Эллиптические кривые: формулы полезные и не очень

Задача 1°. Пусть кривая E задана уравнением Вейерштрасса:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

Введем обозначения:

$$b_2 = a_1^2 + 4a_2, \quad b_4 = 2a_4 + a_1a_3, \quad b_6 = a_3^2 + 4a_6,$$
$$b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2;$$
$$c_4 = b_2^2 - 24b_4, \quad c_6 = -b_2^3 + 36b_2b_4 - 216b_6;$$
$$\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6, \quad j = \frac{c_4^3}{\Delta}.$$

a) Покажите, что линейной заменой переменных над полем k характеристики $\neq 2$ уравнение приводится к виду $y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6$, а над полем характеристики $\neq 2, 3$ к виду $y^2 = x^3 - 27c_4x - 54c_6$.

b) Докажите, что над полем характеристики 2 уравнение можно привести к виду $y^2 + xy = x^3 + a_2x^2 + a_6$, если $j \neq 0$ и к виду $y^2 + a_3y = x^3 + a_4x + a_6$, если $j = 0$.

c) Докажите, что над полем характеристики 3 уравнение можно привести к виду $y^2 = x^3 + a_2x^2 + a_6$, если $j \neq 0$ и к виду $y^2 = x^3 + a_4x + a_6$, если $j = 0$.

d) Покажите, что для кривой вида $y^2 = x^3 + ax + b$ формулы для Δ и j упрощаются и принимают вид: $\Delta = -16 \cdot (4a^3 + 27b^2)$, $j = -1728 \cdot (4a)^3/\Delta$.

e) Убедитесь, что единственные замены переменных, переводящие в уравнение Вейерштрасса (гладкой) эллиптической кривой в уравнение Вейерштраса, имеют следующий вид: $x = u^2x' + r$, $y = u^3y' + u^2sx' + t$.

f) Выведите формулы для преобразования коэффициентов:

$$ua_1' = a_1 + 2s, \quad u^2a_2' = a_2 - sa_1 + 3r - s^2,$$
$$u^3a_3' = a_3 + ra_1 + 2t, \quad u^4a_4' = a_4 - sa_3 + 2ra_2 - (t + rs)a_1 + 3r^2 - 2st,$$
$$u^6a_6' = a_6 + ra_4 + r^2a_2 + r^3 - ta_3 - t^2 - rta_1;$$
$$u^2b_2' = b_2 + 12r, \quad u^4b_4' = b_4 + rb_2 + 6r^2,$$
$$u^6b_6' = b_6 + 2rb_4 + r^2b_2 + 4r^3, \quad u^8b_8' = b_8 + 3rb_6 + 3r^2b_4 + r^3b_2 + 3r^4;$$
$$u^4c_4' = c_4, \quad u^6c_6' = c_6, \quad u^{12}\Delta' = \Delta, \quad j' = j.$$

g) Покажите, что, если уравнения обеих кривых имеют вид $y^2 = x^3 + ax + b$, то формулы замены переменных принимают совсем простую форму: $x = u^2x'$, $y = u^3y'$ и при этом $u^4a' = a$, $u^6b' = b$.

h) Докажите, что кривая E гладкая в том и только том случае, когда $\Delta \neq 0$.

i) Если $\Delta = 0$, то кривая имеет узел (“node”, особая точка с различными касательными) при $c_4 \neq 0$ и точку возврата (“cusp”, особая точка с совпадающими касательными) иначе.

j) Покажите, что эллиптические кривые E и E' изоморфны над $\bar{k}$ тогда и только тогда, когда $j(E) = j(E')$.

k) Убедитесь, что для $j_0 \neq 0, 1728$ кривая

$$y^2 + xy = x^3 - \frac{36}{j_0 - 1728}x - \frac{1}{j_0 - 1728}$$

имеет j-инвариант, равный j_0. Покажите, что j-инварианты кривых $y^2+y=x^3$ и $y^2=x^3+x$ равны 0 и 1728 соответственно.

l) Пусть $P_i=(x_i,y_i)$, $P_3=P_1+P_2$. Выведите следующие формулы для сложения точек на эллиптической кривой:

$$-P_0=(x_0,-y_0-a_1x_0-a_3),$$
$$\lambda=\frac{y_2-y_1}{x_2-x_1},\quad \nu=\frac{y_1x_2-y_2x_1}{x_2-x_1}\quad \text{при } x_1\neq x_2,$$
$$\lambda=\frac{3x_1^2+2a_2x_1+a_4-a_1y_1}{2y_1+a_1x_1+a_3},\quad \nu=\frac{-x_1^3+a_4x_1+2a_6-a_3y_1}{2y_1+a_1x_1+a_3}\quad \text{при } x_1=x_2,$$
$$x_3=\lambda^2+a_1\lambda-a_2-x_1-x_2,\quad y_3=-(\lambda+a_1)x_3-\nu-a_3.$$

m) Убедитесь, что

$$\omega=\frac{dx}{2y+a_1x+a_3}=\frac{dy}{3x^2+2a_2x+a_4-a_1y}$$

является голоморфным дифференциалом на эллиптической кривой, не обращающимся в ноль.

Задача 2° (уравнение кривой в форме Лежандра). Пусть $\operatorname{char} k\neq 2$.

a) Покажите, что любая эллиптическая кривая E/k изоморфна над $\bar{k}$ эллиптической кривой в форме Лежандра $E_\lambda\colon y^2=x(x-1)(x-\lambda)$, $\lambda\in\bar{k},\lambda\neq 0,1$.

b) Покажите, что $j(E_\lambda)=2^8\cdot\frac{(\lambda^2-\lambda+1)^3}{\lambda^2(\lambda-1)^2}$.

c) Убедитесь, что отображение $\bar{k}\setminus\{0,1\}\to\bar{k}$, $\lambda\mapsto j(E_\lambda)$ имеет 6 прообразов во всех точках, кроме $j=0$ и $j=1728$. Сколько прообразов оно имеет в исключительных точках?

Задача 3° (уравнение кривой в форме Дойринга).

a) Пусть E/k — эллиптическая кривая и, либо $\operatorname{char} k\neq 3$, либо $j(E)\neq 0$. Покажите, что над $\bar{k}$ кривая E имеет уравнение Вейерштрасса вида $y^2+\alpha xy+y=x^3$, $\alpha\in\bar{k}$.

b) Убедитесь, что $\Delta(E)=\alpha^3-27$ и $j(E)=\frac{\alpha^3(\alpha^3-24)^3}{\alpha^3-27}$.