In[ ]:=
```
Исходные данные;
p = 1123;
Px = 121;
Py = 951;
P = {Px, Py};
a = 100; b = 10;
c = 1;
```

In[ ]:=
```
Задание 1;
```

In[ ]:=
```
Mod[Px^3 + a * Px^2 + b * Px + c, p] ≠ 0
```
остаток от деления

Out[ ]=
```
True
```

In[ ]:=
```
AmountP =
 Length[g1 = {x, y} /. Flatten[Table[FindInstance[y^2 == x^3 + a * x^2 + b * x + 1 && x == u,
 {x, y}, 2, Modulus → p], {u, 0, p - 1}], 1]]
```
длина; уплостить; табл…; найти частный случай; модуль

Out[ ]=
```
1067
```

In[ ]:=
```
Задание 2;
```

In[ ]:=
```
FactorInteger[AmountP]
```
факторизовать целое число

Out[ ]=
```
{{11, 1}, {97, 1}}
```

In[ ]:=
```
PrimeQ[AmountP]
```
простое число?

Out[ ]=
```
False
```

In[ ]:=
```
Задание 3;
```

```
In[•]:= EllipticAdd[p_, a_, b_, c_, P_List, Q_List] :=
 Module[{lam, x3, y3, P3},
  программный модуль
  Which[
  условный оператор с множественными ветвями
   P == {0}, Q,
        О большое
   Q == {0}, P,
        О большое
   P[[1]] != Q[[1]],
         lam = Mod[(Q[[2]] - P[[2]]) PowerMod[Q[[1]] - P[[1]], p - 2, p], p];
               остаток от деления          степень по модулю
         x3 = Mod[lam^2 - a - P[[1]] - Q[[1]], p];
              остаток от деления
         y3 = Mod[-(lam (x3 - P[[1]]) + P[[2]]), p];
              остаток от деления
         {x3, y3},
   (P == Q) ∧ (P[[2]] == 0), {0},
                             О большое
   (P == Q) ∧ (P != {0}),
                  О большое
        lam = Mod[ (3 * P[[1]]^2 + 2 a * P[[1]] + b) PowerMod[2 P[[2]], p - 2, p], p];
              остаток от деления                    степень по модулю
         x3 = Mod[lam^2 - a - P[[1]] - Q[[1]], p];
              остаток от деления
         y3 = Mod[-(lam (x3 - P[[1]]) + P[[2]]), p];
              остаток от деления
         {x3, y3},
   (P[[1]] == Q[[1]]) ∧ (P[[2]] != Q[[2]]), {0}]]
                                           О большое

In[•]:= i = 1; P1 = P; P2 = P;
While[P2 ≠ {0}, P2 = EllipticAdd[p, a, b, c, P1, P2]; i++];
цикл-пока   О большое
i

Out[•]= 1068

In[•]:= Задание 4;
IntegerDigits[1068, 2]
цифры целого числа

Out[•]= {1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0}

Задание 5;

In[•]:= P =.;
p = 1123; a = 100; b = 10; c = 1;
P[0] = {121, 951};
P[i_] := P[i] = EllipticAdd[p, a, b, c, P[i - 1], P[i - 1]];
Q = EllipticAdd[p, a, b, c,
  EllipticAdd[p, a, b, c, P[10], P[5]], EllipticAdd[p, a, b, c, P[3], P[2]]]

Out[•]= {0}

In[•]:= Задание 7;
aSecr = 340; bSecr = 774;
```

In[•]:=
```
Задание 8;
IntegerDigits[aSecr, 2]
```
цифры целого числа

Out[•]= {1, 0, 1, 0, 1, 0, 1, 0, 0}

In[•]:=
```
IntegerDigits[bSecr, 2]
```
цифры целого числа

Out[•]= {1, 1, 0, 0, 0, 0, 0, 1, 1, 0}

In[•]:=
```
Qa = EllipticAdd[p, a, b, c,
  EllipticAdd[p, a, b, c, P[8], P[6]], EllipticAdd[p, a, b, c, P[4], P[2]]]
```

Out[•]= {947, 893}

In[•]:=
```
Qb = EllipticAdd[p, a, b, c,
  EllipticAdd[p, a, b, c, P[9], P[8]], EllipticAdd[p, a, b, c, P[2], P[1]]]
```

Out[•]= {997, 1062}

In[•]:=
```
i = 1;
P1 = Qa; P2 = P1;
While[P2 ≠ {O}, P2 = EllipticAdd[p, a, b, c, P1, P2]; i++];
```
цикл–пока О большое
```
i
```

Out[•]= 267

In[•]:=
```
i = 1;
P1 = Qb; P2 = P1;
While[P2 ≠ {O}, P2 = EllipticAdd[p, a, b, c, P1, P2]; i++];
```
цикл–пока О большое
```
i
```

Out[•]= 178

In[•]:=
```
Задание 9;
```

In[•]:=
```
IntegerDigits[267, 2]
```
цифры целого числа

Out[•]= {1, 0, 0, 0, 0, 1, 0, 1, 1}

In[•]:=
```
IntegerDigits[178, 2]
```
цифры целого числа

Out[•]= {1, 0, 1, 1, 0, 0, 1, 0}

In[•]:=
```
QA[0] = {947, 893};
QA[i_] := QA[i] = EllipticAdd[p, a, b, c, QA[i - 1], QA[i - 1]];
EllipticAdd[p, a, b, c, EllipticAdd[p, a, b, c, QA[9], QA[8]],
 EllipticAdd[p, a, b, c, QA[2], QA[1]]]
```

Out[•]= {582, 323}

In[•]:=
```
QB[0] = {997, 1062};
QB[i_] := QB[i] = EllipticAdd[p, a, b, c, QB[i - 1], QB[i - 1]];
EllipticAdd[p, a, b, c, EllipticAdd[p, a, b, c, QB[8], QB[6]],
 EllipticAdd[p, a, b, c, QB[4], QB[2]]]
```

Out[•]= {582, 323}

Задание 10;

In[•]:=
```
EllipticPointMultiply[p_, a_, b_, c_, Q_, n_] :=
 Module[{i = n - 1, q = Q, pl = p, al = a, bl = b, cl = c},
  pnt = q;
  While[i > 0, i--; q = EllipticAdd[pl, al, bl, cl, pnt, q]];
  q
 ]
EllipticPointMultiply[p, a, b, c, {121, 951}, aSecr * bSecr]
```

Out[•]= {582, 323}

Задание 11;

```
a = 100; b = 10; c = 1; p = 1123; i = 0;
x1 = 0; y1 = 0; isFound = False;
While[(x1 < p) && (isFound == False),
  If[Solve[y^2 == x1^3 + a * x1^2 + b * x1 + c + i, {y}, Modulus → p] ≠ {},
    y1 = y /. Flatten[Solve[y^2 == x1^3 + a * x1^2 + b * x1 + c + i, {y}, Modulus → p], 1];
    p1 = {x1, y1};
    p2 = {x1, y1};
    rank = 1;
    While[p2 ≠ {0},
     p2 = EllipticAdd[p, a, b, c + i, p1, p2];
     rank++;
    ];
    If[PrimeQ[rank],
     Print["Точка: ", p1, " Порядок: ", rank, " Параметр I: ", i];
     isFound = True,
     x1++;
    ],
    x1++;
   ];
 ];
```

```
Точка: {10, 227} Порядок: 89 Параметр I: 0
```

In[•]:=
```
PrimeQ[89]
```

Out[•]= True