

```

FindPoint[p0_, a0_, b0_, c0_, xm_, rm_] := Module[
  {p = p0, a = a0, b = b0, c = c0, XMin = xm, RankMin = rm, found, x1, y1, i, r, try, y, tP, P, P1, A, s, flag, t, rank},
  found = False;
  x1 = 0;
  y1 = 0;
  i = 0;
  r = Ceiling[Sqrt[Round[p + 1 + 2 * Sqrt[p]]]];
  While[found == False,
    If[Mod[4 * b^3 + 27 * (c + i)^2, p] ≠ 0,
      x1 = XMin; try = 0;
      While[(try < 40) && (found == 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];
          tP = {};
          P = {x1, y1};
          AppendTo[tP, P];
          Do[{P = EllipticAdd[p, a, b, c + i, tP[[1]], P], AppendTo[tP, P]}, {1, 2, r}];
          P1 = Mod[tP[[r]] * {1, -1}, p];
          A = {0};
          s = 0; flag = True;
          While[flag,
            A = EllipticAdd[p, a, b, c + i, P1, A]; s++;
            For[t = 1, t ≤ r, t++,
              If[tP[[t]] == A,
                flag = False; Break[];
              ];
            ];
          ];
          rank = r * s + t;
          Which[rank > RankMin && PrimeQ[rank],
            {Print["P=", tP[[1]], ".
              x=", x1, " ≥ Floor[p/2]=", XMin, ".
              Порядок точки=", rank, " ≥ 2p/3=", RankMin, " и является простым числом.
              Эллиптическая кривая y^2=x^3+", a, "*x^2+", b, "*x+", c + i, " - гладкая. i=", i];
              found = True;},
            rank > RankMin && ! (PrimeQ[rank]), {
              x1++;
              try++;},
            rank ≤ RankMin, {
              x1++;
              try++;}];,
          x1++;
          try++;
          ];
        ];
        i++;];
  ]
]

```