// Section 1.1

// BLS12-381 curve

z := -0xd201000000010000;

r := z^4 - z^2 + 1;

q := ((z - 1)^2 \* r) div 3 + z;

IsPrime(r);

IsPrime(q);

Log(2, r);

Log(2, q);

q mod 27;

q mod 4;

n1 := (q-10) div 27;

n2 := (q-3) div 4;

// sliding window method

n := n1;

// n := n2;

Bits := Intseq(n, 2);

i := #Bits;

k := 5;

y := 0;

chain := { };

U := { };

while i gt 0 do

if Bits[i] eq 0 then

y := 2\*y;

Include(~chain, y);

i := i-1;

else

s := Max(i-k+1, 1);

while Bits[s] eq 0 do

s := s+1;

end while;

for h := 1 to i-s+1 do

y := 2\*y;

Include(~chain, y);

end for;

I := [s..i];

u := Seqint(Bits[I], 2);

Include(~U, u);

y := y + u;

Include(~chain, y);

i := s-1;

end if;

end while;

U eq {1 .. 2^k - 1 by 2};

chain := chain join U join {2};

Exclude(~chain, 0);

n eq Maximum(chain);

#chain;

chain;

////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////

// Section 2.2

F := Rationals();

A2<x,y> := AffinePlane(F);

C7 := Curve(A2, y^7 - x^2\*(x+1));

E7 := Curve(A2, y^2 - (x^3 + 21/4\*x^2 + 7\*x));

numx := 2\*y\*( x^2\*(-y^7 - y^5 - y^2 + y + 1) + x\*(-y^2 + y + 1)\*y^7 +

(y^5 + y^2 - y - 1)\*y^7 );

numy := x^2\*(3\*y^8 + 2\*y^7 + 3\*y^6 + 2\*y^5 + 2\*y^4 - y^3 -

3\*y^2 - 3\*y - 2) + x\*(2\*y^4 - y^3 - 3\*y^2 - 3\*y - 2)\*y^7 +

(-3\*y^6 - 2\*y^5 - 2\*y^4 + y^3 + 3\*y^2 + 3\*y + 2)\*y^7;

den := 2\*y^3\*( x^2 + x\*y^7 - y^7 );

chi := map<C7 -> E7 | [numx/den, numy/den]>;