Question 1B:

```
> restart:
> printf("\nInputs:\n"):
  pol_a := (9*y-7)*x + (5*y^2 + 12);
  pol_b := (13*y+23)*x^2 + (21*y - 11)*x + (11*y - 13);
  p_list := [23, 29, 31, 37];
```

Inputs:

$$pol\_a := (9\,y - 7)\,x + 5\,y^2 + 12$$
$$pol\_b := (13\,y + 23)\,x^2 + (21\,y - 11)\,x + 11\,y - 13$$
$$p\_list := [23, 29, 31, 37] \quad \textbf{(1)}$$

```
> n := nops(p_list):
  in_arr := Array(1..n):

  for i from 1 to n do
      printf("\nStep: %d.\n", i):
      p_i := p_list[i];
      a_i := mods(pol_a, p_i);
      b_i := mods(pol_b, p_i);

      total_deg_y := degree(a_i, y) + degree(b_i, y);
      interp_vals_y := [seq(j, j=0..total_deg_y)];

      pts_eval_y := [];

      for k in interp_vals_y do
          a_ij := Eval(a_i, y=k) mod p_i;
          b_ij := Eval(b_i, y=k) mod p_i;

          total_deg_x := degree(a_ij, x) + degree(b_ij, x);
          interp_vals_x := [seq(l, l=0..total_deg_x)];

          pts_eval_x := [];

          for m in interp_vals_x do
              a_ijk := Eval(a_ij, x=m) mod p_i;
              b_ijk := Eval(b_ij, x=m) mod p_i;
              c_ijk := a_ijk*b_ijk mod p_i;

              pts_eval_x := [op(pts_eval_x), c_ijk];
          od;

          c_ij := Interp(interp_vals_x, pts_eval_x, x) mod p_i;
          pts_eval_y := [op(pts_eval_y), c_ij];
```

```
      od;

      c_i := Interp(interp_vals_y, pts_eval_y, y) mod p_i;
      in_arr[i] := c_i;
  od;
```

Step: 1.

$$p\_i := 23$$

$$a\_i := (9y - 7)x + 5y^2 - 11$$

$$b\_i := -10yx^2 + (-2y - 11)x + 11y + 10$$

$$total\_deg\_y := 3$$

$$interp\_vals\_y := [0, 1, 2, 3]$$

$$pts\_eval\_y := [\,]$$

$$c\_i := (19x^2 + 13x + 9)y^3 + (2x^3 + 5x^2 + 21x + 4)y^2 + (x^3 + 2x^2 + 12x + 17)y + 8x^2 + 5x + 5$$

$$in\_arr_1 := (19x^2 + 13x + 9)y^3 + (2x^3 + 5x^2 + 21x + 4)y^2 + (x^3 + 2x^2 + 12x + 17)y + 8x^2 + 5x + 5$$

Step: 2.

$$p\_i := 29$$

$$a\_i := (9y - 7)x + 5y^2 + 12$$

$$b\_i := (13y - 6)x^2 + (-8y - 11)x + 11y - 13$$

$$total\_deg\_y := 3$$

$$interp\_vals\_y := [0, 1, 2, 3]$$

$$pts\_eval\_y := [\,]$$

$$c\_i := (7x^2 + 18x + 26)y^3 + (x^3 + 14x^2 + 15x + 22)y^2 + (26x^2 + 16)y + 13x^3 + 5x^2 + 17x + 18$$

$$in\_arr_2 := (7x^2 + 18x + 26)y^3 + (x^3 + 14x^2 + 15x + 22)y^2 + (26x^2 + 16)y + 13x^3 + 5x^2 + 17x + 18$$

Step: 3.

$$p\_i := 31$$

$$a\_i := (9y - 7)x + 5y^2 + 12$$

$$b\_i := (13y - 8)x^2 + (-10y - 11)x + 11y - 13$$

$$total\_deg\_y := 3$$

$$interp\_vals\_y := [0, 1, 2, 3]$$

$$pts\_eval\_y := [\,]$$

$$c\_i := (3x^2 + 12x + 24)y^3 + (24x^3 + 25x^2 + 13x + 28)y^2 + (23x^3 + 3x^2 + 27x + 8)y + 25x^3 + 12x^2 + 21x + 30$$

$$in\_arr_3 := (3x^2 + 12x + 24)y^3 + (24x^3 + 25x^2 + 13x + 28)y^2 + (23x^3 + 3x^2 + 27x + 8)y + 25x^3 + 12x^2 + 21x + 30$$

Step: 4.

$$p\_i := 37$$

$$a\_i := (9y - 7)x + 5y^2 + 12$$

$$b\_i := (13y - 14)x^2 + (-16y - 11)x + 11y - 13$$

$$total\_deg\_y := 3$$

$$interp\_vals\_y := [0, 1, 2, 3]$$

$$pts\_eval\_y := [\,]$$

$$c\_i := (28x^2 + 31x + 18)y^3 + (6x^3 + 8x^2 + 7x + 9)y^2 + (5x^3 + 21x^2 + 21x + 21)y + 24x^3 + 20x^2 + 33x + 29$$

$$in\_arr_4 := (28x^2 + 31x + 18)y^3 + (6x^3 + 8x^2 + 7x + 9)y^2 + (5x^3 + 21x^2 + 21x + 21)y + 24x^3 + 20x^2 + 33x + 29 \quad \textbf{(2)}$$

```
> c_val := chrem([seq(in_arr[i], i = 1..n)], p_list);
  c_recovered := mods(c_val, mul(p_list[i], i = 1..n));
```

$$c\_val := 764893 + 765008x + 124062(28x^2 + 31x + 18)y^3 + 124062(6x^3 + 8x^2 + 7x + 9)y^2 + 124062(5x^3 + 21x^2 + 21x + 21)y + 518259(24x^3 + 25x^2 + 13x + 28)y^2 + 518259(23x^3 + 3x^2 + 27x + 8)y + 518259(3x^2 + 12x + 24)y^3 + 422096(7x^2 + 18x + 26)y^3 + 422096(x^3 + 14x^2 + 15x + 22)y^2 + 422096(26x^2 + 16)y + 764888x^3 + 465682(19x^2 + 13x + 9)y^3 + 465682(2x^3 + 5x^2 + 21x + 4)y^2 + 465682(x^3 + 2x^2 + 12x + 17)y + 353x^2$$

$$c\_recovered := -156 - 41x + 124062(28x^2 + 31x + 18)y^3 + 124062(6x^3 + 8x^2 + 7x + 9)y^2 + 124062(5x^3 + 21x^2 + 21x + 21)y - 246790(24x^3 + 25x^2 + 13x + 28)y^2 - 246790(23x^3 + 3x^2 + 27x + 8)y - 246790(3x^2 + 12x + 24)y^3 - 342953(7x^2 + 18x + 26)y^3 - 342953(x^3 + 14x^2 + 15x + 22)y^2 - 342953(26x^2 + 16)y - 161x^3 - 299367(19x^2 + 13x + 9)y^3 - 299367(2x^3 + 5x^2 + 21x + 4)y^2 - 299367(x^3 + 2x^2 + 12x + 17)y + 353x^2 \quad \textbf{(3)}$$

```
> c_recovered_simplified := simplify(c_recovered);
```

$$c\_recovered\_simplified := (-6120275y^2 - 5355227y - 161)x^3 + (-5355278y^3 - 11475431y^2 - 7650580y + 353)x^2 + (-9180483y^3 - 13770838y^2 - 7650432y - 41)x - 15300925y^3 - 14535996y^2 - 9945505y - 156 \quad \textbf{(4)}$$

```
> manual_prod := expand(pol_a*pol_b);
  computed_ans := expand(c_recovered - manual_prod);
```

$$manual\_prod := 117\,x^3\,y^2 + 65\,x^2\,y^3 + 116\,x^3\,y + 304\,x^2\,y^2 + 105\,x\,y^3 - 161\,x^3 - 90\,y\,x^2 + 44\,x\,y^2 + 55\,y^3 + 353\,x^2 + 58\,x\,y - 65\,y^2 - 41\,x + 132\,y - 156$$

$$computed\_ans := -6120392\,x^3\,y^2 - 5355343\,x^2\,y^3 - 5355343\,x^3\,y - 11475735\,x^2\,y^2 - 9180588\,x\,y^3 - 7650490\,y\,x^2 - 13770882\,x\,y^2 - 15300980\,y^3 - 7650490\,x\,y - 14535931\,y^2 - 9945637\,y \qquad \textbf{(5)}$$

```
> c_recovered := mods(expand(c_recovered), mul(p_list[i], i = 1..n));
  printf("\nC recovered matches the expanded product of polynomials A
  and B.\n"):
```

$$c\_recovered := 117\,x^3\,y^2 + 65\,x^2\,y^3 + 116\,x^3\,y + 304\,x^2\,y^2 + 105\,x\,y^3 - 161\,x^3 - 90\,y\,x^2 + 44\,x\,y^2 + 55\,y^3 + 353\,x^2 + 58\,x\,y - 65\,y^2 - 41\,x + 132\,y - 156$$

```
C recovered matches the expanded product of polynomials A and B.
```