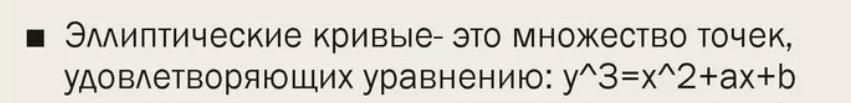
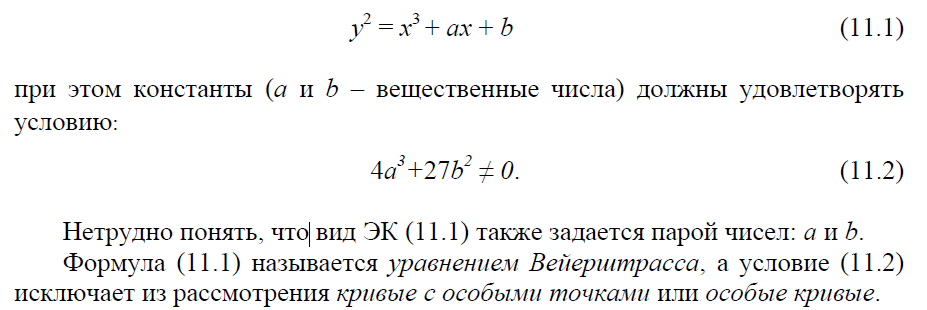
1. **Дать определение эллиптической кривой.**

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

*Эллиптическая кривая* над вещественными числами – это множество точек, описываемых уравнением

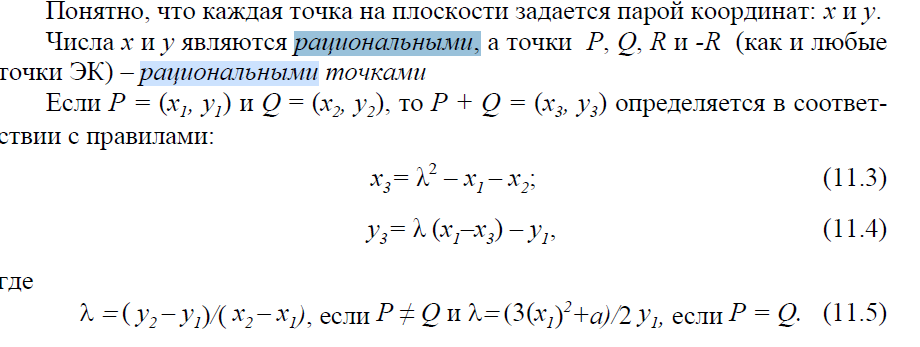


1. **Записать уравнение ЭК над вещественными числами (ЭК в криптографии, ЕСС).**

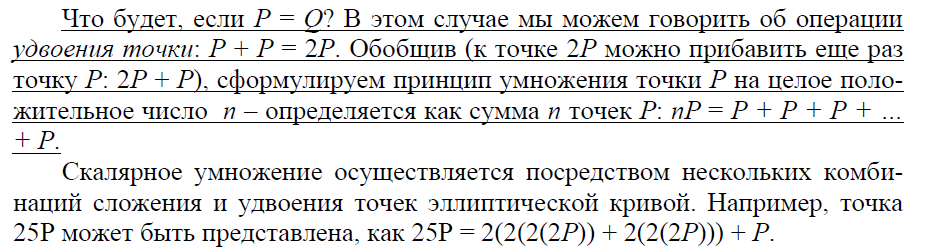


**3. Объяснить и показать на примере правила выполнения основных опе-раций над точками ЭК.**

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



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



**6. Как производится умножение точки *Р* на число *k*, если *k* принимает значение: 2, 5, 11, 20, 32, 100, 256, 751, 1024?**

**7. Составить алгоритм многократного сложения точки ЭК (умножения точки на число) на основе примера 7.**

**8. Привести расчеты для точки Q при известных d и G из примера 7.**

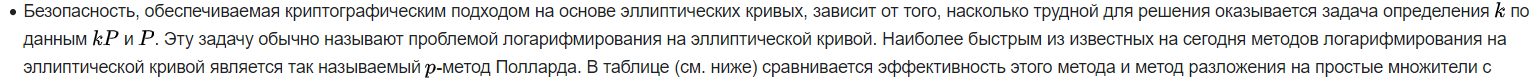
**9. Есть ли отличия в применении операций над точками ЭК над конеч-ными полями и над действительными числами?**

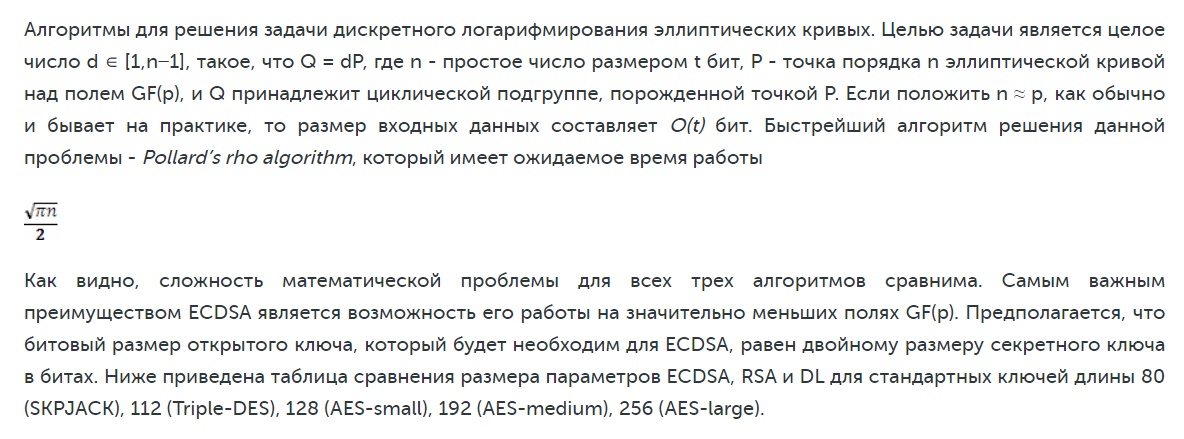
**10. Записать уравнение ЭК при формальном ее представлении в следую-щем виде: Ер(а, b).**

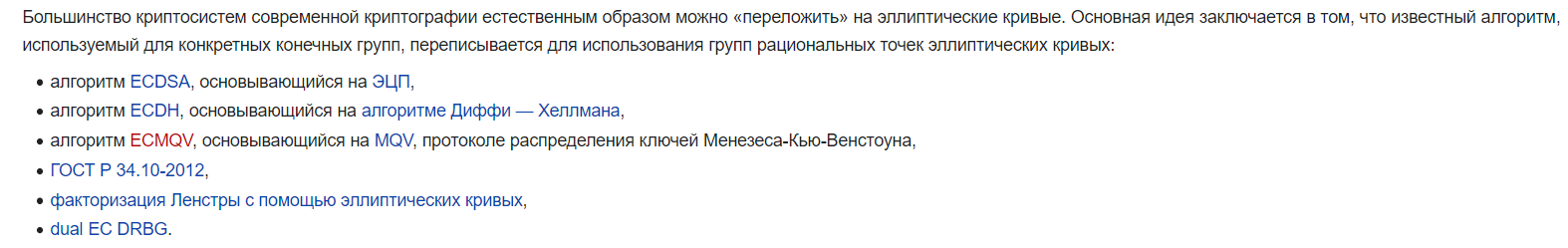
**11. Из какого числа точек состоит ЭК Е11(6, –9)? Дать их координаты.**

**12. Найти все точки ЭК Е11 (1, 2).**

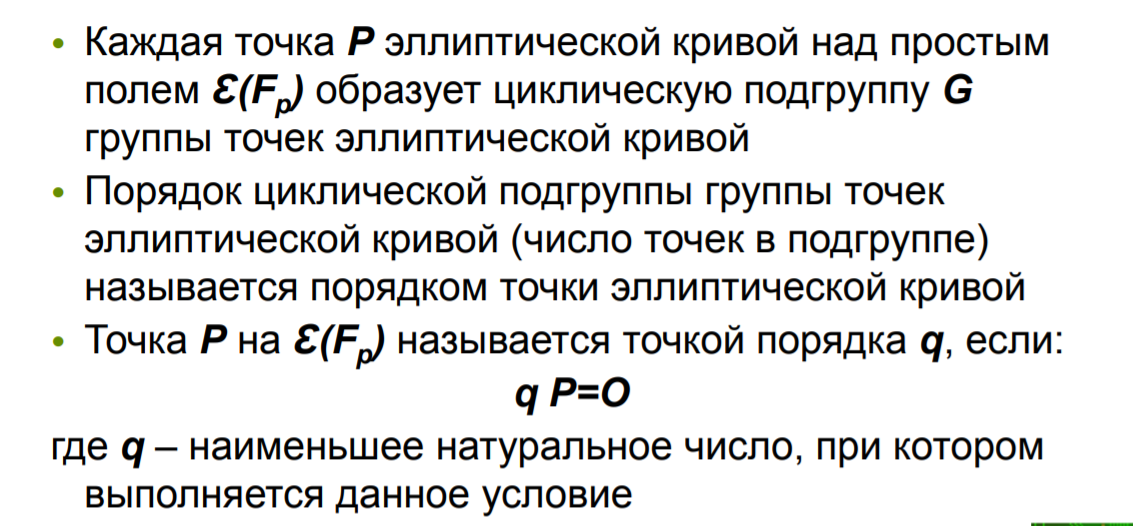
**13. На чем основа криптостойкость систем на основе ЭК? Области при-менения ЭК в криптографии.**

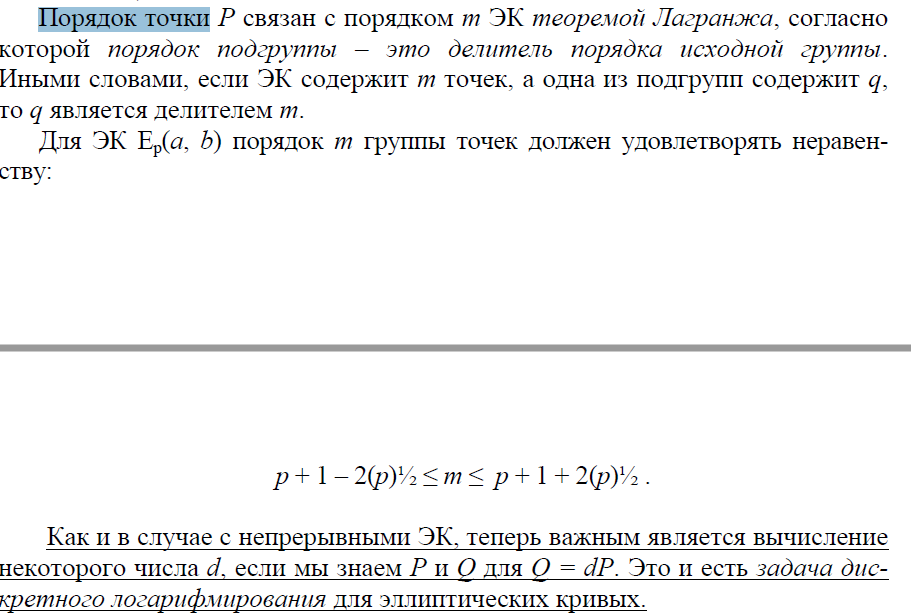


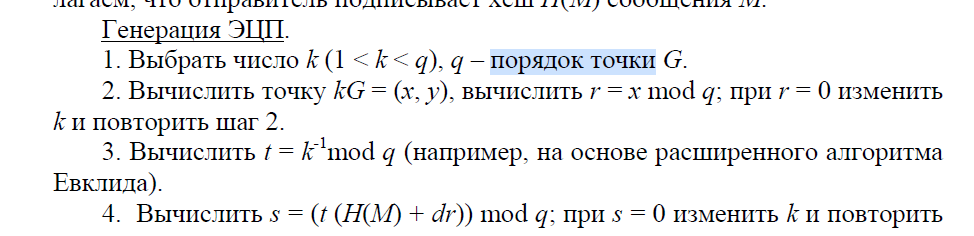




**14. Что такое «порядок точки» ЭК? Показать на примере. Какую роль этот параметр играет в криптографии на основе ЭК?**

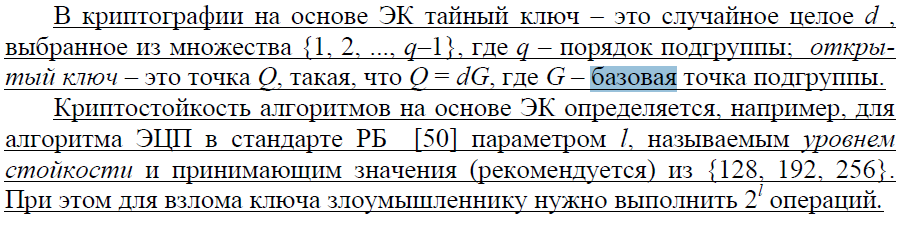




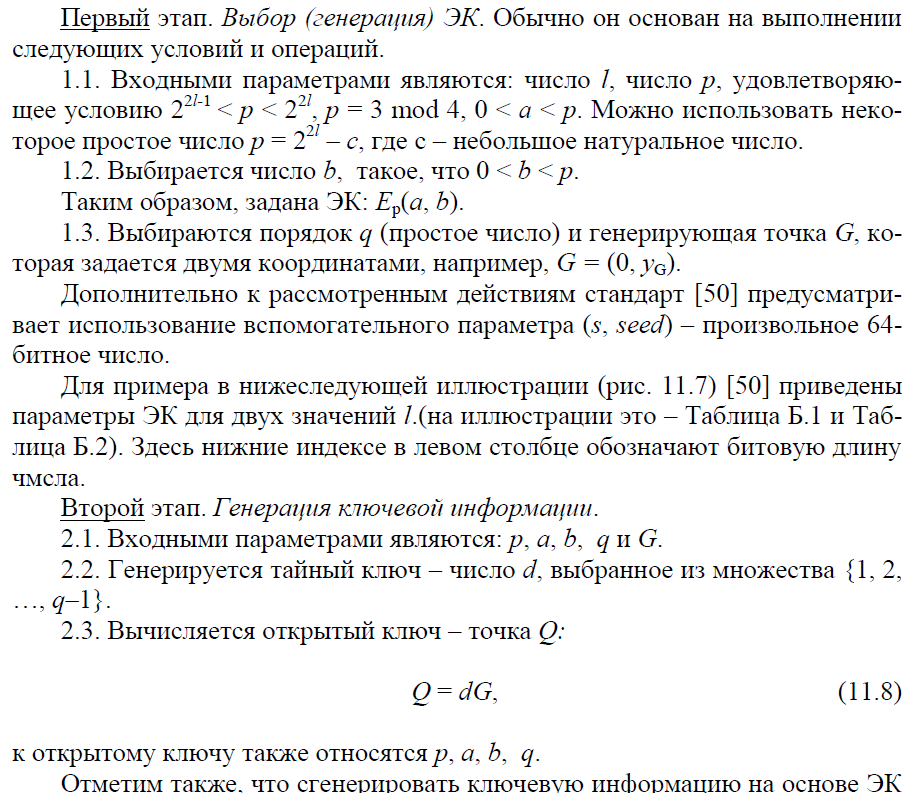


**15. Что такое «базовая точка» ЭК? Какую роль этот параметр играет в криптографии на основе ЭК?**

Точка *P* поля(а,б) называется базовой точкой группы точек эллиптической кривой *E*p(*a*,*b*), если любая точка *Q*  *E*p(*a*,*b*) может быть представлена в виде *Q* = k *P* , где k = 1, 2,…, #*E*p(*a*,*b*) .



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



**17. Сгенерировать ключевую информацию на основе кривой *Е*11 (1, 2).**

