

Algoritmy teorie čísel

Radan Kučera, doplněk, podzimní semestr 2021

Motivace

Někdy (například při řešení diofantických rovnic) potřebujeme pracovat v okruhu R celých algebraických čísel tělesa algebraických čísel K (tj. K je konečné rozšíření \mathbb{Q}).

Motivace

Někdy (například při řešení diofantických rovnic) potřebujeme pracovat v okruhu R celých algebraických čísel tělesa algebraických čísel K (tj. K je konečné rozšíření \mathbb{Q}).

Obecně R není okruh s jednoznačným rozkladem, ale je to Dedekindův okruh,

Motivace

Někdy (například při řešení diofantických rovnic) potřebujeme pracovat v okruhu R celých algebraických čísel tělesa algebraických čísel K (tj. K je konečné rozšíření \mathbb{Q}).

Obecně R není okruh s jednoznačným rozkladem, ale je to Dedekindův okruh, a tedy každý nenulový ideál okruhu R lze jednoznačně rozložit na součin prvoideálů.

Motivace

Někdy (například při řešení diofantických rovnic) potřebujeme pracovat v okruhu R celých algebraických čísel tělesa algebraických čísel K (tj. K je konečné rozšíření \mathbb{Q}).

Obecně R není okruh s jednoznačným rozkladem, ale je to Dedekindův okruh, a tedy každý nenulový ideál okruhu R lze jednoznačně rozložit na součin prvoideálů. Místo rozkládání celého algebraického čísla $a \in R$ na součin ireducibilních prvků okruhu R můžeme rozkládat hlavní ideál aR na součin prvoideálů.

Motivace

Někdy (například při řešení diofantických rovnic) potřebujeme pracovat v okruhu R celých algebraických čísel tělesa algebraických čísel K (tj. K je konečné rozšíření \mathbb{Q}).

Obecně R není okruh s jednoznačným rozkladem, ale je to Dedekindův okruh, a tedy každý nenulový ideál okruhu R lze jednoznačně rozložit na součin prvoideálů. Místo rozkládání celého algebraického čísla $a \in R$ na součin ireducibilních prvků okruhu R můžeme rozkládat hlavní ideál aR na součin prvoideálů.

Pak ale v jisté chvíli se potřebujeme vrátit zpět od ideálu k číslu, které jej generuje, což je však možné jen v případě, že jde o hlavní ideál.

Motivace

Někdy (například při řešení diofantických rovnic) potřebujeme pracovat v okruhu R celých algebraických čísel tělesa algebraických čísel K (tj. K je konečné rozšíření \mathbb{Q}).

Obecně R není okruh s jednoznačným rozkladem, ale je to Dedekindův okruh, a tedy každý nenulový ideál okruhu R lze jednoznačně rozložit na součin prvoideálů. Místo rozkládání celého algebraického čísla $a \in R$ na součin ireducibilních prvků okruhu R můžeme rozkládat hlavní ideál aR na součin prvoideálů.

Pak ale v jisté chvíli se potřebujeme vrátit zpět od ideálu k číslu, které jej generuje, což je však možné jen v případě, že jde o hlavní ideál. V tom případě je generátor tohoto hlavního ideálu určen až na násobení **jednotkou**.

Motivace

Někdy (například při řešení diofantických rovnic) potřebujeme pracovat v okruhu R celých algebraických čísel tělesa algebraických čísel K (tj. K je konečné rozšíření \mathbb{Q}).

Obecně R není okruh s jednoznačným rozkladem, ale je to Dedekindův okruh, a tedy každý nenulový ideál okruhu R lze jednoznačně rozložit na součin prvoideálů. Místo rozkládání celého algebraického čísla $a \in R$ na součin ireducibilních prvků okruhu R můžeme rozkládat hlavní ideál aR na součin prvoideálů.

Pak ale v jisté chvíli se potřebujeme vrátit zpět od ideálu k číslu, které jej generuje, což je však možné jen v případě, že jde o hlavní ideál. V tom případě je generátor tohoto hlavního ideálu určen až na násobení **jednotkou**. Obstrukce kontrolující, zda je daný ideál hlavní, je skryta v **grupě tříd ideálů** Cl_K , kterou lze definovat jako faktorgrupu grupy všech **lomených ideálů** okruhu R podle podgrupy hlavních lomených ideálů.

Motivace

Někdy (například při řešení diofantických rovnic) potřebujeme pracovat v okruhu R celých algebraických čísel tělesa algebraických čísel K (tj. K je konečné rozšíření \mathbb{Q}).

Obecně R není okruh s jednoznačným rozkladem, ale je to Dedekindův okruh, a tedy každý nenulový ideál okruhu R lze jednoznačně rozložit na součin prvoideálů. Místo rozkládání celého algebraického čísla $a \in R$ na součin ireducibilních prvků okruhu R můžeme rozkládat hlavní ideál aR na součin prvoideálů.

Pak ale v jisté chvíli se potřebujeme vrátit zpět od ideálu k číslu, které jej generuje, což je však možné jen v případě, že jde o hlavní ideál. V tom případě je generátor tohoto hlavního ideálu určen až na násobení **jednotkou**. Obstrukce kontrolující, zda je daný ideál hlavní, je skryta v **grupě tříd ideálů** Cl_K , kterou lze definovat jako faktorgrupu grupy všech **lomených ideálů** okruhu R podle podgrupy hlavních lomených ideálů.

Proto potřebujeme popsat následující aritmetické objekty okruhu R : jeho **grupu tříd ideálů** Cl_K a jeho **grupu jednotek** R^\times .

Grupa jednotek R^\times je konečně generovaná

Torzni část W_K grupy R^\times je konečná cyklická grupa obsahující všechny odmocniny z jedné patřící do K .

Grupa jednotek R^\times je konečně generovaná

Torzni část W_K grupy R^\times je konečná cyklická grupa obsahující všechny odmocniny z jedné patřící do K .

\mathbb{Z} -rank grupy R^\times je dán Dirichletovou větou: $R^\times \cong W_K \times \mathbb{Z}^r$, kde $r := \text{rank}_{\mathbb{Z}} R^\times = s + t - 1$, přičemž s je počet reálných vnoření tělesa K a t je počet párů nereálných vnoření tělesa K .

Grupa jednotek R^\times je konečně generovaná

Torzni část W_K grupy R^\times je konečná cyklická grupa obsahující všechny odmocniny z jedné patřící do K .

\mathbb{Z} -rank grupy R^\times je dán Dirichletovou větou: $R^\times \cong W_K \times \mathbb{Z}^r$, kde $r := \text{rank}_{\mathbb{Z}} R^\times = s + t - 1$, přičemž s je počet reálných vnoření tělesa K a t je počet párů nereálných vnoření tělesa K . Tudíž stupeň $[K : \mathbb{Q}] = s + 2t$.

Grupa jednotek R^\times je konečně generovaná

Torzni část W_K grupy R^\times je konečná cyklická grupa obsahující všechny odmocniny z jedné patřící do K .

\mathbb{Z} -rank grupy R^\times je dán Dirichletovou větou: $R^\times \cong W_K \times \mathbb{Z}^r$, kde $r := \text{rank}_{\mathbb{Z}} R^\times = s + t - 1$, přičemž s je počet reálných vnoření tělesa K a t je počet párů nereálných vnoření tělesa K . Tudíž stupeň $[K : \mathbb{Q}] = s + 2t$.

Tato vnoření mohou být určena například takto: existuje $\alpha \in K$ takové, že $K = \mathbb{Q}(\alpha)$.

Grupa jednotek R^\times je konečně generovaná

Torzni část W_K grupy R^\times je konečná cyklická grupa obsahující všechny odmocniny z jedné patřící do K .

\mathbb{Z} -rank grupy R^\times je dán Dirichletovou větou: $R^\times \cong W_K \times \mathbb{Z}^r$, kde $r := \text{rank}_{\mathbb{Z}} R^\times = s + t - 1$, přičemž s je počet reálných vnoření tělesa K a t je počet párů nereálných vnoření tělesa K . Tudíž stupeň $[K : \mathbb{Q}] = s + 2t$.

Tato vnoření mohou být určena například takto: existuje $\alpha \in K$ takové, že $K = \mathbb{Q}(\alpha)$. Minimální polynom $f(X) \in \mathbb{Q}[X]$ čísla α má s reálných kořenů $\alpha_1, \dots, \alpha_s$ a t dvojic komplexně sdružených kořenů $\alpha_{s+1}, \overline{\alpha_{s+1}}, \dots, \alpha_{s+t}, \overline{\alpha_{s+t}}$.

Grupa jednotek R^\times je konečně generovaná

Torzni část W_K grupy R^\times je konečná cyklická grupa obsahující všechny odmocniny z jedné patřící do K .

\mathbb{Z} -rank grupy R^\times je dán Dirichletovou větou: $R^\times \cong W_K \times \mathbb{Z}^r$, kde $r := \text{rank}_{\mathbb{Z}} R^\times = s + t - 1$, přičemž s je počet reálných vnoření tělesa K a t je počet párů nereálných vnoření tělesa K . Tudíž stupeň $[K : \mathbb{Q}] = s + 2t$.

Tato vnoření mohou být určena například takto: existuje $\alpha \in K$ takové, že $K = \mathbb{Q}(\alpha)$. Minimální polynom $f(X) \in \mathbb{Q}[X]$ čísla α má s reálných kořenů $\alpha_1, \dots, \alpha_s$ a t dvojic komplexně sdružených kořenů $\alpha_{s+1}, \overline{\alpha_{s+1}}, \dots, \alpha_{s+t}, \overline{\alpha_{s+t}}$.

Nechť σ_i je vnoření určené $\alpha \mapsto \alpha_i$.

Grupa jednotek R^\times je konečně generovaná

Torzni část W_K grupy R^\times je konečná cyklická grupa obsahující všechny odmocniny z jedné patřící do K .

\mathbb{Z} -rank grupy R^\times je dán Dirichletovou větou: $R^\times \cong W_K \times \mathbb{Z}^r$, kde $r := \text{rank}_{\mathbb{Z}} R^\times = s + t - 1$, přičemž s je počet reálných vnoření tělesa K a t je počet párů nereálných vnoření tělesa K . Tudíž stupeň $[K : \mathbb{Q}] = s + 2t$.

Tato vnoření mohou být určena například takto: existuje $\alpha \in K$ takové, že $K = \mathbb{Q}(\alpha)$. Minimální polynom $f(X) \in \mathbb{Q}[X]$ čísla α má s reálných kořenů $\alpha_1, \dots, \alpha_s$ a t dvojic komplexně sdružených kořenů $\alpha_{s+1}, \overline{\alpha_{s+1}}, \dots, \alpha_{s+t}, \overline{\alpha_{s+t}}$.

Nechť σ_i je vnoření určené $\alpha \mapsto \alpha_i$. Pak σ_i je reálné, právě když $i \leq s$.

Grupa jednotek R^\times je konečně generovaná

Torzni část W_K grupy R^\times je konečná cyklická grupa obsahující všechny odmocniny z jedné patřící do K .

\mathbb{Z} -rank grupy R^\times je dán Dirichletovou větou: $R^\times \cong W_K \times \mathbb{Z}^r$, kde $r := \text{rank}_{\mathbb{Z}} R^\times = s + t - 1$, přičemž s je počet reálných vnoření tělesa K a t je počet párů nereálných vnoření tělesa K . Tudíž stupeň $[K : \mathbb{Q}] = s + 2t$.

Tato vnoření mohou být určena například takto: existuje $\alpha \in K$ takové, že $K = \mathbb{Q}(\alpha)$. Minimální polynom $f(X) \in \mathbb{Q}[X]$ čísla α má s reálných kořenů $\alpha_1, \dots, \alpha_s$ a t dvojic komplexně sdružených kořenů $\alpha_{s+1}, \overline{\alpha_{s+1}}, \dots, \alpha_{s+t}, \overline{\alpha_{s+t}}$.

Nechť σ_i je vnoření určené $\alpha \mapsto \alpha_i$. Pak σ_i je reálné, právě když $i \leq s$.

Tudíž známe \mathbb{Z} -rank r grupy R^\times , ale nalezení fundamentálních jednotek, tj. generátorů grupy R^\times / W_K , je velmi obtížný problém. Přestože je znám algoritmus, jeho časová náročnost se stupněm $[K : \mathbb{Q}]$ roste velmi rychle.

Geometrie jednotek

Logaritmické zobrazení $\ell : R^\times \rightarrow \mathbb{R}^{r+1}$ je definováno předpisem $\ell(\varepsilon) = (\dots, \delta_i \log |\sigma_i(\varepsilon)|, \dots)$, kde $\delta_i = 1$ pro $i \leq s$ a $\delta_i = 2$ jinak.

Geometrie jednotek

Logaritmické zobrazení $\ell : R^\times \rightarrow \mathbb{R}^{r+1}$ je definováno předpisem $\ell(\varepsilon) = (\dots, \delta_i \log |\sigma_i(\varepsilon)|, \dots)$, kde $\delta_i = 1$ pro $i \leq s$ a $\delta_i = 2$ jinak.

Pak $\ker \ell = W_K$ a $\ell(R^\times) \subset \mathcal{H} = \{(x_1, \dots, x_{r+1}) \mid \sum_{i=1}^{r+1} x_i = 0\}$.

Geometrie jednotek

Logaritmické zobrazení $\ell : R^\times \rightarrow \mathbb{R}^{r+1}$ je definováno předpisem $\ell(\varepsilon) = (\dots, \delta_i \log |\sigma_i(\varepsilon)|, \dots)$, kde $\delta_i = 1$ pro $i \leq s$ a $\delta_i = 2$ jinak.

Pak $\ker \ell = W_K$ a $\ell(R^\times) \subset \mathcal{H} = \{(x_1, \dots, x_{r+1}) \mid \sum_{i=1}^{r+1} x_i = 0\}$.

Pro libovolnou r -tici $\eta_1, \dots, \eta_r \in R^\times$ definujeme regulátor

$$R(\eta_1, \dots, \eta_r) = \left| \det(\delta_i \log |\sigma_i(\eta_j)|)_{i,j=1, \dots, r} \right|.$$

Geometrie jednotek

Logaritmické zobrazení $\ell : R^\times \rightarrow \mathbb{R}^{r+1}$ je definováno předpisem $\ell(\varepsilon) = (\dots, \delta_i \log |\sigma_i(\varepsilon)|, \dots)$, kde $\delta_i = 1$ pro $i \leq s$ a $\delta_i = 2$ jinak.

Pak $\ker \ell = W_K$ a $\ell(R^\times) \subset \mathcal{H} = \{(x_1, \dots, x_{r+1}) \mid \sum_{i=1}^{r+1} x_i = 0\}$.

Pro libovolnou r -tici $\eta_1, \dots, \eta_r \in R^\times$ definujeme regulátor

$$R(\eta_1, \dots, \eta_r) = \left| \det(\delta_i \log |\sigma_i(\eta_j)|)_{i,j=1, \dots, r} \right|.$$

Tudíž regulátor $R(\eta_1, \dots, \eta_r)$ je dán r -rozměrným objemem rovnoběžnostěnu daného obrazy $\ell(\eta_1), \dots, \ell(\eta_r)$ v \mathcal{H} .

Geometrie jednotek

Logaritmické zobrazení $\ell : R^\times \rightarrow \mathbb{R}^{r+1}$ je definováno předpisem $\ell(\varepsilon) = (\dots, \delta_i \log |\sigma_i(\varepsilon)|, \dots)$, kde $\delta_i = 1$ pro $i \leq s$ a $\delta_i = 2$ jinak.

Pak $\ker \ell = W_K$ a $\ell(R^\times) \subset \mathcal{H} = \{(x_1, \dots, x_{r+1}) \mid \sum_{i=1}^{r+1} x_i = 0\}$.

Pro libovolnou r -tici $\eta_1, \dots, \eta_r \in R^\times$ definujeme regulátor

$$R(\eta_1, \dots, \eta_r) = \left| \det(\delta_i \log |\sigma_i(\eta_j)|)_{i,j=1, \dots, r} \right|.$$

Tudíž regulátor $R(\eta_1, \dots, \eta_r)$ je dán r -rozměrným objemem rovnoběžnostěnu daného obrazy $\ell(\eta_1), \dots, \ell(\eta_r)$ v \mathcal{H} .

Proto $R(\eta_1, \dots, \eta_r) = 0$, právě když jednotky η_1, \dots, η_r jsou (multiplikativně) závislé.

Geometrie jednotek

Logaritmické zobrazení $\ell : R^\times \rightarrow \mathbb{R}^{r+1}$ je definováno předpisem $\ell(\varepsilon) = (\dots, \delta_i \log |\sigma_i(\varepsilon)|, \dots)$, kde $\delta_i = 1$ pro $i \leq s$ a $\delta_i = 2$ jinak.

Pak $\ker \ell = W_K$ a $\ell(R^\times) \subset \mathcal{H} = \{(x_1, \dots, x_{r+1}) \mid \sum_{i=1}^{r+1} x_i = 0\}$.

Pro libovolnou r -tici $\eta_1, \dots, \eta_r \in R^\times$ definujeme regulátor

$$R(\eta_1, \dots, \eta_r) = \left| \det(\delta_i \log |\sigma_i(\eta_j)|)_{i,j=1, \dots, r} \right|.$$

Tudíž regulátor $R(\eta_1, \dots, \eta_r)$ je dán r -rozměrným objemem rovnoběžnostěnu daného obrazy $\ell(\eta_1), \dots, \ell(\eta_r)$ v \mathcal{H} .

Proto $R(\eta_1, \dots, \eta_r) = 0$, právě když jednotky η_1, \dots, η_r jsou (multiplikativně) závislé.

Regulátor R_K tělesa K je definován jako regulátor libovolného systému fundamentálních jednotek (tj. r -tice jednotek generujících spolu s W_K grupu všech jednotek R^\times).

Geometrie jednotek

Logaritmické zobrazení $\ell : R^\times \rightarrow \mathbb{R}^{r+1}$ je definováno předpisem $\ell(\varepsilon) = (\dots, \delta_i \log |\sigma_i(\varepsilon)|, \dots)$, kde $\delta_i = 1$ pro $i \leq s$ a $\delta_i = 2$ jinak.

Pak $\ker \ell = W_K$ a $\ell(R^\times) \subset \mathcal{H} = \{(x_1, \dots, x_{r+1}) \mid \sum_{i=1}^{r+1} x_i = 0\}$.

Pro libovolnou r -tici $\eta_1, \dots, \eta_r \in R^\times$ definujeme regulátor

$$R(\eta_1, \dots, \eta_r) = \left| \det(\delta_i \log |\sigma_i(\eta_j)|)_{i,j=1, \dots, r} \right|.$$

Tudíž regulátor $R(\eta_1, \dots, \eta_r)$ je dán r -rozměrným objemem rovnoběžnostěnu daného obrazy $\ell(\eta_1), \dots, \ell(\eta_r)$ v \mathcal{H} .

Proto $R(\eta_1, \dots, \eta_r) = 0$, právě když jednotky η_1, \dots, η_r jsou (multiplikativně) závislé.

Regulátor R_K tělesa K je definován jako regulátor libovolného systému fundamentálních jednotek (tj. r -tice jednotek generujících spolu s W_K grupu všech jednotek R^\times).

Platí $[R^\times : \langle W_K \cup \{\eta_1, \dots, \eta_r\} \rangle] = \frac{R(\eta_1, \dots, \eta_r)}{R_K}$, je-li $R(\eta_1, \dots, \eta_r) \neq 0$.

Dedekindova ζ -funkce ζ_K tělesa K

Dedekindova ζ -funkce ζ_K tělesa K je definována v oblasti $z \in \mathbb{C}$, $\Re(z) > 1$, absolutně konvergentní řadou

$$\zeta_K(z) = \sum_A (N(A))^{-z},$$

kde A probíhá množinu všech nenulových ideálů okruhu R a $N(A) = |R/A|$ je absolutní norma A .

Dedekindova ζ -funkce ζ_K tělesa K

Dedekindova ζ -funkce ζ_K tělesa K je definována v oblasti $z \in \mathbb{C}$, $\Re(z) > 1$, absolutně konvergentní řadou

$$\zeta_K(z) = \sum_A (N(A))^{-z},$$

kde A probíhá množinu všech nenulových ideálů okruhu R a $N(A) = |R/A|$ je absolutní norma A .

Protože R je Dedekindův okruh, každý nenulový ideál A je jednoznačně dán jako součin prvoideálů.

Dedekindova ζ -funkce ζ_K tělesa K

Dedekindova ζ -funkce ζ_K tělesa K je definována v oblasti $z \in \mathbb{C}$, $\Re(z) > 1$, absolutně konvergentní řadou

$$\zeta_K(z) = \sum_A (N(A))^{-z},$$

kde A probíhá množinu všech nenulových ideálů okruhu R a $N(A) = |R/A|$ je absolutní norma A .

Protože R je Dedekindův okruh, každý nenulový ideál A je jednoznačně dán jako součin prvoideálů.

Absolutní norma ideálů je multiplikativní, a tedy funkce $\zeta_K(z)$ je dána Eulerovým součinem přes všechny prvoideály okruhu R : je-li $\Re(z) > 1$, pak

$$\zeta_K(z) = \prod_{\mathfrak{p}} (1 - N(\mathfrak{p})^{-z})^{-1}.$$

Grupa tříd ideálů Cl_K je konečná grupa

Erich Hecke dokázal, že funkce $\zeta_K(z)$ má meromorfní prodloužení na celé \mathbb{C} s jediným pólem v $z = 1$.

Grupa tříd ideálů Cl_K je konečná grupa

Erich Hecke dokázal, že funkce $\zeta_K(z)$ má meromorfní prodloužení na celé \mathbb{C} s jediným pólem v $z = 1$. Tento pól je jednoduchý a jeho residuum je

$$\lim_{z \rightarrow 1} (z - 1)\zeta_K(z) = \frac{2^s (2\pi)^t h_K R_K}{|W_K| \cdot \sqrt{|D_K|}},$$

kde $h_K = |\text{Cl}_K|$ je počet tříd ideálů a D_K je diskriminant tělesa K ,

Grupa tříd ideálů Cl_K je konečná grupa

Erich Hecke dokázal, že funkce $\zeta_K(z)$ má meromorfní prodloužení na celé \mathbb{C} s jediným pólem v $z = 1$. Tento pól je jednoduchý a jeho residuum je

$$\lim_{z \rightarrow 1} (z - 1)\zeta_K(z) = \frac{2^s (2\pi)^t h_K R_K}{|W_K| \cdot \sqrt{|D_K|}},$$

kde $h_K = |\text{Cl}_K|$ je počet tříd ideálů a D_K je diskriminant tělesa K , který je definován takto:

Aditivní grupa $(R, +)$ je volná komutativní grupa ranku $\text{rank}_{\mathbb{Z}} R = [K : \mathbb{Q}] = s + 2t$.

Grupa tříd ideálů Cl_K je konečná grupa

Erich Hecke dokázal, že funkce $\zeta_K(z)$ má meromorfní prodloužení na celé \mathbb{C} s jediným pólem v $z = 1$. Tento pól je jednoduchý a jeho residuum je

$$\lim_{z \rightarrow 1} (z - 1)\zeta_K(z) = \frac{2^s (2\pi)^t h_K R_K}{|W_K| \cdot \sqrt{|D_K|}},$$

kde $h_K = |\text{Cl}_K|$ je počet tříd ideálů a D_K je diskriminant tělesa K , který je definován takto:

Aditivní grupa $(R, +)$ je volná komutativní grupa ranku $\text{rank}_{\mathbb{Z}} R = [K : \mathbb{Q}] = s + 2t$. Nechť b_1, \dots, b_{s+2t} je systém nezávislých generátorů grupy $(R, +)$, pak diskriminant D_K je druhá mocnina determinantu

$$\det\left(\sigma_1(b_j), \dots, \sigma_{s+t}(b_j), \overline{\sigma_{s+1}(b_j)}, \dots, \overline{\sigma_{s+t}(b_j)}\right)_{j=1, \dots, s+2t}.$$

Odhad součinu $h_K R_K$

Speciálně pro těleso \mathbb{Q} je Dedekindova ζ -funkce $\zeta_{\mathbb{Q}}$ rovna Riemannově ζ -funkci a platí $\lim_{z \rightarrow 1} (z - 1)\zeta_{\mathbb{Q}}(z) = 1$.

Odhad součinu $h_K R_K$

Speciálně pro těleso \mathbb{Q} je Dedekindova ζ -funkce $\zeta_{\mathbb{Q}}$ rovna Riemannově ζ -funkci a platí $\lim_{z \rightarrow 1} (z - 1)\zeta_{\mathbb{Q}}(z) = 1$.

Proto

$$\frac{2^s (2\pi)^t h_K R_K}{|W_K| \cdot \sqrt{|D_K|}} = \lim_{z \rightarrow 1} \frac{\zeta_K(z)}{\zeta_{\mathbb{Q}}(z)} = \lim_{z \rightarrow 1} \prod_p \frac{1 - p^{-z}}{\prod_{\mathfrak{P}|pR} (1 - N(\mathfrak{P})^{-z})},$$

kde ve vnějším součinu probíhá p všechna prvočísla, zatímco vnitřní součin je vzat přes konečně mnoho prvoideálů \mathfrak{P} vystupujících v rozkladu ideálu pR .

Odhad součinu $h_K R_K$

Speciálně pro těleso \mathbb{Q} je Dedekindova ζ -funkce $\zeta_{\mathbb{Q}}$ rovna Riemannově ζ -funkci a platí $\lim_{z \rightarrow 1} (z - 1)\zeta_{\mathbb{Q}}(z) = 1$.

Proto

$$\frac{2^s (2\pi)^t h_K R_K}{|W_K| \cdot \sqrt{|D_K|}} = \lim_{z \rightarrow 1} \frac{\zeta_K(z)}{\zeta_{\mathbb{Q}}(z)} = \lim_{z \rightarrow 1} \prod_p \frac{1 - p^{-z}}{\prod_{\mathfrak{P}|pR} (1 - N(\mathfrak{P})^{-z})},$$

kde ve vnějším součinu probíhá p všechna prvočísla, zatímco vnitřní součin je vzat přes konečně mnoho prvoideálů \mathfrak{P} vystupujících v rozkladu ideálu pR . Proto spočítáme-li rozklady všech ideálů pR pro všechna prvočísla $p < L$ pro jistou dostatečně velkou hranici L , platí přibližně

$$h_K R_K \doteq \frac{|W_K| \cdot \sqrt{|D_K|}}{2^s (2\pi)^t} \prod_{p < L} \frac{1 - p^{-1}}{\prod_{\mathfrak{P}|pR} (1 - N(\mathfrak{P})^{-1})}.$$

Generátory grupy tříd ideálů Cl_K

Grupa Cl_K je generována třídami obsahujícími prvoideály \mathfrak{P} , jejichž norma

$$N(\mathfrak{P}) \leq \left(\frac{4}{\pi}\right)^t \frac{(s+2t)!}{(s+2t)^{s+2t}} \sqrt{|D_K|}.$$

Generátory grupy tříd ideálů Cl_K

Grupa Cl_K je generována třídami obsahujícími prvoideály \mathfrak{P} , jejichž norma

$$N(\mathfrak{P}) \leq \left(\frac{4}{\pi}\right)^t \frac{(s+2t)!}{(s+2t)^{s+2t}} \sqrt{|D_K|}.$$

Je třeba najít relace mezi třídami obsahujícími tyto prvoideály, tj. jejich součiny, které jsou rovny hlavnímu ideálu.

Generátory grupy tříd ideálů Cl_K

Grupa Cl_K je generována třídami obsahujícími prvoideály \mathfrak{P} , jejichž norma

$$N(\mathfrak{P}) \leq \left(\frac{4}{\pi}\right)^t \frac{(s+2t)!}{(s+2t)^{s+2t}} \sqrt{|D_K|}.$$

Je třeba najít relace mezi třídami obsahujícími tyto prvoideály, tj. jejich součiny, které jsou rovny hlavnímu ideálu. Přitom dokázat, že daný ideál je hlavní, je možné nalezením jeho generátoru.

Generátory grupy tříd ideálů Cl_K

Grupa Cl_K je generována třídami obsahujícími prvoideály \mathfrak{P} , jejichž norma

$$N(\mathfrak{P}) \leq \left(\frac{4}{\pi}\right)^t \frac{(s+2t)!}{(s+2t)^{s+2t}} \sqrt{|D_K|}.$$

Je třeba najít relace mezi třídami obsahujícími tyto prvoideály, tj. jejich součiny, které jsou rovny hlavnímu ideálu. Přitom dokázat, že daný ideál je hlavní, je možné nalezením jeho generátoru. Ale dokázat, že daný ideál hlavní není, znamená dokázat, že jistá diofantická rovnice nemá řešení, což může být velmi obtížné (nemáme-li štěstí, že vede na nějakou kongruenci, která nemá řešení).

Využití odhadu $h_K R_K$ pro určení Cl_K a fundamentálních jednotek

Za bázi faktorizace se vezme množina prvoideálů dělících prvočísla $p < L$, hledají se relace mezi nimi tvaru „součin několika z nich je hlavní ideál, přitom generátor α tohoto hlavního ideálu je nalezen“.

Využití odhadu $h_K R_K$ pro určení Cl_K a fundamentálních jednotek

Za bázi faktorizace se vezme množina prvoideálů dělicích prvočísla $p < L$, hledají se relace mezi nimi tvaru „součin několika z nich je hlavní ideál, přitom generátor α tohoto hlavního ideálu je nalezen“. Tyto relace se uchovávají jako vektory, jejichž složky jsou celá čísla udávající exponenty tohoto součinu a v posledních $s + t$ složkách jsou komplexní logaritmy

$$(\log \sigma_1(\alpha), \dots, \log \sigma_{s+t}(\alpha)).$$

Využití odhadu $h_K R_K$ pro určení Cl_K a fundamentálních jednotek

Za bázi faktorizace se vezme množina prvoideálů dělicích prvočísla $p < L$, hledají se relace mezi nimi tvaru „součin několika z nich je hlavní ideál, přitom generátor α tohoto hlavního ideálu je nalezen“. Tyto relace se uchovávají jako vektory, jejichž složky jsou celá čísla udávající exponenty tohoto součinu a v posledních $s + t$ složkách jsou komplexní logaritmy

$$(\log \sigma_1(\alpha), \dots, \log \sigma_{s+t}(\alpha)).$$

Z nich se Gaussovou eliminací odvodí relace, které určí vztahy mezi generátory grupy Cl_K , a také vektory mající jen nuly ve složkách udávajících exponenty, které odpovídají jednotkám.

Využití odhadu $h_K R_K$ pro určení Cl_K a fundamentálních jednotek

Za bázi faktorizace se vezme množina prvoideálů dělicích prvočísla $p < L$, hledají se relace mezi nimi tvaru „součin několika z nich je hlavní ideál, přitom generátor α tohoto hlavního ideálu je nalezen“. Tyto relace se uchovávají jako vektory, jejichž složky jsou celá čísla udávající exponenty tohoto součinu a v posledních $s + t$ složkách jsou komplexní logaritmy

$$(\log \sigma_1(\alpha), \dots, \log \sigma_{s+t}(\alpha)).$$

Z nich se Gaussovou eliminací odvodí relace, které určí vztahy mezi generátory grupy Cl_K , a také vektory mající jen nuly ve složkách udávajících exponenty, které odpovídají jednotkám.

Je nutné kontrolovat, zda už máme nalezeny generátory grupy jednotek a všechny relace mezi generátory Cl_K .

Využití odhadu $h_K R_K$ pro určení Cl_K a fundamentálních jednotek

Za bázi faktorizace se vezme množina prvoideálů dělicích prvočísla $p < L$, hledají se relace mezi nimi tvaru „součin několika z nich je hlavní ideál, přitom generátor α tohoto hlavního ideálu je nalezen“. Tyto relace se uchovávají jako vektory, jejichž složky jsou celá čísla udávající exponenty tohoto součinu a v posledních $s + t$ složkách jsou komplexní logaritmy

$$(\log \sigma_1(\alpha), \dots, \log \sigma_{s+t}(\alpha)).$$

Z nich se Gaussovou eliminací odvodí relace, které určí vztahy mezi generátory grupy Cl_K , a také vektory mající jen nuly ve složkách udávajících exponenty, které odpovídají jednotkám.

Je nutné kontrolovat, zda už máme nalezeny generátory grupy jednotek a všechny relace mezi generátory Cl_K .

Uurčíme počet prvků \tilde{h}_K nalezené faktorgrupy a spočítáme regulátor \tilde{R}_K generátorů dosud nalezené grupy jednotek a zjistíme, je-li součin $\tilde{h}_K \tilde{R}_K$ přibližně roven nalezenému odhadu $h_K R_K$ (chybí-li jednotky nebo relace, jde o celočíselný násobek $h_K R_K$).

Praktická využití faktu, že rozklad daného velkého přirozeného čísla na prvočinitele je obtížný

RSA (Rivest-Shamir-Adleman, 1977) - nejběžněji užívaný asymetrický kryptosystém založený na obtížnosti rozkladu čísla získaného jako součin dvou velkých prvočísel.

Praktická využití faktu, že rozklad daného velkého přirozeného čísla na prvočinitele je obtížný

RSA (Rivest-Shamir-Adleman, 1977) - nejbližší používaný asymetrický kryptosystém založený na obtížnosti rozkladu čísla získaného jako součin dvou velkých prvočísel.

Většina kryptosystémů užívajících eliptické křivky je založena na tzv. problému diskretního logaritmu (Koblitz, Miller, 1985).

Praktická využití faktu, že rozklad daného velkého přirozeného čísla na prvočinitele je obtížný

RSA (Rivest-Shamir-Adleman, 1977) - nejbližší užívaný asymetrický kryptosystém založený na obtížnosti rozkladu čísla získaného jako součin dvou velkých prvočísel.

Většina kryptosystémů užívajících eliptické křivky je založena na tzv. problému diskretního logaritmu (Koblitz, Miller, 1985).

KMOV (Koyama-Maurer-Okamoto-Vanstone, 1991) - první kryptosystém užívající eliptické křivky založený na obtížnosti rozkladu čísla získaného jako součin dvou velkých prvočísel.

Praktická využití faktu, že rozklad daného velkého přirozeného čísla na prvočinitele je obtížný

RSA (Rivest-Shamir-Adleman, 1977) - nejbližší užívaný asymetrický kryptosystém založený na obtížnosti rozkladu čísla získaného jako součin dvou velkých prvočísel.

Většina kryptosystémů užívajících eliptické křivky je založena na tzv. problému diskretního logaritmu (Koblitz, Miller, 1985).

KMOV (Koyama-Maurer-Okamoto-Vanstone, 1991) - první kryptosystém užívající eliptické křivky založený na obtížnosti rozkladu čísla získaného jako součin dvou velkých prvočísel.

Existují další podobné kryptosystémy; ukážeme si kryptosystém, který navrhli Hamad Alshehhi a Abderrahmane Nitaj (2021).

RSA

Generování klíčů: Je nutné zvolit dvě velká prvočísla p , q (přibližně stejně velká, např. $p < q < 2p$, ale s velkým rozdílem $q - p$),
 $n = pq$, λ je nejmenší společný násobek čísel $p - 1$ a $q - 1$ (je však možná i volba $\lambda = \varphi(n) = (p - 1)(q - 1)$).

RSA

Generování klíčů: Je nutné zvolit dvě velká prvočísla p , q (přibližně stejně velká, např. $p < q < 2p$, ale s velkým rozdílem $q - p$), $n = pq$, λ je nejmenší společný násobek čísel $p - 1$ a $q - 1$ (je však možná i volba $\lambda = \varphi(n) = (p - 1)(q - 1)$).

Dále je nutné zvolit $e \in \mathbb{Z}$, $e > 1$, $(e, \lambda) = 1$ (doporučuje se $e > 2^{16}$) a spočítat $f \in \mathbb{Z}$, $f > 0$, aby $ef \equiv 1 \pmod{\lambda}$.

RSA

Generování klíčů: Je nutné zvolit dvě velká prvočísla p , q (přibližně stejně velká, např. $p < q < 2p$, ale s velkým rozdílem $q - p$), $n = pq$, λ je nejmenší společný násobek čísel $p - 1$ a $q - 1$ (je však možná i volba $\lambda = \varphi(n) = (p - 1)(q - 1)$).

Dále je nutné zvolit $e \in \mathbb{Z}$, $e > 1$, $(e, \lambda) = 1$ (doporučuje se $e > 2^{16}$) a spočítat $f \in \mathbb{Z}$, $f > 0$, aby $ef \equiv 1 \pmod{\lambda}$.

Veřejný klíč: n , e .

RSA

Generování klíčů: Je nutné zvolit dvě velká prvočísla p , q (přibližně stejně velká, např. $p < q < 2p$, ale s velkým rozdílem $q - p$), $n = pq$, λ je nejmenší společný násobek čísel $p - 1$ a $q - 1$ (je však možná i volba $\lambda = \varphi(n) = (p - 1)(q - 1)$).

Dále je nutné zvolit $e \in \mathbb{Z}$, $e > 1$, $(e, \lambda) = 1$ (doporučuje se $e > 2^{16}$) a spočítat $f \in \mathbb{Z}$, $f > 0$, aby $ef \equiv 1 \pmod{\lambda}$.

Veřejný klíč: n , e .

Tajný klíč: f (také p , q , pomocí nichž lze f snadno spočítat).

RSA

Generování klíčů: Je nutné zvolit dvě velká prvočísla p, q (přibližně stejně velká, např. $p < q < 2p$, ale s velkým rozdílem $q - p$), $n = pq$, λ je nejmenší společný násobek čísel $p - 1$ a $q - 1$ (je však možná i volba $\lambda = \varphi(n) = (p - 1)(q - 1)$).

Dále je nutné zvolit $e \in \mathbb{Z}$, $e > 1$, $(e, \lambda) = 1$ (doporučuje se $e > 2^{16}$) a spočítat $f \in \mathbb{Z}$, $f > 0$, aby $ef \equiv 1 \pmod{\lambda}$.

Veřejný klíč: n, e .

Tajný klíč: f (také p, q , pomocí nichž lze f snadno spočítat).

Šifrování: Zpráva je $m \in \mathbb{Z}$, $1 < m < n$. Odesílající použije veřejný klíč a odešle zbytek po dělení čísla m^e číslem n , tj. odešle $x \in \mathbb{Z}$, $0 < x < n$, $x \equiv m^e \pmod{n}$.

RSA

Generování klíčů: Je nutné zvolit dvě velká prvočísla p, q (přibližně stejně velká, např. $p < q < 2p$, ale s velkým rozdílem $q - p$), $n = pq$, λ je nejmenší společný násobek čísel $p - 1$ a $q - 1$ (je však možná i volba $\lambda = \varphi(n) = (p - 1)(q - 1)$).

Dále je nutné zvolit $e \in \mathbb{Z}$, $e > 1$, $(e, \lambda) = 1$ (doporučuje se $e > 2^{16}$) a spočítat $f \in \mathbb{Z}$, $f > 0$, aby $ef \equiv 1 \pmod{\lambda}$.

Veřejný klíč: n, e .

Tajný klíč: f (také p, q , pomocí nichž lze f snadno spočítat).

Šifrování: Zpráva je $m \in \mathbb{Z}$, $1 < m < n$. Odesílající použije veřejný klíč a odešle zbytek po dělení čísla m^e číslem n , tj. odešle $x \in \mathbb{Z}$, $0 < x < n$, $x \equiv m^e \pmod{n}$.

Dešifrování: Příjemce použije tajný klíč, zpráva m je zbytek po dělení čísla x^f číslem n , neboť $m \equiv x^f \pmod{n}$.

RSA

Generování klíčů: Je nutné zvolit dvě velká prvočísla p, q (přibližně stejně velká, např. $p < q < 2p$, ale s velkým rozdílem $q - p$), $n = pq$, λ je nejmenší společný násobek čísel $p - 1$ a $q - 1$ (je však možná i volba $\lambda = \varphi(n) = (p - 1)(q - 1)$).

Dále je nutné zvolit $e \in \mathbb{Z}$, $e > 1$, $(e, \lambda) = 1$ (doporučuje se $e > 2^{16}$) a spočítat $f \in \mathbb{Z}$, $f > 0$, aby $ef \equiv 1 \pmod{\lambda}$.

Veřejný klíč: n, e .

Tajný klíč: f (také p, q , pomocí nichž lze f snadno spočítat).

Šifrování: Zpráva je $m \in \mathbb{Z}$, $1 < m < n$. Odesílající použije veřejný klíč a odešle zbytek po dělení čísla m^e číslem n , tj. odešle $x \in \mathbb{Z}$, $0 < x < n$, $x \equiv m^e \pmod{n}$.

Dešifrování: Příjemce použije tajný klíč, zpráva m je zbytek po dělení čísla x^f číslem n , neboť $m \equiv x^f \pmod{n}$. Protože příjemce zná prvočísla p, q , může výpočet zrychlit tím, že postupně najde zbytky po dělení čísla x^f čísly p a q a pak m určí pomocí Čínské zbytkové věty.

Okruh $\mathbb{Z}[i]$

$\mathbb{Z}[i] = \{a + bi; a, b \in \mathbb{Z}\}$ je okruh s jednoznačným rozkladem
(dokonce eukleidovský vzhledem k normě $N(a + bi) = a^2 + b^2$).

Okruh $\mathbb{Z}[i]$

$\mathbb{Z}[i] = \{a + bi; a, b \in \mathbb{Z}\}$ je okruh s jednoznačným rozkladem (dokonce eukleidovský vzhledem k normě $N(a + bi) = a^2 + b^2$).

Grupa jednotek $\mathbb{Z}[i]^\times = \{1, i, -1, -i\}$.

Okruh $\mathbb{Z}[i]$

$\mathbb{Z}[i] = \{a + bi; a, b \in \mathbb{Z}\}$ je okruh s jednoznačným rozkladem (dokonce eukleidovský vzhledem k normě $N(a + bi) = a^2 + b^2$).

Grupa jednotek $\mathbb{Z}[i]^\times = \{1, i, -1, -i\}$.

Libovolný ideál je hlavní, nenulové prvoideály jsou generovány ireducibilními prvky.

Okruh $\mathbb{Z}[i]$

$\mathbb{Z}[i] = \{a + bi; a, b \in \mathbb{Z}\}$ je okruh s jednoznačným rozkladem (dokonce eukleidovský vzhledem k normě $N(a + bi) = a^2 + b^2$).

Grupa jednotek $\mathbb{Z}[i]^\times = \{1, i, -1, -i\}$.

Libovolný ideál je hlavní, nenulové prvoideály jsou generovány ireducibilními prvky. Každý ireducibilní prvek se vyskytne v rozkladu právě jednoho prvočísla.

Okruh $\mathbb{Z}[i]$

$\mathbb{Z}[i] = \{a + bi; a, b \in \mathbb{Z}\}$ je okruh s jednoznačným rozkladem (dokonce eukleidovský vzhledem k normě $N(a + bi) = a^2 + b^2$).

Grupa jednotek $\mathbb{Z}[i]^\times = \{1, i, -1, -i\}$.

Libovolný ideál je hlavní, nenulové prvoideály jsou generovány ireducibilními prvky. Každý ireducibilní prvek se vyskytne v rozkladu právě jednoho prvočísla.

Prvočíslo $2 = -i(1 + i)^2$, $N(1 + i) = 2$.

Okruh $\mathbb{Z}[i]$

$\mathbb{Z}[i] = \{a + bi; a, b \in \mathbb{Z}\}$ je okruh s jednoznačným rozkladem (dokonce eukleidovský vzhledem k normě $N(a + bi) = a^2 + b^2$).

Grupa jednotek $\mathbb{Z}[i]^\times = \{1, i, -1, -i\}$.

Libovolný ideál je hlavní, nenulové prvoideály jsou generovány ireducibilními prvky. Každý ireducibilní prvek se vyskytne v rozkladu právě jednoho prvočísla.

Prvočíslo $2 = -i(1 + i)^2$, $N(1 + i) = 2$.

Prvočísla $q \equiv 3 \pmod{4}$ jsou ireducibilní prvky, $N(q) = q^2$.

Okruh $\mathbb{Z}[i]$

$\mathbb{Z}[i] = \{a + bi; a, b \in \mathbb{Z}\}$ je okruh s jednoznačným rozkladem (dokonce eukleidovský vzhledem k normě $N(a + bi) = a^2 + b^2$).

Grupa jednotek $\mathbb{Z}[i]^\times = \{1, i, -1, -i\}$.

Libovolný ideál je hlavní, nenulové prvoideály jsou generovány ireducibilními prvky. Každý ireducibilní prvek se vyskytne v rozkladu právě jednoho prvočísla.

Prvočíslo $2 = -i(1 + i)^2$, $N(1 + i) = 2$.

Prvočísla $q \equiv 3 \pmod{4}$ jsou ireducibilní prvky, $N(q) = q^2$.

Prvočísla $p \equiv 1 \pmod{4}$ se rozkládají na součin dvou nesoudělných ireducibilních prvků: $p = \pi\bar{\pi}$, $N(\pi) = N(\bar{\pi}) = p$.

Okruh $\mathbb{Z}[i]$

$\mathbb{Z}[i] = \{a + bi; a, b \in \mathbb{Z}\}$ je okruh s jednoznačným rozkladem (dokonce eukleidovský vzhledem k normě $N(a + bi) = a^2 + b^2$).

Grupa jednotek $\mathbb{Z}[i]^\times = \{1, i, -1, -i\}$.

Libovolný ideál je hlavní, nenulové prvoideály jsou generovány ireducibilními prvky. Každý ireducibilní prvek se vyskytne v rozkladu právě jednoho prvočísla.

Prvočíslo $2 = -i(1 + i)^2$, $N(1 + i) = 2$.

Prvočíslo $q \equiv 3 \pmod{4}$ jsou ireducibilní prvky, $N(q) = q^2$.

Prvočíslo $p \equiv 1 \pmod{4}$ se rozkládají na součin dvou nesoudělných ireducibilních prvků: $p = \pi\bar{\pi}$, $N(\pi) = N(\bar{\pi}) = p$.

Ireducibilní prvek λ se nazývá primární, jestliže $\lambda \equiv 1 \pmod{2 + 2i}$.

Okruh $\mathbb{Z}[i]$

$\mathbb{Z}[i] = \{a + bi; a, b \in \mathbb{Z}\}$ je okruh s jednoznačným rozkladem (dokonce eukleidovský vzhledem k normě $N(a + bi) = a^2 + b^2$).

Grupa jednotek $\mathbb{Z}[i]^\times = \{1, i, -1, -i\}$.

Libovolný ideál je hlavní, nenulové prvoideály jsou generovány ireducibilními prvky. Každý ireducibilní prvek se vyskytne v rozkladu právě jednoho prvočísla.

Prvočíslo $2 = -i(1 + i)^2$, $N(1 + i) = 2$.

Prvočísla $q \equiv 3 \pmod{4}$ jsou ireducibilní prvky, $N(q) = q^2$.

Prvočísla $p \equiv 1 \pmod{4}$ se rozkládají na součin dvou nesoudělných ireducibilních prvků: $p = \pi\bar{\pi}$, $N(\pi) = N(\bar{\pi}) = p$.

Ireducibilní prvek λ se nazývá primární, jestliže $\lambda \equiv 1 \pmod{2 + 2i}$.

Pro každý ireducibilní prvek $\lambda \nmid 2$ existuje jediný asociovaný prvek, který je primární.

Okruh $\mathbb{Z}[i]$

$\mathbb{Z}[i] = \{a + bi; a, b \in \mathbb{Z}\}$ je okruh s jednoznačným rozkladem (dokonce eukleidovský vzhledem k normě $N(a + bi) = a^2 + b^2$).

Grupa jednotek $\mathbb{Z}[i]^\times = \{1, i, -1, -i\}$.

Libovolný ideál je hlavní, nenulové prvoideály jsou generovány ireducibilními prvky. Každý ireducibilní prvek se vyskytne v rozkladu právě jednoho prvočísla.

Prvočíslo $2 = -i(1 + i)^2$, $N(1 + i) = 2$.

Prvočísla $q \equiv 3 \pmod{4}$ jsou ireducibilní prvky, $N(q) = q^2$.

Prvočísla $p \equiv 1 \pmod{4}$ se rozkládají na součin dvou nesoudělných ireducibilních prvků: $p = \pi\bar{\pi}$, $N(\pi) = N(\bar{\pi}) = p$.

Ireducibilní prvek λ se nazývá primární, jestliže $\lambda \equiv 1 \pmod{2 + 2i}$.

Pro každý ireducibilní prvek $\lambda \nmid 2$ existuje jediný asociovaný prvek, který je primární.

Pro libovolný ireducibilní prvek $\lambda \nmid 2$ a libovolné $\alpha \in \mathbb{Z}[i]$, $\lambda \nmid \alpha$ definujme čtvrtý mocninný symbol $(\frac{\alpha}{\lambda})_4$ čísla α vzhledem k λ podmínkou

$$\left(\frac{\alpha}{\lambda}\right)_4 \in \{1, i, -1, -i\}, \quad \left(\frac{\alpha}{\lambda}\right)_4 \equiv \alpha^{(N(\lambda)-1)/4} \pmod{\lambda}.$$

Zákon bikvadratické reciprocity v okruhu $\mathbb{Z}[i]$

Ireducibilní prvek λ se nazývá primární, jestliže $\lambda \equiv 1 \pmod{2+2i}$.

Zákon bikvadratické reciprocity v okruhu $\mathbb{Z}[i]$

Ireducibilní prvek λ se nazývá primární, jestliže $\lambda \equiv 1 \pmod{2+2i}$.

Pro libovolný ireducibilní prvek $\lambda \nmid 2$ a libovolné $\alpha \in \mathbb{Z}[i]$, $\lambda \nmid \alpha$ definujeme čtvrtý mocninný symbol $(\frac{\alpha}{\lambda})_4$ čísla α vzhledem k λ podmínkou $(\frac{\alpha}{\lambda})_4 \in \{1, i, -1, -i\}$, $(\frac{\alpha}{\lambda})_4 \equiv \alpha^{(N(\lambda)-1)/4} \pmod{\lambda}$.

Zákon bikvadratické reciprocity v okruhu $\mathbb{Z}[i]$

Ireducibilní prvek λ se nazývá primární, jestliže $\lambda \equiv 1 \pmod{2+2i}$.

Pro libovolný ireducibilní prvek $\lambda \nmid 2$ a libovolné $\alpha \in \mathbb{Z}[i]$, $\lambda \nmid \alpha$ definujeme čtvrtý mocninný symbol $(\frac{\alpha}{\lambda})_4$ čísla α vzhledem k λ podmínkou $(\frac{\alpha}{\lambda})_4 \in \{1, i, -1, -i\}$, $(\frac{\alpha}{\lambda})_4 \equiv \alpha^{(N(\lambda)-1)/4} \pmod{\lambda}$.

Existence a jednoznačnost mocninného symbolu $(\frac{\alpha}{\lambda})_4$ plyne z toho, že $\mathbb{Z}[i]/(\lambda)$ je těleso mající $N(\lambda)$ prvků, v němž polynom $x^4 - 1$ má čtyři různé kořeny (třídy obsahující čísla $1, i, -1, -i$).

Zákon bikvadratické reciprocity v okruhu $\mathbb{Z}[i]$

Ireducibilní prvek λ se nazývá primární, jestliže $\lambda \equiv 1 \pmod{2+2i}$.

Pro libovolný ireducibilní prvek $\lambda \nmid 2$ a libovolné $\alpha \in \mathbb{Z}[i]$, $\lambda \nmid \alpha$ definujeme čtvrtý mocninný symbol $(\frac{\alpha}{\lambda})_4$ čísla α vzhledem k λ podmínkou $(\frac{\alpha}{\lambda})_4 \in \{1, i, -1, -i\}$, $(\frac{\alpha}{\lambda})_4 \equiv \alpha^{(N(\lambda)-1)/4} \pmod{\lambda}$.

Existence a jednoznačnost mocninného symbolu $(\frac{\alpha}{\lambda})_4$ plyne z toho, že $\mathbb{Z}[i]/(\lambda)$ je těleso mající $N(\lambda)$ prvků, v němž polynom $x^4 - 1$ má čtyři různé kořeny (třídy obsahující čísla $1, i, -1, -i$). Z $\lambda \nmid \alpha$ plyne $\alpha^{N(\lambda)-1} \equiv 1 \pmod{\lambda}$, a tedy $\alpha^{(N(\lambda)-1)/4}$ je jeden z kořenů.

Zákon bikvadratické reciprocity v okruhu $\mathbb{Z}[i]$

Ireducibilní prvek λ se nazývá primární, jestliže $\lambda \equiv 1 \pmod{2+2i}$.
Pro libovolný ireducibilní prvek $\lambda \nmid 2$ a libovolné $\alpha \in \mathbb{Z}[i]$, $\lambda \nmid \alpha$
definujeme čtvrtý mocninný symbol $(\frac{\alpha}{\lambda})_4$ čísla α vzhledem k λ
podmínkou $(\frac{\alpha}{\lambda})_4 \in \{1, i, -1, -i\}$, $(\frac{\alpha}{\lambda})_4 \equiv \alpha^{(N(\lambda)-1)/4} \pmod{\lambda}$.

Existence a jednoznačnost mocninného symbolu $(\frac{\alpha}{\lambda})_4$ plyne z toho,
že $\mathbb{Z}[i]/(\lambda)$ je těleso mající $N(\lambda)$ prvků, v němž polynom $x^4 - 1$
má čtyři různé kořeny (třídy obsahující čísla $1, i, -1, -i$). Z $\lambda \nmid \alpha$
plyne $\alpha^{N(\lambda)-1} \equiv 1 \pmod{\lambda}$, a tedy $\alpha^{(N(\lambda)-1)/4}$ je jeden z kořenů.

Věta 1. *Nechť $\lambda \in \mathbb{Z}[i]$ je ireducibilní, $\lambda \nmid 2$, $\alpha, \beta \in \mathbb{Z}[i]$, $\lambda \nmid \alpha\beta$. Pak*

$$\blacktriangleright x^4 \equiv \alpha \pmod{\lambda} \text{ má řešení v } \mathbb{Z}[i] \iff \left(\frac{\alpha}{\lambda}\right)_4 = 1,$$

Zákon bikvadratické reciprocity v okruhu $\mathbb{Z}[i]$

Ireducibilní prvek λ se nazývá primární, jestliže $\lambda \equiv 1 \pmod{2+2i}$.
Pro libovolný ireducibilní prvek $\lambda \nmid 2$ a libovolné $\alpha \in \mathbb{Z}[i]$, $\lambda \nmid \alpha$ definujeme čtvrtý mocninný symbol $(\frac{\alpha}{\lambda})_4$ čísla α vzhledem k λ podmínkou $(\frac{\alpha}{\lambda})_4 \in \{1, i, -1, -i\}$, $(\frac{\alpha}{\lambda})_4 \equiv \alpha^{(N(\lambda)-1)/4} \pmod{\lambda}$.

Existence a jednoznačnost mocninného symbolu $(\frac{\alpha}{\lambda})_4$ plyne z toho, že $\mathbb{Z}[i]/(\lambda)$ je těleso mající $N(\lambda)$ prvků, v němž polynom $x^4 - 1$ má čtyři různé kořeny (třídy obsahující čísla $1, i, -1, -i$). Z $\lambda \nmid \alpha$ plyne $\alpha^{N(\lambda)-1} \equiv 1 \pmod{\lambda}$, a tedy $\alpha^{(N(\lambda)-1)/4}$ je jeden z kořenů.

Věta 1. *Nechť $\lambda \in \mathbb{Z}[i]$ je ireducibilní, $\lambda \nmid 2$, $\alpha, \beta \in \mathbb{Z}[i]$, $\lambda \nmid \alpha\beta$. Pak*

- ▶ $x^4 \equiv \alpha \pmod{\lambda}$ má řešení v $\mathbb{Z}[i]$ $\iff (\frac{\alpha}{\lambda})_4 = 1$,
- ▶ $(\frac{\alpha\beta}{\lambda})_4 = (\frac{\alpha}{\lambda})_4 (\frac{\beta}{\lambda})_4$,

Zákon bikvadratické reciprocity v okruhu $\mathbb{Z}[i]$

Ireducibilní prvek λ se nazývá primární, jestliže $\lambda \equiv 1 \pmod{2+2i}$.

Pro libovolný ireducibilní prvek $\lambda \nmid 2$ a libovolné $\alpha \in \mathbb{Z}[i]$, $\lambda \nmid \alpha$ definujeme čtvrtý mocninný symbol $(\frac{\alpha}{\lambda})_4$ čísla α vzhledem k λ podmínkou $(\frac{\alpha}{\lambda})_4 \in \{1, i, -1, -i\}$, $(\frac{\alpha}{\lambda})_4 \equiv \alpha^{(N(\lambda)-1)/4} \pmod{\lambda}$.

Existence a jednoznačnost mocninného symbolu $(\frac{\alpha}{\lambda})_4$ plyne z toho, že $\mathbb{Z}[i]/(\lambda)$ je těleso mající $N(\lambda)$ prvků, v němž polynom $x^4 - 1$ má čtyři různé kořeny (třídy obsahující čísla $1, i, -1, -i$). Z $\lambda \nmid \alpha$ plyne $\alpha^{N(\lambda)-1} \equiv 1 \pmod{\lambda}$, a tedy $\alpha^{(N(\lambda)-1)/4}$ je jeden z kořenů.

Věta 1. *Nechť $\lambda \in \mathbb{Z}[i]$ je ireducibilní, $\lambda \nmid 2$, $\alpha, \beta \in \mathbb{Z}[i]$, $\lambda \nmid \alpha\beta$. Pak*

- ▶ $x^4 \equiv \alpha \pmod{\lambda}$ má řešení v $\mathbb{Z}[i]$ $\iff (\frac{\alpha}{\lambda})_4 = 1$,
- ▶ $(\frac{\alpha\beta}{\lambda})_4 = (\frac{\alpha}{\lambda})_4 (\frac{\beta}{\lambda})_4$,
- ▶ $\alpha \equiv \beta \pmod{\lambda} \implies (\frac{\alpha}{\lambda})_4 = (\frac{\beta}{\lambda})_4$.

Zákon bikvadratické reciprocity v okruhu $\mathbb{Z}[i]$

Ireducibilní prvek λ se nazývá primární, jestliže $\lambda \equiv 1 \pmod{2+2i}$.
Pro libovolný ireducibilní prvek $\lambda \nmid 2$ a libovolné $\alpha \in \mathbb{Z}[i]$, $\lambda \nmid \alpha$ definujeme čtvrtý mocninný symbol $(\frac{\alpha}{\lambda})_4$ čísla α vzhledem k λ podmínkou $(\frac{\alpha}{\lambda})_4 \in \{1, i, -1, -i\}$, $(\frac{\alpha}{\lambda})_4 \equiv \alpha^{(N(\lambda)-1)/4} \pmod{\lambda}$.

Existence a jednoznačnost mocninného symbolu $(\frac{\alpha}{\lambda})_4$ plyne z toho, že $\mathbb{Z}[i]/(\lambda)$ je těleso mající $N(\lambda)$ prvků, v němž polynom $x^4 - 1$ má čtyři různé kořeny (třídy obsahující čísla $1, i, -1, -i$). Z $\lambda \nmid \alpha$ plyne $\alpha^{N(\lambda)-1} \equiv 1 \pmod{\lambda}$, a tedy $\alpha^{(N(\lambda)-1)/4}$ je jeden z kořenů.

Věta 1. *Nechť $\lambda \in \mathbb{Z}[i]$ je ireducibilní, $\lambda \nmid 2$, $\alpha, \beta \in \mathbb{Z}[i]$, $\lambda \nmid \alpha\beta$. Pak*

- ▶ $x^4 \equiv \alpha \pmod{\lambda}$ má řešení v $\mathbb{Z}[i]$ $\iff (\frac{\alpha}{\lambda})_4 = 1$,
- ▶ $(\frac{\alpha\beta}{\lambda})_4 = (\frac{\alpha}{\lambda})_4 (\frac{\beta}{\lambda})_4$,
- ▶ $\alpha \equiv \beta \pmod{\lambda} \implies (\frac{\alpha}{\lambda})_4 = (\frac{\beta}{\lambda})_4$.

Věta 2. *Jestliže π a λ jsou nesoudělné primární ireducibilní prvky, pak*

$$(\frac{\pi}{\lambda})_4 = (\frac{\lambda}{\pi})_4 \cdot (-1)^{(N(\pi)-1)(N(\lambda)-1)/16}.$$

Počet bodů na eliptické křivce $y^2 = x^3 - ax$ nad \mathbb{Z}_p

Věta 3. Necht' p je prvočíslo, $a \in \mathbb{Z}$, přičemž $p \neq 2$, $p \nmid a$.

Počet bodů na eliptické křivce $y^2 = x^3 - ax$ nad \mathbb{Z}_p

Věta 3. Necht' p je prvočíslo, $a \in \mathbb{Z}$, přičemž $p \neq 2$, $p \nmid a$. Necht' N je počet bodů na eliptické křivce $y^2 = x^3 - ax$ nad \mathbb{Z}_p .

Počet bodů na eliptické křivce $y^2 = x^3 - ax$ nad \mathbb{Z}_p

Věta 3. Necht' p je prvočíslo, $a \in \mathbb{Z}$, přičemž $p \neq 2$, $p \nmid a$. Necht' N je počet bodů na eliptické křivce $y^2 = x^3 - ax$ nad \mathbb{Z}_p .

- ▶ Je-li $p \equiv 3 \pmod{4}$, pak $N = p + 1$.

Počet bodů na eliptické křivce $y^2 = x^3 - ax$ nad \mathbb{Z}_p

Věta 3. Necht' p je prvočíslo, $a \in \mathbb{Z}$, přičemž $p \neq 2$, $p \nmid a$. Necht' N je počet bodů na eliptické křivce $y^2 = x^3 - ax$ nad \mathbb{Z}_p .

- ▶ Je-li $p \equiv 3 \pmod{4}$, pak $N = p + 1$.
- ▶ Je-li $p \equiv 1 \pmod{4}$ a $p = \pi\bar{\pi}$ je rozklad čísla p na součin dvou primárních ireducibilních prvků v $\mathbb{Z}[i]$, pak

$$N = p + 1 - \overline{\left(\frac{a}{\pi}\right)}_4 \cdot \pi - \left(\frac{a}{\pi}\right)_4 \cdot \bar{\pi}.$$

Počet bodů na eliptické křivce $y^2 = x^3 - ax$ nad \mathbb{Z}_p

Věta 3. *Nechť p je prvočíslo, $a \in \mathbb{Z}$, přičemž $p \neq 2$, $p \nmid a$. Necht' N je počet bodů na eliptické křivce $y^2 = x^3 - ax$ nad \mathbb{Z}_p .*

- ▶ *Je-li $p \equiv 3 \pmod{4}$, pak $N = p + 1$.*
- ▶ *Je-li $p \equiv 1 \pmod{4}$ a $p = \pi\bar{\pi}$ je rozklad čísla p na součin dvou primárních ireducibilních prvků v $\mathbb{Z}[i]$, pak*

$$N = p + 1 - \overline{\left(\frac{a}{\pi}\right)_4} \cdot \pi - \left(\frac{a}{\pi}\right)_4 \cdot \bar{\pi}.$$

Dokažme větu jen pro lehčí první případ: je-li $p \equiv 3 \pmod{4}$, pak Legendreův symbol $\left(\frac{-1}{p}\right) = -1$.

Počet bodů na eliptické křivce $y^2 = x^3 - ax$ nad \mathbb{Z}_p

Věta 3. *Nechť p je prvočíslo, $a \in \mathbb{Z}$, přičemž $p \neq 2$, $p \nmid a$. Necht' N je počet bodů na eliptické křivce $y^2 = x^3 - ax$ nad \mathbb{Z}_p .*

- ▶ *Je-li $p \equiv 3 \pmod{4}$, pak $N = p + 1$.*
- ▶ *Je-li $p \equiv 1 \pmod{4}$ a $p = \pi\bar{\pi}$ je rozklad čísla p na součin dvou primárních ireducibilních prvků v $\mathbb{Z}[i]$, pak*

$$N = p + 1 - \overline{\left(\frac{a}{\pi}\right)}_4 \cdot \pi - \left(\frac{a}{\pi}\right)_4 \cdot \bar{\pi}.$$

Dokažme větu jen pro lehčí první případ: je-li $p \equiv 3 \pmod{4}$, pak Legendreův symbol $\left(\frac{-1}{p}\right) = -1$. Na eliptické křivce leží nevlastní bod O a bod $[0, 0]$.

Počet bodů na eliptické křivce $y^2 = x^3 - ax$ nad \mathbb{Z}_p

Věta 3. *Nechť p je prvočíslo, $a \in \mathbb{Z}$, přičemž $p \neq 2$, $p \nmid a$. Necht' N je počet bodů na eliptické křivce $y^2 = x^3 - ax$ nad \mathbb{Z}_p .*

- ▶ *Je-li $p \equiv 3 \pmod{4}$, pak $N = p + 1$.*
- ▶ *Je-li $p \equiv 1 \pmod{4}$ a $p = \pi\bar{\pi}$ je rozklad čísla p na součin dvou primárních ireducibilních prvků v $\mathbb{Z}[i]$, pak*

$$N = p + 1 - \overline{\left(\frac{a}{\pi}\right)}_4 \cdot \pi - \left(\frac{a}{\pi}\right)_4 \cdot \bar{\pi}.$$

Dokažme větu jen pro lehčí první případ: je-li $p \equiv 3 \pmod{4}$, pak Legendreův symbol $\left(\frac{-1}{p}\right) = -1$. Na eliptické křivce leží nevlastní bod O a bod $[0, 0]$. Pro každé $u = 1, \dots, \frac{p-1}{2}$ spočítejme počet bodů, jejichž x -ová souřadnice je $\pm u$.

Počet bodů na eliptické křivce $y^2 = x^3 - ax$ nad \mathbb{Z}_p

Věta 3. *Nechť p je prvočíslo, $a \in \mathbb{Z}$, přičemž $p \neq 2$, $p \nmid a$. Necht' N je počet bodů na eliptické křivce $y^2 = x^3 - ax$ nad \mathbb{Z}_p .*

- ▶ *Je-li $p \equiv 3 \pmod{4}$, pak $N = p + 1$.*
- ▶ *Je-li $p \equiv 1 \pmod{4}$ a $p = \pi\bar{\pi}$ je rozklad čísla p na součin dvou primárních ireducibilních prvků v $\mathbb{Z}[i]$, pak*

$$N = p + 1 - \overline{\left(\frac{a}{\pi}\right)}_4 \cdot \pi - \left(\frac{a}{\pi}\right)_4 \cdot \bar{\pi}.$$

Dokažme větu jen pro lehčí první případ: je-li $p \equiv 3 \pmod{4}$, pak Legendreův symbol $\left(\frac{-1}{p}\right) = -1$. Na eliptické křivce leží nevlastní bod O a bod $[0, 0]$. Pro každé $u = 1, \dots, \frac{p-1}{2}$ spočítejme počet bodů, jejichž x -ová souřadnice je $\pm u$. Označme $v = u^3 - au$.

Počet bodů na eliptické křivce $y^2 = x^3 - ax$ nad \mathbb{Z}_p

Věta 3. *Nechť p je prvočíslo, $a \in \mathbb{Z}$, přičemž $p \neq 2$, $p \nmid a$. Necht' N je počet bodů na eliptické křivce $y^2 = x^3 - ax$ nad \mathbb{Z}_p .*

- ▶ *Je-li $p \equiv 3 \pmod{4}$, pak $N = p + 1$.*
- ▶ *Je-li $p \equiv 1 \pmod{4}$ a $p = \pi\bar{\pi}$ je rozklad čísla p na součin dvou primárních ireducibilních prvků v $\mathbb{Z}[i]$, pak*

$$N = p + 1 - \overline{\left(\frac{a}{\pi}\right)}_4 \cdot \pi - \left(\frac{a}{\pi}\right)_4 \cdot \bar{\pi}.$$

Dokažme větu jen pro lehčí první případ: je-li $p \equiv 3 \pmod{4}$, pak Legendreův symbol $\left(\frac{-1}{p}\right) = -1$. Na eliptické křivce leží nevlastní bod O a bod $[0, 0]$. Pro každé $u = 1, \dots, \frac{p-1}{2}$ spočítejme počet bodů, jejichž x -ová souřadnice je $\pm u$. Označme $v = u^3 - au$. Je-li $v = 0$, máme dva body $[u, 0], [-u, 0]$.

Počet bodů na eliptické křivce $y^2 = x^3 - ax$ nad \mathbb{Z}_p

Věta 3. *Nechť p je prvočíslo, $a \in \mathbb{Z}$, přičemž $p \neq 2$, $p \nmid a$. Necht' N je počet bodů na eliptické křivce $y^2 = x^3 - ax$ nad \mathbb{Z}_p .*

- ▶ *Je-li $p \equiv 3 \pmod{4}$, pak $N = p + 1$.*
- ▶ *Je-li $p \equiv 1 \pmod{4}$ a $p = \pi\bar{\pi}$ je rozklad čísla p na součin dvou primárních ireducibilních prvků v $\mathbb{Z}[i]$, pak*

$$N = p + 1 - \overline{\left(\frac{a}{\pi}\right)}_4 \cdot \pi - \left(\frac{a}{\pi}\right)_4 \cdot \bar{\pi}.$$

Dokažme větu jen pro lehčí první případ: je-li $p \equiv 3 \pmod{4}$, pak Legendreův symbol $\left(\frac{-1}{p}\right) = -1$. Na eliptické křivce leží nevlastní bod O a bod $[0, 0]$. Pro každé $u = 1, \dots, \frac{p-1}{2}$ spočítejme počet bodů, jejichž x -ová souřadnice je $\pm u$. Označme $v = u^3 - au$. Je-li $v = 0$, máme dva body $[u, 0]$, $[-u, 0]$. Je-li $v \neq 0$, je právě jedno z čísel v , $-v$ kvadratický zbytek modulo p , a tedy z kongruencí $y^2 \equiv v \pmod{p}$ a $y^2 \equiv -v \pmod{p}$ má jedna dvě řešení a druhá žádné.

Počet bodů na eliptické křivce $y^2 = x^3 - ax$ nad \mathbb{Z}_p

Věta 3. *Nechť p je prvočíslo, $a \in \mathbb{Z}$, přičemž $p \neq 2$, $p \nmid a$. Necht' N je počet bodů na eliptické křivce $y^2 = x^3 - ax$ nad \mathbb{Z}_p .*

- ▶ *Je-li $p \equiv 3 \pmod{4}$, pak $N = p + 1$.*
- ▶ *Je-li $p \equiv 1 \pmod{4}$ a $p = \pi\bar{\pi}$ je rozklad čísla p na součin dvou primárních ireducibilních prvků v $\mathbb{Z}[i]$, pak*

$$N = p + 1 - \overline{\left(\frac{a}{\pi}\right)}_4 \cdot \pi - \left(\frac{a}{\pi}\right)_4 \cdot \bar{\pi}.$$

Dokažme větu jen pro lehčí první případ: je-li $p \equiv 3 \pmod{4}$, pak Legendreův symbol $\left(\frac{-1}{p}\right) = -1$. Na eliptické křivce leží nevlastní

bod O a bod $[0, 0]$. Pro každé $u = 1, \dots, \frac{p-1}{2}$ spočítejme počet bodů, jejichž x -ová souřadnice je $\pm u$. Označme $v = u^3 - au$.

Je-li $v = 0$, máme dva body $[u, 0]$, $[-u, 0]$.

Je-li $v \neq 0$, je právě jedno z čísel v , $-v$ kvadratický zbytek modulo p , a tedy z kongruencí $y^2 \equiv v \pmod{p}$ a $y^2 \equiv -v \pmod{p}$ má jedna dvě řešení a druhá žádné. Proto opět dostáváme dva body, jejichž x -ová souřadnice je $\pm u$.

Příklad: eliptická křivka $y^2 = x^3 - 2x$ nad \mathbb{Z}_{101}

Rozložme $p = 101$ v $\mathbb{Z}[i]$.

Příklad: eliptická křivka $y^2 = x^3 - 2x$ nad \mathbb{Z}_{101}

Rozložme $p = 101$ v $\mathbb{Z}[i]$.

Platí $p = 101 = (10 + i)(10 - i) = (1 + 10i)(1 - 10i)$. Označme $\pi = -1 + 10i$, pak π je primární.

Příklad: eliptická křivka $y^2 = x^3 - 2x$ nad \mathbb{Z}_{101}

Rozložme $p = 101$ v $\mathbb{Z}[i]$.

Platí $p = 101 = (10 + i)(10 - i) = (1 + 10i)(1 - 10i)$. Označme $\pi = -1 + 10i$, pak π je primární. Víme, že

$$\left(\frac{2}{\pi}\right)_4 \in \{1, i, -1, -i\}, \quad \left(\frac{2}{\pi}\right)_4 \equiv 2^{(N(\pi)-1)/4} = 2^{25} \pmod{\pi}.$$

Příklad: eliptická křivka $y^2 = x^3 - 2x$ nad \mathbb{Z}_{101}

Rozložme $p = 101$ v $\mathbb{Z}[i]$.

Platí $p = 101 = (10 + i)(10 - i) = (1 + 10i)(1 - 10i)$. Označme $\pi = -1 + 10i$, pak π je primární. Víme, že

$$\left(\frac{2}{\pi}\right)_4 \in \{1, i, -1, -i\}, \quad \left(\frac{2}{\pi}\right)_4 \equiv 2^{(N(\pi)-1)/4} = 2^{25} \pmod{\pi}.$$

Protože $2^{25} \equiv 10 \pmod{101}$, je

$$\left(\frac{2}{\pi}\right)_4 \equiv 10 \equiv 100i \equiv -i \pmod{\pi},$$

a tedy $\left(\frac{2}{\pi}\right)_4 = -i$.

Příklad: eliptická křivka $y^2 = x^3 - 2x$ nad \mathbb{Z}_{101}

Rozložme $p = 101$ v $\mathbb{Z}[i]$.

Platí $p = 101 = (10 + i)(10 - i) = (1 + 10i)(1 - 10i)$. Označme $\pi = -1 + 10i$, pak π je primární. Víme, že

$$\left(\frac{2}{\pi}\right)_4 \in \{1, i, -1, -i\}, \quad \left(\frac{2}{\pi}\right)_4 \equiv 2^{(N(\pi)-1)/4} = 2^{25} \pmod{\pi}.$$

Protože $2^{25} \equiv 10 \pmod{101}$, je

$$\left(\frac{2}{\pi}\right)_4 \equiv 10 \equiv 100i \equiv -i \pmod{\pi},$$

a tedy $\left(\frac{2}{\pi}\right)_4 = -i$. Podle věty 3 pro počet N bodů na eliptické křivce $y^2 = x^3 - 2x$ nad \mathbb{Z}_{101} platí

$$N = p + 1 - \overline{\left(\frac{2}{\pi}\right)_4} \cdot \pi - \left(\frac{2}{\pi}\right)_4 \cdot \bar{\pi} = 102 - i \cdot \pi + i \cdot \bar{\pi} = 122.$$

Okruh $\mathbb{Z}[\omega]$, kde $\omega = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$

$\mathbb{Z}[\omega] = \{a + b\omega; a, b \in \mathbb{Z}\}$ je okruh s jednoznačným rozkladem
(dokonce eukleidovský vzhledem k $N(a + b\omega) = a^2 - ab + b^2$).

Okruh $\mathbb{Z}[\omega]$, kde $\omega = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$

$\mathbb{Z}[\omega] = \{a + b\omega; a, b \in \mathbb{Z}\}$ je okruh s jednoznačným rozkladem (dokonce eukleidovský vzhledem k $N(a + b\omega) = a^2 - ab + b^2$).

Grupa jednotek $\mathbb{Z}[\omega]^\times = \{1, \omega, \omega^2, -1, -\omega, -\omega^2\}$.

Okruh $\mathbb{Z}[\omega]$, kde $\omega = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$

$\mathbb{Z}[\omega] = \{a + b\omega; a, b \in \mathbb{Z}\}$ je okruh s jednoznačným rozkladem (dokonce eukleidovský vzhledem k $N(a + b\omega) = a^2 - ab + b^2$).

Grupa jednotek $\mathbb{Z}[i]^\times = \{1, \omega, \omega^2, -1, -\omega, -\omega^2\}$.

Libovolný ideál je hlavní, nenulové prvoideály jsou generovány ireducibilními prvky.

Okruh $\mathbb{Z}[\omega]$, kde $\omega = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$

$\mathbb{Z}[\omega] = \{a + b\omega; a, b \in \mathbb{Z}\}$ je okruh s jednoznačným rozkladem (dokonce eukleidovský vzhledem k $N(a + b\omega) = a^2 - ab + b^2$).

Grupa jednotek $\mathbb{Z}[\omega]^\times = \{1, \omega, \omega^2, -1, -\omega, -\omega^2\}$.

Libovolný ideál je hlavní, nenulové prvoideály jsou generovány ireducibilními prvky. Každý ireducibilní prvek se vyskytne v rozkladu právě jednoho prvočísla.

Okruh $\mathbb{Z}[\omega]$, kde $\omega = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$

$\mathbb{Z}[\omega] = \{a + b\omega; a, b \in \mathbb{Z}\}$ je okruh s jednoznačným rozkladem (dokonce eukleidovský vzhledem k $N(a + b\omega) = a^2 - ab + b^2$).

Grupa jednotek $\mathbb{Z}[\omega]^\times = \{1, \omega, \omega^2, -1, -\omega, -\omega^2\}$.

Libovolný ideál je hlavní, nenulové prvoideály jsou generovány ireducibilními prvky. Každý ireducibilní prvek se vyskytne v rozkladu právě jednoho prvočísla.

Prvočíslo $3 = -\omega^2(1 - \omega)^2$, $N(1 - \omega) = 3$.

Okruh $\mathbb{Z}[\omega]$, kde $\omega = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$

$\mathbb{Z}[\omega] = \{a + b\omega; a, b \in \mathbb{Z}\}$ je okruh s jednoznačným rozkladem (dokonce eukleidovský vzhledem k $N(a + b\omega) = a^2 - ab + b^2$).

Grupa jednotek $\mathbb{Z}[i]^\times = \{1, \omega, \omega^2, -1, -\omega, -\omega^2\}$.

Libovolný ideál je hlavní, nenulové prvoideály jsou generovány ireducibilními prvky. Každý ireducibilní prvek se vyskytne v rozkladu právě jednoho prvočísla.

Prvočíslo $3 = -\omega^2(1 - \omega)^2$, $N(1 - \omega) = 3$.

Prvočísla $q \equiv 2 \pmod{3}$ jsou ireducibilní prvky, $N(q) = q^2$.

Okruh $\mathbb{Z}[\omega]$, kde $\omega = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$

$\mathbb{Z}[\omega] = \{a + b\omega; a, b \in \mathbb{Z}\}$ je okruh s jednoznačným rozkladem (dokonce eukleidovský vzhledem k $N(a + b\omega) = a^2 - ab + b^2$).

Grupa jednotek $\mathbb{Z}[i]^\times = \{1, \omega, \omega^2, -1, -\omega, -\omega^2\}$.

Libovolný ideál je hlavní, nenulové prvoideály jsou generovány ireducibilními prvky. Každý ireducibilní prvek se vyskytne v rozkladu právě jednoho prvočísla.

Prvočíslo $3 = -\omega^2(1 - \omega)^2$, $N(1 - \omega) = 3$.

Prvočísla $q \equiv 2 \pmod{3}$ jsou ireducibilní prvky, $N(q) = q^2$.

Prvočísla $p \equiv 1 \pmod{3}$ se rozkládají na součin dvou nesoudělných ireducibilních prvků: $p = \pi\bar{\pi}$, $N(\pi) = N(\bar{\pi}) = p$.

Okruh $\mathbb{Z}[\omega]$, kde $\omega = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$

$\mathbb{Z}[\omega] = \{a + b\omega; a, b \in \mathbb{Z}\}$ je okruh s jednoznačným rozkladem (dokonce eukleidovský vzhledem k $N(a + b\omega) = a^2 - ab + b^2$).

Grupa jednotek $\mathbb{Z}[i]^\times = \{1, \omega, \omega^2, -1, -\omega, -\omega^2\}$.

Libovolný ideál je hlavní, nenulové prvoideály jsou generovány ireducibilními prvky. Každý ireducibilní prvek se vyskytne v rozkladu právě jednoho prvočísla.

Prvočíslo $3 = -\omega^2(1 - \omega)^2$, $N(1 - \omega) = 3$.

Prvočísla $q \equiv 2 \pmod{3}$ jsou ireducibilní prvky, $N(q) = q^2$.

Prvočísla $p \equiv 1 \pmod{3}$ se rozkládají na součin dvou nesoudělných ireducibilních prvků: $p = \pi\bar{\pi}$, $N(\pi) = N(\bar{\pi}) = p$.

Ireducibilní prvek λ se nazývá primární, jestliže $\lambda \equiv 2 \pmod{3}$.

Okruh $\mathbb{Z}[\omega]$, kde $\omega = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$

$\mathbb{Z}[\omega] = \{a + b\omega; a, b \in \mathbb{Z}\}$ je okruh s jednoznačným rozkladem (dokonce eukleidovský vzhledem k $N(a + b\omega) = a^2 - ab + b^2$).

Grupa jednotek $\mathbb{Z}[i]^\times = \{1, \omega, \omega^2, -1, -\omega, -\omega^2\}$.

Libovolný ideál je hlavní, nenulové prvoideály jsou generovány ireducibilními prvky. Každý ireducibilní prvek se vyskytne v rozkladu právě jednoho prvočísla.

Prvočíslo $3 = -\omega^2(1 - \omega)^2$, $N(1 - \omega) = 3$.

Prvočísla $q \equiv 2 \pmod{3}$ jsou ireducibilní prvky, $N(q) = q^2$.

Prvočísla $p \equiv 1 \pmod{3}$ se rozkládají na součin dvou nesoudělných ireducibilních prvků: $p = \pi\bar{\pi}$, $N(\pi) = N(\bar{\pi}) = p$.

Ireducibilní prvek λ se nazývá primární, jestliže $\lambda \equiv 2 \pmod{3}$.

Pro každý ireducibilní prvek $\lambda \nmid 3$ existuje jediný asociovaný prvek, který je primární.

Okruh $\mathbb{Z}[\omega]$, kde $\omega = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$

$\mathbb{Z}[\omega] = \{a + b\omega; a, b \in \mathbb{Z}\}$ je okruh s jednoznačným rozkladem (dokonce eukleidovský vzhledem k $N(a + b\omega) = a^2 - ab + b^2$).

Grupa jednotek $\mathbb{Z}[i]^\times = \{1, \omega, \omega^2, -1, -\omega, -\omega^2\}$.

Libovolný ideál je hlavní, nenulové prvoideály jsou generovány ireducibilními prvky. Každý ireducibilní prvek se vyskytne v rozkladu právě jednoho prvočísla.

Prvočíslo $3 = -\omega^2(1 - \omega)^2$, $N(1 - \omega) = 3$.

Prvočísla $q \equiv 2 \pmod{3}$ jsou ireducibilní prvky, $N(q) = q^2$.

Prvočísla $p \equiv 1 \pmod{3}$ se rozkládají na součin dvou nesoudělných ireducibilních prvků: $p = \pi\bar{\pi}$, $N(\pi) = N(\bar{\pi}) = p$.

Ireducibilní prvek λ se nazývá primární, jestliže $\lambda \equiv 2 \pmod{3}$.

Pro každý ireducibilní prvek $\lambda \nmid 3$ existuje jediný asociovaný prvek, který je primární.

Pro libovolný ireducibilní prvek $\lambda \nmid 3$ a libovolné $\alpha \in \mathbb{Z}[i]$, $\lambda \nmid \alpha$ definujme šestý mocninný symbol $(\frac{\alpha}{\lambda})_6$ čísla α vzhledem k λ podmínkou

$$\left(\frac{\alpha}{\lambda}\right)_6 \in \{\pm 1, \pm\omega, \pm\omega^2\}, \quad \left(\frac{\alpha}{\lambda}\right)_6 \equiv \alpha^{(N(\lambda)-1)/6} \pmod{\lambda}.$$

Zákon kubické reciprocity v okruhu $\mathbb{Z}[\omega]$

Ireducibilní prvek λ se nazývá primární, jestliže $\lambda \equiv 2 \pmod{3}$.

Zákon kubické reciprocity v okruhu $\mathbb{Z}[\omega]$

Ireducibilní prvek λ se nazývá primární, jestliže $\lambda \equiv 2 \pmod{3}$.
Pro libovolný ireducibilní prvek $\lambda \nmid 3$ a libovolné $\alpha \in \mathbb{Z}[i]$, $\lambda \nmid \alpha$
definujeme šestý mocninný symbol $(\frac{\alpha}{\lambda})_6$ čísla α vzhledem k λ
podmínkou $(\frac{\alpha}{\lambda})_6 \in \{\pm 1, \pm\omega, \pm\omega^2\}$, $(\frac{\alpha}{\lambda})_6 \equiv \alpha^{(N(\lambda)-1)/6} \pmod{\lambda}$.

Zákon kubické reciprocity v okruhu $\mathbb{Z}[\omega]$

Ireducibilní prvek λ se nazývá primární, jestliže $\lambda \equiv 2 \pmod{3}$.
Pro libovolný ireducibilní prvek $\lambda \nmid 3$ a libovolné $\alpha \in \mathbb{Z}[i]$, $\lambda \nmid \alpha$
definujeme šestý mocninný symbol $(\frac{\alpha}{\lambda})_6$ čísla α vzhledem k λ
podmínkou $(\frac{\alpha}{\lambda})_6 \in \{\pm 1, \pm\omega, \pm\omega^2\}$, $(\frac{\alpha}{\lambda})_6 \equiv \alpha^{(N(\lambda)-1)/6} \pmod{\lambda}$.

Existence a jednoznačnost mocninného symbolu $(\frac{\alpha}{\lambda})_6$ plyne z toho,
že těleso $\mathbb{Z}[\omega]/(\lambda)$ má $N(\lambda)$ prvků a polynom $x^6 - 1$ v něm má
šest různých kořenů (třídy obsahující čísla $\pm 1, \pm\omega, \pm\omega^2$).

Zákon kubické reciprocity v okruhu $\mathbb{Z}[\omega]$

Ireducibilní prvek λ se nazývá primární, jestliže $\lambda \equiv 2 \pmod{3}$.
Pro libovolný ireducibilní prvek $\lambda \nmid 3$ a libovolné $\alpha \in \mathbb{Z}[i]$, $\lambda \nmid \alpha$
definujeme šestý mocninný symbol $\left(\frac{\alpha}{\lambda}\right)_6$ čísla α vzhledem k λ
podmínkou $\left(\frac{\alpha}{\lambda}\right)_6 \in \{\pm 1, \pm\omega, \pm\omega^2\}$, $\left(\frac{\alpha}{\lambda}\right)_6 \equiv \alpha^{(N(\lambda)-1)/6} \pmod{\lambda}$.

Existence a jednoznačnost mocninného symbolu $\left(\frac{\alpha}{\lambda}\right)_6$ plyne z toho,
že těleso $\mathbb{Z}[\omega]/(\lambda)$ má $N(\lambda)$ prvků a polynom $x^6 - 1$ v něm má
šest různých kořenů (třídy obsahující čísla $\pm 1, \pm\omega, \pm\omega^2$). Z $\lambda \nmid \alpha$
plyne $\alpha^{N(\lambda)-1} \equiv 1 \pmod{\lambda}$, a tedy $\alpha^{(N(\lambda)-1)/6}$ je jeden z kořenů.

Zákon kubické reciprocity v okruhu $\mathbb{Z}[\omega]$

Ireducibilní prvek λ se nazývá primární, jestliže $\lambda \equiv 2 \pmod{3}$.
Pro libovolný ireducibilní prvek $\lambda \nmid 3$ a libovolné $\alpha \in \mathbb{Z}[i]$, $\lambda \nmid \alpha$ definujeme šestý mocninný symbol $\left(\frac{\alpha}{\lambda}\right)_6$ čísla α vzhledem k λ podmínkou $\left(\frac{\alpha}{\lambda}\right)_6 \in \{\pm 1, \pm \omega, \pm \omega^2\}$, $\left(\frac{\alpha}{\lambda}\right)_6 \equiv \alpha^{(N(\lambda)-1)/6} \pmod{\lambda}$.

Existence a jednoznačnost mocninného symbolu $\left(\frac{\alpha}{\lambda}\right)_6$ plyne z toho, že těleso $\mathbb{Z}[\omega]/(\lambda)$ má $N(\lambda)$ prvků a polynom $x^6 - 1$ v něm má šest různých kořenů (třídy obsahující čísla $\pm 1, \pm \omega, \pm \omega^2$). Z $\lambda \nmid \alpha$ plyne $\alpha^{N(\lambda)-1} \equiv 1 \pmod{\lambda}$, a tedy $\alpha^{(N(\lambda)-1)/6}$ je jeden z kořenů.

Věta 4. *Nechť $\lambda \in \mathbb{Z}[\omega]$ je ireducibilní, $\lambda \nmid 3$, $\alpha, \beta \in \mathbb{Z}[\omega]$, $\lambda \nmid \alpha\beta$. Pak*

$$\blacktriangleright x^6 \equiv \alpha \pmod{\lambda} \text{ má řešení v } \mathbb{Z}[\omega] \iff \left(\frac{\alpha}{\lambda}\right)_6 = 1,$$

Zákon kubické reciprocity v okruhu $\mathbb{Z}[\omega]$

Ireducibilní prvek λ se nazývá primární, jestliže $\lambda \equiv 2 \pmod{3}$.
Pro libovolný ireducibilní prvek $\lambda \nmid 3$ a libovolné $\alpha \in \mathbb{Z}[i]$, $\lambda \nmid \alpha$ definujeme šestý mocninný symbol $(\frac{\alpha}{\lambda})_6$ čísla α vzhledem k λ podmínkou $(\frac{\alpha}{\lambda})_6 \in \{\pm 1, \pm \omega, \pm \omega^2\}$, $(\frac{\alpha}{\lambda})_6 \equiv \alpha^{(N(\lambda)-1)/6} \pmod{\lambda}$.

Existence a jednoznačnost mocninného symbolu $(\frac{\alpha}{\lambda})_6$ plyne z toho, že těleso $\mathbb{Z}[\omega]/(\lambda)$ má $N(\lambda)$ prvků a polynom $x^6 - 1$ v něm má šest různých kořenů (třídy obsahující čísla $\pm 1, \pm \omega, \pm \omega^2$). Z $\lambda \nmid \alpha$ plyne $\alpha^{N(\lambda)-1} \equiv 1 \pmod{\lambda}$, a tedy $\alpha^{(N(\lambda)-1)/6}$ je jeden z kořenů.

Věta 4. *Nechť $\lambda \in \mathbb{Z}[\omega]$ je ireducibilní, $\lambda \nmid 3$, $\alpha, \beta \in \mathbb{Z}[\omega]$, $\lambda \nmid \alpha\beta$. Pak*

- ▶ $x^6 \equiv \alpha \pmod{\lambda}$ má řešení v $\mathbb{Z}[\omega] \iff (\frac{\alpha}{\lambda})_6 = 1$,
- ▶ $x^3 \equiv \alpha \pmod{\lambda}$ má řešení v $\mathbb{Z}[\omega] \iff (\frac{\alpha}{\lambda})_6 = \pm 1$,

Zákon kubické reciprocity v okruhu $\mathbb{Z}[\omega]$

Ireducibilní prvek λ se nazývá primární, jestliže $\lambda \equiv 2 \pmod{3}$.
Pro libovolný ireducibilní prvek $\lambda \nmid 3$ a libovolné $\alpha \in \mathbb{Z}[i]$, $\lambda \nmid \alpha$ definujeme šestý mocninný symbol $(\frac{\alpha}{\lambda})_6$ čísla α vzhledem k λ podmínkou $(\frac{\alpha}{\lambda})_6 \in \{\pm 1, \pm \omega, \pm \omega^2\}$, $(\frac{\alpha}{\lambda})_6 \equiv \alpha^{(N(\lambda)-1)/6} \pmod{\lambda}$.

Existence a jednoznačnost mocninného symbolu $(\frac{\alpha}{\lambda})_6$ plyne z toho, že těleso $\mathbb{Z}[\omega]/(\lambda)$ má $N(\lambda)$ prvků a polynom $x^6 - 1$ v něm má šest různých kořenů (třídy obsahující čísla $\pm 1, \pm \omega, \pm \omega^2$). Z $\lambda \nmid \alpha$ plyne $\alpha^{N(\lambda)-1} \equiv 1 \pmod{\lambda}$, a tedy $\alpha^{(N(\lambda)-1)/6}$ je jeden z kořenů.

Věta 4. *Nechť $\lambda \in \mathbb{Z}[\omega]$ je ireducibilní, $\lambda \nmid 3$, $\alpha, \beta \in \mathbb{Z}[\omega]$, $\lambda \nmid \alpha\beta$. Pak*

- ▶ $x^6 \equiv \alpha \pmod{\lambda}$ má řešení v $\mathbb{Z}[\omega] \iff (\frac{\alpha}{\lambda})_6 = 1$,
- ▶ $x^3 \equiv \alpha \pmod{\lambda}$ má řešení v $\mathbb{Z}[\omega] \iff (\frac{\alpha}{\lambda})_6 = \pm 1$,
- ▶ $(\frac{\alpha\beta}{\lambda})_6 = (\frac{\alpha}{\lambda})_6 (\frac{\beta}{\lambda})_6$,

Zákon kubické reciprocity v okruhu $\mathbb{Z}[\omega]$

Ireducibilní prvek λ se nazývá primární, jestliže $\lambda \equiv 2 \pmod{3}$.
Pro libovolný ireducibilní prvek $\lambda \nmid 3$ a libovolné $\alpha \in \mathbb{Z}[i]$, $\lambda \nmid \alpha$ definujeme šestý mocninný symbol $(\frac{\alpha}{\lambda})_6$ čísla α vzhledem k λ podmínkou $(\frac{\alpha}{\lambda})_6 \in \{\pm 1, \pm \omega, \pm \omega^2\}$, $(\frac{\alpha}{\lambda})_6 \equiv \alpha^{(N(\lambda)-1)/6} \pmod{\lambda}$.

Existence a jednoznačnost mocninného symbolu $(\frac{\alpha}{\lambda})_6$ plyne z toho, že těleso $\mathbb{Z}[\omega]/(\lambda)$ má $N(\lambda)$ prvků a polynom $x^6 - 1$ v něm má šest různých kořenů (třídy obsahující čísla $\pm 1, \pm \omega, \pm \omega^2$). Z $\lambda \nmid \alpha$ plyne $\alpha^{N(\lambda)-1} \equiv 1 \pmod{\lambda}$, a tedy $\alpha^{(N(\lambda)-1)/6}$ je jeden z kořenů.

Věta 4. *Nechť $\lambda \in \mathbb{Z}[\omega]$ je ireducibilní, $\lambda \nmid 3$, $\alpha, \beta \in \mathbb{Z}[\omega]$, $\lambda \nmid \alpha\beta$. Pak*

- ▶ $x^6 \equiv \alpha \pmod{\lambda}$ má řešení v $\mathbb{Z}[\omega] \iff (\frac{\alpha}{\lambda})_6 = 1$,
- ▶ $x^3 \equiv \alpha \pmod{\lambda}$ má řešení v $\mathbb{Z}[\omega] \iff (\frac{\alpha}{\lambda})_6 = \pm 1$,
- ▶ $(\frac{\alpha\beta}{\lambda})_6 = (\frac{\alpha}{\lambda})_6 (\frac{\beta}{\lambda})_6$,
- ▶ $\alpha \equiv \beta \pmod{\lambda} \implies (\frac{\alpha}{\lambda})_6 = (\frac{\beta}{\lambda})_6$.

Zákon kubické reciprocity v okruhu $\mathbb{Z}[\omega]$

Ireducibilní prvek λ se nazývá primární, jestliže $\lambda \equiv 2 \pmod{3}$.
Pro libovolný ireducibilní prvek $\lambda \nmid 3$ a libovolné $\alpha \in \mathbb{Z}[i]$, $\lambda \nmid \alpha$ definujeme šestý mocninný symbol $(\frac{\alpha}{\lambda})_6$ čísla α vzhledem k λ podmínkou $(\frac{\alpha}{\lambda})_6 \in \{\pm 1, \pm \omega, \pm \omega^2\}$, $(\frac{\alpha}{\lambda})_6 \equiv \alpha^{(N(\lambda)-1)/6} \pmod{\lambda}$.

Existence a jednoznačnost mocninného symbolu $(\frac{\alpha}{\lambda})_6$ plyne z toho, že těleso $\mathbb{Z}[\omega]/(\lambda)$ má $N(\lambda)$ prvků a polynom $x^6 - 1$ v něm má šest různých kořenů (třídy obsahující čísla $\pm 1, \pm \omega, \pm \omega^2$). Z $\lambda \nmid \alpha$ plyne $\alpha^{N(\lambda)-1} \equiv 1 \pmod{\lambda}$, a tedy $\alpha^{(N(\lambda)-1)/6}$ je jeden z kořenů.

Věta 4. *Nechť $\lambda \in \mathbb{Z}[\omega]$ je ireducibilní, $\lambda \nmid 3$, $\alpha, \beta \in \mathbb{Z}[\omega]$, $\lambda \nmid \alpha\beta$. Pak*

- ▶ $x^6 \equiv \alpha \pmod{\lambda}$ má řešení v $\mathbb{Z}[\omega] \iff (\frac{\alpha}{\lambda})_6 = 1$,
- ▶ $x^3 \equiv \alpha \pmod{\lambda}$ má řešení v $\mathbb{Z}[\omega] \iff (\frac{\alpha}{\lambda})_6 = \pm 1$,
- ▶ $(\frac{\alpha\beta}{\lambda})_6 = (\frac{\alpha}{\lambda})_6 (\frac{\beta}{\lambda})_6$,
- ▶ $\alpha \equiv \beta \pmod{\lambda} \implies (\frac{\alpha}{\lambda})_6 = (\frac{\beta}{\lambda})_6$.

Věta 5. *Jestliže π a λ jsou primární ireducibilní prvky takové, že $N(\pi) \neq N(\lambda)$, pak $(\frac{\pi}{\lambda})_6 = \pm (\frac{\lambda}{\pi})_6$.*

Počet bodů na eliptické křivce $y^2 = x^3 + b$ nad \mathbb{Z}_p

Věta 6. Necht' p je prvočíslo, $b \in \mathbb{Z}$, přičemž $p > 3$, $p \nmid b$.

Počet bodů na eliptické křivce $y^2 = x^3 + b$ nad \mathbb{Z}_p

Věta 6. *Nechť p je prvočíslo, $b \in \mathbb{Z}$, přičemž $p > 3$, $p \nmid b$. Necht' N je počet bodů na eliptické křivce $y^2 = x^3 + b$ nad \mathbb{Z}_p .*

Počet bodů na eliptické křivce $y^2 = x^3 + b$ nad \mathbb{Z}_p

Věta 6. *Nechť p je prvočíslo, $b \in \mathbb{Z}$, přičemž $p > 3$, $p \nmid b$. Nechť N je počet bodů na eliptické křivce $y^2 = x^3 + b$ nad \mathbb{Z}_p .*

- ▶ *Je-li $p \equiv 2 \pmod{3}$, pak $N = p + 1$.*

Počet bodů na eliptické křivce $y^2 = x^3 + b$ nad \mathbb{Z}_p

Věta 6. *Nechť p je prvočíslo, $b \in \mathbb{Z}$, přičemž $p > 3$, $p \nmid b$. Nechť N je počet bodů na eliptické křivce $y^2 = x^3 + b$ nad \mathbb{Z}_p .*

- ▶ *Je-li $p \equiv 2 \pmod{3}$, pak $N = p + 1$.*
- ▶ *Je-li $p \equiv 1 \pmod{3}$ a $p = \pi\bar{\pi}$ je rozklad čísla p na součin dvou primárních ireducibilních prvků v $\mathbb{Z}[\omega]$, pak*

$$N = p + 1 + \overline{\left(\frac{4b}{\pi}\right)_6} \cdot \pi + \left(\frac{4b}{\pi}\right)_6 \cdot \bar{\pi}.$$

Počet bodů na eliptické křivce $y^2 = x^3 + b$ nad \mathbb{Z}_p

Věta 6. *Nechť p je prvočíslo, $b \in \mathbb{Z}$, přičemž $p > 3$, $p \nmid b$. Nechť N je počet bodů na eliptické křivce $y^2 = x^3 + b$ nad \mathbb{Z}_p .*

- ▶ *Je-li $p \equiv 2 \pmod{3}$, pak $N = p + 1$.*
- ▶ *Je-li $p \equiv 1 \pmod{3}$ a $p = \pi\bar{\pi}$ je rozklad čísla p na součin dvou primárních ireducibilních prvků v $\mathbb{Z}[\omega]$, pak*

$$N = p + 1 + \overline{\left(\frac{4b}{\pi}\right)_6} \cdot \pi + \left(\frac{4b}{\pi}\right)_6 \cdot \bar{\pi}.$$

Dokažme větu jen pro lehčí první případ: je-li $p \equiv 2 \pmod{3}$, pak zobrazení $f : \mathbb{Z}_p \rightarrow \mathbb{Z}_p$ určené předpisem $f(t) = t^3$ je bijekce, neboť na nulu se zobrazí jen nula a zúžení f na \mathbb{Z}_p^\times je homomorfismus grup s triviálním jádrem.

Počet bodů na eliptické křivce $y^2 = x^3 + b$ nad \mathbb{Z}_p

Věta 6. *Nechť p je prvočíslo, $b \in \mathbb{Z}$, přičemž $p > 3$, $p \nmid b$. Nechť N je počet bodů na eliptické křivce $y^2 = x^3 + b$ nad \mathbb{Z}_p .*

- ▶ *Je-li $p \equiv 2 \pmod{3}$, pak $N = p + 1$.*
- ▶ *Je-li $p \equiv 1 \pmod{3}$ a $p = \pi\bar{\pi}$ je rozklad čísla p na součin dvou primárních ireducibilních prvků v $\mathbb{Z}[\omega]$, pak*

$$N = p + 1 + \overline{\left(\frac{4b}{\pi}\right)_6} \cdot \pi + \left(\frac{4b}{\pi}\right)_6 \cdot \bar{\pi}.$$

Dokažme větu jen pro lehčí první případ: je-li $p \equiv 2 \pmod{3}$, pak zobrazení $f : \mathbb{Z}_p \rightarrow \mathbb{Z}_p$ určené předpisem $f(t) = t^3$ je bijekce, neboť na nulu se zobrazí jen nula a zúžení f na \mathbb{Z}_p^\times je homomorfismus grup s triviálním jádrem. Proto pro každé $y \in \mathbb{Z}_p$ existuje jediné $x \in \mathbb{Z}_p$ splňující $f(x) = y^2 - b$.

Počet bodů na eliptické křivce $y^2 = x^3 + b$ nad \mathbb{Z}_p

Věta 6. *Nechť p je prvočíslo, $b \in \mathbb{Z}$, přičemž $p > 3$, $p \nmid b$. Nechť N je počet bodů na eliptické křivce $y^2 = x^3 + b$ nad \mathbb{Z}_p .*

- ▶ *Je-li $p \equiv 2 \pmod{3}$, pak $N = p + 1$.*
- ▶ *Je-li $p \equiv 1 \pmod{3}$ a $p = \pi\bar{\pi}$ je rozklad čísla p na součin dvou primárních ireducibilních prvků v $\mathbb{Z}[\omega]$, pak*

$$N = p + 1 + \overline{\left(\frac{4b}{\pi}\right)_6} \cdot \pi + \left(\frac{4b}{\pi}\right)_6 \cdot \bar{\pi}.$$

Dokažme větu jen pro lehčí první případ: je-li $p \equiv 2 \pmod{3}$, pak zobrazení $f : \mathbb{Z}_p \rightarrow \mathbb{Z}_p$ určené předpisem $f(t) = t^3$ je bijekce, neboť na nulu se zobrazí jen nula a zúžení f na \mathbb{Z}_p^\times je homomorfismus grup s triviálním jádrem. Proto pro každé $y \in \mathbb{Z}_p$ existuje jediné $x \in \mathbb{Z}_p$ splňující $f(x) = y^2 - b$. Pro každé $y \in \mathbb{Z}_p$ tedy existuje jediné $x \in \mathbb{Z}_p$ tak, že $[x, y]$ leží na eliptické křivce.

Počet bodů na eliptické křivce $y^2 = x^3 + b$ nad \mathbb{Z}_p

Věta 6. *Nechť p je prvočíslo, $b \in \mathbb{Z}$, přičemž $p > 3$, $p \nmid b$. Nechť N je počet bodů na eliptické křivce $y^2 = x^3 + b$ nad \mathbb{Z}_p .*

- ▶ *Je-li $p \equiv 2 \pmod{3}$, pak $N = p + 1$.*
- ▶ *Je-li $p \equiv 1 \pmod{3}$ a $p = \pi\bar{\pi}$ je rozklad čísla p na součin dvou primárních ireducibilních prvků v $\mathbb{Z}[\omega]$, pak*

$$N = p + 1 + \overline{\left(\frac{4b}{\pi}\right)_6} \cdot \pi + \left(\frac{4b}{\pi}\right)_6 \cdot \bar{\pi}.$$

Dokažme větu jen pro lehčí první případ: je-li $p \equiv 2 \pmod{3}$, pak zobrazení $f : \mathbb{Z}_p \rightarrow \mathbb{Z}_p$ určené předpisem $f(t) = t^3$ je bijekce, neboť na nulu se zobrazí jen nula a zúžení f na \mathbb{Z}_p^\times je homomorfismus grup s triviálním jádrem. Proto pro každé $y \in \mathbb{Z}_p$ existuje jediné $x \in \mathbb{Z}_p$ splňující $f(x) = y^2 - b$. Pro každé $y \in \mathbb{Z}_p$ tedy existuje jediné $x \in \mathbb{Z}_p$ tak, že $[x, y]$ leží na eliptické křivce. Kromě nevlastního bodu O existuje na eliptické křivce tedy právě p bodů.

Příklad: eliptická křivka $y^2 = x^3 + 2$ nad \mathbb{Z}_{103}

Rozložme $p = 103$ v $\mathbb{Z}[\omega]$.

Příklad: eliptická křivka $y^2 = x^3 + 2$ nad \mathbb{Z}_{103}

Rozložme $p = 103$ v $\mathbb{Z}[\omega]$.

Hledáme tedy $u, v \in \mathbb{Z}$, aby $u^2 - uv + v^2 = p$.

Příklad: eliptická křivka $y^2 = x^3 + 2$ nad \mathbb{Z}_{103}

Rozložme $p = 103$ v $\mathbb{Z}[\omega]$.

Hledáme tedy $u, v \in \mathbb{Z}$, aby $u^2 - uv + v^2 = p$.

Pak $4p = (2u - v)^2 + 3v^2$, lze tedy postupovat dosazováním malých přirozených čísel za v .

Příklad: eliptická křivka $y^2 = x^3 + 2$ nad \mathbb{Z}_{103}

Rozložme $p = 103$ v $\mathbb{Z}[\omega]$.

Hledáme tedy $u, v \in \mathbb{Z}$, aby $u^2 - uv + v^2 = p$.

Pak $4p = (2u - v)^2 + 3v^2$, lze tedy postupovat dosazováním malých přirozených čísel za v . V našem případě

$$4p = 412 = 20^2 + 3 \cdot 2^2.$$

Příklad: eliptická křivka $y^2 = x^3 + 2$ nad \mathbb{Z}_{103}

Rozložme $p = 103$ v $\mathbb{Z}[\omega]$.

Hledáme tedy $u, v \in \mathbb{Z}$, aby $u^2 - uv + v^2 = p$.

Pak $4p = (2u - v)^2 + 3v^2$, lze tedy postupovat dosazováním malých přirozených čísel za v . V našem případě

$4p = 412 = 20^2 + 3 \cdot 2^2$. Proto $11 + 2\omega$ je ireducibilní prvek dělicí p , není však primární.

Příklad: eliptická křivka $y^2 = x^3 + 2$ nad \mathbb{Z}_{103}

Rozložme $p = 103$ v $\mathbb{Z}[\omega]$.

Hledáme tedy $u, v \in \mathbb{Z}$, aby $u^2 - uv + v^2 = p$.

Pak $4p = (2u - v)^2 + 3v^2$, lze tedy postupovat dosazováním malých přirozených čísel za v . V našem případě

$4p = 412 = 20^2 + 3 \cdot 2^2$. Proto $11 + 2\omega$ je ireducibilní prvek dělící p , není však primární. Je třeba jej vynásobit vhodnou mocninou ω , abychom dostali koeficient u ω dělitelný třemi.

Příklad: eliptická křivka $y^2 = x^3 + 2$ nad \mathbb{Z}_{103}

Rozložme $p = 103$ v $\mathbb{Z}[\omega]$.

Hledáme tedy $u, v \in \mathbb{Z}$, aby $u^2 - uv + v^2 = p$.

Pak $4p = (2u - v)^2 + 3v^2$, lze tedy postupovat dosazováním malých přirozených čísel za v . V našem případě

$4p = 412 = 20^2 + 3 \cdot 2^2$. Proto $11 + 2\omega$ je ireducibilní prvek dělící p , není však primární. Je třeba jej vynásobit vhodnou mocninou ω , abychom dostali koeficient u ω dělitelný třemi. Platí $(11 + 2\omega)\omega = 11\omega + 2(-1 - \omega) = -2 + 9\omega$, což také není primární, ale vynásobením -1 dostaneme hledaný primární ireducibilní prvek $\pi = 2 - 9\omega$.

Příklad: eliptická křivka $y^2 = x^3 + 2$ nad \mathbb{Z}_{103}

Rozložme $p = 103$ v $\mathbb{Z}[\omega]$.

Hledáme tedy $u, v \in \mathbb{Z}$, aby $u^2 - uv + v^2 = p$.

Pak $4p = (2u - v)^2 + 3v^2$, lze tedy postupovat dosazováním malých přirozených čísel za v . V našem případě

$4p = 412 = 20^2 + 3 \cdot 2^2$. Proto $11 + 2\omega$ je ireducibilní prvek dělící p , není však primární. Je třeba jej vynásobit vhodnou mocninou ω , abychom dostali koeficient u ω dělitelný třemi. Platí $(11 + 2\omega)\omega = 11\omega + 2(-1 - \omega) = -2 + 9\omega$, což také není primární, ale vynásobením -1 dostaneme hledaný primární ireducibilní prvek $\pi = 2 - 9\omega$.

Potřebujeme spočítat $(\frac{4b}{\pi})_6$, v tomto případě je $4b = 8$ třetí mocnina, a tak můžeme použít Legendreův symbol

$g^{(p-1)/6} = 2^{(p-1)/2} \equiv (\frac{2}{p}) \pmod{p}$. Je tedy $(\frac{8}{\pi})_6 = (\frac{2}{103}) = 1$.

Příklad: eliptická křivka $y^2 = x^3 + 2$ nad \mathbb{Z}_{103}

Rozložme $p = 103$ v $\mathbb{Z}[\omega]$.

Hledáme tedy $u, v \in \mathbb{Z}$, aby $u^2 - uv + v^2 = p$.

Pak $4p = (2u - v)^2 + 3v^2$, lze tedy postupovat dosazováním malých přirozených čísel za v . V našem případě

$4p = 412 = 20^2 + 3 \cdot 2^2$. Proto $11 + 2\omega$ je ireducibilní prvek dělící p , není však primární. Je třeba jej vynásobit vhodnou mocninou ω , abychom dostali koeficient u ω dělitelný třemi. Platí $(11 + 2\omega)\omega = 11\omega + 2(-1 - \omega) = -2 + 9\omega$, což také není primární, ale vynásobením -1 dostaneme hledaný primární ireducibilní prvek $\pi = 2 - 9\omega$.

Potřebujeme spočítat $(\frac{4b}{\pi})_6$, v tomto případě je $4b = 8$ třetí mocnina, a tak můžeme použít Legendreův symbol

$8^{(p-1)/6} = 2^{(p-1)/2} \equiv (\frac{2}{p}) \pmod{p}$. Je tedy $(\frac{8}{\pi})_6 = (\frac{2}{103}) = 1$.

Podle věty 6 pro počet N bodů na eliptické křivce $y^2 = x^3 + 2$ nad \mathbb{Z}_{103} platí

$$N = p + 1 + \overline{(\frac{8}{\pi})_6} \cdot \pi + (\frac{8}{\pi})_6 \cdot \bar{\pi} = 104 + \pi + \bar{\pi} = 104 + 4 - 9\omega - 9\omega^2 = 117.$$

KMOV – základní myšlenka

Nechť $n = pq$ pro velká prvočísla $p \neq q$, kde $p \equiv q \equiv 2 \pmod{3}$.

KMOV – základní myšlenka

Nechť $n = pq$ pro velká prvočísla $p \neq q$, kde $p \equiv q \equiv 2 \pmod{3}$.
Libovolnou dvojici $A = [u, v]$, kde $u, v \in \mathbb{Z}$ jsou taková, že
 $b = v^2 - u^3$ je nesoudělné s n , lze interpretovat jako bod ležící
současně na dvou eliptických křivkách daných rovnicí $y^2 = x^3 + b$,
totiž na \mathcal{E}_p nad \mathbb{Z}_p a na \mathcal{E}_q nad \mathbb{Z}_q .

KMOV – základní myšlenka

Nechť $n = pq$ pro velká prvočísla $p \neq q$, kde $p \equiv q \equiv 2 \pmod{3}$.
Libovolnou dvojici $A = [u, v]$, kde $u, v \in \mathbb{Z}$ jsou taková, že $b = v^2 - u^3$ je nesoudělné s n , lze interpretovat jako bod ležící současně na dvou eliptických křivkách daných rovnicí $y^2 = x^3 + b$, totiž na \mathcal{E}_p nad \mathbb{Z}_p a na \mathcal{E}_q nad \mathbb{Z}_q . Podle věty 6 platí $|\mathcal{E}_p| = p + 1$ a $|\mathcal{E}_q| = q + 1$.

KMOV – základní myšlenka

Nechť $n = pq$ pro velká prvočísla $p \neq q$, kde $p \equiv q \equiv 2 \pmod{3}$.
Libovolnou dvojici $A = [u, v]$, kde $u, v \in \mathbb{Z}$ jsou taková, že $b = v^2 - u^3$ je nesoudělné s n , lze interpretovat jako bod ležící současně na dvou eliptických křivkách daných rovnicí $y^2 = x^3 + b$, totiž na \mathcal{E}_p nad \mathbb{Z}_p a na \mathcal{E}_q nad \mathbb{Z}_q . Podle věty 6 platí $|\mathcal{E}_p| = p + 1$ a $|\mathcal{E}_q| = q + 1$.

I v případě, že neznáme p a q , lze pomocí výpočtů prováděných modulo n takové dvojice reprezentující body na obou křivkách sčítat, problémy vzniknou jen v případě, že výsledný bod je neutrální prvek na právě jedné z těchto dvou křivek.

KMOV – základní myšlenka

Nechť $n = pq$ pro velká prvočísla $p \neq q$, kde $p \equiv q \equiv 2 \pmod{3}$. Libovolnou dvojici $A = [u, v]$, kde $u, v \in \mathbb{Z}$ jsou taková, že $b = v^2 - u^3$ je nesoudělné s n , lze interpretovat jako bod ležící současně na dvou eliptických křivkách daných rovnicí $y^2 = x^3 + b$, totiž na \mathcal{E}_p nad \mathbb{Z}_p a na \mathcal{E}_q nad \mathbb{Z}_q . Podle věty 6 platí $|\mathcal{E}_p| = p + 1$ a $|\mathcal{E}_q| = q + 1$.

I v případě, že neznáme p a q , lze pomocí výpočtů prováděných modulo n takové dvojice reprezentující body na obou křivkách sčítat, problémy vzniknou jen v případě, že výsledný bod je neutrální prvek na právě jedné z těchto dvou křivek. Avšak jsou-li prvočísla p, q opravdu velká, nalezení takového bodu je krajně nepravděpodobné (víme, že znalost takového bodu znamená znalost rozkladu n na součin prvočísel).

KMOV – základní myšlenka

Nechť $n = pq$ pro velká prvočísla $p \neq q$, kde $p \equiv q \equiv 2 \pmod{3}$. Libovolnou dvojici $A = [u, v]$, kde $u, v \in \mathbb{Z}$ jsou taková, že $b = v^2 - u^3$ je nesoudělné s n , lze interpretovat jako bod ležící současně na dvou eliptických křivkách daných rovnicí $y^2 = x^3 + b$, totiž na \mathcal{E}_p nad \mathbb{Z}_p a na \mathcal{E}_q nad \mathbb{Z}_q . Podle věty 6 platí $|\mathcal{E}_p| = p + 1$ a $|\mathcal{E}_q| = q + 1$.

I v případě, že neznáme p a q , lze pomocí výpočtů prováděných modulo n takové dvojice reprezentující body na obou křivkách sčítat, problémy vzniknou jen v případě, že výsledný bod je neutrální prvek na právě jedné z těchto dvou křivek. Avšak jsou-li prvočísla p, q opravdu velká, nalezení takového bodu je krajně nepravděpodobné (víme, že znalost takového bodu znamená znalost rozkladu n na součin prvočísel).

Nechť λ je společný násobek čísel $p + 1$ a $q + 1$.

KMOV – základní myšlenka

Nechť $n = pq$ pro velká prvočísla $p \neq q$, kde $p \equiv q \equiv 2 \pmod{3}$. Libovolnou dvojici $A = [u, v]$, kde $u, v \in \mathbb{Z}$ jsou taková, že $b = v^2 - u^3$ je nesoudělné s n , lze interpretovat jako bod ležící současně na dvou eliptických křivkách daných rovnicí $y^2 = x^3 + b$, totiž na \mathcal{E}_p nad \mathbb{Z}_p a na \mathcal{E}_q nad \mathbb{Z}_q . Podle věty 6 platí $|\mathcal{E}_p| = p + 1$ a $|\mathcal{E}_q| = q + 1$.

I v případě, že neznáme p a q , lze pomocí výpočtů prováděných modulo n takové dvojice reprezentující body na obou křivkách sčítat, problémy vzniknou jen v případě, že výsledný bod je neutrální prvek na právě jedné z těchto dvou křivek. Avšak jsou-li prvočísla p, q opravdu velká, nalezení takového bodu je krajně nepravděpodobné (víme, že znalost takového bodu znamená znalost rozkladu n na součin prvočísel).

Nechť λ je společný násobek čísel $p + 1$ a $q + 1$. Pak pro každé přirozené číslo $t \equiv 1 \pmod{\lambda}$ platí $t \cdot A = A$.

KMOV – použití

Generování klíčů: Je nutné zvolit velká prvočísla $p \equiv q \equiv 2 \pmod{3}$ (přibližně stejně velká, např. $p < q < 2p$, ale s velkým rozdílem $q - p$), $n = pq$, λ je (nejmenší) společný násobek čísel $p + 1$ a $q + 1$ (je možné vzít $\lambda = (p + 1)(q + 1)$).

KMOV – použití

Generování klíčů: Je nutné zvolit velká prvočísla $p \equiv q \equiv 2 \pmod{3}$ (přibližně stejně velká, např. $p < q < 2p$, ale s velkým rozdílem $q - p$), $n = pq$, λ je (nejmenší) společný násobek čísel $p + 1$ a $q + 1$ (je možné vzít $\lambda = (p + 1)(q + 1)$). Dále je nutné zvolit $e \in \mathbb{Z}$, $e > 1$, $(e, \lambda) = 1$ a spočítat $f \in \mathbb{Z}$, $f > 0$, aby $ef \equiv 1 \pmod{\lambda}$.

KMOV – použití

Generování klíčů: Je nutné zvolit velká prvočísla $p \equiv q \equiv 2 \pmod{3}$ (přibližně stejně velká, např. $p < q < 2p$, ale s velkým rozdílem $q - p$), $n = pq$, λ je (nejmenší) společný násobek čísel $p + 1$ a $q + 1$ (je možné vzít $\lambda = (p + 1)(q + 1)$). Dále je nutné zvolit $e \in \mathbb{Z}$, $e > 1$, $(e, \lambda) = 1$ a spočítat $f \in \mathbb{Z}$, $f > 0$, aby $ef \equiv 1 \pmod{\lambda}$.

Veřejný klíč: n , e .

KMOV – použití

Generování klíčů: Je nutné zvolit velká prvočísla $p \equiv q \equiv 2 \pmod{3}$ (přibližně stejně velká, např. $p < q < 2p$, ale s velkým rozdílem $q - p$), $n = pq$, λ je (nejmenší) společný násobek čísel $p + 1$ a $q + 1$ (je možné vzít $\lambda = (p + 1)(q + 1)$). Dále je nutné zvolit $e \in \mathbb{Z}$, $e > 1$, $(e, \lambda) = 1$ a spočítat $f \in \mathbb{Z}$, $f > 0$, aby $ef \equiv 1 \pmod{\lambda}$.

Veřejný klíč: n , e .

Tajný klíč: f (také p , q , pomocí nichž lze f snadno spočítat).

KMOV – použití

Generování klíčů: Je nutné zvolit velká prvočísla $p \equiv q \equiv 2 \pmod{3}$ (přibližně stejně velká, např. $p < q < 2p$, ale s velkým rozdílem $q - p$), $n = pq$, λ je (nejmenší) společný násobek čísel $p + 1$ a $q + 1$ (je možné vzít $\lambda = (p + 1)(q + 1)$). Dále je nutné zvolit $e \in \mathbb{Z}$, $e > 1$, $(e, \lambda) = 1$ a spočítat $f \in \mathbb{Z}$, $f > 0$, aby $ef \equiv 1 \pmod{\lambda}$.

Veřejný klíč: n , e .

Tajný klíč: f (také p , q , pomocí nichž lze f snadno spočítat).

Šifrování: Zpráva je dvojice $[m_1, m_2]$, kde $m_1, m_2 \in \mathbb{Z}$, $1 < m_1 < n$, $1 < m_2 < n$.

KMOV – použití

Generování klíčů: Je nutné zvolit velká prvočísla $p \equiv q \equiv 2 \pmod{3}$ (přibližně stejně velká, např. $p < q < 2p$, ale s velkým rozdílem $q - p$), $n = pq$, λ je (nejmenší) společný násobek čísel $p + 1$ a $q + 1$ (je možné vzít $\lambda = (p + 1)(q + 1)$). Dále je nutné zvolit $e \in \mathbb{Z}$, $e > 1$, $(e, \lambda) = 1$ a spočítat $f \in \mathbb{Z}$, $f > 0$, aby $ef \equiv 1 \pmod{\lambda}$.

Veřejný klíč: n , e .

Tajný klíč: f (také p , q , pomocí nichž lze f snadno spočítat).

Šifrování: Zpráva je dvojice $[m_1, m_2]$, kde $m_1, m_2 \in \mathbb{Z}$, $1 < m_1 < n$, $1 < m_2 < n$. Odesílající interpretuje dvojici $A = [m_1, m_2]$ jako bod ležící současně na eliptických křivkách \mathcal{E}_p nad \mathbb{Z}_p a na \mathcal{E}_q nad \mathbb{Z}_q daných rovnicí $y^2 = x^3 + b$, kde $b = m_2^2 - m_1^3$ (případ b soudělného s n je nepravděpodobný).

KMOV – použití

Generování klíčů: Je nutné zvolit velká prvočísla $p \equiv q \equiv 2 \pmod{3}$ (přibližně stejně velká, např. $p < q < 2p$, ale s velkým rozdílem $q - p$), $n = pq$, λ je (nejmenší) společný násobek čísel $p + 1$ a $q + 1$ (je možné vzít $\lambda = (p + 1)(q + 1)$). Dále je nutné zvolit $e \in \mathbb{Z}$, $e > 1$, $(e, \lambda) = 1$ a spočítat $f \in \mathbb{Z}$, $f > 0$, aby $ef \equiv 1 \pmod{\lambda}$.

Veřejný klíč: n , e .

Tajný klíč: f (také p , q , pomocí nichž lze f snadno spočítat).

Šifrování: Zpráva je dvojice $[m_1, m_2]$, kde $m_1, m_2 \in \mathbb{Z}$, $1 < m_1 < n$, $1 < m_2 < n$. Odesílající interpretuje dvojici $A = [m_1, m_2]$ jako bod ležící současně na eliptických křivkách \mathcal{E}_p nad \mathbb{Z}_p a na \mathcal{E}_q nad \mathbb{Z}_q daných rovnicí $y^2 = x^3 + b$, kde $b = m_2^2 - m_1^3$ (případ b soudělného s n je nepravděpodobný). Použije veřejný klíč a spočítá bod $B = e \cdot A$, který pak odešle (výpočty provádí modulo n).

KMOV – použití

Generování klíčů: Je nutné zvolit velká prvočísla $p \equiv q \equiv 2 \pmod{3}$ (přibližně stejně velká, např. $p < q < 2p$, ale s velkým rozdílem $q - p$), $n = pq$, λ je (nejmenší) společný násobek čísel $p + 1$ a $q + 1$ (je možné vzít $\lambda = (p + 1)(q + 1)$). Dále je nutné zvolit $e \in \mathbb{Z}$, $e > 1$, $(e, \lambda) = 1$ a spočítat $f \in \mathbb{Z}$, $f > 0$, aby $ef \equiv 1 \pmod{\lambda}$.

Veřejný klíč: n, e .

Tajný klíč: f (také p, q , pomocí nichž lze f snadno spočítat).

Šifrování: Zpráva je dvojice $[m_1, m_2]$, kde $m_1, m_2 \in \mathbb{Z}$, $1 < m_1 < n$, $1 < m_2 < n$. Odesílající interpretuje dvojici $A = [m_1, m_2]$ jako bod ležící současně na eliptických křivkách \mathcal{E}_p nad \mathbb{Z}_p a na \mathcal{E}_q nad \mathbb{Z}_q daných rovnicí $y^2 = x^3 + b$, kde $b = m_2^2 - m_1^3$ (případ b soudělného s n je nepravděpodobný). Použije veřejný klíč a spočítá bod $B = e \cdot A$, který pak odešle (výpočty provádí modulo n).

Dešifrování: Příjemce použije tajný klíč a spočítá zprávu $A = f \cdot B$ (výpočty může provádět modulo n , anebo postup zrychlit tak, že počítá postupně modulo p a modulo q , pak užije Čínskou zbytkovou větu).

Kryptosystém Alshehhi-Nitaj – základní myšlenka

Nechť pro přirozená čísla r, s je $p = (4r + 3)^2 + (4s + 2)^2$ prvočíslo.

Kryptosystém Alshehhi-Nitaj – základní myšlenka

Nechť pro přirozená čísla r, s je $p = (4r + 3)^2 + (4s + 2)^2$ prvočíslo. Pak $p \equiv 5 \pmod{8}$ a p se v $\mathbb{Z}[i]$ rozkládá na součin $p = \pi\bar{\pi}$, kde $\pi = (4r + 3) + (4s + 2)i$ je primární ireducibilní prvek.

Kryptosystém Alshehhi-Nitaj – základní myšlenka

Nechť pro přirozená čísla r, s je $p = (4r + 3)^2 + (4s + 2)^2$ prvočíslo.

Pak $p \equiv 5 \pmod{8}$ a p se v $\mathbb{Z}[i]$ rozkládá na součin $p = \pi\bar{\pi}$, kde $\pi = (4r + 3) + (4s + 2)i$ je primární ireducibilní prvek.

Označme $u = 4r + 3$, $v = 4s + 2$, tedy $\pi = u + iv$, najdeme $c \in \mathbb{Z}$, aby $cv \equiv u \pmod{p}$.

Kryptosystém Alshehhi-Nitaj – základní myšlenka

Nechť pro přirozená čísla r, s je $p = (4r + 3)^2 + (4s + 2)^2$ prvočíslo.

Pak $p \equiv 5 \pmod{8}$ a p se v $\mathbb{Z}[i]$ rozkládá na součin $p = \pi\bar{\pi}$, kde $\pi = (4r + 3) + (4s + 2)i$ je primární ireducibilní prvek.

Označme $u = 4r + 3$, $v = 4s + 2$, tedy $\pi = u + iv$, najdeme $c \in \mathbb{Z}$, aby $cv \equiv u \pmod{p}$. Protože $c^2v^2 \equiv u^2 \equiv -v^2 \pmod{p}$, je $c^2 \equiv -1 \pmod{p}$. Zvolme libovolně $a \in \mathbb{Z}$, $p \nmid a$.

Kryptosystém Alshehhi-Nitaj – základní myšlenka

Nechť pro přirozená čísla r, s je $p = (4r + 3)^2 + (4s + 2)^2$ prvočíslo. Pak $p \equiv 5 \pmod{8}$ a p se v $\mathbb{Z}[i]$ rozkládá na součin $p = \pi\bar{\pi}$, kde $\pi = (4r + 3) + (4s + 2)i$ je primární ireducibilní prvek.

Označme $u = 4r + 3$, $v = 4s + 2$, tedy $\pi = u + iv$, najdeme $c \in \mathbb{Z}$, aby $cv \equiv u \pmod{p}$. Protože $c^2v^2 \equiv u^2 \equiv -v^2 \pmod{p}$, je $c^2 \equiv -1 \pmod{p}$. Zvolme libovolně $a \in \mathbb{Z}$, $p \nmid a$. Podle věty 3 pro počet N bodů na eliptické křivce $y^2 = x^3 - ax$ platí

$$N = p + 1 - \overline{\left(\frac{a}{\pi}\right)_4} \cdot \pi - \left(\frac{a}{\pi}\right)_4 \cdot \bar{\pi}.$$

Kryptosystém Alshehhi-Nitaj – základní myšlenka

Nechť pro přirozená čísla r, s je $p = (4r + 3)^2 + (4s + 2)^2$ prvočíslo. Pak $p \equiv 5 \pmod{8}$ a p se v $\mathbb{Z}[i]$ rozkládá na součin $p = \pi\bar{\pi}$, kde $\pi = (4r + 3) + (4s + 2)i$ je primární ireducibilní prvek.

Označme $u = 4r + 3$, $v = 4s + 2$, tedy $\pi = u + iv$, najdeme $c \in \mathbb{Z}$, aby $cv \equiv u \pmod{p}$. Protože $c^2v^2 \equiv u^2 \equiv -v^2 \pmod{p}$, je $c^2 \equiv -1 \pmod{p}$. Zvolme libovolně $a \in \mathbb{Z}$, $p \nmid a$. Podle věty 3 pro počet N bodů na eliptické křivce $y^2 = x^3 - ax$ platí

$$N = p + 1 - \overline{\left(\frac{a}{\pi}\right)_4} \cdot \pi - \left(\frac{a}{\pi}\right)_4 \cdot \bar{\pi}.$$

Víme, že $\left(\frac{a}{\pi}\right)_4 \in \{1, i, -1, -i\}$, $\left(\frac{a}{\pi}\right)_4 \equiv a^{(p-1)/4} \pmod{\pi}$.

Kryptosystém Alshehhi-Nitaj – základní myšlenka

Nechť pro přirozená čísla r, s je $p = (4r + 3)^2 + (4s + 2)^2$ prvočíslo. Pak $p \equiv 5 \pmod{8}$ a p se v $\mathbb{Z}[i]$ rozkládá na součin $p = \pi\bar{\pi}$, kde $\pi = (4r + 3) + (4s + 2)i$ je primární ireducibilní prvek.

Označme $u = 4r + 3$, $v = 4s + 2$, tedy $\pi = u + iv$, najdeme $c \in \mathbb{Z}$, aby $cv \equiv u \pmod{p}$. Protože $c^2v^2 \equiv u^2 \equiv -v^2 \pmod{p}$, je $c^2 \equiv -1 \pmod{p}$. Zvolme libovolně $a \in \mathbb{Z}$, $p \nmid a$. Podle věty 3 pro počet N bodů na eliptické křivce $y^2 = x^3 - ax$ platí

$$N = p + 1 - \overline{\left(\frac{a}{\pi}\right)_4} \cdot \pi - \left(\frac{a}{\pi}\right)_4 \cdot \bar{\pi}.$$

Víme, že $\left(\frac{a}{\pi}\right)_4 \in \{1, i, -1, -i\}$, $\left(\frac{a}{\pi}\right)_4 \equiv a^{(p-1)/4} \pmod{\pi}$. Rozlišme

- ▶ $a^{(p-1)/4} \equiv 1 \pmod{p}$, pak $\left(\frac{a}{\pi}\right)_4 = 1$ a $N = p + 1 - 2u$.

Kryptosystém Alshehhi-Nitaj – základní myšlenka

Nechť pro přirozená čísla r, s je $p = (4r + 3)^2 + (4s + 2)^2$ prvočíslo. Pak $p \equiv 5 \pmod{8}$ a p se v $\mathbb{Z}[i]$ rozkládá na součin $p = \pi\bar{\pi}$, kde $\pi = (4r + 3) + (4s + 2)i$ je primární ireducibilní prvek.

Označme $u = 4r + 3$, $v = 4s + 2$, tedy $\pi = u + iv$, najdeme $c \in \mathbb{Z}$, aby $cv \equiv u \pmod{p}$. Protože $c^2v^2 \equiv u^2 \equiv -v^2 \pmod{p}$, je $c^2 \equiv -1 \pmod{p}$. Zvolme libovolně $a \in \mathbb{Z}$, $p \nmid a$. Podle věty 3 pro počet N bodů na eliptické křivce $y^2 = x^3 - ax$ platí

$$N = p + 1 - \overline{\left(\frac{a}{\pi}\right)_4} \cdot \pi - \left(\frac{a}{\pi}\right)_4 \cdot \bar{\pi}.$$

Víme, že $\left(\frac{a}{\pi}\right)_4 \in \{1, i, -1, -i\}$, $\left(\frac{a}{\pi}\right)_4 \equiv a^{(p-1)/4} \pmod{\pi}$. Rozlišme

- ▶ $a^{(p-1)/4} \equiv 1 \pmod{p}$, pak $\left(\frac{a}{\pi}\right)_4 = 1$ a $N = p + 1 - 2u$.
- ▶ $a^{(p-1)/4} \equiv -1 \pmod{p}$, pak $\left(\frac{a}{\pi}\right)_4 = -1$ a $N = p + 1 + 2u$.

Kryptosystém Alshehhi-Nitaj – základní myšlenka

Nechť pro přirozená čísla r, s je $p = (4r + 3)^2 + (4s + 2)^2$ prvočíslo. Pak $p \equiv 5 \pmod{8}$ a p se v $\mathbb{Z}[i]$ rozkládá na součin $p = \pi\bar{\pi}$, kde $\pi = (4r + 3) + (4s + 2)i$ je primární ireducibilní prvek.

Označme $u = 4r + 3$, $v = 4s + 2$, tedy $\pi = u + iv$, najdeme $c \in \mathbb{Z}$, aby $cv \equiv u \pmod{p}$. Protože $c^2v^2 \equiv u^2 \equiv -v^2 \pmod{p}$, je $c^2 \equiv -1 \pmod{p}$. Zvolme libovolně $a \in \mathbb{Z}$, $p \nmid a$. Podle věty 3 pro počet N bodů na eliptické křivce $y^2 = x^3 - ax$ platí

$$N = p + 1 - \overline{\left(\frac{a}{\pi}\right)_4} \cdot \pi - \left(\frac{a}{\pi}\right)_4 \cdot \bar{\pi}.$$

Víme, že $\left(\frac{a}{\pi}\right)_4 \in \{1, i, -1, -i\}$, $\left(\frac{a}{\pi}\right)_4 \equiv a^{(p-1)/4} \pmod{\pi}$. Rozlišme

- ▶ $a^{(p-1)/4} \equiv 1 \pmod{p}$, pak $\left(\frac{a}{\pi}\right)_4 = 1$ a $N = p + 1 - 2u$.
- ▶ $a^{(p-1)/4} \equiv -1 \pmod{p}$, pak $\left(\frac{a}{\pi}\right)_4 = -1$ a $N = p + 1 + 2u$.
- ▶ $a^{(p-1)/4} \equiv c \pmod{p}$, pak $\left(\frac{a}{\pi}\right)_4 \equiv c \pmod{\pi}$, a tedy $\overline{\left(\frac{a}{\pi}\right)_4} \cdot \pi + \left(\frac{a}{\pi}\right)_4 \cdot \bar{\pi} \equiv c(u - iv) \equiv 2cu \equiv 2c^2v \equiv -2v \pmod{\pi}$.

Kryptosystém Alshehhi-Nitaj – základní myšlenka

Nechť pro přirozená čísla r, s je $p = (4r + 3)^2 + (4s + 2)^2$ prvočíslo. Pak $p \equiv 5 \pmod{8}$ a p se v $\mathbb{Z}[i]$ rozkládá na součin $p = \pi \bar{\pi}$, kde $\pi = (4r + 3) + (4s + 2)i$ je primární ireducibilní prvek.

Označme $u = 4r + 3$, $v = 4s + 2$, tedy $\pi = u + iv$, najdeme $c \in \mathbb{Z}$, aby $cv \equiv u \pmod{p}$. Protože $c^2 v^2 \equiv u^2 \equiv -v^2 \pmod{p}$, je $c^2 \equiv -1 \pmod{p}$. Zvolme libovolně $a \in \mathbb{Z}$, $p \nmid a$. Podle věty 3 pro počet N bodů na eliptické křivce $y^2 = x^3 - ax$ platí

$$N = p + 1 - \overline{\left(\frac{a}{\pi}\right)}_4 \cdot \pi - \left(\frac{a}{\pi}\right)_4 \cdot \bar{\pi}.$$

Víme, že $\left(\frac{a}{\pi}\right)_4 \in \{1, i, -1, -i\}$, $\left(\frac{a}{\pi}\right)_4 \equiv a^{(p-1)/4} \pmod{\pi}$. Rozlišme

- ▶ $a^{(p-1)/4} \equiv 1 \pmod{p}$, pak $\left(\frac{a}{\pi}\right)_4 = 1$ a $N = p + 1 - 2u$.
- ▶ $a^{(p-1)/4} \equiv -1 \pmod{p}$, pak $\left(\frac{a}{\pi}\right)_4 = -1$ a $N = p + 1 + 2u$.
- ▶ $a^{(p-1)/4} \equiv c \pmod{p}$, pak $\left(\frac{a}{\pi}\right)_4 \equiv c \pmod{\pi}$, a tedy

$$\overline{\left(\frac{a}{\pi}\right)}_4 \cdot \pi + \left(\frac{a}{\pi}\right)_4 \cdot \bar{\pi} \equiv c(u - iv) \equiv 2cu \equiv 2c^2 v \equiv -2v \pmod{\pi}.$$

Protože $\overline{\left(\frac{a}{\pi}\right)}_4 \cdot \pi + \left(\frac{a}{\pi}\right)_4 \cdot \bar{\pi} \in \mathbb{Z}$, je $\overline{\left(\frac{a}{\pi}\right)}_4 \cdot \pi + \left(\frac{a}{\pi}\right)_4 \cdot \bar{\pi} \equiv -2v \pmod{p}$.

Kryptosystém Alshehhi-Nitaj – základní myšlenka

Nechť pro přirozená čísla r, s je $p = (4r + 3)^2 + (4s + 2)^2$ prvočíslo. Pak $p \equiv 5 \pmod{8}$ a p se v $\mathbb{Z}[i]$ rozkládá na součin $p = \pi \bar{\pi}$, kde $\pi = (4r + 3) + (4s + 2)i$ je primární ireducibilní prvek.

Označme $u = 4r + 3$, $v = 4s + 2$, tedy $\pi = u + iv$, najdeme $c \in \mathbb{Z}$, aby $cv \equiv u \pmod{p}$. Protože $c^2 v^2 \equiv u^2 \equiv -v^2 \pmod{p}$, je $c^2 \equiv -1 \pmod{p}$. Zvolme libovolně $a \in \mathbb{Z}$, $p \nmid a$. Podle věty 3 pro počet N bodů na eliptické křivce $y^2 = x^3 - ax$ platí

$$N = p + 1 - \overline{\left(\frac{a}{\pi}\right)}_4 \cdot \pi - \left(\frac{a}{\pi}\right)_4 \cdot \bar{\pi}.$$

Víme, že $\left(\frac{a}{\pi}\right)_4 \in \{1, i, -1, -i\}$, $\left(\frac{a}{\pi}\right)_4 \equiv a^{(p-1)/4} \pmod{\pi}$. Rozlišme

- ▶ $a^{(p-1)/4} \equiv 1 \pmod{p}$, pak $\left(\frac{a}{\pi}\right)_4 = 1$ a $N = p + 1 - 2u$.
- ▶ $a^{(p-1)/4} \equiv -1 \pmod{p}$, pak $\left(\frac{a}{\pi}\right)_4 = -1$ a $N = p + 1 + 2u$.
- ▶ $a^{(p-1)/4} \equiv c \pmod{p}$, pak $\left(\frac{a}{\pi}\right)_4 \equiv c \pmod{\pi}$, a tedy

$$\overline{\left(\frac{a}{\pi}\right)}_4 \cdot \pi + \left(\frac{a}{\pi}\right)_4 \cdot \bar{\pi} \equiv c(u - iv) \equiv 2cu \equiv 2c^2 v \equiv -2v \pmod{\pi}.$$

Protože $\overline{\left(\frac{a}{\pi}\right)}_4 \cdot \pi + \left(\frac{a}{\pi}\right)_4 \cdot \bar{\pi} \in \mathbb{Z}$, je $\overline{\left(\frac{a}{\pi}\right)}_4 \cdot \pi + \left(\frac{a}{\pi}\right)_4 \cdot \bar{\pi} \equiv -2v \pmod{p}$. Platí $|\pi| = |\bar{\pi}| = \sqrt{p} < \frac{p}{4}$, $|2v| < 2\sqrt{p} < \frac{p}{2}$, tedy

$$\overline{\left(\frac{a}{\pi}\right)}_4 \cdot \pi + \left(\frac{a}{\pi}\right)_4 \cdot \bar{\pi} = -2v, \text{ a proto } N = p + 1 + 2v.$$

Kryptosystém Alshehhi-Nitaj – základní myšlenka

Nechť pro přirozená čísla r, s je $p = (4r + 3)^2 + (4s + 2)^2$ prvočíslo. Pak $p \equiv 5 \pmod{8}$ a p se v $\mathbb{Z}[i]$ rozkládá na součin $p = \pi \bar{\pi}$, kde $\pi = (4r + 3) + (4s + 2)i$ je primární ireducibilní prvek.

Označme $u = 4r + 3$, $v = 4s + 2$, tedy $\pi = u + iv$, najdeme $c \in \mathbb{Z}$, aby $cv \equiv u \pmod{p}$. Protože $c^2 v^2 \equiv u^2 \equiv -v^2 \pmod{p}$, je $c^2 \equiv -1 \pmod{p}$. Zvolme libovolně $a \in \mathbb{Z}$, $p \nmid a$. Podle věty 3 pro počet N bodů na eliptické křivce $y^2 = x^3 - ax$ platí

$$N = p + 1 - \overline{\left(\frac{a}{\pi}\right)}_4 \cdot \pi - \left(\frac{a}{\pi}\right)_4 \cdot \bar{\pi}.$$

Víme, že $\left(\frac{a}{\pi}\right)_4 \in \{1, i, -1, -i\}$, $\left(\frac{a}{\pi}\right)_4 \equiv a^{(p-1)/4} \pmod{\pi}$. Rozlišme

▶ $a^{(p-1)/4} \equiv 1 \pmod{p}$, pak $\left(\frac{a}{\pi}\right)_4 = 1$ a $N = p + 1 - 2u$.

▶ $a^{(p-1)/4} \equiv -1 \pmod{p}$, pak $\left(\frac{a}{\pi}\right)_4 = -1$ a $N = p + 1 + 2u$.

▶ $a^{(p-1)/4} \equiv c \pmod{p}$, pak $\left(\frac{a}{\pi}\right)_4 \equiv c \pmod{\pi}$, a tedy

$$\overline{\left(\frac{a}{\pi}\right)}_4 \cdot \pi + \left(\frac{a}{\pi}\right)_4 \cdot \bar{\pi} \equiv c(u - iv) \equiv 2cu \equiv 2c^2 v \equiv -2v \pmod{\pi}.$$

Protože $\overline{\left(\frac{a}{\pi}\right)}_4 \cdot \pi + \left(\frac{a}{\pi}\right)_4 \cdot \bar{\pi} \in \mathbb{Z}$, je $\overline{\left(\frac{a}{\pi}\right)}_4 \cdot \pi + \left(\frac{a}{\pi}\right)_4 \cdot \bar{\pi} \equiv -2v \pmod{p}$. Platí $|\pi| = |\bar{\pi}| = \sqrt{p} < \frac{p}{4}$, $|2v| < 2\sqrt{p} < \frac{p}{2}$, tedy

$$\overline{\left(\frac{a}{\pi}\right)}_4 \cdot \pi + \left(\frac{a}{\pi}\right)_4 \cdot \bar{\pi} = -2v, \text{ a proto } N = p + 1 + 2v.$$

▶ $a^{(p-1)/4} \equiv -c \pmod{p}$, pak analogicky $N = p + 1 - 2v$.

Kryptosystém Alshehhi-Nitaj – použití

Generování klíčů: Je nutné zvolit velká přirozená čísla r_1, s_1, r_2, s_2 , aby pro $u_1 = 4r_1 + 3$, $v_1 = 4s_1 + 2$, $u_2 = 4r_2 + 3$, $v_2 = 4s_2 + 2$ byla $p_1 = u_1^2 + v_1^2$ a $p_2 = u_2^2 + v_2^2$ různá prvočísla.

Kryptosystém Alshehhi-Nitaj – použití

Generování klíčů: Je nutné zvolit velká přirozená čísla r_1, s_1, r_2, s_2 , aby pro $u_1 = 4r_1 + 3$, $v_1 = 4s_1 + 2$, $u_2 = 4r_2 + 3$, $v_2 = 4s_2 + 2$ byla $p_1 = u_1^2 + v_1^2$ a $p_2 = u_2^2 + v_2^2$ různá prvočísla. Pak $n = p_1 p_2$.

Kryptosystém Alshehhi-Nitaj – použití

Generování klíčů: Je nutné zvolit velká přirozená čísla r_1, s_1, r_2, s_2 , aby pro $u_1 = 4r_1 + 3$, $v_1 = 4s_1 + 2$, $u_2 = 4r_2 + 3$, $v_2 = 4s_2 + 2$ byla $p_1 = u_1^2 + v_1^2$ a $p_2 = u_2^2 + v_2^2$ různá prvočísla. Pak $n = p_1 p_2$. Dále je nutné zvolit $e \in \mathbb{Z}$, $e > 1$, které je nesoudělné s každým z čísel $(p_i + 1)^2 - 4u_i^2$, $(p_i + 1)^2 - 4v_i^2$, $i = 1, 2$.

Kryptosystém Alshehhi-Nitaj – použití

Generování klíčů: Je nutné zvolit velká přirozená čísla r_1, s_1, r_2, s_2 , aby pro $u_1 = 4r_1 + 3$, $v_1 = 4s_1 + 2$, $u_2 = 4r_2 + 3$, $v_2 = 4s_2 + 2$ byla $p_1 = u_1^2 + v_1^2$ a $p_2 = u_2^2 + v_2^2$ různá prvočísla. Pak $n = p_1 p_2$. Dále je nutné zvolit $e \in \mathbb{Z}$, $e > 1$, které je nesoudělné s každým z čísel $(p_i + 1)^2 - 4u_i^2$, $(p_i + 1)^2 - 4v_i^2$, $i = 1, 2$.

Veřejný klíč: n, e .

Kryptosystém Alshehhi-Nitaj – použití

Generování klíčů: Je nutné zvolit velká přirozená čísla r_1, s_1, r_2, s_2 , aby pro $u_1 = 4r_1 + 3$, $v_1 = 4s_1 + 2$, $u_2 = 4r_2 + 3$, $v_2 = 4s_2 + 2$ byla $p_1 = u_1^2 + v_1^2$ a $p_2 = u_2^2 + v_2^2$ různá prvočísla. Pak $n = p_1 p_2$. Dále je nutné zvolit $e \in \mathbb{Z}$, $e > 1$, které je nesoudělné s každým z čísel $(p_i + 1)^2 - 4u_i^2$, $(p_i + 1)^2 - 4v_i^2$, $i = 1, 2$.

Veřejný klíč: n, e .

Tajný klíč: $u_1, v_1, u_2, v_2, p_1, p_2$.

Kryptosystém Alshehhi-Nitaj – použití

Generování klíčů: Je nutné zvolit velká přirozená čísla r_1, s_1, r_2, s_2 , aby pro $u_1 = 4r_1 + 3$, $v_1 = 4s_1 + 2$, $u_2 = 4r_2 + 3$, $v_2 = 4s_2 + 2$ byla $p_1 = u_1^2 + v_1^2$ a $p_2 = u_2^2 + v_2^2$ různá prvočísla. Pak $n = p_1 p_2$. Dále je nutné zvolit $e \in \mathbb{Z}$, $e > 1$, které je nesoudělné s každým z čísel $(p_i + 1)^2 - 4u_i^2$, $(p_i + 1)^2 - 4v_i^2$, $i = 1, 2$.

Veřejný klíč: n, e .

Tajný klíč: $u_1, v_1, u_2, v_2, p_1, p_2$.

Šifrování: Zpráva je číslo $m \in \mathbb{Z}$, $0 < m < n$.

Kryptosystém Alshehhi-Nitaj – použití

Generování klíčů: Je nutné zvolit velká přirozená čísla r_1, s_1, r_2, s_2 , aby pro $u_1 = 4r_1 + 3$, $v_1 = 4s_1 + 2$, $u_2 = 4r_2 + 3$, $v_2 = 4s_2 + 2$ byla $p_1 = u_1^2 + v_1^2$ a $p_2 = u_2^2 + v_2^2$ různá prvočísla. Pak $n = p_1 p_2$. Dále je nutné zvolit $e \in \mathbb{Z}$, $e > 1$, které je nesoudělné s každým z čísel $(p_i + 1)^2 - 4u_i^2$, $(p_i + 1)^2 - 4v_i^2$, $i = 1, 2$.

Veřejný klíč: n, e .

Tajný klíč: $u_1, v_1, u_2, v_2, p_1, p_2$.

Šifrování: Zpráva je číslo $m \in \mathbb{Z}$, $0 < m < n$. Odesílající zvolí náhodné $r \in \mathbb{Z}$, $0 < r < n$ (je možné toto r použít k podpisu), může ověřit, že $(m, n) = 1$, $(r, n) = 1$, $(m^2 - r^3, n) = 1$, což skoro jistě platí, jinak by „uhádl“ rozklad n (s výjimkou případu $n \mid m^2 - r^3$) a spočítá $a \in \mathbb{Z}$ splňující $ra \equiv m^2 - r^3 \pmod{n}$.

Kryptosystém Alshehhi-Nitaj – použití

Generování klíčů: Je nutné zvolit velká přirozená čísla r_1, s_1, r_2, s_2 , aby pro $u_1 = 4r_1 + 3$, $v_1 = 4s_1 + 2$, $u_2 = 4r_2 + 3$, $v_2 = 4s_2 + 2$ byla $p_1 = u_1^2 + v_1^2$ a $p_2 = u_2^2 + v_2^2$ různá prvočísla. Pak $n = p_1 p_2$. Dále je nutné zvolit $e \in \mathbb{Z}$, $e > 1$, které je nesoudělné s každým z čísel $(p_i + 1)^2 - 4u_i^2$, $(p_i + 1)^2 - 4v_i^2$, $i = 1, 2$.

Veřejný klíč: n, e .

Tajný klíč: $u_1, v_1, u_2, v_2, p_1, p_2$.

Šifrování: Zpráva je číslo $m \in \mathbb{Z}$, $0 < m < n$. Odesílající zvolí náhodné $r \in \mathbb{Z}$, $0 < r < n$ (je možné toto r použít k podpisu), může ověřit, že $(m, n) = 1$, $(r, n) = 1$, $(m^2 - r^3, n) = 1$, což skoro jistě platí, jinak by „uhádl“ rozklad n (s výjimkou případu $n \mid m^2 - r^3$) a spočítá $a \in \mathbb{Z}$ splňující $ra \equiv m^2 - r^3 \pmod{n}$. Platí $(a, n) = 1$ a lze interpretovat dvojici $A = [r, m]$ jako bod ležící současně na eliptických křivkách \mathcal{E}_{p_1} nad \mathbb{Z}_{p_1} a na \mathcal{E}_{p_2} nad \mathbb{Z}_{p_2} daných rovnicí $y^2 = x^3 + ax$.

Kryptosystém Alshehhi-Nitaj – použití

Generování klíčů: Je nutné zvolit velká přirozená čísla r_1, s_1, r_2, s_2 , aby pro $u_1 = 4r_1 + 3$, $v_1 = 4s_1 + 2$, $u_2 = 4r_2 + 3$, $v_2 = 4s_2 + 2$ byla $p_1 = u_1^2 + v_1^2$ a $p_2 = u_2^2 + v_2^2$ různá prvočísla. Pak $n = p_1 p_2$. Dále je nutné zvolit $e \in \mathbb{Z}$, $e > 1$, které je nesoudělné s každým z čísel $(p_i + 1)^2 - 4u_i^2$, $(p_i + 1)^2 - 4v_i^2$, $i = 1, 2$.

Veřejný klíč: n, e .

Tajný klíč: $u_1, v_1, u_2, v_2, p_1, p_2$.

Šifrování: Zpráva je číslo $m \in \mathbb{Z}$, $0 < m < n$. Odesílající zvolí náhodné $r \in \mathbb{Z}$, $0 < r < n$ (je možné toto r použít k podpisu), může ověřit, že $(m, n) = 1$, $(r, n) = 1$, $(m^2 - r^3, n) = 1$, což skoro jistě platí, jinak by „uhádl“ rozklad n (s výjimkou případu $n \mid m^2 - r^3$) a spočítá $a \in \mathbb{Z}$ splňující $ra \equiv m^2 - r^3 \pmod{n}$. Platí $(a, n) = 1$ a lze interpretovat dvojici $A = [r, m]$ jako bod ležící současně na eliptických křivkách \mathcal{E}_{p_1} nad \mathbb{Z}_{p_1} a na \mathcal{E}_{p_2} nad \mathbb{Z}_{p_2} daných rovnicí $y^2 = x^3 + ax$. Odesílající pak spočítá bod $B = e \cdot A$, který odešle (výpočty provádí modulo n).

Kryptosystém Alshehhi-Nitaj – dešifrování

Příjemce použije tajný klíč a najde zbytky po dělení obou souřadnic bodu B prvočísky p_1 a p_2 , tím získá bod $B_1 = [x_1, y_1]$ na \mathcal{E}_{p_1} a bod $B_2 = [x_2, y_2]$ na \mathcal{E}_{p_2} .

Kryptosystém Alshehhi-Nitaj – dešifrování

Příjemce použije tajný klíč a najde zbytky po dělení obou souřadnic bodu B prvočísky p_1 a p_2 , tím získá bod $B_1 = [x_1, y_1]$ na \mathcal{E}_{p_1} a bod $B_2 = [x_2, y_2]$ na \mathcal{E}_{p_2} . Díky podmínkám při volbě e je násobení číslem e automorfismem na obou křivkách, a tedy body B_1, B_2 nemají řád 2, a tedy obě souřadnice těchto bodů jsou nenulové.

Kryptosystém Alshehhi-Nitaj – dešifrování

Příjemce použije tajný klíč a najde zbytky po dělení obou souřadnic bodu B prvočísky p_1 a p_2 , tím získá bod $B_1 = [x_1, y_1]$ na \mathcal{E}_{p_1} a bod $B_2 = [x_2, y_2]$ na \mathcal{E}_{p_2} . Díky podmínkám při volbě e je násobení číslem e automorfismem na obou křivkách, a tedy body B_1, B_2 nemají řád 2, a tedy obě souřadnice těchto bodů jsou nenulové. Pro každé $i = 1, 2$ určí a_i z kongruence $a_i x_i \equiv y_i^2 - x_i^3 \pmod{p_i}$. Spočítá $a_i^{(p_i-1)/4}$ modulo p_i , čímž získá počet N_i bodů na eliptické křivce \mathcal{E}_{p_i} , neboť

- ▶ Je-li $a_i^{(p_i-1)/4} \equiv \pm 1 \pmod{p_i}$, pak $N_i = p_i + 1 \mp 2u_i$.
- ▶ Je-li $v_i \cdot a_i^{(p_i-1)/4} \equiv \pm u_i \pmod{p_i}$, pak $N_i = p_i + 1 \pm 2v_i$.

Najde f_i , aby $e \cdot f_i \equiv 1 \pmod{N_i}$ a spočítá bod $C_i = f_i \cdot B_i$ na \mathcal{E}_{p_i} .

Kryptosystém Alshehhi-Nitaj – dešifrování

Příjemce použije tajný klíč a najde zbytky po dělení obou souřadnic bodu B prvočísky p_1 a p_2 , tím získá bod $B_1 = [x_1, y_1]$ na \mathcal{E}_{p_1} a bod $B_2 = [x_2, y_2]$ na \mathcal{E}_{p_2} . Díky podmínkám při volbě e je násobení číslem e automorfismem na obou křivkách, a tedy body B_1, B_2 nemají řád 2, a tedy obě souřadnice těchto bodů jsou nenulové. Pro každé $i = 1, 2$ určí a_i z kongruence $a_i x_i \equiv y_i^2 - x_i^3 \pmod{p_i}$. Spočítá $a_i^{(p_i-1)/4}$ modulo p_i , čímž získá počet N_i bodů na eliptické křivce \mathcal{E}_{p_i} , neboť

- ▶ Je-li $a_i^{(p_i-1)/4} \equiv \pm 1 \pmod{p_i}$, pak $N_i = p_i + 1 \mp 2u_i$.
- ▶ Je-li $v_i \cdot a_i^{(p_i-1)/4} \equiv \pm u_i \pmod{p_i}$, pak $N_i = p_i + 1 \pm 2v_i$.

Najde f_i , aby $e \cdot f_i \equiv 1 \pmod{N_i}$ a spočítá bod $C_i = f_i \cdot B_i$ na \mathcal{E}_{p_i} . Pak užije Čínskou zbytkovou větu, aby našel bod C , jehož souřadnice modulo p_1 dávají C_1 a modulo p_2 dávají C_2 . Platí $C = A$ (pro získání zprávy m stačí spočítat y -ovou souřadnici, pro případné ověření podpisu je nutné určit i x -ovou).

Kryptosystém Alshehhi-Nitaj – možnost podpisu

Možností, jak podepsat zprávu, je hodně, probereme jednu z nich.

Kryptosystém Alshehhi-Nitaj – možnost podpisu

Možností, jak podepsat zprávu, je hodně, probereme jednu z nich. Obě strany se předem dohodnou na metodě, jak vhodně odvodit číslo $z \in \mathbb{Z}$ ze znalosti n , aby $z^2 > n > 2z$, například $z = \lceil 100\sqrt{n} \rceil$.

Kryptosystém Alshehhi-Nitaj – možnost podpisu

Možností, jak podepsat zprávu, je hodně, probereme jednu z nich. Obě strany se předem dohodnou na metodě, jak vhodně odvodit číslo $z \in \mathbb{Z}$ ze znalosti n , aby $z^2 > n > 2z$, například $z = \lfloor 100\sqrt{n} \rfloor$.

Předpokládejme, že odesílatel si vytvořil veřejný a tajný klíč pro RSA, jehož modul $\tilde{n} = \tilde{p} \cdot \tilde{q}$ splňuje $2z < \tilde{n} < n$.

Kryptosystém Alshehhi-Nitaj – možnost podpisu

Možností, jak podepsat zprávu, je hodně, probereme jednu z nich. Obě strany se předem dohodnou na metodě, jak vhodně odvodit číslo $z \in \mathbb{Z}$ ze znalosti n , aby $z^2 > n > 2z$, například $z = \lceil 100\sqrt{n} \rceil$.

Předpokládejme, že odesílatel si vytvořil veřejný a tajný klíč pro RSA, jehož modul $\tilde{n} = \tilde{p} \cdot \tilde{q}$ splňuje $2z < \tilde{n} < n$. Tajný klíč \tilde{f} , \tilde{p} , \tilde{q} zná jen odesílatel, veřejný klíč \tilde{n} , \tilde{e} zná i příjemce (a je si jist, že skutečně patří odesílateli, tj. že klíč není podvržen).

Kryptosystém Alshehhi-Nitaj – možnost podpisu

Možností, jak podepsat zprávu, je hodně, probereme jednu z nich. Obě strany se předem dohodnou na metodě, jak vhodně odvodit číslo $z \in \mathbb{Z}$ ze znalosti n , aby $z^2 > n > 2z$, například $z = \lceil 100\sqrt{n} \rceil$.

Předpokládejme, že odesílatel si vytvořil veřejný a tajný klíč pro RSA, jehož modul $\tilde{n} = \tilde{p} \cdot \tilde{q}$ splňuje $2z < \tilde{n} < n$. Tajný klíč \tilde{f} , \tilde{p} , \tilde{q} zná jen odesílatel, veřejný klíč \tilde{n} , \tilde{e} zná i příjemce (a je si jist, že skutečně patří odesílateli, tj. že klíč není podvržen).

Odesílatel vyjádří zprávu m v z -adické poziční soustavě jako $m = tz + s$ a užitím svého tajného klíče spočítá zbytek w po dělení čísla $(t + s + 1)^{\tilde{f}}$ číslem \tilde{n} .

Kryptosystém Alshehhi-Nitaj – možnost podpisu

Možností, jak podepsat zprávu, je hodně, probereme jednu z nich. Obě strany se předem dohodnou na metodě, jak vhodně odvodit číslo $z \in \mathbb{Z}$ ze znalosti n , aby $z^2 > n > 2z$, například $z = \lceil 100\sqrt{n} \rceil$.

Předpokládejme, že odesílatel si vytvořil veřejný a tajný klíč pro RSA, jehož modul $\tilde{n} = \tilde{p} \cdot \tilde{q}$ splňuje $2z < \tilde{n} < n$. Tajný klíč \tilde{f} , \tilde{p} , \tilde{q} zná jen odesílatel, veřejný klíč \tilde{n} , \tilde{e} zná i příjemce (a je si jist, že skutečně patří odesílateli, tj. že klíč není podvržen).

Odesílatel vyjádří zprávu m v z -adické poziční soustavě jako $m = tz + s$ a užitím svého tajného klíče spočítá zbytek w po dělení čísla $(t + s + 1)^{\tilde{f}}$ číslem \tilde{n} . Při šifrování volí náhodně celé číslo $g \geq 0$ tak, aby $r = g\tilde{n} + w < n$.

Kryptosystém Alshehhi-Nitaj – možnost podpisu

Možností, jak podepsat zprávu, je hodně, probereme jednu z nich. Obě strany se předem dohodnou na metodě, jak vhodně odvodit číslo $z \in \mathbb{Z}$ ze znalosti n , aby $z^2 > n > 2z$, například $z = \lceil 100\sqrt{n} \rceil$.

Předpokládejme, že odesílatel si vytvořil veřejný a tajný klíč pro RSA, jehož modul $\tilde{n} = \tilde{p} \cdot \tilde{q}$ splňuje $2z < \tilde{n} < n$. Tajný klíč \tilde{f} , \tilde{p} , \tilde{q} zná jen odesílatel, veřejný klíč \tilde{n} , \tilde{e} zná i příjemce (a je si jist, že skutečně patří odesílateli, tj. že klíč není podvržen).

Odesílatel vyjádří zprávu m v z -adické poziční soustavě jako $m = tz + s$ a užitím svého tajného klíče spočítá zbytek w po dělení čísla $(t + s + 1)^{\tilde{f}}$ číslem \tilde{n} . Při šifrování volí náhodně celé číslo $g \geq 0$ tak, aby $r = g\tilde{n} + w < n$. Pak $r \equiv (t + s + 1)^{\tilde{f}} \pmod{\tilde{n}}$.

Kryptosystém Alshehhi-Nitaj – možnost podpisu

Možností, jak podepsat zprávu, je hodně, probereme jednu z nich. Obě strany se předem dohodnou na metodě, jak vhodně odvodit číslo $z \in \mathbb{Z}$ ze znalosti n , aby $z^2 > n > 2z$, například $z = \lceil 100\sqrt{n} \rceil$.

Předpokládejme, že odesílatel si vytvořil veřejný a tajný klíč pro RSA, jehož modul $\tilde{n} = \tilde{p} \cdot \tilde{q}$ splňuje $2z < \tilde{n} < n$. Tajný klíč \tilde{f} , \tilde{p} , \tilde{q} zná jen odesílatel, veřejný klíč \tilde{n} , \tilde{e} zná i příjemce (a je si jist, že skutečně patří odesílateli, tj. že klíč není podvržen).

Odesílatel vyjádří zprávu m v z -adické poziční soustavě jako $m = tz + s$ a užitím svého tajného klíče spočítá zbytek w po dělení čísla $(t + s + 1)^{\tilde{f}}$ číslem \tilde{n} . Při šifrování volí náhodně celé číslo $g \geq 0$ tak, aby $r = g\tilde{n} + w < n$. Pak $r \equiv (t + s + 1)^{\tilde{f}} \pmod{\tilde{n}}$.

Příjemce tím, že spočítá bod C , najde čísla r, m .

Kryptosystém Alshehhi-Nitaj – možnost podpisu

Možností, jak podepsat zprávu, je hodně, probereme jednu z nich. Obě strany se předem dohodnou na metodě, jak vhodně odvodit číslo $z \in \mathbb{Z}$ ze znalosti n , aby $z^2 > n > 2z$, například $z = \lceil 100\sqrt{n} \rceil$.

Předpokládejme, že odesílatel si vytvořil veřejný a tajný klíč pro RSA, jehož modul $\tilde{n} = \tilde{p} \cdot \tilde{q}$ splňuje $2z < \tilde{n} < n$. Tajný klíč \tilde{f} , \tilde{p} , \tilde{q} zná jen odesílatel, veřejný klíč \tilde{n} , \tilde{e} zná i příjemce (a je si jist, že skutečně patří odesílateli, tj. že klíč není podvržen).

Odesílatel vyjádří zprávu m v z -adické poziční soustavě jako $m = tz + s$ a užitím svého tajného klíče spočítá zbytek w po dělení čísla $(t + s + 1)^{\tilde{f}}$ číslem \tilde{n} . Při šifrování volí náhodně celé číslo $g \geq 0$ tak, aby $r = g\tilde{n} + w < n$. Pak $r \equiv (t + s + 1)^{\tilde{f}} \pmod{\tilde{n}}$.

Příjemce tím, že spočítá bod C , najde čísla r, m .

Určí pak z, t, s stejným postupem jako odesílatel a zjistí, zda $r^{\tilde{e}} \equiv t + s + 1 \pmod{\tilde{n}}$.

Kryptosystém Alshehhi-Nitaj – možnost podpisu

Možností, jak podepsat zprávu, je hodně, probereme jednu z nich. Obě strany se předem dohodnou na metodě, jak vhodně odvodit číslo $z \in \mathbb{Z}$ ze znalosti n , aby $z^2 > n > 2z$, například $z = \lceil 100\sqrt{n} \rceil$.

Předpokládejme, že odesílatel si vytvořil veřejný a tajný klíč pro RSA, jehož modul $\tilde{n} = \tilde{p} \cdot \tilde{q}$ splňuje $2z < \tilde{n} < n$. Tajný klíč \tilde{f} , \tilde{p} , \tilde{q} zná jen odesílatel, veřejný klíč \tilde{n} , \tilde{e} zná i příjemce (a je si jist, že skutečně patří odesílateli, tj. že klíč není podvržen).

Odesílatel vyjádří zprávu m v z -adické poziční soustavě jako $m = tz + s$ a užitím svého tajného klíče spočítá zbytek w po dělení čísla $(t + s + 1)^{\tilde{f}}$ číslem \tilde{n} . Při šifrování volí náhodně celé číslo $g \geq 0$ tak, aby $r = g\tilde{n} + w < n$. Pak $r \equiv (t + s + 1)^{\tilde{f}} \pmod{\tilde{n}}$.

Příjemce tím, že spočítá bod C , najde čísla r, m .

Určí pak z, t, s stejným postupem jako odesílatel a zjistí, zda $r^{\tilde{e}} \equiv t + s + 1 \pmod{\tilde{n}}$.

Pokud ano, uvěří, že zpráva pochází opravdu od odesílatele, neboť jen on znal číslo \tilde{f} (platí $1 < t + s + 1 < \tilde{n}$).