

## Эллиптические кривые в криптографии

### Обязательные задачи

Осенний семестр 2011/2012 учебного года

- (1) Найдите все порождающие элементы в группе  $\mathbb{F}_{37}^*$ .
- (2) Сколько решений имеет уравнение  $x^n - 1 = 0$  в поле  $\mathbb{F}_{16}$  для  $n = 2, 12, 10$ ?
- (3) Найдите все неприводимые многочлены степени 4 над  $\mathbb{F}_3$ .
- (4) Сколько существует неприводимых многочленов степени 6 над  $\mathbb{F}_4$ ?
- (5) При каком  $a$  кривая, заданная уравнением  $x^3 + y^3 + z^3 + axyz = 0$  в  $\mathbb{P}^2$ , приводима?
- (6) При каком  $a$  кривая, заданная уравнением  $x^3 + y^3 + z^3 + axyz = 0$  в  $\mathbb{P}^2$ , особа?
- (7) Найдите все особые точки кривой, заданной уравнением  $y^4 - xz^3 - 4xyz^2 - 2xy^2z + x^2z^2 = 0$  в  $\mathbb{P}^2$ .
- (8) Найдите координаты всех точек перегиба кубической кривой Ферма  $x^3 + y^3 + z^3 = 0$ .
- (9) Найдите точки перегиба кривой  $x^2y + y^2z + z^2x = 0$  (характеристика – произвольная).
- (10) Найдите координаты всех точек перегиба кубической кривой  $x^3 + y^3 + z^3 + axyz = 0$ .
- (11) Найдите нормальную форму Вейерштрасса кубической кривой Ферма  $x^3 + y^3 + z^3 = 0$ .
- (12) Вычислите  $j$ -инвариант кривой Ферма  $x^3 + y^3 + z^3 = 0$ .
- (13) Постройте эллиптическую кривую с  $j$ -инвариантом  $j = 7$ .
- (14) Выбрав в качестве нейтрального элемента точку  $(0 : 1 : 0)$ , на кривой  $y^2 + y = x^3 - x$  найти  $nP$  для  $P = (0, 0)$  и любого  $n$ .
- (15) Найдите все точки порядка 2 на кривой  $y^2 = x^3 + x$ .
- (16) Найдите все точки порядка 3 на кривой  $y^2 - x^3 + 2 = 0$  над полем  $\mathbb{F}_{47}$ .
- (17) Выписать явные формулы для группового закона на эллиптической кривой  $y^2 + y = x^3$  над полем характеристики 2 (в качестве нейтрального элемента возьмите бесконечную точку).
- (18) Сколько существует точек порядка 3 на эллиптической кривой  $y^2 + y = x^3$  над полем  $\mathbb{F}_q$  для  $q = 2, 4, 5, 7, 8$ ?
- (19) Воспользуйтесь групповым законом и постройте семейство рациональных решений уравнения  $y^2 = x^3 + x - 1$ .
- (20) Найдите порядок точки  $P = (0, 4)$  на эллиптической кривой  $y^2 = x^3 + 16$ .
- (21) Найдите порядок точки  $P = (0, 1)$  на эллиптической кривой  $y^2 = x^3 + x + 1$  над полем  $\mathbb{F}_3$ .
- (22) Найдите порядок точки  $P = (2, 3)$  на эллиптической кривой  $y^2 = x^3 + 1$  над полем  $\mathbb{F}_5$ .
- (23) Опишите точки порядка 3 на эллиптической кривой  $y^2 = x^3 + cx^2 + ax + b$  над полем характеристики 3.
- (24) Как можно выразить  $\wp''$  через  $\wp$ ?
- (25) Сколько имеется точек порядка  $n$  на эллиптической кривой над  $\mathbb{C}$ ?
- (26) Найдите порядок точки  $P = (2, 1)$  на эллиптической кривой  $y^2 = x^3 + x + 1$  над полем характеристики 5.
- (27) Найдите порядок точки  $P = (2, 1)$  на эллиптической кривой  $y^2 = x^3 + x$  над полем характеристики 3.

- (28) Найдите порядок точки  $P = (2, 2)$  на эллиптической кривой  $y^2 = x^3 + 1$  над полем характеристики 5.
- (29) Существует ли на проективной плоскости конечное множество точек, удовлетворяющих следующему условию: прямая, проходящая через две из них проходит еще ровно через одну из них?
- (30) Найдите все  $\mathbb{F}_4$ -точки эллиптической кривой  $y^2 + y = x^3$ .
- (31) Найдите порядок точки  $P = (0, 1)$  на эллиптической кривой  $y^2 + y = x^3$  над полем характеристики 2.
- (32) Найдите все  $\mathbb{F}_4$ -точки эллиптической кривой  $y^2 + xy = x^3 + 1$ .
- (33) Найдите порядок точки  $P = (1, 0)$  на эллиптической кривой  $y^2 + xy = x^3 + 1$  над полем характеристики 2.
- (34) Найдите порядок точки  $P = (5, 2)$  на эллиптической кривой  $y^2 = x^3 + x$  над полем характеристики 7.
- (35) Найдите все точки порядка 2 на эллиптической кривой  $y^2 = x^3 + x$  над полем характеристики 5.
- (36) Найдите все точки порядка 4 на эллиптической кривой  $y^2 = x^3 + x$  над полем характеристики 3.
- (37) Пусть решетка  $\Lambda$  порождается элементами 1 и  $i$ . Найдите группу автоморфизмов эллиптической кривой  $\mathbb{C}/\Lambda$ . Ответ обоснуйте.
- (38) Пусть решетка  $\Lambda$  порождается элементами 1 и  $(-1 + i\sqrt{3})/2$ . Найдите группу автоморфизмов эллиптической кривой  $\mathbb{C}/\Lambda$ . Ответ обоснуйте.
- (39) Пусть  $X \subset \mathbb{A}^2$  – неприводимая кривая, заданная уравнением  $f_{d-1}(x, y) + f_d(x, y) = 0$ , где  $f_{d-1}$  и  $f_d$  – многочлены степеней  $d - 1$  и  $d$  соответственно. Докажите, что  $X$  рациональна. Выпишите рациональную параметризацию.
- (40) Докажите, что если многочлен  $x^3 + ax + b$  имеет кратный корень, то кривая, заданная в  $\mathbb{A}^2$  уравнением  $y^2 = x^3 + ax + b$  рациональна. Выпишите рациональную параметризацию.
- (41) Докажите, что кривая  $y^3 = x^4 - 4x^3 + 6x^2 - 4x + 3y^2 - 3y + 2$  рациональна. Выпишите рациональную параметризацию.