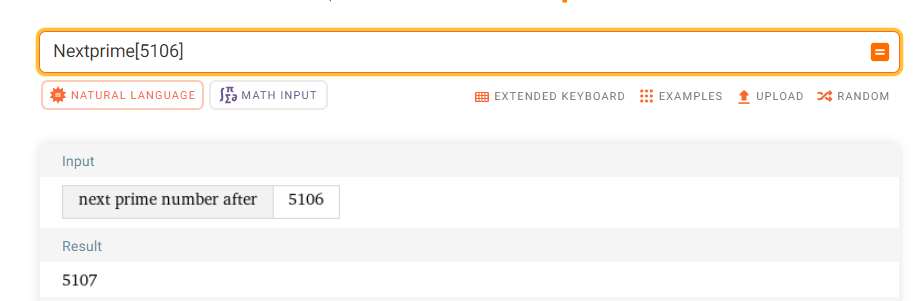
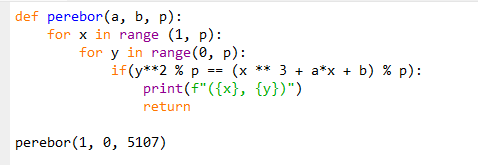
1. Инициалы ДИЕ, значит p = 5106. Найдём следующее за 5106 простое число.



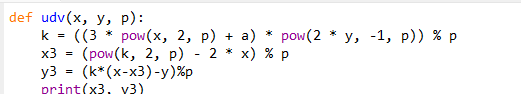
Значит, p=5107

1. Найдём одно решение уравнения 𝑦2 = 𝑥3 + 𝑎𝑥 + 𝑏 (𝑚𝑜𝑑 5107). Перебором находим точку P = (2, 773):





1. Найдём 151P = 128P + 16P + 4P + 2P + P. Используем удвоение точки:



2P= (1660, 138)

4P= (3483, 1845)

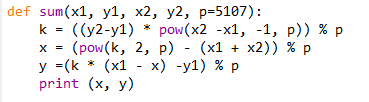
8P= (2091, 621)

16P= (14, 1760)

32P= (265, 2198)

64P= (3276, 3663)

128P= (2990, 924)



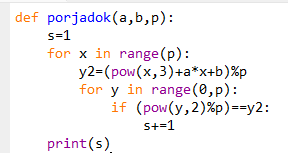
3P = 2P + P = (1660, 138) + (2, 773) = (3401, 3532)

7P = 4P + 3P = (3483, 1845) + (3401, 3532) = (4471, 1541)

23P = 16P + 7P = (14, 1760) + (4471, 1541) = (2991, 1629)

151P = 128P + 23P = (2990, 924) + (2991, 1629) = (772, 24)

1. Найдём порядок кривой с помощью перебора - 5108:



1. Разложим 5108 на множители. 5108 = 22 \* 1277

Простые делители 5108 равны 2 и 1277

|G|/2 = 2554, |G|/1277 = 4

Надо проверить только 2554P, т.к. 4P ≠ E

Для нахождения 2554P используем алгоритм быстрого умножения. Разложим 1277 на сумму степеней двойки:

1277P = 1024P + 128P + 64P + 32P + 16P + 8P + 4P + P

1024P = (5028, 2905)

5P = 4P + P = (3483, 1845) + (2, 773) = (3556, 3731)

13P = 8P + 5P = (2091, 621) + (3458, 33) = (2178, 4005)

29P = 16P + 13P = (14, 1760) + (2178, 4005) = (2597, 226)

61P = 32P +29P = (265, 2198) + (2597, 226) = (4170, 4284)

125P = 64P + 61P = (3276, 3663) + (4170, 4284) = (3299, 4290)

253P = 128P + 125P = (2990, 924) + (3299, 4290) = (2561, 4840)

1277P = 1024P + 253P = (5028, 2905) + (2561, 4840) = (5106, 2435)

Используем удвоение точки:

2 \* 1277P = 2554P = (0, 0)

2 ∙ (0,0) = E – бесконечно удалённая точка, значит, 5108P = E, т. е. |P| = 5108