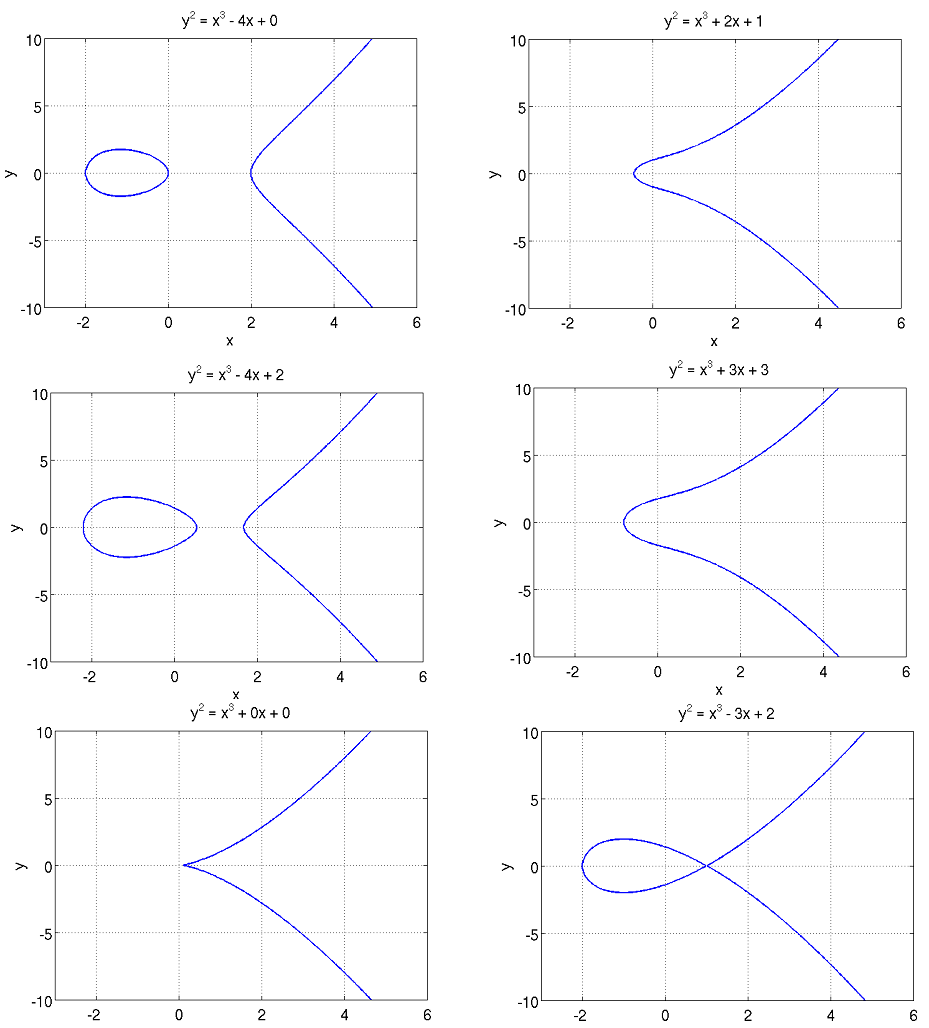
Факторизация целых чисел с помощью алгоритма Ленстры

*1 часть. Эллиптическая кривая и операции на ней.*

Эллиптическая кривая — это набор точек, описывающихся уравнением Вейерштрассе: https://habrastorage.org/r/w1560/getpro/habr/post_images/04d/94b/911/04d94b9114370a5c5fab166df84d765c.png

Примеры типичных ЭК:  


Эллиптическую кривую E называют сингулярной , если на кривой существует хотя бы одна особая точка (x;y), в которой одновременно ∂f/∂x=0 и ∂f/∂y=0. В противном случае кривая называется несингулярной. Такие кривые являются гладкими, т.е. не имеют точек возврата и самопересечений, в любой их точке можно провести касательную. Именно эти кривые и представляют интерес для криптографии.

Эллиптические кривые представленые на первых 4-х рисунках называются гладкими. В то время как две нижние кривые относятся к т.н. сингулярным эллиптическим кривым.

Над полем действительных чисел эллиптическая кривая задается уравнением y^2 = x^3 + ax + b. Так как y = +-sqrt(x^3 + ax + b), то график кривой симметричен относительно оси абсцисс. Точки его пересечения с этой осью – корни кубического уравнения x^3 + ax + b = 0.

Дискриминант этого уравнения . При этом:

♦ если D<0, то уравнение имеет три разных действительных корня α, β и γ. Типичный график – кривая 1 из двух частей;

♦ если D=0, то уравнение имеет действительные корни α, β, β, два из которых одинаковы. Типичный график – кривая 2. В этом случае точка (β;0) – особая, а кривая сингулярная;

♦ если D>0, то уравнение имеет один действительный корень α и два комплексных.

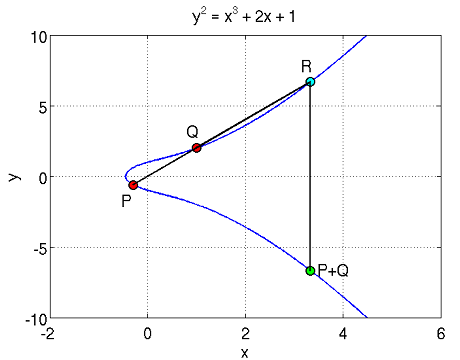
Таким образом, если характеристика поля не равна 2 и не равна 3, то кривая y^2 = x^3 + ax + b (mod p) будет несингулярной при условии что ее дискриминант не равен нулю. Отсюда вытекает следующее неравенство: https://habrastorage.org/r/w1560/getpro/habr/post_images/b69/234/f91/b69234f91932f51eeb83b726597d4c28.png.

**Поговорим об арифметических операциях на кривой.**

Арифметические операции в эллиптической криптографии производятся над точками кривой. Основной операцией является «сложение».

Cимметрия кривой относительно оси Ox дает наглядное определение обратной точки. А именно: обратной точкой для точки P(x;y) на эллиптической кривой называют точку -P(x;-y).

Замечательным свойством несингулярных кривых является то, что любая прямая, проходящая через две различные точки кривой пересекает кривую в единственной точке. Кроме того, касательная к эллиптической кривой в любой точке (кроме точек перегиба) пересекает ее еще в одной точке. Такие особенности позволяют задать групповую операцию, называемую сложением точек эллиптической кривой. Суммой двух точек P и Q называется точка R = P + Q, обратная третьей точке пересечения эллиптической кривой и прямой, проходящей через точки P и Q.

Сложение двух точек легко представить графически:  


Если суммируемые точки P и Q совпадают, то P + Q = P + P = R, что равносильно удвоению точки R=2P. При PQ= секущая PQ превращается в касательную к кривой и геометрически удвоенная точка 2P – это точка, обратная к точке пересечения этой касательной и эллиптической кривой.

Найдем координаты точки R = P + Q = (x3, y3), выразив их через координаты точек P = (x1, y1) и Q(x2, y2). При этом точки P и Q могут быть различными или совпадающими. В соответствии с этим имеем два случая:

1. P≠±Q. Запишем уравнение прямой PQ. Угловой коэффициент прямой PQ равен:   
   x3 = lamb^2 – x1 – x2,   
   y3 = lamb \* (x1 – x3) – y1;
2. При P = Q, R = 2P. Угловой коэффициент прямой равен: .   
   x3 = lamb^2 – 2x1,  
   y3 = lamb \* (x1 – x3) – y1;

Замечание: Формулы сложения и удвоения точек эллиптической кривой справедливы для всех полей, в том числе и конечных, кроме полей характеристик 2 и 3. В последнем случае приведение по модулю 2 или 3 приведет в этих формулах к 0^(-1)

Итак, чтобы построить группу E точек эллиптической кривой, выберем в качестве нейтрального элемента группы точку O(x; ∞), для которой положим:   
P + (-P) = O, ∀ P ∈ E.   
Прямая, проходящая через точки P и -P, перпендикулярна к оси абсцисс и поэтому можно принять, что третья точка пересечения перпендикуляра и кривой уходит в бесконечность вдоль оси ординат. Поэтому точку O называют точкой на бесконечности (бесконечно удаленной точкой) кривой.  
Согласно теореме Анри Пуанкаре множество точек эллиптической кривой вместе с введенной точкой на бесконечности образует коммутативную группу относительно операции сложения точек: для этого есть все необходимые свойства – замкнутость, коммутативность, ассоциативность, наличие обратного элемента и нейтральный элемент.  
**Следовательно, приходим к такому определению группы точек на ЭК:**  
Группой точек эллиптической кривой над конечным полем называется множество точек (x;y), координаты которых принадлежат полю и удовлетворяют уравнению: , если характеристика поля p ≠ 2;3 и a,b принадлежат полю, и . К группе точек эллиптической кривой также относится точка O(x; ∞).

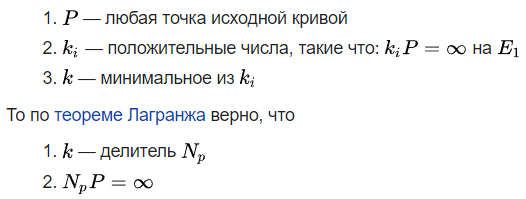
Из вышеизложенных операций сложения и удвоения точки, а так же из того, что множество точек образует группу на ЭК вытекает операция умножения точки на число **m в** группе точек. Умножение точки на число есть ни что иное как сложение точки самой с собой m раз.

Еще одно определение, которое понадобится нам для алгоритма Ленстры – это порядок точки. Порядок точки P – это наименьшее натуральное число n, при котором nP = O.

*2 часть. Алгоритм Ленстры факторизации числа на эллиптической кривой.*

**Обоснование и идея**(тут надо напрячься)

Уравнение https://habrastorage.org/r/w1560/getpro/habr/post_images/04d/94b/911/04d94b9114370a5c5fab166df84d765c.png�2=�3+��+�, взятое по модулю числа *n* задаёт эллиптическую кривую *�E*. Если числа *p* и *q* — два простых делителя числа *n*, то вышеупомянутое уравнение будет верно и при взятии по модулю *p* или по модулю *q*. То есть мы имеем две ЭК : ***E\_1 (mod p)*** и ***E\_2 (mod q)***, которые задают, соответственно, две эллиптические кривые (меньшие, чем ***E*** �). Однако ***E\_1*** �1и ***E\_2*** �2с заданной операцией сложения ⊞ — не только эллиптические кривые: они также являются группами. Пусть они содержат *Np* и *Nq* элементов, соответственно, тогда если:



Порядок группы точек, лежащих на эллиптической кривой ***E***  |�| над **Z***p*, согласно теореме Хассе ограничен:

.

Для случайно выбранной эллиптической кривой порядки *Np* и *Nq* являются случайными числами, ограниченными по теореме Хассе (см. ниже). Маловероятно, что большинство простых делителей *Np* и *Nq* совпадают, и вероятно, что при вычислении *eP* встретится некоторый ��=∞*k\*P = ∞* по модулю *р*, но не по модулю *q*, или наоборот. Если это так, то *kP* не существует на исходной кривой, а в вычислениях было найдено такое *v*, что либо НОД (*v*, *p*) = *p*, либо НОД (*v*, *q*) = *q*, но не одновременно. Тогда НОД (*v*, *n*) является нетривиальным делителем числа *n*.

≤|�|≤

**Вычислительная сложность**

Пусть наименьший делитель числа n равен p. Тогда количество выполняемых арифметических операций можно оценить величиной: .   
Если заменить *p* на �1/2n^(1/2), то получим субэкспоненциальную оценку сложности: ��[1/2;1]. Если сравнивать метод эллиптических кривых с другими методами факторизации, которые, в основном, имеют экспоненциальную сложность, то он является одним из самых быстрых. (Третьим после метода квадратичного решета(2 место) и метода решета числового поля(1 место)).

**Схема работы алгоритма**

1. Этап

* Выберем случайным образом числа x,y,a из диапазона [0, N-1], которые будут задавать нашу ЭК
* Вычислим оставшийся коэффициент b = y^2 – x^3 – a\*x (mod N) и g = GCD(N, 4\*a^3 + 27\*b^2). Если g = n, заново выбираем коэффициенты ЭК. Если 1 < g < N, тогда прекратим вычисление – делитель найден. Если же g = 1, определяем кривую найденными коэффициентами и базовую точку-генератор P\_0(x,y);
* Присвоим изменяемому параметру P(x,y) начальное значение равное P\_0;

1. Этап. Вычисление.

* Выберем число B, которое будет являться верхней границей для делителя числа N.
* Для каждого простого числа p < B найдем наибольшую степень r такую, что p^r < B.
* Выполним цикл for(i = 2; i < r; i++) P = p\*P. В результате которого точка P домножится на p^r.   
  При чем в цикле после каждой итерации необходимо проверять, определена ли точка Q = Q1 + Q2 на нашей ЭК. Если нет, то выходим из цикла до его завершения.
* Далее рассматриваем 3 случая:
  + Q1 (x1, y1) == Q2 (x2, y2)  
    Вычисляем d = (y1 + y2, N). Если при этом 1 < d < N, то найден нетривиальный делитель N. Алгоритм заканчивает свою работу. Если d == N, запускаем алгоритм заново.
  + Q1 (x1, y1) != Q2 (x2, y2) and x1 несравнимо с x2 (mod N)  
    Вычисляем d = (x1 - x2, N). Если при этом 1 < d < N, то найден нетривиальный делитель N. Алгоритм заканчивает свою работу. Если d == N, запускаем алгоритм заново.
  + Q1 (x1, y1) != Q2 (x2, y2) and y1 несравнимо с -y2 (mod N)  
    Вычисляем d = (y1 + y2, N). Если при этом 1 < d < N, то найден нетривиальный делитель N. Алгоритм заканчивает свою работу. Если d == N, запускаем алгоритм заново.

**Разбор алгоритма на примере.**

Факторизуем число N = 9.

* Выберем случайные значения x,y,a = 1,3,5 соответственно.
* Вычислим b = y^2 – x^3 – a\*x (mod N) и g = GCD(N, 4\*a^3 + 27\*b^2). b = 3, g = 1. Задаем базовую точку-генератор P\_0 = (1,3).
* Присвоим параметру P значение P\_0 = (1,3)
* Присвоим параметру B значение равное N/2 = 5
* Найдем все такие r для простых чисел p < B, что p^r < B.   
  В нашем случае это 3-1, 5-1, 7-1
* В цикле сложим точку Q = P саму с собой p^r раз.  
  Для 3^1 получаем максимум три итерации: Q = Q + P -> Q()

Еще одним важным понятием эллиптической криптографии является **порядок эллиптической кривой**, который показывает количество точек кривой над конечным полем.  
Теорема Хассе утверждает, что если N — количество точек кривой, определенной над полем Zq с q элементами тогда справедливо равенство:  
https://habrastorage.org/r/w1560/getpro/habr/post_images/f75/a87/ae8/f75a87ae841364889b7f2b4700e46784.png

https://habrastorage.org/r/w1560/getpro/habr/post_images/6eb/d2f/38d/6ebd2f38df6ad717b6f674e2d5a03182.png