Криптографија
- осми део -

доц. др Драган Ђокић

Математички факултет, Универзитет у Београду

dragan.djokic@matf.bg.ac.rs

10. - 14. март 2025.

Факторизација помоћу ЕК

Хоћемо да факторишемо број n за који верујемо да је сложен

Факторизација помоћу ЕК

Хоћемо да факторишемо број n за који верујемо да је сложен

- Претпоставимо супротно: n је прост

Факторизација помоћу ЕК

Хоћемо да факторишемо број n за који верујемо да је сложен

- Претпоставимо супротно: n је прост
- Онда је $\mathbb{Z}_n$ поље

Факторизација помоћу ЕК

Хоћемо да факторишемо број n за који верујемо да је сложен

- Претпоставимо супротно: n је прост
- Онда је $\mathbb{Z}_n$ поље
- Изаберемо неку елиптичку криву $E(\mathbb{Z}_n)$ и неку тачку P са те криве

Факторизација помоћу ЕК

Хоћемо да факторишемо број n за који верујемо да је сложен

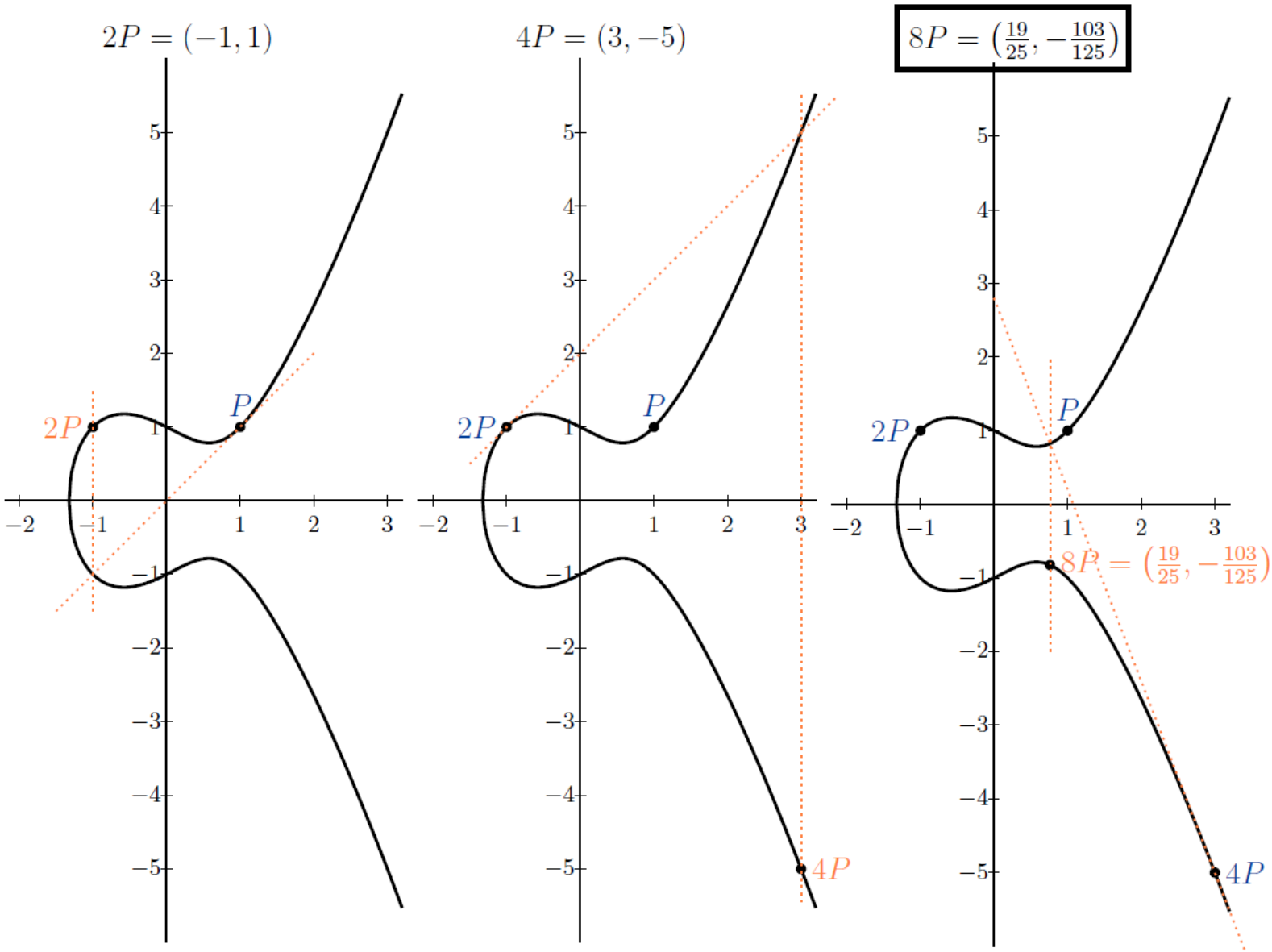
- Претпоставимо супротно: n је прост
- Онда је $\mathbb{Z}_n$ поље
- Изаберемо неку елиптичку криву $E(\mathbb{Z}_n)$ и неку тачку P са те криве
- Кренемо да рачунамо $2P$, $3P$, $4P$, ... (или $2P$, $4P$, $8P$, ...) и негде ће се појавити проблем са дељењем (нпр. у формули за сабирање тачака)
  - Практично рачунамо све у $\mathbb{Q}$, па редукујемо $\bmod n$

Факторизација помоћу ЕК

Хоћемо да факторишемо број n за који верујемо да је сложен

- Претпоставимо супротно: n је прост
- Онда је $\mathbb{Z}_n$ поље
- Изаберемо неку елиптичку криву $E(\mathbb{Z}_n)$ и неку тачку P са те криве
- Кренемо да рачунамо $2P$, $3P$, $4P$, ... (или $2P$, $4P$, $8P$, ...) и негде ће се појавити проблем са дељењем (нпр. у формули за сабирање тачака)
  - Практично рачунамо све у $\mathbb{Q}$, па редукујемо $\bmod n$
- Када се у имениоцу појави број g који није инвертибилан по модулу n, онда ће НЗД$(g, n) > 1$ бити прави делилац n

Пример: За растављање 35 користимо ЕК $y^2 = x^3 - x + 1$ над $\mathbb{Z}_{35}$ (није поље) и $P = (1, 1)$



НЗД$(35, 25) = 5$ је делилац 35

Example

We want to factor 4453. Let E be the elliptic curve $y^2 = x^3 + 10x - 2 \bmod 4453$ and let $P = (1, 3)$. Let's try to compute $3P$. First, we compute $2P$. The slope of the tangent line at P is

$$\frac{3x^2 + 10}{2y} = \frac{13}{6} \equiv 3713 \pmod{4453}.$$

We used the fact that $\gcd(6, 4453) = 1$ to find $6^{-1} \equiv 3711 \pmod{4453}$. Using this slope, we find that $2P = (x, y)$, with

$$x \equiv 3713^2 - 2 \equiv 4332, \quad y \equiv -3713(x - 1) - 3 \equiv 3230.$$

To compute $3P$, we add P and $2P$. The slope is

$$\frac{3230 - 3}{4332 - 1} = \frac{3227}{4331}.$$

But $\gcd(4331, 4453) = 61 \neq 1$. Therefore, we cannot find $4331^{-1} \pmod{4453}$, and we cannot evaluate the slope. However, we have found the factor 61 of 4453, and therefore $4453 = 61 \cdot 73$.

Ленстрин метод

- У примерима смо имали среће да међу mP-овима брзо наиђемо на проблем са дељењем, генерално то није случај

Ленстрин метод

- У примерима смо имали среће да међу mP-овима брзо наиђемо на проблем са дељењем, генерално то није случај

Ленстрин метод:

- претпоставка: n има прост чинилац p тд. кардиналност $|E(\mathbb{Z}_p)|$ је B-гладак број за неко мало B (инспирисано Полардовим $(p-1)$-методом)

Ленстрин метод

- У примерима смо имали среће да међу mP-овима брзо наиђемо на проблем са дељењем, генерално то није случај

Ленстрин метод:

- претпоставка: n има прост чинилац p тд. кардиналност $|E(\mathbb{Z}_p)|$ је B-гладак број за неко мало B (инспирисано Полардовим $(p-1)$-методом)
- не погађати које m ради, већ покушати са $m = \text{НЗС}(1, 2, \ldots, B)$ или $m = B!$ (m не зависи ни од n ни од p)

Ленстрин метод

- У примерима смо имали среће да међу mP-овима брзо наиђемо на проблем са дељењем, генерално то није случај

Ленстрин метод:

- претпоставка: n има прост чинилац p тд. кардиналност $|E(\mathbb{Z}_p)|$ је B-гладак број за неко мало B (инспирисано Полардовим $(p-1)$-методом)
- не погађати које m ради, већ покушати са $m = \text{НЗС}(1, 2, \ldots, B)$ или $m = B!$ (m не зависи ни од n ни од p)
- знамо да $|E(\mathbb{Z}_p)|$ дели ове m, па ће бити $mP = \mathcal{O}$ на $E(\mathbb{Z}_p)$ тј. појавиће се именилац g који је дељив са p

Ленстрин метод

- У примерима смо имали среће да међу mP-овима брзо наиђемо на проблем са дељењем, генерално то није случај

Ленстрин метод:

- претпоставка: n има прост чинилац p тд. кардиналност $|E(\mathbb{Z}_p)|$ је B-гладак број за неко мало B (инспирисано Полардовим $(p-1)$-методом)
- не погађати које m ради, већ покушати са $m = \text{НЗС}(1, 2, \ldots, B)$ или $m = B!$ (m не зависи ни од n ни од p)
- знамо да $|E(\mathbb{Z}_p)|$ дели ове m, па ће бити $mP = \mathcal{O}$ на $E(\mathbb{Z}_p)$ тј. појавиће се именилац g који је дељив са p
- али нећемо рачунати $\bmod p$, већ $\bmod n$

Дакле, рачунамо mP на $E(\mathbb{Z}_n)$. Може да се деси:

Дакле, рачунамо mP на $E(\mathbb{Z}_n)$. Може да се деси:

- ако успемо да израчунамо mP без проблема - претпоставка о B-глаткости није испуњена, покушати са већим B или другом елиптичом кривом

Дакле, рачунамо mP на $E(\mathbb{Z}_n)$. Може да се деси:

- ако успемо да израчунамо mP без проблема - претпоставка о B-глаткости није испуњена, покушати са већим B или другом елиптичом кривом
- ако се као именилац појави g дељив са n - променити тачку P

Дакле, рачунамо mP на $E(\mathbb{Z}_n)$. Може да се деси:

- ако успемо да израчунамо mP без проблема - претпоставка о B-глаткости није испуњена, покушати са већим B или другом елиптичом кривом
- ако се као именилац појави g дељив са n - променити тачку P
- ако се као именилац појави g које није дељиво са n, али није ни инвертибилно по модулу n - онда је НЗД(g, n) прави делилац n

Упаривања на елиптичким кривама

Дефиниција

За пресликавање $e : E(\mathbb{F}_q) \times E(\mathbb{F}_q) \longrightarrow \mathbb{F}_q \setminus \{0\}$ кажемо да је упаривање (билинеарно пресликавање) на $E(\mathbb{F}_q)$ ако важи

$$(\forall P_1, P_2, Q \in E(\mathbb{F}_q))\ e(P_1 \oplus P_2, Q) = e(P_1, Q) \cdot e(P_2, Q)$$
$$(\forall P, Q_1, Q_2 \in E(\mathbb{F}_q))\ e(P, Q_1 \oplus Q_2) = e(P, Q_1) \cdot e(P, Q_2)$$

Упаривања на елиптичким кривама

Дефиниција

За пресликавање $e : E(\mathbb{F}_q) \times E(\mathbb{F}_q) \longrightarrow \mathbb{F}_q \setminus \{0\}$ кажемо да је упаривање (билинеарно пресликавање) на $E(\mathbb{F}_q)$ ако важи

$$(\forall P_1, P_2, Q \in E(\mathbb{F}_q))\ e(P_1 \oplus P_2, Q) = e(P_1, Q) \cdot e(P_2, Q)$$
$$(\forall P, Q_1, Q_2 \in E(\mathbb{F}_q))\ e(P, Q_1 \oplus Q_2) = e(P, Q_1) \cdot e(P, Q_2)$$

- Последица: За све $P, Q \in E(\mathbb{F}_q)$ и $a, b \in \mathbb{N}$ важи

$$e(aP, bQ) = e(P, Q)^{ab}$$

Упаривања на елиптичким кривама

Дефиниција

За пресликавање $e : E(\mathbb{F}_q) \times E(\mathbb{F}_q) \longrightarrow \mathbb{F}_q \setminus \{0\}$ кажемо да је упаривање (билинеарно пресликавање) на $E(\mathbb{F}_q)$ ако важи

$$(\forall P_1, P_2, Q \in E(\mathbb{F}_q))\ e(P_1 \oplus P_2, Q) = e(P_1, Q) \cdot e(P_2, Q)$$
$$(\forall P, Q_1, Q_2 \in E(\mathbb{F}_q))\ e(P, Q_1 \oplus Q_2) = e(P, Q_1) \cdot e(P, Q_2)$$

- Последица: За све $P, Q \in E(\mathbb{F}_q)$ и $a, b \in \mathbb{N}$ важи

$$e(aP, bQ) = e(P, Q)^{ab}$$

- Дифи-Хелманов проблем над ЕК (помоћу P, aP и bP одредити abP) своди на проблем дискретног логаритма у $\mathbb{F}_q$

Упаривања на елиптичким кривама

Дефиниција

За пресликавање $e : E(\mathbb{F}_q) \times E(\mathbb{F}_q) \longrightarrow \mathbb{F}_q \setminus \{0\}$ кажемо да је упаривање (билинеарно пресликавање) на $E(\mathbb{F}_q)$ ако важи

$$(\forall P_1, P_2, Q \in E(\mathbb{F}_q))\ e(P_1 \oplus P_2, Q) = e(P_1, Q) \cdot e(P_2, Q)$$
$$(\forall P, Q_1, Q_2 \in E(\mathbb{F}_q))\ e(P, Q_1 \oplus Q_2) = e(P, Q_1) \cdot e(P, Q_2)$$

- Последица: За све $P, Q \in E(\mathbb{F}_q)$ и $a, b \in \mathbb{N}$ важи

$$e(aP, bQ) = e(P, Q)^{ab}$$

- Дифи-Хелманов проблем над ЕК (помоћу P, aP и bP одредити abP) своди на проблем дискретног логаритма у $\mathbb{F}_q$
- Детаљније о упаривањима: Craig Costello: *Pairings for beginners*, Главе 4 и 5

- Кажемо да је упаривање e допустиво ако је
  - недегенерисано:
    - $(\forall Q)\ e(P,Q) = 1 \implies P = \mathcal{O}$
    - $(\forall P)\ e(P,Q) = 1 \implies Q = \mathcal{O}$
  - ефективно израчунљиво

- Кажемо да је упаривање e допустиво ако је
  - недегенерисано:
    - $(\forall Q)\ e(P,Q) = 1 \implies P = \mathcal{O}$
    - $(\forall P)\ e(P,Q) = 1 \implies Q = \mathcal{O}$
  - ефективно израчунљиво
- Често се уместо на групама $E(\mathbb{F}_q)$ и $\mathbb{F}_q \setminus \{0\}$ упаривање дефинише на неким њиховим подгрупама
  - Упаривање је пресликавање $e : G_1 \times G_2 \longrightarrow G$ које задовољава претх. захтеве, где је $G_1, G_2 \leqslant E(\mathbb{F}_q)$ и $G \leqslant \mathbb{F}_q\{0\}$

- Кажемо да је упаривање e допустиво ако је
  - недегенерисано:
    - $(\forall Q)\ e(P,Q) = 1 \implies P = \mathcal{O}$
    - $(\forall P)\ e(P,Q) = 1 \implies Q = \mathcal{O}$
  - ефективно израчунљиво
- Често се уместо на групама $E(\mathbb{F}_q)$ и $\mathbb{F}_q \setminus \{0\}$ упаривање дефинише на неким њиховим подгрупама
  - Упаривање је пресликавање $e : G_1 \times G_2 \longrightarrow G$ које задовољава претх. захтеве, где је $G_1, G_2 \leqslant E(\mathbb{F}_q)$ и $G \leqslant \mathbb{F}_q\{0\}$
- Пример: Нека r дели и $q-1$ и $|E(\mathbb{F}_q)|$
  - $P \in E(\mathbb{F}_q)$ тачка реда r (тј. r је најмањи број за који важи $rP = \mathcal{O}$) и нека је $G_1 = \langle P \rangle = \{\mathcal{O}, P, 2P, \ldots, (r-1)P\}$
  - $G_2 = \langle Q \rangle$, где је тачка Q реда r
  - $G = Z_r = \{\zeta \in \mathbb{F}_q \mid \zeta^r = 1\}$ група r-тих корена из јединице
  - За сваки корен $\zeta \in G$ имамо по једно упаривање $e(aP, bQ) = \zeta^{ab}$

- r-торзиона подгрупа: $E(\mathbb{F}_q)[r] = \{P \in E(\mathbb{F}_q) \mid \underbrace{rP = \mathcal{O}}_{\substack{\text{ред } P \\ \text{дели } r}}\}$

- r-торзиона подгрупа: $E(\mathbb{F}_q)[r] = \{P \in E(\mathbb{F}_q) \mid \underbrace{rP = \mathcal{O}}_{\substack{\text{ред } P \\ \text{дели } r}}\}$
- За $q = p^\alpha$ имамо Фробенијусово пресликавање $\pi : \mathbb{F}_q \longrightarrow \mathbb{F}_q$, $\pi(g) = g^p$
  - Ако $\mathbb{F}_p = \mathbb{Z}_p$ видимо као потпоље $\mathbb{F}_q$ онда је π идентитет на $\mathbb{Z}_p$, а није на $\mathbb{F}_q$
  - π индукује и пресликавање $\pi : E(\mathbb{F}_q) \longrightarrow E(\mathbb{F}_q)$, $\pi(x, y) = (\pi(x), \pi(y))$ и $\pi(\mathcal{O}) = \mathcal{O}$

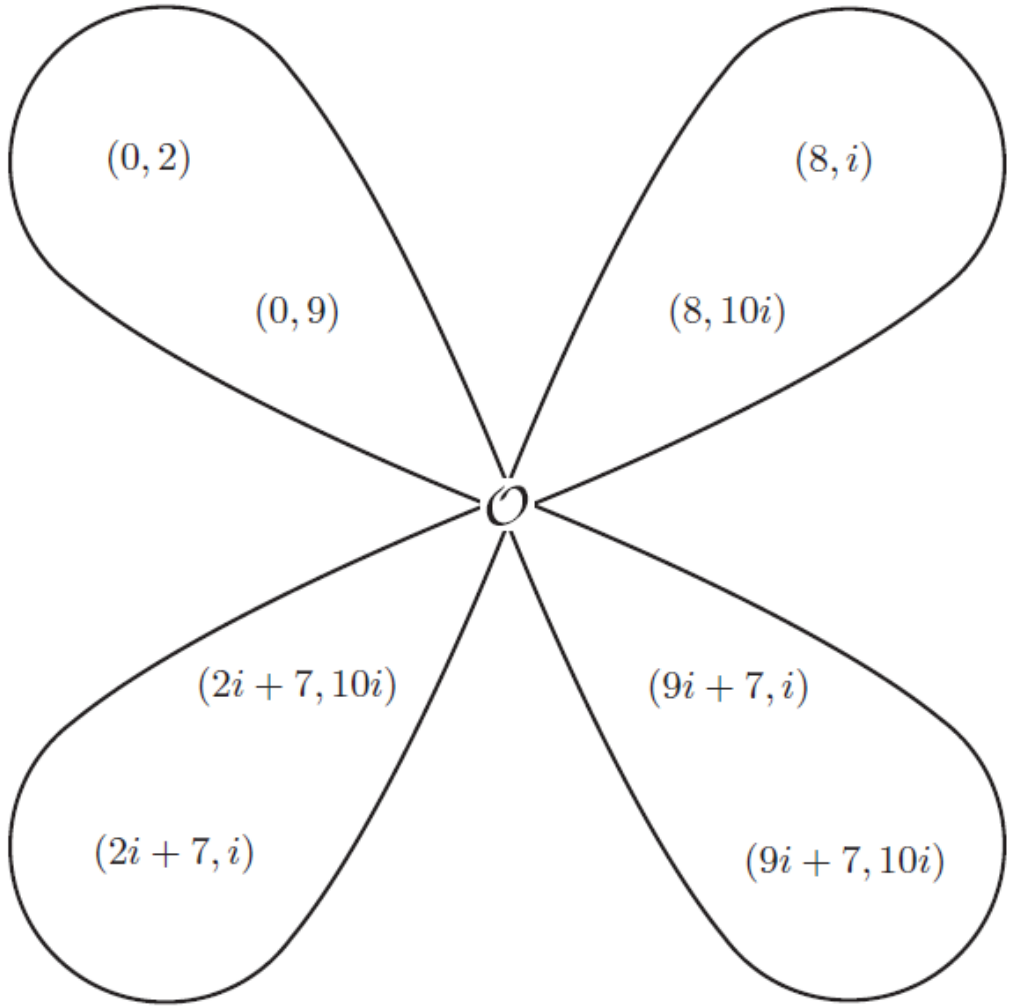
- r-торзиона подгрупа: $E(\mathbb{F}_q)[r] = \{P \in E(\mathbb{F}_q) \mid \underbrace{rP = \mathcal{O}}_{\substack{\text{ред } P \\ \text{дели } r}}\}$
- За $q = p^\alpha$ имамо Фробенијусово пресликавање $\pi : \mathbb{F}_q \longrightarrow \mathbb{F}_q$, $\pi(g) = g^p$
  - Ако $\mathbb{F}_p = \mathbb{Z}_p$ видимо као потпоље $\mathbb{F}_q$ онда је π идентитет на $\mathbb{Z}_p$, а није на $\mathbb{F}_q$
  - π индукује и пресликавање $\pi : E(\mathbb{F}_q) \longrightarrow E(\mathbb{F}_q)$, $\pi(x, y) = (\pi(x), \pi(y))$ и $\pi(\mathcal{O}) = \mathcal{O}$

Теорема

За свако r које дели $|E(\mathbb{F}_q)|$

1. $E(\mathbb{F}_q)[r] \cong \mathbb{Z}_r \times \mathbb{Z}_r$
2. $E(\mathbb{F}_q)[r]$ има тачно $r + 1$ подгрупу реда r
3. Рестрикција: $\pi|_{E(\mathbb{F}_q)[r]}$ има тачно две сопствене вредности 1 и p
4. Сопствени потпростори $\mathcal{G}_1$ и $\mathcal{G}_2$ који одговарају сопственим вредностима 1 и p, редом, су 2 групе са списка из дела 2.

Пример: Елиптичка крива $E: \ y^2 = x^3 + 4$ над пољем $\mathbb{F}_{121} = \{a + bi \,|\, 0 \leqslant a, b \leqslant 10\}$, где је $i^2 = -1$. Имамо 3-торзиону подгрупу $E(\mathbb{F}_{121})[3]$ која садржи 9 тачака и која има 4 подгрупе са по 3 тачке



Горе лево је $\mathcal{G}_1$: $\pi(0,2) = (0,2)$, $\pi(0,9) = (0,9)$,
горе десно је $\mathcal{G}_2$: $\pi(8,i) = 3(8,i)$, $\pi(8,10i) = 3(8,10i)$

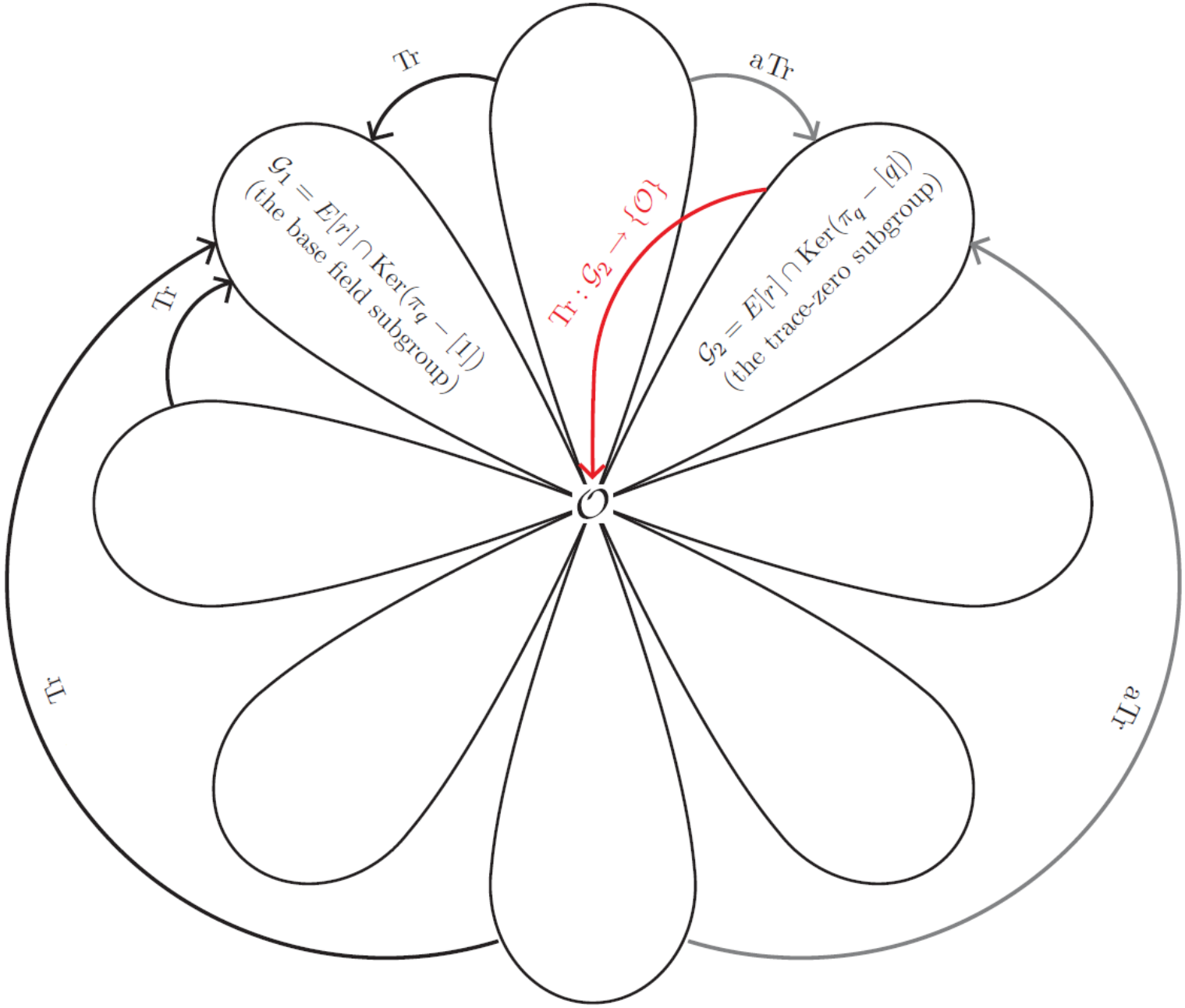
- Постоји више типова упаривања - у зависности од тога да ли је нека група G_1, G_2 (из дефиниције) баш једнака $\mathcal{G}_1$, $\mathcal{G}_2$ (из претх. теореме)

- Постоји више типова упаривања - у зависности од тога да ли је нека група G_1, G_2 (из дефиниције) баш једнака $\mathcal{G}_1$, $\mathcal{G}_2$ (из претх. теореме)
- Најзначајнији тип (за zero knowledge proofs) је $G_1 = \mathcal{G}_1$ и $G_2 = \mathcal{G}_2$

- Постоји више типова упаривања - у зависности од тога да ли је нека група G_1, G_2 (из дефиниције) баш једнака $\mathcal{G}_1$, $\mathcal{G}_2$ (из претх. теореме)
- Најзначајнији тип (за zero knowledge proofs) је $G_1 = \mathcal{G}_1$ и $G_2 = \mathcal{G}_2$
- Постоје сурјекције
  - траг $\mathrm{Tr} : E\left(\mathbb{F}_q\right)[r] \longrightarrow \mathcal{G}_1$,
    $\mathrm{Tr}(P) = P \oplus \pi(P) \oplus \pi^2(P) \oplus \cdots \oplus \pi^{\alpha-1}(P)$
    (где је α из $q = p^\alpha$)
  - анти-траг $\mathrm{aTr} : E\left(\mathbb{F}_q\right)[r] \longrightarrow \mathcal{G}_2$, $\mathrm{aTr}(P) = (rP) \ominus \mathrm{Tr}(P)$

- Постоји више типова упаривања - у зависности од тога да ли је нека група G_1, G_2 (из дефиниције) баш једнака $\mathcal{G}_1$, $\mathcal{G}_2$ (из претх. теореме)
- Најзначајнији тип (за zero knowledge proofs) је $G_1 = \mathcal{G}_1$ и $G_2 = \mathcal{G}_2$
- Постоје сурјекције
  - траг $\mathrm{Tr} : E(\mathbb{F}_q)[r] \longrightarrow \mathcal{G}_1$, $\mathrm{Tr}(P) = P \oplus \pi(P) \oplus \pi^2(P) \oplus \cdots \oplus \pi^{\alpha-1}(P)$ (где је α из $q = p^\alpha$)
  - анти-траг $\mathrm{aTr} : E(\mathbb{F}_q)[r] \longrightarrow \mathcal{G}_2$, $\mathrm{aTr}(P) = (rP) \ominus \mathrm{Tr}(P)$
- Свако упаривање $e : \mathcal{G}_1 \times \mathcal{G}_2 \longrightarrow Z_r$ (где је Z_r група r-тих корена из 1) се може проширити до упаривања

$$\widehat{e} : E(\mathbb{F}_q)[r] \times E(\mathbb{F}_q)[r] \longrightarrow Z_r, \qquad \widehat{e}(P,Q) = e(\mathrm{Tr}(P), \mathrm{aTr}(Q))$$


Tr
aTr
$\mathrm{Tr} : \mathcal{G}_2 \to \{\mathcal{O}\}$
$\mathcal{G}_1 = E[r] \cap \mathrm{Ker}(\pi_q - [1])$
(the base field subgroup)
$\mathcal{G}_2 = E[r] \cap \mathrm{Ker}(\pi_q - [q])$
(the trace-zero subgroup)
Tr
$\mathcal{O}$
Tr
aTr