3. Gaussova celá čísla

3.1. Uvažujme čísla 3, 5, 19, 101, 103, 149 a 157.

(a) Která z nich jsou prvočinitelé oboru $\mathbf{Z}[i]$?
(b) Čísla, pro něž je to možné, napište jako součet čtverců.
(c) Ta čísla, kerá nejsou prvočinitely rozložte v oboru $\mathbf{Z}[i]$ na součin prvočinitelů.

□

Všimněme si, že všechna uvedená čísla jsou lichá prvočísla.

(a) Podle věty z přednášky stačí zjistit, zda je zbytek po dělení daného prvočísla čtyřkou roven jedné či třem. Zřejmě

$$3 \equiv 3, \quad 5 \equiv 1, \quad 19 \equiv 3, \quad 101 \equiv 1, \quad 103 \equiv 3, \quad 149 \equiv 1, \quad 157 \equiv 1 \pmod 4.$$

Proto jsou prvočinitelem v oboru $\mathbf{Z}[i]$ právě čísla 3, 19 a 103.

(b) Připomenutá věta z přednášky, říká, že součtem čtverců jsou právě prvočísla, která jsou rozložitelná nad $\mathbf{Z}[i]$. Snadno zkusmo spočítáme, že

$$5 = 1^2 + 2^2, \quad 101 = 1^2 + 10^2, \quad 149 = 7^2 + 10^2, \quad 157 = 6^2 + 11^2.$$

(c) Z přednášky opět víme, že prvočinitelé $\mathbf{Z}[i]$ jsou právě ta prvočísla, která nejsou součet čtverců, a jakmile $p = a^2 + b^2 = (a + bi)(a - bi)$ pro nějaké prvočíslo p, pak jsou Gausova čísla $(a + bi)$ a $(a - bi)$ zřejmě prvočinitelé (jejich norma je totiž prvočíselná). Přímo z (b) tedy dostáváme rozklady na prvočinitele:

$$5 = (1 + 2i)(1 - 2i), \quad 101 = (1 + 10i)(1 - 10i),$$
$$149 = (7 + 10i)(7 - 10i), \quad 157 = (6 + 11i)(6 - 11i).$$

□

3.2. Najděte v grupách $\mathbf{Z}_5^*$ $\mathbf{Z}_{101}^*$, $\mathbf{Z}_{149}^*$ a $\mathbf{Z}_{157}^*$ všechny druhé odmocniny z -1.

Pro každé z prvočísel p hledáme prvky $a \in \mathbf{Z}_p^*$, pro něž $a^2 \equiv -1 (\mathrm{mod}\ p)$, tedy $p/a^2 + 1$. To znamená, že potřebujeme najít kořeny polynomu $x^2 + 1$ v tělese $\mathbf{Z}_p$. Všimněme si, že -1 je v grupě $\mathbf{Z}_p^*$ (jediný) prvek řádu 2 a hledáme prvky $\mathbf{Z}_4^*$ řádu 4. Protože 4 dělí $5 - 1$, $101 - 1$, $149 - 1$ i $157 - 1$, druhé odmocniny z -1 existují a jsou právě 2.

Už jsme našli rozklady $5 = 1^2 + 2^2 = 1^2 + (-2)^2 = 1^2 + 3^2$ v $\mathbf{Z}_5$ a $101 = 1^2 + 10^2 = 1^2 + (-10)^2 = 1^2 + 91^2$ v $\mathbf{Z}_{101}$, proto okamžitě dostáváme 2 a 3 druhé odmocniny z -1 v grup v grupě $\mathbf{Z}_5^*$ a 10 a 91 druhé odmocniny z -1 v grup v grupě $\mathbf{Z}_{101}^*$.

Nyní předpkládejme, že $a^2 \equiv -1 (\mathrm{mod}\ 149)$, tedy $149/a^2 + 1$ v oboru celých čísel, proto $149/a^2 + 1$ v oboru $\mathbf{Z}[i]$. V úloze (b) jsme zjistili, že $149 = (7 + 10i)(7 - 10i)$ je rozklad na prvočinitele, tedy například $(7 + 10i)$ dělí $a^2 + 1 = (a + i)(a - i)$ v oboru $\mathbf{Z}[i]$. Podle definice prvočinitele víme, že buď $(7 + 10i)/(a + i)$ nebo $(7 + 10i)/(a - i)$. Předpokládáme-li například, že $(7 + 10i)/(a + i)$, víme, že existuje $(x + yi) \in \mathbf{Z}[i]$, pro které $(7 + 10i) \cdot (x + yi) = (7x - 10y) + (10x + 7y)i = a + i$, a proto

$$7x - 10y = a, \qquad 10x + 7y = 1.$$

Snadno najdeme řešení $(x, y) = (5, -7)$ druhé rovnice (poznamenejme, že jde právě o Bezoutovy koeficienty nutně nesoudělných hodnot 7 a 10), díky němuž spočítáme

$a = 7 \cdot 5 + 10 \cdot 7 = 105$. Zbylou odmocninu nemusíme hledat pomocí úvahy $(7 - 10i)/(a+i)$, stačí vzít v tělese $\mathbf{Z}_{149}$ prvek opačný k nalezenému, tedy $149-105 = 44$. Čísla 44 a 105 jsou obě druhé odmocniny z -1 v grupě $\mathbf{Z}^*_{149}$.

Analogicky budeme postupovat i v grupě $\mathbf{Z}^*_{157}$. Opět uvážíme, že hledáme $a \in \mathbf{Z}^*_{157}$, aby v oboru $\mathbf{Z}[i]$

$$(6 + 11i)(6 - 11i) = 157/a^2 + 1 = (a + i)(a - i),$$

což vede na rovnice

$$6x - 11y = a, \qquad 11x + 6y = 1.$$

Snadno najdeme $(x, y) = (5, -9)$ splňující druhou rovnici, proto $a = 6 \cdot 5 + 11 \cdot 9 = 129$. Tedy Čísla 129 a $157 - 129 = 28$ jsou obě druhé odmocniny z -1 v grupě $\mathbf{Z}^*_{157}$. □

3.3. Uvažujme grupu $\mathbf{Z}^*_{317}$.

(a) Rozhodněte, pro která m existuje $a_m \in \mathbf{Z}^*_{317}$, pro něž $a_m^2 = 2^m$.
(b) Ověřte, že je prvek 2^{79} prvek řádu 4.
(c) Najděte všechny prvky řádu 4.

Předně si všimněme, že 317 je prvočíslo a $317 - 1 = 4 \cdot 79$, kde 79 je prvočíslo. Grupa $\mathbf{Z}^*_{317}$ je proto cyklická řádu 316 a obsahuje právě dva prvky řádu 4.

(a) Na přednášce bylo dokázáno pro každé prvočíslo p, že $2 = a^2$ v grupě $\mathbf{Z}^*_p$, právě když $p \equiv \pm 1 \bmod 8$. Protože $317 \equiv 5 \bmod 8$, vidíme, že 2 není čtvercem. Uvědomme si, že množina $D = \{a^2 |\ a \in \mathbf{Z}^*_{317}\}$ je podgrupa grupy $\mathbf{Z}^*_{317}$ indexu 2 (v izomorfní cyklické grupě $\mathbf{Z}_{316}$ s aditivním zápisem odpovídá právě podgrupě násobků dvojky, tedy podgrupě $2\mathbf{Z}_{316} = \langle 2 \rangle$), proto $2^m \in D$, právě když je m liché.

(b) Protože $(2^{79})^4 = 2^{316} = 1$ podle Lagrangeovy věty, musí mít prvek 2^{79} exponent 4, tedy je řádu 1,2 nebo 4. Ovšem prvek řádu 1 i prvek řádu 2 je v cyklické grupě jediný (1, resp. 316) a protože $\mathbf{Z}^*_{317}$ obsahuje pogrupu řádu 4, musí být oba čtvercem ($1 = 316^2$ a 316 je čtvercem odmocniny z -1, tedy právě kteréhokoli prvku řádu 4). Díky (a) je tedy 2^{79} nutně řádu 4.

(c) Stačí abychom vyčíslili 2^{79} v grupě $\mathbf{Z}^*_{317}$, což lze snadno provést i ručně:

$$2^{10} = 1024 \equiv 73, \quad 2^{20} \equiv 73^2 \equiv -60, \quad 2^{18} \equiv -15, \quad (\text{mod } 317)$$

$$2^{38} \equiv 4 \cdot 15^2 \equiv -51, \quad 2^{79} \equiv 8 \cdot 51^2 \equiv 8 \cdot 65 \equiv 203 \quad (\text{mod } 317)$$

Zjistili jsme, že $203^2 \equiv (-203)^2 \equiv -1 (\text{mod } 317)$, tedy 203 a $317 - 203 = 114$ jsou oba prvky řádu 4 grupy $\mathbf{Z}^*_{317}$. □

28.4.

3.4. Najděte přirozená čísla a, b, aby $317 = a^2 + b^2$.

V předchozí úloze jsme zjistili, že $114^2 + 1 \equiv 0 (\text{mod } 317)$, tedy, že $317/114^2 + 1 = (114 + i)(114 - i)$ v oboru $\mathbf{Z}[i]$. O hledaných hodnotách a, b ovšem víme, že $317 = a^2 + b^2 = (a + bi)(a - bi)$ a že $a + bi$ i $a - bi$ jsou prvočinitelé oboru $\mathbf{Z}[i]$, proto nutně buď $a + bi/114 + i$ nebo $a + bi/114 - i$, budeme-li hledat celá a, b, můžeme si vybrat například podmínku $a + bi/114 + i$. Zjistili jsme, že hledaný prvočinitel je společným dělitelem čísel 317 a $114 + i$, tudíž stačí abychom Eukleidovým algoritmem našli největší společný dělitel těchto dvou Gaussových celých čísel:

0. $z_0 = 317$.

1. $z_1 = 114 + i$.
2. Určíme nejprve komplexní $c_1 = \frac{317}{114+i} = \frac{317\cdot(114-i)}{114^2+1} = \frac{317\cdot(114)}{114^2+1} - i\frac{317}{114^2+1}$, a okamžitě vidíme, že 3 je nejbližší celé číslo k číslu $\frac{317\cdot(114)}{114^2+1}$ a 0 je nejbližší celé číslo k $\frac{317}{114^2+1}$. Nyní dostaneme $z_2 = 317 - 3\cdot(114+i) = -25 - 3i$.
3. Abychom určili podíl při dělení se zbytkem, opět spočítáme $c_2 = \frac{114+i}{-25-3i} = \frac{(114+i)\cdot(-25+3i)}{25^2+3^2} = \frac{-114\cdot(25)-3}{634} - i\frac{114\cdot 3-25}{634} = -\frac{5}{2} + i\frac{1}{2}$, a zbývá najít zbytek $z_3 = 114 + i + 4\cdot(-25-3i) = 14 - 11i$.
4. Snadnu už nahlédneme, že $14 - 11i / -25 - 3i$, tedy $14 - 11i$ je hledaný největší společný dělitel.

Zjistili jsme, že $317 = (14 - 11i)(14 + 11i) = 14^2 + 11^2$.

Závěrem poznamenejme, že kdybychom spočítali $114^2 + 1 = 317\cdot 41$ a uvědomili si, že $41 = 4^2 + 5^2 = (4 - 5i)(4 + 5i)$, stačilo by nám pro nalezení ireducibilního rozkladu čísla 317 v oboru $\mathbf{Z}[i]$ spočítat buď podíl $\frac{114+i}{4-5i}$ nebo $\frac{114+i}{4+5i}$. Vidíme, že zatímco $\frac{114+i}{4-5i} \notin \mathbf{Z}[i]$, dostáváme $\frac{114+i}{4-5i} = 11 + 14i \| 14 - 11i$. □

4. Charaktery a kvadratické zbytky

Připomeňme, že *charakterem* komutativní grupy rozumíme každý její homomorfismus do grupy $(\mathbf{C}^*, \cdot, ^{-1}, 1)$. Je-li χ charakter komutativní grupy A jehož obraz $\chi(A)$ je konečný, potom zřejmě $|\chi(a)| = 1$ pro všechna $a \in A$.

4.1. Najděte všechny charaktery

(a) aditivní grupy $\mathbf{Z}_2$,
(b) aditivní grupy $\mathbf{Z}_3$,
(c) aditivní grupy $\mathbf{Z}_n$ pro každé přirozené n,
(d) aditivní grupy $\mathbf{Z}_2 \times \mathbf{Z}_2$,
(e) multiplikativní grupy $\mathbf{Z}_5^*$,

(a) Jistě $\chi(0) = 1$ pro každý charakter χ, tedy zbývá rozhodnout kam se zobarazí prvek 1 grupy $\mathbf{Z}_2$. Protože je $\chi(1)\cdot\chi(1) = \chi(1+1) = \chi(0) = 1$ musí být $\chi(1)$ kořenem polynomu $x^2 - 1$. Zřejmě tedy máme právě dva charaktery, první konstatntní $\chi_0 \equiv 1$ a druhý daný podmínkou $\chi_1(1) = -1$.

(b) Uvážíme-li, že je $\mathbf{Z}_3$ cyklická grupa řádu 3, stačí nám najít obraz generátoru v grupě $\mathbf{C}^*$, který bude exponentu 3. Prvky exponentu 3 jsou právě všechny kořeny polynomu $x^3 - 1$, tedy čísla 1, $-\frac{1}{2} + \frac{\sqrt{3}}{2}i$ a $-\frac{1}{2} - \frac{\sqrt{3}}{2}i$, proto najdeme právě tři charaktery: konstantní $\chi_0 \equiv 1$ a dva nekonstatntní χ_1 a χ_2 dané podmínkou $\chi_1(1) = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$ a $\chi_2(1) = -\frac{1}{2} - \frac{\sqrt{3}}{2}i$, pro pořádek uveďme jejich hodnoty na celém definičním oboru:

$$\chi_1(0) = 1, \quad \chi_1(1) = -\frac{1}{2} + \frac{\sqrt{3}}{2}i, \quad \chi_1(2) = -\frac{1}{2} - \frac{\sqrt{3}}{2}i,$$

$$\chi_2(0) = 1, \quad \chi_2(1) = -\frac{1}{2} - \frac{\sqrt{3}}{2}i, \quad \chi_2(2) = -\frac{1}{2} + \frac{\sqrt{3}}{2}i,$$

(c) Podobně jako v úloze (b) stačí uvážit, že je charakter χ určen obrazem generátoru grupy $\mathbf{Z}_n$ a že $\chi(\mathbf{Z}_n)$ leží v množině všech kořenů polynomu $x^n - 1$.

Uvážíme-li, že kořeny polynomu $x^n - 1$ tvoří cyklickou grupu

$$\langle e^{\frac{2\pi}{n}i} \rangle = \{1, e^{2\frac{2\pi}{n}i}, e^{3\frac{2\pi}{n}i}, \ldots, e^{(n-1)\frac{2\pi}{n}i}\},$$

kde $e^{k\frac{2\pi}{n}i} = \cos(k\frac{2\pi}{n}) + i\sin(k\frac{2\pi}{n})$, máme pro každé $j \in \mathbf{Z}_n$ charakter χ_j daný vztahem $\chi_j(1) = e^{j\frac{2\pi}{n}i}$. Tedy existuje právě n různých charakterů a determinuje je předpis $\chi_j(k) = e^{jk\frac{2\pi}{n}i}$.

(d) Uvažujme charakter χ grupy $\mathbf{Z}_2 \times \mathbf{Z}_2$. V příkladu (a) jsme popsali homomorfismy $\mathbf{Z}_2$ do $\mathbf{C}^*$. Protože jsou inkluze ν_1 a ν_2 grupy $\mathbf{Z}_2$ do grupy $\mathbf{Z}_2 \times \mathbf{Z}_2$ dané předpisem $\nu_1(a) = (a, 0)$ a $\nu_1(a) = (0, a)$ zřejmě homomorfismy, zobrazení $\chi\nu_1$ a $\chi\nu_2$ jsou charaktery grupy $\mathbf{Z}_2$. Protože $\chi((1,1)) = \chi((1,0)+(0,1)) = \chi((1,0))\cdot\chi((0,1))$, určují obrazy prvků $(1,0)$ a $(0,1)$ právě jeden homomorfismus. Tedy máme právě 4 charaktery grupy $\mathbf{Z}_2 \times \mathbf{Z}_2$; konstantu $\chi_{++} \equiv 1$ a dále

$$\chi_{-+}((0,0)) = 1, \quad \chi_{-+}((1,0)) = -1, \quad \chi_{-+}((0,1)) = 1, \quad \chi_{-+}((1,1)) = -1,$$

$$\chi_{+-}((0,0)) = 1, \quad \chi_{+-}((1,0)) = 1, \quad \chi_{+-}((0,1)) = -1, \quad \chi_{+-}((1,1)) = -1,$$

$$\chi_{--}((0,0)) = 1, \quad \chi_{--}((1,0)) = -1, \quad \chi_{--}((0,1)) = -1, \quad \chi_{--}((1,1)) = 1.$$

(e) Protože je $\mathbf{Z}_5^*$ cyklická grupa řádu 4, stačí nám najít její generátor a využít příkladu (c) (tentokrát ovšem pracujeme s cyklickou grupou v multiplikativním zápisu). Generátorem je například prvek 2, proto podle (c) existují právě 4 charaktery $\mathbf{Z}_5^*$ dané předpisem $\chi_j(2^k) = e^{jk\frac{\pi}{2}i} = i^{jk}$ pro $j \in \mathbf{Z}_4$. Opět můžeme snadno všechny charaktery po prvcích popsat:

$$\chi_0(1) = \chi_0(2) = \chi_0(3) = \chi_0(4) = 1,$$

$$\chi_1(1) = 1, \quad \chi_1(2) = i, \quad \chi_1(3) = -i, \quad \chi_1(4) = -1,$$

$$\chi_2(1) = \chi_2(4) = 1, \quad \chi_2(2) = \chi_2(3) = -1,$$

$$\chi_3(1) = 1, \quad \chi_3(2) = -i, \quad \chi_3(3) = i, \quad \chi_3(4) = -1,$$

□

Protože charaktery konečné komutativní grupy můžeme po složkách násobit, dále konstanta 1 je jistě charakter a pro charakter $\overline{\chi}$ komplexně sdružený k charakteru χ platí $\chi \cdot \overline{\chi} \equiv 1$, máme na množině charakterů strukturu (multiplikativní) komutativní grupy.

4.2. Ověřte, že je grupa charakterů grupy $\mathbf{Z}_{11}^*$ cyklická a najděte všechny její generátory.

Na přednášce bylo dokázáno, že je grupa charakterů grupy A izomorfní grupě A. Protože je grupa $\mathbf{Z}_{11}^*$ cyklická řádu 10, je i grupa charakterů cyklická řádu 10 a musíme najít právě 4 její generátory. Navíc si uvědomme, že pro každý charakter χ je obraz $\chi(\mathbf{Z}_{11}^*)$ podgrupou desetiprvkové cyklické podgrupy $\langle e^{\frac{\pi}{5}i} \rangle$ grupy $\mathbf{C}^*$. Protože generátory grupy charakterů musí být prosté homomorfismy a prosté homomorfimsy grupy $\mathbf{Z}_{11}^*$ do grupy $\langle e^{\frac{\pi}{5}i} \rangle$ jsou právě čtyři (obě grupy jsou totiž cyklické řádu 10), potřebujeme najít právě izomorfismy grupy $\mathbf{Z}_{11}^*$ do grupy $\langle e^{\frac{\pi}{5}i} \rangle$. Homomorfismus cyklické grupy je ovšem určen obrazem generátoru a o izomorfismus půjde právě tehdy, když se generátor definičníáho oboru zobrazí na generátor oboru hodnot (tj. cyklické grupy stejného řádu).

Nyní zbývá nahlédnout, že například prvek 2 je generátorem grupy $\mathbf{Z}_{11}^*$, neboť $2^5 \equiv -1 \pmod{11}$, a že generátory grupy $\langle e^{\frac{\pi}{5}i}\rangle$ jsou právě prvky $e^{k\frac{\pi}{5}i}$ pro k nesoudělné s číslem 10 pomocí popisu 4.1(c) a analogicky k úvaze 4.1(e) jsou hledanými generátory charaktery

$$\chi_1(2^k) = e^{k\frac{\pi}{5}i}, \quad \chi_3(2^k) = e^{3k\frac{\pi}{5}i}, \quad \chi_7(2^k) = e^{7k\frac{\pi}{5}i}, \quad \chi_9(2^k) = e^{9k\frac{\pi}{5}i}.$$

Všimněme si, že $\chi_9 = \overline{\chi_1} = \chi_1^{-1}$ a $\chi_7 = \overline{\chi_3} = \chi_3^{-1}$ Z popisu 4.1(c) vidíme, že každý z charakterů je mocninou (například) charakteru χ_1, tedy na to, abychom ověřili, že je grupa charakterů cyklická jsme nemuseli používat větu z přednášky. □

5.5.

4.3. Popište konečné grupy, pro něž existuje prostý charakter.

Vezměme grupu $(G, \cdot, ^{-1}, 1)$ řádu n a nějaký její charakter χ. Podle Lagrangeovy věty $g^n = 1$, proto i $\chi(g)^n = \chi(g^n) = 1$ pro každý $g \in G$, tedy všechny prvky grupy $\chi(G)$ jsou kořeny polynomu $x^n - 1$ nad tělesem komplexních čísel. To znamená, že $\chi(G)$ je podgrupa grupy $\langle e^{\frac{2\pi}{n}i}\rangle \subseteq C^*$. Protože je grupa $\langle e^{\frac{2\pi}{n}i}\rangle$ cyklická, je cyklická i její podgrupa $\chi(G)$. Předpokládáme-li, že je χ prosté, potom musí jít izomorfismus grup G a $\chi(G) = \langle e^{\frac{2\pi}{n}i}\rangle$, tudíž je nutně cyklická grupa G. Vidíme, že prostý charakter existuje právě pro cyklické konečné grupy. □

4.4. Dokažte pro konečnou cyklickou grupu $(G, \cdot, ^{-1}, 1)$ a nějaký její charakter χ ekvivalenci následujících tvrzení:

(1) χ je prosté,
(2) $\chi^j \not\equiv 1$ pro žádné $j = 1, \ldots, |G| - 1$,
(3) χ generuje grupu charakterů grupy $(G, \cdot, ^{-1}, 1)$,
(4) je-li g generátor G, pak existuje k nesoudělné s $|G|$, pro které $\chi(g) = e^{\frac{2k\pi}{n}i}$

(1)⇔(4) χ je prosté právě když zobrazí generátor grupy G na generátor grupy $\langle e^{\frac{2\pi}{n}i}\rangle$, je ovšem snadné nahlédnout, že generétory gruipy $\langle e^{\frac{2\pi}{n}i}\rangle$ jsou právě prvky $e^{\frac{2k\pi}{n}i}$ pro k nesoudělné s $|G|$.

(2)⇔(3) je zřejmé.

(4)⇒(2) Jesliže $\mathrm{NSD}(k, |G|) = 1$, potom $\chi(g)^j = e^{\frac{2jk\pi}{n}i} \neq 1$ pro všechna $j = 1, \ldots, |G| - 1$, protože $\chi(g)$ generuje grupu $\chi(G)$ řádu $|G|$.

(2)⇒(1) Kdyby χ nebylo prosté, žádné χ^j by nebylo prosté, ačkoli prostý charakter podle předchozí úlohy existuje, proto $\langle\chi\rangle$ není celá grupa charakterů. □

4.5. Popište všechny charaktery χ grupy $\mathbf{Z}_n^*$ splňující podmínku $\chi^2 \equiv 1$, jestliže

(a) $n = 31$,
(b) $n = 65$

Předně si uvědomme, že hledáme prvky grupy charakterů exponentu 2. Jedním takovým charakterem je konstantní jednička, zbývá tedy najít všechny involuce grupy charakterů. Všimněme si, že pro každou involuci χ grupy charakterů platí, že $\chi(\mathbf{Z}_n^*) = \{-1, 1\}$.

Připomeňme navíc, že grupa charakterů je izomorfní původní grupě, tedy obvyklým způsobem snadno nahlédneme kolik involucí je třeba najít.

(a) Protože je $\mathbf{Z}_{31}^*$ cyklická, a proto obsahuje jedinou involuci, zbývá nám najít jediný charakter. Zjistíme-li, že například 3 je generátorem grupy $\mathbf{Z}_{31}^*$, pak hledaný

charakter určuje podmínka $\chi(3) = -1$, proto $\chi(3^j) = (-1)^j$. Kromě toho jsme si mohli uvědomit, že jedinou involuci grupy $\mathbf{Z}_{31}^*$ máme z přednášky označenu Legendrovým symbolem, tj $\chi(a) = \left(\frac{a}{31}\right)$, což říká, že $\chi(a) = 1$ právě tehdy, když je a kvadratickým zbytkem modulo 31.

(b) Protože $\mathbf{Z}_{65}^* \cong \mathbf{Z}_5^* \times \mathbf{Z}_{13}^* \cong \mathbf{Z}_4 \times \mathbf{Z}_3 \times \mathbf{Z}_4 \times$, vidíme, že budeme hledat právě 3 involuce. Uvažujme-li χ_5 nějaký charakter grupy $\mathbf{Z}_5^*$ a χ_{13} nějaký charakter grupy $\mathbf{Z}_{13}^*$, pak je zobrazení χ dané předpisem $\chi((a,b)) = \chi_5(a) \cdot \chi_{13}(b)$ charakter grupy $\mathbf{Z}_5^* \times \mathbf{Z}_{13}^*$.

Připomeňme, že Legendrův symbol určuje jedinou involuci $\left(\frac{=}{5}\right)$ na grupě $\mathbf{Z}_5^*$ a podobně $\left(\frac{=}{13}\right)$ je jediná involuce na grupě $\mathbf{Z}_{13}^*$. Protože Čínská věta o zbytcích indukuje homomorfismus multiplikativních grup dostaneme hledané charaktery jako složení:

$$\chi_{10}(k) = \left(\frac{k \bmod 5}{5}\right) = \left(\frac{k}{5}\right), \ \chi_{01}(k) = \left(\frac{k \bmod 13}{13}\right) = \left(\frac{k}{13}\right),$$

$$\chi_{11}(k) = \left(\frac{k \bmod 5}{5}\right)\left(\frac{k \bmod 13}{13}\right) = \left(\frac{k}{5}\right)\left(\frac{k}{13}\right) = \left(\frac{k}{65}\right).$$

V posledním řádku jsme použili Jacobiho symbol. □

4.6. Rozhodněte, zda jsou kvadratickým zbytkem

(a) prvky 5 a 7 grupy $\mathbf{Z}_{13}^*$,
(b) prvky 9, 27 a 32 grupy $\mathbf{Z}_{47}^*$,
(c) prvky 55, 111 a 112 grupy $\mathbf{Z}_{137}^*$.

Budeme využívat Větu o reciprocitě a (výše užívaná) tvrzení o tom, zda jsou prvky -1 a 2 kvadratické zbytky:

(a) Počítáme:

$$\left(\frac{5}{13}\right) = \left(\frac{13}{5}\right)(-1)^{\frac{13-1}{2}\cdot\frac{5-1}{2}} = \left(\frac{3}{5}\right) = \left(\frac{-1}{5}\right)\left(\frac{2}{5}\right) = 1 \cdot (-1) = -1,$$

$$\left(\frac{7}{13}\right) = \left(\frac{13}{7}\right)(-1)^{\frac{13-1}{2}\cdot\frac{7-1}{2}} = \left(\frac{-1}{7}\right) - 1.$$

Tedy ani 5 ani 7 nejsou modulo 13 kvadratické zbytky.

(b) Protože $9 = 3^2$ je určitě 9 kvadratický zbytek modulo 47, dál počítáme jako v (a):

$$\left(\frac{27}{47}\right) = \left(\frac{3}{47}\right)\left(\frac{9}{47}\right) = \left(\frac{3}{47}\right) = (-1)^{\frac{3-1}{2}\cdot\frac{47-1}{2}}\left(\frac{-1}{3}\right) = (-1)\cdot(-1) = 1,$$

$$\left(\frac{32}{47}\right) = \left(\frac{2}{47}\right)^5 = \left(\frac{2}{47}\right) = 1.$$

Zjistili jsme, že všechny hodnoty 9, 27 a 32 jsou kvadratické zbytky modulo 47

(c) Opět pracujeme s Lagendrovými symboly:

$$\left(\frac{55}{137}\right) = \left(\frac{5}{137}\right)\left(\frac{11}{137}\right) = \left(\frac{2}{5}\right)\left(\frac{5}{11}\right) = (-1)\left(\frac{1}{5}\right) = -1,$$

$$\left(\frac{111}{137}\right) = \left(\frac{-26}{137}\right) = \left(\frac{-1}{137}\right)\left(\frac{2}{137}\right)\left(\frac{13}{137}\right) = 1 \cdot 1 \cdot \left(\frac{13}{137}\right) = \left(\frac{5}{13}\right) = -1,$$

$$\left(\frac{112}{137}\right) = \left(\frac{-25}{137}\right) = \left(\frac{-1}{137}\right)\left(\frac{5}{137}\right)^2 = 1 \cdot 1 = 1.$$

Tentokrát jsme zjistili, že 55 a 111 nejsou kvadratické zbytky modulo 134, zatímco 112 je kvadratický zbytek modulo 134. □

12.5.

4.7. Rozhodněte, zda jsou kvadratickým zbytkem čísla 4301 a 7367 modulo prvočíslo 24851.

Budeme tentokrát pracovat s Jacobiho symboly, s kterými díky dokázanému lemmatu můžeme pracovat stejně jako s Lagendrovými symboly, ovšem nemusíme pro použití Věty o reciprocitě lichá čísla rozkládat na prvočíselný rozklad. Pro zpřehlednění zápisu využijme zřejmého faktu, že $a \equiv 1 (\mathrm{mod}\ 4)$, právě když $(a) \mathrm{mod}\ 100 \equiv 1 (\mathrm{mod}\ 4)$, tudíž v exponentech zjišťujících sudost čísla $\frac{n-1}{2}$ budeme psát jen poslední dvě cifry čísla $n-1$.

$$\left(\frac{4301}{24851}\right) = (-1)^{\frac{1-1}{2}\cdot\frac{51-1}{2}} \left(\frac{24851}{4301}\right) = \left(\frac{3346}{4301}\right) = \left(\frac{-1}{4301}\right)\cdot\left(\frac{955}{4301}\right) =$$

$$= (-1)^{\frac{1-1}{2}}(-1)^{\frac{1-1}{2}\cdot\frac{55-1}{2}} \left(\frac{481}{955}\right) = (-1)^{\frac{81-1}{2}\cdot\frac{55-1}{2}} \left(\frac{955}{481}\right) = \left(\frac{-7}{481}\right) =$$

$$= \left(\frac{-1}{481}\right)\cdot\left(\frac{7}{481}\right) = (-1)^{\frac{81-1}{2}}\cdot\left(\frac{481}{7}\right) = \left(\frac{-1}{7}\right)\cdot\left(\frac{2}{7}\right) = -1.$$

Stejně uvažujeme i v druhém případu:

$$\left(\frac{7367}{24851}\right) = (-1)^{\frac{67-1}{2}\cdot\frac{51-1}{2}} \left(\frac{2750}{7367}\right) = -\left(\frac{2}{7367}\right)\cdot\left(\frac{1375}{7367}\right) =$$

$$= -(-1)\cdot\left(\frac{492}{1375}\right) = \left(\frac{2}{1375}\right)^2\cdot\left(\frac{123}{1375}\right) = -\left(\frac{22}{123}\right) =$$

$$= -\left(\frac{2}{123}\right)\cdot\left(\frac{11}{123}\right) = -(-1)\cdot(-1)\cdot\left(\frac{2}{11}\right) = 1.$$

Zjistili jsme, že čísla 4301 není kvadratickým zbytkem modulo 24851, zatímco číslo 7367 kvadratickým zbytkem je. □

Kvadratické zbytky můžeme zjišťovat i modulo složená čísla, uvědomme si ovšem, že k tomu nelze přímočaře použít Jacobiho symboly.

4.8. Najděte všechny kvadratické zbytky grupy $\mathbf{Z}_{21}^*$.

Najprve využijeme Čínskou větu o zbytcích, abychom kvadratické zbytky spočítali. Protože

$$\mathbf{Z}_{21}^* \cong \mathbf{Z}_3^* \times \mathbf{Z}_7^* \cong \mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_3,$$

stačí spočítat počet prvků podgrupy $2(\mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_3) = \{0\} \times \{0\} \times \mathbf{Z}_3$ grupy $\mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_3$, vidíme tedy, že grupa $\mathbf{Z}_{21}^*$ obsahuje právě 3 kvadratické zbytky. Nyní snadno už snadno nahlédneme, že se jedná o prvky $1^2 = 1$, $2^2 = 4$ a $4^2 = 16$. □

Všimněme si, že 5 není kvadratický zbytek modulo 21. Ovšem 5 není kvadratický zbytek ani modulo 3 ani modulo 7, proto je hodnota Jacobiho symbolu $\left(\frac{5}{21}\right) = \left(\frac{5}{3}\right)\left(\frac{5}{7}\right) = 1$.

4.9. Spočítejte kvadratické zbytky grupy $\mathbf{Z}_{75}^*$ a $\mathbf{Z}_{225}^*$.

Opět využijeme Čínskou větu o zbytcích, která nám dává izomorfismus

$$\mathbf{Z}_{75}^* \cong \mathbf{Z}_3^* \times \mathbf{Z}_{25}^* \cong \mathbf{Z}_2 \times \mathbf{Z}_4 \times \mathbf{Z}_5.$$

Protože $2(\mathbf{Z}_2 \times \mathbf{Z}_4 \times \mathbf{Z}_5) = \{(0, 2a, b) |\ a \in \mathbf{Z}_2, b \in \mathbf{Z}_5\}$, máme v grupě $\mathbf{Z}_{75}^*$ právě 10 kvadratických zbytků.

S grupou $\mathbf{Z}_{225}^*$ pracujeme stejně, tentokrát máme izomorfismus

$$\mathbf{Z}_{225}^* \cong \mathbf{Z}_{3^2}^* \times \mathbf{Z}_{5^2}^* \cong \mathbf{Z}_6 \times \mathbf{Z}_{20} \cong \mathbf{Z}_2 \times \mathbf{Z}_4 \times \mathbf{Z}_3 \times \mathbf{Z}_5$$

a $2(\mathbf{Z}_2 \times \mathbf{Z}_4 \times \mathbf{Z}_3 \times \mathbf{Z}_5) = \{(0, 2a, b, c) |\ a \in \mathbf{Z}_2, b \in \mathbf{Z}_3, c \in \mathbf{Z}_5\}$, tudíž v grupě $\mathbf{Z}_{225}^*$ je právě 30 kvadratických zbytků. □

Konečně poznamenejme, že hodnota Jacobiho symbolu $\left(\frac{a}{225}\right) = \left(\frac{a}{3}\right)^2 \left(\frac{a}{5}\right)^2 = 1$ pro každé $a \in \mathbf{Z}_{225}^*$, ačkoli jsme zjistili, že $\mathbf{Z}_{225}^*$ obsahuje $\varphi(225) - 30 = 90$ kvadratických nezbytků.

5. Hustota prvočísel

5.1. Najděte na základě dokázaných tvrzení dolní odhad počtu všech deseticiferných prvočísel.

Na přednášce byl dokázán horní a dolní odhad počtu $\pi(n)$ prvočísel mensích jak n. Vyžijeme horní odhad pro $n = 10^9$ a dolní odhad pro $n = 10^{10}$, tedy

$$\pi(10^9) < 3 \cdot \frac{10^9}{\log(10^9)}, \quad \pi(10^{10}) \geq \frac{10^{10}}{\log(10^{10})} \cdot (\log 2 - \frac{\log(10^{10}+1)}{10^{10}}).$$

Odečteme-li od sebe tyto hodnoty dostaneme dolní odhad počtu prvočísel mezi čísly 10^9 a 10^{10}, tedy právě deseticiferných prvočísel

$$\frac{10^{10}}{\log(10^{10})} \cdot (\log 2 - \frac{\log(10^{10}+1)}{10^{10}}) - 3 \cdot \frac{10^9}{\log(10^9)} \geq \frac{10^9}{\log(10)}(0.693 - \frac{1}{3}) \geq 1.5 \cdot 10^8.$$

Další úlohy

(1) Uvažujme prvočísla $p = 13, 113, 313, 613$.
   (a) Rozložte čísla na součin prvočinitelů v oboru $\mathbf{Z}[i]$,
   (b) napište čísla jako součet čtverců.
   (c) najděte v grupách $\mathbf{Z}_p^*$ všechny druhé odmocniny z -1.

(2) Najděte v grupě $\mathbf{Z}_{313 \cdot 317}^*$ všechny druhé odmocniny z -1.

(3) Spočítejte rozklad na prvočinitele čísla 330 v oboru $\mathbf{Z}[i]$.

(4) Najděte všechny generátory grupy grupy charakterů grup $\mathbf{Z}_{43}^*$, $\mathbf{Z}_{81}^*$.

(5) Najděte všechny charaktery řádu 7 grupy $\mathbf{Z}_{296}^*$.

(6) Popište všechny involuce grup charakterů grupy $\mathbf{Z}_{66}^*$, $\mathbf{Z}_{147}^*$ a $\mathbf{Z}_{1071}^*$.

(7) Spočítejte hodnoty $\left(\frac{2617}{3533}\right)$, $\left(\frac{2533}{3533}\right)$, $\left(\frac{8791}{20359}\right)$ $\left(\frac{93757}{128713}\right)$.

(8) Spočítejte kvadratické zbytky grup $\mathbf{Z}_{625}^*$, $\mathbf{Z}_{1155}^*$ a $\mathbf{Z}_{1683}^*$.