Uvod u aritmetiku eliptičkih krivulja

1. Eliptičke krivulje nad $\mathbf{C}$ (skica) - 3. lekcija

Već smo vidjeli da se eliptička krivulja (točnije skup svih njenih kompleksnih točaka, uključujući i beskonačno daleku točku) može parametrizirati (uniformizirati) dvostrukoperiodnim kompleksnim funkcijama h, h', koje se dobiju integriranjem po torusu $E(\mathbf{C})$ (od sad ćemo eliptičku krivulju zadanu jednadžbom $y^2 = x^3 + ax + b$ označavati kao E, skup njenih kompleksnih točaka, uključujući i beskonačno daleku točku, kao $E(\mathbf{C})$, skup realnih točaka kao $E(\mathbf{R})$ i sl.). Do baze za rešetku perioda Abel je izvorno došao integriranjem po pripadnom torusu. Einsensteinova je ideja da se krene od $\mathbf{C}$ i od po volji odabrane dvodimenzionalne rešetke

$$L = \{m\omega_1 + n\omega_2\},\ m, n \in \mathbf{Z}$$

gdje su ω_1, ω_2 $\mathbf{R}$-linearno nezavisni kompleksni brojevi koji čine bazu rešetke, pa da se konstruiraju meromorfne funkcije kojima je L skup perioda. On je dao i prijedlog kako se tako funkcije mogu konstruirati. Eisenstein je umro mlad, a njegovu ideju razradio je Weierstrass.

Weierstarssove $\mathcal{P}$ i $\mathcal{P}'$ funkcija

Neka je $L = \mathbf{Z}\omega_1 \oplus \mathbf{Z}\omega_2$ fiksirana rešetka u $\mathbf{C}$ (gdje su ω_1, ω_2 linearno nezavisni nad $\mathbf{R}$). **Weierstrassova $\mathcal{P}$ funkcija** (pridužena rešetki L) je funkcija zadana redom:

$$\mathcal{P}(z) := \frac{1}{z^2} + \sum_{\omega \in L \setminus \{0\}} [\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}] \tag{1}$$

Da bi se naglasilo o kojoj je rešetki riječ često se piše $\mathcal{P}_L(z)$ ili slično. Vrijedi sljedeće (a dokaže se standardnim postupkom):
(I) Red (1) konvergira apsolutno na $\mathbf{C} \setminus L$.
(II) Red (1) konvergira uniformno na kompaktima od $\mathbf{C} \setminus L$.

Svojstvo (I) potvrdjuje da je (1) dobro definirano tj. da ne ovisi o redoslijedu zbrajanja, a skupa s (II) da je $\mathcal{P}$ analitička funkcija na $\mathbf{C} \setminus L$, koja se može derivirati član po član. Dalje, vrijedi (što ćemo i dokazati):

(i) $\mathcal{P}$ je parna funkcija. Naime, $\mathcal{P}(-z) := \frac{1}{z^2} + \sum_{\omega \in L \setminus \{0\}} [\frac{1}{(z-(-\omega))^2} - \frac{1}{(-\omega)^2}] = \mathcal{P}(z)$, jer je $-L = L$.

(ii) $\mathcal{P}'(z) := -2\sum_{\omega\in L}\frac{1}{(z-\omega)^3}$ je L-periodna (tj. za periode ima sve elemente iz L, odnodno ima dva nezavisna perioda pa je dvostruko periodna) neparna analitička na $\mathbf{C}\setminus L$ funkcija. Zato kažemo da je $\mathcal{P}'$ **eliptička funkcija** (ili, preciznije, L-eliptička funkcija). Periodnost ide izravnim uvrštavanjem i korištenjem $-L = L$, a neparnost kao i u (i).
(iii) $\mathcal{P}$ takodjer je periodna, pa je eliptička. Naime, iz
$\mathcal{P}'(z+\omega) = \mathcal{P}'(z)$, za svaki fiksirani $\omega \in L$ i svaki $z \in \mathbf{C}$ (uz interpretaciju da je vrijednost u točkama rešetke beskonačna), integriranjem se dobije $\mathcal{P}(z+\omega) = \mathcal{P}(z) + C$, za svaki fiksirani $\omega \in L$ i svaki $z \in \mathbf{C}$, gdje je C kompleksna konstanta ovisna samo o izabranom ω. Uvrštavanjem $z = -\frac{\omega}{2}$ iz parnosti od $\mathcal{P}$ proizlazi da je $C = 0$. Kako sve vrijedi za bilo koji ω, $\mathcal{P}$ je eliptička.
(iv) (Laurentov razvoj od $\mathcal{P}$ oko ishodišta). Za $z \neq 0$ sa svojstvom $|z| < \min\{|\omega|,\ \omega \in L\setminus\{0\}\}$ vrijedi

$$\mathcal{P}(z) = \frac{1}{z^2} + 3G_4 z^2 + 5G_6 z^4 + 7G_8 z^6 + ...$$

gdje je

$$G_k := \sum{}' \frac{1}{\omega^k}$$

za $k \geq 3$ Eisensteinov red (znak sume s crticom znači da se sumira po svim ne-nul elementima rešetke - uočite da za neparne indekse k je $G_k = 0$, a za parne ≥ 4 red apsolutno konvergira). Za dokaz je dovoljno razmotriti:

$$\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} = \frac{1}{\omega^2}\Big[\frac{1}{(1-\frac{z}{\omega})^2} - 1\Big]\frac{1}{\omega^2}\sum_{n=1}^{\infty}(n+1)\frac{z^n}{\omega^n}$$

Sumirajući po svim $\omega \neq 0$ dobijemo traženi razvoj.
(v) $\mathcal{P}$ je meromorfna na $\mathbf{C}$ s polovima 2. reda u L, a $\mathcal{P}'$ je meromorfna na $\mathbf{C}$ s polovima 3. reda u L. Naime, iz razvoja (iv) se vidi da je u 0 pol 2. reda, a zbog eliptičnosti (tj. L-periodnosti) tako je u svakoj točki rešetke.
(vi) Vrijedi

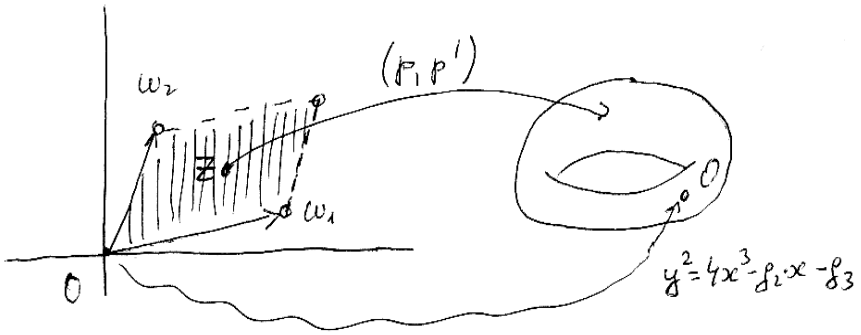
$$\mathcal{P}'(z)^2 = 4\mathcal{P}(z)^3 - g_2\mathcal{P}(z) - g_3$$

gdje je $g_2 := 60G_4,\ g_3 := 140G_6$. Naime, iz razvoja (iv) dobije se:
$\mathcal{P}'(z)^2 = \frac{4}{z^6} - \frac{24G_4}{z^2} - 80G_6 + ...$

$\mathcal{P}(z)^3 = \frac{1}{z^6} + \frac{9G_4}{z^2} + 15G_6 + ...,$
pa je $H(z) := \mathcal{P}'(z)^2 - 4\mathcal{P}(z)^3 + g_2\mathcal{P}(z) + g_3$ analitička L-periodna funkcija na $\mathbf{C}$ sa svojstvom $H(0) = 0$. Ona je omedjena na fundamentalnom periodu, pa i na cijelom $\mathbf{C}$, pa je konstanta. Kako joj je jedna vrijednost 0 ona je nula-funkcija, što smo i trebali.
(vii) preslikavanje $\mathbf{C} \mapsto E(\mathbf{C})$, $z \mapsto (\mathcal{P}(z), \mathcal{P}'(z))$, $L \mapsto O$,

gdje je $E : y^2 = 4x^3 - g_2x - g_3$ pripadna eliptička krivulja s beskonačno dalekom točkom O, je dobro definirana surjekcija (da je preslikavanje dobro definirano slijedi iz (vi)). Ona inducira bijekciju

$$\mathbf{C}/L \cong E(\mathbf{C})$$



Sl. 1.

Time smo dobili uniformizaciju eleptičke krivulje E eliptičkim funkcijama $\mathcal{P}, \mathcal{P}'$ (sl.1). Za preciznu formulaciju ove tvrdnje i dokaz trebalo bi uvesti nekoliko novih pojmova i dokazati nekoliko (standardnih) činjenica, što izostavljamo. Posebno gornja bijekcija je analitički izomorfizam grupa, što će imati smisla tek kad definiramo grupnu operaciju na $\mathbf{C}$.
Umjesto toga podrobno ćemo sve ilustrirati na jednom primjeru. Najprije bez dokaza navodimo još jednu dobro poznatu formulu.

(IV) Kako je $G_k := \sum' \frac{1}{(m\omega_1 + n\omega_2)^k} = \frac{1}{(\omega_1)^k} \sum' \frac{1}{(m+n\tau)^k}$, gdje je $\tau := \frac{\omega_2}{\omega_1}$ i možemo smatrati da je iz gornje poluravnine $\mathcal{H}$, vidimo da je gotovo dovoljno razmatrati Eisensteinove redove za rešetke razapete bazom $\{1, \tau\}$ za $\tau \in \mathcal{H}$, definirane kao:

$$G_k(\tau) := \sum' \frac{1}{(m + n\tau)^k}.$$

Vrijedi:

$$G_{2k}(\tau) = 2\zeta(2k) + 2\frac{(2\pi i)^{2k}}{(2k-1)!} \sum_{k=1}^{\infty} \sigma_{2k-1}(n) e^{2\pi i n \tau}, \tag{2}$$

gdje je ζ Riemannova zeta funkcija, a $\sigma_r(n) := \sum_{d|n} d^r$, funkcija koja zbraja r-te potencije djelitelja broja n.

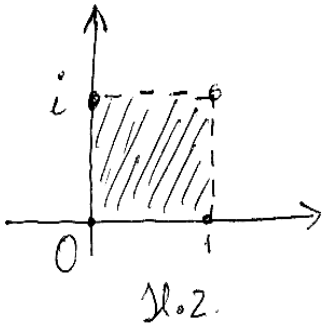
Primjer. Neka je $L := \mathbf{Z} \oplus \mathbf{Z}i$ rešetka razepeta s $\{1, i\}$ (vidi sl.2. gdje je predočen fundamentalni paralelogram). Tada je:

$\mathcal{P}(z) = \frac{1}{z^2} + \sum{}' [\frac{1}{(z-m-ni)^2} - \frac{1}{(m+ni)^2}]$,

$\mathcal{P}'(z) = \frac{-2}{z^3} - 2\sum{}' \frac{1}{(z-m-ni)^3}$,

$g_2 := 60G_4 = 60\sum{}' \frac{1}{(m+ni)^4}$,

$g_3 := 140G_6 = \sum{}' \frac{1}{\quad} - \frac{140}{6}\sum{}' \frac{1}{(n-mi)^6} = -g_3$, pa je $g_3 = 0$.

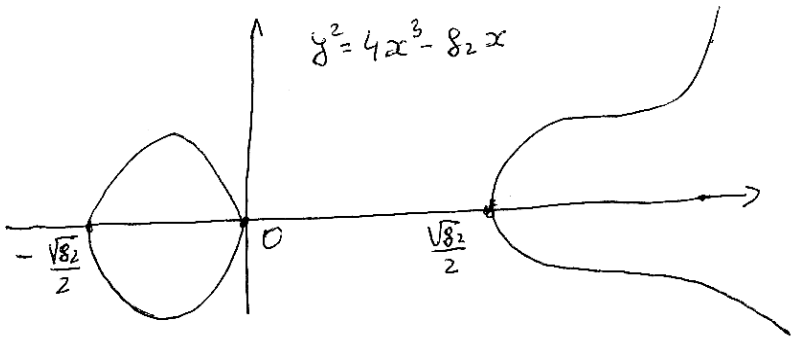


Sl. 2.

Nadalje, izravnim uvrštavanjem u (2) dobije se $g_2 > 0$, pa je eliptička krivulja

$$E : y^2 = 4x^3 - g_2 x$$

definirana jednadžbom s realnim koeficijentima i $E(\mathbf{R})$ ima dvije komponente povezanosti, kao na sl.3. Želimo razjasniti koje se točke fundamentalnog paralelograma preko uniformizacije $z \mapsto (\mathcal{P}(z), \mathcal{P}'(z))$ preslikavaju u ove realne točke od E.



Sl. 3.

a) Točke presjeka s x-osi: one karakterizirane uvjetom $y = 0$, tj. $\mathcal{P}'(z) = 0$, pa treba naći nultočke te funkcije. Kako je općenito $\mathcal{P}'(\frac{\omega}{2}) = \mathcal{P}'(\frac{\omega}{2} - \omega) =$

$\mathcal{P}'(-\frac{\omega}{2}) = -\mathcal{P}'(\frac{\omega}{2})$ vidimo da je u našem fundamentalnom paralelogramu

$$\mathcal{P}'(\frac{1}{2}) = \mathcal{P}'(\frac{i}{2}) = \mathcal{P}'(\frac{1+i}{2}) = 0$$

To su, očito, jedina rješenja jednadžbe $\mathcal{P}'(z) = 0$ u fundamentalnom periodu (a poslije se sve ponavlja).
b) Tražimo z za koje je $\mathcal{P}(z)$ realno. Kako definicijske redove možemo zbrajati po volji i kako je rešetka invarijantna na konjugiranje (pri konjugiranju prelazi u sebe), vrijedi

$$\overline{\mathcal{P}(z)} = \mathcal{P}(\bar{z})$$

(tj. konjugiranje je "homomorfizam" za beskonačnu sumu). Zato je za sve t za koje je $0 < t < 1$:
$\overline{\mathcal{P}(t)} = \mathcal{P}(t)$
$\overline{\mathcal{P}(ti)} = \mathcal{P}(-ti) = \mathcal{P}(ti)$, zbog parnosti
$\overline{\mathcal{P}(\frac{1}{2} + ti)} = \mathcal{P}(\frac{1}{2} - ti) = \mathcal{P}(-\frac{1}{2} + ti) = \mathcal{P}(\frac{1}{2} + ti)$, zbog parnosti i periodnosti
$\overline{\mathcal{P}(\frac{i}{2} + t)} = \mathcal{P}(-\frac{i}{2} + t) = \mathcal{P}(\frac{i}{2} + t)$, zbog periodnosti
Tako smo našli 4 intervala u fundamentalnom periodu koje funkcija $\mathcal{P}$ preslikava u 4 realna intervala na koje $-\frac{\sqrt{g_2}}{2}$, 0 i $\frac{\sqrt{g_2}}{2}$ dijeli realnu os. Funkcija $\mathcal{P}$ na tim intervalima nije injektivna, već svaku vrijednost osim $-\frac{\sqrt{g_2}}{2}$, 0 i $\frac{\sqrt{g_2}}{2}$ postiže dva puta (u točkama simetričnim s obzirom na $\frac{1}{2}, \frac{i}{2}, \frac{1+i}{2}$). To izravno proizlazi iz identiteta

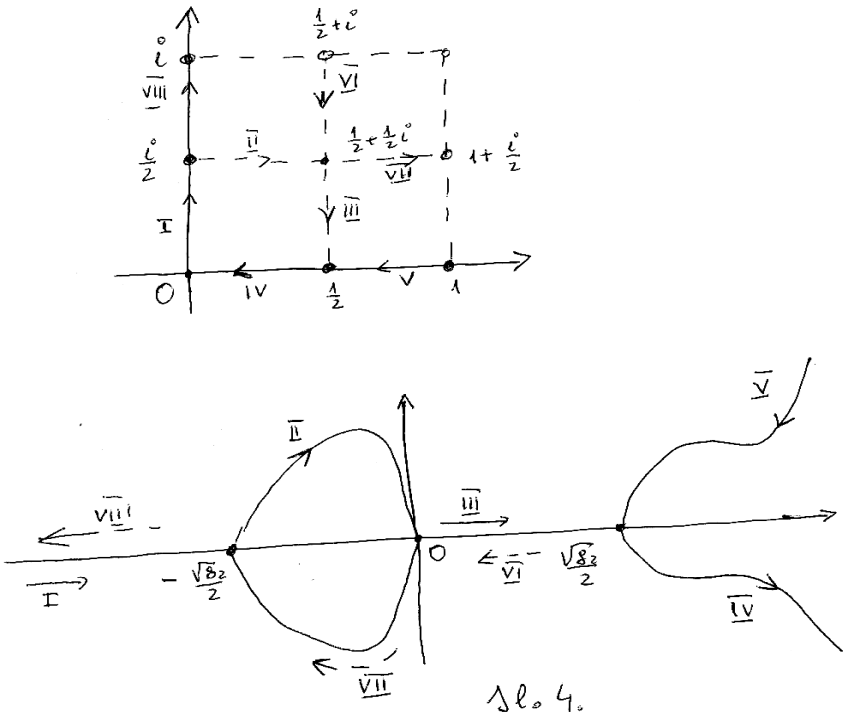
$$\mathcal{P}(\frac{\omega}{2} - z) = \mathcal{P}(\frac{\omega}{2} + z)$$

koji vrijedi za svaki z i svaki period ω (za bilo koju rešetku). Uočite, takodjer da vrijedi

$$\mathcal{P}'(\frac{\omega}{2} - z) = -\mathcal{P}'(\frac{\omega}{2} + z)$$

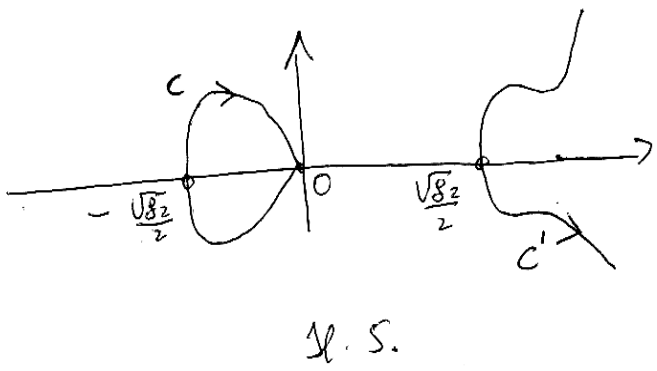
pa u gornjim točkama $\mathcal{P}'$ prima suprotne vrijednosti.
Zato u prvom dijelu svakog od tih intervala $\mathcal{P}$ primi svaku vrijednost iz odredjenog intervala na x-osi, a u drugom dijelu iste te vrijednosti u suprotnom redoslijedu, pri čemu $\mathcal{P}'$ postiže suprotne vrijednosti (u slučaju realnih vrijednosti jednom ispod osi x, a jednom iznad). Zato smo ta 4 intervala podijelili na 8 poluintervala kao na sl.4. i predočili ponašanje $\mathcal{P}$ i $\mathcal{P}'$ funkcije (tu $\mathcal{P}$ u prva četiri intervala prima redom sve realne vrijednosti od $-\infty$ do $+\infty$, a druga četiri u suprotnom redoslijedu, a $\mathcal{P}'$ prima suprotne vrijednosti). Pri odredjivanju putanje sluv zili smo se programskim paketom Mathematica, pune oznake odnose se na prve 4 poluintervala, a iscrtkane na druga 4. Na onim dijelovima nad kojima su druge koordinate imaginarne (tj. prve negativne) oznaku putanje stavljamo iznad x-osi ako su imaginarni dijelovi

pozitivni.



Sl. 4.

Rekonstrukcija perioda $1, i$ **integriranjem po torusu**.
Uvedimo sljedeće oznake (vidi sl.5.):



Sl. 5.

Realni ciklus koji ne sadrži O označimo kao c (dobije se preslikavan-

jem intervala $II \cup VII$), a onaj drugi kao c' (dobije se preslikavanjem intervala $IV \cup V$, c, c' su suprotno orijentirani). Nevidljive imaginarne cikluse označimo kao γ (dobije se preslikavanjem intervala $III \cup VI$), odnosno kao γ' (dobije se preslikavanjem intervala $I \cup VIII$). Tada je (uz zamjenu $x = \mathcal{P}(z),\ y = \mathcal{P}'(z);\ dx = \mathcal{P}'(z)dz$)

$\int_c \frac{dx}{y} = \int_{\frac{i}{2}}^{\frac{1}{2}+\frac{i}{2}} dz + \int_{\frac{1}{2}+\frac{i}{2}}^{1+\frac{i}{2}} dz = 1.$

U prijevodu na standardno integriranje po x osi, značenje je:

$\int_{-\frac{\sqrt{g_2}}{2}}^{0} \frac{dx}{\sqrt{4x^3-g_2x-g_3}} + \int_{0}^{-\frac{\sqrt{g_2}}{2}} \frac{dx}{-\sqrt{4x^3-g_2x-g_3}} = 2\int_{-\frac{\sqrt{g_2}}{2}}^{0} \frac{dx}{\sqrt{4x^3-g_2x-g_3}} = 1.$

Lako se vidi da se integriranjem po c' dobije -1 (što je logično jer su c i $-c'$ homologni).

Slično se dobije:

$\int_{\gamma'} \frac{dx}{y} = \int^{\frac{i}{}}$