# ЗАДАНИЕ 1

Проверить сингулярность данных эллиптических кривых и определить принадлежность точек этим кривым.

|  |  |
| --- | --- |
| Эллиптические кривые | Точки |
|  |  |

Несингулярность означает, что кривая не имеет точек возврата и самопересечения, в любой её точке можно провести касательную. Иначе кривая является сингулярной. В сингулярных кривых вычисление дискретного логарифма (основная проблема) является в общем смысле легко разрешимой задачей. Только несингулярные кривые обладают необходимыми характеристика для криптографической стойкости. И именно они используются на практике.

Условие проверки несингулярности в общем виде для кривой вида :

:

Несингулярная

:

Несингулярная

:

Несингулярная

Для проверки принадлежности точки кривой подставим её координаты в уравнение кривой.

: и

Левая часть:

Правая часть:

Левая часть не равна правой, значит точка не принадлежит кривой.

: и

Левая часть

Правая часть:

Левая часть равна правой, значит точка принадлежит кривой.

: и

Левая часть:

Правая часть:

Левая часть не равна правой, значит точка не принадлежит кривой/

: и

Левая часть:

Правая часть:

Левая часть равна правой, значит точка принадлежит кривой.

: и

Левая часть:

Правая часть:

Левая часть не равна правой, значит точка не принадлежит кривой.

: и

Левая часть:

Правая часть:

Левая часть не равна правой, значит точка не принадлежит кривой.

: и

Левая часть:

Правая часть:

Левая часть не равна правой, значит точка не принадлежит кривой.

: и

Левая часть:

Правая часть:

Левая часть не равна правой, значит точка не принадлежит кривой.

: и

Левая часть:

Правая часть:

Левая часть равна правой, значит точка принадлежит кривой.

: и

Левая часть:

Правая часть:

Левая часть не равна правой, значит точка не принадлежит кривой.

: и

Левая часть:

Правая часть:

Левая часть не равна правой, значит точка не принадлежит кривой.

: и

Левая часть:

Правая часть:

Левая часть не равна правой, значит точка не принадлежит кривой.

# ЗАДАНИЕ 2

Для данной эллиптической кривой и точке на ней найти:

|  |  |
| --- | --- |
| Входные данные | Скалярное произведение |
|  |  |

В эллиптических кривых определены следующие операции:

|  |  |
| --- | --- |
| Операция | Формула в поле характеристики , и |
| Обратная точка |  |
| Точка на бесконечности | - |
| Сложение точек |  |
| Удвоение точки |  |

Также определяется

Геометрический смысл этих операций заключается в том, что сумма точек — это третья точка пересечения проведённой через них прямой с кривой, а удвоение точки – это точка пересечения касательной, проведённой через эту точку с кривой.

Для нахождения представим в виде суммы степеней двойки.

Значит

Удвоим

Получим , удвоив .

Получили, что . Следовательно