Prisjetimo se:

$KLPT_{\mathcal{O}_0}(I)$ - za dani lijevi $\mathcal{O}_0$-ideal računa $J \sim I$ norme ℓ

Prema lemi koju smo zadnji put dokazali problem se svodi na traženje elementa dane norme u integralnom idealu $I \subset \mathcal{O}_0$.

Ideja za traženje elementa dane norme M: uvrštavanje

Norma je kvadratna forma, npr. ako je $\langle 1, i, j, k \rangle$ standardna baza za $H = \left(\frac{a,b}{\mathbb{Q}}\right)$ i $\mathcal{O}$ red generiran s $\langle 1, i, j, k \rangle$ onda $\alpha = x + iy + jz + kw \in \mathcal{O}$ $(x, y, z, w \in \mathbb{Z})$

ima normu M ako $x^2 - ay^2 - bz^2 + abw^2 = M$. ← traženi prikaz ove jednadžbe u $\mathbb{Z}$

Ideja je uvrstiti proizvolje $z, w \in \mathbb{Z}$ u nekoj intervalu te potražiti svesh na rješenja jednadžbe $x^2 - ay^2 = M + bz_0^2 - abw_0^2 = \tilde{M}$

u našem slučaju $a = -d$ je "velik" negativan broj pa imamo jednadžbu

$$x^2 + dy^2 = \tilde{M}$$

kako efikasno naći rješenja (ako postoji)?

(idući odjeljak)

jasno je, za "slučajni" $\tilde{M}$, vjerojatnije je da rješenja postoji ako je d što manji

— zato u definiciji specijalnog reda tražimo da je red $R = \mathbb{Z}[\omega] \subset B_{\infty,p}$ minimalne diskriminante — d je minimalan

Cornacchia-in algoritam za rješavanje jednadžbe (1908)

$$x^2 + dy^2 = m \quad \text{gdje je} \quad 1 \le d < m \quad \text{i} \quad (d, m) = 1$$

Algoritam:

1°) nađite rješenje $x_0^2 \equiv -d \pmod m$

2°) Koristeći Euklidov algoritam definirajte nizove (a_n) i (r_n)

$$x_0 = a_0 \cdot m + r_0$$

$$m = a_1 \cdot r_0 + r_1$$

$$\vdots$$

$$r_i = a_{i+2} r_{i+1} + r_{i+2}$$

$$\vdots$$

sve dok

$$r_n^2 < m \le r_{n-1}^2$$

3°) Ako polazna jednadžba ima rješenja ono je oblika.

$$x = r_n \quad i \quad y = \sqrt{\frac{m - r_n^2}{d}}$$

* Zašto? (seminar!?) verižni razlomci (iclegja)

$$\Leftarrow \quad x^2 + dy^2 = m$$

$$\left(\frac{x}{y}\right)^2 \equiv -d \pmod m$$

kvadratni slobodan, $x_0^2 \equiv -d \pmod m$.

$$\Rightarrow \quad x + x_0 y \equiv 0 \ (m) \quad i \quad 0 < |x| < \sqrt{d} \quad i \quad 0 < y < \sqrt{\frac{m}{d}}$$

$\| \quad k \cdot m$

$$\Downarrow$$

$$\left| y \cdot \frac{x_0}{m} - k \right| < \frac{1}{\sqrt{m/d}} < \frac{1}{y} \quad \left(tj. \left| \frac{x_0}{m} - \frac{k}{y} \right| < \frac{1}{y^2} \right)$$

$\frac{k}{y}$ je "dobra" aproksimacija od $\frac{x_0}{m}$

Neka je dan x i $\frac{p_n}{q_n}$ konvergenta od x.

Teorem: (Farey, 1904) Neka su p i q dva relativno prosta broja t.d.

$$|q \cdot x - p| < \frac{1}{q} \quad \left(tj. \left| x - \frac{p}{q} \right| < \frac{1}{q^2} \right)$$

Tada postoji $n \in \mathbb{N}$ t.d. $\frac{p}{q} = \frac{p_n}{q_n}$ ili

$$\frac{p}{q} = \frac{p_n - p_{n-1}}{q_n - q_{n-1}}, \quad \frac{p_n + p_{n-1}}{q_n + q_{n-1}}$$

Prethodni algoritam nam je važan za algoritam **RepresentInteger$_{G_0}$(M)**

- za dani $M \in \mathbb{N}$, $M > p$ pronaći $\gamma = x + yw + zj + tjw$ t.d. $nrd(\gamma) = M$.

1. Postavi $m = \left\lfloor \sqrt{\frac{M}{p(1+q)}} \right\rfloor$ i slučajno odaberi $z, t \in [-m, m]^2$.

   Postavi $M' = M - p \cdot f(z,t)$. (Prisjetimo se: $nrd(\gamma) = f(x,y) + p \cdot f(z,t)$ gdje je $f(u,v) = nr(u + wv) = u^2 + dv^2$)

2. Ako Cornacchia(M') nema rješenja vrati se na 1

   inače $x, y = \text{Cornacchia}(M')$

3. vrati $\gamma = x + wy + j(z + wt)$

$w^2 = -q$

$j^2 = -p$

Kao i u algoritmu **Strong Approximation**:

- za dani prost broj N t.d. $\left(\frac{\ell}{N}\right) = -1$ i $c, D \in \mathbb{Z}$

izračunaj $\mu = \lambda \mu_0 + N \mu_1$ gdje je $\mu_0 = j(C + \omega D)$, $\mu_1 \in \mathcal{O}_0$

t.d. $\mathrm{nr}(\mu) = \ell^{e_1}$ za neki $e_1 \in \mathbb{N}$.

može i biti pN^3

1. odaberi $e_1 \geq pN^4$ t.d. $\dfrac{\ell^{e_1}}{p(c^2+qD^2)}$ je kvadratni ostatak modulo N

ako je prevelik, njišnji je "veliki" (više o tome kasnije)

ako e_1 nije dovoljno veliki, neće biti rješenja

— sa λ označimo njegov kvadratni korijen

2. slučajno odaberi z, t t.d. $\ell^{e_1} - pf(\lambda C + Nz, \lambda D + Nt) \equiv 0 \pmod{N^2}$

(ima N rješenja)

3. postavi $M = \dfrac{\ell^{e_1} - pf(\lambda C + Nz, \lambda D + Nt)}{N^2}$ i odredi ima li $f(x,y) = M$

rješenja (Cornacchia). Ako nema rješenja, odi na 2. korak.

4. vrati $\mu = \lambda j((c+Dw)+N(x+wy+j(z+wt))$

Q: Zašto nam treba ekstremni red G_0?

Prisjetimo se originalnog $KLPT_e(I)$ algoritma.

1. $L = \text{EquivalentPrimeIdeal}(I)$; $L = \chi_I(\delta)$ za neki $\delta \in I$, $N = nr(I)$. ← prost.
2. $\gamma = \text{RepresentInteger}_{G_0}(Ne^{e_0})$ za neki $e_0 \in \mathbb{N}$ ← normalni oblik
3. $(C_0:D_0) = \text{IdealModConstraint}(L,\gamma)$ $\left(\mu_0 = \frac{d}{dj}((C_0+wD_0) \text{ i } \gamma\mu_0 \in I\right)$ ← specijalna struktura uhvaćena rješavanjem jednadžbi.
4. $\nu = \text{StrongApproximate}_e(N,C_0,D_0)$; $\beta = \gamma\nu$; $nr(\beta) = N \cdot e^e$ za neki e. i $\beta \in I$

ideja: potraži ν oblika $\nu = \lambda \cdot \mu_0 + N\mu_1$ (λ: skalar; μ_1: $nr(\mu_1)$; $\in G_0$)

zašto tog oblika? zato što $\gamma(\lambda\cdot\mu_0 + N\cdot\mu_1) \in I$ za svaki λ,μ_1

jer $N\mathcal{O}_0 \subseteq I$ (jer je $\operatorname{mr}(I)=N$)

zašto? vanjski oprezniko

Dakle, želimo pronaći $\lambda\in\mathbb{Q}$ i $\mu_1\in\mathcal{O}_0$ t.d. $\operatorname{mr}(\lambda\mu_0 + N\mu_1) = \ell^e$ (*)

$j((z_0+D_0w)$
$\|$
kako zahtijevamo da je $\mu_0\in jR$

jednadžbu (*) rješavamo tako

da u $\mu_1 = x_0 + wy_0 \vee j(z_0+t_0w)$

slučajno odaberemo z_0 i to te jednadžbu (koristeći ortogonalnost $R \perp jR$ iz def.)

rješavamo (ovrmachia-in algoritmom (arsente se da je to ono što radimo u prethodnom algoritmu).

teško analizirati osim ako $\lambda\mu_0 \perp N\mu_1$

$\Rightarrow$ tada je $\operatorname{mr}(\lambda\mu_0 + N\mu_1) = \operatorname{mr}(\lambda\mu_0) + \operatorname{mr}(N\mu_1)$

(originalni)

Koji je nedostatak KLPT algoritma? Opišimo identifikacijski protokol u kojim se koristi.

setup: P, E_0/F_p s.s. s poznatim prstenom $End(E_0) \simeq R_0$ koji je specijalan red; D_c glatki broj oko λ bitova i $D = 2^e$

gdje je e veći od dijametra grafa supers. 2-izogenija

Da bi dokazao znanje o tajni γ dokazatelj (prover) pokreće sljedeći protokol s verifikatorom (verifier)

tajna izogenija ...

keygen: odaberi slučajan šetnju $\tau : E_0 \to E_A$ koju vodi do eliptičke krivulje E_A. E_A je javni ključ dok je τ tajni ključ.

protokol

obavezivanje: dokazatelj generira slučajnu (tajnu) izogenijsku šetnju $\gamma : E_0 \to E_1$ i pošalje E_1 verifikatoru.

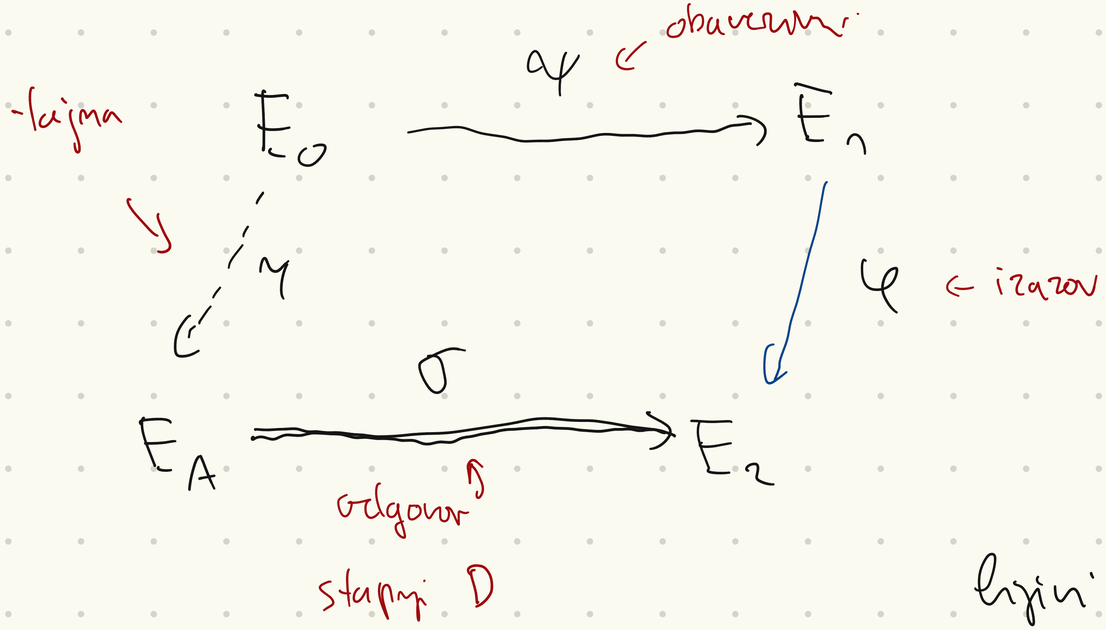
izazov: verifikator šalje opis cikličke izogenije $\varphi : E_1 \to E_2$ stupnja D_c dokazatelju

kako ju konstruirati? kasnije...

odgovor: iz izogenije $\varphi \circ \gamma \circ \hat{\tau} : E_A \to E_2$ dokazatelj konstruira novu izogeniju $\sigma : E_A \to E_2$ stupnja D s.d. $\hat{\varphi} \circ \sigma$ cikličku i šalje σ verifikatoru.

Verifikacija: verifikator prihvaća dokaz tj. odgovor ako je

σ izogenija stupnja D iz E_A u E_2 i $\hat{\varphi} \circ \sigma$ je cikličke



Kako dokazitelj generira σ?

prvi pokušaj:

* pretvori izogeniju

$\varphi \circ \gamma \circ \hat{\gamma} : E_A \to E_2$ u

lijevi $\mathcal{O}_A \simeq End(E_A)$ ideal te primitivni KLPT

algoritam koji vrati ekvivalentan ideal norme 2^e.

Taj ideal "pretvori" u izogeniju $\sigma : E_A \to E_2$ stupnja 2^e.

Što je problem? Moramo prvo objasniti kako alg. funkcionira kad znamo $\mathcal{O}_A$ nije specijalan.

Neka je $I \subset B_{p,\infty}$ općenit lijevi $\mathcal{O}_L(I)$ i desni $\mathcal{O}_R(I)$ ideal.

Kako KLPT algoritam primijeniti na I?

a) Definirajmo dva ideala I_1 i I_2 t.d. $\mathcal{O}_L(I_1) = \mathcal{O}_0$, $\mathcal{O}_R(I_1) = \mathcal{O}_L(I)$
(konstruirajmo)
i $\mathcal{O}_L(I_2) = \mathcal{O}_0$, $\mathcal{O}_R(I_2) = \mathcal{O}_R(I)$ (kako ih možemo izračunati?)

b) Primijenimo KLPT algoritam na I_1 i I_2 (možemo jer su to lijevi $\mathcal{O}_0$-ideali gdje je $\mathcal{O}_0$ specijalan)
te dobijemo ekvivalentne lijeve $\mathcal{O}_0$-ideale J_1 i J_2 čije su norme potencije od 2.

c) Po Deuringovoj korespondenciji ideali J_1 i J_2 odgovaraju izogenijama (stupanj $= 2^k$)
$E_0 \to E_A$ i $E_0 \to E_2$ koje nam onda daju izogeniju $E_A \to E_0 \to E_2$
traženog stupnja (potencija od 2).

Što je ovdje problem? Izogenija σ (zbog nyine konstrukcije) odaje dio puta $E_A \to E_0$ što otkriva informaciju o tajni $\tau: E_0 \to E_A$ (pokazao je u [25] da je to "ekvivalentno" otkrivanju te tajne).

Želimo da protokol ima **zero-knowledge** svojstvo i zbog toga nam treba generalizacija KLPT algoritma.

Par riječi o konceptu **zero-knowledge proof** (protocol):

U grubo, to je metoda kojom dokazitelj dokaže verifikatoru da posjeduje neku tajnu (u naše slučaju da zna izgovoriti) bez da išta otkrije o toj tajni (zato se zove zero-knowledge)

Primjer: Kako dokazati prijatelju koji je slijep na boje da su dvije kuglice različitih boja (recimo zelena i crvena)? ...

Protokol mora imati tri svojstva:

1. **potpunost** (completeness) ako dokazitelj zna tajnu, onda to može dokazati
2. **smislenost** (soundness) ako ne zna, onda ne može prevariti
3. **nula-znanje** (zero-knowledge) verifikator u procesu ne saznaje ništa o tajni

Primjeri: • identifikacija

• Zcoin (block chains)

• ....

Generalizacija KLPT algoritma

Neka je $\mathcal{O}_0$ i dalje specijalan ekstreman red te $\mathcal{O}$ proizvoljan maksimalan red. Želimo generalizirati KLPT algoritam na proizvoljne ulazne $\mathcal{O}$-ideale, ali i dalje želimo raditi u $\mathcal{O}$. Zato promatramo red $\mathcal{I} = \mathcal{O} \cap \mathcal{O}_0$.

← presjek dva maksimalna reda nazivamo Eichlerov red

Natrag na teoriju... **Eichlerovi redovi**

Pretpostavimo da je $B = G_0 \cap G$ gdje su G_0 i G (dodatna pretpostavka)

povezani idealom I norme $nr(I)$ t.d. $\forall n \in \mathbb{N}_{n>1}\ I \nmid n G_L(I)$

↑ to znači:

ovaj uvjet se često javlja i ekvivalentan je tome

$G_L(I) = G_0$ i

$G_R(I) = G$

G_0 G

\ /

I

da je pripadna (Deuring) izogenija $\varphi_I : E_0 \to E$ cikličke

$End(E_0) \simeq G_0$

$End(E) \simeq G$

po definiciji $\ker \varphi_I = \{ P \in E(\overline{\mathbb{F}}_{p^2}) : f(P) = 0 \ \ \forall f \in I \}$

dakle $I \subset n G_L(I)$ za neki $n \in \mathbb{N}_{n>1}$ onda $E[n](\overline{\mathbb{F}}_{p^2}) \subset \ker \varphi_I$

pa φ_I ne može biti cikličke...

U tom slučaju $[\mathcal{O} : \mathfrak{I}] = [\mathcal{O}_K : \mathfrak{D}] = nr(I)$

↑ kako se definirana norma ideala i čiji kojih ima svojstva? I je bilo koji $\mathcal{O}$-ideal ($I \subset \mathcal{O}$)

- $nr(I) := \gcd(\{nr(\alpha) : \alpha \in I\}) = \sqrt{[\mathcal{O} : I]}$

↑ zašto?

- $I \bar{I} = nr(I)\,\mathcal{O}$
- $nr(IJ) = nr(I)\,nr(J)$
- $nr(\alpha) = nr(\alpha\mathcal{O}) = nr(\mathcal{O}\alpha)$

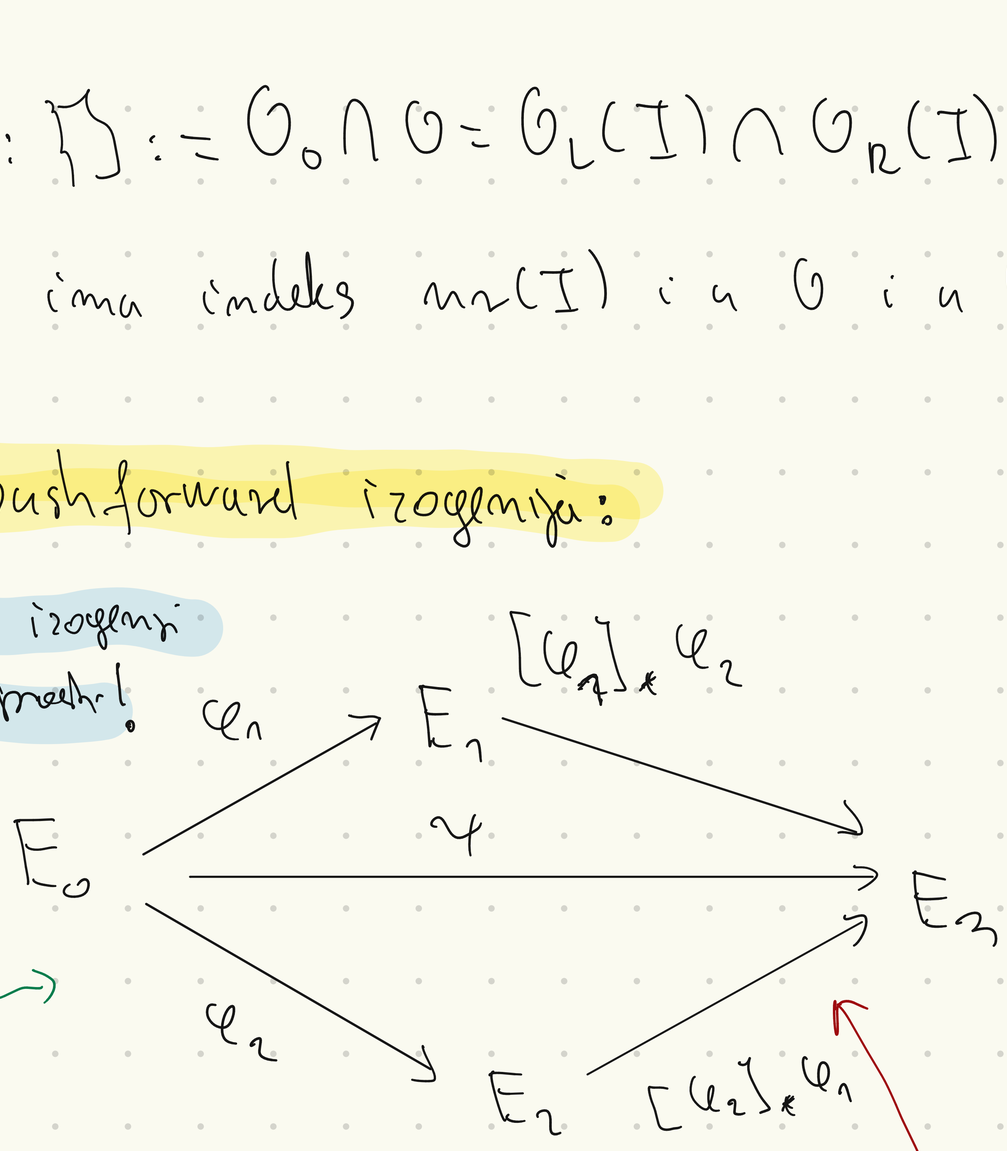
Propozicija : $\{\} := \mathcal{O}_0 \cap \mathcal{O} = \mathcal{O}_L(I) \cap \mathcal{O}_R(I) = \mathbb{Z} + I$

dokaz: $\mathbb{Z}+I$ ima indeks $nr(I)$ i u $\mathcal{O}$ i u $\mathcal{O}_0$ pa tvrdnja slijedi (d.z.)

Pullback i pushforward izogenija:

stupnjevi N_1 i N_2 izogenija φ_1 i φ_2 su relativno prosti!

↑ pretpostavka



SIDH

(E_3 je zajednički faktor)

pushforward:

$$\ker\left([\varphi_2]_* \varphi_1\right) = \varphi_2\left(\ker(\varphi_1)\right)$$

$$\ker\left([\varphi_1]_* \varphi_2\right) = \varphi_1\left(\ker(\varphi_2)\right)$$

$$\Downarrow$$

$$\psi = [\varphi_2]_* \varphi_1 \circ \varphi_2 = [\varphi_1]_* \varphi_2 \circ \varphi_1$$

$\Leftarrow$ dijagram komutira : $\ker\psi = \ker\varphi_1 \vee \ker\varphi_2$

Pullback se definira preko dualne izogenije: Ako su dani

$\varphi_1 : E_0 \to E_1$ i $\varphi_2 : E_1 \to E_m$ (stupnjevi su relativno prosti) onda

$[\varphi_1]^* \varphi_2 = [\hat{\varphi}_1]_* \varphi_2$ (vrijedi $\varphi_2 = [\varphi_1]^* [\varphi_1]_* \varphi_2$)

Definirajmo ova dva pojma i na idealima (preko Deuringove korespodencije)

$[I]_* J := \overline{I}[\varphi_J]_* \varphi_I$ koji odgovara izogeniji $[\varphi_J]_* \varphi_I$.

Slično i za pullback.

Na nicon ideala imamo jednostavan opis pullbacka.

Uz oznake kao i ranije neka je $I_1 = I_{e_1}$, $I_2 = I_{e_2}$, $J_1 = [I_2]_* I_1$

$J_2 = [I_1]_* I_2$ i $K = I_4$.

Lema: Ako je $\gcd(N_1, N_2) = 1$ ideali J_1, J_2 i K su dobro definirani i vrijede:

(i) $K = I_1 \cap I_2$

(ii) $J_2 = I_1^{-1}(I_1 \cap I_2)$, $J_1 = I_2^{-1}(I_1 \cap I_2)$

(iii) $I_2 = [I_1]^* J_2 = I_1 J_2 + N_2 \mathcal{O}_0$

← jednostavan opis pullbacka