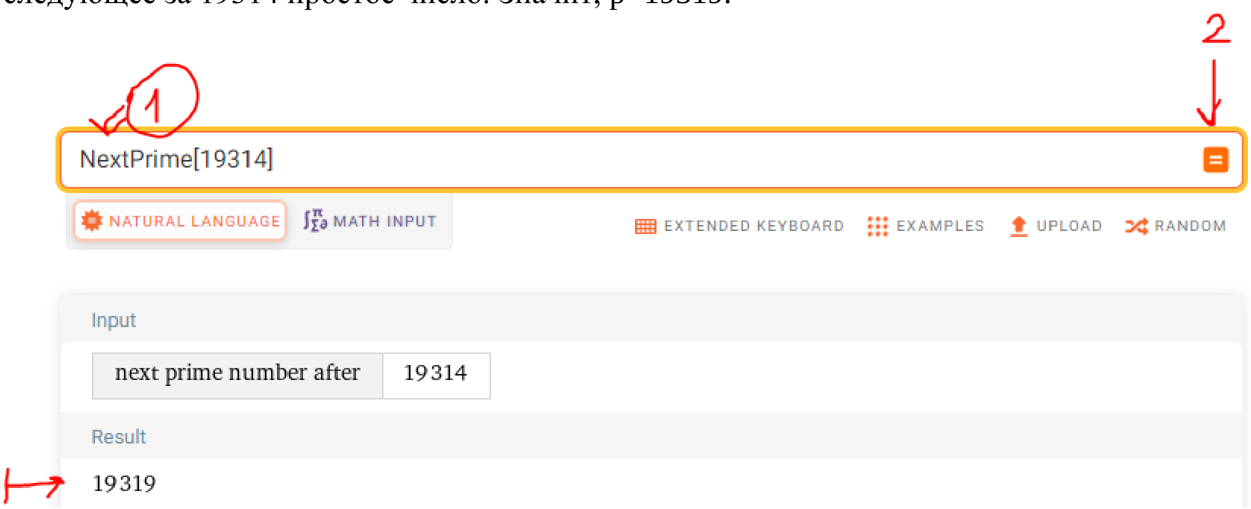
ЛАБОРАТОРНОЕ занятие по вычислениям на эллиптической кривой.
Задание

1) Выбрать простое p примерно равное mnk, где m, n, k – номера букв в инициалах (можно взять только две буквы).
2) Перебором найти на линии $y^2 = x^3 + ax + b$ точку P с минимальным положительным $x$ ($a$=1, $b$=0).
3) Найти 151P для заданной точки.
4) * Найти порядок линии.
5) *Найти порядок точки P.

Замечания
1. Для вычислений желательно использовать компьютерные программы, например, программа SimpleNumber.exe находится в папке SimpleNumber\SimpleNumber, тест Миллера – Рабина: файл Test Millera-Rabina.exe.
2. Некоторые действия можно выполнить различными способами, поэтому в примере первое число означает номер шага, а второе число номер способа, то есть если есть пункты 1-1 и 1-2, то они делают одно и тоже действие, но используют различные средства. В Вашем индивидуальном решении можно использовать любой из них (один).

**Пример 1**.
1-1) Инициалы СВН. Смотрим номера букв: С=19, В=3, Н=14, значит, число p=19314.
$p \vdots 2 \Rightarrow$ не простое, значит, возьмём следующее нечётное число: p=19315
$p \vdots 5 \Rightarrow$ не простое, значит, возьмём следующее нечётное число: p=19317
$19317 \vdots 3 \Rightarrow$ не простое, значит, возьмём следующее нечётное число: p=19319.
p не делится на простые числа 2,3,5,7,11,13,17,19, поэтому проверим его с помощью теста Миллера-Рабина. С помощью проверок с 10 свидетелями простоты убеждаемся, что с вероятностью всего лишь 1/1000000 это число может быть составным.
Замечание: поиск простого числа описывался в лабораторной работе по тесту Миллера-Рабина.

1-2) Инициалы СВН. Смотрим номера букв: С=19, В=3, Н=14, значит, число p=19314.Найдём через вольфрам альфа (https://ru.wolframalpha.com/) командой NextPrime следующее за 19314 простое число. Значит, p=19319.




2) Найдём одно решение уравнения $y^2 = x^3 + ax + b \ (mod\ 19319)$ (для каждого $x$ перебираем все $y$ от 0 до p-1=19318 пока не получим верное равенство).
Перебором находим точку P = (1,139).

3) Представим 151 в виде последовательности удвоений. Сначала представим 151 в двоичном виде. $2^7 = 128 < 151$,     $2^8 = 256 > 151$ Запишем степени двойки:

| $k$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|---|
| $2^k$ | 2 | 4 | 8 | 16 | 32 | 64 | 128 | 256 |

Последовательно отнимаем максимальную степень двойки, не превосходящую текущее число:

151-128=23,     23-16=7,     7-4=3,     3-2=1

Таким образом, $151 = 128 + 16 + 4 + 2 + 1 = 2^7 + 2^4 + 2^1 + 1$, значит,

$$151P = 128P + 16P + 4P + 2P + P$$

$2^k P$ находится с помощью последовательного удвоения точки.

Напомним правило сложения двух точек $P = (x_1, y_1)$, $Q = (x_2, y_2)$ лежащих на эллиптической кривой.

I) Если $x_2 \neq x_1$, то $k = (y_2 - y_1) \cdot (x_2 - x_1)^{-1}$, $x = k^2 - (x_1 + x_2)$, $y = k(x_1 - x) - y_1$.

II) Если $x_2 = x_1$ и $y_1 + y_2 = 0$, то $P + Q = E = (*; \infty)$ – бесконечно удалённая точка

III) Если $x_2 = x_1$ и $y_2 = y_1$, то $k = (3x_1^2 + a) \cdot (2y_1)^{-1}$, $x = k^2 - 2x_1$, $y = k(x_1 - x) - y_1$.

Замечания.

1) Все вычисления выполняются по модулю p/

2) I – сложение точек с разными абсциссами; II – сложение противоположных точек, всегда даёт нейтральную точку; III – сложение одинаковых точек, также называется удвоением.

3) Сложение различных точек и удвоение используют различные формулы для промежуточной величины k, но формулы для x и y идентичны.

Найдём $2P = P + P = 2 \cdot (1{,}139)$ Используем формулы удвоения точки (по модулю p=19319):

$k = (3x_1^2 + a) \cdot (2y_1)^{-1} = (3 \cdot 1^2 + 1) \cdot (2 \cdot 139)^{-1} = 4 \cdot 14524 = 139 \ (mod\ 19319)*$

*Замечание. Вычисление обратного см. приложение 1.

$$x = k^2 - 2x_1 = 139^2 - 2 \cdot 1 = 19319 = 0,$$
$$y = k(x_1 - x) - y_1 = 139 \cdot (1 - 0) - 139 = 0$$
$$2P = (0{,}0)$$

Найдём $4P = 2P + 2P = 2 \cdot (0{,}0)$ Используем формулы удвоения точки (по модулю p=19319):

Так как $x_2 = x_1$ и $y_1 + y_2 = 0$, то $2 \cdot (0{,}0) = E$– бесконечно удалённая точка.

Так как $4P = E$, то $8P = 4P + 4P = E + E = E$ и т.д. $4kP = E =>$

$$151P = 128P + 16P + 4P + 2P + P = E + E + E + (0{,}0) + (1{,}139) = (0{,}0) + (1{,}139)$$
$$k = (y_2 - y_1) \cdot (x_2 - x_1)^{-1} = (139 - 0) \cdot (1 - 0)^{-1} = 139,$$
$$x = 139^2 - (0 + 139) = 19182,$$
$$y = k(x_1 - x) - y_1 = 139 \cdot (1 - 0) - 0 = 139$$
$$151P = (19182{,}139)$$

4) Найдём порядок кривой с помощью перебора (см. Приложение 2): 19320

5) В процессе вычисления было найдено, что $4P = E$. Найдём делители 4: это 2, значит, достаточно проверить $\left(\frac{4}{2}\right) P = 2P \neq E$, значит, порядок P равен 4.

Ответ. 1) p=19319, 2) P=(1,139), 3) $151P = (19182{,}139)$; 4) $|G| = 19320$; 5) $|P| = 4$.

**Пример 2**. Сделаем все те же действия для эллиптической кривой $y^2 = x^3 + ax + b$, где $a = 20,\ b = 22$.

Замечание. Этот пример вычислительно сложный, число p=313241 является 14-тибитным, переборные алгоритмы работают долго, но всё же не очень долго. Пример приведён для наглядности вычислений, повторять такой пример без специальных программ и алгоритмов не рекомендуется. Напомним, что для реальных криптографических задач используются не менее, чем 256-тибитные числа из G(p) или G(p^n).

1) Инициалы ЭЮЯ. Номера букв в алфавите: Э=31, Ю=32, Я=33. С помощью команды NextPrime[313233] находим простое число p=313241
2) С помощью команд a,b,p=20,22,313241 и proba(a,b,p) находим точку эллиптической кривой (3, 16565) (см. приложение 2).
3) Так как $151P = 128P + 16P + 4P + 2P + P$, то вычислим промежуточные точки:

$$2P = 2 \cdot (3, \quad 16565)$$

$k = (3x_1^2 + a) \cdot (2y_1)^{-1} = (3 \cdot 3^2 + 20) \cdot (2 \cdot 16565)^{-1}\ (mod\ 313241)*$

С помощью команды print(gcdex(2*16565,313241)) найдём обратный элемент. Получим: (1, -50215, 5311), значит, $(2 \cdot 16565)^{-1} = -50215 = 263026\ (mod\ 313214)$

Поэтому $k = 47 \cdot 263026 = 12362222 = 145823\ (mod\ 313241)$

$$x = k^2 - 2x_1 = 145823^2 - 2 \cdot 3 = 21264347323 = 295279\ (mod\ 313241),$$

$$y = k(x_1 - x) - y_1 = 145823 \cdot (3 - 295279) - 16565 = -43058048713 = 59147$$

То есть $2P = (295279,\ 59147)$

$$4P = 2 \cdot 2P = 2 \cdot (295279, \quad 59147) = (145452, \quad 56088)$$

Продолжая аналогично, получим:

$$8P = 2 \cdot 4P = 2 \cdot (145452, \quad 56088) = (66413, \quad 72431)$$

$$16P = 2 \cdot 8P = 2 \cdot (66413, \quad 72431) = (290599, \quad 127491)$$

$$32P = 2 \cdot 16P = 2 \cdot (290599, \quad 127491) = (86170, \quad 104335)$$

$$64P = 2 \cdot 32P = 2 \cdot (86170, \quad 104335) = (292650, \quad 220324)$$

$$128P = 2 \cdot 64P = 2 \cdot (292650, \quad 220324) = (62131, \quad 147945)$$

$$151P = 128P + 16P + 4P + 2P + P$$

$$3P = 2P + P = (295279, \quad 59147) + (3, 16565) = (127932, \quad 220265)*$$

*Используем формулы сложения точек с разными *x*.

$$k = (y_2 - y_1) \cdot (x_2 - x_1)^{-1} = (16565 - 59147) \cdot (3 - 295279)^{-1} =$$

$$= \left\{ \begin{matrix} \text{Командой print}\big(\text{obr}(-295279{,}313241)\big)\text{находим обратный элемент:} \\ (-295276)^{-1} = 280182 \end{matrix} \right\} =$$

$$= -42582 \cdot 280182 = -11930709924\ = 13284\ \ (mod\ 313241),$$

$$x = k^2 - (x_1 + x_2) = 13284^2 - (295279 + 3) = 176169374 = 127932\ \ (mod\ 313241),$$

$$y = k(x_1 - x) - y_1 = 13284 \cdot (295279 - 127932) - 59147 = 2222978401 =$$
$$= 220265\ \ (mod\ 313241),$$

$$7P = 4P + 3P = (145452, \quad 56088) + (127932, \quad 220265) = (140220, \quad 270773)$$

$$23P = 16P + 7P = (290599, \quad 127491) + (140220, \quad 270773) =$$
$$= (105212, \quad 156356)$$

$$151P = 128P + 23P = (62131, \quad 147945) + (105212, \quad 156356) =$$
$$= (98182, \quad 39108)$$

4) Найдём порядок кривой с помощью перебора print(porjadok(20,22,313241)):
313184
Вычисления на обычном ПК заняли несколько часов.

5) В пункте 4 было найдено |G|=313184. Разложим это число на множители: $313184 = 2^5 \cdot 9787$, значит (см. утверждения 1 и 2 приложения 3), порядок любого элемента может быть только $2^{k_1} \cdot 9787^{k_2}$, где $0 \le k_1 \le 5,\ \ 0 \le k_2 \le 1$, то есть

$$|P| \in \{1,2,4,8,16,32,9787,19574,39148,78296,156592,313184\}$$

313184 P = E. Простые делители 313184 равны 2 и 9787. $\frac{|G|}{2} = 156592$, $\frac{|G|}{9787} = 32$, значит, достаточно проверить $32P$ и $156592\ P$. В пункте 3 найдено, что $32P \neq E$

Для нахождения $156592\ P$ используем алгоритм быстрого умножения (с помощью удвоений). Разложим 9787 на сумму степеней двойки:

| $t$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $2^t$ | 1 | 2 | 4 | 8 | 16 | 32 | 64 | 128 | 256 | 512 | 1024 | 2048 | 4096 | 8192 |

$$9787 = 8192 + 1595 = 2^{13} + 1024 + 571 = 2^{13} + 2^{10} + 512 + 59 =$$
$$= 2^{13} + 2^{10} + 2^9 + 32 + 27 = 2^{13} + 2^{10} + 2^9 + 2^5 + 16 + 11 =$$
$$= 2^{13} + 2^{10} + 2^9 + 2^5 + 2^4 + 2^3 + 2 + 1 =$$
$$= 1 + 2 + 8 + 16 + 32 + 512 + 1024 + 8192$$
$$256P = 2 \cdot 128P = 2 \cdot (62131,\qquad 147945) = (26793,\qquad 219730)$$
$$512P = 2 \cdot 256P = (76849,\qquad 220967)$$
$$1024P = 2 \cdot 512P = (71538,\qquad 237641)$$
$$2048P = 2 \cdot 1024P = (68157,\qquad 15081)$$
$$4096P = 2 \cdot 2048P = (242214,\qquad 186976)$$
$$8192P = 2 \cdot 4096P = (88667,\qquad 220798)$$

В пункте 3 найдено:

$$3P = 2P + P = (295279,\qquad 59147) + (3, 16565) = (127932,\qquad 220265)$$

Вычислим пошагово 9787 P:

$$11P = 3P + 8P = (127932,\qquad 220265) + (66413,\qquad 72431) = (121122,\qquad 1329),$$
$$27P = 11P + 16P = (287103,\qquad 118859),$$
$$59P = 27P + 32P = (215606,\qquad 118353),$$
$$571P = 59P + 512P = (168488,\qquad 302393),$$
$$1595P = 571P + 1024P = (227824,\qquad 192351),$$
$$9787P = 1595P + 8192P = (197962,\qquad 9052),$$

Теперь снова перейдём к удвоению точек пока не дойдём до 156592 P или до точки E:

$$19574P = 2 \cdot 9787P = (228397,\qquad 278716)$$
$$39148P = 2 \cdot 19574P = (146232,\qquad 197830)$$
$$78296P = 2 \cdot 39148P = (8349{,}0)$$

Так как для $78296P + 78296P$ выполняется условие $x_2 = x_1$ и $y_1 + y_2 = 0$, то $2 \cdot (8349{,}0) = E$– бесконечно удалённая точка, значит, $156592P = E$, т. е. $|P| = 156592$, так как по критерию порядка точки (утверждение 2 из приложения 3) достаточно проверить, что для $k_i = \frac{k}{p_i}$, то есть $k_1 = \frac{156592}{8797} = 16$ и $k_2 = \frac{156592}{2} = 78296$ не выполнялось $kP = E$. В ходе решения было показано, что $16P = (290599,\ 127491) \neq E$,

$$78296P = (8349{,}0) \neq E.$$

Ответ. 1) p=313241, 2) P = (3, 16565), 3) $151P = (98182,\ 39108)$; 4) $|G| = 313184$; 5) $|P| = 156592$.

Приложение 1 Вычисление обратного элемента

Вычисление обратного элемента можно выполнить на сайте https://ru.wolframalpha.com/ с помощью команды PowerMod[a,-1,p], где a – исходное число, обратное к которому мы ищем, p – модуль (см.рис.1).

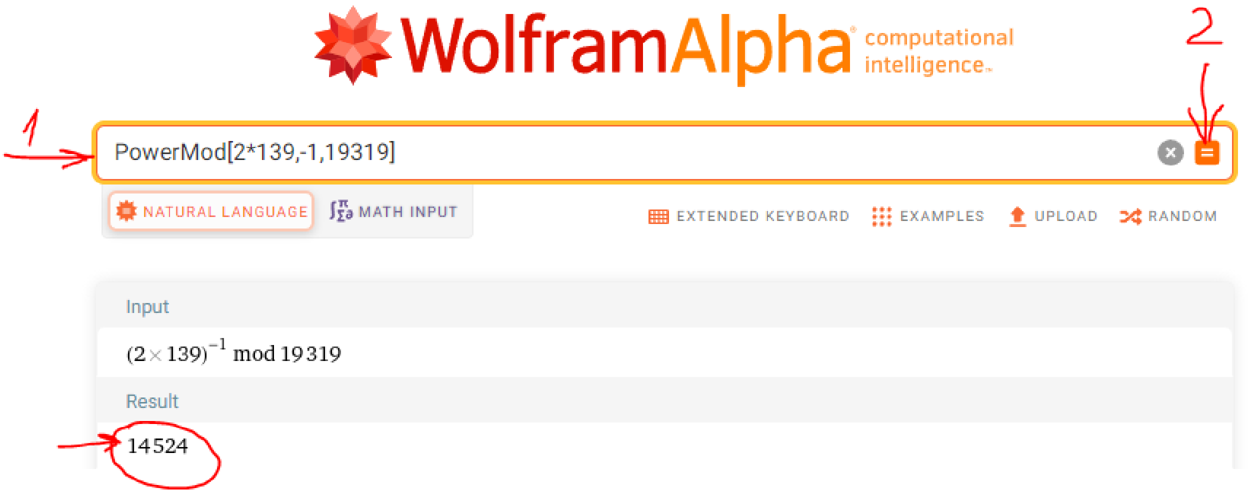
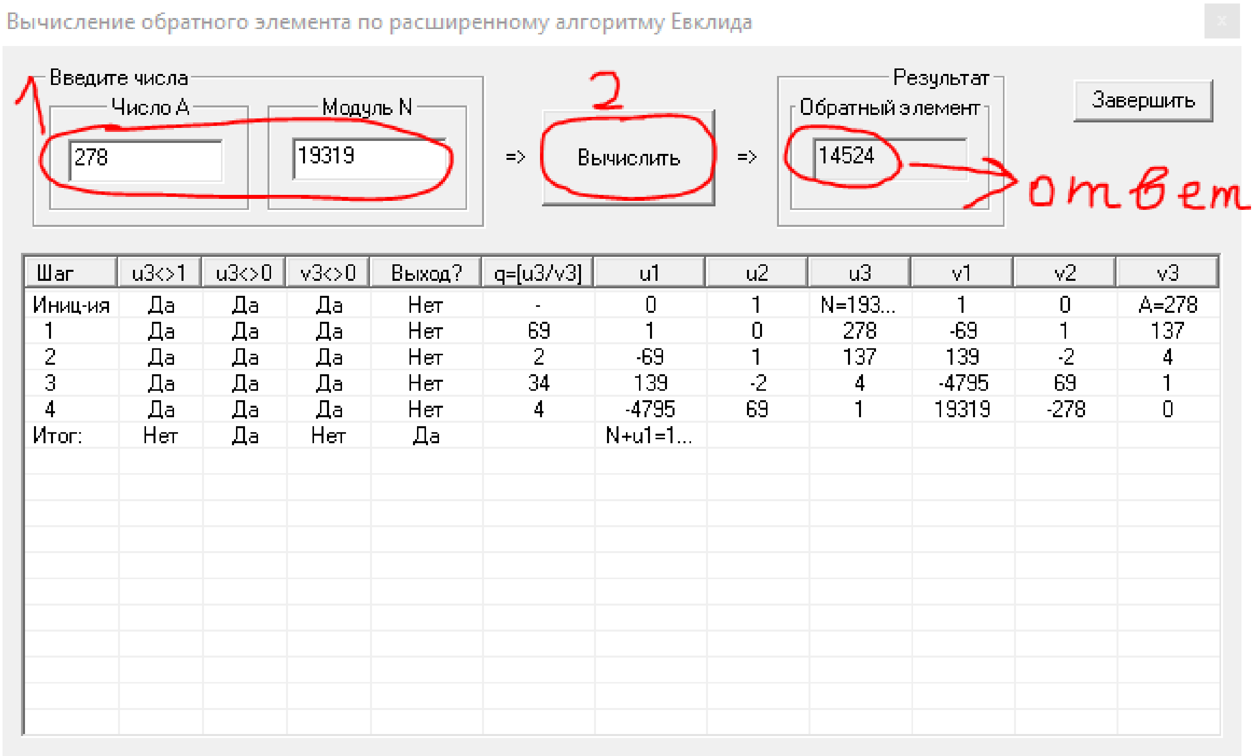



Рисунок 1 – Вычисление обратного элемента на сайте https://ru.wolframalpha.com/

Также обратный элемент можно вычислить с помощью программы EvklidExAlg.exe




| Шаг | u3<>1 | u3<>0 | v3<>0 | Выход? | q=[u3/v3] | u1 | u2 | u3 | v1 | v2 | v3 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Иниц-ия | Да | Да | Да | Нет | - | 0 | 1 | N=193... | 1 | 0 | A=278 |
| 1 | Да | Да | Да | Нет | 69 | 1 | 0 | 278 | -69 | 1 | 137 |
| 2 | Да | Да | Да | Нет | 2 | -69 | 1 | 137 | 139 | -2 | 4 |
| 3 | Да | Да | Да | Нет | 34 | 139 | -2 | 4 | -4795 | 69 | 1 |
| 4 | Да | Да | Да | Нет | 4 | -4795 | 69 | 1 | 19319 | -278 | 0 |
| Итог: | Нет | Да | Нет | Да | | N+u1=1... | | | | | |

Рисунок 2 – Вычисление обратного элемента с помощью EvklidExAlg.exe

Приложение 2 Программы на языке Phyton

1) Следующая функция перебирает конечные точки в поле GF(p) пока не найдёт точку, лежащую на эллиптической кривой.

```
def proba(a,b,p):
#перебирает все конечные точки кривой y^2=x^3+ax+b в поле GF(p)
#если точка лежит на кривой, то функция возвращает эту точку и заканчивает работу
  for x in range(1,p):
     y2=(pow(x,3)+a*x+b)%p
     for y in range(0,p):
         if (pow(y,2)%p)==y2:
             return x,y
```

Для показа результата в онлайн версии нужно вывести результат следующей командой:

```
print(proba(1,0,19319))
```

2) Следующая рекурсивная функция реализует расширенный алгоритм Евклида. Она может быть использована для поиска обратного элемента

```
def gcdex(a, b):
    if b == 0:
        return a, 1, 0
    else:
        d, x, y = gcdex(b, a % b)
        return d, y, x - y * (a // b)
```

Например, команда print(gcdex(278,19319)) даёт результат:

(1, -4795, 69)
это означает, что НОД(278,19319), а остальные числа означают множители исходных чисел, дающие НОД, то есть:

$$-4795 \cdot 278 + 69 \cdot 19319 = 1$$

Отсюда следует, что $-4795 \cdot 278 = 1\ (mod\ 19319)$, значит,

$$278^{-1} = -4795 = 14524\ (mod\ 19319)$$

Командой

```
g2=gcdex(278,19319)[1]
```

можно сразу получить обратное число. Также можно использовать функцию нахождения обратного элемента к $a$ по модулю $b$.

```
def obr(a, b):
#Находит a^(-1) mod b, то есть такое c, что ac=1(mod b)
    g=gcdex(a, b)
    if g[0] == 1:
        return g[1]%b
    else:
        return 0
```

print(obr(278,19319)) даёт результат 14524.

3) Определение. Порядком эллиптической кривой называется количество точек на ней.

Теорема Хассе. Если эллиптическая кривая задана над полем содержащим $q$ элементов, то число $|G|$ точек на ней удовлетворяет неравенству

$$q + 1 - \sqrt{q} \leq |G| \leq q + 1 + \sqrt{q}$$

Для практического вычисления количества точек на кривой L в 1985 г. был предложен алгоритм Шуфа, который весьма сложен, но даёт существенный выигрыш в скорости для чисел больших $10^{100}$.

Найдём перебором количество точек на кривой (перебираем все конечные точки и добавляем одну бесконечную).

На языке Phyton:

```
def porjadok(a,b,p):
#находит перебором количество всех точек: все конечные точки кривой y^2=x^3+ax+b в поле GF(p) + одна бесконечная
  s=1  #всегда есть одна точка -бесконечная, E=O
  for x in range(p): #переберaем x от 0 до <p, то есть до p-1
     y2=(pow(x,3)+a*x+b)%p
     for y in range(0,p):
         if (pow(y,2)%p)==y2:
             s+=1
  return(s)
print(porjadok(a,b,p))

def porjadoktime(a,b,p):
#находит перебором количество всех точек: все конечные точки кривой y^2=x^3+ax+b в поле GF(p) + одна бесконечная
#эта версия команды дополнительно считает время выполнения команды
  now1 = datetime.datetime.now() #запоминаем время начала работы
  s=porjadok(a,b,p)
  now2 = datetime.datetime.now()
  delta = now2 - now1
  print("Порядок кривой y^2=x^3+",a," x + ",b," (mod ",p,") равен ",s,". Время выполнения ",delta," сек")
```

Замечание1. Вычисление с помощью online версии Phyton приводит к сбою через 1 минуту (стоит ограничение на время выполнения команды). Вычисление в локальной версии Phyton для p=19319 заняло 2 минуты 23 секунды.

Вычисление в локальной версии Wolfram Mathematica для p=19319 заняло 946 сек ≈ 16 минут.

Вычисление в локальной версии Julia для p=19319 заняло 184 сек ≈ 3 минуты.

Программа в Julia

```
using Nemo
p=19319
F=GF(p)
function porjadok(a,b,p)
        s=1
```

```
    for x in 0:(p-1)
      for y in 0:(p-1)
        y2= (F(x))^3+a*F(x)+b
        if y2 == (F(y))^2
          s=s+1
        end
      end
    end
    println("Порядок кривой y^2=x^3+$a x + $b (mod $p) равен $s")
end
```

@elapsed porjadok(1,0,19319) #команда вычисляет количество всех точек на эллиптической кривой, включая бесконечную, при этом замеряет затраченное на вычисления время в секундах.

Результат:

Порядок кривой y^2=x^3+1 x + 0 (mod 19319) равен 19320

184.270869199

То есть вычисления заняли 3 минуты и 4 сек.

Программа вычисления порядка кривой в Wolfram Mathematica:

```
{a, b, p} = {1, 0, 19319};
s = 1;
Timing[For[x = 0, x < p, x++,
  For[y = 0, y < p, y++,
   If[Mod[x^3 + a x + b - y^2, p] == 0, s += 1]]]]
```

Замечание2. Эксперимент проводился не в специально созданных условиях, поэтому нельзя считать результат абсолютно точным.

Замечание3. В примере 1 используется поле с q = p = 19319, значит, $\sqrt{q} = 138,99 \ldots$

$$19319 + 1 - 138,99 \ldots \leq |G| \leq 19319 + 1 + 138,99,$$
$$19320 - 138 \leq |G| \leq 19320 + 138$$
$$19182 \leq |G| \leq 19458$$

Фактически для a=1, b=0 получили |G|=19320, что удовлетворяет теореме Хассе.

Приложение 3 Нахождение порядка элемента

Определение. Порядком точки эллиптической кривой называется минимальное $k$ такое, что $kP = E$.

Если порядок элемента большой, то поиск порядка точки перебором всех кратных точек $kP$ является долгим и неэффективным.

Утверждение 1. Порядок элемента является делителем порядка группы. Если обозначить порядок группы $N$, то $NP = E$.

Утверждение 2. Если $kP = E$, где $k = p_1^{a_1} \cdot p_2^{a_2} \cdot \ldots \cdot p_m^{a_m}$– каноническое разложение $k$ на простые множители. Обозначим $k_i = \frac{k}{p_i}$. Если при этом $k_iP \neq E$ $\forall i = 1, \ldots, m$, то порядок точки $P$ равен $k$.