```
> restart;
```

Sous-ensembles

```
> Parcourt := proc(n)
  local E, F, i, j, k, l, t, c, d;
  E := {seq([i], i = 1..n)};
  for l from 1 to n - 1 do
       t := nops(E);
       print(t, binomial(n, l));
       F := {};
       for i from 1 to t do
           c := E[i][l];
                for k from c + 1 to n do
                       F := F union {[seq(E[i][m], m = 1..l), k]}
                od;
        od;
        E := F
  od;
  end:
> Parcourt(15);
```

15, 15

105, 105

455, 455

1365, 1365

3003, 3003

5005, 5005

6435, 6435

6435, 6435

5005, 5005

3003, 3003

1365, 1365

455, 455

105, 105

15, 15

$$\{[1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15]\} \quad (1.1)$$

```
> ?Isirreduct
> randpoly(x, degree = 5, dense);
```

$$77 + 91\,x^5 + 68\,x^4 - 10\,x^3 + 31\,x^2 - 51\,x \quad (1.2)$$

```
> P := % mod 3;
```

$$P := 2 + x^5 + 2\,x^4 + 2\,x^3 + x^2 \quad (1.3)$$

```
> Irreduc(P) mod 3;
```

$$true \quad (1.4)$$

```
>
```

Un système résistant

```
> Partage := proc(n, p, s, t)
  local i, a, h, j, P;
  h := rand(0..p − 1);
  a := array(1 .. n − 1);
  for j from 1 to n − 1 do
  a[j] := h( );
  P := s + add(a[k]·x^k, k = 1..n − 1)
  od;
  i := [seq(subs(x = t[l], P) mod p, l = 1..n)];
  end:
> t := [seq(i, i = 1..20)];
```

$t := [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20]$ **(2.1)**

```
> X := Partage(20, 23, 15, t);
```

$X := [16, 17, 13, 7, 15, 12, 16, 22, 11, 16, 1, 22, 12, 21, 9, 10, 13, 19, 9, 16]$ **(2.2)**

```
> Secret := proc(n, p, t, X)
  local P;
  P := Interp(t, X, x) mod p;
  subs(x = 0, P)
  end:
> Secret(20, 23, t, X);
```

15 **(2.3)**

```
> Partage2 := proc(n, p, m, b, s, t)
  local i, a, h, j, P;
  a := array(1..n − 1);
  for j from 1 to n − 1 do
  a[j] := subs(x = b, randpoly(x, degree = m − 1, dense, coeffs = rand(0..p − 1)));
  P := s + add(a[k]·x^k, k = 1..n − 1)
  od;
  i := [seq(evala(subs(x = t[l], P) mod p) mod p, l = 1..n)];
  end:
> PolyIrr := proc(p, m)
  local Q, r, c;
  r := false;
  c := 0;
  while r = false do
  Q := x^m + randpoly(x, degree = m − 1, dense, coeffs = rand(0..p − 1));
  r := Irreduc(Q) mod p;
  c := c + 1
  od;
  [Q, c];
  end:
> 2^8;
```

(2.4)

$$256 \quad (2.4)$$

> $PolyIrr(2, 256);$

$$[1 + x^{94} + x^{17} + x^{196} + x^{190} + x^{88} + x^{176} + x^{109} + x^{102} + x^{209} + x^{145} + x^{150} + x^{223} + x^{210} + x^{201} + x^{248} + x^{246} + x^{151} + x^{44} + x^{256} + x^{250} + x^{46} + x^{226} + x^{205} + x^{194} + x^{182} + x^{156} + x^{139} + x^{55} + x^{180} + x^{5} + x^{3} + x^{50} + x^{47} + x^{45} + x^{42} + x^{37} + x^{35} + x^{33} + x^{32} + x^{31} + x^{30} + x^{26} + x^{25} + x^{22} + x^{12} + x^{7} + x^{100} + x^{97} + x^{95} + x^{93} + x^{87} + x^{86} + x^{84} + x^{83} + x^{81} + x^{80} + x^{79} + x^{77} + x^{75} + x^{74} + x^{73} + x^{72} + x^{70} + x^{69} + x^{67} + x^{66} + x^{64} + x^{62} + x^{60} + x^{59} + x^{54} + x^{237} + x^{172} + x^{167} + x^{161} + x^{119} + x^{252} + x^{251} + x^{247} + x^{244} + x^{240} + x^{239} + x^{238} + x^{234} + x^{233} + x^{231} + x^{228} + x^{227} + x^{225} + x^{221} + x^{220} + x^{219} + x^{218} + x^{213} + x^{207} + x^{203} + x^{198} + x^{197} + x^{195} + x^{193} + x^{184} + x^{183} + x^{178} + x^{175} + x^{174} + x^{171} + x^{164} + x^{153} + x^{147} + x^{146} + x^{143} + x^{141} + x^{137} + x^{136} + x^{134} + x^{131} + x^{129} + x^{128} + x^{127} + x^{126} + x^{125} + x^{123} + x^{120} + x^{118} + x^{116} + x^{110} + x^{107} + x^{106} + x^{104} + x^{103} + x^{254} + x^{101}, 242] \quad (2.5)$$

> $PolyIrr(3, 64);$

$$[2 + x^{17} + x^{41} + 2\,x^{11} + 2\,x^{44} + 2\,x^{46} + 2\,x^{55} + 2\,x^{5} + x^{4} + x^{2} + x^{6} + x^{50} + 2\,x^{48} + 2\,x^{47} + x^{45} + x^{43} + x^{39} + x^{37} + 2\,x^{36} + x^{35} + x^{33} + x^{32} + 2\,x^{30} + x^{28} + x^{26} + 2\,x^{25} + x^{24} + 2\,x^{23} + 2\,x^{21} + 2\,x^{20} + 2\,x^{19} + 2\,x^{15} + x^{14} + x^{12} + x^{9} + x^{7} + x^{64} + x^{62} + x^{61} + x^{59} + 2\,x^{58} + x^{57} + 2\,x^{53} + 2\,x^{51} + 2\,x^{63} + 2\,x^{8}, 20] \quad (2.6)$$

> $q := PolyIrr(2, 6)[1];$

$$q := x^6 + 1 + x^5 + x^2 + x \quad (2.7)$$

> $alias(b = RootOf(q, x) \bmod 2);$

$$b \quad (2.8)$$

```
> Choixt := proc(n, p, m, b)
   local t, r;
   r := 0;
   while r < n do
   t := {seq(subs(x = b, randpoly(x, degree = m − 1, dense, coeffs = rand(0 ..p − 1))), i
      = 1 ..2· n)} minus {0};
   r := nops(t);
   od;
   t := [seq(t[i], i = 1 ..n)];
   end:
```

> $t := Choixt(40, 2, 6, b);$

$$t := [1, b^2, b^3, b^4, 1 + b^3, 1 + b^4, 1 + b^5, 1 + b, b^2 + 1, b^2 + b, b^3 + b^2, b^3 + b, b^4 + b^2, b^4 + b^3, b^5 + b^4, b^5 + b, 1 + b^3 + b, 1 + b^4 + b^2, 1 + b^5 + b^2, 1 + b^5 + b^3, 1 + b^5 + b^4, 1 + b^5 + b, b^3 + b^2 + b, b^4 + b^2 + b, b^4 + b^3 + b^2, b^5 + b^3 \quad (2.9)$$

$+ b, b^5 + b^4 + b^2, b^5 + b^4 + b^3, b^5 + b^4 + b, 1 + b^3 + b^2 + b, 1 + b^4 + b^2 + b,$
$1 + b^4 + b^3 + b^2, 1 + b^4 + b^3 + b, 1 + b^5 + b^2 + b, 1 + b^5 + b^3 + b^2, 1 + b^5$
$+ b^3 + b, 1 + b^5 + b^4 + b, b^4 + b^3 + b^2 + b, b^5 + b^3 + b^2 + b, b^5 + b^4 + b^2$
$+ b]$

```
> s := subs(x = b, randpoly(x, degree = 5, dense, coeffs = rand(0..1)));
```

$$s := b^4 + b^3 + b^2 + b \qquad \textbf{(2.10)}$$

```
> X := Partage2(40, 2, 6, b, s, t);
```

$$X := [b^3 + b^2 + b, b^5 + b^4 + b^3 + b, 1 + b^5 + b^3 + b^2 + b, b^5 + b^4 + b, 0, b^4 + b^3 + b, b^5 + b^2 + b, b^5, b^5 + b^4, b^5 + b^3 + b^2 + b, 1 + b^4 + b^2 + b, b^4, 1 + b^4 + b^3 + b^2, b^3 + b, 1 + b^4 + b^2, b^5, b^4 + b^2 + b, 1 + b^5 + b^2, 1 + b^5 + b^3 + b^2 + b, 1 + b^5 + b, b^5 + b^2, 1 + b^5 + b^4 + b, 1 + b^5 + b^2, 1 + b^4 + b^3 + b^2, b^5 + b^4 + b^2, b^5 + b^4 + b^3 + b, 0, b^5 + b^4 + b^2, b^5 + b^3 + b, b^5 + b, b^2 + b + 1, b^4 + b^3 + b^2, 1 + b^4 + b^2 + b, b^5 + b^3, b^4 + b^3 + b^2, b, b^4, b^5 + b^4 + b^3 + b, 1 + b^4 + b, 1 + b^4 + b^2] \qquad \textbf{(2.11)}$$

```
> Secret2 := proc(n, p, b, t, X)
  local P;
  P := evala(Interp(t, X, x) mod p) mod p;
  evala(subs(x = 0, P)) mod p
  end:
> Secret2(40, 2, b, t, X);
```

$$b^4 + b^3 + b^2 + b \qquad \textbf{(2.12)}$$

```
>
```

Partage de secret avec seuil

```
> PSeuil := proc(n, k, p, s, t)
  local i, a, h, j, P;
  h := rand(0..p - 1);
  a := array(1..k - 1);
  for j from 1 to k - 1 do
  a[j] := h();
  P := s + add(a[l]·x^l, l = 1..k - 1)
  od;
  i := [seq(subs(x = t[l], P) mod p, l = 1..n)];
  end:
```

Première méthode de décodage

```
> SecretSeuil := proc(n, k, p, t, X)
  local E, F, G, H, N, i, j, l, c, P, T, Y, b, taille;
  P := Interp(t, X, x) mod p;
  if degree(P, x) < k then return [subs(x = 0, P), 0] fi;
```

```
E := { seq( [ i ], i = 1 ..n ) };
N := { seq( i, i = 1 ..n ) };
for b from 1 to n do
    H := N minus { E [ b ] [ 1 ] };
    Y := [ seq( X [ H [ a ] ], a = 1 ..n − 1 ) ];
    T := [ seq( t[ H [ a ] ], a = 1 ..n − 1 ) ];
    P := Interp( T, Y, x ) mod p;
    if degree( P, x ) < k then return [ subs( x = 0, P ), [ b ] ] fi;
od;
for l from 1 to floor( (n − k)/2 ) do
        print( l );
        taille := nops( E );
        F := { };
        for i from 1 to taille do
            c := E [ i ] [ l ];
                for b from c + 1 to n do
                    G := [ seq( E [ i ] [ m ], m = 1 ..l ), b ];
                    H := N minus { op( G ) };
                    Y := [ seq( X [ H [ a ] ], a = 1 ..n − l − 1 ) ];
                    T := [ seq( t[ H [ a ] ], a = 1 ..n − l − 1 ) ];
                    P := Interp( T, Y, x ) mod p;
                    if degree( P, x ) < k then return [ subs( x = 0, P ), G ] fi;
                    F := F union { G }
                od;
        od;
        E := F;
od;
erreur;
end:
> t := [ seq( i, i = 1 ..20 ) ];
          t := [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20]      (3.1.1)
> X := PSeuil( 20, 18, 23, 15, t );
          X := [16, 3, 7, 8, 4, 17, 0, 12, 21, 0, 20, 5, 12, 8, 3, 14, 16, 19, 21, 12]      (3.1.2)
> SecretSeuil( 20, 18, 23, t, X );
                                     [15, 0]                                             (3.1.3)
> XX := X;
          XX := [16, 3, 7, 8, 4, 17, 0, 12, 21, 0, 20, 5, 12, 8, 3, 14, 16, 19, 21, 12]     (3.1.4)
> XX [ 7 ] := 3;
                                     XX_7 := 3                                           (3.1.5)
> X := PSeuil( 20, 12, 23, 15, t );
          X := [0, 7, 8, 16, 4, 22, 20, 14, 19, 2, 11, 11, 5, 11, 1, 0, 9, 13, 10, 17]      (3.1.6)
> XX := X; XX [ 5 ] := 1; XX [ 6 ] := 0; XX [ 20 ] := 3;
          XX := [0, 7, 8, 16, 4, 22, 20, 14, 19, 2, 11, 11, 5, 11, 1, 0, 9, 13, 10, 17]
                                     XX_5 := 1
```

$$XX_6 := 0$$

$$XX_{20} := 3 \tag{3.1.7}$$

```
> SecretSeuil(20, 12, 23, t, XX);
```

$$1$$

$$2$$

$$[15, [5, 6, 20]] \tag{3.1.8}$$

Seconde méthode de décodage

```
> Equation := proc(m, k, l, p, X, Y)
  local P, Q1, Q2, E, q1, q2, R, S, d, v;
  Q1 := add(q1[i]·x^i, i = 0..m − 1 − l);
  Q2 := add(q2[i]·x^i, i = 0..m − l − k);
  E := {seq(subs(x = X[j], Q1) + Y[j]·subs(x = X[j], Q2) mod p = 0, j = 1
     ..m)};
  S := solve(E) mod p;
  assign(S);
  v := [[seq(q1[i], i = 0..m − 1 − l)], [seq(q2[i], i = 0..m − l − k)]];
  q1 :='q1'; q2 :='q2';
  v;
  end:
> Decode := proc(m, k, l, p, X, Y)
  local v, E, R, S, Q1, Q2, P, d, r;
  v := Equation(m, k, l, p, X, Y);
 Q1 := add(v[1][i]·x^(i − 1), i = 1..m − l);
  Q2 := add(v[2][i]·x^(i − 1), i = 1..m − l − k + 1);
  R := Rem(Q1, Q2, x,'P') mod p;
  r := subs(x = 0,-P mod p);
  end:
> Decode := proc(m, k, l, p, X, Y)
  local P, Q1, Q2, E, q1, q2, R, S, d, v, i, ni, h, j, r, spe;
  Q1 := add(q1[i]·x^i, i = 0..m − 1 − l);
  Q2 := add(q2[i]·x^i, i = 0..m − l − k);
  E := {seq(subs(x = X[j], Q1) + Y[j]·subs(x = X[j], Q2) mod p = 0, j = 1
     ..m)};
  S := solve(E) mod p;
  Q1 := subs(S, Q1); Q2 := subs(S, Q2);
  i := indets([Q1, Q2]);
  ni := nops(i);
  h := rand(0..p − 1);
  r := 0;
  while r = 0 do
    for j from 2 to ni do
      spe := h();
      Q1 := subs(i[j] = spe, Q1);
```

```
        Q2 := subs(i[j] = spe, Q2);
      od;
      r := Q2;
    od;
    P := -Quo(Q1, Q2, x) mod p;
    subs(x = 0, P);
    end:
> t := [seq(i, i = 1 ..8)];
```
$$t := [1, 2, 3, 4, 5, 6, 7, 8] \quad (3.2.1)$$
```
> X := PSeuil(8, 6, 11, 3, t);
```
$$X := [5, 7, 6, 5, 6, 3, 8, 0] \quad (3.2.2)$$
```
> XX := X; XX[1] := 0;
```
$$XX := [5, 7, 6, 5, 6, 3, 8, 0]$$
$$XX_1 := 0 \quad (3.2.3)$$
```
> Q1 := add(q1[i]·x^i, i = 0 ..6);
  Q2 := add(q2[i]·x^i, i = 0 ..1);
  E := {seq(subs(x = t[j], Q1) + XX[j]·subs(x = t[j], Q2) mod 11 = 0, j = 1
    ..8)}; nops(E);
```
$$Q1 := q1_0 + q1_1\,x + q1_2\,x^2 + q1_3\,x^3 + q1_4\,x^4 + q1_5\,x^5 + q1_6\,x^6$$
$$Q2 := q2_0 + q2_1\,x$$
$$E := \{q1_0 + q1_1 + q1_2 + q1_3 + q1_4 + q1_5 + q1_6 = 0, q1_0 + 2\,q1_1 + 4\,q1_2 + 8\,q1_3 + 5\,q1_4 + 10\,q1_5 + 9\,q1_6 = 0, q1_0 + 3\,q1_1 + 9\,q1_2 + 5\,q1_3 + 4\,q1_4 + q1_5 + 3\,q1_6 = 0, q1_0 + 4\,q1_1 + 5\,q1_2 + 9\,q1_3 + 3\,q1_4 + q1_5 + 4\,q1_6 + 7\,q2_0 + 6\,q2_1 = 0, q1_0 + 5\,q1_1 + 3\,q1_2 + 4\,q1_3 + 9\,q1_4 + q1_5 + 5\,q1_6 + 5\,q2_0 + 3\,q2_1 = 0, q1_0 + 6\,q1_1 + 3\,q1_2 + 7\,q1_3 + 9\,q1_4 + 10\,q1_5 + 5\,q1_6 + q2_0 + 6\,q2_1 = 0, q1_0 + 7\,q1_1 + 5\,q1_2 + 2\,q1_3 + 3\,q1_4 + 10\,q1_5 + 4\,q1_6 + q2_0 + 7\,q2_1 = 0, q1_0 + 8\,q1_1 + 9\,q1_2 + 6\,q1_3 + 4\,q1_4 + 10\,q1_5 + 3\,q1_6 + 8\,q2_0 + 9\,q2_1 = 0\}$$
$$8 \quad (3.2.4)$$
```
> S := solve(E) mod 11;
```
$$S := \{q1_0 = 8\,q2_0, q1_1 = 2\,q2_0, q1_2 = 9\,q2_0, q1_3 = 7\,q2_0, q1_4 = 8\,q2_0, q1_5 = 8\,q2_0, q1_6 = 2\,q2_0, q2_0 = q2_0, q2_1 = 10\,q2_0\} \quad (3.2.5)$$
```
> assign(S);
> q1[0];
```
$$8\,q2_0 \quad (3.2.6)$$
```
> indets([Q1, Q2]);
```
$$\{x, q2_0\} \quad (3.2.7)$$
```
> Q1; Q2;
```

$$8\,q2_0 + 2\,q2_0\,x + 9\,q2_0\,x^2 + 7\,q2_0\,x^3 + 8\,q2_0\,x^4 + 8\,q2_0\,x^5 + 2\,q2_0\,x^6$$

$$q2_0 + 10\,q2_0\,x \qquad \textbf{(3.2.8)}$$

> $Q1 := subs(q2[0] = 1, Q1);\ Q2 := subs(q2[0] = 1, Q2);$

$$Q1 := 8 + 2\,x + 9\,x^2 + 7\,x^3 + 8\,x^4 + 8\,x^5 + 2\,x^6$$

$$Q2 := 1 + 10\,x \qquad \textbf{(3.2.9)}$$

> $R := Rem(Q1, Q2, x, 'P')$ **mod** $11;$

$$R := 0 \qquad \textbf{(3.2.10)}$$

> $-P$ **mod** $11;$

$$3 + x + 3\,x^2 + 7\,x^3 + 10\,x^4 + 2\,x^5 \qquad \textbf{(3.2.11)}$$

> $q1 := 'q1';\ q2 := 'q2';$

$$q1 := q1$$

$$q2 := q2 \qquad \textbf{(3.2.12)}$$

> $Decode(8, 6, 1, 11, t, XX);$

$$3 \qquad \textbf{(3.2.13)}$$

> $X := PSeuil(8, 4, 11, 3, t);$

$$X := [3, 5, 1, 5, 9, 5, 7, 7] \qquad \textbf{(3.2.14)}$$

> $XX := X;\ XX[1] := 1;\ XX[5] := 5;$

$$XX := [3, 5, 1, 5, 9, 5, 7, 7]$$

$$XX_1 := 1$$

$$XX_5 := 5 \qquad \textbf{(3.2.15)}$$

> $Decode(8, 4, 2, 11, t, XX);$

$$3 \qquad \textbf{(3.2.16)}$$

> $t := [seq(i, i = 1..8)];$

$$t := [1, 2, 3, 4, 5, 6, 7, 8] \qquad \textbf{(3.2.17)}$$

> $X := PSeuil(8, 4, 11, 3, t);$

$$X := [0, 3, 3, 2, 2, 5, 2, 6] \qquad \textbf{(3.2.18)}$$

> $XX := X;\ XX[1] := 1;$

$$XX := [0, 3, 3, 2, 2, 5, 2, 6]$$

$$XX_1 := 1 \qquad \textbf{(3.2.19)}$$

> $Decode(8, 4, 2, 11, t, XX);$

$$3 \qquad \textbf{(3.2.20)}$$

> $t := [seq(i, i = 1..20)];$

$$t := [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20] \qquad \textbf{(3.2.21)}$$

> $X := PSeuil(20, 12, 23, 3, t);$

$$X := [11, 7, 6, 7, 7, 11, 6, 22, 2, 4, 12, 10, 13, 9, 3, 22, 18, 22, 4, 5] \qquad \textbf{(3.2.22)}$$

> $XX := X;\ XX[1] := 1;\ XX[5] := 1;\ XX[20] := 0;$

$$XX := [11, 7, 6, 7, 7, 11, 6, 22, 2, 4, 12, 10, 13, 9, 3, 22, 18, 22, 4, 5]$$

$$XX_1 := 1$$

$$XX_5 := 1$$

$$XX_{20} := 0 \tag{3.2.23}$$

> $Decode(20, 12, 3, 23, t, XX);$

$$3 \tag{3.2.24}$$

>

Plus de menteurs

Exemple 1. m=26, k=7, delta=2, l<12.

> $t := [seq(i, i = 1..26)];$

$$t := [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26] \tag{3.3.1.1}$$

> $X := PSeuil(26, 7, 29, 15, t);$

$$X := [17, 6, 16, 18, 5, 17, 19, 9, 8, 19, 13, 0, 11, 20, 9, 2, 10, 3, 25, 17, 15, 27, 24, 16, 10, 24] \tag{3.3.1.2}$$

> $h := rand(0..28);$

$h :=$ **proc**( )
    proc( ) **option** *builtin* = *RandNumberInterface*; **end proc**(6, 29, 5)
end proc (3.3.1.3)

> $XX := X;$**for** i **from** 1 **to** 11 **do** $XX[i] := h()$ **od**;

$XX := [17, 6, 16, 18, 5, 17, 19, 9, 8, 19, 13, 0, 11, 20, 9, 2, 10, 3, 25, 17, 15, 27, 24, 16, 10, 24]$

$$XX_1 := 15$$

$$XX_2 := 0$$

$$XX_3 := 5$$

$$XX_4 := 12$$

$$XX_5 := 13$$

$$XX_6 := 6$$

$$XX_7 := 27$$

$$XX_8 := 6$$

$$XX_9 := 2$$

$$XX_{10} := 13$$

$$XX_{11} := 28 \tag{3.3.1.4}$$

> $Q := add\left(add\left(q[i,j]\cdot x^i\cdot y^j, i = 0..14 - 6\cdot j\right), j = 0..2\right);$

$$Q := q_{5,1}\,x^5\,y + q_{2,2}\,x^2\,y^2 + q_{7,0}\,x^7 + q_{1,2}\,x\,y^2 + q_{8,1}\,x^8\,y + q_{2,0}\,x^2 + q_{1,1}\,x\,y + q_{12,0}\,x^{12} + q_{3,0}\,x^3 + q_{9,0}\,x^9 + q_{1,0}\,x + q_{7,1}\,x^7\,y + q_{5,0}\,x^5 + q_{0,1}\,y \tag{3.3.1.5}$$

$$+ q_{4,1} x^4 y + q_{0,2} y^2 + q_{11,0} x^{11} + q_{6,1} x^6 y + q_{10,0} x^{10} + q_{8,0} x^8 + q_{4,0} x^4 + q_{3,1} x^3 y + q_{6,0} x^6 + q_{2,1} x^2 y + q_{13,0} x^{13} + q_{0,0} + q_{14,0} x^{14}$$

> $E := \{seq(subs(x = t[i], subs(y = XX[i], Q)) \bmod 29 = 0, i = 1..26)\}:$

> $S := solve(E) \bmod 29;$

$$S := \{q_{0,0} = 0, q_{0,1} = 10\, q_{7,0}, q_{0,2} = 9\, q_{7,0}, q_{1,0} = 21\, q_{7,0}, q_{1,1} = 25\, q_{7,0}, q_{1,2} = q_{7,0}, q_{2,0} = 21\, q_{7,0}, q_{2,1} = 16\, q_{7,0}, q_{2,2} = 14\, q_{7,0}, q_{3,0} = 4\, q_{7,0}, q_{3,1} = 14\, q_{7,0}, q_{4,0} = 5\, q_{7,0}, q_{4,1} = 9\, q_{7,0}, q_{5,0} = 24\, q_{7,0}, q_{5,1} = 17\, q_{7,0}, q_{6,0} = 10\, q_{7,0}, q_{6,1} = 4\, q_{7,0}, q_{7,0} = q_{7,0}, q_{7,1} = 25\, q_{7,0}, q_{8,0} = 21\, q_{7,0}, q_{8,1} = 11\, q_{7,0}, q_{9,0} = 4\, q_{7,0}, q_{10,0} = 21\, q_{7,0}, q_{11,0} = 28\, q_{7,0}, q_{12,0} = 18\, q_{7,0}, q_{13,0} = 28\, q_{7,0}, q_{14,0} = 27\, q_{7,0}\} \quad \textbf{(3.3.1.6)}$$

> $Q := subs(S, Q);$

$$Q := 21\, q_{7,0} x^2 + 18\, q_{7,0} x^{12} + 4\, q_{7,0} x^3 + 4\, q_{7,0} x^9 + 21\, q_{7,0} x + 24\, q_{7,0} x^5 + 10\, q_{7,0} y + 9\, q_{7,0} y^2 + 28\, q_{7,0} x^{11} + 21\, q_{7,0} x^{10} + 21\, q_{7,0} x^8 + 5\, q_{7,0} x^4 + 10\, q_{7,0} x^6 + 28\, q_{7,0} x^{13} + 27\, q_{7,0} x^{14} + q_{7,0} x^7 + 25\, q_{7,0} x^7 y + 9\, q_{7,0} x^4 y + 17\, q_{7,0} x^5 y + 25\, q_{7,0} x y + 16\, q_{7,0} x^2 y + 14\, q_{7,0} x^3 y + 4\, q_{7,0} x^6 y + 11\, q_{7,0} x^8 y + q_{7,0} x y^2 + 14\, q_{7,0} x^2 y^2 \quad \textbf{(3.3.1.7)}$$

> $Q := subs(q[7,0] = 1, Q);$

$$Q := 21\, x + 10\, y + 5\, x^4 + 18\, x^{12} + 27\, x^{14} + 9\, y^2 + 9\, y x^4 + 16\, y x^2 + 25\, x y + 14\, y^2 x^2 + 11\, y x^8 + 4\, x^6 y + x y^2 + 17\, x^5 y + 14\, x^3 y + 21\, x^2 + 21\, x^8 + 10\, x^6 + 24\, x^5 + 4\, x^3 + 28\, x^{13} + 28\, x^{11} + 4\, x^9 + 21\, x^{10} + x^7 + 25\, x^7 y \quad \textbf{(3.3.1.8)}$$

> $Q0 := subs(x = 0, Q);$

$$Q0 := 10\, y + 9\, y^2 \quad \textbf{(3.3.1.9)}$$

> $msolve(Q0 = 0, 29);$

$$\{y = 0\}, \{y = 15\} \quad \textbf{(3.3.1.10)}$$

> $P := 15;$

$$P := 15 \quad \textbf{(3.3.1.11)}$$

> $dQ := diff(Q, y);$

$$dQ := 10 + 18\, y + 9\, x^4 + 16\, x^2 + 25\, x + 28\, y x^2 + 11\, x^8 + 4\, x^6 + 2\, x y + 17\, x^5 + 14\, x^3 + 25\, x^7 \quad \textbf{(3.3.1.12)}$$

> $dQP := subs(y = P, dQ) \bmod 29;$

$$dQP := 19 + 9\, x^4 + x^2 + 26\, x + 11\, x^8 + 4\, x^6 + 17\, x^5 + 14\, x^3 + 25\, x^7 \quad \textbf{(3.3.1.13)}$$

> $QP := subs(y = P, Q) \bmod 29;$

$$QP := 12\, x + 24\, x^4 + 18\, x^{12} + 27\, x^{14} + 18\, x^2 + 12\, x^8 + 12\, x^6 + 18\, x^5 + 11\, x^3 \quad \textbf{(3.3.1.14)}$$

$$+ 28x^{13} + 28x^{11} + 4x^{9} + 21x^{10} + 28x^{7}$$

> $series\left(\frac{QP}{dQP}, x, 2\right)$ **mod** 29;

$$22x + O(x^2) \quad \textbf{(3.3.1.15)}$$

> $P := P - convert(\%, polynom)$ **mod** 29;

$$P := 15 + 7x \quad \textbf{(3.3.1.16)}$$

> $dQP := expand(subs(y = P, dQ))$ **mod** 29;

$$dQP := 19 + 7x + 9x^4 + 15x^2 + 7x^3 + 11x^8 + 4x^6 + 17x^5 + 25x^7 \quad \textbf{(3.3.1.17)}$$

> $QP := expand(subs(y = P, Q))$ **mod** 29;

$$QP := 25x^4 + 18x^{12} + 27x^{14} + 3x^2 + 13x^8 + 15x^6 + 23x^5 + 9x^3 + 28x^{13} + 28x^{11} + 23x^9 + 21x^{10} + 27x^7 \quad \textbf{(3.3.1.18)}$$

> $series\left(\frac{QP}{dQP}, x, 4\right)$ **mod** 29;

$$20x^2 + 16x^3 + O(x^4) \quad \textbf{(3.3.1.19)}$$

> $P := P - convert(\%, polynom)$ **mod** 29;

$$P := 15 + 7x + 9x^2 + 13x^3 \quad \textbf{(3.3.1.20)}$$

> $dQP := expand(subs(y = P, dQ))$ **mod** 29;

$$dQP := 19 + 7x + 3x^2 + 27x^3 + 26x^4 + 4x^5 + 11x^8 + 4x^6 + 25x^7 \quad \textbf{(3.3.1.21)}$$

> $QP := expand(subs(y = P, Q))$ **mod** 29;

$$QP := 23x^4 + 18x^{12} + 27x^{14} + 26x^8 + 2x^6 + 3x^5 + 28x^{13} + 26x^{11} + 10x^9 + 10x^{10} + x^7 \quad \textbf{(3.3.1.22)}$$

> $series\left(\frac{QP}{dQP}, x, 8\right)$ **mod** 29;

$$18x^4 + 21x^5 + 17x^6 + O(x^8) \quad \textbf{(3.3.1.23)}$$

> $P := P - convert(\%, polynom)$ **mod** 29;

$$P := 15 + 7x + 9x^2 + 13x^3 + 11x^4 + 8x^5 + 12x^6 \quad \textbf{(3.3.1.24)}$$

> $expand(subs(y = P, Q))$ **mod** 29;

$$0 \quad \textbf{(3.3.1.25)}$$

> $expand(subs(y = P, Q))$;

$$2175 + 2581x + 11136x^4 + 6467x^{12} + 2175x^{14} + 6757x^2 + 18270x^8 + 17429x^6 + 14500x^5 + 8584x^3 + 3248x^{13} + 9570x^{11} + 14094x^9 + 11803x^{10} + 16269x^7 \quad \textbf{(3.3.1.26)}$$

> $discrim(Q, y)$ **mod** 29;

$$x^{16} + 5x^{15} + 13x^{14} + 14x^{13} + 27x^{12} + 13x^{11} + 16x^{10} + 5x^9 + 23x^8 + 18x^7 + 11x^6 + 14x^5 + 25x^4 + 24x^3 + 18x^2 + 5x + 13 \quad \textbf{(3.3.1.27)}$$

> $Factor(\%)$ **mod** 29;

(3.3.1.28)

$$\left(x^4+4x^3+9x^2+25x+23\right)^2\left(x^4+13x^3+4x^2+20x+8\right)^2 \quad \textbf{(3.3.1.28)}$$

> $collect(Q, y);$

$$\left(7+4x^2+22x\right)y^2+\left(18+x^3+13x^7+10x^5+23x^4+4x^2+6x+3x^8+16x^6\right)y+11+24x+25x^5+20x^4+23x^{12}+6x^{14}+16x^9+17x^3+19x^{13}+15x^{11}+15x^6+16x^{10}+6x^7+x^8+17x^2 \quad \textbf{(3.3.1.29)}$$

Exemple 2. m=31,k=5, delta=3, l<18.

> $p1 := x^4+x+1;$

$$p1 := x^4+x+1 \quad \textbf{(3.3.2.1)}$$

> $p2 := x^4+2\cdot x^2+2;$

$$p2 := x^4+2x^2+2 \quad \textbf{(3.3.2.2)}$$

> $p3 := x^5+3;$

$$p3 := x^5+3 \quad \textbf{(3.3.2.3)}$$

> $QQ := expand((y-p1)\cdot(y-p2)\cdot(y-p3))$ **mod** $37;$

$$QQ := 31+31x+11y+28x^4+31y^2+9yx^4+8yx^2+5xy+35y^2x^4+35y^2x^2+yx^8+3x^6y+36xy^2+2x^9y+4x^5y+2x^3y+31x^2+32x^8+29x^6+32x^5+31x^3+y^3+36x^{13}+35x^{11}+34x^9+36x^{10}+35x^7+2x^7y+36x^5y^2 \quad \textbf{(3.3.2.4)}$$

> $degree(QQ, x); degree(QQ, y);$

$$13$$
$$3 \quad \textbf{(3.3.2.5)}$$

> $\dfrac{(3\cdot 31-1)}{4}-6;$

$$17 \quad \textbf{(3.3.2.6)}$$

> $t := [seq(i, i=1..31)];$

$$t := [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31] \quad \textbf{(3.3.2.7)}$$

> $X := [seq(subs(x=i, p1) \textbf{ mod } 37, i=1..14), seq(subs(x=i, p2) \textbf{ mod } 37, i=15..28), 0, 0, 0];$

$$X := [3, 19, 11, 2, 2, 8, 4, 35, 22, 21, 1, 29, 11, 25, 17, 5, 0, 28, 28, 0, 5, 17, 34, 4, 10, 11, 27, 28, 0, 0, 0] \quad \textbf{(3.3.2.8)}$$

> $Q := add\left(add\left(q[i,j]\cdot x^i\cdot y^j, i=0..13-4\cdot j\right), j=0..3\right);$

$$Q := q_{5,1}x^5y+q_{2,2}x^2y^2+q_{7,0}x^7+q_{3,2}x^3y^2+q_{1,2}xy^2+q_{8,1}x^8y+q_{2,0}x^2+q_{1,1}xy+q_{12,0}x^{12}+q_{3,0}x^3+q_{5,2}x^5y^2+q_{9,0}x^9+q_{1,0}x+q_{1,3}xy^3+q_{9,1}x^9y+q_{7,1}x^7y+q_{5,0}x^5+q_{4,2}x^4y^2+q_{0,1}y+q_{4,1}x^4y+q_{0,3}y^3+q_{0,2}y^2+q_{11,0}x^{11}+q_{6,1}x^6y+q_{10,0}x^{10} \quad \textbf{(3.3.2.9)}$$

$+ q_{8,0} x^8 + q_{4,0} x^4 + q_{3,1} x^3 y + q_{6,0} x^6 + q_{2,1} x^2 y + q_{13,0} x^{13} + q_{0,0}$

> $E := \{seq(subs(x = t[i], subs(y = X[i], Q)) \textbf{ mod } 37 = 0, i = 1..31)\}$:

> $S := solve(E) \textbf{ mod } 37;$

$$S := \{q_{0,0} = 30 q_{4,0}, q_{0,1} = 20 q_{4,0}, q_{0,2} = 10 q_{4,0}, q_{0,3} = 14 q_{4,0}, q_{1,0} = 9 q_{4,0}, q_{1,1} = 32 q_{4,0}, q_{1,2} = 22 q_{4,0}, q_{1,3} = 3 q_{4,0}, q_{2,0} = 3 q_{4,0}, q_{2,1} = 5 q_{4,0}, q_{2,2} = 3 q_{4,0}, q_{3,0} = 23 q_{4,0}, q_{3,1} = 28 q_{4,0}, q_{3,2} = 4 q_{4,0}, q_{4,0} = q_{4,0}, q_{4,1} = 14 q_{4,0}, q_{4,2} = 9 q_{4,0}, q_{5,0} = 26 q_{4,0}, q_{5,1} = 9 q_{4,0}, q_{5,2} = 36 q_{4,0}, q_{6,0} = 22 q_{4,0}, q_{6,1} = 32 q_{4,0}, q_{7,0} = 16 q_{4,0}, q_{7,1} = 13 q_{4,0}, q_{8,0} = 29 q_{4,0}, q_{8,1} = 14 q_{4,0}, q_{9,0} = 6 q_{4,0}, q_{9,1} = 30 q_{4,0}, q_{10,0} = 2 q_{4,0}, q_{11,0} = 20 q_{4,0}, q_{12,0} = 0, q_{13,0} = 5 q_{4,0}\} \tag{3.3.2.10}$$

> $Q := subs(S, Q);$

$$Q := q_{4,0} x^4 + 30 q_{4,0} + 3 q_{4,0} x^2 + 23 q_{4,0} x^3 + 6 q_{4,0} x^9 + 9 q_{4,0} x + 26 q_{4,0} x^5 + 20 q_{4,0} y + 14 q_{4,0} y^3 + 10 q_{4,0} y^2 + 20 q_{4,0} x^{11} + 2 q_{4,0} x^{10} + 29 q_{4,0} x^8 + 22 q_{4,0} x^6 + 5 q_{4,0} x^{13} + 28 q_{4,0} x^3 y + 32 q_{4,0} x^6 y + 13 q_{4,0} x^7 y + 5 q_{4,0} x^2 y + 14 q_{4,0} x^8 y + 32 q_{4,0} x y + 14 q_{4,0} x^4 y + 30 q_{4,0} x^9 y + 36 q_{4,0} x^5 y^2 + 3 q_{4,0} x y^3 + 22 q_{4,0} x y^2 + 4 q_{4,0} x^3 y^2 + 3 q_{4,0} x^2 y^2 + 9 q_{4,0} x^4 y^2 + 9 q_{4,0} x^5 y + 16 q_{4,0} x^7 \tag{3.3.2.11}$$

> $Q := subs(q[4, 0] = 1, Q);$

$$Q := 30 + 9 x + 20 y + x^4 + 10 y^2 + 14 y x^4 + 5 y x^2 + 32 x y + 9 y^2 x^4 + 3 y^2 x^2 + 14 y x^8 + 32 x^6 y + 22 x y^2 + 30 x^9 y + 9 x^5 y + 28 x^3 y + 3 x^2 + 29 x^8 + 22 x^6 + 26 x^5 + 23 x^3 + 14 y^3 + 5 x^{13} + 20 x^{11} + 6 x^9 + 2 x^{10} + 16 x^7 + 4 x^3 y^2 + 3 x y^3 + 13 x^7 y + 36 x^5 y^2 \tag{3.3.2.12}$$

> $Q0 := subs(x = 0, Q);$

$$Q0 := 30 + 20 y + 10 y^2 + 14 y^3 \tag{3.3.2.13}$$

> $msolve(Q0 = 0, 37);$

$$\{y = 1\}, \{y = 2\}, \{y = 28\} \tag{3.3.2.14}$$

```
> Poly := proc(Q, y0, n, p)
  local P, dQ, QP, dQP, r, S;
  r := 1;
  P := y0;
  dQ := diff(Q, y);
  while r < n do
  r := 2·r;
  QP := expand(subs(y = P, Q)) mod p;
  dQP := expand(subs(y = P, dQ)) mod p;
```

$S := series\left(\frac{QP}{dQP}, x, r\right)$ **mod** p;

$P := P - convert(S, polynom)$ **mod** p;

od;

end:

> $Q - QQ$ **mod** 37;

$$36 + 15\,x + 9\,y + 10\,x^4 + 16\,y^2 + 5\,y\,x^4 + 34\,y\,x^2 + 27\,x\,y + 11\,y^2\,x^4 + 5\,y^2\,x^2 + 13\,y\,x^8 + 29\,x^6\,y + 23\,x\,y^2 + 28\,x^9\,y + 5\,x^5\,y + 26\,x^3\,y + 9\,x^2 + 34\,x^8 + 30\,x^6 + 31\,x^5 + 29\,x^3 + 13\,y^3 + 6\,x^{13} + 22\,x^{11} + 9\,x^9 + 3\,x^{10} + 18\,x^7 + 4\,x^3\,y^2 + 3\,x\,y^3 + 11\,x^7\,y \tag{3.3.2.15}$$

> $Poly(Q, 1, 5, 37)$;

$$x^4 + x + 1 \tag{3.3.2.16}$$

> $expand(subs(y = \%, Q))$ **mod** 37;

$$0 \tag{3.3.2.17}$$

Exemple 3. ==31, k=5, delta=3, l<18.

> $X := PSeuil(31, 5, 37, 3, t)$;

$$X := [31, 15, 11, 11, 17, 4, 31, 19, 10, 19, 34, 16, 10, 34, 5, 35, 24, 30, 10, 5, 29, 32, 11, 10, 9, 35, 14, 30, 29, 4, 32] \tag{3.3.3.1}$$

> $h := rand(0..36)$;

$h :=$ **proc**( )

proc( ) **option** *builtin = RandNumberInterface*; **end proc**(6, 37, 6)

end proc (3.3.3.2)

> $XX := X$;**for** i **from** 1 **to** 17 **do** $XX[i] := h()$ **mod** 37 **od**;

$XX := [31, 15, 11, 11, 17, 4, 31, 19, 10, 19, 34, 16, 10, 34, 5, 35, 24, 30, 10, 5, 29, 32, 11, 10, 9, 35, 14, 30, 29, 4, 32]$

$$XX_1 := 8$$
$$XX_2 := 21$$
$$XX_3 := 31$$
$$XX_4 := 33$$
$$XX_5 := 8$$
$$XX_6 := 2$$
$$XX_7 := 33$$
$$XX_8 := 4$$
$$XX_9 := 2$$
$$XX_{10} := 8$$
$$XX_{11} := 23$$

$$XX_{12} := 36$$
$$XX_{13} := 29$$
$$XX_{14} := 15$$
$$XX_{15} := 28$$
$$XX_{16} := 2$$
$$XX_{17} := 2 \quad \textbf{(3.3.3.3)}$$

> $Q := add\left(add\left(q[i,j]\cdot x^i\cdot y^j, i=0..13-4\cdot j\right), j=0..3\right);$

$$Q := q_{5,1}\,x^5\,y + q_{2,2}\,x^2\,y^2 + q_{7,0}\,x^7 + q_{1,2}\,x\,y^2 + q_{8,1}\,x^8\,y + q_{2,0}\,x^2 + q_{1,1}\,x\,y + q_{12,0}\,x^{12} + q_{3,0}\,x^3 + q_{9,0}\,x^9 + q_{1,0}\,x + q_{7,1}\,x^7\,y + q_{5,0}\,x^5 + q_{0,1}\,y + q_{4,1}\,x^4\,y + q_{0,2}\,y^2 + q_{11,0}\,x^{11} + q_{6,1}\,x^6\,y + q_{10,0}\,x^{10} + q_{8,0}\,x^8 + q_{4,0}\,x^4 + q_{3,1}\,x^3\,y + q_{6,0}\,x^6 + q_{2,1}\,x^2\,y + q_{13,0}\,x^{13} + q_{0,0} + q_{1,3}\,x\,y^3 + q_{3,2}\,x^3\,y^2 + q_{9,1}\,x^9\,y + q_{5,2}\,x^5\,y^2 + q_{4,2}\,x^4\,y^2 + q_{0,3}\,y^3 \quad \textbf{(3.3.3.4)}$$

> $E := \{seq(subs(x=t[i], subs(y=XX[i], Q))\ \textbf{mod}\ 37 = 0, i=1..31)\}:$

> $S := solve(E)\ \textbf{mod}\ 37;$

$$S := \{q_{0,0} = 29\,q_{2,0}, q_{0,1} = 2\,q_{2,0}, q_{0,2} = 7\,q_{2,0}, q_{0,3} = 32\,q_{2,0}, q_{1,0} = 32\,q_{2,0}, q_{1,1} = 11\,q_{2,0}, q_{1,2} = 21\,q_{2,0}, q_{1,3} = 27\,q_{2,0}, q_{2,0} = q_{2,0}, q_{2,1} = 36\,q_{2,0}, q_{2,2} = q_{2,0}, q_{3,0} = 23\,q_{2,0}, q_{3,1} = 21\,q_{2,0}, q_{3,2} = 21\,q_{2,0}, q_{4,0} = 36\,q_{2,0}, q_{4,1} = 29\,q_{2,0}, q_{4,2} = 6\,q_{2,0}, q_{5,0} = 35\,q_{2,0}, q_{5,1} = 29\,q_{2,0}, q_{5,2} = 0, q_{6,0} = 8\,q_{2,0}, q_{6,1} = 7\,q_{2,0}, q_{7,0} = 28\,q_{2,0}, q_{7,1} = 17\,q_{2,0}, q_{8,0} = 5\,q_{2,0}, q_{8,1} = 18\,q_{2,0}, q_{9,0} = 25\,q_{2,0}, q_{9,1} = 17\,q_{2,0}, q_{10,0} = 31\,q_{2,0}, q_{11,0} = 12\,q_{2,0}, q_{12,0} = 14\,q_{2,0}, q_{13,0} = 27\,q_{2,0}\} \quad \textbf{(3.3.3.5)}$$

> $Q := subs(S, Q);$

$$Q := 6\,q_{2,0}\,x^4\,y^2 + q_{2,0}\,x^2 + 29\,q_{2,0} + 32\,q_{2,0}\,y^3 + 27\,q_{2,0}\,x^{13} + 8\,q_{2,0}\,x^6 + 36\,q_{2,0}\,x^4 + 5\,q_{2,0}\,x^8 + 31\,q_{2,0}\,x^{10} + 12\,q_{2,0}\,x^{11} + 7\,q_{2,0}\,y^2 + 2\,q_{2,0}\,y + 35\,q_{2,0}\,x^5 + 32\,q_{2,0}\,x + 25\,q_{2,0}\,x^9 + 23\,q_{2,0}\,x^3 + 14\,q_{2,0}\,x^{12} + 28\,q_{2,0}\,x^7 + 7\,q_{2,0}\,x^6\,y + 21\,q_{2,0}\,x\,y^2 + 29\,q_{2,0}\,x^5\,y + q_{2,0}\,x^2\,y^2 + 11\,q_{2,0}\,x\,y + 27\,q_{2,0}\,x\,y^3 + 36\,q_{2,0}\,x^2\,y + 17\,q_{2,0}\,x^9\,y + 17\,q_{2,0}\,x^7\,y + 18\,q_{2,0}\,x^8\,y + 21\,q_{2,0}\,x^3\,y^2 + 21\,q_{2,0}\,x^3\,y + 29\,q_{2,0}\,x^4\,y \quad \textbf{(3.3.3.6)}$$

> $Q := subs(q[2,0]=1, Q);$

$$Q := 29 + 32\,x + 2\,y + 36\,x^4 + 14\,x^{12} + 7\,y^2 + 29\,y\,x^4 + 36\,y\,x^2 + 11\,x\,y + 6\,y^2\,x^4 + y^2\,x^2 + 18\,y\,x^8 + 7\,x^6\,y + 21\,x\,y^2 + 17\,x^9\,y + 29\,x^5\,y + 21\,x^3\,y \quad \textbf{(3.3.3.7)}$$

$$+ x^2 + 5x^8 + 8x^6 + 35x^5 + 23x^3 + 32y^3 + 27x^{13} + 12x^{11} + 25x^9 + 31x^{10} + 21x^3y^2 + 28x^7 + 17x^7y + 27xy^3$$

> $Q0 := subs(x = 0, Q);$

$$Q0 := 29 + 2y + 7y^2 + 32y^3 \tag{3.3.3.8}$$

> $msolve(Q0 = 0, 37);$

$$\{y = 3\} \tag{3.3.3.9}$$

> $Poly(Q, 3, 5, 37);$

$$3 + 23x + 7x^2 + 13x^3 + 22x^4 \tag{3.3.3.10}$$

> $expand(subs(y = \%, Q))$ **mod** $37;$

$$0 \tag{3.3.3.11}$$

>