for possible combinations of c_0, c_2, c_3:

	c_0	c_1	c_2
1	1	-1	5
2	1	-5	5
3	1	1	1
4	1	5	1
5	1	-3	1
6	1	-15	1
7	23	1	-5
8	23	5	-5
9	23	-1	-1
10	23	-5	-1
11	23	3	-1
12	23	15	-1
13	79	1	-5
14	79	5	-5
15	79	-1	-1
16	79	-5	-1
17	79	3	-1
18	79	15	-1

	c_0	c_2	c_3
1	1	1	1
2	79	-1	-1
3	23	-1	-397
4	1	5	1091
5	79	-5	-1091

which gives us the possible combinations of c_0, c_1, c_2, c_3. We also compute the leading coefficient of the Lagrange polynomial $g_{\mathbf{c}}$

	c_0	c_1	c_2	c_3	
1	1	1	1	1	1
2	1	5	1	1	$\frac{1}{8}$
3	1	-3	1	1	$-\frac{1}{8}$
4	1	-15	1	1	$-\frac{1}{2}$
5	79	-1	-1	-1	-1
6	79	-5	-1	-1	$-\frac{9}{8}$
7	79	3	-1	-1	$-\frac{7}{8}$
8	79	15	-1	-1	$-\frac{1}{2}$
9	23	-1	-1	-397	$-\frac{9}{8}$
10	23	-5	-1	-397	$-\frac{5}{4}$
11	23	3	-1	-397	-1
12	23	15	-1	-397	$-\frac{5}{8}$
13	1	-1	5	1091	$\frac{17}{8}$
14	1	-5	5	1091	2
15	79	1	-5	-1091	$-\frac{25}{8}$
16	79	5	-5	-1091	-3

Now one can test only 4 of these combinations by dividing f by the corresponding Lagrange polynomials (the first combination corresponds to the polynomial 1). The combination $c_0 = 23, c_1 = 3, c_2 = -1, c_3 = -397$ gives the Lagrange polynomial $-x^3 - x^2 - x + 2$ and the combination $c_0 = 79, c_1 = 5, c_2 = -5, c_3 = -1091$ gives the Lagrange polynomial $-3x^3 - x^2 - 2x + 1$ which are both factors of f. Finally, we get $f = (3x^3 + x^2 + 2x - 1)(x^3 + x^2 + x - 2)$.