UVOD U ARITMETIKU ELIPTIČKIH KRIVULJA
SEMINAR : MINIMALNA JEDNADŽBA

KRISTINA KRULIĆ

Neka je E eliptička krivulja nad $\mathbb{R}$ i

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{1}$$

je Weiestrassova jednadžba za E čiji su koeficijenti $a_i \in \mathbb{Z}$.
Standardna zamjena varijabli:

$$\begin{aligned}
b_2 &= a_1^2 + 4a_2 \\
b_4 &= 2a_4 + a_1a_3 \\
b_6 &= a_3^2 + 4a_6 \\
b_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2 \\
c_4 &= b_2^2 - 24b_4 \\
c_6 &= -b_2^3 + 36b_2b_4 - 216b_6
\end{aligned}$$

pa dobijemo

$$y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6, \text{ odnosno } y^2 = x^3 - 27c_4x - 54c_6$$

(karakteristika jednadžbi različita od 2 i 3).
Jednadžbu (1) nazivamo MINIMALNA jednadžba za prost broj p ako se stupanj od p koji dijeli diskriminantu Δ ne može smanjiti dozvoljenom zamjenom varijabli nad $\mathbb{Q}$ sa svojstvom da su novi koeficijent p-cjelobrojni. (ili $|\Delta|_p$ se ne može povećati s takvom zamjenom varijabli gdje je $p-$norma definirana sa $|x|_p = p^{-\alpha}$, $x = \frac{p^\alpha r}{s}$ i r, s su cijeli brojevi koje ne dijeli p.
Jednadžbu (1) nazivamo GLOBALNO MINIMALNA WEIESTRASSOVA JEDNADŽBA ako je minimalna za sve proste brojeve p i ako su njeni koeficijenti cijeli brojevi.
Zamjena varijabli u Weierstrassovoj jednadžbi je oblika

$$x = u^2x' + r \text{ i } y = u^3y' + su^2x' + t. \tag{2}$$

Utjecaj na koeficijente a_i, b_i, c_i dan je u Tablici 1.

Tablica 1.

$$\begin{aligned}
ua_1' &= a_1 + 2s \\
u^2a_2' &= a_2 - sa_1 + 3r - s^2 \\
u^3a_3' &= a_3 + ra_1 + 2t \\
u^4a_4' &= a_4 - sa_3 + 2ra_2 - (t + rs)a_1 + 3r^2 - 2st \\
u^6a_6' &= a_6 + ra_4 + r^2a_2 + r^3 - ta_3 - t^2 - rta_1
\end{aligned}$$

$$\begin{aligned} u^2 b_2^{'} &= b_2 + 12r \\ u^4 b_4^{'} &= b_4 + rb_2 + 6r^2 \\ u^6 b_6^{'} &= b_6 + 2rb_4 + r^2 b_2 + 4r^3 \end{aligned}$$

$$\begin{aligned} u^4 c_4^{'} &= c_4 \\ u^6 c_6^{'} &= c_6 \\ u^{12}\Delta^{'} &= \Delta \end{aligned}$$

Lema 1. *Neka je p prost broj i svi koeficijenti jednadžbe* (1) su $p-$cjelobrojni. Ako je $|\Delta|_p > p^{-12}$ ili $|c_4|_p > p^{-4}$ ili $|c_6|_p > p^{-6}$, onda je jednadžba minimalna za prost broj p.
Ako je $p > 3$ i $|\Delta|_p \leq p^{-12}$ i $|c_4|_p \leq p^{-4}$, onda jednadžba nije minimalna za taj prost broj p.

Dokaz. Pretpostavimo da zamjena varijabli (2) vodi na sustav $p-$cjelobrojnih koeficijenata $\{a_i^{'}\}$ sa svojstvom

$$1 \geq |\Delta^{'}|_p > |\Delta|_p .$$

Budući je $u^{12}\Delta^{'} = \Delta$, onda vrijedi $|u^{12}|_p |\Delta^{'}|_p = |\Delta|_p$. Tada je $|u|_p < 1$ i vrijedi $|u|_p \leq p^{-1}$ te zaključujemo

$$|\Delta|_p = |u|_p^{12} |\Delta^{'}|_p \leq p^{-12}.$$

Pokažimo tvrdnju i za c_4.
Pretpostavimo

$$1 \geq |c_4^{'}|_p > |c_4|_p.$$

Znamo $u^4 c_4^{'} = c_4$ pa tada vrijedi:

$$|u^4|_p |c_4^{'}|_p = |c_4|_p$$

odnosno

$$|c_4|_p = |u|_p^4 |c_4^{'}|_p \leq p^{-4}.$$

Analogno za c_6.
Pretpostavimo sada $p > 3$ i $|\Delta|_p \leq p^{-12}$ i $|c_4|_p \leq p^{-4}$. Tada vrijedi $1728\Delta = c_4^3 - c_6^2$, $(1728 = 3^3 2^6$ pa je $|1728|_p = 1)$ te je $|c_6|_p \leq p^{-6}$.
Zbog standardne zamjene varijabli od jednadžbe (1) dobijemo jednadžbu

$$y^2 = x^3 - 27c_4 x - 54c_6 \tag{3}$$

sa diskriminantom $\Delta^{'} = 2^{12}3^{12}\Delta$.
(podsjetnik: ako je (3) minimalna jednadžba, njezina diskriminanta je $2^6 3^9 (c_4^3 - c_6^2)$ pa se razlikuje za faktor $2^{12}3^{12}$ od diskriminate jednadžbe $1728\Delta = c_4^3 - c_6^2$.)
Sad napravimo zamjenu varijabli: $u = p, r = s = t = 0$ i dobijemo jednadžbu

$$y^2 = x^3 - 27(c_4 p^{-4})x - 54(c_6 p^{-6})$$

koja ima $p-$cjelobrojne koeficijente. Znamo $|c_4 p^{-4}|_p \leq 1$ i $|c_6 p^{-6}|_p \leq 1$ te da za diskriminantu vrijedi $\Delta^{''} = p^{-12}\Delta^{'}$ pa $|\Delta^{''}|_p = p^{12}|\Delta^{'}|_p = p^{12}|\Delta|_p$. Zaključujemo da dana jednažba nije minimalna za dani prost broj p. Time je dokaz gotov.

Primjer 1. *Neka je* $E : y^2 + xy + y = x^3 + x^2 + 22x - 9$ *Weierstrassova jednadžba i* p *prost broj. Računamo koeficijente:* $b_2, b_4, b_6, b_8, c_4, \Delta$. *Dobijemo* $b_2 = 5, b_4 = 45, b_6 = -550, \Delta = -5^2 2^{15}, c_4 = -5 \cdot 211$.
Tada vrijedi:

$$
\begin{aligned}
|\Delta|_p &= 1 \text{ za } p \neq 2 \text{ i } 5 \\
|\Delta|_5 &= \frac{1}{25},\ |\Delta|_2 = 2^{-15} \\
|c_4|_p &= 1 \text{ za } p \neq 5 \text{ i } 211 \\
|c_4|_5 &= 1/5,\ |c_4|_{211} = 1/211
\end{aligned}
$$

$\Longrightarrow |c_4|_p > p^{-4}$. *Zaključujemo da je dana jednadžba minimalna Weierstrassova jednadžba za svaki prost broj* p.

Propozicija 1. *Neka je* p *prost broj i* E *eliptička krivulja nad* $\mathbb{Q}$.
(a) Postoji zamjena varijabli od E *nad* $\mathbb{Q}$ *takva da je rezultirajuća jednadžba minimalna za prost broj* p.
(b) Ako E *ima* $p-$*cjelobrojne koeficijente, onda zamjena varijabli u (a) ima* u, r, s, t *sve* $p-$*cjelobrojne koeficijente.*
(c) Dvije minimalne jednadžbe za p*, a dobivene su od* E *povezane su zamjenom varijabli u kojoj vrijedi* $|u|_p = 1$ *i* r, s, t *su* $p-$*cjelobrojni.*

Dokaz. (a) Bez smanjenja općenitosti možemo pretpostaviti da elipička krivulja ima $p-$cjelobrojne koeficjente. Tada je $|\Delta|_p \leq 1$.
Budući je rang od $|\ |_p$ diskretno udaljen od 0, $|\Delta|_p$ može biti povećana samo konačno mnogo puta ako želimo zadržati $|\Delta|_p \leq 1$. Stoga u konačno mnogo koraka možemo dobiti minimalnu jednadžbu za svaki prost broj p.

(b) Neka E ima koeficijente $\{a_i\}$, a minimalna jednadžba $\{a_i^{'}\}$. Znamo da je $|\Delta^{'}|_p \geq |\Delta|_p$ pa stoga $|u|_p \leq 1$. Iz Tablice 1. vidimo da su i koeficijenti $\{b_i\}$ te $\{b_i^{'}\}$ $p-$cjelobrojni.
Pretostavimo da je $p \neq 3$.
Ako je $|r|_p > 1$, onda jednadžba $u^8 b_8^{'} = b_8 + 3rb_6 + 3r^2 b_4 + r^3 b_2 + 3r^4$ ima $3r^4$ kao najveći izraz u $p-$normi na desnoj strani. No to je kontradikcija pa zaključujemo da je $|r|_p \leq 1$.
Ako je $p = 3$, onda gledamo jednadžbu $u^6 b_6^{'} = b_6 + 2rb_4 + r^2 b_2 + 4r^3$ i zaključujemo $|r|_p \leq 1$.
Slično zaključujemo i za s i t pa vrijedi $|s|_p \leq 1$ i $|t|_p \leq 1$.

(c) Ako koristimo tvrdnju (b) za zamjenu varijabli za dvije minimalne jednadžbe, onda zaključujemo $|u|_p \leq 1$ i r, $t\,s$ su $p-$cjelobrojni. Sad koristimo (b) za inverznu promjenu varijabli koja uključuje u^{-1} pa vidimo da je $|u^{-1}|_p \leq 1$, odnosno $|u|_p = 1$.

Teorem 1. *(Neron) Ako je* E *eliptička krivulja nad* $\mathbb{Q}$*, onda postoji zamjena varijabli na* $\mathbb{Q}$ *takva da je rezultirajuća jednadžba globalna minimalna Weierstrassova jednadžba. Dvije takve rezultirajuće globalne minimalne Weierstrassove jednadžbe povezane su zamjenom varijabli* $u = \pm 1$ *i* r, $s\,t \in \mathbb{Z}$.

Dokaz. Jedinstvenost proizlazi iz prethodne propozicije (b) dio. Ostaje dokazati egzistenciju.

Pretpostavimo da E ima cjelobrojne koeficijente a_i. Za svaki p koji dijeli diskriminantu Δ izaberimo zamjenu varijabli u_p, r_p, s_p, t_p nad $\mathbb{Q}$ tako da nova jednadžba ima koeficijente $a_{i,p}$ i minimalna je za p. (Propozicija 1. (a) dio)
Po Propoziciji 1. (b) u_p, r_p, s_p, t_p su $p-$cjelobrojni.
Novu diskriminantu označimo sa Δ_p. Tada koristeći Tablicu 1. vrijedi:

$$|u_p|_p^{12}|\Delta_p|_p = |\Delta|_p.$$

Označimo $u_p = p^{d_p}v_p$ sa $|v_p|_p = 1$.
Definirajmo $u = \Pi_{p|\Delta}p^{d_p}$.
Sad napravimo zamjenu varijabli $\{u,\, r,\, s,\, t\}$ u orginalnoj jednadžbi koja vodi na jednadžbu sa cjelobrojnim koeficijentima $a_i^{'}$ i diskriminantom $\Delta^{'}$. Vrijedi $u^{12}\Delta^{'} = \Delta$ pa imamo $|\Delta^{'}|_p = |u|_p^{-12}|\Delta|_p = |\Delta_p|_p$.
Dakle, nova jednadžba je minimalna za svaki prost broj p. Sada trebamo odrediti r, s i t.
Za svaki $p|\Delta$ označimo $r_p = p^{\rho_p}m_p/n_p$ sa $m_p,$, $n_p \in \mathbb{Z}$, $|m_p|_p = |n_p|_p = 1$. Neka je n_p^{-1} inverz od n_p modulo p^{6d_p}. Dobili smo kongruenciju

$$r \equiv p^{\rho_p}m_pn_p^{-1} \mod p^{6d_p}. \tag{4}$$

Po kineskom teoremu o ostacima možemo naći cijeli broj r tako da jednadžba (4) bude zadovoljena za svaki $p|\Delta$. Tada $|n_pr - p^{\rho_p}m_p|_p \le p^{-6d_p}$ i $|r - r_p|_p \le p^{-6d_p}$ za svaki p. Slično možemo naći s i t takve da

$$|s - s_p|_p \le p^{-6d_p} \text{ i } |t - t_p|_p \le p^{-6d_p}, \text{ za svaki } p.$$

Definirali smo zamjenu varijabli $\{u,\, r,\, t,\, s\}$. Ostaje nam još pokazati da su koeficijent $\{a_i^{'}\}$ cjelobrojni.
Provjerimo za sve proste p da $|a_1^{'}|_p \le 1, ..., |a_6^{'}|_p \le 1$ koristeći formule iz Tablice 1. Ako p ne dijeli Δ, onda $|u|_p = 1$ i $r,\, t,\, s \in \mathbb{Z}$ pa dobijemo $|a_i^{'}|_p \le 1$. Za $p|\Delta$ provjerimo svaki $|a_i^{'}|_p$. Ilustrirajmo za $a_2^{'}$.

$$\begin{aligned}
u^2a_2^{'} &= a_2 - sa_1 + 3r - s^2 \\
&= (a_2 - s_pa_1 + 3r_p - s_p^2) - (s - s_p)a_1 + 3(r - r_p) - (s^2 - s_p^2) \\
&= u_p^2a_{2,p}^{'} - (s - s_p)a_1 + 3(r - r_p) - (s - s_p)(s + s_p)
\end{aligned}$$

$$\begin{aligned}
|u|_p^2|a_2^{'}|_p &\le \max\{|u_p^2|_p|a_{2,p}^{'}|_p,\, |(s - s_p)a_1|_p,\, |3(r - r_p)|_p,\, |(s - s_p)(s + s_p)|_p\} \\
&\le \max\{|u_p^2|_p,\, |(s - s_p)|_p,\, |(r - r_p)|_p\} \\
&\le \max\{|u_p^2|_p,\, p^{-6d_p}\} \le |u_p^2|_p.
\end{aligned}$$

Znamo $|u|_p^2 = |u_p^2|_p$ pa zaključujemo $|a_2^{'}|_p \le 1$. Analogno ostale.
Time je dokaz gotov.

Literatura:

[1] A. W. Knapp, *Elliptic Curves, Princeton University Press, 290-294.*
[2] *J. H. Silverman, The Arithmetic of Elliptic Curves, Springer-Verlag, 223-227.*