Uvod u aritmetiku eliptičkih krivulja

Frobeniusov element (skica) - 23. lekcija

Galoisova grupa $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ za matematiku je još uvijek zagonetna i daleko smo od njena eksplicitnog opisa. Jedan od očitih elemenata te grupe jest kompleksno konjugiranje (koje je restrikcija standardnog kompleksnog konjugiranja na polju kompleksnih brojeva, koje se može karakterizirati i time da ostavlja na miru polje realnih brojeva). Sjetimo se da, uz standardno upotpunjenje polja racionalnih brojeva do polja realnih brojeva, imamo i p-adska upotpunjenja, za svaki prosti broj p. Frobeniusovi elementi bit će p-adski analogoni kompleksnog konjugiranja i imat će važnu ulogu u aritmetici. Mi nećemo sustavno razvijati tu analogiju, već ćemo do tog pojma doći od **Frobeniusova automorfizma** konačnog polja (koji onda definira i Frobeniusov automorfizam eliptičke krivulje nad konačnim poljem), preko **Frobeniusovih automorfizama** konačnog abelovog proširenja od $\mathbf{Q}$ i **Frobeniusovih elemenata** (bilo kakvih) konačnih Galoisovih proširenja od $\mathbf{Q}$.

Frobeniusov automorfizam konačnog polja.
Podsjetimo da je $\mathbf{F}_p$ minimalno polje karakteristike p (prost broj) i da ima p elemenata, a možemo ga realizirati kao skup ostataka modulo p ili kao kvocijentni prsten $\mathbf{Z}/p\mathbf{Z}$. Ako fiksiramo jedno algebarsko zatvorenje $\bar{\mathbf{F}}_p$ od $\mathbf{F}_p$, onda za svaki prirodni broj n postoji točno jedno podpolje od $\bar{\mathbf{F}}_p$ koje ima p^n elemenata. To je polje

$$\mathbf{F}_{p^n} = \{x \in \bar{\mathbf{F}}_p : x^{p^n} = x\}.$$

Sva su ta polja algebarska proširenja od $\mathbf{F}_p$, sva su Galoisova, i nema drugih konačnih proširenja od $\mathbf{F}_p$ koji su u $\bar{\mathbf{F}}_p$ (drugim riječima, za svaki n postoji jedinstveno proširenje stupnja n). Takodjer se vidi:

$$\mathbf{F}_{p^m} \subseteq \mathbf{F}_{p^n} \text{ akko } m|n.$$

Nadalje, Galoisova grupa $\mathrm{Gal}(\mathbf{F}_{p^n}/\mathbf{F}_p$ je **ciklička** i generirana **Frobeniusovim automorfizmom** $Frob_p$ zadanim kao

$$Frob_p(x) := x^p.$$

Podsjetimo da je grupna operacija kompozicija, pa ako, radi jednostavnosti, pišemo σ umjesto $Frob_p$, onda je

$$\mathrm{Gal}(\mathbf{F}_{p^n}/\mathbf{F}_p = \{1, \sigma, \sigma^2, ..., \sigma^{n-1}\}$$

gdje je $\sigma^k := \sigma \circ \sigma \circ ... \circ \sigma$ (k puta), tj. $\sigma^k(x) = x^{p^k}$, za sve x.
Uočite da je fiksno polje Frobeniusova automorfizma upravo minimalno polje $\mathbf{F}_p$.
Uočite takodjer da formula za Frobeniusov automorfizam ne ovisi o n, već samo o p. Zato su $Frob_p$ za različite n uskladjeni pa je tom formulom zadan i automorfizam polja $\bar{\mathbf{F}}_p$ nad $\mathbf{F}_p$.

Frobeniusov automorfizam eliptičke krivulje.
Neka je E eliptička krivulja definirana nad poljem $\mathbf{F}_p$. Tada je formulom

$$\phi_p(x, y) := (x^p, y^p)$$

zadan morfizam $\phi_p : E \to E$ (pri tom točke od E razmatramo s koordinatama iz $\bar{\mathbf{F}}_p$). Dakle, ϕ_p je zadan djelovanjem Frobeniusova automorfizma na koordinatama.
Uočite da vrijedi $\phi_p(P) = P$ akko P je definirana nad $\mathbf{F}_p$.
To znači da je broj $\mathbf{F}_p$-racionalnih točaka na E jednak broju nultočaka morfizma $\phi_p - 1$, gdje 1 označava morfizam identiteta; ta je činjenica polazna za dokaz Hasse-Weilova teorema.

Frobeniusov automorfizam konačnog abelova proširenja od $\mathbf{Q}$.
Neka je $K/\mathbf{Q}$ konačno abelovo proširenje. To znači da je ono konačnog stupnja (posebice, tada je ono i algebarsko), Galoisovo i da je Galoisova grupa G abelova. Pokazat će se da za svaki prosti p (osim njih konačno mnogo - koji se granaju u K) jednoznačno možemo definirati automorfizam σ iz G koji ima jaku vezu s Frobeniusovim automorfizmom odredjenog proširenja od $\mathbf{F}_p$, zato ćemo taj σ takodjer zvati Frobeniusovim automorfizmom i označavati $Frob_p$.
Kako je G konačna grupa, a prostih brojeva ima beskonačno mnogo, to znači da će bar jedan σ biti $Frob_p$ za beskonačno mnogo p. Teorem Čebotareva govori da je svakom σ tako pridruženo "jednako mnogo" prostih brojeva, tj. da za svaki σ skup svih onih prostih brojeva p za koje je $\sigma = Frob_p$ čini $|G|$-ti dio skupa svih prostih brojeva (zanemarujući konačno mnogo onih koji se granaju. To ćemo preciznije formulirati poslije. Započet ćemo s jednim

primjerom.

Primjer 1. Neka je $K = \mathbf{Q}(i) = \{a + bi : a, b \in \mathbf{Q}\}$ polje Gaussovih brojeva. To je proširenje 2. stupnja, s Galoisovom grupom $G = \{1, \sigma\}$ gdje je σ kompleksno konjugiranje, tj. $\sigma(a + bi) = a - bi$.
Uz polje Gaussovih brojeva prirodno ide prsten cijelih Gaussovih brojeva $\mathbf{Z}[i] = \{a + bi : a, b \in \mathbf{Z}\}$, koji treba gledati kao prirodno proširenje prstena cijelih brojeva $\mathbf{Z}$. Prsten $\mathbf{Z}[i]$ ima jednoznačnu faktorizaciju koja se može opisati ovako:
(i) ako je $p = 3$ modulo 4, onda je p prost i u $\mathbf{Z}[i]$. Kažemo da je p inertan.
(ii) (i) ako je $p = 1$ modulo 4, onda je $p = (u + vi)(u - vi)$ umnožak dvaju prostih u $\mathbf{Z}[i]$, medjusobno kompleksno konjugiranih. Kažemo da se p cijepa.
(iii) $2 = i(1-i)^2$ je umnožak od kvadrata od $1-i$ koji je prost u $\mathbf{Z}[i]$ i broja i koji je invertibilan u $\mathbf{Z}[i]$ (još su invertibilni ± 1 i $-i$). Kažemo da se 2 grana.
Na primjer $3, 7, 11, 19, 23, ...$ ostaju prosti u $\mathbf{Z}[i]$, dok je
$5 = (2 + i)(2 - i),\ 13 = (3 + 2i)(3 - 2i),\ 17 = (4 + i)(4 - i)...$
Podsjetimo da je kvocijent $\mathbf{Z}/p\mathbf{Z}$ minimalno konačno polje $\mathbf{F}_p$.
Uočite da je za inertne p analogni kvocijentni prsten $\mathbf{Z}[i]/p\mathbf{Z}[i]$ kvadratno proširenje od $\mathbf{F}_p$.
Naime, taj je prsten izomorfan prstenu $\mathbf{F}_p[\eta]$ uz $\eta^2 + 1 = 0$, koji se ostvaruje tako da se klasi od $a + bi$ pridruži $\bar{a} + \bar{b}\eta$, gdje je $\bar{a} := a$ modulo p itd.
Kako je $p = 3$ modulo 4, -1 nije kvadrat u $\mathbf{F}_p$ pa je $X^2 + 1$ ireducibilan polinom nad $\mathbf{F}_p$, tj. prsten $\mathbf{F}_p[\eta]$ je polje drugog stupnja nad $\mathbf{F}_p$, pa je izomorfan polju $\mathbf{F}_{p^2}$.
Sad imamo Frobeniusov automorfizam $Frob_p : x \mapsto x^p$ proširenja $\mathbf{F}_{p^2}/\mathbf{F}_p$, koje ima Galoisovu grupu $\{1, Frob_p\}$, koja je pak prirodno izomorfna Galoisovoj grupi $\{1, \sigma\}$ proširenja $K/\mathbf{Q}$. Naime, σ preslikava prsten cijelih brojeva u sebe, takodjer ostavlja na miru prosti element p, pa i pripadni ideal $p\mathbf{Z}[i]$, zato se djelovanje od σ može prenijeti na kvocijent $\mathbf{Z}[i]/p\mathbf{Z}[i]$ prema formuli

$$\sigma(\overline{a + bi} = \overline{\sigma(a + bi)}$$

Zato je $\sigma(\bar{a} + \bar{b}\eta) = \overline{a - bi} = \bar{a} - \bar{b}\eta = (\bar{a} + \bar{b}\eta)^p$. Naime, kako je $eta^2 = -1$ i $p = 3$ modulo 4, vrijedi $(\bar{a} + \bar{b}\eta)^p = \bar{a}^p + \bar{b}^p\eta^p = \bar{a} + \bar{b}(-1)$. Dakle, pri tom prirodnom izomorfizmu σ prelazi u $Frob_p$ (kako je jedino i moguće), pa zato definiramo $\sigma = Frob_p$ za sve $p = 3$ modulo 4. Naravno, pri tom izomorfizmu, identitet u G prelazi u identitet za konačno polje.
Ako je pak $p = 1$ modulo 4, tj. $p = (u + vi)(u - vi)$, onda je

$\mathbf{Z}[i]/(u+vi)\mathbf{Z}[i] \cong \mathbf{F}_p \cong \mathbf{Z}[i]/(u-vi)\mathbf{Z}[i]$
jer je sad -1 kvadrat u $\mathbf{F}_p$. Zato je sad pripadni Frobeniusov automorfizam identitet (proširenje je stupnja 1), pa je $Frob_p = 1$ za sve $p = 1$ modulo 4. Ako želimo uspostaviti analogiju s prvim slučajem (kad je p inertan), sad σ prosti element $u+vi$ prebacuje u $u-vi$ (i obratno), dok ih na miru ostavlja samo identitet 1, pa je σ odmah isključen iz razmatranja.

Općenito, neka je K konačno abelovo proširenje stupnja n od $\mathbf{Q}$ i neka je G pripadajuća Galoisova grupa. Neka je O_K pripadni prsten cijelih brojeva. Taj prsten ne mora (i u pravilu nije) biti s jednoznačnom faktorizacijom. Umjesto toga jednoznačna je faktorizacija na proste ideale. Posebno za glavne ideale pO_K u O_K generirane prostim brojevima p vrijedi (za sve osim konačno mnogo njih koji se granaju)
$pO_K = \mathcal{P}_1\mathcal{P}_2...\mathcal{P}_m$, umnožak na **različite** proste ideale. Pri tom je
$O_K/\mathcal{P}_1 \cong O_K/\mathcal{P}_2 \cong ... \cong O_K/\mathcal{P}_m \cong \mathbf{F}_p^f$,
za neki prirodni broj f koji se zove indeks inercije od p i vrijedi $mf = n$.
Ako je $f = 1$ onda kažemo da se p potpuno rastavlja (cijepa), a ako je $f = n$, onda p ostaje prost (inertan). Za svaki od ovih $\mathcal{P}_j$ kažemo da dijeli pO_K i pišemo $\mathcal{P}_j | pO_K$ (odnosno da je iznad p jer je $\mathcal{P}_j \cap \mathbf{Z} = (p)$ - ideal u $\mathbf{Z}$ generiran s p).
Ovi $\mathcal{P}_j$ medjusobno su povezani, kako ćemo ubrzo vidjeti. Ako je $\mathcal{P}$ neki prost ideal u O_K i $\sigma \in G$ automorfizam od K, onda je skup

$$\sigma(\mathcal{P}) := \{\sigma(x) : x \in \mathcal{P}\}$$

opet prost ideal.
Fiksirajmo načas jedan prost broj p i jedan prosti ideal $\mathcal{P}$ iznad p. Neka je $O_K/\mathcal{P} \cong \mathbf{F}_p^f$ (*), tj. f je indeks inercije u p. Definirajmo:
$D_\mathcal{P} = \{\sigma \in G : \sigma(\mathcal{P}) = \mathcal{P}\}$ - grupa rastavljanja u $\mathcal{P}$ (dekompozicijska grupa)
Postoji prirodni surjektivni homomorfizam $D_\mathcal{P} \to \mathrm{Gal}(\mathbf{F}_p^f/\mathbf{F}_p)$. Naime, preko izomorfizma (*), svaki $\sigma \in D_\mathcal{P}$ djeluje na konačno polje preko

$$\sigma(u \ mod \ \mathcal{P}) := \sigma(u) \ mod \ \mathcal{P}$$

za svaki $u \in O_K$.
Taj je homomorfizam izomorfizam ako se p ne grana i tada postoji jedinstveni automorfizam iz G (preciznije iz dekompozicijske grupe) koji se preslikava u $Frob_p$ i njega nazivamo Frobeniusovim automorfizmom u $\mathcal{P}$ - oznaka $Frob_\mathcal{P}$. Lako se vidi da $D_\mathcal{P}$ pa tako niti $Frob_\mathcal{P}$ ne ovise o izboru prostog ideala iznad

p, pa je tako jednoznačno odredjen Frobeniusov automorfizam u p - oznaka $Frob_p$ (kao i za konačna polja).
Iz gornjeg opisa slijedi da je $Frob_p$ jednoznačno odredjeno kao:

$$Frob_p(u) = u^p \text{ modulo } \mathcal{P}$$

za neki (pa onda za svaki) $\mathcal{P}$ iznad p.

Primjer 2. (peti korijeni iz jedinice).
Neka je $K := \mathbf{Q}(\mu_5)$ polje generirano (bilo kojim) primitivnim petim korijenom iz jedinice, na pr. neka je $\mu_5 = e^{\frac{2\pi i}{5}}$. To je polje Galoisovo (jer sadrži i ostale pete korijene iz jedinice, koje su potencije od μ_5). Minimalni polinom je $f(X) := X^4 + X^3 + X^2 + X + 1$ (dobije se dijeljenjem polinoma $X^5 - 1$ s $X - 1$), pa je proširenje stupnja $n = 4$. Galoisova grupa je ciklička reda 4 izomorfna grupi $\{1, 2, 3, 4\}$ uz množenje modulo 5 (uočite da su izvodnice brojevi 2 i 3), tj. $\text{Gal}(K/\mathbf{Q}) = \{1, \sigma, \sigma^2, \sigma^3\}$, gdje je, na primjer, $\sigma(\mu_5) = \mu_5^2$ (drugi je izbor da bude $\sigma(\mu_5) = \mu_5^3$). Sad je $\sigma^2(\mu_5) = \sigma(\mu_5^2) = \mu_5^4$ itd.
Pokazuje se da je tu prsten cijelih brojeva $O_K = \mathbf{Z}[\mu_5]$, grana se jedino broj 5.
(I) Prosti brojevi p za koje je $Frob_p = 1$, tj. $f = 1$ su upravo oni za koje se pO_K rastavlja na umnožak četiri različita prosta (jer mora biti $m = 4$) i ako je $\mathcal{P}$ jedan od tih faktora, onda je

$$pO_K = \mathcal{P}\sigma(\mathcal{P})\sigma^2(\mathcal{P})\sigma^3(\mathcal{P})$$

Prema teoremu Čebotareva ima $\frac{1}{4}$ takvih prostih p. To su inače svi oni p za koje se minimalni piolinom f modulo p rastavlja na različite linearne faktore.
(II) Prosti brojevi p za koje je $Frob_p = \sigma$, tj. $f = 4$, jer σ generira grupu 4-tog reda, imaju svojstvo da je pO_K prost (odnosno da je f ireducibilan modulo p). Analogno je s onim p za koji je $Frob_p = \sigma^3$ (jer je i σ_3 izvodnica. Prema teoremu Čebotareva ima $\frac{2}{4} = \frac{1}{2}$ takvih prostih p.
(III) Ostaju prosti p za koje je $Frob_p = \sigma^2$, tj. $f = 2$, jer σ^2 generira grupu 2-gog reda. Oni imaju svojstvo da je

$$pO_K = \mathcal{Q}\sigma(\mathcal{Q})$$

gdje je $\mathcal{Q}$ jedan od prostih djelitelja (naime 1 i σ^2 čine dekompozicijsku grupu i oni fiksiraju Q, dok ga σ ne fiksira; uočite i to da je $\sigma^3(Q) = \sigma(Q)$). Takvih p ima jedna četvrtina i to su upravo oni za koje se f modulo p rastavlja na

umnožak dvaju različitih ireducibilnih polinoma drugog stupnja.
Napomenimo da je u ovomu slučaju O_K prsten s jednoznačnom faktorizacijom, pa se gornji rastavi mogu napisati pomoću prostih brojeva umjesto ideala (ali to ne činimo).
Dirichletov teorem o prostim projevima u aritmetičkim nizovima vodi do preciznije tvrdnje: u (I) spadaju oni prosti koji su kongruentni 1 modulo 5, u (II) oni kongruentni 2 odnosno 3, a u (III) oni kongruentni 4 modulo 5.
Na primjer, $19 = 4$ modulo 5, a

$$X^4 + X^3 + X^2 + X + 1 = (X^2 + 5X + 1)(X^2 - 4X + 1) \text{ modulo } 5$$

je rastav na ireducibilne faktore, što potvrdjuje da je $f = 2$.

Frobeniusov element konačnog Galoisova proširenja.
Za razliku od abelova proširenja, tu Frobeniusov element u p (za nerazgranati p) nije dobro definiran, već samo njegova klasa konjugiranosti. Podsjetimo, ako je G neka grupa i $h \in G$, onda je klasa konjugiranosti od h, prema definiciji, $\{g^{-1}hg : g \in G\}$. Očito je da su klase konjugiranosti u abelovoj grupi jednočlane (i obratno). Općenito, klase konjugiranosti čine particiju grupe na disjunktne podskupove - biti u istoj klasi konjugiranosti je relacija ekvivalencije).

Primjer 3. Klase konjugiranosti u $\mathbf{S_3}$.
Kako je poznato, simetrična grupa S_3 izomorfna je grupi

$$\{1, \sigma, \sigma^2, \tau, \sigma\tau, \sigma^2\tau\}$$

gdje je $\sigma^3 = \tau^2 = 1$ i $\tau\sigma = \sigma^2\tau$
(odakle onda slijedi i da je $\tau\sigma^2 = \sigma\tau$; takodjer vrijedi $(\sigma\tau)^2 = (\sigma^2\tau)^2 = 1$).
Ova grupa ima tri klase konjugiranosti.
Klasa konjugiranosti od 1 je $\{1\}$ (to je uvijek tako).
Klasa konjugiranosti od σ je $\{\sigma, \sigma^2\}$ jer je $\tau^{-1}\sigma\tau = \tau\sigma\tau = \sigma^2\tau\tau = \sigma^2$ (a daljnjim se konjugiranjem ništa novo ne dobiva - provjerite).
Klasa konjugiranosti od τ je $\{\tau, \sigma\tau, \sigma^2\tau\}$ jer je, na primjer, $\sigma^{-1}\tau\sigma = \sigma^2\tau\sigma = \sigma^4\tau = \sigma\tau$ (slično se dobije i da je $\sigma^2\tau$ u klasi).

Frobeniusov element za konačna neabelova proširenja.
Neka je $K/\mathbf{Q}$ Galoisovo proširenje stupnja n s Galoisovom grupom G (općenito neabelovom) i prstenom cijelih brojeva O_K. Fiksirajmo neki prost broj p koji

se ne grana u K. Tada je glavni ideal pO_K umnožak različitih prostih ideala i neka je $\mathcal{P}$ jedan od njih.
Kao i u abelovom slučaju definiramo grupu razlaganja $D_{\mathcal{P}}$ u $\mathcal{P}$ (koje se sastoje od onih $g \in G$ za koje je $g(\mathcal{P}) = \mathcal{P}$ i pripadno konačno polje $\mathbf{F}_{p^f} \cong O_K/\mathcal{P}$. Kao i prije, $D_{\mathcal{P}}$ je ciklička reda f i imamo prirodni izomorfizam izmedju $D_{\mathcal{P}}$ i $\mathrm{Gal}(\mathbf{F}_{p^f}/\mathbf{F}_p)$ koja je generirana Frobeniusovim automorfizmom $Frob_p : x \mapsto x^p$, pa postoji jedinstven element u $D_{\mathcal{P}}$ koji pri tom izomorfizmu korespondira $Frob_p$ pa ga označavamo kao $Frob_{\mathcal{P}}$, odredjen je kongruencijom

$$Frob_{\mathcal{P}}(u) = u^p \text{ modulo } \mathcal{P}.$$

Ako je $\mathcal{Q}$ neki drugi prosti ideal iznad p, onda postoji $g \in G$ tako da bude $\mathcal{Q} = g(\mathcal{P})$ i tada je

$$D_{\mathcal{Q}} = gD_{\mathcal{P}}g^{-1}$$

i prema tomu i

$$Frob_{\mathcal{Q}} = gFrob_{\mathcal{P}}g^{-1},$$

tj. Frobeniusovi automorfizmi u različitim prostim idealima iznad p medjusobno su konjugirani. Takodjer, indeks inercije f jednak je za sve proste ideale iznad p, i ako se pO_K rastavlja na umnožak m prostih faktora, onda je

$$mf = n \ (**)$$

Uočite, takodjer, da vrijedi čim je $\mathcal{P}$ iznad p onda je i $g(\mathcal{P})$ iznad p za svaki $g \in G$. Zato su svi elementi iz klase konjugiranosti od $Frob_{\mathcal{P}}$ Frobeniusovi elementi u nekim prostim idealima nad p. To omogućuje definiciju:

Frobeniusovim elementom $Frob_p$ u prostom broju p zovemo klasu konjugiranosti Frobeniusova automorfizma $Frob_{\mathcal{P}}$ za bilo koji prosti ideal $\mathcal{P}$ iznad p (i ona ne ovisi o tom izboru).

Teorem Čebotareva.
Neka je K konačno Galoisovo proširenje od $\mathbf{Q}$ stupnja n s Galoisovom grupom G. Neka je $A \subset G$ podskup zatvoren na konjugiranje (na primjer, klasa konjugiranosti). Tada je

$$\mu(\{p : \ p \text{ prost i } Frob_p \subseteq A\} = \frac{\mathrm{card}A}{n},$$

pri čemu je μ **Dirichletova gustoća**, definirana za podskupove skupa prostih brojeva kao

$$\mu(B) := \lim_{X\to\infty} \frac{\mathrm{card}(\{p : p \le X\} \cap B)}{\mathrm{card}\{p : p \le X\}}$$

(ako limes postoji).

Primjer 4. Frobeniusovi elementi u $\mathrm{Gal}(\mathbf{Q}(\sqrt[3]{2}, \rho)/\mathbf{Q})$.
Poznato je da je polje $K := \mathbf{Q}(\sqrt[3]{2}, \rho)$, gdje je $\rho = e^{\frac{2\pi i}{3}}$, Galoisovo stupnja 6, s Galoisovom grupom izomorfnom S_3 (pa prema tomu nije abelovo). Takodjer u K se granaju 2 i 3, pa njih izključujemo iz razmatranja.
Sjetimo se identifikacije $S_3 = \{1, \sigma, \sigma^2, \tau, \sigma\tau, \sigma^2\tau\}$ i klasa konjugiranosti $\{1\}$, $\{\sigma, \sigma^2\}$ i $\{\tau, \sigma\tau, \sigma^2\tau\}$. Sad imamo:
(I) $Frob_p = 1$ akko $f = 1$, tj. pO_K se potpuno rastavlja (na 6 prostih faktora), i ako je $\mathcal{P}$ jedan od prostih faktora onda je

$$pO_K = \mathcal{P}(\sigma\mathcal{P})(\sigma^2\mathcal{P})(\tau\mathcal{P})(\sigma\tau\mathcal{P})(\sigma^2\tau\mathcal{P}).$$

Teorem Čebotareva kaže da ima šestina takvih prostih p.
(II) $Frob_p = \{\sigma, \sigma^2\}$ akko je $f = 3$ (jer σ generira cikličku grupu reda 3), pa je $m = 2$ u (**), i ako je $\mathcal{P}$ jedan od faktora od pO_K onda je

$$pO_K = \mathcal{P}(\tau\mathcal{P})$$

(uočite da je $\tau\mathcal{P} = \sigma\tau\mathcal{P} = \sigma^2\tau\mathcal{P}$). Teorem Čebotareva kaže da ima dvije sestine takvih prostih p.
(III) $Frob_p = \{\tau, \sigma\tau, \sigma^2\tau\}$ akko je $f = 2$ (naime, svaki od tih elemenata je drugog reda) pa, ako je za $\mathcal{P}$ iznad p onda je

$$pO_K = \mathcal{P}(\sigma\mathcal{P})(\sigma^2\mathcal{P}).$$

Teorem Čebotareva kaže da ima tri šestine takvih prostih p.
Uočite da ne postoji ni jedan p za koji je pO_K prost.