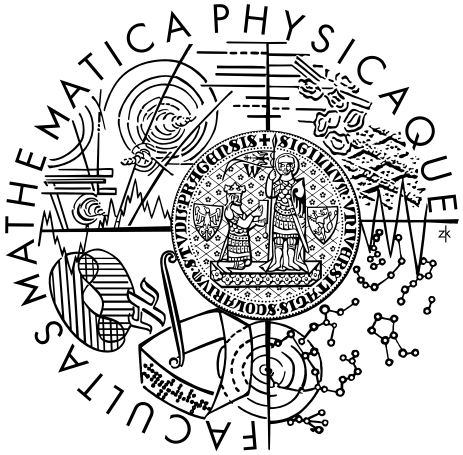
Univerzita Karlova v Praze
Matematicko-fyzikální fakulta

BAKALÁŘSKÁ PRÁCE



Michael Skotnica

Maximální množiny bodů na diskrétní torické mřížce bez trojic bodů ležících na stejné přímce

Katedra aplikované matematiky

Vedoucí bakalářské práce:	RNDr. Martin Tancer, Ph.D.
Studijní program:	Informatika
Studijní obor:	Obecná informatika

Praha 2016

Prohlašuji, že jsem tuto bakalářskou práci vypracoval(a) samostatně a výhradně s použitím citovaných pramenů, literatury a dalších odborných zdrojů.

Beru na vědomí, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorského zákona v platném znění, zejména skutečnost, že Univerzita Karlova v Praze má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle §60 odst. 1 autorského zákona.

V ..... dne ..... Podpis autora

Název práce: Maximální množiny bodů na diskrétní torické mřížce bez trojic bodů ležících na stejné přímce

Autor: Michael Skotnica

Katedra: Katedra aplikované matematiky

Vedoucí bakalářské práce: RNDr. Martin Tancer, Ph.D., Katedra aplikované matematiky

Abstrakt: Označme $\tau(T_{m\times n})$ maximální počet bodů na diskrétní torické mřížce o rozměrech $m \times n$ bez trojic bodů ležících na jedné přímce. Práce se zabývá otázkou, jaká je hodnota $\tau(T_{m\times n})$ pro různá m, n. Jedná se o variantu problému, který je znám jako no-three-in-line-problem. Nejdříve uvádíme některé poznatky z článků, které se touto otázkou již zabývaly. Některé z nich jsou zde zobecněny. Dále nově vylepšujeme horní a dolní odhady pro případy, které v předchozích článcích nebyly vyřešeny, zejména pro případy, kdy rozměry mřížky jsou mocniny prvočísla. Nakonec definujeme posloupnost $(\tau(T_{m\times n}))_{n\in\mathbb{N}}$, o které dokážeme, že je periodická pro libovolné pevné m.

Klíčová slova: diskrétní torická mřížka, kombinatorika bodů na přímkách, prvočísla, dělitelnost

Title: Maximal point sets on discrete toric grid with no three colinear points

Author: Michael Skotnica

Department: Department of Applied Mathematics

Supervisor: RNDr. Martin Tancer, Ph.D., Department of Applied Mathematics

Abstract: Let $\tau(T_{m\times n})$ denote maximal number of points on a discrete toric grid of the sizes $m \times n$ with no three colinear points. This thesis examines $\tau(T_{m\times n})$ for various m, n. It is a variant of the well-known no-three-in-line-problem. First, we present some previously known results. Then we generalize them in various directions. In particular we improve upper and lower bounds for cases which have not been solved in previous papers especially for cases when the sizes of the grid are prime powers. At the end we define the sequence $(\tau(T_{m\times n}))_{n\in\mathbb{N}}$ and we prove that it is periodic for all fixed m.

Keywords: discrete toric grid, combinatorics of points on lines, prime numbers, divisibility

Rád bych poděkoval vedoucímu práce RNDr. Martinu Tancerovi, Ph.D. za cenné rady, připomínky a podněty k práci, také za věnovaný čas a trpělivost.

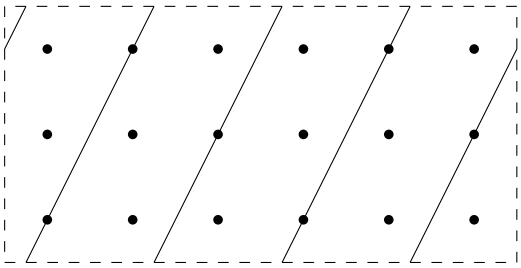
Dále bych chtěl poděkovat svým rodičům za podporu během studia.

Obsah

Úvod

V roce 1917 zformuloval anglický matematik Henry Dudeney otázku, kolik bodů lze nejvýše umístit na mřížku o rozměrech [1] $n \times n$ tak, aby žádné tři neležely na stejné přímce. Tento problém je znám jako **No-three-in-line-problem**. Stále však není vyřešen. V roce 2012 se proto rozhodli autoři Fowler, Groot, Pandya a Snapp ve článku **The no-three-in-line-problem on a torus**[1] formulovat a analyzovat variantu tohoto problému, ve které se snažíme umístit co nejvíce bodů v obecné poloze na torickou mřížku o rozměrech $m \times n$ pro m,$n \in \mathbb{N}$. Tuto torickou mřížku (neboli diskrétní torus) budeme označovat $T_{m\times n}$ a získáme ji jako kartézský součin množin $\{0,1,\ldots,m-1\} \times \{0,1,\ldots n-1\} \subset \mathbb{Z}^2$. Jako její přímku potom budeme rozumět obraz libovolné přímky l ze $\mathbb{Z}^2$ takový, že každý bod $(x,y) \in l$ zobrazíme na $(x \pmod m), y \pmod n)$. Autoři vyřešili tento problém pro případ, kdy m a n jsou nesoudělná a dále pro rozměry $p \times p$ a $p \times p^2$. Toto pak zobecnili Misiak, Stępień, A. Szymaszkiewicz, L. Szymaszkiewicz a Zwierzchowski (viz [2]) tak, že vyřešili problém pro případ, kdy největší společný dělitel m a n je prvočíslo.

Na obrázku vidíme přímku na torické mřížce o rozměrech 6×3.



V této práci si ukážeme poznatky z těchto dvou zmíněných článků a některé z nich zobecníme. Dále se budeme zabývat úpravou horních a dolních odhadů zejména pro případy, kdy největší společný dělitel rozměrů je mocnina prvočísla. Podíváme se také, jak se výsledky mění v případech, kdy jednu souřadnici mřížky zafixujeme a druhou měníme. Nejprve ale uveďme základní definici.

Definice. Pomocí $T_{m\times n}$ budeme označovat diskrétní torus (v práci budeme pro zkrácení používat pouze torus) o rozměrech $m \times n$ pro m,$n \in \mathbb{N}$ a $\tau(T_{a\times b})$ nám pak označuje velikost maximální množiny bodů na toru takové, že žádné tři body z této množiny neleží na stejné přímce.

Pro účely tohoto úvodu ještě poznamenejme, že GCD(m,n) pro m,$n \in \mathbb{N}$ označuje největšího společného dělitele čísel m,n.

Nyní se podívejme podrobněji na obsah a výsledky práce. V první části (1) se podíváme na základní vlastnosti torické mřížky potřebné pro další kapitoly.

Dále se v kapitole 2 podíváme, které případy jsou mezi sebou převoditelné. Půjde o zobecnění poznatků Misiaka a kol. [2], kteří ukázali, že $\tau(T_{xm\times yn}) \geq \tau(T_{m\times n})$ pro m,n,x,$y \in \mathbb{N}$ a že $\tau(T_{p\times p}) = \tau(T_{xp\times yp})$, kde p je prvočíslo a x,y,p jsou po dvou nesoudělná. My si ukážeme následující větu.

Věta 2.4. *Mějme $x, y, m, n \in \mathbb{N}$ taková, že* GCD(x,y) $= 1$, GCD(m,y) $= 1$ *a* GCD(n,x) $= 1$. *Potom $\tau(T_{xm\times yn}) = \tau(T_{m\times n})$.*

[1] rozumíme $\{0,\ldots,n-1\}^2 \subset \mathbb{Z}^2$

Díky tomu víme, že má smysl řešit problém jen pro rozměry, které mají stejná prvočísla v prvočíselném rozkladu.

Pomocí této věty budeme v kapitole 4 uvažovat, co se děje s hodnotami τ, když jeden rozměr toru necháme konstantní a druhý měníme. To nám definuje posloupnost $\tau(T_{z\times 1}), \tau(T_{z\times 2}), \tau(T_{z\times 3}), \ldots$ pro $z \geq 2$(případ $z = 1$ je triviální). Takovou posloupnost budeme označovat $P_z(x)$ a nahlédneme, že je periodická.

Věta 4.5. *Nechť $z \in \mathbb{N}$. Pak posloupnost P_z je periodická.*

Uvidíme, že zvlášť pěknou periodu dostaneme pro případ, kdy z je mocnina prvočísla. Dává nám to také motivaci zabývat se právě případy $T_{p^a\times p^b}$ pro p prvočíslo a a,$b \in \mathbb{N}$. Pokud se totiž vyřeší hodnoty posloupnosti v periodě pro nějakou mocninu prvočísla p^a, budeme umět určit hodnotu τ pro případ $T_{m,n}$, kde $\mathrm{GCD}(m,n) = p^a$.

V části 3.1 se budeme věnovat horním odhadům τ. Základní odhad, který platí pro obecné rozměry a ze kterého budeme vycházet je následující.

Věta 3.1. *Nechť $T_{m\times n}$, kde m,$n \in \mathbb{N}$ je torus. Potom $\tau(T_{m\times n}) \leq 2\,\mathrm{GCD}(m,n)$.*

Tento odhad už se objevil v článku [2]. Často však je velmi nadsazený. Proto ho vylepšíme pro mocniny prvočísla p.

Věta 3.10. *Buď $T_{p^a\times p^a}$ torus, kde p je prvočíslo, $a \in \mathbb{N}$. Potom $\tau(T_{p^a\times p^a}) \leq p^a + p^{\lceil \frac{a}{2}\rceil - 1} + 1$.*

Případ, kdy $a = 1$, už se objevil v článku Misiaka a kol. [2], kde je také ukázáno, jak odhad ještě vylepšit o 1. Tento poznatek si ukážeme.

Ukážeme si také jedno zobecnění, kdy dojdeme k hornímu odhadu pro $T_{pq\times pq}$, kde p,q jsou různá prvočísla.

Věta 3.15. *Mějme torus $T_{pq\times pq}$, kde p,q jsou prvočísla a nechť $kp < q$, kde $k \in \mathbb{N}$. Potom $\tau(T_{pq\times pq}) \leq pq + p + q + 2 - kp$.*

Dolním odhadům se budeme věnovat v části 3.2. Podíváme se na konstrukci pro p prvočíslo, kterou opět použili Misiak a kol. [2] a která nám dává $\tau(T_{p\times p^2}) \geq 2p$, což v kombinaci s výše uvedeným, obecným horním odhadem dává rovnost.

Věta 3.16. *Pro p prvočíslo $\tau(T_{p\times p^2}) = 2p$.*

Poté konstrukci zobecníme tak, abychom dostali dolní odhad pro případy $T_{p^a\times p^{a+1}}$.

Věta 3.17. *Mějme $a, b \in \mathbb{N}$ taková, že $a + 1 = b$, a buď p prvočíslo. Označme $z := a \pmod 3$. Potom platí:*

1. *Pokud $z = 0$, pak $\tau(T_{p^a\times p^b}) \geq 4p^{\frac{a}{3}}$.*
2. *Pokud $z = 1$, pak $\tau(T_{p^a\times p^b}) \geq 2p^{\lceil \frac{a}{3}\rceil}$.*
3. *Pokud $z = 2$, pak $\tau(T_{p^a\times p^b}) \geq 4p^{\lceil \frac{a}{3}\rceil}$.*

Horní odhad $2\,\mathrm{GCD}(m,n)$ (věta 3.1) nám také říká, jakého potenciálního maxima může nabývat výše definovaná posloupnost $P_z(x)$. Toto maximum je přirozeně $2z$. To nás vede k otázce, jestli této hodnoty někdy nabývá, případně pro jakou nejmenší hodnotu x to nastává. Jak už bylo zmíněno, práce se věnuje hlavně případům, kdy rozměry mřížky jsou mocniny prvočísla. Pro $z = p^a$ si ukážeme, že $P_{p^a}(x)$ tohoto potenciálního maxima dosahuje.

Věta 3.19. $\tau(T_{p^a \times p^{(a-1)p+2}}) = 2p^a$ *pro* $a \in N$ *a* p *prvočíslo.*

Pro $p = 2$ půjde ještě druhá souřadnice snížit o 1.

Věta 3.20. $\tau(T_{2^a \times 2^{2a-1}}) = 2^{a+1}$ *pro* $a \in N$.

Díky tomuto také dostaneme periodu pro P_{p^a} (4.3), která bude $p^{(a-1)p+2}$, resp. 2^{2a-1} pro P_{2^a}. Tato perioda ale ovšem nemusí být nejmenší.

1. Potřebná teorie a základní vlasnosti

V této části si nejprve uvedeme potřebné věty a definice zejména z algebry, které budeme využívat. Bude se jednat o známá tvrzení, jejichž důkaz nebude předmětem této práce. Dále se budeme zabývat základními vlastnostmi torické mřížky, na kterých budeme stavět v dalších kapitolách. Poznamenejme, že GCD(a,b) bude označovat největšího společného dělitele $a,b \in \mathbb{Z}$, lcm(a,b) potom nejmenší společný násobek $a,b \in \mathbb{Z}$. Dále $\mathrm{ord}_G(x)$ bude označovat řád prvku x v grupě G.

1.1 Důležité věty

Protože budeme často řešit rovnice s kongruencemi, uveďme základní tvrzení, které pro tyto rovnice platí a podle kterých se budeme řídit při úpravách.

Lemma 1.1 (viz např. [5] nebo [4]). *Buďte $a,b,c,d \in \mathbb{Z}$ a $k,n \in \mathbb{N}$, kde $n > 1$. Potom platí:*

1. *Jestliže $a \equiv b \pmod n$ a $c \equiv d \pmod n$, pak $a + c \equiv b + d \pmod n$, $a - c \equiv b - d \pmod n$, $ac \equiv bd \pmod n$ a $a^k \equiv b^k \pmod n$.*
2. *Jestliže $c \neq 0$, potom $a \equiv b \pmod n$ právě tehdy, když $ca \equiv cb \pmod{cn}$.*
3. *Jestliže $\mathrm{GCD}(c, n) = 1$, pak $a \equiv b \pmod n$ právě tehdy, když $ca \equiv cb \pmod n$.*

Využijeme také poznatek, který přímo plyne z Eukleidova algoritmu na hledání největšího společného dělitele a který říká, že největší společný dělitel dvou čísel je jejich lineární kombinací.

Věta 1.2 (O Bézoutových koeficientech, viz např. [5]). *Mějme $c,d \in \mathbb{Z}$. Potom existují $k,l \in \mathbb{Z}$ taková, že $\mathrm{GCD}(c,d) = kc + ld$.*

Dále bude třeba zmínit důležitou větu, která se týká grup typu $\mathbb{Z}_n$ a jejich kartézských součinů pro $n \in \mathbb{N}$. Tato věta je známa jako čínská zbytková věta, uvedeme si ji ve dvou verzích, ve kterých ji budeme potřebovat.

Věta 1.3 (Čínská zbytková věta, viz např. [5] nebo [4]). *Mějme kladná celá čísla $n_1, n_2, \ldots, n_k$ a číslo $n = \prod_{i=1}^{k} n_i$. Definujme zobrazení $H\colon \mathbb{Z}_n \to \prod_{i=1}^{k} \mathbb{Z}_i$ předpisem $H(x) = (x \pmod{n_1}, x \pmod{n_2}, \ldots, x \pmod{n_k})$. Pak toto zobrazení H je slučitelné se sčítáním a násobením, a navíc je bijekce právě tehdy, když $n_1, n_2, \ldots, n_k$ jsou po dvou nesoudělná.*

Z této věty nám plyne, že pokud máme $n, n_1, n_2 \in \mathbb{Z}$ taková, že $n = n_1 n_2$, soustava

$$\begin{aligned} x &\equiv a \pmod{n_1} \\ x &\equiv b \pmod{n_2} \end{aligned}$$

má řešení a toto řešení je jednoznačné v $\mathbb{Z}_n$, protože mezi Z_n a $Z_{n_1} \times Z_{n_2}$ je bijekce (zobrazení H z věty 1.3). Tedy prvek $(a,b) \in \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}$ má odpovídající prvek $x \in \mathbb{Z}_n$ takový, že $H(x) = (a,b)$. Druhá verze nám dá obecnější poznatek pro soustavu dvou rovnic s kongruencemi.

Věta 1.4 (Čínská zbytková věta, viz např. [2]). *Mějme $m,n \in \mathbb{N}$, $a,b \in \mathbb{Z}$. Potom soustava rovnic*

$$\begin{aligned} x &\equiv a \pmod{m} \\ x &\equiv b \pmod{n} \end{aligned}$$

je řešitelná právě tehdy, když $a \equiv b \pmod{\mathrm{GCD}(m,n)}$, a toto řešení je jednoznačné v $\mathbb{Z}_{\mathrm{lcm}(m,n)}$.

Nakonec ještě zmíníme jednu potřebnou větu z teorie čísel.

Věta 1.5 (Dirichletova věta, viz např. [3]). *Buďte k,l kladná celá čísla taková, že $\mathrm{GCD}(k,l) = 1$. Potom existuje nekonečně mnoho prvočísel ve tvaru $k + yl$, kde $y \in \mathbb{N}$.*

1.2 Základní vlastnosti

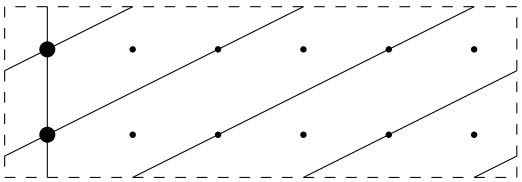
Nyní už se podíváme na základní vlastnosti torické mřížky a přímek na ní. Pro tyto účely nejprve zmíníme jednu definici.

Definice 1.6. Buď n přirozené číslo. Potom definujme zobrazení $f_n : \mathbb{Z} \to \mathbb{Z}_n$ pomocí předpisu $f_n(k) = k \pmod{n}$.

Jak již bylo řečeno v úvodu, přímku na toru $T_{m\times n}$ chápeme jako obraz přímky ze $\mathbb{Z}^2$ tak, že každý bod (x,y) této přímky zobrazíme na $(f_m(x), f_n(y))$. Přímku ze $\mathbb{Z}^2$ můžeme napsat ve tvaru $\{(b_1,b_2) + k(v_1,v_2); k \in \mathbb{Z}\}$, kde $(b_1,b_2),(v_1,v_2) \in \mathbb{Z}^2$. Bod (b_1,b_2) označuje počáteční bod a (v_1,v_2) je vektor, který přímku generuje. Zároveň předpokládáme, že $\mathrm{GCD}(v_1,v_2) = 1$. Chceme totiž, aby každé dva body ze $\mathbb{Z}^2$ ležely společně na právě jedné přímce (viz [2]). Obraz této přímky na toru potom bude $\{f_m(b_1), f_n(b_2)) + (f_m(kv_1), f_n(kv_2)); k \in \mathbb{Z}\}$. My budeme ale pro účely této práce přímku na toru zapisovat jako $\{(b_1,b_2) + k(v_1,v_2); k \in \mathbb{Z}\}$ a budeme implicitně předpokládat, že body jsou zobrazeny na torus. Zároveň budeme samozřejmě i na toru předpokládat, že $\mathrm{GCD}(v_1,v_2) = 1$.

Je dobré si všimnout, že vzorem přímky na toru je nekonečně mnoho přímek ze $\mathbb{Z}^2$, které nejsou nutně rovnoběžné. Např. všechny přímky ze $\mathbb{Z}^2$ ve tvaru $\{(2i,0) + k(0,1); k \in \mathbb{Z}\}$ pro $i \in \mathbb{Z}$ nám na $T_{2\times 2}$ dají jednu přímku. Stejnou přímku na $T_{2\times 2}$ nám dá také $\{k(2,1); k \in \mathbb{Z}\}$.

Také se může stát, že přímka $p_1 \subseteq T_{m\times n}$, která je obrazem přímky $l_1 \subset \mathbb{Z}^2$, je podmnožinou přímky $p_2 \subseteq T_{m\times n}$, která je obrazem přímky $l_2 \subset \mathbb{Z}^2$, jak vidíme na obrázku níže.



V práci se často budeme potřebovat podívat, jaké přímky leží mezi dvěma body $(a_1, a_2), (b_1,b_2)$ toru $T_{m\times n}$. Tyto přímky budou obrazy přímek mezi body $(a_1+\alpha_1 m, a_2+\alpha_2 n)$ a $(b_1+\beta_1 m, b_2+\beta_2 n)$ v $\mathbb{Z}^2$ pro $\alpha_1, \alpha_2, \beta_1, \beta_2 \in \mathbb{Z}$. Úlohu hledaní přímky mezi dvěma body v $\mathbb{Z}^2$ můžeme posunutím převést na hledání přímky procházející počátkem a nějakým bodem ze $\mathbb{Z}^2$. Pokud má tento bod nesoudělné souřadnice, může být zároveň použit jako vektor generující hledanou přímku. V opačném případě souřadnice vydělíme jejich největším společným dělitelem a takový vektor potom použijeme na generování hledané přímky. Zkusme podobně postupovat i na toru. Tedy mějme torus $T_{m\times n}$ a bez újmy na obecnosti body (0,0) a bod (a_1, a_2). Podíváme se, že takto získáme některé hledané přímky.

Nejprve uvažujme, že $\mathrm{GCD}(a_1, a_2) = 1$. V takovém případě se podívejme na přímku $l = \{k(a_1, a_2); k \in \mathbb{Z}\} \subseteq T_{m\times n}$. Tato přímka jistě bude ležet mezi počátkem a bodem (a_1, a_2). Může se nám ale stát, že na toru bude existovat i jiná přímka $p \neq l$ procházející těmito dvěma body. Tato přímka pak bude nutně nadmnožinou přímky l, protože přímka p je generována nějakým vektorem, jehož násobkem je (a_1, a_2). Budou tudíž jeho násobkem také násobky (a_1, a_2), a tedy i celá přímka l. Později si ale ukážeme (lemma 1.8), kdy toto nenastane a mezi počátkem a (a_1, a_2) bude ležet právě jedna přímka.

Nyní předpokládejme, že $g = \mathrm{GCD}(a_1, a_2) \neq 1$. V tomto případě budeme hledat vektor (x,y), který po vynásobení číslem g dává (a_1, a_2). Dostaneme soustavu

$$\begin{aligned} gx &\equiv a_1 \pmod{m} \\ gy &\equiv a_2 \pmod{n}. \end{aligned}$$

Zde bude záležet, jestli g je soudělné s m, resp. n. Pokud g není soudělné s např. m, dle lemmatu 1.1 dostaneme $\frac{x}{g} \equiv \frac{a_1}{g} \pmod{m}$. V opačném případě označme $h = \mathrm{GCD}(g, m)$. Rovnici pak upravíme dle 1.1 na $\frac{gx}{h} \equiv \frac{a_1}{h} \pmod{\frac{m}{h}}$. Díky tomu budeme potom hledat přímky mezi počátkem a více body, které už ale budou mít nesoudělné souřadnice.

Poznamenejme také, že na torus $T_{m\times n}$ můžeme nahlížet také jako na grupu $\mathbb{Z}_m \times \mathbb{Z}_n$ (viz [1]). V takovém případě přímka toru, která prochází počátkem, je nějaká cyklická podgrupa $\mathbb{Z}_m \times \mathbb{Z}_n$, která je generována prvkem z $\mathbb{Z}_m \times \mathbb{Z}_n$, který chápeme jako vektor. Pokud $\mathrm{GCD}(m,n) = 1$, je z Čínské zbytkově věty (1.3) grupa $\mathbb{Z}_m \times \mathbb{Z}_n$ izomorfní s grupou $\mathbb{Z}_{mn}$, která je cyklická. Grupa $\mathbb{Z}_m \times \mathbb{Z}_n$ je pak také cyklická, a tudíž všechny body na toru $T_{m\times n}$ leží na jedné přímce, a proto bude v takovém případě $\tau(T_{m\times n}) = 2$.

Dále, jak už bylo zmiňováno výše, se podíváme, v jakém případě bude mezi počátkem a bodem (a_1, a_2) s nesoudělnými souřadnicemi ležet jen jedna přímka. Nejprve ale musíme uvést lemma, které nám říká, jak určit délku přímky.

Lemma 1.7. *Mějme torus $T_{m\times n}$, kde $m, n \in \mathbb{N}$. Dále mějme na toru přímku $l = \{b + k(\alpha, \beta); k \in \mathbb{Z}\} \subseteq T_{m\times n}$ pro $b \in T_{m\times n}$ a $\alpha \in \mathbb{Z}_m, \beta \in \mathbb{Z}_n$ taková, že $\mathrm{GCD}(\alpha, \beta) = 1$. Potom délka přímky l je $\mathrm{lcm}(\frac{m}{\mathrm{GCD}(m,\alpha)}, \frac{n}{\mathrm{GCD}(n,\beta)})$.*

Důkaz. Přímka l je generovaná vektorem (α, β). Délka přímky l je potom rovna řádu (α, β) v grupě $\mathbb{Z}_m \times \mathbb{Z}_n$. Ten vypočítáme:

$$\mathrm{ord}_{\mathbb{Z}_m\times\mathbb{Z}_n}((\alpha, \beta)) = \mathrm{lcm}(\mathrm{ord}_{\mathbb{Z}_m}(\alpha), \mathrm{ord}_{\mathbb{Z}_n}(\beta)).$$

Řád prvku h v grupě $\mathbb{Z}_x$ potom dostaneme jako

$$\mathrm{ord}_{\mathbb{Z}_x}(h) = \frac{\mathrm{lcm}(h,x)}{h} = \frac{\frac{hx}{\mathrm{GCD}(h,x)}}{h} = \frac{x}{\mathrm{GCD}(h,x)}.$$

□

Lemma 1.8. *Mějme torus $T_{m\times n}$. Dále předpokládejme, že m, n mají stejná prvočísla v prvočíselném rozkladu. Pak mezi počátkem a bodem (a_1, a_2) s nesoudělnými souřadnicemi leží právě jedna přímka.*

Důkaz. Již víme, že mezi počátkem a (a_1, a_2) leží přímka $l = \{k(a_1, a_2); k \in \mathbb{Z}\} \subseteq T_{m\times n}$. Pro spor předpokládejme, že mezi těmito body leží i jiná přímka p, která, jak již víme, musí být nadmnožinou l. Nechť je tato přímka generována vektorem (b_1, b_2). Musí tedy platit, že existuje $i \in \mathbb{Z}$ takové, že

$$\begin{aligned} ib_1 &\equiv a_1 \pmod m \\ ib_2 &\equiv a_2 \pmod n. \end{aligned}$$

Z toho plyne, že $a_1 = ib_1 - \alpha_1 m$ a $a_2 = ib_2 - \alpha_2 n$ pro vhodná $\alpha_1, \alpha_2 \in \mathbb{Z}$. Poznamenejme, že $\mathrm{GCD}(ib_1 - \alpha_1 m, m) = \mathrm{GCD}(ib_1, m)$ a $\mathrm{GCD}(ib_2 - \alpha_2 n, n) = \mathrm{GCD}(ib_2, n)$. Z lemmatu 1.7 se podívejme na délku l, která bude $\mathrm{lcm}(\frac{m}{\mathrm{GCD}(ib_1,m)}, \frac{n}{\mathrm{GCD}(ib_2,n)})$. Pokud má být délka přímky l menší než délka přímky p, musí alespoň jeden ze zlomků být menší, než kdybychom počítali délku pro p z vektoru (b_1, b_2). Bez újmy na obecnosti nechť $\frac{m}{\mathrm{GCD}(ib_1,m)} < \frac{m}{\mathrm{GCD}(b_1,m)}$. Potom $\mathrm{GCD}(ib_1, m) > \mathrm{GCD}(b_1, m)$. Tedy $g := \mathrm{GCD}(i, m) \neq 1$. Protože m,n mají stejná prvočísla ve svém prvočíselném rozkladu, $h := \mathrm{GCD}(i, n) \neq 1$. Položme $v := \mathrm{GCD}(g,h)$. Potom (a_1, a_2) můžeme napsat jako $(v(\frac{ib_1}{v} - \frac{\alpha_1 m}{v}), v(\frac{ib_2}{v} - \frac{\alpha_2 n}{v}))$. To ale znamená, že $\mathrm{GCD}(a_1,a_2) \neq 1$, což je spor. □

Na závěr této části ještě podle článku Misiaka a kol.[2] zmíníme, jak pro tři body na toru $T_{m\times n}$ určit, zda leží na jedné přímce.

V $\mathbb{Z}^2$ takovou úlohu vyřešíme následovně. Mějme A,B,$C \in \mathbb{Z}^2$; $A = (a_1,a_2)$, $B = (b_1, b_2), C = (c_1, c_2)$. Potom definujme $D(A,B,C)$ jako determinant

$$\begin{vmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ 1 & 1 & 1 \end{vmatrix}$$

Body si tedy zobrazíme do $\mathbb{Z}^3$ tak, že všechny leží v rovině ρ, která má třetí souřadnici 1. Body pak budou ležet na jedné přímce právě tehdy, když leží na jedné rovině, která prochází počátkem (taková rovina má s rovinou ρ jako průnik právě přímku), což je ekvivalentní s tím, že $D(A,B,C) = 0$. Jak již bylo výše uvedeno, přímka na toru mezi body A,B je obrazem přímek ze $\mathbb{Z}^2$ mezi body $(a_1 + \alpha_1 m, a_2 + \alpha_2 n)$ a $(b_1 + \beta_1 m, b_2 + \beta_2 n)$. Z toho nám plyne následující lemma.

Lemma 1.9. *Mějme torus $T_{m\times n}$ pro m,$n \in \mathbb{N}$ a na něm tři body A,B,C. Tyto body leží na jedné přímce právě tehdy, když existují $\alpha_1, \alpha_2, \beta_1, \beta_2, \gamma_1, \gamma_2 \in \mathbb{Z}$ taková, že $D((a_1 + \alpha_1 m, a_2 + \alpha_2 n), (b_1 + \beta_1 m, b_2 + \beta_2 n), (c_1 + \gamma_1 m, c_2 + \gamma_2 n)) = 0$.*

Někdy nám bude stačit jednodušší lemma, které však dává jen jednu implikaci.

Lemma 1.10 (viz [2]). *Mějme torus $T_{m\times n}$ pro $m,n \in \mathbb{N}$. Jestliže body $A,B,C \in T_{m\times n}$ leží na jedné přímce, potom $D(A,B,C) = 0 \pmod{\mathrm{GCD}(m,n)}$.*

Důkaz. Pro úplnost si uvedeme i důkaz. Rozepisování determinantu pak uvidíme i v dalších tvrzeních. Z lemmatu 1.9 dostáváme

$$\begin{aligned} 0 &= D((a_1+\alpha_1 m, a_2+\alpha_2 n),(b_1+\beta_1 m, b_2+\beta_2 n),(c_1+\gamma_1 m, c_2+\gamma_2 n)) = \\ &= D(A,B,C) + nD((a_1,\alpha 2),(b_1,\beta_2),(c_1,\gamma_2)) + mD((\alpha_1,a_2),(\beta_1,b_2),(\gamma_1,b_2)) + \\ &+ mnD((\alpha_1,\alpha_2),(\beta_1,\beta_2),(\delta_1,\delta 2)) \end{aligned}$$

pro vhodná $\alpha_1,\alpha_2,\beta_1,\beta_2,\gamma_1,\gamma_2 \in \mathbb{Z}$. Aby tento výraz byl nulový, musí jít z $D(A,B,C)$ určitě vytknout $\mathrm{GCD}(m,n)$. □

V praxi budeme používat obměnu tohoto lemmatu. Pokud tedy zjistíme, že $D(A,B,C)$ je nenulový, tyto tři body jistě neleží na jedné přímce.

2. Převádění

V této části se podívejme, pro jaké rozměry torů můžeme jistě říct, že mají stejnou hodnotu τ. Na začátku uveďme lemma, které nám na to dá podmínky.

Lemma 2.1 (viz [2]). *Mějme tory $V = T_{xm\times yn}$ a $M = T_{m\times n}$, kde $m, n, x, y \in \mathbb{N}$ a zobrazení $f : V \to M$ definované jako $f((a_1,a_2)) = (a_1 \pmod m, a_2 \pmod n)$. Potom platí:*

1. *Pokud obraz každé přímky na V je přímka na M, pak $\tau(V) \geq \tau(M)$.*
2. *Pokud vzor každé přímky na M je přímka na V, tak $\tau(V) \leq \tau(M)$.*

Důkaz.

1. Mějme největší množinu z M takovou, že žádné tři její body neleží na stejné přímce. Požadavek, aby žádné tři body nebyly kolineární, bude tato množina splňovat i v toru V, protože kdyby ve V nějakými třemi body z této množiny šla proložit přímka, tak tato přímka má obraz v M, tedy i v M by šlo těmito třemi body proložit přímku, což z předpokladu nelze. Tedy $\tau(V) \geq \tau(M)$.
2. Nechť X je největší množina v toru V taková, že žádné tři body neleží na stejné přímce. Nechť X_o je obraz X v toru M. Teoreticky by se mohlo stát, že se nějaké tři body z V zobrazí do M na společnou přímku. To ale nenastane, protože vzor této přímky je přímka ve V, tudíž by body ležely na stejné přímce i ve V. Dále by se mohlo stát, že nějaké dva body a,b z X se do X_o zobrazí na jeden bod c. Nechť $d \in X_o$ a $d \neq c$. Vzor přímky cd je přímka ve V, na které leží $a, b \in X$ a nějaký vzor bodu d, který patří do množiny X. Tedy 3 body z množiny X by ležely na stejné přímce, což je spor s definicí X. Dostáváme tudíž, že $|X| = |X_o|$ a žádné tři body z X_o neleží na stejné přímce. Z toho plyne, že $\tau(V) \leq \tau(M)$.

□

Podmínka 1 v lemmatu je zřejmě splněna, z čehož nám plyne následující důsledek.

Důsledek 2.2 (viz [2]). *Buďte $m, n, x, y \in \mathbb{N}$. Potom $\tau(T_{xm\times yn}) \geq \tau(T_{m\times n})$.*

Lemma 2.3. *Mějme $x, y, m, n \in \mathbb{N}$ taková, že* GCD(x,y) = 1, GCD(m,y) = 1 *a* GCD(n,x) = 1. *Nechť $T_{xm\times yn}$ a $T_{m\times n}$ jsou tory.*
Uvažujme standardní zobrazení (definované v lemmatu 2.1) z toru $T_{xm\times yn}$ do $T_{m\times n}$. Potom vzor každé přímky na $T_{m\times n}$ je přímka na $T_{xm\times yn}$.

Důkaz. Označme $M = T_{m\times n}$ a $V = T_{xm\times yn}$. Stačí dokázat, že vzor každé přímky na M, která prochází bodem $(0, 0)$ je přímka na V, protože ostatní přímky jsou jen posunutí těchto přímek.

Uvažume tedy přímky r, které prochází 0. Budou ve tvaru $r = \{k(\alpha, \beta); k \in \mathbb{Z}\}$, kde GCD$(\alpha, \beta) = 1$. Nejprve definujeme čísla $\gamma, \delta \in \mathbb{N}$ tak, aby platilo

$$\gamma \equiv \alpha \pmod m \tag{2.1}$$
$$\delta \equiv \beta \pmod n. \tag{2.2}$$

Pro další výpočty budeme potřebovat, aby γ a δ byly ve vhodném tvaru, který dále vytvoříme. V každém případě musí být $\gamma = \alpha + km$ a $\delta = \beta + ln$, pro nějaká k,$l \in \mathbb{N}_0$. Položme $A := \mathrm{GCD}(\alpha, m)$ a $B := \mathrm{GCD}(\beta, n)$. Dostáváme

$$\gamma = A(\frac{\alpha}{A} + k\frac{m}{A})$$
$$\delta = B(\frac{\beta}{B} + l\frac{n}{B}).$$

Jelikož $\frac{\alpha}{A}$ a $\frac{m}{A}$ jsou nesoudělná, můžeme využít Dirichletovu větu(1.5), která nám dá nějaké prvočíslo P_1 větší než $mnxy$ ve tvaru $P_1 = \frac{\alpha}{A} + h\frac{m}{A}$ pro vhodné h. Podobně získáme prvočíslo $P_2 \neq P_1$ větší než $mnxy$ ve tvaru $P_2 = \frac{\beta}{B} + g\frac{n}{B}$, protože $\frac{\beta}{B}$ a $\frac{n}{B}$, jsou taktéž nesoudělná. Dostaneme tedy čísla γ,δ ve tvaru nutném pro další výpočty:

$$\gamma = P_1 A \tag{2.3}$$
$$\delta = P_2 B. \tag{2.4}$$

Zároveň je splněno (2.1) a (2.2). Nyní definujme přímku $R = \{k(\gamma, \delta); k \in \mathbb{Z}\}$ na toru V. Ukážeme, že tato přímka je právě vzor přímky r. Z definice γ, δ je zřejmě obraz přímky R přímka r. Nechť (a_1, a_2) je z obrazu přímky r. Uvažme rovnice

$$i \equiv \delta a_1 \pmod{\delta x m} \tag{2.5}$$
$$i \equiv \gamma a_2 \pmod{\gamma y n}. \tag{2.6}$$

Nejprve předpokládejme, že $\delta a_1 \equiv \gamma a_2 \pmod{\mathrm{GCD}(\delta x m, \gamma y n)}$ (že to platí, nahlédneme později). Pak nám čínská zbytková věta(1.4) dá existenci řešení těchto rovnic. Z definice A a B platí, že $A \mid \alpha$ a $B \mid \beta$. Jelikož $\mathrm{GCD}(\alpha, \beta) = 1$ dostaneme, že $\mathrm{GCD}(\gamma, \delta) = 1$. Proto $i = \gamma\delta k$ pro nějaké vhodné $k \in \mathbb{Z}$ (díky (2.5) a (2.6)). Úpravou dostaneme

$$\gamma k \equiv a_1 \pmod{xm}$$
$$\delta k \equiv a_2 \pmod{yn}$$

pro vhodné $k \in \mathbb{Z}$. Zbývá dokázat, že $\delta a_1 \equiv \gamma a_2 \pmod{\mathrm{GCD}(\delta x m, \gamma y n)}$. Protože (a_1, a_2) je vzor přímky r, platí

$$a_1 \equiv \alpha j \pmod{m}$$
$$a_2 \equiv \beta j \pmod{n}$$

pro nějaké $j \in \mathbb{N}_0$. Postupnou úpravou (z definice γ, δ) získáme

$$a_1 = \gamma j \pmod{m}$$
$$a_2 = \delta j \pmod{n}$$
$$\delta a_1 = \delta\gamma j \pmod{\delta m}$$
$$\gamma a_2 = \delta\gamma j \pmod{\gamma n}.$$

Tudíž $\delta a_1 \equiv \gamma a_2 \pmod{\mathrm{GCD}(\delta m, \gamma n)}$. Můžeme upravit s využitím předpokladů a (2.3), (2.4):

$$\begin{aligned}\mathrm{GCD}(\delta m, \gamma n) &= \mathrm{GCD}(P_2 B m, P_1 A n) = \mathrm{GCD}(AB\frac{m}{A}, AB\frac{n}{B}) = \\ &= \mathrm{GCD}(x\frac{m}{A}, y\frac{n}{B})AB = \mathrm{GCD}(P_2 B x A\frac{m}{A}, P_1 A y B\frac{n}{B}) = \\ &= \mathrm{GCD}(\delta x m, \gamma y n),\end{aligned}$$

čímž je důkaz hotový. □

Věta 2.4. *Mějme* $x, y, m, n \in \mathbb{N}$ *taková, že* GCD(x,y) = 1, GCD(m,y) = 1 *a* GCD(n,x) = 1. *Potom* $\tau(T_{xm\times yn}) = \tau(T_{m\times n})$.

Důkaz. Jednu nerovnost máme z 2.2, druhá nerovnost plyne z 2.1 a 2.3. □

Poznámka 2.5. Když se na tory díváme jako na grupy $\mathbb{Z}_c \times \mathbb{Z}_d$, tak vidíme, že vzor přímky $l = \{(0,k); k \in \{0, \ldots, n-1\}\}$ z toru $T_{m\times n}$ na toru $T_{xm\times yn}$ je podgrupa $m\mathbb{Z}_{xm}\times\mathbb{Z}_{yn}$. Aby vzor byl přímkou, musí být tato podgrupa cyklická. $m\mathbb{Z}_{xm}$ je izomorfní s $\mathbb{Z}_x$, tedy $m\mathbb{Z}_{xm}\times\mathbb{Z}_{yn} \cong \mathbb{Z}_x\times\mathbb{Z}_{yn}$, která je z čínské zbytkové věty (1.3) a např. věty 1.7 izomorfní se $\mathbb{Z}_{xyn}$, a tedy cyklická právě, když GCD(x,y) = 1 a GCD(n,x) = 1. Analogicky pro přímku $l = \{(k,0); k \in \{0, \ldots, m-1\}\}$ dostáváme převoditelnost právě, když GCD(x,y) = 1 a GCD(m, y). Díky čemuž dostáváme v lemmatu 2.3 ekvivalenci.

3. Odhady

3.1 Horní odhady

V této části se podíváme na horní odhady pro různé případy. Nejprve se podívejme na horní odhad z článku Misiaka a kol.[2], který platí pro libovolný torus.

Věta 3.1 (viz [2]). *Nechť $T_{m\times n}$, kde $m,n \in \mathbb{N}$, je torus. Potom $\tau(T_{m\times n}) \leq 2\,\mathrm{GCD}(m,n)$.*

Důkaz. Pro úplnost uvedeme i důkaz podle článku. Podívejme se na skupinu přímek $\mathbb{L} = \{l_s; s \in \{0,1,\ldots,\mathrm{GCD}(m,n)-1\}$, kde $l_s = \{(k,k-s); k \in \mathbb{Z}\}$. Přímek ve skupině je $\mathrm{GCD}(m,n)$. Dále nahlédneme, že každý bod z toru leží na právě jedné přímce ze skupiny $\mathbb{L}$.

Mějme tedy libovolný bod $(x,y) \in T_{m\times n}$. Definujme $d = x - y$. Potom dle čínské zbytkové věty(1.4) existuje $k \in \mathbb{Z}$, pro které platí

$$\begin{aligned} k &\equiv x \pmod m \\ k &\equiv y + d \pmod n, \end{aligned}$$

protože $x = y + d$. Z toho hned vidíme, že bod (x,y) leží na přímce l_d.

Nyní je třeba ověřit jednoznačnost. Pro spor předpokládejme, že existují $s_1, s_2 \in \{0,1,\ldots,\mathrm{GCD}(m,n)-1\}$ taková, že bod (x,y) leží na přímce l_{s_1} i l_{s_2}. To znamená, že existují k_1, k_2 taková, že $k_1 \equiv k_2 \pmod a$ a $k_1 - s_1 \equiv k_2 - s_2 \pmod b$. Po úpravě dostaneme, že soustava

$$\begin{aligned} k_1 - k_2 &\equiv 0 \pmod m \\ k_1 - k_2 &\equiv s_1 - s_2 \pmod n \end{aligned}$$

má řešení. To ale z čínské zbytkové věty(1.4) znamená, že také $0 \equiv s_1 - s_2 \pmod{\mathrm{GCD}(m,n)}$, a tedy i $s_1 = s_2$. Tzn., že přímky ze skupiny $\mathbb{L}$ jsou disjunktní a pokrývají celý torus.

Zbývá si uvědomit, že pokud chceme na torus $T_{m\times n}$ umístit množinu bodů tak, aby žádné tři body neležely na jedné přímce, mohou být na každé přímce ze skupiny $\mathbb{L}$ nejvýše dva body. Tudíž $\tau(T_{m\times n}) \leq 2\mathrm{GCD}(m,n)$. □

Z výsledků, pro malé hodnoty m, n (viz [1]) je vidět, že tento odhad je pro mnohé případy nadsazený. Zkusme se podívat, jestli pro nějaké případy nejde vylepšit. Konkrétně nás budou zajímat případy $T_{p^a\times p^a}$, kde p je prvočíslo, $a \in \mathbb{N}$. Nejprve ale budeme potřebovat pomocná tvrzení, která v této části využijeme.

Lemma 3.2. *Mějme torus $T_{m\times m}$, kde $m \in \mathbb{N}$. Potom všechny přímky na toru mají stejnou délku, která je rovna m.*

Důkaz. Máme danou libovolnou přímku. Nechť $(v_1,v_2) \in T_{m\times m}$ je vektor, který ji generuje. Označme $g_1 = \mathrm{GCD}(m,v_1)$ a $g_2 = \mathrm{GCD}(m,v_2)$. Dle lemmatu 1.7 spočteme délku d přímky jako $d = \mathrm{lcm}(\frac{m}{g_1}, \frac{m}{g_2})$. Protože $\mathrm{GCD}(v_1,v_2) = 1$, nemají g_1 a g_2 žádné společné prvočíslo v prvočíselném rozkladu. Tudíž $d = m$. □

Lemma 3.3. *Mějme torus $T_{p^a \times p^b}$, kde p je prvočíslo, a,b $\in \mathbb{N}$, $a \leq b$. Mějme bod $(x,y) \in T_{p^a \times p^b}$. Nechť $g := \mathrm{GCD}(x, y)$. Pokud $\mathrm{GCD}(g, p) = 1$, pak mezi počátkem a bodem (x,y) leží právě jedna přímka.*

Důkaz. Jistě přímka, která prochází bodem $(\frac{x}{g}, \frac{y}{g})$, prochází i bodem (x, y). Naopak pokud máme přímku generovanou $(v_1, v_2) \in T_{p^a \times p^b}$, která prochází (x, y), platí pro nějaké $k \in \mathbb{Z}$

$$\begin{aligned} kv_1 &\equiv x \pmod{p^a} \\ kv_2 &\equiv y \pmod{p^b}. \end{aligned}$$

Protože $\mathrm{GCD}(g, p) = 1$, má g inverzní prvek modulo p^b. Označme ho g^{-1}. Potom platí

$$\begin{aligned} g^{-1}kv_1 &\equiv \frac{x}{g} \pmod{p^a} \\ g^{-1}kv_2 &\equiv \frac{y}{g} \pmod{p^b}. \end{aligned}$$

Tudíž přímka prochází bodem (x,y) právě, když prochází bodem $(\frac{x}{g}, \frac{y}{g})$. Z lemmatu 1.8 víme, že bodem $(\frac{x}{g}, \frac{y}{g})$ prochází právě jedna přímka. □

Následující lemma už nám dá nahlédnout, jakým způsobem budeme horní odhad konstruovat.

Lemma 3.4. *Libovolným bodem toru $T_{p^a \times p^a}$, kde p je prvočíslo, $a \in \mathbb{N}$, prochází právě $p^{a-1}(p + 1)$ přímek.*

Důkaz. Stačí se podívat na přímky, které procházejí počátkem. Pro ostatní body je jen posuneme. Nejprve definujme množiny bodů, které budou sloužit jako vektory generující přímky:

$$\begin{aligned} X &= \{(1, pk); k \in \{0, \ldots, 2^{a-1} - 1\}\} \\ Y &= \{(k, 1); k \in \{0, \ldots, 2^a - 1\}\}. \end{aligned}$$

Nyní jako hledané přímky vezmeme ty, které jsou určeny vektory z $X \cup Y$ a které procházejí počátkem. To znamená přímky ve tvaru $\{iv; i \in \mathbb{Z}\}$ pro $v \in X \cup Y$. Je potřeba ověřit, že jsou to všechny přímky, které počátkem procházejí.

Nechť tedy $(a_1, a_2) \in T_{p^a \times p^a}$ je vektor, který generuje přímku procházející počátkem. Připomeňme, že předpokládáme $\mathrm{GCD}(a_1, a_2) = 1$. Musíme ověřit, že existuje vektor b z množiny $X \cup Y$, který generuje přímku, na které leží (a_1, a_2). Rozlišíme dva případy:

1. $\mathrm{GCD}(a_2, p) = 1$.
   V takovém případě vezmeme vektor z množiny Y ve tvaru $(k,1)$. Budeme ho násobit číslem a_2, aby nám jeho $a_2$násobek dal (a_1, a_2). Zbývá ověřit, jestli existuje takové k, pro které to bude platit. Dostáváme rovnici $a_2k \equiv a_1 \pmod{p^a}$. Využijeme předpokladu, který nám zaručuje, že a_2 je invertibilní modulo p^a. Po úpravě získáme $a_2^{-1}a_2k \equiv k \equiv a_2^{-1}a^1 \pmod{p^a}$. Tím získáme vhodné k, a tedy hledaný vektor, který generuje přímku, na které leží (a_1, a_2).

2. GCD$(a_2, p) = p$ a zároveň $(a_1, p) = 1$.
   Teď budeme hledat naopak vektor z množiny X. To vede na rovnici $a_1 pk \equiv a_2 \pmod{p^a}$. Prvek a_1 je z předpokladu invertibilní modulo p^a, tudíž jím můžeme rovnici vydělit. Zároveň a_2 je násobek p, tudíž můžeme rovnici vydělit i p. Dostáváme $k \equiv a_1^{-1} \frac{a_2}{p} \pmod{p^{a-1}}$.

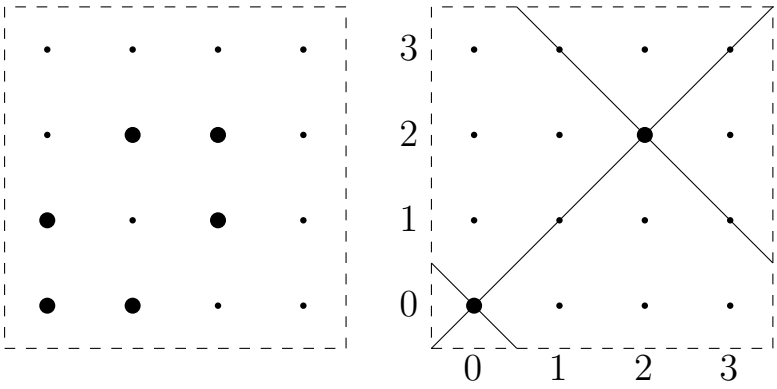
Jiný případ nenastane, protože a_1, a_2 jsou nesoudělná. Pro (a_1, a_2) jsme našli přímku, která jím prochází, je generovaná vektorem z $X \cup Y$ a která nutně musí být přímkou generovanou (a_1, a_2), jelikož z 1.8 existuje mezi (a_1, a_2) a počátkem pouze jedna přímka. Nakonec $|X \cup Y| = p^{a-1}(p+1)$. □

Z tohoto lemmatu nám přímo plyne horní odhad.

Věta 3.5. *Buď p prvočíslo a $a \in \mathbb{N}$. Potom $\tau(T_{p^a \times p^a}) \leq p^{a-1}(p+1) + 1$.*

Důkaz. Mějme nějakou maximální množinu na $T_{p^a \times p^a}$ bez trojic bodů na jedné přímce. Vezměme libovolný bod z této množiny. Potom díky lemmatu 3.4 tímto bodem prochází $p^{a-1}(p+1)$ přímek a na každé z nich může být nejvýše jeden další bod. □

Příklad 3.6. Podívejme se na případ, kdy $p = a = 2$. Tedy mějme torus $T_{4\times4}$.



Na levém obrázku máme umístěných 6 bodů, u kterých snadno ověříme (stačí dle 1.10), že žádné tři neleží na jedné přímce. Tudíž $\tau(T_{4\times4}) \geq 6$. Horní odhad z předchozí věty je 7. Na pravém obrázku vidíme, že mezi body (0,0) a (2,2) leží 2 přímky. To znamená, že umístění bodu (2,2) na torus nám zablokuje dvě přímky procházející počátkem. Z toho plyne, že aby τ mohlo nabývat horního odhadu, nesmíme na torus umístit dva body, mezi kterými jsou dvě přímky. To se nám ale nepodaří. Dostáváme, že $\tau(T_{4\times4}) = 6$.

Zkusme nyní využít podobnou argumentaci obecněji ke zlepšení horních odhadů pro $a > 1$.

Definice 3.7. Mějme torus $T_{p^a \times p^a}$, kde p je prvočíslo. Dále mějme $b \leq a$. Definujme ekvivalenci R_b pro prvky toru následovně. $(k,l) R_b (m,n)$ právě, když $k \equiv m \pmod{p^b}$ a $l \equiv n \pmod{p^b}$. Že se jedná o ekvivalenci je zřejmé.

Lemma 3.8. *Mějme torus $T_{p^a \times p^a}$, kde p je prvočíslo, $b \leq a$. Dále mějme ekvivalenci R_b. Potom mezi každými dvěma body z jedné třídy této ekvivalence leží alespoň p^b přímek.*

Důkaz. Bez újmy na obecnosti uvažujme třídu ekvivalence $[(0,0)]_{R_b}$. Budeme postupovat indukcí dle b. Začneme pro $b = a$ (což je nejjednodušší případ), poté pro $b < a$ budeme předpokládat, že tvrzení platí pro všechna větší b.

Pokud tedy $b = a$, tvrzení triviálně platí, protože každý bod na toru je samostatná třída.

Mějme tedy $b < a$. Podívejme se, kolik přímek leží mezi mezi libovolnými dvěma body třídy $[(0,0)]_{R_b}$. Opět bez újmy na obecnosti předpokládejme, že jeden z těchto bodů je počátek, protože nám půjde jen o vektory generující přímky. Uvažujme tedy body (0,0) a $(\alpha p^b, \beta p^b)$, kde $\alpha, \beta \in \{0, 1, \ldots, p^{a-b} - 1\}$ a nejsou obě nulová. Rozlišíme případy:

1. $p \nmid \alpha$
   Pro α tudíž existuje inverzní prvek α^{-1}v $\mathbb{Z}_{p^a}$. Uvažujme vektory $(1, \alpha^{-1}(\beta + lp^{a-b}))$, kde $l \in \{0, \ldots, p^b - 1\}$. Je jich p^b, každý má stejnou první souřadnici, tudíž budou generovat p^b různých přímek, protože všechny přímky na toru mají velikost p^a (lemma 3.2). Zároveň pro αp^bnásobek tohoto vektoru platí

   $$\begin{aligned} 1\alpha p^b &\equiv \alpha p^b \pmod{p^a} \\ \alpha\alpha^{-1} p^b(\beta + lp^{a-b})) &\equiv \beta p^b \pmod{p^a}. \end{aligned}$$

   To znamená, že přímka procházející počátkem, která je generována tímto vektorem, také prochází bodem $(\alpha p^b, \beta p^b)$.

2. $p \nmid \beta$
   Rozebere se analogicky pro vektory ve tvaru $(\beta^{-1}(\alpha + lp^{a-b}), 1)$, kde $l \in \{0, \ldots, p^b - 1\}$.

3. $p \mid \alpha$ a zároveň $p \mid \beta$
   V tomto případě bude bod $(\alpha p^b, \beta p^b)$ spolu s počátkem zároveň v ekvivalenční třídě pro větší b. Z indukčního předpokladu je tudíž mezi ním a počátkem více než p^b přímek.

□

Poznámka 3.9. Pro zajímavost se podívejme, že odhad počtu přímek, které procházejí dvěma body ekvivalenční třídy ekvivalence R_b, je těsný. Stejně jako v důkazu předchozího lemmatu (3.8) uvažujme počátek a bod třídy $[(0,0)]_{R_b}$ ve tvaru $(\alpha p^b, \beta p^b)$. Pokud nalezneme přímku, která prochází bodem (x,y), který splňuje rovnice

$$x \equiv \alpha \pmod{p^{a-b}} \tag{3.1}$$

$$y \equiv \beta \pmod{p^{a-b}}, \tag{3.2}$$

bude tato přímka jistě procházet i bodem $(\alpha p^b, \beta p^b)$, protože pro p^bnásobek (x,y) platí

$$\begin{aligned} p^b x &\equiv \alpha p^b \pmod{p^a} \\ p^b y &\equiv \beta p^b \pmod{p^a}. \end{aligned}$$

Naopak uvažujme přímku, která je generovaná vektorem (v_1,v_2) a prochází bodem $(\alpha p^b, \beta p^b)$. Potom pro vhodné $k \in \mathbb{Z}$ platí

$$kv_1 \equiv \alpha p^b \pmod{p^a} \tag{3.3}$$
$$kv_2 \equiv \beta p^b \pmod{p^a}. \tag{3.4}$$

Protože jako vektory generující přímku uvažujeme jen ty, které mají nesoudělné souřadnice, nutně platí, že $p \nmid v_1$ nebo $p \nmid v_2$. Bez újmy na obecnosti $p \nmid v_1$. Z rovnice (3.3) plyne, ze $kv_1 = \alpha p^b + sp^a$ pro vhodné $s \in \mathbb{Z}$. A tudíž $p^b \mid k$. Dostaneme

$$\frac{k}{p^b} v_1 \equiv \alpha \pmod{p^{a-b}}$$
$$\frac{k}{p^b} v_2 \equiv \beta \pmod{p^{a-b}}.$$

Tím jsme ukázali, že přímka procházející prochází bodem $(\alpha p^b, \beta p^b)$ právě, když prochází nějakým bodem (x,y), který splňuje (3.1) a (3.2).

Náš odhad bude těsný v případě, že $p \nmid \alpha$ nebo $p \nmid \beta$. V takovémto případě mezi počátkem a bodem, který splňuje (3.1) a (3.2) prochází právě jedna přímka (lemma 3.3). Bez újmy na obecnosti předpokládejme, že $p \nmid \alpha$. Potom z důkazu lemmatu 3.8 z části 1 máme množinu vektorů ve tvaru $(1, \alpha^{-1}(\beta + lp^{a-b}))$, kde $l \in \{0, \ldots, p^b - 1\}$. Je potřeba ukázat, že pro každý bod, který splňuje (3.1) a (3.2), najdeme přímku, která prochází jím a počátkem a která lze vygenerovat nějakým z těchto vektorů.

Mějme tedy bod $(\alpha + k_1 p^{a-b}, \beta + k_2 p^{a-b})$. Hledáme takově z, že $z(1, \alpha^{-1}(\beta + lp^{a-b})) = (\alpha + k_1 p^{a-b}, \beta + k_2 p^{a-b})$. Je vidět (lemma 3.2), že z musí být $\alpha + k_1 p^{a-b}$. Nyní je třeba ověřit, že najdeme vhodné l. Dostáváme

$$\begin{aligned}
(\alpha + k_1 p^{a-b})(\alpha^{-1}(\beta + lp^{a-b})) &\equiv \beta + k_2 p^{a-b} \pmod{p^a} \\
\beta + lp^{a-b} + k_1 p^{a-b}\alpha^{-1}\beta + k_1\alpha^{-1} l p^{2a-2b} &\equiv \beta + k_2 p^{a-b} \pmod{p^a} \\
l(1 + k_1\alpha^{-1} p^{a-b}) &\equiv k_2 - k_1\alpha^{-1}\beta \pmod{p^b}.
\end{aligned}$$

Výraz $(1 + k_1 \alpha p^{a-b})$ má k sobě jistě inverzní prvek modulo p^b. Proto $l = (1 + k_1\alpha p^{a-b})^{-1}(k_2 - k_1\alpha^{-1}\beta) \pmod{p^b}$.

Poznatku z lemmatu 3.8 využijeme v následujícím tvrzení, kde zlepšíme horní odhad.

Věta 3.10. *Buď $T_{p^a \times p^a}$ torus, kde p je prvočíslo, $a \in \mathbb{N}$. Potom $\tau(T_{p^a \times p^a}) \leq p^a + p^{\lceil \frac{a}{2} \rceil - 1} + 1$.*

Důkaz. Nechť M je množina bodů na $T_{p^a \times p^a}$ taková, že $|M| = \tau(T_{p^a \times p^a})$ a žádné tři body z M neleží na jedné přímce. Budeme předpokládat, že $|M| > p^a$. Pokud tomu tak není, tvrzení platí. Uvažujme ekvivalenci R_1. Počet jejich tříd je p^2, protože zbytků po dělení p je p a my máme dvě souřadnice. Obecně platí, že v rámci libovolné ekvivalenční třídy ekvivalence R_k existuje p^2 ekvivalenčních tříd ekvivalence R_{k+1}, protože čísla se stejným zbytkem po dělení p^k mají p zbytků po dělení p^{k+1}. Uvažujme posloupnost ekvivalenčních tříd $T^{(1)}, T^{(2)}, \ldots, T^{(n)}$ definovanou induktivně následovně:

- $T^{(1)}$ je třída ekvivalence R_1 taková, která obsahuje více než p^{a-2} bodů množiny M. Taková třída jistě bude existovat z Dirichletova principu, protože $|M| > p^a$ a počet tříd je p^2.

- $T^{(k)}$ pro $k \in \{1, \ldots, n\}$ je třída ekvivalence R_k, která je obsažena v $T^{(k-1)}$ a obsahuje více než p^{a-2k} bodů z množiny M. Tento krok můžeme opět díky Dirichletovu principu udělat, jelikož $T^{(k-1)}$ obsahuje více než p^{a-2k+2} bodů a tříd ekvivalence R^k, které jsou v $T^{(k-1)}$ je p^2, jak je uvedeno výše.

Zřejmě n může být nejvýše $\lfloor \frac{a}{2} \rfloor$. Nyní uvažujme bod $c \in M$, který je obsažen ve všech třídách $T^{(1)}, \ldots, T^{(\lfloor \frac{a}{2} \rfloor)}$. Dle lemmatu 3.4 bodem c prochází právě $p^{a-1}(p+1)$ přímek. Na každé takové přímce může ležet nejvýše jeden bod z M (viz větu 3.5). Proto dostáváme horní odhad $p^{a-1}(p+1)+1$. Pokud ovšem nějaký bod z $M \setminus \{c\}$ leží na dalších t přímkách procházejících c, horní odhad se sníží o t a toho využijeme.

Vezmeme si nyní třídu $T^{(1)}$, kde je alespoň p^{a-2} bodů z M vyjma c. Každý z těchto bodů leží na p přímkách, které procházejí bodem c, tedy pro každý takový bod se sníží horní odhad z věty 3.5 o $p-1$. Musíme uvažovat nejhorší případ, tedy započítáme p^{a-2} bodů z této třídy. Nicméně nějakých p^{a-4} bodů vyjma c je také určitě součástí nějaké vyšší třídy. Celkem za tuto třídu tedy snížíme horní odhad o $(p^{a-2} - p^{a-4})(p-1)$.

Obecně pro $T^{(k)}$, kde $k \in \{1, \ldots, \lfloor \frac{a}{2} \rfloor - 1\}$, máme vyjma c dosud nezapočítaných p^{a-2k} bodů z M a p^{a-2k-2} jich započítáme v dalších krocích. Každý z těchto bodů leží na p^k přímkách, které prochází c, tedy za $T^{(k)}$ máme snížený odhad o $(p^{a-2k} - p^{a-2k-2})(p^k - 1)$.

Skončíme ve třídě $T^{(\lfloor \frac{a}{2} \rfloor)}$, kde máme dosud nezapočítaných $p^{a-2\lfloor \frac{a}{2} \rfloor}$ bodů z M vyjma c. Zároveň z nich žádné už nezapočítáme v dalších krocích a každý z těchto bodů leží na $p^{\lfloor \frac{a}{2} \rfloor}$ přímkách, které prochází bodem c. Odhad se tedy sníží za tyto body o $(p^{a-2\lfloor \frac{a}{2} \rfloor})(p^{\lfloor \frac{a}{2} \rfloor} - 1)$.

Celkem se tedy odhad sníží o

$$(p^{a-2\lfloor \frac{a}{2} \rfloor})(p^{\lfloor \frac{a}{2} \rfloor} - 1) + \sum_{k=1}^{\lfloor \frac{a}{2} \rfloor - 1} (p^{a-2k} - p^{2k-2})(p^k - 1) =$$

$$= (p^{a-2\lfloor \frac{a}{2} \rfloor})(p^{\lfloor \frac{a}{2} \rfloor} - 1) + \sum_{k=1}^{\lfloor \frac{a}{2} \rfloor - 1} p^{a-k} - \sum_{k=1}^{\lfloor \frac{a}{2} \rfloor - 1} p^{a-k-2} + \sum_{k=1}^{\lfloor \frac{a}{2} \rfloor - 1} p^{a-2k-2} - \sum_{k=1}^{\lfloor \frac{a}{2} \rfloor - 1} p^{a-2k} =$$

$$= (p^{a-2\lfloor \frac{a}{2} \rfloor})(p^{\lfloor \frac{a}{2} \rfloor} - 1) + \sum_{k=1}^{\lfloor \frac{a}{2} \rfloor - 1} p^{a-k} - \sum_{k=3}^{\lfloor \frac{a}{2} \rfloor + 1} p^{a-k} + \sum_{k=2}^{\lfloor \frac{a}{2} \rfloor} p^{a-2k} - \sum_{k=1}^{\lfloor \frac{a}{2} \rfloor - 1} p^{a-2k} =$$

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

$$= p^{a-1} - p^{a-\lfloor \frac{a}{2} \rfloor - 1} = p^{a-1} - p^{\lceil \frac{a}{2} \rceil - 1}.$$

Tudíž $\tau(T_{p^a \times p^a}) \leq p^a + p^{a-1} + 1 - (p^{a-1} - p^{\lceil \frac{a}{2} \rceil - 1}) = p^a + p^{\lceil \frac{a}{2} \rceil - 1} + 1$. □

Bohužel se ale zdá, že odhad je těsný jen pro $p = 2, a = 2$.

V případě, že $a = 1$, tzn. $T_{p \times p}$, bude mezi každými dvěma body ležet pouze jedna přímka (lemma 1.8), tedy nemůžeme použít argument s třídami. Nicméně pokud $p \neq 2$, můžeme vylepšit odhad o 1 jiným argumentem z článku Misiaka a kol.[2], který si teď ukážeme.

Věta 3.11 (viz [2]). *Buď p liché prvočíslo. Potom $\tau(T_{p\times p}) \leq p+1$.*

Důkaz. Pro spor předpokládejme, že lze umístit $p+2$ bodů, tj. předchozí horní odhad (věta 3.5). Označme si množinu těchto bodů M. Z důkazu věty 3.5 víme, že když si zvolíme libovolný bod z M, musí na každé přímce, která jím prochází, ležet nějaký další bod z M. Z toho dostáváme, že každá přímka na toru buď neobsahuje žádný bod, nebo obsahuje dva body z M. Kdyby obsahovala jen jeden, tak by tímto bodem procházela přímka, na které by neležel jiný bod z M.
Vezměme si libovolný bod, který nepatří do M. Potom každá přímka, která prochází tímto bodem obsahuje buď žádný bod, nebo dva body z M. Zároveň tímto bodem a libovolným bodem z M prochází jen jedna přímka. Z toho vyplývá, že M má sudou velikost, což je spor. □

Zkusme se nyní podívat, jestli podobně jako ve větě 3.10 nemůžeme postupovat pro případ $T_{pq\times pq}$, kde p,q jsou různá prvočísla. Uvidíme, že pro tento případ získáme také lepší horní odhad, který je závislý na tom, jak jsou od sebe p, q vzdálená. Nejprve se podívejme, kolik přímek prochází libovolným bodem na $T_{pq\times pq}$.

Lemma 3.12. *Mějme $T_{pq\times pq}$, kde p, q jsou různá prvočísla. Pak libovolným bodem toru prochází $pq+p+q+1$ přímek.*

Důkaz. Důkaz bude v podstatě stejný jako u 3.4. Budeme muset ale rozlišit více případů. Definujme tedy množiny vektorů, které nám budou hledané přímky generovat.

$$\begin{aligned} A &= \{(1,k); k \in \{0,1,\dots pq-1\}\} \\ B &= \{(kp,1); k \in \{0,1,\dots q-1\}\} \\ C &= \{(kq,1); k \in \{0,1,\dots p-1\}\} \\ D &= \{(p,q),(q,p)\} \end{aligned}$$

Mějme přímku, která prochází počátkem a je generovaná vektorem (a_1, a_2). Argumenty důkazu jsou stejné jako u 3.4. Pouze rozebereme jednotlivé případy:

1. $\mathrm{GCD}(a_1, p) = 1$ a zároveň $\mathrm{GCD}((a_1, q) = 1$.
   Jelikož a_1 má inverzní prvek, použijeme přímku generovanou vektorem z A pro $k = a_1^{-1}a_2$. Dostaneme, že $a_1(1, a_1^{-1}a_2) \equiv (a_1, a_2)$.

2. $\mathrm{GCD}(a_1, p) \neq 1$ a zároveň $\mathrm{GCD}(a_2, q) = 1$.
   Buď a_2^{-1} inverzní prvek k a_2 v $\mathbb{Z}_q$. Použijeme vektor z množiny B pro $k = \frac{a_1}{p}a_2^{-1} \pmod q$. Když bod vynásobíme a_2, v druhé souřadnici dostaneme a_2. V první souřadnici dostáváme

   $$kpa_2 \equiv \frac{a_1}{p}pa_2^{-1}a_2 \equiv a_1 \pmod{pq},$$

   protože $k \equiv \frac{a_1}{p}a_2^{-1} \pmod q$, a tedy $ka_2 \equiv \frac{a_1}{p} \pmod q$.

3. $\mathrm{GCD}(a_1, q) \neq 1$ a zároveň $\mathrm{GCD}(a_2, p) = 1$.
   Analogicky jako předchozí případ. Použije se vektor z množiny C.

4. $\mathrm{GCD}(a_1, p) \neq 1$ a zároveň $\mathrm{GCD}(a_2, q) \neq 1$. V tomto případě $(a_1,a_2) = (\gamma p, \delta q)$, kde $\gamma \in \{0,1,\ldots,q-1\}, \beta \in \{0,1,\ldots,p-1\}$. Příslušnou přímku nám zde vygeneruje vektor $(p, q) \in D$. Vynásobíme ho číslem h. Ověříme, že takové h existuje:

$$\begin{aligned} hp &\equiv \gamma p \pmod{pq} \\ hq &\equiv \delta q \pmod{pq}. \end{aligned}$$

   Po úpravě:

$$\begin{aligned} h &\equiv \gamma \pmod{q} \\ h &\equiv \delta \pmod{p}. \end{aligned}$$

   Protože $\mathrm{GCD}(p, q) = 1$, čínská zbytková věta (1.3) nám dává existenci h.

5. $\mathrm{GCD}(a_1, q) \neq 1 \wedge \mathrm{GCD}(a_2, p) \neq 1$. Analogicky pro vektor $(q, p) \in D$

Případy $\mathrm{GCD}(a_1, q) \neq 1$ a zároveň $\mathrm{GCD}(a_1, p) \neq 1$, $\mathrm{GCD}(a_2, q) \neq 1$ a zároveň $\mathrm{GCD}(a_2, p) \neq 1$ z principu nemohou nastat. Nakonec $|A \cup B \cup C \cup D| = pq+p+q+1$, protože $B \cap C = \{(0,1)\}$. □

Podobně jako v případě pro $T_{p^a \times p^a}$ (3.7) definujme ekvivalenci.

Definice 3.13. Mějme torus $T_{pq\times pq}$, kde p, q jsou různá prvočísla. Definujme ekvivalenci R_p resp. R_q tak, že $(k,l)R_x(m,n)$ právě, když $k \equiv m \pmod{x}$ a zároveň $l \equiv n \pmod{x}$, kde $x \in \{p,q\}$.

Formulujme tvrzení pro třídy ekvivalence.

Lemma 3.14. *Nechť $T_{pq\times pq}$ je torus a p,q jsou různá prvočísla. Dále mějme třídu ekvivalence R_x, kde $x \in \{p,q\}$. Potom mezi každými dvěma body třídy této ekvivalence leží alespoň $x + 1$ přímek.*

Důkaz. Důkaz bude až na jednu výjimku stejný jako v lemmatu 3.8. Budeme bez újmy na obecnosti předpokládat ekvivalenci R_p a třídu $[(0,0)]_{R_p}$. Hledáme tedy přímky mezi počátkem a $(\alpha p, \beta p)$, kde $\alpha, \beta \in \{1 \ldots q-1\}$ a nejsou obě nulová. Nejprve uvažujme, že $\alpha \neq 0$. V takovém případě bude mít α inverzní prvek v $\mathbb{Z}_q$. Označme ho α^{-1}. Tento prvek bude i v $\mathbb{Z}_{pq}$, kde ho budeme značit stejně, nemusí zde ale plnit funkci inverzního prvku k α, obecně bude platit, že $\alpha\alpha^{-1} \equiv 1 + hq \pmod{pq}$ pro vhodné $h \in \mathbb{Z}$.

Podobně jako v lemmatu 3.8 uvažujme množinu vektorů $\mathbb{V} = \{(1, \alpha^{-1}(\beta + lq)); l \in \{0, 1, \ldots, p-1\}\}$. Tyto vektory generují různé přímky. Zároveň pro vhodné $h \in \mathbb{Z}$ platí

$$\begin{aligned} 1\alpha p &\equiv \alpha p \pmod{pq} \\ \alpha p\alpha^{-1}(\beta + lq) \equiv p(1 + hq)(\beta + lq) &\equiv \beta p \pmod{pq}. \end{aligned}$$

To znamená, že přímka generována vektorem z $\mathbb{V}$ prochází bodem $(\alpha p, \beta p)$. Takto jsme získali p přímek.

Zbývá nahlédnout, že ještě existuje alespoň jedna další přímka, která prochází $(\alpha p, \beta p)$ a není generována vektorem z $\mathbb{V}$. Protože p,q jsou různá prvočísla,

GCD(p,q) = 1. Z věty 1.2 můžeme 1 napsat jako lineární kombinaci p,q. To znamená, že jako lineární kombinaci můžeme napsat i číslo α. Existují tedy r,$s \in \mathbb{Z}$ taková, že $\alpha + rq = sp$. Protože $\alpha < q$, s není násobkem q. Z toho dostáváme, že $s \pmod q$ má inverzní prvek modulo q, který označíme s^{-1}. Podívejme se na vektor $w := (p, \beta s^{-1} + vq \pmod{pq})$, kde $v \in \mathbb{Z}$ je zvoleno tak, aby jeho souřadnice byly nesoudělné. Potom přímka generována tímto vektorem jistě neprochází bodem, který má v první souřadnici 1, jelikož p nemá v $\mathbb{Z}_{pq}$ inverzní prvek. Taková přímka tudíž není generována vektorem z $\mathbb{V}$. Zároveň vynásobením w číslem $\alpha + rq = sp$ dostaneme

$$\begin{aligned} p(\alpha + rq) &\equiv p\alpha + rpq \equiv \alpha p \pmod{pq} \\ sp(\beta s^{-1} + vq) &\equiv \beta p(1 + cq) + svpq \equiv \beta p \pmod{pq}, \end{aligned}$$

protože $ss^{-1} \equiv (1 + cq) \pmod{pq}$ pro vhodné $c \in \mathbb{Z}$. Přímka generována w tedy prochází $(\alpha p, \beta p)$. Máme tudíž $p + 1$ přímek mezi počátkem a $(\alpha p, \beta p)$.

Nakonec dodejme, že analogicky se bude postupovat v případě, že $\alpha = 0$. Potom určitě β bude mít inverzní prvek v $\mathbb{Z}_q$. Množina vektorů $\mathbb{V}$ potom bude $\{(\beta^{-1}(\alpha + lq)), 1); l \in \{0, 1, \ldots, p-1\}\}$. Analogicky dostaneme i hledanou přímku, která není generována vektorem z $\mathbb{V}$. □

Věta 3.15. *Mějme torus $T_{pq\times pq}$, kde p,q jsou prvočísla a nechť $kp < q$, kde $k \in \mathbb{N}$. Potom $\tau(T_{pq\times pq}) \leq pq + p + q + 2 - kp$.*

Důkaz. Budeme postupovat podobně jako u věty 3.10. Předpokládejme, že máme množinu bodů M na toru, která splňuje naši podmínku. Zároveň nechť M je co do počtu prvků maximální. Předpokládejme, že $|M|$ je alespoň pq, jinak jsme hotovi. Uvažujme třídy ekvivalence R_p. Je jich p^2. Protože $|M| \geq pq > kp^2$, z Dirichletova principu musí v nějaké třídě být víc než k bodů. V kombinaci s lemmaty 3.12, 3.14 a se stejným argumentem jako v 3.10 dostáváme $\tau(T_{pq\times pq}) \leq pq+p+q+2-kp$. □

3.2 Dolní odhady

V této části se budeme zabývat dolními odhady τ.

Uvažujme konkrétní množiny bodů z článku [2] na toru a to na $T_{p^a \times p^b}$, kde p je prvočíslo, $a, b \in \mathbb{N}$ a $a < b$. My si pomocí nich ukážeme větu z tohoto článku, která nám říká, že $\tau(T_{p\times p^2}) = 2p$. Poté je použijeme ještě k dolním odhadům pro jiné případy.

Definujme $X = \{(i,i^2p); i \in M\}$ a $Y = \{(i,i^2p+1); i \in M\}$, kde $M \subseteq \{0,1\ldots,p^a-1\}$ upřesníme později. Jistě budou tyto dvě množiny disjunktní. Podíváme se, jak můžeme zvolit množinu M pro různé kombinace a a b. Nejprve uvažme, že vezmeme dva body z množiny X a jeden z množiny Y. Tzn. mějme body (k, k^2p), (l, l^2p), (m, m^2p+1) a spočtěme jejich determinant:

$$\begin{aligned} D :&= D((k, k^2p), (l, l^2p),(m, m^2p+1)) = \\ &= kl^2p + k^2mp + lm^2p + l - ml^2p - m^2kp - k - lk^2p = \\ &= (l-k) + p(l-k)(m-k)(m-l) = (l-k)(1+p(m-k)(m-l)). \end{aligned}$$

Jak lze vidět podle lemmatu 1.10, tato kombinace bodů nám výběr množiny M neomezuje, jelikož $(l-k) < p^a$ a $p \nmid (1+p(m-k)(m-l))$. Dostáváme, že $D \not\equiv 0 \pmod{\mathrm{GCD}(p^a, p^b) = p^a}$. Rozklad D ve stejném tvaru dostaneme i pokud jsou dva body z Y a jeden z X.

Nyní se podívejme, co se stane, když budou všechny tři body z množiny X, resp. Y (což je jen posunutá množina X). Zde je třeba počítat pečlivěji pro body obecně v $\mathbb{Z}^2$ dle lemmatu 1.9. Máme $A = (k+\alpha_1 p^a, k^2p+\alpha_2 p^b)$, $B = (l+\beta_1 p^a, k^2p+\beta_2 p^b)$, $C = (m+\gamma_1 p^a, m^2p+\gamma_2 p^b)$ pro $k,l,m \in M$ a $\alpha_1,\alpha_2,\beta_1,\beta_2,\gamma_1,\gamma_2 \in \mathbb{Z}$. Dostaneme

$$\begin{aligned} D(A,B,C) = D((k, k^2p), (l, l^2p), (m, m^2p)) + p^a D((\alpha_1, k^2p), (\beta_1,l^2p), (\gamma_1, m^2p))+ \\ +p^b D((k, \alpha_2), (l, \beta_2), (m, \gamma_2)) + p^{a+b} D((\alpha_1, \alpha_2), (\beta_1, \beta_2), (\gamma_1, \gamma_2)) = \\ = p(l-k)(m-k)(m-l) + p^{a+1}Q, \end{aligned}$$

kde $Q = D((\alpha_1, k^2), (\beta_1,l^2), (\gamma_1, m^2)) + p^{b-a-1} D((k, \alpha_2), (l, \beta_2), (m, \gamma_2)) +$ $+ p^{b-1} D((\alpha_1, \alpha_2), (\beta_1, \beta_2), (\gamma_1, \gamma_2))$. Pokud platí, že $p^a \nmid (l-k)(m-k)(m-l)$, je determinant určitě nenulový. Na základě a lze nyní určit množinu M, resp. její velikost, z čehož dostaneme dolní odhady pro $\tau(T_{p^a\times p^b})$. Je vidět, že stejných výsledků dosáhneme, když definovaná množina bodů bude mít i nějakou mocninu prvočísla v druhé souřadnici.

Věta 3.16 (viz [2])**.** *Pro p prvočíslo $\tau(T_{p\times p^2}) = 2p$.*

Důkaz. Zvolme $M = \{0,\ldots,p-1\}$. Zřejmě pro každá různá $k,l,m \in M$ bude $(l-k),(m-k),(m-l) < p$. Tedy $p \nmid (l-k)(m-k)(m-l)$. Tedy $p = |M| = |X| = |Y|$. Dostáváme $|X \cup Y| = 2p$. V kombinaci s horním odhadem $2p$ (věta 3.1) máme danou rovnost. □

Podívejme se, jak můžeme definovat množinu M, pokud $b = a+1$. Stojí za povšimnutí, že pro $a = 2$ můžeme použít množinu $M = \{0,\ldots,2p-1\}$, což nám dá dolní odhad $\tau(T_{p^2\times p^b}) \leq 4p$. Pokud budeme mít $p = 2$, pak je dolní odhad roven hornímu, tedy $\tau(T_{4\times 8}) = 8$. Pro $a = 3$ nemůžeme použít větší množinu, nicméně pro $a = 4$ už můžeme použít $M = \{0,\ldots,p^2-1\}$. Jde vidět, že možnost, jak zvolit M, bude záviset na hodnotě $z := a \pmod 3$.

Věta 3.17. *Mějme $a, b \in \mathbb{N}$ taková, že $a + 1 = b$, a buď p prvočíslo. Označme $z := a \pmod 3$. Potom platí:*

1. *Pokud $z = 0$, pak $\tau(T_{p^a \times p^b}) \geq 4p^{\frac{a}{3}}$*
2. *Pokud $z = 1$. pak $\tau(T_{p^a \times p^b}) \geq 2p^{\lceil \frac{a}{3} \rceil}$*
3. *Pokud $z = 2$, pak $\tau(T_{p^a \times p^b}) \geq 4p^{\lceil \frac{a}{3} \rceil}$*

Důkaz. Zopakujme z předchozích poznatků, že hledáme množinu M takovou, že pro všechny trojice k, l, $m \in M$; k, l, m jsou navzájem různá, platí $p^a \nmid (l-k)(m-k)(m-l)$. Označme $g_1 := \mathrm{GCD}(p^a, l-k), g_2 := \mathrm{GCD}(p^a, m-k)$ a $g_3 := \mathrm{GCD}(p^a, m-l)$. Jedná se o největší společné dělitele p^a a jednotlivých závorek. Vyjádřeme $(l-k)(m-k)(m-l) = g_1 g_2 g_3 z_1 z_2 z_3$, kde $z_1 = \frac{(l-k)}{g_1}$, $z_2 = \frac{(m-k)}{g_1}$ a $z_3 = \frac{(m-l)}{g_3}$. Platí, že $p \nmid z_i$. Jinak by g_i nebyl největší společný dělitel. Z toho dostáváme, že $p^a | (l-k)(m-k)(m-l)$ právě, když $p^a | g_1 g_2 g_3$.

2. Pokud $z = 1$, můžeme zvolit $M = \{0, \ldots, p^{\lceil \frac{a}{3} \rceil} - 1\}$. Největší společný dělitel p^a a každé závorky bude potom nejvýše $p^{\lfloor \frac{a}{3} \rfloor}$. Tedy $g_1 g_2 g_3 \leq p^{3\lfloor \frac{a}{3} \rfloor} = p^{a-1}$ a $p^a \nmid g_1 g_2 g_3$.

3. Pokud $z = 2$, můžeme množinu M zdvojnásobit. Tedy $M = \{0, \ldots, 2p^{\lceil \frac{a}{3} \rceil} - 1\}$. Vede to k tomu, že nejvýše jeden člen g_i může nabývat $p^{\lceil \frac{a}{3} \rceil}$. Tudíž $g_1 g_2 g_3 \leq p^{\lceil \frac{a}{3} \rceil + 2\lfloor \frac{a}{3} \rfloor} = p^{3\lfloor \frac{a}{3} \rfloor + 1} = p^{a-1}$ díky předpokladu, že $z = 2$.

1. Za předpokladu, že $z = 0$ použijeme stejnou množinu M jako pro $a - 1$. To smíme udělat díky 2.2. Potom $\lceil \frac{a-1}{3} \rceil = \frac{a}{3}$.

Celkový počet umístěných bodů bude potom $2|M|$. □

Přirozeně se nabízí také otázka, jestli pro dostatečně velké b dosáhne někdy $\tau(T_{p^a\times p^b})$ potenciálního maxima, které je z věty 3.1 $2p^a$. Ukážeme si, že tohoto maxima dosáhne a použijeme k tomu opět již zmíněné a používané množiny z článku [2]. Tedy $X = \{(i,i^2p); i \in M\}$ a $Y = \{(i,i^2p+1); i \in M\}$. Nyní se nebudeme snažit mít množinu M co největší. Použijeme $M = \{0,\dots,p-1\}$ jako v případě $T_{p\times p^2}$. Těchto $2p$ bodů budeme ale na torus vhodně kopírovat.

Nejprve je ale třeba zmínit lemma, které budeme používat.

Lemma 3.18. *Mějme torus $T_{p^a\times p^b}$, kde p je prvočíslo, a,$b \in \mathbb{N}$ a na něm body $A = (s_1, s_2)$, $B = (s_1 + kp^{a-1}, s_2)$, $C = (u_1, u_2)$, kde $k \in \{0,\dots,p-1\}$, které splňují následující podmínku. Pro $A - C =: V = (v_1, v_2)$ platí, že $p \nmid \mathrm{GCD}(v_1, v_2)$. Dále nechť A', B', C' jsou obrazy bodů A, B, C při standardním zobrazením f definovaným v lemmatu 2.1 na torus $T_{p^{a-1}\times p^b}$. Předpokládejme ještě, že přímka l mezi body A a C na toru $T_{p^a\times p^b}$ má stejnou velikost jako přímka l' mezi body A' a C' na toru $T_{p^{a-1}\times p^b}$. Potom A,B,C neleží na jedné přímce.*

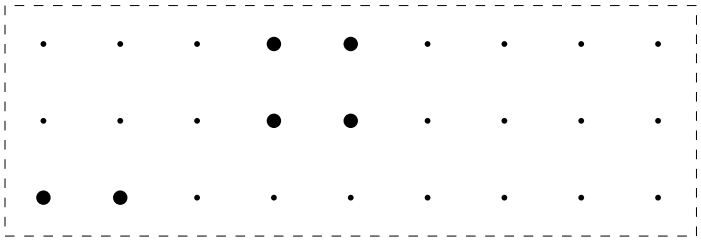
Důkaz. Dle lemmatu 3.3 je mezi A, C na toru $T_{p^a\times p^b}$ právě jedna přímka l. Dle stejného argumentu je mezi A' a C' na toru $T_{p^{a-1}\times p^b}$ také právě jedna přímka l'. Jelikož $A' = f(A)$ a $C' = f(C)$, je $f(l) = l'$. Kdyby na přímce l ležel ještě bod B, pro který platí $f(B) = A'$, tak by se dva body přímky l zobrazily na jeden, tudíž by přímka l nemohla mít stejnou délku jako l'. □

Věta 3.19. *$\tau(T_{p^a\times p^{(a-1)p+2}}) = 2p^a$ pro $a \in N$ a p prvočíslo.*

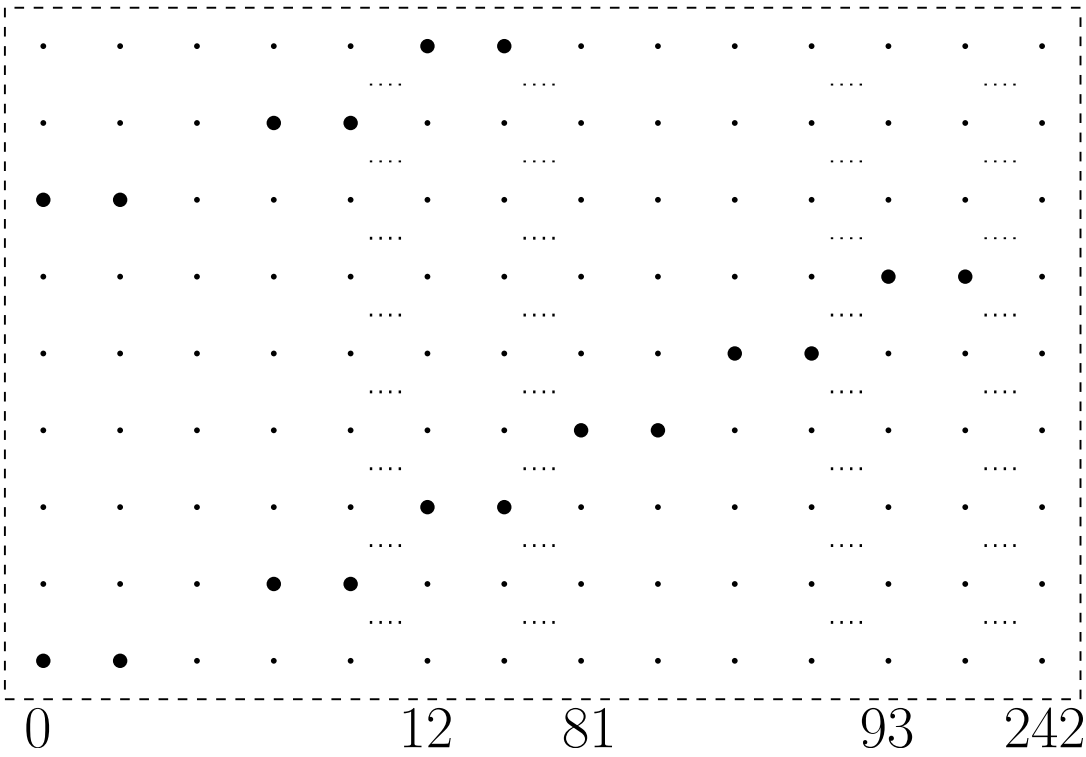
Důkaz. Nejprve si ukážeme, jak body na toru budou vypadat, poté indukcí dle a dokážeme, že žádné tři body neleží na jedné přímce. Označme si $X = \{(i,i^2p); i \in M\}$, $Y = \{(i,i^2p+1); i \in M\}$, kde $M = \{0,\dots,p-1\}$, a označme $Z = X \cup Y$.

Konstrukci si ukážeme induktivně. Pro $a = 1$ použijeme množinu Z. Pro $a > 1$ vezmeme množinu pro případ $a-1$, kterou označíme N, a budeme ji celou $(p-1)$krát kopírovat. Nechť $w \in N$. Pak jeho první kopie bude $w + (p^{a-1}, p^{(a-2)p+4})$. Druhá kopie bude $w + (2p^{a-1}, p^{(a-2)p+5}), \dots, (p-1)$. kopie pak bude $w + ((p-1)p^{a-1}, p^{(a-2)p+p+2})$.

Důležité je upozornit, že se nám stane, že konstrukcí dostaneme body mimo rozsah toru, což znamená, že na toru potom budou umístěné body, které jako souřadnice mají zbytky po dělení příslušnými rozměry. Množina N pro předchozí případ bude mít takovéto body. Pokud ji použijeme na větším toru, bude to znamenat, že popsané body už nebudeme uvažovat modulo rozměry pro předchozí případ $a-1$, ale modulo rozměry pro současný případ a. Ukážeme si to na obrázcích. Na prvním obrázku vidíme případ pro $p = 3$ a $a = 1$.



Na následujícím obrázku je pak případ pro $p = 3$ a $a = 2$.



Nyní musíme ověřit, že po takové konstrukci nebudou žádné tři body ležet na jedné přímce.

Nejprve předpokládejme, že $a = 1$. Zde použijeme pouze množinu Z. Díky větě 3.16 již víme, že žádné tři body z této množiny neleží na jedné přímce.

Nechť tedy $a > 1$. Z indukčího předpokladu máme množinu N pro torus $T_{p^{a-1}\times p^{(a-2)p+2}}$ a zkopírujeme jí dle definice konstrukce. Ověříme, že žádné tři body z množiny vzniklé tímto kopírováním nejsou kolineární. První si uvědomíme, že je třeba testovat jen trojice bodů takové, které obsahují dvě kopie nějakého bodu $w \in N$ (případně kopii a „originál“). Takovéto body budou z definice konstrukce ve tvaru $(w_1 + up^{a-1}, w_2 + p^q)$ a $(w_1 + vp^{a-1}, w_2 + p^r)$ pro u,$v \in \{0, \ldots, p-1\}$, q,$r \geq (a-2)p+4$, a tedy od sebe budou vzdáleny o násobek p^{a-1} v první souřadnici a o násobek $p^{(a-2)p+4}$ v souřadnici druhé. Jiné trojice nemá smysl testovat, protože obraz[1] takové trojice na toru $T_{p^{a-1}\times p^{(a-2)p+2}}$ budou tři různé body z N. Tedy kdyby tato trojice ležela na jedné přímce, tak obraz této přímky na toru $T_{p^{a-1}\times p^{(a-2)p+2}}$ je přímka, na které leží tři body z N, což z indukčího předpokladu nelze.

Pro některé případy využijeme ještě postupu, kdy si trojici bodů zobrazíme na menší torus $T_{p^a\times p^{(a-2)p+4}}$, a ukážeme, že tyto obrazy neleží na jedné přímce. Z definice konstrukce totiž vyplývá, že obrazy této trojice budou tři různé body. Zároveň víme, že obraz přímky z našeho většího toru je také přímka na menším toru, tedy pokud by ležely tři body na větším toru na jedné přímce, musí i jejich obrazy na menším toru ležet na jedné přímce.

Nyní rozeberme jednotlivé případy trojic bodů z množiny, kterou jsme získali popsanou konstrukcí.

Nejprve předpokládejme, že máme dva body, které vznikly postupným kopírováním množiny X a jeden bod, který vznikl kopírováním Y. Předpokládejme, že

[1] uvažujeme standardní zobrazení definované v lemmatu 2.1

bod vzniklý kopírováním X je ve tvaru $A = (k, k^2p)$, kde k,$m \in \{0, \ldots, p-1\}$. Pokud ne, tak to můžeme zařídit posunutím. Další bod tedy musí být ve tvaru $B = (k+up^{a-1}, k^2p+xp^q)$ pro vhodná u,x,$q \in \mathbb{N}$. Poznamenejme, že $q \geq (a-2)p+4 \geq a$ z definice konstrukce. Poslední bod bude pak ve tvaru $C = (m+ps_1, m^2p+ps_2+1)$ pro vhodné $s_1, s_2 \in \mathbb{N}_0$. Bod C totiž jistě bude v obou souřadnicích posunut oproti (m,m^2p+1) o nějaký násobek p. Spočteme $D(A,B,C)$.

$$\begin{aligned} D(A,B,C) &= D((k,k^2p),(k+up^{a-1},k^2p+xp^q),(m+ps_1,m^2p+ps_2+1)) = \\ &= kxp^q + up^a + up^{a-1} + up^a s_2 - mxp^q - xp^{q+1}s_1 - up^a = \\ &= p^{a-1}(u+pR), \end{aligned}$$

kde R je zbytek po vytknutí p^a z ostatních členů. Jistě $u > 0$, jinak by bod A a B byl tentýž. Zároveň z definice konstrukce $u < p$. Proto $D(A,B,C) \not\equiv 0 \pmod{p^a}$, a tedy z lemmatu 1.10 body A,B a C neleží na jedné přímce.

Analogicky pokud budeme mít dva body, které vznikly kopírováním Y a jeden bod, který vznikl kopírováním X. Budeme mít tedy body

$$\begin{aligned} A &= (k, k^2p+1), \\ B &= (l+ps_1, l^2p+ps_2), \\ C &= (k+up^{a-1}, k^2p+xp^q+1). \end{aligned}$$

Dostáváme

$$\begin{aligned} D(A,B,C) &= k^2up^a + up^{a-1} + lxp^q + s_1k^2p^a + s_1xp^{q+1} - up^al^2 - up^as_2 - xp^qk = \\ &= p^{a-1}(u+pR). \end{aligned}$$

Tudíž ani v tomto případě A,B a C neleží na jedné přímce.

Nyní se podívejme na trojice bodů takové, že všechny vznikly postupným kopírováním X. Případ, kdy všechny tři body vznikly kopírováním Y je pak jen posunutí. Mějme tedy body

$$\begin{aligned} A &= (k+\sigma_1, k^2p+\sigma_2), \\ B &= (k+\sigma_1+up^{a-1}, k^2p+\sigma_2+xp^q), \\ C &= (m+\sigma_3, m^2p+\sigma_4), \end{aligned}$$

kde $\sigma_1, \ldots, \sigma_4$ jsou vhodné násobky p, které zatím nemusíme upřesňovat, nicméně je třeba poznamenat, že ze σ_4 a σ_2 lze z definice konstrukce vytknout alespoň p^4, dále $q \geq (a-2)p+4$, u,$x \in \mathbb{N}$ a k,$m \in \{0, \ldots, p-1\}$.

1. Nejprve předpokládáme, že $k \neq m$. Zobrazme si nyní tyto body do menšího toru $T_{p^a \times p^{(a-2)p+4}}$, obrazy označme A', B', C'. Dostáváme, že

$$\begin{aligned} A' &= (k+\sigma_1, k^2p+\sigma_2'), \\ B' &= (k+\sigma_1+up^{a-1}, k^2p+\sigma_2'), \\ C' &= (m+\sigma_3, m^2p+\sigma_4'), \end{aligned}$$

kde σ_2', σ_4' jsou opět násobky p s tím, že z nich lze vytknout alespoň p^4. Podívejme se na přímku mezi A' a C'. Bude dána vektorem $A'-C' = ((k-m)+\sigma_1-\sigma_3, p(k-m)(k+m)+\sigma_2'-\sigma_4')$. Vektor $A'-C'$ tedy můžeme napsat

ve tvaru $(v_1, p^h v_2)$, kde $p \nmid v_1, v_2$ a $h \in \{1,2\}$ podle toho, jestli $k + m = p$. Délka d této přímky pak bude dle lemmatu 1.7 $d = \text{lcm}(p^a, p^{(a-2)p+4-h})$. Dále zobrazme body A', B', C' na torus$T_{p^{a-1} \times p^{(a-2)p+4}}$, obrazy označme A'', B'', C''. Platí, že

$$\begin{aligned} A'' &= (k + \sigma_1', k^2 p + \sigma_2'), \\ B'' &= A'', \\ C'' &= (m + \sigma_3', m^2 p + \sigma_4'), \end{aligned}$$

kde σ_1' a σ_3' jsou násobky p. Potom přímka mezi body A'' a B'' je dána vektorem $A''-C'' = ((k-m)+\sigma_1'-\sigma_3', p(k-m)(k+m)+\sigma_2'-\sigma_4')) = (v_1', p^h v_2')$, kde $p \nmid v_1', v_2'$. Tedy délka d' této přímky bude $d' = \text{lcm}(p^{a-1}, p^{(a-2)p+4-h})$. Platí, že $(a-2)p + 4 - h \geq a$ pro $a > 1$. Tedy $d' = d$ a dle lemmatu 3.18 A', B', C' neleží na jedné přímce. Tedy ani A,B,C neleží na jedné přímce.

2. Zbývá ověřit případ, kdy $k = m$. Nejprve předpokládejme, že všechny body tedy vznikly kopírováním jednoho bodu z X, ale nejsou všechny kopie jednoho bodu z N. Bez újmy na obecnosti předpokládejme, že jeden z těchto bodů je počátek, jinak posuneme. Budeme mít tedy body

$$\begin{aligned} A &= (0,0), \\ B &= (up^{a-1}, xp^q), \\ C &= (vp^t, yp^r), \end{aligned}$$

kde u,x,v,y jsou nesoudělná s p, $q \in \{p^{(a-2)p+4}, \ldots, p^{(a-1)p+2}\}$, $t \leq a-2$, $r \leq (a-2)p + 2$. Podívejme se opět, co se s těmito body stane, když je zobrazíme standardním zobrazením na torus $T_{p^a \times p^{(a-2)p+4}}$. Dostáváme body

$$\begin{aligned} A' &= (0,0), \\ B' &= (up^{a-1}, 0), \\ C' &= (vp^t, y'p^r) \end{aligned}$$

pro vhodné y', které není dělitelné p. Nyní si spočítáme, jaké jsou délky přímek mezi A' a C'. Podobně jako v poznámce 3.9 dostaneme, že přímka, která prochází počátkem, tedy bodem A', a C', prochází i body (ω_1, ω_2) ve tvaru

$$\begin{aligned} \omega_1 &\equiv v \pmod{p^{a-t}} \\ \omega_2 &\equiv y'p^{r-t} \pmod{p^{(a-2)p+2-t}}. \end{aligned}$$

Každá přímka mezi A' a C' bude mít tedy délku $d = \text{lcm}(p^a, \frac{p^{(a-2)p+4}}{p^{r-t}})$ dle lemmatu 1.7. Zobrazme nyní body A', C' na torus $T_{p^{a-1} \times p^{(a-2)p+4}}$. Dostaneme body

$$\begin{aligned} A'' &= A', \\ C'' &= (v'p^t, y'p^r) \end{aligned}$$

pro vhodné v', které není dělitelné p. Délka d' každé přímky mezi A'' a B'' bude $d' = \text{lcm}(p^{a-1}, \frac{p^{(a-2)p+4}}{p^{r-t}})$. Protože pro všechny kombinace r,t v souladu

s definicí konstrukce platí, že $r-t \leq (a-2)p-a+4$, je $(a-2)p+4-(r-t) \geq a$, a proto $d = d'$. Což díky lemmatu 3.18 znamená, že body A', B', C' neleží na jedné přímce, tedy ani A, B, C neleží na jedné přímce.

Nakonec se podívejme na případ, kdy jsou všechny tři body kopie jednoho bodu z N. Bez újmy na obecnosti nechť jsou všechny tři kopie počátku, jinak posuneme. Dostáváme body

$$\begin{aligned} A &= (up^{a-1}, p^q), \\ B &= (vp^{a-1}, p^r), \\ C &= (wp^{a-1}, p^r) \end{aligned}$$

pro nějaká navzájem různá $q,r,s \in \{p^{(a-2)p+4}, \ldots, p^{(a-1)p+2}\}$ a dle konstrukce odpovídající navzájem různá $u,v,w \in \{0, \ldots, p-1\}$. Zde nemůžeme použít postup jako v předchozím případě, protože obrazy těchto tří bodů na toru $T_{p^{a-1} \times p^{(a-2)p+4}}$ budou shodné. Bude třeba počítat determinant. Označme $b := p^{(a-1)p+2}$ a označme D obecný determinant pro tyto body dle lemmatu 1.9. Potom

$$\begin{aligned} D = {} & D(((up^{a-1}, p^q), (vp^{a-1}, p^r), (wp^{a-1}, p^s)) + p^{a+1} D((\alpha_1, p^q), (\beta_1, p^r), (\gamma_1, p^s)) + \\ & + p^b D((up^{a-1}, \alpha_2)(vp^{a-1}, \beta_2)(wp^{a-1}, \gamma_2)) + p^{a+b}((\alpha_1,\alpha_2), (\beta_1, \beta_2), (\gamma_1, \gamma_2)) = \\ & = p^{a+r-1}(u-w) + p^{a+q-1}(w-v) + p^{a+s-1}(v-u) + p^{a+1}(p^r(\alpha_1 - \gamma_1) + \\ & + p^q(\gamma_1 - \beta_1) + q^s(\beta_1 - \alpha_1)) + p^{a+b-1}Q + p^{a+b}W \end{aligned}$$

pro vhodná $Q,W \in \mathbb{Z}$. Nechť bez újmy na obecnosti q je nejmenší nenulové číslo z $\{q,r,s\}$. Potom jistě $q < b$. Proto z výrazu D můžeme vytknout p^{a+q-1} a dostaneme $p^{a+q-1}((w-v)+pH)$ pro vhodné $H \in \mathbb{Z}$. Proto $D \neq 0$, a tedy body A,B,C díky lemmatu 1.9 neleží na jedné přímce.

□

Poznamenejme ještě, že pro $p = 2$ lze druhá souřadnice toru ještě snížit o 1. Tudíž platí následující tvrzení.

Věta 3.20. *$\tau(T_{2^a \times 2^{2a-1}}) = 2^{a+1}$ pro $a \in N$.*

Důkaz. Pro torus $T_{2\times 2}$ můžeme jistě použít všechny čtyři jeho body, což jsou v podstatě také body množin $X = \{(i,i^2p); i \in \{0,1\}\}$ a $Y = \{(i,i^2p+1); i \in \{0,1\}\}$. Dále pro $a > 1$ vezmeme stejně jako ve větě 3.19 množinu pro $a-1$, kterou označíme N a jednou ji zkopírujeme. Nechť $w \in N$. Pak jeho kopie bude $w + (2^{a-1}, 2^{(2a-1)})$. Důkaz je skoro stejný jako v předchozím případě, rozeberou se tedy různé případy. Využije se např. vlastnost, že pro $p = 2$ nebude nikdy $k + m = p$ pro různá $k,m \in \{0, \ldots, p-1\}$. □

Pro úplnost, ale již bez důkazu, uveďme ještě tvrzení z článku [1], resp. [2].

Věta 3.21 (viz [1] nebo [2])**.** *Buď p prvočíslo, potom $T_{p\times p} \geq p+1$.*

Z čehož potom plyne následující důsledek.

Důsledek 3.22 (viz [1] nebo [2])**.** *Buď p prvočíslo, potom $T_{p\times p} = p+1$.*

Důkaz. Kombinace horního odhadu 3.11 a dolního odhadu 3.21. □

4. Posloupnosti

Nyní se podívejme, jak se bude chovat τ, pokud jeden rozměr toru zafixujeme a druhý budeme měnit.

Definice 4.1. Nechť $z \in \mathbb{N}\backslash\{1\}$. Pak definujme posloupnost $P_z(x)$ tak, že $P_z(x) = \tau(T_{z\times x})$.

Například pro $z = 2$ dostáváme posloupnost 2,4,2,4,... Při prozkoumání malých hodnot z se zdá, že posloupnosti P_z jsou periodické. Otázka je, jestli to platí pro každé $z \in \mathbb{N}$. Poznamenejme, že P_z může nabývat jen konečně mnoha hodnot a to konkrétně $2, \ldots, 2z$ (lemma 3.1). Z toho plyne, že posloupnost nabývá nějakého maxima, které je nejvýše $2z$.

Věta 4.2. *Buď p prvočíslo, $a \in \mathbb{N}$. Označme $t = \max_{x\in\mathbb{N}} P_{p^a}(x)$. Dále označme $m = \min\{x; P_{p^a}(x) = t\}$. Potom posloupnost P_{p^a} je periodická s periodou m.*

Důkaz. Z minimality m plyne $m = p^b$ pro $b \in \mathbb{N}$. Kdyby totiž m bylo ve tvaru hp^e pro $e \in \mathbb{N}$ a $h > 1$ takové, že $p \nmid h$, z věty 2.4 dostaneme, že $P_{p^a}(p^e) = P_{p^a}(hp^e)$. A tedy by m nebylo minimální. Mějme tedy libovolné $x \in \{1 \ldots p^b\}$. Ukažme, že $P_{p^a}(x) = P_{p^a}(x + \alpha p^b)$, pro libovolné $\alpha \in \mathbb{N}$. Rozepišme $x = rp^l$, kde $l \geq b$ a $\mathrm{GCD}(r, p) = 1$. Potom z věty 2.4 víme, že $P_{p^a}(x) = P_{p^a}(p^l)$. Rozlišíme 2 případy:

1. $x < p^b$
   Pak $x + \alpha p^b = p^l(r + \alpha p^{b-l})$. Protože $b - l \geq 1$, bude $\mathrm{GCD}(r + \alpha p^{b-l}, p) = 1$. Dle věty 2.4 $P_{p^a}(r + \alpha m) = P_{p^a}(p^l) = P_{p^a}(x)$.

2. $x = p^b$
   Pak $x + \alpha p^b = p^b(1 + \alpha)$. Jelikož $P_{p^a}(p^b)$ je maximální hodnota posloupnosti, tak z důsledku 2.2 $P_{p^a}(p^b) = P_{p^a}(np^b)$, pro jakýkoliv nenulový násobek n.

Tudíž pro každé $x \in \mathbb{N} : P_{p^a}(x) = P_{p^a}(x + \alpha m)$. □

Důsledek 4.3. *Posloupnost P_{p^a}, kde p je prvočíslo, $a \in \mathbb{N}$, je periodická s periodou $p^{(a-1)p+2}$.*

Důkaz. Z věty 3.19 víme, že $P_{p^a}(p^{(a-1)p+2}) = 2p^a$, což je z věty 3.1 maximum této posloupnosti. Tudíž z vět 2.4 a 4.2 je $p^{(a-1)p+2}$ jistě násobkem nejmenší periody, a tedy je také periodou. □

Důsledek 4.4. *Posloupnost P_{2^a}, kde $a \in \mathbb{N}$, je periodická s periodou 2^{2a-1}.*

Důkaz. Podobně jako v předchozím případě, s využitím věty 3.20. □

Pro mocniny prvočísla periodicita vychází docela pěkně. Otázkou zůstává, jestli lze postup zobecnit pro libovolné $z \in \mathbb{N} \setminus \{1\}$. Uvažujme tedy libovolné z. Můžeme ho napsat jako součin prvočísel. Nechť n je počet prvočísel v rozkladu z a $I = \{1, \ldots, n\}$. Pak $z = \prod_{i=1}^{n} p_i^{a_i}$, kde p_i je dané prvočíslo rozkladu a a_i jeho mocnina.

Věta 4.5. *Nechť $z \in \mathbb{N}$. Pak posloupnost P_z je periodická.*

Důkaz. Buď $z = \prod_{i=1}^{n} p_i^{a_i}$ prvočíselný rozklad čísla z. Pak definujme $m_z = \prod_{i=1}^{n} p_i^{b_i}$ pro b_i taková, aby platila následující podmínka.

$$\text{Pro každé } J \subseteq I : P_z(\prod_{j\in\overline{J}} p_j^{b_j} \prod_{j\in J} p_j^{c_j}) = P_z(\prod_{j\in\overline{J}} p_j^{d_j} \prod_{j\in J} p_j^{c_j}) \tag{4.1}$$

pro libovolná $d_j \geq b_j$, $c_j < b_j$ a kde $\overline{J} := I \setminus J$. Toto číslo nám bude sloužit jako perioda. Je ale nejprve třeba ukázat, že vůbec existuje pro každé $z \in \mathbb{N} \setminus \{1\}$.

Mějme $\prod_{i=1}^{n} p_i^{b_i^{(0)}}$ pro libovolné $b_i^{(0)} \geq a_i$ takové, aby platilo, že $P_z(\prod_{i=1}^{n} p_i^{b_i^{(0)}})$ je maximum posloupnosti přes všechna x ve tvaru $\prod_{i=1}^{n} p_i^{b_i}$. Z věty 2.4 víme, že to bude i maximum přes všechna možná x. Tuto hodnotu označíme $\max P_z$. Ukážeme, jak z tohoto čísla dostaneme hledané m_z. Označme $B^{(0)} = (b_1^{(0)})_{i\in I}$, tedy hodnoty mocnin pro jednotlivá prvočísla. Tyto hodnoty budeme postupně zvětšovat na $B^{(1)} = (b_i^{(1)})_{i\in I}$, $B^{(2)} = (b_i^{(2)})_{i\in I}$, ..., dokud nedostaneme mocniny pro hledané m_z. Nejprve ještě poznamenejme, že dvojici $J \subseteq I$ a $C = (c_j)_{j\in J}$ takové, že $c_j < b_j^{(i-1)}$ pro $j \in J$ v i. kroku, budeme nazývat konfiguraci a značit $K(C,J)$.

Začneme tedy tím, že máme výše definované $v := \prod_{i=1}^{n} p_i^{b_i^{(0)}}$, a tedy i $B^{(0)}$. Pokud už v splňuje naši podmínku (4.1), jsme hotovi. Předpokládejme tedy, že podmínka nebude splněna. To nám dokazují konfigurace $K(C,J)$, pro které platí, že existují $d_j; d_j \geq b_j^{(0)}$ pro $j \in \overline{J}$, taková, že hodnota $P_z(\prod_{j\in\overline{J}} p_j^{b_j^{(0)}} \prod_{j\in J} p_j^{c_j}) < P_z(\prod_{j\in\overline{J}} p_j^{d_j} \prod_{j\in J} p_j^{c_j}) =: R$ (opačná nerovnost z důsledku 2.2 nenastane). Předpokládejme navíc, že číslo R už nevzroste zvýšením nějakých d_j pro $j \in \overline{J}$. To si můžeme dovolit, protože P_z může nabývat pouze konečně mnoha hodnot a platí důsledek 2.2. Pro každou konfiguraci $K(C,J)$, pro kterou není podmínka (4.1) splněna, potom položme $b_j^{K(C,J)} = d_j$ (rozumíme příslušné d_j pro danou konfiguraci), kde $j \in \overline{J}$.

Pro $j \in J$ položme $b_j^{K(C,J)} = b_j$. Definujme nyní posloupnost hodnot $B^{(1)}$ tak, že $b_i^{(1)}$ bude maximální $b_i^{K(C,J)}$ přes všechny konfigurace $K(C,J)$, pro které není podmínka (4.1) splněna. Z této konstrukce vyplývá, že pro hodnotu $\prod_{i=1}^{n} p_i^{b_i^{(1)}}$ bude podmínka splněna pro všechny $K(C,J)$ takové, že $c_j < b_i^{(0)}$, kde $j \in J$. Protože jsme zvýšili mocninu u nějakých z prvočísel $p_i; i \in I$, dostaneme nové možné konfigurace $K(C,J)$ takové, že existuje $j \in J$, pro které $c_j \geq b_j^{(0)}$. Pro tyto konfigurace nemusí být ale podmínka (4.1) splněna.

Tento postup proto několikrát zopakujeme. Obecně v k. kroku začínáme s hodnotou $\prod_{j\notin J} p_j^{b_j^{(k-1)}}$. Pokud už je pro ni podmínka (4.1) splněna, jsme hotovi. Pokud ne, pro každou konfiguraci $K(C,J)$, která nesplňuje podmínku opět najdeme d_j taková, že $P_z(\prod_{j\notin J} p_j^{d_j} \prod_{j\in J} p_j^{c_j})$ se už nezvýší při zvýšení mocnin u p_j pro $j \in \overline{J}$. Položíme $b_j^{K(C,J)} = d_j$ pro $j \in \overline{J}$ a $b_j^{K(C,J)} = b_j^{(k-1)}$ pro $j \in J$. Jako $b_i^{(k)}$ potom vezmeme maximální $b_i^{K(C,J)}$ přes všechny konfigurace $K(C,J)$ nesplňující podmínku a tím definujeme $B^{(k)}$. Pro hodnotu $\prod_{i=1}^{n} p_i^{b_i^{(k)}}$ pak bude podmínka (4.1) splněna pro všechny $K(C,J)$ takové, že $c_j < b_i^{(k-1)}$, kde $j \in J$.

Je potřeba nahlédnout, že po konečně mnoha krocích budeme mít hledané m_z. Podívejme se tedy, co se stane po $n-1$ krocích. Pro spor předpokládejme, že podmínka ještě není splněna. Mějme tedy pro nějaké $J \subseteq I$ a $c_j < b_j^{(n-1)}$, kde $j \in J$, výraz $P_z(\prod_{j\in\overline{J}} p_j^{b_j^{(n-1)}} \prod_{j\in J} p_j^{c_j})$ takový, že hodnota P_z se ještě dá zvýšit zvýšením mocnin u $p_j; j \in \overline{J}$. Označme $J_k = \{j; j \in J, b^{(k-1)} \leq c_j < b_j^{(k)}\}$ pro $k \in \{1,\ldots,n-1\}$. Dodefinujme pak $J_0 = \{j; j \in J, c_j < b_j^{(0)}\}$. Množin $J_0, J_1, \ldots, J_{n-1}, \overline{J}$ je dohromady $n+1$, jsou navzájem disjunktní a všechny jsou podmnožiny I. Jelikož $|I| = n$, musí být nějaká z těchto množin prázdná. Aby mělo smysl hovořit o nesplněné podmínce, $\overline{J}$ to být nemůže. Pokud bude prázdná J_{n-1}, podmínka musí být splněna, protože to bylo zařízeno v $(n-1)$. kroku. Pokud bude prázdná množina J_0, dostáváme z důsledku 2.2 a z volby $B^{(0)}$

$$\max P_z = P_z(\prod_{i=1}^{n} p_i^{b_i^{(0)}}) \leq P_z(\prod_{j\in\overline{J}} p_j^{b_j^{(n-1)}} \prod_{j\in J} p_j^{c_j}),$$

protože v takovém případě pro každé $j \in J$ platí, že $b_j^{(0)} \leq c_j$ a také pro každé $j \in \overline{J}$ platí, že $b^{(0)} \leq b_j^{(n-1)}$. Což díky důsledku 2.2 znamená, že výraz $P_z(\prod_{j\in\overline{J}} p_j^{b_j^{(n-1)}} \prod_{j\in J} p_j^{c_j})$ už není možné zvýšit.

Nechť je tedy prázdná množina J_h pro $h \in \{1,\ldots,n-2\}$. Z důsledku 2.2 dostáváme

$$P_z(\prod_{j\in\overline{J}} p_j^{b_j^{(n-1)}} \prod_{j\in J} p_j^{c_j}) = P_z(\prod_{j\in\overline{J}} p_j^{b_j^{(n-1)}} \prod_{j\in J_0} p_j^{c_j} \cdots \prod_{j\in J_{h-1}} p_j^{c_j} \prod_{j\in J_{h+1}} p_j^{c_j} \cdots \prod_{j\in J_{n-1}} p_j^{c_j}) \geq$$
$$\geq P_z(\prod_{j\in\overline{J}} p_j^{b_j^{(h)}} \prod_{j\in M} p_j^{c_j} \prod_{j\in V} p_j^{b_j^{(h)}}) = P_z(\prod_{j\in\overline{M}} p_j^{b_j^{(h)}} \prod_{j\in M} p_j^{c_j}) =: Q,$$

kde $M = \bigcup_{0\leq k\leq h-1} J_k$, $\overline{M} = I \setminus M$ a $V = \bigcup_{h+1\leq k\leq n-1} J_k$. Hodnota Q už ale nevzroste zvyšováním mocnin $b_j^{(h)}$ u $p_j; j \in \overline{M}$ (neboli $j \in V \cup \overline{J}$). To jsme totiž zařídili v h. kroku. Protože $b_j^{(h)} \leq c^j$ pro $j \in V$ a $b_j^{(h)} \leq b_j^{(n-1)}$ pro $j \in \overline{J}$, dostáváme spor.

Nyní už přistupme k samotnému důkazu periodicity P_z.

Potřebujeme ukázat, že pro každé $x \leq m_z$ a pro každé $\alpha \in \mathbb{N}_0 : P_z(x) = P_z(x + \alpha m)$. Označme $\mathbb{P} = \{p_1,\ldots,p_n\}$. Tj. množina právě takových prvočísel, která jsou v prvočíselném rozkladu z. Vezměme libovolné $x \in \{1,\ldots,m_z\}$. Můžeme rozepsat jako $x = r\prod_{i=1}^{n} p_i^{s_i}$. Kde pro r platí, že $\mathrm{GCD}(r,p) = 1$ pro každé $p \in \mathbb{P}$. Z věty 2.4 víme, že $P_z(x) = P_z(\prod_{i=1}^{n} p_i^{s_i})$. Rozlišíme dva případy:

1. $s_i < b_i$ pro každé $i \in \{1,\ldots n\}$
   Potom $x + \alpha m_z = \prod_{i=1}^{n} p_i^{s_i}(r + \alpha\prod_{i=1}^{n} p_i^{b_i-s_i})$. Výraz v závorce je jistě nesoudělný se všemi $p \in \mathbb{P}$. Tudíž $P_z(x + \alpha m_z) = P_z(\prod_{i=1}^{n} p_i^{s_i}) = P_z(x)$ dle věty 2.4.

2. Existuje $i \in \{1,\ldots,n\}$ takové, že $s_i \geq b_i$.
   Nechť $K \subseteq \{1,\ldots,n\}$ je množina takových i, pro která $s_i < b_i$, $L \subseteq \{1,\ldots,n\}$ množina takových i, pro která $s_i = b_i$ a $M \subseteq \{1,\ldots n\}$ množina takových i, pro která $s_i > b_i$. Dostáváme

$x+\alpha m_z = \prod_{i\in K} p_i^{s_i} \prod_{i\in L\cup M} p_i^{b_i}(r \prod_{i\in M} p_i^{s_i-b_i} + \alpha \prod_{i\in K} p_i^{b_i-s_i})$. Může se nám stát, že sčítance v závorce se nám sečtou na násobek nějakého prvočísla p_i pro $i \in L \cup M$. Zde využijeme toho, jak je definováno m_z, díky čemuž nám to nevadí a hodnotu P_z nám vynásobení výrazem v závorce neovlivní, protože z definice m_z platí, že $P_z(\prod_{i\in K} p_i^{s_i} \prod_{i\in L\cup M} p_i^{b_i})$ nevzroste zvýšením mocnin u p_i, kde $i \in L \cup M$. Neovlivní ji ani vynásobení jakýmkoliv číslem, které nemá v prvočíselném rozkladu p_i pro $i \in I$ (věta 2.4). Dostáváme, že $P_z(x + \alpha m) = P_z(\prod_{i\in K} p_i^{s_i} \prod_{i\in L\cup M} p_i^{b_i}) = P_z(\prod_{i=1}^{n} p_i^{s_i}) = P_z(x)$, což platí opět z vlastnosti m_z.

Tudíž pro každé $x \in \{1, \ldots, m_z\}$ platí, že $P_z(x + \alpha m_z) = P_z(x)$. □

Seznam použité literatury

[1] J. Fowler, A. Groot, D. Pandya, and B. Snapp. The no-three-in-line problem on a torus. 2012. arXiv: 1203.6604.

[2] A. Misiak, Z. Stępień, A. Szymaszkiewicz, L. Szymaszkiewicz, and M. Zwierzchowski. A note on the no-three-in-line problem on a torus. *Discrete Mathematics*, 339(1):217–221, 2016.

[3] A. Selberg. An Elementary Proof of Dirichlet's Theorem About Primes in an Arithmetic Progression. *Annals of Mathematics*, 50(2):297–304, 1949.

[4] D. Stanovský. *Základy algebry.* MatfyzPress, Praha, 2010. ISBN: 9788073781057.

[5] J. Žemlička. Algebra I pro informatiky. `http://www.karlin.mff.cuni.cz/~zemlicka/15-16/alg_skripta.pdf`, 2016.