Домашна работа 2, №45342, група 3, Информатика

Иво Стратев

25 май 2017 г.

Задача 1.

Нека $R = \{a, b, c, d\}$ е пръстен със следните таблици за събиране и умножение:

+	a	b	c	d
a	d	c	b	a
b	c	d	a	b
c	b	a	d	c
d	a	b	c	d

*	a	b	c	d
a		d	d	d
b				d
c	a	b		d
d	d	d	d	d

Да се попълнят празните места в таблицата за умножение и да се опишат всички идеали на R

Решение:

$cc = c(a + b) = ca + cb = a + b = c$

+	a	b	c	d
a	d	c	b	a
b	c	d	a	b
c	b	a	d	c
d	a	b	c	d

*	a	b	c	d
a		d	d	d
b				d
c	a	b	c	d
d	d	d	d	d

$aa = a(c + b) = ac + ab = d + d = d$

+	a	b	c	d
a	d	c	b	a
b	c	d	a	b
c	b	a	d	c
d	a	b	c	d

*	a	b	c	d
a	d	d	d	d
b				d
c	a	b	c	d
d	d	d	d	d

$ba = (c + a)a = ca + aa = a + d = a$

+	a	b	c	d
a	d	c	b	a
b	c	d	a	b
c	b	a	d	c
d	a	b	c	d

*	a	b	c	d
a	d	d	d	d
b	a			d
c	a	b	c	d
d	d	d	d	d

$bb = (c + a)b = cb + ab = b + d = b$

+	a	b	c	d
a	d	c	b	a
b	c	d	a	b
c	b	a	d	c
d	a	b	c	d

*	a	b	c	d
a	d	d	d	d
b	a	b		d
c	a	b	c	d
d	d	d	d	d

$bc = (c + a)c = cc + ac = c + d = c$

+	a	b	c	d
a	d	c	b	a
b	c	d	a	b
c	b	a	d	c
d	a	b	c	d

*	a	b	c	d
a	d	d	d	d
b	a	b	c	d
c	a	b	c	d
d	d	d	d	d

Идеали на R:

Очевидно d е нулевия елемент на R

Тривиалните идеали на $R : \{d\},\ R$

Нетривиални идеали на R**:**

$$\begin{cases} a + d,\ d + a \in \{d, a\} \\ \forall r \in R\ ra,\ ar \in \{d, a\} \\ \forall r \in R\ rd = dr = d \in \{d, a\} \end{cases} \implies \{d, a\} \triangleleft R$$

$ba = a \notin \{d, b\} \implies \{d, b\} \ntriangleleft R$

$ca = a \notin \{d, c\} \implies \{d, c\} \ntriangleleft R$

$b + a = c \notin \{d, a, b\} \implies \{d, a, b\} \ntriangleleft R$

$c + a = b \notin \{d, a, c\} \implies \{d, a, c\} \ntriangleleft R$

$b + c = a \notin \{d, b, c\} \implies \{d, b, c\} \ntriangleleft R$

$a + a = d \notin \{a, b, c\} \implies \{a, b, c\} \ntriangleleft R$

Отговор: Идеалите на R **са:** $\{d\},\ \{d, a\},\ R$

Задача 2.

Нека $I = (387) \triangleleft \mathbb{Z}$ и $J = \{x \in \mathbb{Z} \mid \exists n = n(x) \in \mathbb{N}\ :\ x^n \in I\}$

Тв. $J \triangleleft \mathbb{Z}$

Док-во:

Нека $x, y \in J$ $(x - y) \in J \iff \exists k = k(x - y) \in \mathbb{N} :\ (x - y)^k \in I$

$\mathbb{Z}$ е комутативен пръстен с 1 $\implies$

$$(x-y)^k = \sum_{i=0}^{k} \binom{k}{i} x^i (-y)^{k-i} = \sum_{i=0}^{k} (-1)^{k-i} \binom{k}{i} x^i y^{k-i}$$

$$x, y \in J \implies \begin{cases} \exists n = n(x) \in \mathbb{N} : \ x^n \in I \\ \exists m = m(y) \in \mathbb{N} : \ y^m \in I \end{cases}$$

При $k = n + m$ $(x-y)^{n+m} = \displaystyle\sum_{i=0}^{n+m} (-1)^{n+m-i} \binom{n+m}{i} x^i y^{n+m-i} =$

$$= \sum_{i=0}^{n-1} (-1)^{n+m-i} \binom{n+m}{i} x^i y^{n+m-i} + \sum_{l=n}^{n+m} (-1)^{n+m-l} \binom{n+m}{l} x^l y^{n+m-l} =$$

$$= \sum_{i=0}^{n-1} (-1)^{n+m-i} \binom{n+m}{i} x^i y^{n-i} y^m + \sum_{l=n}^{n+m} (-1)^{n+m-l} \binom{n+m}{l} x^{l-n} y^{n+m-l} x^n$$

$$\forall t \in 0, \ldots, (n+m) \ \ (-1)^{n+m-t} \binom{n+m}{t} \in \mathbb{Z}$$

$$\forall t \in 0, \ldots, (n-1) \ \ n - t \geq 1 \implies x^t y^{n-t} \in \mathbb{Z} \quad \underset{\Longrightarrow}{y^m \in I}$$

$$\forall t \in 0, \ldots, (n-1) \ \ (-1)^{n+m-t} \binom{n+m}{t} x^t y^{n-t} y^m \in I \implies$$

$$\sum_{i=0}^{n-1} (-1)^{n+m-i} \binom{n+m}{i} x^i y^{n-i} y^m \in I$$

$$\forall t \in n, \ldots, (n+m) \ \ t - n \geq 0 \implies x^{t-n} y^{n+m-t} \in \mathbb{Z} \quad \underset{\Longrightarrow}{x^n \in I}$$

$$\forall t \in n, \ldots, (n+m) \ \ (-1)^{n+m-t} \binom{n+m}{t} x^{t-n} y^{n+m-t} x^n \in I \implies$$

$$\sum_{l=n}^{n+m} (-1)^{n+m-l} \binom{n+m}{l} x^{l-n} y^{n+m-l} x^n \in I \implies$$

$$(x-y)^{n+m} \in I \implies (x-y) \in J \implies \forall a, b \in J \ a - b \in J$$

Нека $z \in \mathbb{Z}, \ j \in J \implies \exists h = h(j) \in \mathbb{N} : \ j^h \in I$

$\mathbb{Z}$ е комутативен пръстен с 1 $\implies (zj)^h = z^h j^h \quad \underset{\Longrightarrow}{z^h \in \mathbb{Z}} \in I \implies$

$zj \in J \implies \forall r \in \mathbb{Z}, \ \forall g \in J \ rg \in J \implies J \triangleleft \mathbb{Z} \quad \square$

Тв. $I \subset J$

Док-во:

Нека $k \in I \implies k^1 = k \in I \subset \mathbb{Z} \implies k \in J \implies$

$\forall j \in I \ j \in J \implies I \subset J \quad \square$

$387 = 3^2.43$

Тв. $J = (3.43)$

Док-во:

Нека $K = (3.43) = \{3.43z \mid z \in \mathbb{Z}\}$

$I = (387) = (3^2.43) = \{3^2.43z \mid z \in \mathbb{Z}\}$

Нека $j \in J \implies \exists n = n(j) \in \mathbb{N} : \ j^n \in I \implies \exists k \in \mathbb{Z} : \ j^n = 3^2.43.k \implies$

$3.43|j^n \implies 3|j \ \wedge \ 43|j \implies 3.43|j \implies j \in K \implies \forall a \in J \ a \in K \implies J \subseteq K$

Нека $k \in K \implies \exists b \in \mathbb{Z} : \ k = 3.43.b \implies$

$\begin{cases} k^1 \in I, & 3|b \\ k^2 \in I, & 3 \not| b \end{cases} \implies k \in J \implies \forall h \in K \ h \in J \implies K \subseteq J \implies J = K = (3.43) \quad \square$

Задача 3.

Нека $I = (2 + \sqrt{-11}) \triangleleft \mathbb{Z}\left[\sqrt{-11}\right] = \{a + b\sqrt{-11} \mid a, \ b \in \mathbb{Z}\}$

$J = \{a + b\sqrt{-11} \mid a, \ b \in \mathbb{Z} : \ 15 \mid b + 7a\}$

Да се докаже, че: $I = J \ \wedge \ \mathbb{Z}\left[\sqrt{-11}\right]/I \cong \mathbb{Z}_{15}$

Решение:

Нека $z \in I \implies \exists a, \ b \in \mathbb{Z} : \ z = (a + b\sqrt{-11})(2 + \sqrt{-11}) =$

$= 2a + 2b\sqrt{-11} + a\sqrt{-11} + i^2 11b = (2a - 11b) + (a + 2b)\sqrt{-11}$

Нека $A = 2a - 11b, \ B = a + 2b \implies B + 7A = a + 2b + 14a - 77b =$

$= 15a - 75b = 15(a - 5b) \implies 15 \mid B + 7A \implies z \in J \implies \forall r \in I \ r \in J \implies I \subseteq J$

Нека $j \in J \implies \exists C, \ D \in \mathbb{Z} : \ j = C + D\sqrt{-11} \ \wedge \ 15 \mid D + 7C \implies$

$\exists k \in \mathbb{Z} : \ D + 7C = 15k \implies D = 15k - 7C$

Нека $C = 2c - 11d, \ D = c + 2d \implies C - 2D = C - 30k + 14C =$

$= 15(C - 2k) = -15d \implies d = 2k - C \in \mathbb{Z} \implies c = D - 2d \in \mathbb{Z} \implies$

$j = C + D\sqrt{-11} = (c + d\sqrt{-11})(2 + \sqrt{-11}) \implies j \in I \implies \forall t \in J \ t \in I \implies J \subseteq I$

$\implies I = J$

Нека $c,\ d \in \mathbb{Z}\left[\sqrt{-11}\right]:\ c = a_1 + b_1\sqrt{-11},\ d = a_2 + b_2\sqrt{-11} \implies$

$c+I = d+I \iff c-d = 0+I = I \iff c-d \in I \iff (a_1-a_2)+(b_1-b_2)\sqrt{-11} \in I$

$\iff 15 \mid (b_1 - b_2) + 7(a_1 - a_2) \iff 15 \mid (b_1 + 7a_1) - (b_2 + 7a_2)$

$\iff (b_1 + 7a_1) \equiv (b_2 + 7a_2) \pmod{15} \iff 13(b_1 + 7a_1) \equiv 13(b_2 + 7a_2) \pmod{15}$

$\iff (13b_1 + 91a_1) \equiv (13b_2 + 91a_2) \pmod{15} \iff (a_1 + 13b) \equiv (a_2 + 13b) \pmod{15}$

$15 = 2.7 + 1 \implies 1 = 15 - 2.7 \implies \overline{1} = \overline{15 - 2.7} = \overline{15} + \overline{-2.7} = \overline{13.7} = \overline{13}.\overline{7}$

$$\begin{aligned} \varphi:\ \ \mathbb{Z}\left[\sqrt{-11}\right] &\ \to\ \mathbb{Z}_{15} \\ a + b\sqrt{-11} &\ \mapsto\ \overline{a + 13b} \end{aligned}$$

$\varphi(c+d) = \varphi(a_1 + b_1\sqrt{-11} + a_2 + b_2\sqrt{-11}) = \varphi((a_1 + a_2) + (b_1 + b_2)\sqrt{-11}) =$

$= \overline{(a_1 + a_2) + 13(b_1 + b_2)} = \overline{a_1 + 13b_1} + \overline{a_2 + 13b_2} = \varphi(a_1 + b_1\sqrt{-11}) + \varphi(a_2 + b_2\sqrt{-11}) =$

$= \varphi(c) + \varphi(d) \implies \forall u,\ v \in \mathbb{Z}\left[\sqrt{-11}\right]\ \varphi(u+v) = \varphi(u) + \varphi(v)$

$\varphi(cd) = \varphi((a_1 + b_1\sqrt{-11})(a_2 + b_2\sqrt{-11})) = \varphi((a_1a_2 - 11b_1b2) + (a_1b_2 + b_1a_2)\sqrt{-11}) =$

$= \overline{(a_1a_2 - 11b_1b2) + 13(a_1b_2 + b_1a_2)} = \overline{(a_1a_2 + 4b_1b2) + 13(a_1b_2 + b_1a_2)} =$

$= \overline{(a_1a_2 + 169b_1b2) + 13(a_1b_2 + b_1a_2)} = \overline{a_1(a_2 + 13b_2) + 13b_1(a_2 + 13b_2)} =$

$= \overline{(a_1 + 13b_1)(a_2 + 13b_2)} = \overline{(a_1 + 13b_1)}\ \overline{(a_2 + 13b_2)} = \varphi(a_1 + 13b_1)\varphi(a_2 + 13b_2) =$

$= \varphi(c)\varphi(d) \implies \forall x,\ y \in \mathbb{Z}\left[\sqrt{-11}\right]\ \varphi(xy) = \varphi(x)\varphi(y) \implies \varphi$ е ХММ на пръстени

$Im\varphi = \{\tau \in \mathbb{Z}_{15} \mid \exists \delta \in \mathbb{Z}\left[\sqrt{-11}\right]:\ \tau = \varphi(\delta)\} = \{\varphi(\delta) \mid \delta \in \mathbb{Z}\left[\sqrt{-11}\right]\} \implies$

$Im\varphi \subseteq \mathbb{Z}_{15} \implies Im\varphi = \mathbb{Z}_{15} \iff \mathbb{Z}_{15} \subseteq Im\varphi$

$\forall \mu \in \{0,\ \ldots,\ 14\}\ \mu + 0\sqrt{-11} \in \mathbb{Z}\left[\sqrt{-11}\right]\ \wedge\ \varphi(\mu + 0\sqrt{-11}) = \overline{\mu + 13.0} = \overline{\mu} \implies$

$\forall \alpha \in \mathbb{Z}_{15}\ \exists \beta \in \mathbb{Z}\left[\sqrt{-11}\right]:\ \varphi(\beta) = \alpha \implies \alpha \in Im\varphi \implies \mathbb{Z}_{15} \subseteq Im\varphi \implies Im\varphi = \mathbb{Z}_{15}$

$Ker\varphi = \{\delta \in \mathbb{Z}\left[\sqrt{-11}\right] \mid \varphi(\delta) = \overline{0}\} = \{s + m\sqrt{-11} \in \mathbb{Z}\left[\sqrt{-11}\right] \mid \overline{s + 13m} = \overline{0}\} =$

$= \{s + m\sqrt{-11} \in \mathbb{Z}\left[\sqrt{-11}\right] \mid s + 13m \equiv 0 \pmod{15}\} =$

$= \{s + m\sqrt{-11} \in \mathbb{Z}\left[\sqrt{-11}\right] \mid 7s + 91m \equiv 0 \pmod{15}\} =$

$= \{s + m\sqrt{-11} \in \mathbb{Z}\left[\sqrt{-11}\right] \mid m + 7s \equiv 0 \pmod{15}\} =$

$\{s + m\sqrt{-11} \in \mathbb{Z}\left[\sqrt{-11}\right] \mid 15 \mid m + 7s\} = J = I \implies$

От теорема за ХММ-ите на пръстени $\implies \mathbb{Z}\left[\sqrt{-11}\right]/I \cong \mathbb{Z}_{15} \quad \square$

Задача 4.

Нека $f(x) = x^3 + \overline{2}x^2 + \overline{1} \in \mathbb{Z}_3[x]$

$\mathbb{Z}_3 = \{\overline{0},\ \overline{1},\ \overline{2}\}$

$f(\overline{0}) = \overline{1} \neq \overline{0}$

$f(\overline{1}) = \overline{1} + \overline{2}.\overline{1} + \overline{1} = \overline{4} = \overline{1} \neq \overline{0}$

$f(\overline{2}) = \overline{8} + \overline{2}.\overline{4} + \overline{1} = \overline{17} = \overline{2} \neq \overline{0}$

$\implies f$ е неразложим над $\mathbb{Z}_3 \implies \mathbb{Z}_3[x]/(f)$ е поле

Нека $g(x) = x^2 + x + \overline{1} \in \mathbb{Z}_3[x]$

$$
\begin{array}{l}
- \begin{array}{l} x^3 + \overline{2}x^2 + \overline{1} \ : \ x^2 + x + \overline{1} = x + \overline{1} \\ x^3 + x^2 + x \end{array} \\
\quad \overline{} \\
\quad - \begin{array}{l} x^2 + \overline{2} + 1 \\ x^2 + x + \overline{1} \end{array} \\
\qquad \overline{\phantom{x^2 + x + \overline{1}}} \\
\qquad\qquad x
\end{array}
$$

Нека $q(x) = x + \overline{1},\ r = x \in \mathbb{Z}_3[x]$

$f = gq + r \implies r = f - gq$

$$
\begin{array}{l}
- \begin{array}{l} x^2 + x + \overline{1} \ : \ x = x + \overline{1} \\ x^2 \end{array} \\
\quad \overline{\phantom{x^2 + x + \overline{1}}} \\
\quad - \begin{array}{l} x + \overline{1} \\ x \end{array} \\
\qquad \overline{\phantom{x + \overline{1}}} \\
\qquad\qquad \overline{1}
\end{array}
$$

$\implies (f, g) = \overline{1}$

$g = rq + (f, g) \implies$

$(f,g) = \overline{1} = g - rq = g - (f - gq)q = g - fq + q^2g = (1+q^2)g - fq \implies$

$((1+q^2)g + (-q)f) + (f) = \overline{1} + (f) \implies$

$((1+q^2)g + (f)) + ((-q)f) + (f)) = \overline{1} + (f) \implies$

$(1+q^2)g + (f) = \overline{1} + (f) \implies$

$1 + (x+\overline{1})^2 = x^2 + \overline{2}x + \overline{2}$ е обратният елемент на $x^2 + x + \overline{1}$ в $\mathbb{Z}_3[x]/(f)$

Проверка:

$gg^{-1} = (x^2 + x + \overline{1})(x^2 + \overline{2}x + \overline{2}) = x^4 + \overline{2}x^3 + \overline{2}x^2 + x^3 + \overline{2}x^2 + \overline{2}x + x^2 + \overline{2}x + \overline{2} =$

$= x^4 + \overline{2}x^2 + x + \overline{2}$

$$
\begin{array}{rl}
- & \begin{array}{l} x^4 + \overline{2}x^2 + x + \overline{2} \ : \ x^3 + \overline{2}x^2 + \overline{1} = x + \overline{1} \\ x^4 + \overline{2}x^3 + x \end{array} \\
\hline
& \begin{array}{rl} - & \begin{array}{l} x^3 + \overline{2}x^2 + \overline{2} \\ x^3 + \overline{2}x^2 + \overline{1} \end{array} \\ \hline & \overline{1} \end{array}
\end{array}
$$

Задача 5.

Нека $\mathbb{Q}(i) = \{a + bi \mid a, b \in \mathbb{Q}\},\ \mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\},$

$\mathbb{U} = \mathbb{Z}[i]^*, \quad \forall \alpha = a + bi \in \mathbb{Q}(i)\ N(\alpha) = a^2 + b^2$

a)

Тв. $\forall \alpha \in \mathbb{Q}(i)\ N(\alpha) = |\alpha|^2 = \alpha\overline{\alpha}$

Док-во:

Нека $\alpha = a + bi \in \mathbb{Q}(i)$. Гледайки на $\mathbb{Q}(i)$ като подпространство на $\mathbb{C}$, на което гледаме като двумерно Евклидово пространство и следвайки дефиницията за дължина на вектор получаваме $|\alpha| = \sqrt{<\alpha, \alpha>} = \sqrt{a^2 + b^2} \mid ()^2 \implies$

$|\alpha|^2 = (\sqrt{a^2 + b^2})^2 = a^2 + b^2 = N(\alpha)$

По дефиниция $\overline{\alpha} = a - bi \implies \alpha\overline{\alpha} = (a + bi)(a - bi) = a^2 - abi + abi - b^2i^2 =$

$= a^2 + b^2 = N(\alpha) \implies N(\alpha) = |\alpha|^2 = \alpha\overline{\alpha} \implies \forall \beta \in \mathbb{Q}(i)\ N(\beta) = |\beta|^2 = \beta\overline{\beta} \quad \square$

Тв. $\forall \alpha,\ \beta \in \mathbb{Q}(i)\ N(\alpha\beta) = N(\alpha)N(\beta)$

Док-во:

Нека $\alpha = a+bi,\ \beta = c+di \in \mathbb{Q}(i)\ N(\alpha\beta) = N((a+bi)(c+di)) = N(ac-bd+(ad+bc)i) =$

$= (ac-bd)^2 + (ad+bc)^2 = (ac)^2 - 2acbd + (bd)^2 + (ad)^2 + 2adbc + (bc)^2 =$

$= a^2c^2 + b^2d^2 + a^2d^2 + b^2c^2 = a^2(c^2+d^2) + b^2(c^2+d^2) = (c^2+d^2)(a^2+b^2) =$

$= N(\beta)N(\alpha) = N(\alpha)N(\beta) \implies \forall q, t \in \mathbb{Q}(i)\ N(qt) = N(q)N(t) \quad \square$

Тв. $\forall \alpha \in \mathbb{Q}(i)\backslash\{0\}\ N\left(\frac{1}{\alpha}\right) = \frac{1}{N(\alpha)}$

Док-во:

Нека $\alpha = a+bi \in \mathbb{Q}(i)\backslash\{0\}\ \frac{1}{\alpha} = \frac{\overline{\alpha}}{\alpha\overline{\alpha}} = \frac{a-bi}{N(\alpha)} = \frac{a}{N(\alpha)} - \frac{b}{N(\alpha)}i \implies$

$N\left(\frac{1}{\alpha}\right) = \frac{a}{N(\alpha)}^2 + \left(-\frac{b}{N(\alpha)}\right)^2 = \frac{a^2}{N(\alpha)^2} + \frac{b^2}{N(\alpha)^2} = \frac{a^2+b^2}{N(\alpha)^2} = \frac{N(\alpha)}{N(\alpha)^2} = \frac{1}{N(\alpha)} \implies$

$\forall \beta \in \mathbb{Q}(i)\backslash\{0\}\ N\left(\frac{1}{\beta}\right) = \frac{1}{N(\beta)} \quad \square$

Тв. $\forall \alpha \in \mathbb{Q}(i),\ \beta \in \mathbb{Q}(i)\backslash\{0\}\ N\left(\frac{\alpha}{\beta}\right) = \frac{N(\alpha)}{N(\beta)}$

Док-во:

$\forall \alpha \in \mathbb{Q}(i),\ \beta \in \mathbb{Q}(i)\backslash\{0\}\ N\left(\frac{\alpha}{\beta}\right) = N\left(\alpha\frac{1}{\beta}\right) = N(\alpha)N\left(\frac{1}{\beta}\right) = N(\alpha)\frac{1}{N(\beta)} = \frac{N(\alpha)}{N(\beta)} \quad \square$

б)

Тв. $\mathbb{U} = \{\alpha \in \mathbb{Z}[i] \mid N(\alpha) = 1\} = \{1,\ -1,\ i,\ -i\}$

Док-во: $\mathbb{U} = \{\alpha \in \mathbb{Z}[i] \mid N(\alpha) = 1\}$

Нека $\alpha,\ \beta \in \mathbb{U}:\ \alpha\beta = 1 \implies N(\alpha\beta) = N(1) \implies$

$N(\alpha)N(\beta) = 1 \iff N(\alpha) = 1 \land N(\beta) = 1 \implies \alpha,\ \beta \in \{z \in \mathbb{Z}[i] \mid N(z) = 1\} \implies$

$\forall u \in \mathbb{U}\ u \in \{u \in \mathbb{Z}[i] \mid N(u) = 1\} \implies \mathbb{U} \subseteq \{z \in \mathbb{Z}[i] \mid N(z) = 1\}$

Нека $\gamma \in \{z \in \mathbb{Z}[i] \mid N(z) = 1\} \implies N(\gamma) = \gamma\overline{\gamma} = 1 \implies \gamma,\ \overline{\gamma} \in \mathbb{U} \implies$

$\forall t \in \{z \in \mathbb{Z}[i] \mid N(z) = 1\}\ t,\ \bar{t} \in \mathbb{U} \implies \{z \in \mathbb{Z}[i] \mid N(z) = 1\} \subseteq \mathbb{U} \implies$

$\mathbb{U} = \{z \in \mathbb{Z}[i] \mid N(z) = 1\} \quad \square$

Док-во: $\mathbb{U} = \{1,\ -1,\ i,\ -i\}$

Нека $\alpha = a+bi \in \mathbb{Z}[i] \implies N(\alpha) = a^2+b^2 = 1 \implies a^2 = 1-b^2 = (1-b)(1+b) \implies$

$1-b=1+b \implies b=0 \implies a^2=1 \implies a=\pm 1 \implies$

$(a,b)=(\pm 1,0)$ е решение $\implies (a,b)=(0,\pm 1)$ също е решение, защото

$N(\alpha)$ е симетричен относно a и $b \implies$

$\mathbb{U}=\{a+bi \in \mathbb{Z}[i] \mid (a,b)=(\pm 1,0) \vee (a,b)=(0,\pm 1)\}=$

$=\{\pm 1+0i, 0\pm 1i\}=\{1,\ -1,\ i,\ -i\} \quad \square$

в)

Казваме, че две цели гаусови числа за асоциирани и пишем:

$\beta \sim \alpha \iff \exists \varepsilon \in \mathbb{U}:\ \beta=\varepsilon\alpha$

Тв. $\forall \alpha \in \mathbb{Z}[i]\ \beta \sim \alpha \iff N(\beta)=N(\alpha)$

Док-во:

Нека $\alpha,\ \beta \in \mathbb{Z}[i]:\ \beta \sim \alpha \iff \exists \varepsilon \in \mathbb{U}:\ \beta=\varepsilon\alpha \iff N(\beta)=N(\varepsilon\alpha) \iff$

$\iff N(\beta)=N(\varepsilon)N(\alpha) \iff N(\beta)=1N(\alpha) \iff N(\beta)=N(\alpha) \quad \square$

Тв асоциираността на цели гаусови числа е релация на еквивалентност

Док-во:

$\forall \alpha \in \mathbb{Z}[i] \implies \alpha=1\alpha \implies N(\alpha)=N(1)N(\alpha)=N(\alpha) \implies$

$\alpha \sim \alpha \implies \sim$ е рефлексивна

$\forall \alpha,\beta \in \mathbb{Z}[i]:\ \alpha \neq \beta, \alpha \sim \beta \implies \exists \varepsilon \in \mathbb{U}:\ \alpha=\varepsilon\beta \implies \varepsilon^{-1}\alpha=\beta \implies$

$\beta \sim \alpha \implies \sim$ е симетрична

$\forall \alpha,\ \beta,\ \gamma \in \mathbb{Z}[i]:\ \alpha \sim \beta \wedge \beta \sim \gamma \implies \exists \varepsilon,\ \delta \in \mathbb{U}:\ \alpha=\varepsilon\beta \wedge \beta=\delta\gamma$

$N(\varepsilon\delta)=N(\varepsilon)\mathbb{N}(\delta)=1.1=1 \implies \varepsilon\delta \in \mathbb{U} \implies$

$\alpha=\varepsilon\delta\gamma \implies \alpha \sim \gamma \implies \sim$ е транзитивна $\implies \sim$ е релация на еквивалентност

Следствие:

$\forall \alpha \in \mathbb{Z}[i] \quad [\alpha]=\{\beta \in \mathbb{Z}[i] \mid \alpha \sim \beta\}=\{\varepsilon\alpha \mid \varepsilon \in \mathbb{U}\}$

г)

Тв $\forall c, d \in \mathbb{Z},\ d \neq 0\ \exists!\ q,\ r \in \mathbb{Z}:\ c = qd + r\ \wedge\ |r| \leq \frac{1}{2}d$

Док-во:

Нека $c, d \in \mathbb{Z}$ делим ги с частно и остатък и получаваме:

$\exists!\ q,\ r \in \mathbb{Z}:\ c = qd + r\ \wedge\ 0 \leq r < d$ Сега ако $r \leq \dfrac{1}{2}d$ полагаме $q' = q\ \wedge\ r' = r$.

Ако $r > \dfrac{1}{2}d$ полагаме $q' = q + 1\ \wedge\ r' = r - d \implies |r'| = |r - d| = |d - r| < \frac{1}{2}d \implies$

$c = q'd + r'\ \wedge\ |r'| \leq \frac{1}{2}d \implies \forall z,\ t \in \mathbb{Z}\ \exists!\ u,\ v \in \mathbb{Z}:\ z = ut + v\ \wedge\ |v| \leq \frac{1}{2}t \quad \square$

Тв. $\forall \alpha,\ \beta \in \mathbb{Z}[i],\ \beta \neq 0\ \exists q,\ r \in \mathbb{Z}[i] : \alpha = \beta q + r\ \wedge\ N(r) < N(\beta)$

Док-во:

Нека $\alpha,\ \beta \in \mathbb{Z}[i],\ \beta \neq 0$

$\dfrac{\alpha}{\beta} = \dfrac{\alpha\overline{\beta}}{\beta\overline{\beta}} = \dfrac{\alpha\overline{\beta}}{N(\beta)}$, полагаме $\alpha\overline{\beta} = a + bi,\ a, b \in \mathbb{Z}$

Делим a и b с частно и остатък на $N(\beta)$: $\begin{cases} a = q_1 N(\beta) + r_1,\ q_1,\ r_1 \in \mathbb{Z}:\ |r_1| \leq \frac{1}{2}N(\beta) \\ \\ b = q_2 N(\beta) + r_2,\ q_2,\ r_2 \in \mathbb{Z}:\ |r_2| \leq \frac{1}{2}N(\beta) \end{cases}$

$\implies \frac{\alpha}{\beta} = \frac{q_1 N(\beta) + r_1 + (q_2 N(\beta) + r_2)i}{N(\beta)} = q_1 + q_2 i + \frac{r_1 + r_2 i}{N(\beta)} \implies \alpha = (q_1 + q_2 i)\beta + \frac{r_1 + r_2 i}{\overline{\beta}}$

Полагаме $q = q_1 + q_2 i \in \mathbb{Z}[i]\ \wedge\ r = \alpha - q\beta = \frac{r_1 + r_2 i}{\overline{\beta}} \in \mathbb{Z}[i]$

$N(r) = N\left(\frac{r_1 + r_2 i}{\overline{\beta}}\right) = \frac{N(r_1 + r_2 i)}{N(\overline{\beta})} = \frac{r_1^2 + r_2^2}{\overline{\beta}.\overline{\overline{\beta}}} = \frac{r_1^2 + r_2^2}{\overline{\beta}\beta} =$

$= \frac{r_1^2 + r_2^2}{N(\beta)} \leq \frac{\frac{1}{4}N(\beta)^2 + \frac{1}{4}N(\beta)^2}{N(\beta)} = \frac{1}{2}N(\beta) < N(\beta) \implies N(r) < N(\beta) \implies$

$\forall \gamma,\ \delta \in \mathbb{Z}[i],\ \delta \neq 0\ \exists u,\ t \in \mathbb{Z}[i] : \gamma = \delta u + t\ \wedge\ N(t) < N(\delta) \quad \square$

д)

Тв. $\forall I \trianglelefteq \mathbb{Z}[i]\ \exists z \in I :\ I = (z)$

Док-во:

Нека $I \neq \{0\} \trianglelefteq \mathbb{Z}[i] \implies \exists z \neq 0 \in I : \forall a \in I\ N(z) \leq N(a) \implies$

$\forall r \in \mathbb{Z}[i]\ rz \in (z)\ \wedge\ rz \in I \implies (z) \subseteq I$

Нека $x \in I\ \wedge\ \exists q,\ r \in \mathbb{Z}[i]:\ x = zq + r\ \wedge\ N(r) \leq N(z) \implies r = x - zq \implies r \in I$

Ако $r \neq 0 \implies \lightning(\forall b \in I\ N(z) \leq N(b)) \implies r = 0 \implies x = zq \implies x \in (z) \implies$

$\forall h \in I\ h \in (z) \implies I \subseteq (z) \implies I = (z) \implies \forall J \trianglelefteq \mathbb{Z}[i]\ \exists j \in J :\ J = (j) \quad \square$

е)

Тв. Нека $\rho, \alpha, \beta \in \mathbb{Z}[i] : \ \rho \notin \mathbb{U}, \ \rho = \alpha\beta$
$N(\beta) = N(\rho) \vee N(\alpha) = N(\rho) \iff \alpha \in \mathbb{U} \vee \beta \in \mathbb{U}$
Число ρ **с тези свойства ще наричаме просто в** $\mathbb{Z}[i]$

Док-во:

$N(\beta) = N(\rho) \iff \beta \sim \rho \iff \alpha \in \mathbb{U}$

$N(\alpha) = N(\rho) \iff \alpha \sim \rho \iff \beta \in \mathbb{U} \quad \square$

ж)

Тв. $\forall \alpha, \ \beta \in \mathbb{Z}[i] : \ \beta \mid \alpha \implies N(\beta) \mid N(\alpha)$

Док-во:

Нека $\alpha, \ \beta \in \mathbb{Z}[i] : \ \beta \mid \alpha \implies \exists \gamma \in \mathbb{Z}[i] : \ \alpha = \gamma\beta \implies$

$N(\alpha) = N(\beta\gamma) = N(\beta)N(\gamma) \implies N(\beta) \mid N(\alpha) \implies$

$\forall a, \ b \in \mathbb{Z}[i] : \ b \mid a \implies N(b) \mid N(a) \quad \square$

Тв. Нека ρ **е просто в** $\mathbb{Z}$**. Тоагава** ρ **е просто в** $\mathbb{Z}[i]$ **или съществува просто** $\pi \in \mathbb{Z}[i] : \ \rho = \pi\overline{\pi}, \ N(\pi) = N(\overline{\pi}) = \rho$

Док-во:

Нека ρ не е просто в $\mathbb{Z}[i] \implies \exists \alpha, \ \beta \in \mathbb{Z}[i] \backslash \mathbb{U} : \ \rho = \alpha\beta \implies$

$N(\rho) = N(\rho + 0i) = \rho^2 = N(\alpha\beta) = N(\alpha)N(\beta) \implies N(\alpha) = N(\beta) = \rho \implies$

$\alpha\beta = \rho = N(\alpha) \implies \beta = \frac{N(\alpha)}{\alpha} = \frac{\alpha\overline{\alpha}}{\alpha} = \overline{\alpha} \implies \rho = \alpha\overline{\alpha}$

Остава да докажем, че α е просто в $\mathbb{Z}[i]$

Нека $\gamma \in \mathbb{Z}[i] : \ \gamma \mid \alpha \implies N(\gamma) \mid N(\alpha) \implies N(\gamma) \mid \rho \implies$

$N(\gamma) = 1 \ \vee \ N(\gamma) = \rho \implies \gamma \in \mathbb{U} \ \vee \ \gamma \sim \alpha \implies \alpha$ е просто в $\mathbb{Z}[i] \quad \square$

з)

Тв. $\forall z \in \mathbb{Z} \ z^2 \equiv 0 \pmod 4 \ \vee \ z^2 \equiv 1 \pmod 4$

Док-во:

Нека $z \in \mathbb{Z}$

Ако $z \equiv 0 \pmod 4 \implies z^2 \equiv 0 \pmod 4$

Ако $z \equiv 1 \pmod 4 \implies z^2 \equiv 1 \pmod 4$

Ако $z \equiv 2 \pmod 4 \implies z^2 \equiv 2^2 \equiv 0 \pmod 4$

Ако $z \equiv 3 \pmod 4 \implies z^2 \equiv 3^2 \equiv 1 \pmod 4 \quad \square$

Тв. Нека p е просто в $\mathbb{Z}:\ p \equiv 3 \pmod 4 \implies \nexists\, x,\ y \in \mathbb{Z}:\ x^2 + y^2 = p$

Док-во:

$\forall x,\ y \in \mathbb{Z},\ z = x^2 + y^2 \implies z \equiv 0 \pmod 4 \ \vee\ z \equiv 1 \pmod 4 \ \vee\ z \equiv 2 \pmod 4 \implies$

$z \not\equiv 3 \pmod 4 \implies z \not\equiv p \pmod 4 \implies \nexists\, a,\ b \in \mathbb{Z}:\ a^2 + b^2 = p \quad \square$

и)

Тв. Нека p е просто в $\mathbb{Z}:\ p \equiv 3 \pmod 4 \implies p$ е просто и в $\mathbb{Z}[i]$

Док-во:

Нека $\beta = a + bi \in \mathbb{Z}[i]$ е прост делител на $p \implies \exists \alpha \in \mathbb{Z}[i]:\ p = \alpha\beta \implies$

$N(p) = N(p + 0i) = p^2 = N(\alpha\beta) = N(\alpha)N(\beta) \implies N(\beta) = p \ \vee\ N(\beta) = p^2 \implies$

$N(\beta) = p^2\ (a^2 + b^2 \neq p) \implies N(\alpha) = 1 \implies \alpha \in \mathbb{U} \implies$

$\beta \sim p \implies \beta$ е просто в $\mathbb{Z}[i] \quad \square$

к)

Тв. Нека p е просто в $\mathbb{Z}:\ p \equiv 1 \pmod 4 \implies$

$\left(\left(\frac{p-1}{2}\right)!\right)^2 \equiv -1 \pmod p \ \wedge\ \exists m \in \mathbb{N}:\ p \mid (m^2 + 1)$

Док-во:

$p \equiv 1 \pmod 4 \implies \exists k \in \mathbb{N}:\ p = 4k + 1 \implies \frac{p-1}{2} = 2k \in \mathbb{N}$

От теоремата на Уилсън получаваме: $(p-1)! \equiv (4k)! \equiv (2k)! \displaystyle\prod_{n=2k+1}^{4k} n \equiv \prod_{n=1}^{2k} n \prod_{n=1}^{2k} (p-n) \equiv$

$$\equiv \prod_{n=1}^{2k} n \prod_{n=1}^{2k} (-n) \equiv (-1)^{2k} \left(\prod_{n=1}^{2k} n\right)^2 \equiv ((2k)!)^2 \equiv -1 \pmod p \implies$$

$((2k)!)^2 + 1 \equiv 0 \pmod p \implies p \,\Big|\, \Big(((2k)!)^2 + 1\Big) \quad \square$

л)

Тв. Нека p е просто число $\implies \sqrt{p} \in \mathbb{R}\backslash\mathbb{Q}$

Док-во:

Допс. противното: нека $\sqrt{p} = \frac{a}{b} \in \mathbb{Q}:\ a,\ b \in \mathbb{N} \implies p = \frac{a^2}{b^2} \implies pb^2 = a^2$

Нека $p^{k'_1} \prod\limits_{i=2}^{m} p_i'^{k'_i}$ е каноничното представяне на a и нека

$p^{k''_1} \prod\limits_{i=2}^{n} p_i''^{k''_i}$ е каноничното представяне на b тогава

$$pp^{2k''_1} \prod_{i=2}^{n} p_i''^{2k''_i} = p^{2k'_1} \prod_{i=2}^{m} p_i'^{2k'_i} \implies p^{2k''_1+1} = p^{2k'_1} \implies 2k''_1 + 1 = 2k'_1$$

$$\implies 2(k'_1 - k''_1) = 1 \implies k'_1 - k''_1 = \frac{1}{2},\ k'_1,\ k''_1 \in \mathbb{N} \cup \{0\} \implies$$

$$k'_1 - k''_1 \in \mathbb{Z} \implies \frac{1}{2} \in \mathbb{Z} \implies \lightning \implies \sqrt{p} \in \mathbb{R}\backslash\mathbb{Q} \quad \square$$

Тв. Нека p е просто в $\mathbb{Z}:\ p \equiv 1 \pmod 4,\ m \in \mathbb{N}:\ p \mid (m^2+1)$
Нека $P = \{a \in \mathbb{N} \mid 0 \le a < \sqrt{p}\},\ M = \{x + my \mid x,\ y \in P\} \implies$
$\exists x_1 + my_1,\ x_2 + my_2 \in M : x_1 + my_1 \neq x_2 + my_2,\ x_1 + my_1 \equiv x_2 + my_2 \pmod p$
Нека $x = x_1 - x_2,\ y = y_1 - y_2 \implies p \mid (x + my) \ \wedge\ p \mid (x^2 + y^2) \ \wedge\ p = x^2 + y^2 \implies$
$\exists \pi$ **- просто** $\in \mathbb{Z}[i]:\ p = \pi\overline{\pi},\ N(\pi) = N(\overline{\pi}) = p,\ \nexists\, \varepsilon \in \mathbb{U}:\ \overline{\pi} = \varepsilon\pi$

Док-во:

$$\forall r \in \mathbb{R}\ \lfloor r \rfloor := \max\{m \in \mathbb{Z} \mid m \le r\},\ [[r]] := r - \lfloor r \rfloor \implies r = \lfloor r \rfloor + [[r]]$$

p е просто число $\implies \sqrt{p} \in \mathbb{R}\backslash\mathbb{Q} \implies [[\sqrt{p}]] > 0 \implies \mathbb{N} \ni \lfloor \sqrt{p} \rfloor < \sqrt{p}$

$$|P| = 1 + \lfloor \sqrt{p} \rfloor,\ |\mathbb{Z}_p| = p,\ |M| = |P|^2 \implies |M| - (|\mathbb{Z}_p| + 1) =$$

$$= (1 + \lfloor \sqrt{p} \rfloor)^2 - p - 1 = 2\lfloor \sqrt{p} \rfloor + \lfloor \sqrt{p} \rfloor^2 - \sqrt{p}^2 =$$

$$= 2\lfloor \sqrt{p} \rfloor + \lfloor \sqrt{p} \rfloor^2 - (\lfloor \sqrt{p} \rfloor + [[\sqrt{p}]])^2 =$$

$$= 2\lfloor \sqrt{p} \rfloor - 2\lfloor \sqrt{p} \rfloor[[\sqrt{p}]] - [[\sqrt{p}]]^2 = 2\lfloor \sqrt{p} \rfloor(1 - [[\sqrt{p}]]) - [[\sqrt{p}]]^2$$

Допс. $\quad 2\lfloor \sqrt{p} \rfloor(1 - [[\sqrt{p}]]) - [[\sqrt{p}]]^2 \le 0 \implies$

$$1 < 2\lfloor \sqrt{p} \rfloor(1 - [[\sqrt{p}]]) \le [[\sqrt{p}]]^2 < 1\ (0 < [[\sqrt{p}]] < 1\ \wedge\ [[\sqrt{p}]] \ll \lfloor \sqrt{p} \rfloor) \implies$$

$$\lightning \implies 2\lfloor \sqrt{p} \rfloor(1 - [[\sqrt{p}]]) - [[\sqrt{p}]]^2 > 0 \implies |M| > (|\mathbb{Z}_p| + 1) \implies$$

от принципа на Дирихле $\implies$

$\exists x_1 + my_1,\ x_2 + my_2 \in M : x_1 + my_1 \neq x_2 + my_2,\ x_1 + my_1 \equiv x_2 + my_2 \pmod p \implies$

$p \mid (x_1 + my_1 - (x_2 + my_2)) \implies p \mid (x_1 - x_2) + m(y_1 - y_2)) \implies$

$p \mid x + my \implies \exists k \in \mathbb{N} :\ x + my = kp \implies x = kp - my \implies$

$x^2 + y^2 = (kp - my)^2 + y^2 = k^2p^2 - 2kpmy + m^2y^2 + y^2 =$

$= k^2p^2 - 2kpmy + (m^2 + 1)y^2 \implies p \mid (x^2 + y^2)$

Ако $x = 0 \implies x_1 = x_2 \implies my_1 \equiv my_2 \pmod p \implies (y_1,\ y_2 \in P)$

$y_1 = y_2 \implies x_1 + my_1 = x_2 + my_2 \implies \lightning \implies |x| > 0$

Ако $y = 0 \implies y_1 = y_2 \implies x_1 \equiv x_2 \pmod p \implies (x_1,\ x_2 \in P)$

$x_1 = x_2 \implies x_1 + my_1 = x_2 + my_2 \implies \lightning \implies |y| > 0$

$x_1, x_2 \in P \implies 0 < |x| = |x_1 - x_2| \leq \lfloor \sqrt{p} \rfloor \implies 0 < x^2 \leq \lfloor \sqrt{p} \rfloor^2 < p$

$y_1, y_2 \in P \implies 0 < |y| = |y_1 - y_2| \leq \lfloor \sqrt{p} \rfloor \implies 0 < y^2 \leq \lfloor \sqrt{p} \rfloor^2 < p \implies$

$0 < x^2 + y^2 < 2p \ \wedge\ p \mid (x^2 + y^2) \implies x^2 + y^2 = p \implies p = (x - iy)(x + iy) \implies$

$\exists \pi \in \mathbb{Z}[i] :\ \ \pi = x + yi,\ \overline{\pi} = x - yi \implies N(\pi) = N(\overline{\pi}) = p \implies$

p не е просто в $\mathbb{Z}[i] \implies \pi$ е просто в $\mathbb{Z}[i]$

$1\pi = \pi = x + yi \neq x - yi$

$-1\pi = -x - yi \neq x - yi$

$i\pi = xi - y = -y + xi \neq x - yi$

$-i\pi = y - xi \neq x - yi \implies$

$\implies \pi \not\sim \overline{\pi} \implies \nexists\ \varepsilon \in \mathbb{U} :\ \overline{\pi} = \varepsilon\pi \quad \square$

м)

Тв. Нека $\pi \in \mathbb{Z}[i],\ \pi$ **е просто в** $\mathbb{Z}[i] \iff \exists \varepsilon \in \mathbb{U},\ \rho \in \mathbb{Z}[i] :\ \pi = \varepsilon\rho \implies$
$(\rho = 1 + i\ \vee\ \rho \equiv 3 \pmod 4)$ **е просто в** $\mathbb{Z} \vee N(\rho) \equiv 1 \pmod 4$ **е просто в** $\mathbb{Z})$

Док-во:

Нека $\exists \varepsilon \in \mathbb{U},\ \rho \in \mathbb{Z}[i] :\ \pi = \varepsilon\rho \implies \pi \sim \rho$ такива съществуват, защото

$\forall z \in \mathbb{Z}[i]\ 1.z = z,\ 1 \in \mathbb{U}$ и нека ρ е просто в $\mathbb{Z}[i] \implies \rho \mid N(\rho) = \rho\overline{\rho}$

$\forall z \in \mathbb{Z}[i]\ N(z) \in \mathbb{N} \implies$ от основната теорема на аритметиката, получаваме, че ρ дели някое просто число. Нека означим това просто число с r тогава нека $\exists \tau \in \mathbb{Z}[i]: \ r = \tau\rho$.

$\implies N(r) = N(\tau\rho) = N(\tau)N(\rho) \implies N(\rho) = r \ \vee \ N(\rho) = r^2$

Ако $r = 2 \implies N(\rho) = 2 \ \vee \ N(\rho) = 4$

Ако $N(r) = 4 \implies \rho \sim 2 = (1+i)(1-i) = (-1+i)(-1-i) \implies$

2 не е просто $\implies N(\rho) = 2 \implies \rho \in [1+i] \implies \rho$ е просто в $\mathbb{Z}[i]$

Ако $r \equiv 3 \pmod 4 \overset{\text{от з)}}{\implies} r$ е просто в $\mathbb{Z}[i] \ \wedge \ \rho \mid r \implies$

$\rho \sim r \implies \rho$ е просто в $\mathbb{Z}[i]$

Ако $r \equiv 1 \pmod 3$ Ако $N(\rho) = r^2$ от доказаното в л) ще следва к) от където ще следва, че ρ не е просто в $\mathbb{Z}[i] \implies N(\rho) = r \implies$ от ж) получаваме, че ρ е просто в $\mathbb{Z}[i]$ $\square$