Uvod u aritmetiku eliptičkih krivulja

1. Uvod i motivacija - 1. lekcija

Začetci ideje o eliptičkim krivuljama mogu se nazrijeti kod Diofanta (vjerojatno u 3. stoljeću) u postupku rješavanja jednadžba u racionalnim brojevima (diofantskih jednadžba). Nakon stoljeća zaborava Bachet je u 17. stoljeću ponovno otkrio slične postupke, a Newton ih geometrijski interpretirao. Preko Fermata (17. st.), Poincarea (19.-20. st.), Mordella, Weila, Serra i drugih, razvoj te ideje doveo je koncem 20. stolječa do rješenja Fermatova teorema (Wiles). Uz taj, aritmetički aspekt eliptičkih krivulja, postoji i onaj geometrijski i analitički, koji se kroz razvoj pojma eliptičkih integrala i eliptičkih funkcija može pratiti od 17. st. (Wallis, Newton), preko 18. st. (J.Bernoulli, MacLaurin, Fagnano, Euler), 19. st. (Legendre, Gauss, Abel, Jacobi, Riemann, Weierstrass, Klein, Poincare), do današnjih dana.

Integrali racionalnih funkcija

Racionalna funkcija je funkcija F koja se može zapisati kao kvocijent dvaju polinoma, dakle

$$F = \frac{g}{h}$$

gdje su f, g polinomi (koeficijenti mogu biti u bilo kojem polju, ali, u ovom kontekstu smatramo da su to realni brojevi; takodjer, racionalne funkcije mogu biti u jednoj, dvjema ili u više varijabla). Poznato je da se

$$\int \frac{g(x)}{h(x)} dx \tag{1}$$

može uvijek izraziti u terminima elementarnih funkcija. Na primjer,
$\int \frac{dx}{1+x^2} = arctg(x) + C$ i $\frac{dx}{x} = \ln x + C$, za $x > 0$.

Integrali oblika $\int R(x, \sqrt{ax^2 + bx + c})dx$

Po složenosti, nakon integrala racionalnih funkcija, dolaze integrali koji se mogu zapisati pomoću x i $\sqrt{ax + b}$, za neke realne brojeve a, b. Oni se, nakon jednostavne zamjene varijabla, svode na integrale racionalnih fukcija. Nešto su složeniji integrali koji se mogu zapisati u obliku

$$\int R(x, \sqrt{ax^2 + bx + c})dx \tag{2}$$

gdje je R racionalna funkcija u dvjema varijablama, primjerice $\int \frac{x+1}{2+\sqrt{3x^2-4x+5}}dx$. I ti se integrali mogu **racionalizirati**, tj. prikladnom zamjenom varijabla svesti na integrale racionalnih funkcija (tu je bitno da se racionalizacija može provesti pomoću racionalnih funkcija). Jedna od metoda su **Eulerove supstitucije**, koje se na dijele na one:
(I) vrste, za $a > 0$,
(II) vrste, za $D > 0$, gdje je D diskriminanta polinoma $f(x) := ax^2 + bx + c$, i
(III) vrste, ako je $c > 0$.

Na primjer, za (III) vrstu zamjena je: $\sqrt{ax^2 + bx + c} = tx + \sqrt{c}$, odakle se dobije $x = \frac{2\sqrt{c}t-b}{a-t^2}$ i $dx = \frac{2\sqrt{c}t^2-2bt+2a\sqrt{c}}{(a-t^2)^2}dt$ (tu se vidi da je x racionalna funkcija od t).

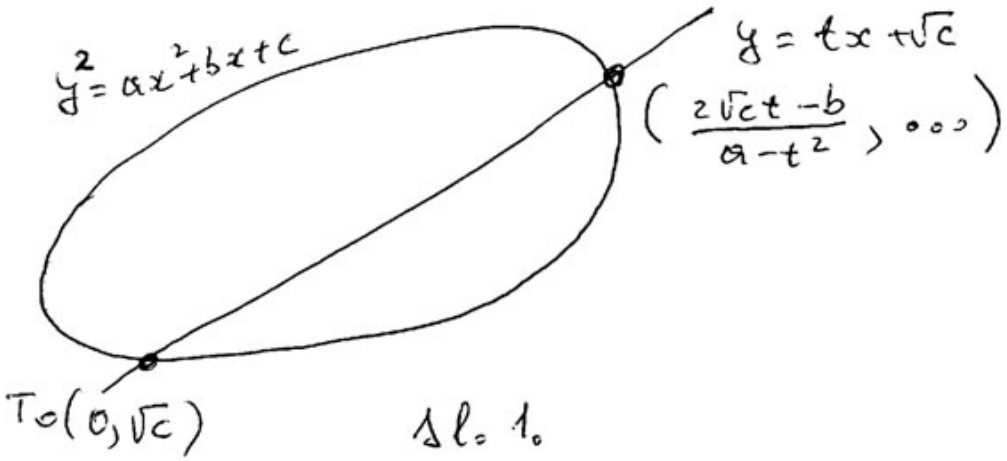
Pokazuje se da se te supstitucije temelje na geometrijskim svojstvima krivulje

$$y^2 = ax^2 + bx + c \tag{3}$$

koja se prirodno pojavljuje uz ovakav integral, odnosno na činjenici da je to krivulja 2. reda - **konika** (tu zanemarujemo trivijalni slučaj, kad je $D = 0$). Naime, uvjet $c > 0$ osigurava postojanje točke s realnim koordinatama $T_0(0, \sqrt{c})$ na krivulji, a

$$y = tx + \sqrt{c} \tag{4}$$

za $t \in \mathbf{R}$ je jednadžba pramena pravaca kroz T_0 (osim jednog pravca). Kako je krivulja konika, svaki od tih pravaca (osim tangente) presijeca krivulju u još jednoj točki T, koja nužno ima realne koordinate, čime se uspostavlja bijekcija izmedju točaka konike i realnih parametara t (osim jednog izuzetka); kažemo da smo **parametrizirali** koniku. Lako se vidi da je prva koordinata točke T upravo $x = \frac{2\sqrt{c}t-b}{a-t^2}$ kao u (III) Eulerovoj supstituciji, a za $y \geq 0$ je $y = \sqrt{ax^2 + bx + c}$, pa (4) postaje zamjena $\sqrt{ax^2 + bx + c} = tx + \sqrt{c}$ (sl.1.).



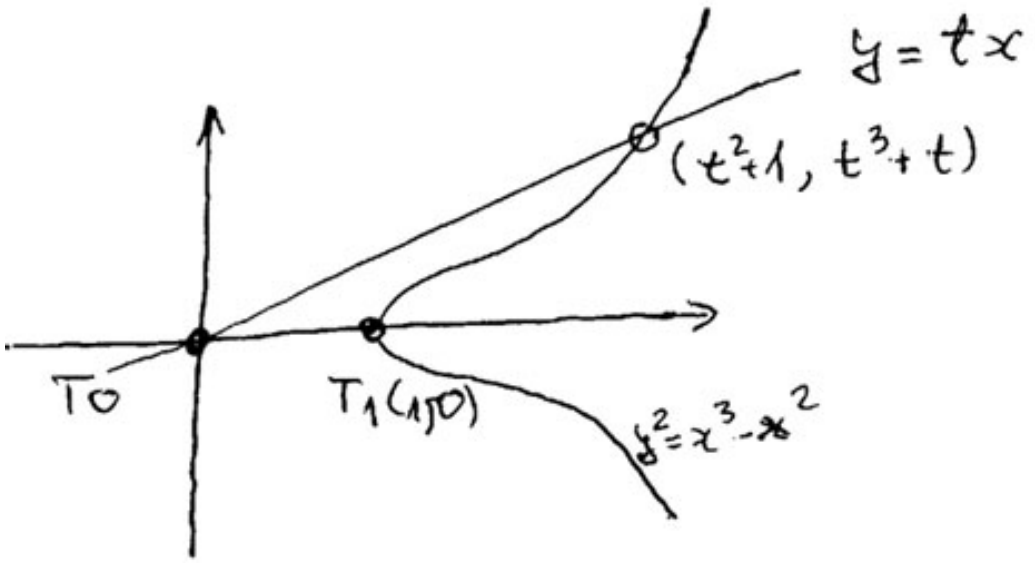
Uočite da su tu x i y racionalne funkcije od t; takodjer (inverzna transformacija) t je racionalna funkcija od x i y.

Eliptički integrali

Situacija se bitno usložnjava za integrale oblika $\int R(x, \sqrt{f(x)}dx$ gdje je f polinom 3. stupnja: $f(x) := ax^3 + bx^2 + cx + d$, te a, b, c, d realni brojevi i $a \neq 0$.

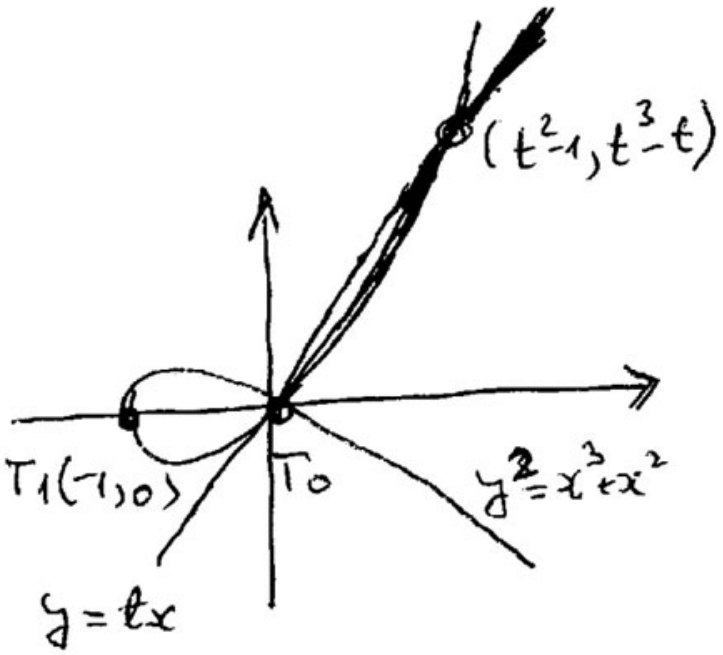
Napomena 1. Polinom f može se zamjenom $X := \sqrt[3]{a}x$ svesti na oblik $f(X) = X^3 - 3AX^2 + BX + C = (X - A)^3 - (3A^2 - B)X + (C + A^3)$, a ovaj, dalje, zamjenom $X - A := u$, na oblik $f(u) = u^3 + pu + q$, za realne p, q. Imajući to na pameti, obično ćemo kubni polinom pisati u obliku $f(x) = x^3 + ax + b$.
Neki integrali s $\sqrt{x^3 + ax + b}$ su poput onih iz (2).

Primjer 1. (a) $\int \frac{dx}{\sqrt{x^3 - x^2}}$ racionalizirat ćemo tako da pogledamo pripadnu krivulju $y^2 = x^3 - x^2$ (sl.2) i uočimo izoliranu točku $T_0(0.0)$.



Sl. 2

Vidimo da pravci $y = tx$ kroz T_0 parametriziraju tu krivulju, uvrštavanjem u jednadžbu krivulje i kraćenjem dobije se $x = t^2 + 1$ pa se integral racionalizira: $\int \frac{2t}{t(t^2+1}dt$. Uočite da analogon postupak s pravcima kroz točku $T_1(1, 0)$ ne bi urodio plodom (za razliku od integrala (2) gdje nije bitan izbor točke). (b) Uz $\int \frac{dx}{\sqrt{x^3+x^2}}$, prirodno ide krivulja $y^2 = x^3 + x^2$, kojoj se odmah uočavaju dvije točke: $T_0(0, 0)$ i $T_1(-1, 0)$. Kao i u a), parametrizacija pravcima kroz T_0 uspijeva, a kroz T_1 ne uspijeva (sl. 3.).



Sl. 3.

Ono što je uspjelo s integralima iz Primjera 1, nikako nije uspijevalo matematičarima 18. st. općenito s integralima poput

$$\int \frac{dx}{\sqrt{x^3 + ax + b}} \tag{5}$$

Slično je bilo i s integralima $\int \frac{dx}{\sqrt{f(x)}}$ za polinome f četvrtog stupnja, na primjer $\int \frac{dx}{\sqrt{x^4-1}}$. Takvi integrali i integrali (5), uz uvjet da podintegralni polinomi nemaju višestrukih korijena, primjeri su **eliptičkih integrala**. Koncem 18. st. shvatilo se da se takvi integrali ne mogu riješiti u terminima elementarnih funkcija (puno objašnjenje tek je od sredine 19. st.). Uspjeh u Primjeru 1 omogućen je upravo činjenicom što su podintegralni polinomi višestruke korijene, a točka kroz koju se provlače pravci bila ona koja odgovara tim dvostrukim korijenima. Na jeziku krivulja to je bila **singularna točka**. O tome čemo više govoriti poslije.

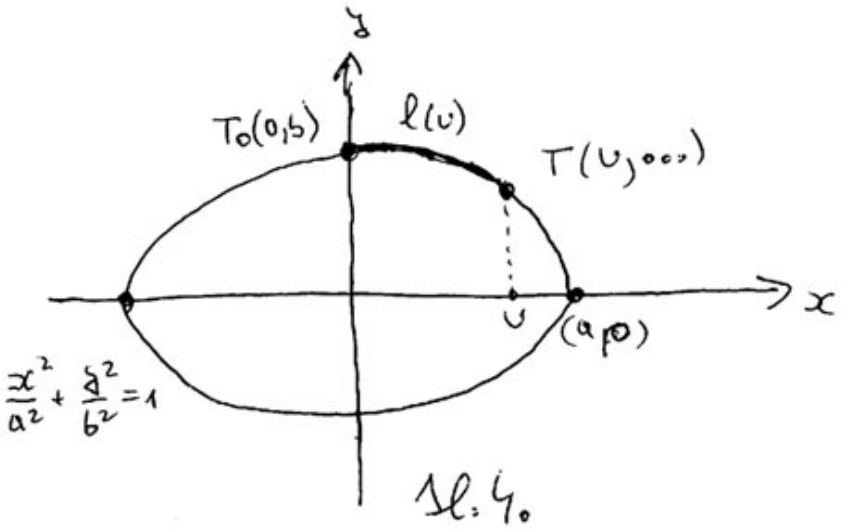
Naziv Eliptički integral

Taj naziv nastaje od *elipse*, zato što se pojavljuje u problemu odredjivanja duljine luka elipse. Problem odredjivanja opsega elipse još je iz starogrčkih vremena, a naročito je postao aktualan nakon Keplerovih zakona (početkom 17. st.). Za razliku od formule za površinu unutar elipse $P = \pi ab$ koja je prirodno poopćenje formule za površinu kruga $P = \pi r^2 = \pi r \cdot r$, a ostvaruje se zamjenom jednog r u a, a drugog u b, tako se nešto ne dogadja s opsegom: izraz $2\pi r$ tj. $\pi(r + r)$ pri analognom postupku prelazi u $\pi(a + b)$, što je uvijek, osim za $a = b = r$ manje od opsega elipse. U 17. st. uočeno je da je odredjivanje formule za opseg elipse problem integralnog računa i prva rješenja (u obliku beskonačnog reda) dali su Wallis, Newton i, poslije njih, MacLaurin. Red s vrlo brzom konvergencijom čekao je 19. st. Takav je Gauss-Kummerov red:

$$O = \pi(a + b) \sum_{n \geq 0} [\binom{\frac{1}{2}}{n}^2 h^n]$$

gdje je $h := (\frac{a-b}{a+b})^2$. Ramanujan je pronašao vrlo preciznu približnu formulu $O \approx \pi(a + b)(3 - \sqrt{4 - h})$.

Za odredjivanje duljine luka krivulje, predpostavimo da je $a > b$ i pogledajmo sl.4.



Tu je:
$\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1$ - jednadžba elipse,
$y = \frac{b}{a}\sqrt{a^2 - x^2}$ - jednadžba gornje poluelipse
$y' = -\frac{b}{a}\frac{x}{\sqrt{a^2-x^2}}$,
$l(u)$ - duljina lika elipse od točke $T_0(0, b)$ do točke $T(u, ...)$.
Kako je
$l(u) = \int_0^u \sqrt{1 + y'^2}dx$, dobijemo

$$l(u) = a\int_0^{\frac{u}{a}} \sqrt{\frac{1 - k^2t^2}{1 - t^2}}dt \tag{6}$$

gdje je $t = ax$ i $k^2 = 1 - \frac{b^2}{a^2}$. Posebno je opseg elipse

$$O = 4a\int_0^1 \sqrt{\frac{1 - k^2t^2}{1 - t^2}}dt$$

Ako stavimo $t = \sin\phi$, što je dio prirodne parametrizacije elipse $x = a\sin\phi$, dobijemo $l(u) = a\int_0^{arcsin\frac{u}{a}} \sqrt{1 - k^2\sin^2\phi}d\phi$, odnosno $O = 4a\int_0^{\frac{\pi}{2}} \sqrt{1 - k^2\sin^2\phi}d\phi$. Drugi korijen se može rastaviti u red potencija i integrirati član po član. Tako imamo MacLaurinov rezultat iz 1742.

$$O = 2\pi a(1 - \frac{1}{4}k^2 - \frac{3}{64}k^4 - \frac{5}{256}k^6 - ...)$$

Integral (6), samo bez granica (radi jednostavnosti), dalje se može napisati kao $a\int \frac{1-k^2t^2}{\sqrt{(1-t^2)(1-k^2t^2)}}dt$, odnosno kao

$$a\int \frac{dt}{\sqrt{(1 - t^2)(1 - k^2t^2)}} - ak^2\int \frac{t^2dt}{\sqrt{(1 - t^2)(1 - k^2t^2)}}$$

Prvi od ovih integrala obično se zove **eliptički integral prve vrste**, a drugi **eliptički integral treće vrste** (ako su u tim integralima granice od 0 do 1 kaže se da su **potpuni**).

Svodjenje $\int \frac{dt}{\sqrt{(1-t^2)(1-k^2t^2)}}$ na oblik $\int \frac{dz}{\sqrt{f(z)}}$, $degf = 3$.

Pokazuje se da se integrali gornjeg tipa s polinomom 4. stupnja pod korijenom uvijek mogu svesti na one s s polinomom 3. stupnja pod korijenom (ali daljnja redukcija općenito nije moguća). Stavimo:

$z = \frac{1}{1-t},\ t = 1 - \frac{1}{z},\ dt = \frac{1}{z^2}dz$ i dobit ćemo:
$\int \frac{dt}{\sqrt{(1-t^2)(1-k^2t^2)}} = \int \frac{dz}{\sqrt{\frac{1+t}{1-t}\frac{1-kt}{1-t}\frac{1+kt}{1-t}}} = \int \frac{dz}{\sqrt{(2z-1)((1-k)z+k)((k+1)z-k)}}$.

Tu se pojavljuje slična situacija onoj s formulama za rješenje algebarskih jednadžba u radikalima:
(I) za $n = 1$ i $n = 2$, tj. za jednadžbe $ax + b = 0$ i $ax^2 + bx + c = 0$ formule su poznate od davnina.
(II) Za $n = 3$ čekalo se gotovo do polovice 16. st., a slučaj $n = 4$ reducira se na kubni. Pokazalo se da je za uporabu formule (u slučaju realnih rješenja) presudno uvodjenje kompleksnih brojeva.
(III) Za $n \geq 5$ nema općenite formule i za zapis rješenja treba uvesti nove funkcije.

Za integrale $\int \frac{dx}{\sqrt{f(x)}}$ uz $n = degf$ vrijedi:
(I) za $n = 1$ i $n = 2$ integral se racionalizira racionalnim funkcijama, pa se izražava elementarnim funkcijama.
(II) za $n = 3$ integral se općenito ne racionalizira racionalnim funkcijama, već tzv. eliptičkim funkcijama (uniformizacija) i nije elementaran (o tome ćemo više reći poslije). Slučaj $n = 4$ svodi se na $n = 3$. Pokazuje se da je za pravilno tretiranje potrebno uvodjenje kompleksnih brojeva.
(III) za $n \geq 5$ za uniformizaciju su potrebne druge vrste funkcija.