Uvod u aritmetiku eliptičkih krivulja

Opća Weiestrassova jednadžba

Kubika nad poljem k u projektivnim koordinatama u Weiestrassovoj formi dana je sa

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3 \tag{1}$$

gdje su $a_1, \ldots, a_6$ iz polja k. Ako želimo odrediti nove točke na krivulji, u jednadžbu (1) stavimo $Z = 0$ i dobivamo $X = 0$, a odatle $Y \neq 0$. Stoga možemo staviti $Y = 1$ i dobivamo točku $O(0, 1, 0)$. To je beskonačno daleka točka. Možemo zamišljati da beskonačno daleki pravac $Z = 0$ siječe krivulju u jednoj točki, tj. O. Taj pravac je tangenta, a O je trostruka točka, tj. točka infleksije ili fleks. Primjenom supstitucije

$$x = \frac{X}{Z},\ y = \frac{Y}{Z}$$

dobivamo pripadnu afinu jednadžbu

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{2}$$

Prednost ove forme je jednostavniji zapis.

Primjer 1 *Afina jednadžba $y^2 = x^3 + 1$ uz zamjenu $x = \frac{X}{Z}$, $y = \frac{Y}{Z}$ prelazi u pripadnu projektivnu jednadžbu $ZY^2 = X^3 + Z^3$.*

$\diamondsuit$

Primjer 2 *Pogledajmo projektivnu jednadžbu $X^3 + Y^3 = Z^3$. Uvedimo supstituciju $\dfrac{X}{Z} = \dfrac{3x}{y}$, $\dfrac{Y}{Z} = \dfrac{y-9}{y}$. Rješavanjem toga sustava dobivamo*

$$x = \frac{3X}{Z - Y},\ y = \frac{9Z}{Z - Y}.$$

Uz to polazna jednadžba postaje afina jednadžba $y^2 - 9y = x^3 - 27$.

$\diamondsuit$

Postavljanjem uvjeta na karakteristiku polja k jednadžbu (2) možemo transformirati u jednostavniji oblik. Neka je *char* $k \neq 2$. Sada je

$$\begin{aligned} y^2 + a_1xy + a_3y &= \left(y + \frac{1}{2}(a_1x + a_3)\right)^2 - \frac{1}{4}(a_1x + a_3)^2 = x^3 + a_2x^2 + a_4x + a_6, \\ \left(y + \frac{1}{2}(a_1x + a_3)\right)^2 &= \frac{1}{4}(a_1x + a_3)^2 + x^3 + a_2x^2 + a_4x + a_6. \end{aligned}$$

Sada uvedimo zamjenu $\frac{1}{2}y = y + \frac{1}{2}(a_1x + a_3)$.
Dobivamo

$$\begin{aligned} \frac{1}{4}y^2 &= \frac{1}{4}(a_1^2x^2 + 2a_1a_3x + a_3^2) + x^3 + a_2x^2 + a_4x + a_6, \\ y^2 &= 4x^3 + (a_1^2 + 4a_2)x^2 + 2(a_1a_3 + 2a_4)x + a_3^2 + 4a_6. \end{aligned}$$

Označimo

$$\begin{aligned} b_2 &= a_1^2 + 4a_2 \\ b_4 &= 2a_4 + a_1a_3 \\ b_6 &= a_3^2 + 4a_6. \end{aligned}$$

Dobivamo jednadžbu

$$y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6. \tag{3}$$

Naka je sada *char* $k \neq 3$. U (3) napravimo zamjenu $x = \dfrac{x - 3b_2}{36}$, $y = \dfrac{y}{108}$. Dobivamo

$$\left(\frac{y}{108}\right)^2 = 4\left(\frac{x - 3b_2}{36}\right)^3 + b_2\left(\frac{x - 3b_2}{36}\right)^2 + 2b_4\frac{x - 3b_2}{36} + b_6.$$

Potenciranjem i množenjem zajedničkim nazivnikom dobivamo

$$\begin{aligned} y^2 &= x^3 + (648b_4 - 27b_2^2)x + 11664b_6 - 1944b_2b_4 + 54b_2^3, \\ y^2 &= x^3 - 27(b_2^2 - 24b_4)x - 54(-b_2^3 + 36b_2b_4 - 216b_6). \end{aligned}$$

Označimo

$$\begin{aligned} c_4 &= b_2^2 - 24b_4 \\ c_6 &= -b_2^3 + 36b_2b_4 - 216b_6. \end{aligned}$$

Rezultat je još jednostavnija jednadžba

$$y^2 = x^3 - 27c_4x - 54c_6. \tag{4}$$

Primjer 3 *Afinu jednadžbu* $y^2 - 9y = x^3 - 27$ *iz* primjera 2 *transformirajmo u oblik* (4).

$$\begin{aligned} b_2 &= a_1^2 + 4a_2 = 0 + 0 = 0, \\ b_4 &= 2a_4 + a_1a_3 = 0 + 0 = 0, \\ b_6 &= a_3^2 + 4a_6 = (-9)^2 + 4(-27) = -27, \\ c_4 &= b_2^2 - 24b_4 = 0 \\ c_6 &= -b_2^3 + 36b_2b_4 - 216b_6 = 0 + 0 - 216(-27) = 5832. \end{aligned}$$

Slijedi

$$\begin{aligned} y^2 &= x^3 - 27c_4x - 54c_6 \\ &= x^3 - 54 \cdot 5832 \\ &= x^3 - 314928 \\ &= x^3 - 2^4 3^9. \end{aligned}$$

$\diamondsuit$

Označimo $b_8 = a_1^2 a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2$.

Definicija 1 *Diskrininanta Δ krivulje* (2) *dana je formulom*

$$\Delta = -b_2^2 b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6.$$

Lako se provjeri da je $1728\Delta = c_4^3 - c_6^2$. Zanima nas što se događa sa singularnošću krivulje, ako ju promotrimo nad $\mathbb{Q}$, modulo neki prost broj p. U tu svrhu cilj nam je dokazati sljedeći teorem:

Teorem 1 *Kubika* (2) *je singularna ako i samo ako je* $\Delta = 0$.

U svrhu dokaza teorema 1, promotrimo neka svojstva diskriminante polinoma trećeg stupnja. Neka je

$$\begin{aligned} f(x) &= x^3 - \alpha x^2 + \beta x - \gamma \\ &= (x - r_1)(x - r_2)(x - r_3) \end{aligned}$$

normirani polinom trećeg stupnja s korijenima r_1, r_2, r_3 nad poljem k. Ovdje su

$$\alpha = r_1 + r_2 + r_3, \quad \beta = r_1r_2 + r_1r_3 + r_2r_3, \quad \gamma = r_1r_2r_3.$$

Izračunajmo Vandermondeovu determinantu $V(r_1, r_2, r_3)$. Vrijedi

$$det \begin{pmatrix} 1 & 1 & 1 \\ r_1 & r_2 & r_3 \\ r_1^2 & r_2^2 & r_3^2 \end{pmatrix} = (r_3 - r_1)(r_3 - r_2)(r_1 - r_2) \tag{5}$$

Sada je

$$\begin{pmatrix} 1 & 1 & 1 \\ r_1 & r_2 & r_3 \\ r_1^2 & r_2^2 & r_3^2 \end{pmatrix} \begin{pmatrix} 1 & r_1 & r_1^2 \\ 1 & r_2 & r_2^2 \\ 1 & r_3 & r_3^2 \end{pmatrix} = \begin{pmatrix} 3 & \sigma_1 & \sigma_2 \\ \sigma_1 & \sigma_2 & \sigma_3 \\ \sigma_2 & \sigma_3 & \sigma_4 \end{pmatrix} \tag{6}$$

gdje je $\sigma_i = r_1^i + r_2^i + r_3^i$, $i = 1, 2, 3, 4$.

Diskriminanta d polinoma $f(x)$ jednaka je $d = (r_1 - r_2)^2(r_1 - r_3)^2(r_2 - r_3)^2$. Sada možemo dokazati sljedeće:

Propozicija 1 *Diskriminanta d polinoma $f(x)$ jednaka je* $d = det \begin{pmatrix} 3 & \sigma_1 & \sigma_2 \\ \sigma_1 & \sigma_2 & \sigma_3 \\ \sigma_2 & \sigma_3 & \sigma_4 \end{pmatrix}$,

gdje je

$$\begin{aligned} \sigma_1 &= \alpha, \\ \sigma_2 &= \alpha^2 - 2\beta, \\ \sigma_3 &= \alpha^3 - 3\alpha\beta + 3\gamma, \\ \sigma_4 &= \alpha^4 - 4\alpha^2\beta + 2\beta^2 + 4\alpha\gamma. \end{aligned}$$

Dokaz:
Dokaz direktno slijedi iz formula (5) i (6) i prethodne definicije.

$\square$

Primjer 4 *Neka je $f(x) = x^3 - 6x^2 + 11x - 6$. Prethodnim algoritmom odredimo diskriminantu polinoma $f(x)$.*

Uočimo da su korijeni polinoma $f(x)$ jednaki $r_1 = 1, r_2 = 2, r_3 = 3$. Tada je

$$\begin{aligned} f(x) &= (x-1)(x-2)(x-3), \\ \alpha &= r_1 + r_2 + r_3 = 1 + 2 + 3 = 6, \\ \beta &= r_1r_2 + r_1r_3 + r_2r_3 = 1 \cdot 2 + 1 \cdot 3 + 2 \cdot 3 = 11, \\ \gamma &= r_1r_2r_3 = 1 \cdot 2 \cdot 3 = 6. \end{aligned}$$

Stoga je

$$\begin{aligned} \sigma_1 &= \alpha = 6, \\ \sigma_2 &= \alpha^2 - 2\beta = 14, \\ \sigma_3 &= \alpha^3 - 3\alpha\beta + 3\gamma = 36, \\ \sigma_4 &= \alpha^4 - 4\alpha^2\beta + 2\beta^2 + 4\alpha\gamma = 98. \end{aligned}$$

Konačno

$$d = det \begin{pmatrix} 3 & \sigma_1 & \sigma_2 \\ \sigma_1 & \sigma_2 & \sigma_3 \\ \sigma_2 & \sigma_3 & \sigma_4 \end{pmatrix} = det \begin{pmatrix} 3 & 6 & 14 \\ 6 & 14 & 36 \\ 14 & 36 & 98 \end{pmatrix} = 4.$$

$\diamondsuit$

Diskriminanta polinoma $g(x) = x^3 + px + q$ jednaka je $d = -4p^3 - 27q^2$. (To slijedi iz prethodne propozicije za $\alpha = 0, \beta = p, \gamma = -q$). Iz prethodnog razmatranja također zaključujemo da je diskriminanta kubičnog polinoma jednaka nuli ako i samo ako taj polinom ima barem dva jednaka korijena. Važnost diskriminante u ispitivanju singularnosti kubike sadržana je u sljedećoj propoziciji:

Propozicija 2 *Neka je k polje, char $k \neq 2$, $C \in k$, $C \neq 0$. Krivulja*

$$y^2 = C(x^3 - \alpha x^2 + \beta x - \gamma)$$

je nesingularna ako i samo ako polinom $f(x) = C(x^3 - \alpha x^2 + \beta x - \gamma)$ ima različite korijene u k.

U svrhu dokaza navedimo poznatu činjenicu:
Neka je F krivulja nad poljem k. Ako točka (X_0, Y_0, Z_0) leži na krivulji, onda je ona nesingularna točka ako i samo ako je barem jedna od parcijalnih dreivacija $\frac{\partial F}{\partial X}, \frac{\partial F}{\partial Y}, \frac{\partial F}{\partial Z}$ u točki (X_0, Y_0, Z_0) različita od 0.
Dokaz:
Pokazali smo da singularnosti ne može biti u beskonačnoj točki i na beskonačnom pravcu. Također znamo, ako je $F(X, Y, Z) = 0$ jednadžba krivulje u projektivnoj ravnini, pripadna jednadžba u afinoj ravnini je $f(x, y) = 0$, gdje je $f(x, y) = F(x, y, 1)$. Stoga je prirodno promotriti točku $(x_0, y_0, 1)$. Stavimo $F(X, Y, Z) = ZY^2 - C(X^3 - \alpha ZX^2 + \beta Z^2 X - \gamma Z^3)$. Krivulja je singularna ako na njoj postoji točka $P = (x_0, y_0, 1)$ takva da je zadovoljeno

$$\frac{\partial F}{\partial X}(P) = 0 \quad \Leftrightarrow \quad 3x_0^2 - 2\alpha x_0 + \beta = 0, \tag{7}$$

$$\frac{\partial F}{\partial Y}(P) = 0 \quad \Leftrightarrow \quad 2y_0 = 0, \tag{8}$$

$$\frac{\partial F}{\partial Z}(P) = 0 \quad \Leftrightarrow \quad y_0^2 = C(-\alpha x_0^2 + 2\beta x_0 - 3\gamma). \tag{9}$$

Odatle slijedi $0 = y_0 = f(x_0) = f'(x_0)$. Primjenom (9) dobivamo

$$\begin{aligned}
0 = 3f(x_0) - x_0 f'(x_0) &= 3C(x^3 - \alpha x^2 + \beta x - \gamma) - Cx_0(3x_0^2 - 2\alpha x_0 + \beta) \\
&= 3Cx_0^3 - 3C\alpha x_0^2 + 3C\beta x_0 - 3C\gamma - 3Cx_0^3 + 2C\alpha x_0^2 - Cx_0\beta \\
&= -C\alpha x_0^2 + 2Cx_0\beta - 3C\gamma \\
&= C(-\alpha x_0^2 + 2x_0\beta - 3\gamma)
\end{aligned}$$

Zaključujemo da treća jednadžba ne daje ništa novo, pa je ona na neki način višak. Stoga je jedini kandidat za singularnu točku nad k točka $(x_0, 0, 1)$, gdje je x_0 korijen of f. Ta točka je singularna ako i samo ako je x_0 višestruki korijen od f.

□

Propozicija 3 *Neka je char $k \neq 2$, d_b diskriminanta polinoma s desne strane u (3), d_c diskriminanta polinoma s desne strane u (4). Tada je*

$$\begin{aligned}
d_c &= 2^{12} 3^{12} d_b, \\
\Delta &= 2^4 d_b.
\end{aligned}$$

Dokaz: Pogledajmo najprije za $char\, k \neq 3$. Važno je uočiti da ako u kubičnom polinomu x zamijenimo s $\frac{x}{C}$, onda je diskriminanta novoga polinoma jednaka C^6 puta diskriminanta polaznoga polinoma (to je zato jer se svaki korijen množi sa C). Takvu zamjenu koristili smo tijekom transformacije (3) u (4) uz $C = 36 = 2^2 3^2$. To sada daje

$$d_c = C^6 d_b = 2^{12} 3^{12} d_b$$

a to je upravo ono što trebamo. Sada je

$$\begin{aligned} d_c &= -4(-27c_4)^3 - 27(54c_6)^2 = (c_4^3 - c_6^2)2^2 3^9 = 1728\, 2^2\, 3^9 \Delta, \text{ tj.} \\ 2^{12} 3^{12} d_b &= 1728\, 2^2 3^9 \Delta = 2^6 3^3 2^2 3^9 \Delta, \text{ tj.} \\ \Delta &= 2^4 d_b. \end{aligned}$$

Dokažimo sada tvrdnje za slučaj $char\, k = 3$. $d_c = -4(-27c_4)^3 - 27(54c_6)^2 = 0$ (jer je 3 nula u karakteristici 3), pa vrijedi prva tvrdnja. Diskriminanta d_b jednaka je diskriminanti polinoma $y^2 = C(x^3 - \alpha x^2 + \beta x - \gamma)$ iz propozicije 2, za

$$C = 1,\ \alpha = -\frac{b_2}{4},\ \beta = \frac{b_4}{2},\ \gamma = -\frac{b_6}{4}.$$

Sada iskoristimo propoziciju 1 koja nam daje

$$d = det \begin{pmatrix} 3 & \sigma_1 & \sigma_2 \\ \sigma_1 & \sigma_2 & \sigma_3 \\ \sigma_2 & \sigma_3 & \sigma_4 \end{pmatrix}$$

gdje je

$$\begin{aligned} \sigma_1 &= \alpha, \\ \sigma_2 &= \alpha^2 - 2\beta, = \alpha^2 + \beta \\ \sigma_3 &= \alpha^3 - 3\alpha\beta + 3\gamma = \alpha^3, \\ \sigma_4 &= \alpha^4 - 4\alpha^2\beta + 2\beta^2 + 4\alpha\gamma = \alpha^4 - \alpha^2\beta - \beta^2 + \alpha\gamma, \end{aligned}$$

uz

$$\alpha = -b_2,\ \ \beta = -b_4,\ \ \gamma = -b_6.$$

Računanjem determinante gornje matrice (uz uvjet $3 = 0$) dobivamo

$$\begin{aligned} d_b &= 2\sigma_1\sigma_2\sigma_3 - \sigma_2^3 - \sigma_1^2\sigma_4 = -\sigma_1\sigma_2\sigma_3 - \sigma_2^3 - \sigma_1^2\sigma_4, \text{ tj.} \\ d_b &= -\beta^3 - \alpha^2\beta^2 - \alpha^3\gamma = b_4^3 + b_2^2 b_4^2 - b_2^3 b_6. \end{aligned}$$

Računom se lako provjeri da je $4b_8 = b_2 b_6 - b_4^2$ u bilo kojoj karakteristici. Sada je po definiciji

$$\begin{aligned} \Delta &= -b_2^2 b_8 - 8b_4^3 - 27b_6^2 + 9b_2 b_4 b_6. \\ &= -b_2^2 b_8 + b_4^3 = -b_2^2(b_2 b_6 - b_4^2) + b_4^3 = -b_2^3 b_6 + b_2^2 b_4^2 + b_4^3 \end{aligned}$$

jer je $4b_8 = b_8$ u karakteristici 3. Sada je direktno zadovoljeno $\Delta = 2^4 d_b$, jer je $2^4 = 16 = 1 + 15 = 1$ u karakteristici 3. Time je tvrdnja propozicije u potpunosti dokazana.

□

Dokaz teorema 1:
Neka je $char\, k \neq 2$. Tada je (2) singularna ako i samo ako je (3) singularna, a to je ako i samo ako desna strana u (3) ima višestruke korijene (prema propoziciji 2), tj. ako i samo ako je $d_b = 0$. To prema prethodnoj propoziciji vrijedi ako i samo ako je $\Delta = 0$.
Neka je sada $char\, k = 2$. Tada je

$$\begin{aligned}\Delta &= -b_2^2 b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6 = b_2^2b_8 + b_6^2 + b_2b_4b_6 \\ &= a_1^6a_6 + a_1^5a_3a_4 + a_1^4a_2a_3^2 + a_1^4a_4^2 + a_3^4 + a_1^3a_3^3.\end{aligned}$$

Sada nastupamo analogno kao u dokazu propozicije 2. Iz (1) slijedi $F(X,Y,Z) = Y^2Z + a_1XYZ + a_3YZ^3 - (X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3)$. Krivulja je singularna ako na njoj postoji točka $P = (x_0, y_0, 1)$ takva da je zadovoljeno

$$\frac{\partial F}{\partial X}(P) = 0 \quad \Leftrightarrow \quad a_1y_0 + x_0^2 + a_4 = 0, \tag{10}$$

$$\frac{\partial F}{\partial Y}(P) = 0 \quad \Leftrightarrow \quad a_1x_0 + a_3 = 0, \tag{11}$$

$$\frac{\partial F}{\partial Z}(P) = 0 \quad \Leftrightarrow \quad y_0^2 + a_1x_0y_0 + a_2x_0^2 + a_6 = 0. \tag{12}$$

Treba pokazati da je $\Delta = 0$. Pretpostavimo da je $a_1 = 0$. Tada je $\Delta = 0$ ako i samo ako je $a_3 = 0$, a to je ako i samo ako je zadovoljeno (11). Uočimo da je $x_0(10)+y_0(11)$+krivulja = (12). Stoga, da bi u ovom slučaju pokazali singularnost, dovoljno je provjeriti ima li sustav

$$\begin{aligned}0 &= x_0^2 + a_4 \\ y_0^2 &= x_0^3 + a_2x_0^2 + a_4x_0 + a_6.\end{aligned}$$

rješenja u $\overline{k}$. Ali mi sigurno možemo izabrati $x_0 \in \overline{k}$ tako da vrijedi prva jednadžba. Nakon toga taj x_0 uvrstimo u drugu jednadžbu i odaberemo $y_0 \in \overline{k}$ tako da i ona bude istinita. Time je taj slučaj riješen.
Pretpostavimo da je sada $a_1 \neq 0$. Sada iz (11) slijedi $x_0 = a_1^{-1}a_3$. To uvrstimo u (10) i dobivamo $y_0 = a_1^{-3}a_3^2 + a_1^{-1}a_4$. Sada to uvrstimo u (2), tj. jednadžbu krivulje i dobivamo

$$(a_1^{-6}a_3^4 + a_1^{-2}a_4^2) + (a_1^{-3}a_3^3 + a_1^{-1}a_3a_4) + (a_1^{-3}a_3^3 + a_1^{-1}a_3a_4) + a_1^{-3}a_3^3 + a_1^{-2}a_2a_3^2 + a_1^{-1}a_3a_4 + a_6 = 0, \text{ tj.}$$

$$a_1^{-6}a_3^4 + a_1^{-3}a_3^3 + a_1^{-2}a_4^2 + a_1^{-2}a_2a_3^2 + a_1^{-1}a_3a_4 + a_6 = 0 \tag{13}$$

Sada je bitno uočiti da je upravo (13) jednako $a_1^{-6}\Delta$. Stoga je $(x_0, y_0, 1)$ singularna točka ako i samo ako je $\Delta = 0$. Time smo dokazali tvrdnju teorema.

□

Primjer 5 *Ilustrirajmo prethodni teorem na krivuljama iz prethodnih primjera.*

Imamo sljedeće

$$
\begin{aligned}
E_1 &: \; y^2 - 9y = x^3 - 27 \\
E_2 &: \; y^2 = x^3 - 2^4 3^9.
\end{aligned}
$$

Tada je $\Delta_{E_1} = -3^9$ i $\Delta_{E_2} = 2^{12}3^9$. Slijêdeći prethodni teorem zaključujemo da je E_1 singularna modulo 3, a E_2 singularna modulo 2 i modulo 3.

$\diamondsuit$