1. **Дать определение эллиптической кривой.**

Определение 1. Эллиптические кривые – математический объект, который может быть определен над любым полем.

Определение 2. Эллиптическая кривая над вещественными числами – это множество точек, описываемых уравнением у2 = х3 + aх + b, при этом константы (а и b – вещественные числа) должны удовлетворять условию: 4a3+27b2 ≠ 0.

**2. Записать уравнение ЭК над вещественными числами (ЭК в криптографии, ЕСС).**

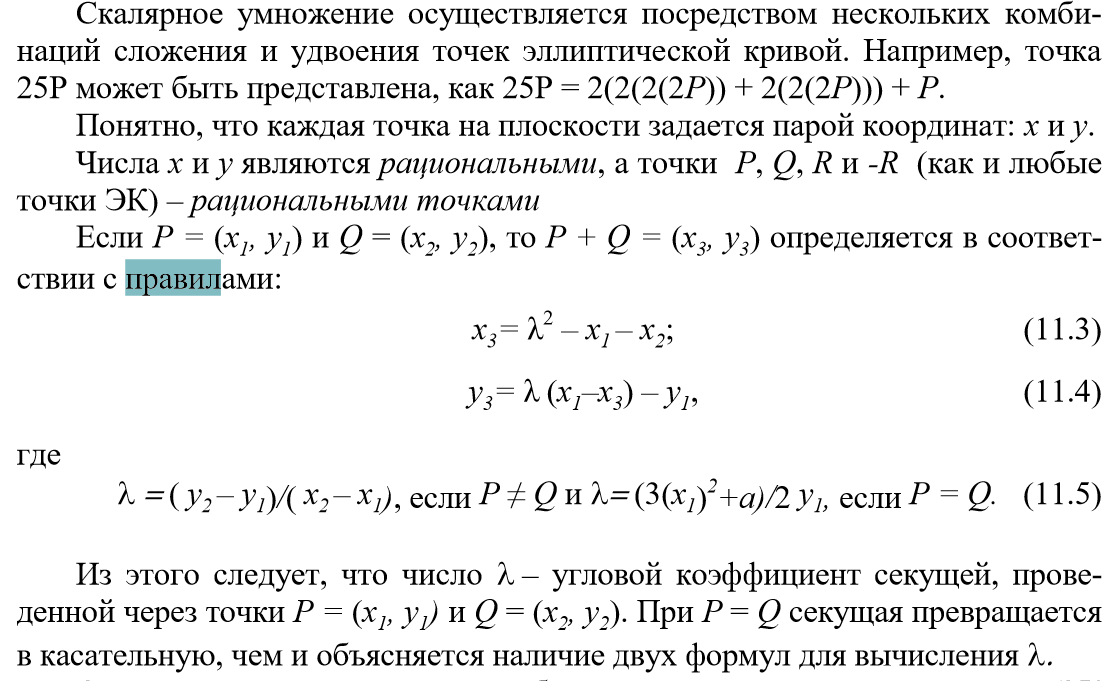
Эллиптическая кривая над вещественными числами – это множество точек, описываемых уравнением у2 = х3 + aх + b (11.1)

при этом константы (а и b – вещественные числа) должны удовлетворять условию: 4a3+27b2 ≠ 0. (11.2)

Формула (11.1) называется уравнением Вейерштрасса, а условие (11.2) исключает из рассмотрения кривые с особыми точками или особые кривые.

**3. Объяснить и показать на примере правила выполнения основных операций над точками ЭК.**

Cложение задается следующим правилом: сумма трех ненулевых точек P, Q и -R, лежащих на одной прямой, будет равна P + Q + (-R) = О.



**4. Что такое «рациональная точка»?**

Каждая точка на плоскости задается парой координат: х и у. Числа х и у являются рациональными, а точки P, Q, R и -R (как и любые точки ЭК) – рациональными точками.

**5. Как производится умножение точки ЭК?**

Скалярное умножение осуществляется посредством нескольких комбинаций сложения и удвоения точек эллиптической кривой. Например, точка 25P может быть представлена, как 25P = 2(2(2(2P)) + 2(2(2P))) + P.

**9. Есть ли отличия в применении операций над точками ЭК над конечными полями и над действительными числами?**

Эллиптическая кривая над полем Fp задается теми же уравнениями, что и ЭК над действительными числами, только все вычисления производятся по модулю р

у2 ≡ х3 + aх + b (mod p)

**13. На чем основа криптостойкость систем на основе ЭК? Области применения ЭК в криптографии.**

Криптостойкость алгоритмов на основе ЭК определяется, например, для алгоритма ЭЦП в стандарте РБ [50] параметром l, называемым уровнем стойкости и принимающим значения (рекомендуется) из {128, 192, 256}. При этом для взлома ключа злоумышленнику нужно выполнить операций.

* в алгоритмах согласования (передача) ключевой информации (на основе идеи Диффи-Хеллмана),
* в алгоритмах асимметричного шифрования/дешифрования сообщений,
* в алгоритмах генерации/верификации ЭЦП.

**14. Что такое «порядок точки» ЭК? Показать на примере. Какую роль этот параметр играет в криптографии на основе ЭК?**

Наименьшее значение числа q, для которого выполняется равенство qР = О, называется порядком точки Р.

Порядок точки Р связан с порядком m ЭК теоремой Лагранжа, согласно которой порядок подгруппы – это делитель порядка исходной группы. Иными словами, если ЭК содержит m точек, а одна из подгрупп содержит q, то q является делителем m.

**15. Что такое «базовая точка» ЭК? Какую роль этот параметр играет в криптографии на основе ЭК?**

Точка Р называется генератором или базовой точкой циклической подгруппы (такую точку во многих документах обозначают символом G).

В криптографии на основе ЭК тайный ключ – это случайное целое d, выбранное из множества {1, 2, ..., q–1}, где q – порядок подгруппы; открытый ключ – это точка Q, такая, что Q = dG, где G – **базовая** точка подгруппы.

**16. Объяснить порядок формирования ключевой информации на основе ЭК.**

Первый этап. Выбор (генерация) ЭК. Обычно он основан на выполнении следующих условий и операций.

1.1. Входными параметрами являются: число l, число р, удовлетворяющее условию 22l-1 < р < 22l, р = 3 mod 4, 0 < a < p. Можно использовать некоторое простое число р = 22l – с, где с – небольшое натуральное число.

1.2. Выбирается число b, такое, что 0 < b < p. Таким образом, задана ЭК: Ер(а, b).

1.3. Выбираются порядок q (простое число) и генерирующая точка G, которая задается двумя координатами, например, G = (0, уG). Дополнительно к рассмотренным действиям стандарт предусматривает использование вспомогательного параметра (s, seed) – произвольное 64битное число.

Второй этап. Генерация ключевой информации.

2.1. Входными параметрами являются: *р, а, b, q и G*.

2.2. Генерируется тайный ключ – число d, выбранное из множества *{1, 2, …, q–1*}.

2.3. Вычисляется открытый ключ – точка Q: Q = dG

к открытому ключу также относятся р, а, b, q.

17. Сгенерировать ключевую информацию на основе кривой Е11 (1, 2).