Luca De Feo: Mathematics of Isogeny Based Cryptography

Charles, Goren, Lauter: Cryptographic hash functions from expanders graphs

T. Tao: Basic theory of expander graphs (blog)

Grafovi u kriptografiji - hash funkcija

Što je to kriptografska hash funkcija?

Algoritam koji preslikava poruke proizvoljne duljine u string fiksne duljine. U idealnoj situaciji bi trebala imati sljedeća svojstva

- fja. je deterministička
- brzo se računa
- teško je pronaći inverz (idealno, brut-force pretraga je jedina opcija)
- teško je pronaći dvije poruke s jednakom vrijednošću
- mala razlika u poruci generira hash vrijednost koja se čini da je nekorelirana s prethodnom vrijednošću

Koriste se najviše u autentifikaciji (digitalni potpisi i slično).

bitcoin rudarenje

Primjer: SHA-3 (224, 256, 384 ili 512 bitna output)

Što su to graf ekspander? (eng. expanders)

može imati višestruke bridove i petlje

Neformalno, to je neusmjereni graf $G = (V, E)$

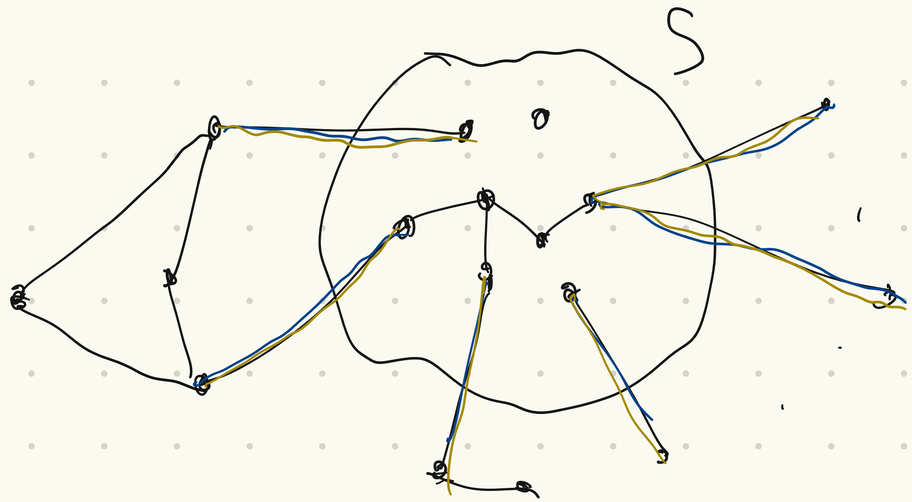
skup vrhova — skup bridova

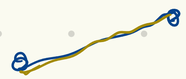
sa svojstvom da se svaki njegov podskup vrhova $S \subset V$

"brzo proširuju" (ekspandira) u smislu da je povezan s velikim vrhova iz komplementa $\bar{S} = V - S$.

Preciznije, za podskup $S \subset V$ definiramo njegov rub ∂S

kao skup svih bridova koji povezuju S i $\bar{S}$.



 $\in \partial S$

postoji i drugu definiciju

Ekspanzijski parametar od G (expansion parameter) se definira sa

kvantificira ekspanderska svojstva grafa

$$h(G) = \min_{\substack{S \subset V \\ |S| \leq \frac{|V|}{2}}} \frac{|\partial S|}{|S|}.$$

broj bridova koji izlazi iz vrha

stupanj svakog vrha je d

Od ekspandera se obično traži da budu d-regularni.

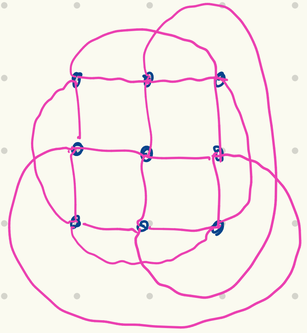
(Ta pretpostavka olakšava analizu njihovih svojstava.)

Primjer 1. Potpun graf s n vrhova. Za svaki S, $|\partial S| = |S| \cdot |\bar{S}| = |S|(n-|S|)$

$$\Rightarrow h(G) = \min_{|S| \leq \frac{n}{2}} (n-|S|) = \left\lceil \frac{n}{2} \right\rceil .$$

Primjer 2. G = $n \times n$ kvadratna rešetka (periodičnim rubnim uvjetima dobivamo graf 4-regularan)
(torus)

$n=3$



$$h(G) = O\left(\frac{1}{n}\right)$$

Primjer 3. G = slučajni d-regularan graf

$h(G) \approx \frac{d}{2}$ zašto?

Napomena: Ako graf G nije povezan onda je $h(G)=0$

Familiju grafova su često zanimljivi!

Def: Za familiju $G_j = (V_j, E_j)$ d-regularnih grafova t.d. $|V| = n_j$ (gdje je niz (n_j) rastući) kažemo da je familija **ekspandera** ako postoji konstanta $c > 0$ t.d.

$$h(G_j) \geq c \quad \forall j.$$

Neke konstrukcije:

3-regularan

Primjer 1. Neka je p prost. Vrhovi V_p grafa G_p su elementi polja $\mathbb{F}_p$.

Vrh $x \neq 0$ je spojen bridom s vrhovima $x-1$, $x+1$ i x^{-1}

Vrh $x = 0$ je spojen s $p-1$, 0 i 1.

Lubotsky, Phillips, Sarnak $\Rightarrow$ G_p je familija ekspandera (1988)

za razliku od slučajnih grafova, s ovom familijom možemo efikasno raditi

"troše" puno memorije

Karakterizacija preko matrica susjedstva (adjacency matrix)

pretp. da graf nema višestrukih bridova

$n \times n$ matrica $A(G)$ t.d. $A_{ij} = 1$ ako i samo ako su vrhovi i i j spojeni bridom, $A_{ij} = 0$ inače

Q: Kako odrediti $h(G)$? Po definiciji nije praktično.

Pomoću svojstvenih vrijednosti matrice $A(G)$!

spektar grafa G

izomorfni grafovi imaju jednake spektre (za što?)

jer je G neusmjeren ↙ ↘ spektralni teorem

$A(G)$ je realna simetrična matrica pa se može dijagonalizirati nad $\mathbb{R}$.

Svojstvene vrijednosti označavamo sa $\lambda_1(G) \geq \lambda_2(G) \geq \dots \geq \lambda_n(G)$.

Kako je G d-regularan, vektor $(1,1,\dots,1)^T$ je svojstveni sa svojst. vrijednosti d. Može se pokazati da je $\lambda_1(G) = d$.

Zadatak: d-regularan graf G je povezan akko i samo akko je $\lambda_1(G) > \lambda_2(G)$

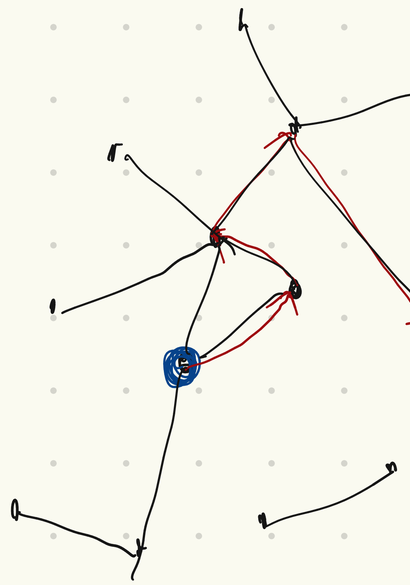
Def. $\Delta(G) := \lambda_1(G) - \lambda_2(G)$ (gap of the graph G)

Teorem: Vrijedi:

$$\frac{\Delta(G)}{2} \leq h(G) \leq \sqrt{2d\,\Delta(G)}$$

ako je $\mathcal{F}$ familija Δ omeđen odozdo, onda je familija ekspanderskih (s mjerom > 0)

Primjena: slučajne šetnje na ekspanderima



Markovljevog lanca

Markovljeva tranzicijska matrica

koja opisuje šetnju je $\hat{A}(G) := \frac{A(G)}{d}$ (zašto?)

ovo je "specijalna" matrica – dvostruko stohastička

kvadratna matrica ne-negativnih realnih brojeva

sa svojstvom da je suma elemenata u svakom retku

i stupcu jednaka 1: $\sum_i a_{ij} = \sum_j a_{ij} = 1$

Q: Gdje "završavaju" slučajne šetnje na d-regularnim grafovima? Je li svaki vrh jednako vjerojatan?

kakva je stacionarna distribucija Markovljevog lanca definiranog s $\tilde{A}(G)$?, je li uniformna?

$\pi_i = \pi_j \; \forall i,j$

vektor π sa svojstvom: $\pi \tilde{A}(G) = \pi$

tj. π^T je svojstveni vektor od $\tilde{A}(G)$ sa svojstvenom vrijednošću 1 koji je normaliziran t.d.

$$\sum \pi_i = 1.$$

Teorem: Stacionarnu distribuciju Markovljivog lanca definiranog tranzicijskom matricom M je uniformna ako i samo ako je M dvostruko stohastička.

Q: Koliko dugo trebamo čekati da se šetnja "razmaže" po cijelom grafu ako znamo da je stacionarna distribucija uniformna? Koliko brzo distribucija šetnje od t koraka konvergira stacionarnoj distribuciji, kad $t \to \infty$?

Teorem: Neka je u uniformna stacionarna distribucija Markovljevog lanca danog ($n \times m$) matricom M. Ako je P početna (bilo koja) distribucija onda nakon šetnji od t koraka imamo

$$\| M^t P - u \|_1 \leq \sqrt{n}\, \lambda_2(M)^t$$

↑ što je razmak $\Delta(M)$ veći to je konvergencija brža! ($\lambda_1(M) = 1$)

U našem slučaju

$$\| \tilde{A}(G)^t P - u \|_1 \leq \sqrt{n} \left(1 - \frac{h(G)^2}{2d^2}\right)^t$$

Još jedno svojstvo slučajnih šetnji na ekspanderima

– "brzo se kreću"

Neka je $B \subset V$ i X_0 slučajno odabrani vrh grafa koji će biti početak slučajne šetnje $X_0, X_1, \dots, X_t$. Označimo sa $B(t)$ događaj da je $X_j \in B$ za svaki $j \in \{0, 1, \dots, t\}$. Vrijedi (ako $\lambda_1(G) = d$)

Teorem: $$Pr(B(t)) \leq \left(\frac{\lambda_2(G)}{d} + \frac{|B|}{n} \right)^t$$

- Pr ↑ vjerojatnost
- $\frac{\lambda_2(G)}{d}$ ← što je $\lambda_2(G)$ manji to će se šetnja kraće zadržavati na "istom mjestu"
- $\frac{|B|}{n}$ ↑ $n = \#V$

Što se može reći o $\lambda_2(G_m)$ za familiju k-regularnih povezanih grafova G_m (t.d. $\lim \#V(G_m) = +\infty$)?

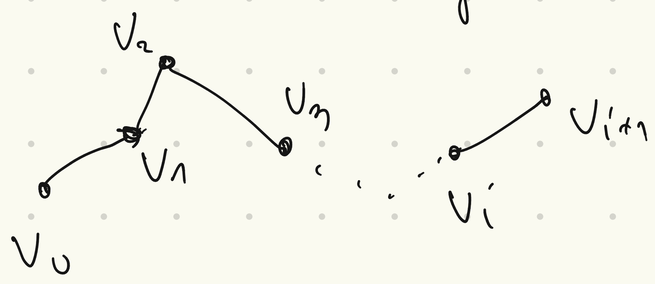
Teorem (Alon-Boppana)

$$\liminf_m \lambda_2(G_m) \geq 2\sqrt{k-1}$$

Definicija Za k-regularan povezan graf G kažemo da je **Ramanujanov** ako vrijedi $\lambda_2(G) \leq 2\sqrt{k-1}$. Familija takvih grafova je optimalna u odnosu na veličinu λ_2.

Konstrukcija hash funkcija iz ekspandera

Radi jednostavnosti pretpostavimo da je G k-regularan ekspander gdje je $k = 2^e + 1$. Input hash funkcije podijelimo na blokove duljine e. Počevši od fiksnog vrha v_0, konstruiramo "slučajnu šetnju" $v_0, v_1, \ldots, v_i, \ldots$ tako da u svakom koraku iz trenutnog vrha v_i koristeći jedan blok odaberemo jedan od preostalih $k-1 = 2^e$ bridova (nema vraćanja) te se tim bridom prošećemo do novog vrha v_{i+1}. Vrh na kojem završi šetnju je output hash funkcije.



Pizer: Ramanujan Graphs and Hecke Operators, Bulletin of the AMS

Primjer Ramanujanovog grafa – grafovi izogenija supersingularnih eliptičkih krivulja

- Označimo sa $G(p,\ell)$ graf čiji su vrhovi j-invarijante supersingularnih eliptičkih krivulja u karakteristici p.

Znamo da je $\#V(G(p,\ell)) = \left\lfloor \frac{p}{12} \right\rfloor + \varepsilon$, gdje je $\varepsilon \in \{0,1,2\}$.

($j(E) \in \mathbb{F}_p$ ili $\mathbb{F}_{p^2}$)

(Za $p \equiv 1 \pmod{12}$ vrijedi $\varepsilon = 0$.) U konkretnoj implementaciji hash funkcije

$p \approx 2^{256}$ i $p \equiv 1 \pmod{12}$,

Dva vrha $j(E_1)$ i $j(E_2)$ su povezana bridom ako postoji izogenija stupnja ℓ između E_1 i E_2, zato je graf $\ell+1$-regularan.

Teorem (Ramanujan-Petersson slutnja)

Graf $G(p,\ell)$ je Ramanujanov.

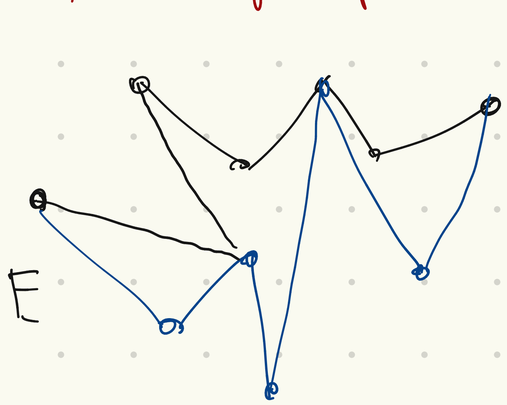
matrica susjedstva ovog grafa (tzv. Brandtova matrica) opisuje djelovanje ℓ-tog Heckeovog operatora na prostoru kasp formi težine 2 i nivoa p pa ograde na svojstvene vrijednosti dolaze od Ramanujan-Petersonove slutnje za modulame forme

Collision resistance – gruba analiza

↑

svojstvo hash funkcije – teško je pronaći dvije vrijednosti koje

funkcija preslikava u istu vrijednost



← dva puta duljine $n=5$ od $j(E)$ do $j(E')$

Dva ovakva puta definiraju dvije izogenije $f, g: E \to E'$ stupnja ℓ^n,

odnosno endomorfizam $\hat{g} f \in End(E)$ stupnja ℓ^{2n}.

dualna izogenija

Najbolji poznati algoritam koji računa prsten endomorfizama supersingularne e.k. E nad $\mathbb{F}_{p^2}$ je eksponencijalan u p.

Osnovni pojmovi – eliptičke krivulje

eliptička krivulja, Weierstrassova jednadžba, izogenija, stupanj izogenije,
dualna izogenija, grupovna operacija, opis izogenije preko jezgre,
broj točaka na elip. krivulji na konačnom polju (Hasseova ograda), obične
i supersingularne eliptičke krivulje, prsten endomorfizama, kvaternionska
algebra, Vélujeva formula.

1. Eliptičke krivulje

bilo koji polje

Eliptičku krivulju je projektivna nesingularna krivulja genusa 1 nad K sa specificiranom K-racionalnom točkom.

ekvivalentno je izomorfnom

Ako je $\mathrm{char}\, K \neq 2, 3$, onda se takva krivulja može zapisati u kratkom Weierstrassovom obliku (kao skup rješenja jednadžbe)

$$y^2 z = x^3 + axz^2 + bz^3 \quad \text{gdje su } a, b \in K \text{ i } 4a^3 + 27b^2 \neq 0$$

projektivna jednadžba. $(x : y : z) \in \mathbb{P}^2(K)$

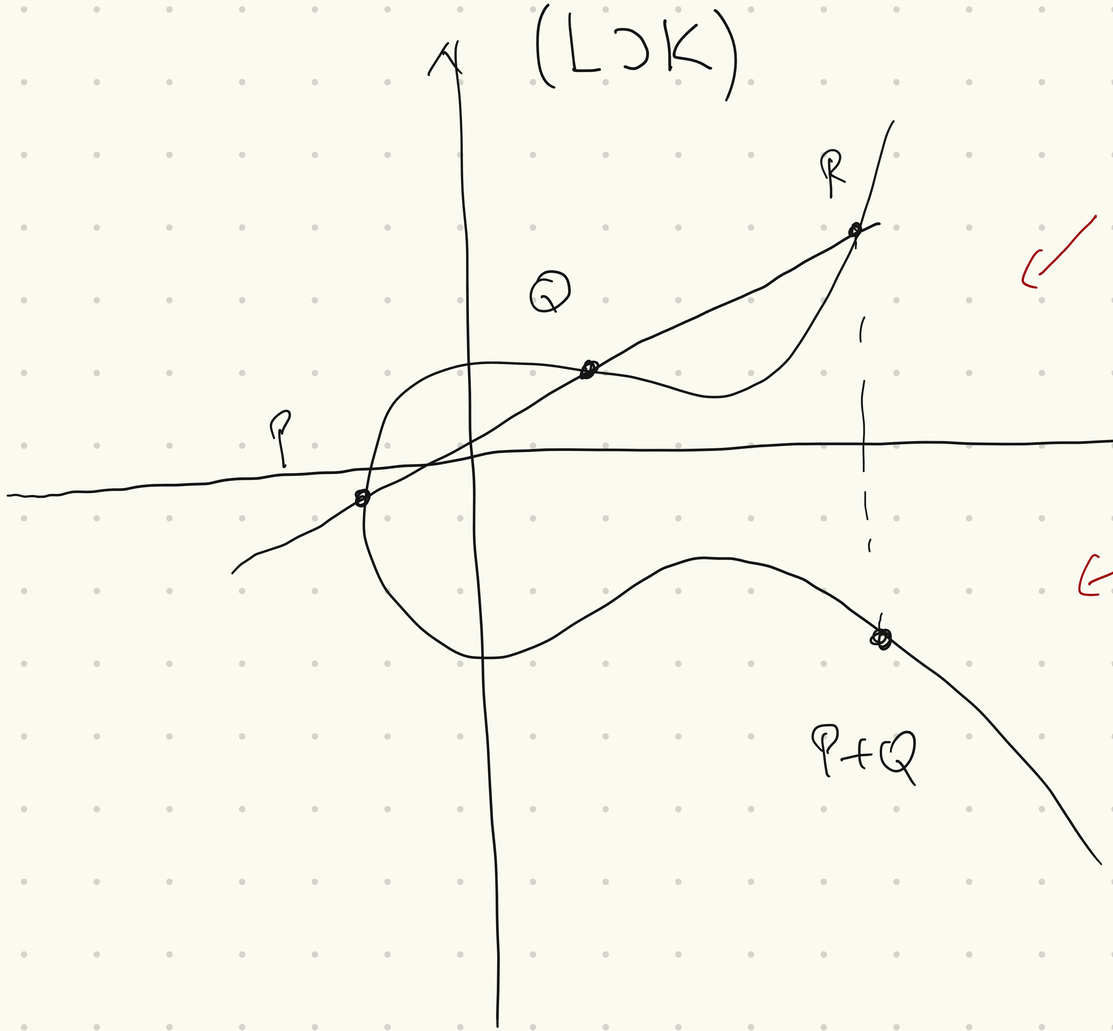
uvjet nesing.

točka u beskonačnosti $\mathcal{O}$

ima koordinate $[0 : 1 : 0]$

afina jednadžba se dobije uvrštavanjem $z = 1$ $\quad y^2 = x^3 + ax + b$

Na skupu točaka $E(L)$ možemo definirati operaciju zbrajanja.



ilustracija definicija zbrajanja za $K=\mathbb{R}$

konstrukciju točke $P+Q$ se može opisati analitički – takva definicija ima smisla za svako polje K

asocijativnost nije očita.

$(E(L), +)$ je abelova grupa

Za $m \in \mathbb{N}$, $E[m] := \{P \in E(\bar{K}) : mP = O\}$ torzija.

Propozicija (o torziji):

- ako $\operatorname{char} K \nmid m^{\in \mathbb{N}}$, onda $E[m] \simeq (\mathbb{Z}/m\mathbb{Z})^2$
- ako je $p = \operatorname{char} K > 0$, onda za svaki i $E[p^i] \simeq \mathbb{Z}/p^i\mathbb{Z}$

$$E[p] \simeq \begin{cases} \mathbb{Z}/p\mathbb{Z}, & \text{tada kažemo da je } E \text{ običan.} \\ \{O\} & \text{kažemo da je } E \text{ supersingularna} \end{cases}$$

$E[p^i] = \{O\}$

2. Preslikavanja između krivulja

Def: Izogenija φ eliptičkih krivulja $E_1 \xrightarrow{\varphi} E_2$ je morfizam algebarskih krivulja E_1 i E_2 koji preslikava istaknutu točku krivulje E_1 u istaknutu točku krivulje E_2, tj. $\varphi(\mathcal{O}_1) = \mathcal{O}_2$.

Teorem: Izogenija $E_1 \xrightarrow{\varphi} E_2$ je homomorfizam grupa $(E_1, +)$ i $(E_2, +)$.

Za eliptičku krivulju E/K s $K(E)$ definiramo njino polje funkcija. Ako je $E: y^2 = x^3 + ax + b$, onda je $K(E) = K(x, y)$.

Izogenija $\phi: E_1 \to E_2$ prirodno definira injekcija $K(E_2) \xrightarrow{\phi^*} K(E_1)$

koja funkciji $h \in K(E_2)$ pridružuje funkciju $\phi^* h = h \circ \phi \in K(E_1)$

Stupanj izogenije ϕ se definira kao stupanj proširenja

$$\deg \phi = [K(E_1) : \phi^* K(E_2)].$$

ako je ovo proširenje separabilno, inseparabilno ili

ako je $\mathrm{char} K = 0$ onda je ϕ automatski separabilna. Čisto inseparabilno, onda kažemo da je izogenija ϕ

isto tako

Teorem: Ako je ϕ separabilna onda je $\deg \phi = \#\ker \phi$.

$$\#\ker\phi = \#\{P \in E_1(\bar{K}) : \phi(P) = 0\}$$

Primjer: Ako je $E/\mathbb{F}_p : y^2 = x^3 + 1$, onda je $\phi : E \to E$ $(\phi \in \mathrm{End}(E))$

definirana s $\phi(x,y) = (x^p, y^p)$ čista inseparabilna izogenija

Vrijedi da je $\deg \phi = p$, ali $\#\ker \phi = 1$.

Frobeniusov endomorfizam.

ϕ je važan jer $E(\mathbb{F}_p) = \ker(I - \phi)$ pa primijenom

Cauchy-Schwartz nejednakosti dobivamo slijedeći teorem.

Teorem (Hasse) Neka je $E/\mathbb{F}_p$ eliptička krivulja. Standardno s

a_p označimo $a_p = p + 1 - \#E(\mathbb{F}_p)$. Vrijedi:

$$|a_p| \leq 2\sqrt{p}.$$

Separabilna izogenija $\phi : E_1 \to E_2$ je do na automorfizam krivulje E_2 jednoznačno određena svojom jezgrom $\ker \phi$.

Teorem: Neka je E_1 eliptička krivulja i neka je G konačna podgrupa od E_1 (preciznije podgrupa od $E_1(\bar{K})$).

Tada postoji jedinstvena eliptička krivulja E_2 i jedinstvena (do na autom. od E_2) separabilna izogenija $\phi : E_1 \to E_2$ takva da je $\ker \phi = G$. Pišemo $E_1/G := E_2$.

Ovaj teorem je jako koristan jer sada možemo pefljati s izogenijama u terminima teorji grupa što je puno jednostavnije nego raditi s polinomima.
Veza između grupe $G \subset E(\bar{K})$ i izogenije $E \to E/G$ je dana Vélouvim formulama.

Teorem (Vélu) Neka je $E: y^2 = x^3 + ax + b$ e.k. nad K i neka je $G \subset E(\bar{K})$ neka konačna podgrupa. Tada je separabilna izogenija $\phi: E \to E/G$ s jezgrom G dana formulom

$$\phi(P) = \left(x(P) + \sum_{Q \in G \setminus \{O\}} \left[x(P+Q) - x(Q) \right], \; y(P) + \sum_{Q \in G \setminus \{O\}} \left[y(P+Q) - y(Q) \right] \right)$$

gdje krivulja E/G ima jednadžbu $y^2 = x^3 + a'x + b'$

za neke eksplicitne a' i b'.

Još su nam važne **dualne izogenije**.

Teorem / Definicija (dualna izogenija) Neka je

$\phi : E \to E'$ izogenija stupnja m. Tada postoji jedinstvena izogenija $\hat{\phi} : E' \to E$ takva da je

zovemo ju dualna izogeniji od ϕ

$$\hat{\phi} \circ \phi = [m]_E \quad \text{i} \quad \phi \circ \hat{\phi} = [m]_{E'}.$$

množenje s m, tj. $\underbrace{P+P+\dots+P}_{m \text{ puta}}$

Vrijedi: i) $\hat{\phi}$ je definirana nad $k \iff \phi$ je definirana nad k

ii) $\deg \phi = \deg \hat{\phi}$

iii) $\hat{\phi} = \phi$

iv) $\widehat{\phi+\psi} = \hat{\phi} + \hat{\psi}$

v) $\widehat{\phi \circ \psi} = \hat{\psi} \circ \hat{\phi}$

za svaku izogeniju ψ

($k > K$, K je polje def. od E)

Napomena: $E \xrightarrow{\phi} E'$ je definirana nad k znači

a) koef. polinoma koji definiraju ϕ su u polju k

$\iff$

b) $\ker \phi \subset E(\bar{K})$ je invarijantna na djelovanje od $\mathrm{Gal}(\bar{K}/k)$

tj. $\forall \sigma \in \mathrm{Gal}(\bar{K}/k) \quad \sigma(\ker \phi) \subseteq \ker \phi$.