BAKALÁŘSKÁ PRÁCE

Filip Hrdinka

Osobní identifikační číslo v zemích Evropy

Katedra matematiky

Vedoucí bakalářské práce: doc. RNDr. Antonín Jančařík, Ph.D.

Studijní program: Specializace v pedagogice

Studijní obor: Matematika a informační technologie
se zaměřením na vzdělávání

2024

Prohlašuji, že jsem tuto bakalářskou práci vypracoval(a) samostatně a výhradně s použitím citovaných pramenů, literatury a dalších odborných zdrojů. Tato práce nebyla využita k získání jiného nebo stejného titulu.

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 má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle §60 odst. 1 autorského zákona.

V ..... dne ....

Podpis autora

Děkuji panu docentu Jančaříkovi za cenné rady při vypracování bakalářské práce.

Název práce: Osobní identifikační číslo v zemích Evropy

Autor: Filip Hrdinka

Katedra: Katedra matematiky

Vedoucí bakalářské práce: doc. RNDr. Antonín Jančařík, Ph.D., Katedra matematiky

Abstrakt: Většina národních identifikačních čísel má kontrolní číslice, které pomocí předem daného algoritmu dokáží odhalit určitou část chyb, které jsou způsobené lidským faktorem. Tyto algoritmy a kontrolní číslice budeme souhrnně nazývat kontrolní systém. Každá země má jiné národní identifikační číslo s jiným kontrolním systémem.
Cílem této práce je zaměřit se na detekci nejčastějších typů chyb, co lidé dělají. K tomu v této práci odvodíme vhodná kritéria a podmínky k rozhodnutí, jaké množství chyb bude díky kontrolní číslici odhaleno.
Ve finále byla podle těchto podmínek zhodnocena účinnost detekce chyb národních identifikačních čísel ve vybraných zemích Evropy. V této práci se zjistilo, že nejčastější kontrolní systémy v národních identifikačních číslech jsou založeny na dělitelnosti čísel 10, 11 a 23. Při kontrolním systému založeným na dělitelnosti 10 je více neodhalitelných chyb, než u ostatních, ale výhodou je, že kontrolní číslice je vždy jednociferná. U prvočísel jako je 11 a 23 je výhoda lepší detekce chyb, ale kontrolní číslice může být i dvojciferná.
V tomto tématu se využívá znalost dělitelnosti, kombinatoriky a obecně logického myšlení. Cílem práce je zjistit a zhodnotit, jestli je toto téma vhodné do výuky matematiky a informatiky. Tento cíl byl naplněn, protože v RVP základní školy matematiky a informatiky se vyskytuje mnoho zmínek, které přímo souvisí s tímto tématem.

Klíčová slova: kontrolní číslice národní identifikační číslo dělitelnost

Title: Personal identification number in Europe

Author: Filip Hrdinka

Department: Department of mathematics

Supervisor: doc. RNDr. Antonín Jančařík, Ph.D., Department of mathematics

Abstract: Most national identification numbers have check digits that can detect a certain proportion of human errors using a predefined algorithm. These algorithms and check digits will be collectively referred to as the checking system. Each country has a different national identification number with a different checking system.
The goal of this paper is to focus on detecting the most common types of errors people make. To do this, in this paper we derive suitable criteria and conditions to decide how many errors will be detected due to the check digit.
Finally, the effectiveness of error detection of national identification numbers in selected European countries was evaluated according to these conditions. In this work, it was found that the most common checking systems in national identification numbers are based on the divisibility of the numbers 10, 11 and 23. The checking system based on divisibility of 10 has more undetectable errors than the others, but the advantage is that the check digit is always single digit. For prime numbers such as 11 and 23, there is the advantage of better error detection, but the check digit can be double-digit.
This topic uses knowledge of divisibility, combinatorics, and logical thinking in general. The aim of this paper is to investigate and evaluate whether this topic is suitable for teaching mathematics and computer science. This objective has been fulfilled because there are many references in the Primary School Mathematics and Computer Science that are directly related to this topic.

Keywords: check digit national identification number divisibility

Obsah

Úvod

Většina států Evropy má nějaké národní identifikační číslo. Toto číslo se přiřazuje občanům daného státu a slouží k mnoha účelům, zejména pak k jejich identifikaci a ověření jejich totožnosti.
V tomto čísle bývají zahrnuty i základní informace o danému občanovi, např. pohlaví nebo datum narození.
Je skutečně nutné, aby člověk při uvádění tohoto čísla byl pozorný a napsal ho bez chyb. Při chybném zápisu může dojít k záměně nebo k problému s identifikací.
Proto existuje ve většině takových identifikačních čísel kontrolní číslice, s jejíž pomocí dokážeme odhalit mnoho chyb, které člověk ve svém národním identifikačním čísle může udělat.
Národní identifikační číslo má tedy ve svém znění unikátní číslo přiřazené občanovi a kontrolní číslici, která je vypočtena z ostatních číslic.
Pokud je kontrolní číslice zadaná správně a v čísle je chyba, je možné, že díky kontrolní číslici ji odhalíme. Je mnoho chyb, které mohou lidé při zapisování identifikačního čísla udělat, například výměna dvou vedlejších číslic, záměna číslice za jinou, nebo zdvojená číslice.
Cílem práce je popsat národní identifikační čísla zemí s vhodnými,současně co nejvíce různorodými způsoby výpočtu kontrolní číslice. Cílem je uvést jejich strukturu a další obecné informace o národním identifikačním číslu.
Cílem práce je zaměřit se na nejčastější typy chyb, odvodit vhodná kritéria a podmínky k rozhodnutí, jaké množství chyb bude díky kontrolní číslici odhaleno. Úkolem práce bude zjistit pomocí odvozených podmínek odhalení jednotlivých chyb míru detekce různých evropských zemí. Ve finále bude zhodnocena účinnost detekce chyb národních identifikačních čísel ve vybraných zemích Evropy.
V tomto tématu se hodně využívá znalost dělitelnosti, kombinatoriky a obecně logického myšlení. Je to situace, která je velmi praktická a vychází z reálného života. Cílem práce je také zjistit a zhodnotit, jestli je toto téma vhodné do výuky matematiky a informatiky. Bude se proto zabývat otázkou, zda lze vytvořit praktickou hodinu výuky, která bude vyhovovat RVP pro základní školu.

1. Základní pojmy

1.1 Kongruence

Definice 1 (Kongruence). *Nechť z,a* $\in \mathbb{Z}, m \in \mathbb{N}$. *Čísla z a a jsou kongruentní modulo m, právě tehdy když* $z - a = km$, *kde* $k \in \mathbb{Z}$. *Značíme:*

$$z \equiv a \,(mod\, m)$$

(Křížek, Somer a Šolcová, 2018, s.40)

Definice 2 (Zbytková třída). *Nechť* $r \in \mathbb{Z}, m \in \mathbb{N}$ *Potom zbytkovou třídou modulo m nazveme množinou:*

$$Z_m = \{z \in \mathbb{Z} | z \equiv r(mod\, m)\}$$

Věta 1. *Nechť* $a \equiv b \,(mod\, m), c \in \mathbb{Z}$. *Potom* $ac \equiv bc \,(mod\, m)$.

Věta 2. *Nechť* $ac \equiv bc \,(mod\, m)$ *a* $NSD(m,c) = 1$. *Potom* $a \equiv b \,(mod\, m)$.

Věta 3. *Nechť* $a_1 \equiv b_1 \,(mod\, m) a\ a_2 \equiv b_2 \,(mod\, m)$. *Potom:*

$$a_1 + a_2 \equiv b_1 + b_2 \,(mod\, m)$$
$$a_1.a_2 \equiv b_1.b_2 \,(mod\, m)$$
$$a_1 - a_2 \equiv b_1 - b_2 \,(mod\, m)$$

(Křížek, Somer a Šolcová, 2018, s.40)

1.2 Systém kontrolních číslic

Definice 3 (Kontrolní číslice). *Nechť je* Z_k *zbytková třída.*
Zadefinujeme si zobrazení:

$$\sigma_1, \sigma_2 ... \sigma_n$$

Zobrazení σ_i *je definováno*

$$Z_k \to Z_k$$

$$x \to mx$$

Kontrolovaný řetězec je

$$a_1, a_2, a_3 .. a_{n-1}$$

a a_n *je kontrolní číslice,* $n \in \mathbb{N}$ *určená tak, že pokud je daný řetězec napsán správně, tak platí, že*

$$\sigma_1(a_1) + \sigma_2(a_2) ... + \sigma_n(a_n) \equiv 0 \,(mod\, k)$$

Kontrolní součet nemusí být nutně kongruentní s nulou, ale je nutné, aby byl kongruentní s jedním číslem. (Gallian, 1996, s. 14)

Definice 4 (Vektor kontrolovaného řetězce a vektor vah)**.** *Máme kontrolní systém, kde máme definovaná zobrazení*

$$\sigma_1, \sigma_2 ... \sigma_n$$

a tato zobrazení můžeme převést do skalárního součinu dvou vektorů. První nazveme vektor kontrolovaného řetězce a druhý vektor vah.

$$(a_1, a_2 ... a_n).(w_1, w_2 ... w_n) \equiv 0 \ (mod\ k)$$

(Gallian, 1996, s.14)

1.3 Typy chyb a jejich frekvence

Kontrolní systém je navržen tak, aby dokázal odhalit co nejvíce chyb, kterých se mohou lidé dopustit. Statisticky bylo zjištěno, že lidé se nejčastěji dopouští určitých typů chyb, na které se kontrolní systémy soustředí. V tabulce v příloze jsou uvedeny nejčastější chyby a jejich relativní frekvence.

V následující sekci se podíváme na jednotlivé typy chyb a odvodíme podmínky, pod nimiž jsou odhalitelné.

1.4 Jednoduchá chyba

Definice 5 (Jednoduchá chyba)**.** *Jednoduchá chyba typu $a \rightarrow b$ vznikne, pokud v kontrolovaném řetězci nahradíme nějaké jedno číslo a_i, za nějaké jiné b_i takové, že platí:*

$$w_1.a_1 + w_2.a_2 ... + w_{i-1}.a_{i-1} + w_i.a_i + w_{i+1}.a_{i+1} ... + w_n.a_n \equiv w_1.a_1 + w_2.a_2 ...$$
$$+ w_{i-1}.a_{i-1} + w_i.b_i + w_{i+1}.a_{i+1} ... + w_n.a_n \ (mod\ k)$$

(Gallian, 1996 s. 15)

Věta 4. *Jednoduchou chybu odhalíme, pokud platí podmínka, že $NSD(w_i, k) = 1$, kde w_i je váha z vektoru vah a k je modul.*

Jednoduchá chyba bude odhalitelná, pokud bude platit:

$$a_i.w_i \equiv b_i.w_i \ (mod\ k)$$

Tuto rovnici můžeme upravit následujícím způsobem:

$$a.w_i - b.w_i \equiv 0 \ (mod\ k)$$
$$w_i.(a_i - b_i) \equiv 0 \ (mod\ k)$$

Pokud chceme, aby se zbytek po dělení číslem k násobku $w_i.(a_i - b_i)$ rovnal nule, tak buď w_i, $a_i - b_i$, nebo celý násobek $w_i.(a_i - b_i)$ musí být dělitelný číslem k.
Celý daný násobek může být dělitelný číslem k, pokud w_i i $a_i - b_i$ budou mít jiný dělitel čísla k než jedničku.
Protože jsou čísla omezena rozsahem $0...k-1$, tak $a_i - b_1$ nikdy nebude násobek

čísla k, protože nelze vytvořit číslo, které je větší nebo rovno k.
Tím pádem podmínka neodhalitelnosti je, že pro příslušnou váhu z vektoru vah platí, že $NSD(w_i, k) = 1$.
Tím zaručíme, že daný násobek nebude nikdy dělitelný k. Pokud ale není splněna podmínka, tak to neznamená, že chyba nebude automaticky odhalena. V tu chvíli se jen nemůžeme na danou podmínku spolehnout a musíme otestovat, kdy se násobek $w_i.(a_i - b_i)$ rovná nějakému násobku k.

Pokud tedy nebude splněna podmínka, existuje váha, která má společný dělitel s číslem k jiným než jedna. To znamená, že u těchto vah existují číslice, které když vynásobíme danou vahou a vydělíme číslem k,budou mít stejný zbytek po dělení.

Počet možných chyb u jednoduché chyby je stejný jako počet možných zbytků po dělení číslem k.

V případě reálných kontrolních systémů se tato chyba v podstatě nevyskytuje, protože základní pravidlo, kterým volíme vektor vah, je takové, aby všechna čísla byla nesoudělná s číslem k. (Gallian, 1996, s.15)

1.5 Transpozice vedlejších číslic

Definice 6 (Transpozice vedlejších číslic)**.** *Transpozice vedlejších číslic typu $ab \rightarrow ba$ vznikne, pokud v kontrolovaném řetězci vyměníme mezi sebou nějaké a_i za jiné b_{i+1} tak, že platí:*

$$w_1.a_1 + w_2.a_2 ... + w_{i-1}.a_{i-1} + w_i.a_i + w_{i+1}.b_{i+1} ... + w_n.a_n \equiv w_1.a_1 + w_2.a_2 \\ ... + w_{i-1}.a_{i-1} + w_i.b_{i+1} + w_{i+1}.a_i ... + w_n.a_n \ (mod\ k)$$

(Gallian, 1996, s. 15)

Věta 5. *Transpozici vedlejších číslic odhalíme, pokud platí podmínka, že $NSD(w_i - w_{i+1}, k) = 1$, kde w_i je váha z vektoru vah a k je modul.*

Transpozice vedlejších číslic bude neodhalitelná, pokud bude platit:

$$a_i.w_i + b_{i+1}.w_{i+1} \equiv b_{i+1}.w_i + a_i.w_{i+1}\ (mod\ k)$$

Tuto kongruenční rovnici můžeme upravit následujícím způsobem:

$$a_i.w_i - b_{i+1}.w_i + a_i.w_{i+1} - b_{i+1}.w_{i+1} \equiv 0\ (mod\ k) \\ w_i.(a_i - b_{i+1}) - w_{i+1}(a_i - b_{i+1}) \equiv 0\ (mod\ k) \\ (a_i - bi + 1).(w_i - w_{i+1}) \equiv 0\ (mod\ k)$$

Takže podobně jako u jednoduché chyby bude transpozice vedlejších chyb určitě odhalená, pokud platí, že $NSD(w_i - w_{i+1}, k\ ) = 1$. Pokud podmínka není splněna, musíme zjistit, pro které číslice je odhalitelná a pro které ne. (Gallian, 1996, s. 16)

1.6 Skoková transpozice

Definice 7 (Transpozice vedlejších číslic)**.** *Skoková transpozice typu abc → cba vznikne, pokud v kontrolovaném řetězci vyměníme mezi sebou nějaké a_i za jiné c_{i+2} tak, že platí:*

$$w_1.a_1 + w_2.a_2... + w_{i-1}.a_{i-1} + w_i.a_i + w_{i+1}.b_{i+1} + w_{i+2}.c_{i+2}... + w_n.a_n \equiv w_1.a_1 + \\ + w_2.a_2... + w_{i-1}.a_{i-1} + w_i.b_{i+1} + w_{i+1}.a_i... + w_n.a_n \ (mod\ k)$$

(Gallian, 1996, s.15)

Věta 6. *Skokovou transpozici odhalíme, pokud platí podmínka, že $NSD(w_i - w_{i+2}, k) = 1$, kde w_i je váha z vektoru vah a k je modul.*

Skoková transpozice je odhalena, pokud platí:

$$a.w_i + b.w_{i+1} + c.w_{i+2} \equiv c.w_i + b.w_{i+1} + a.w_{i+2} \ (mod\ k)$$

Tuto kongruenční rovnici lze upravit následujícím způsobem:

$$a_i.w_i + c_{i+2}.w_{i+2} \equiv c_{i+2}.w_i + a_i.w_{i+2} \ (mod\ k)$$
$$a_i.w_i - c_{i+2}.w_i + c_{i+2}.w_{i+2} - a_i.w_{i+2} \equiv 0 \ (mod\ k)$$
$$w_i.(a_i - c_{i+2}) - w_{i+2}.(a_i - c_{i+2}) \equiv 0 \ (mod\ k)$$
$$(w_i - w_{i+2}).(a_i - c_{i+2}) \equiv 0 \ (mod\ k)$$

Podobně jako v předchozích odstavcích bude skoková transpozice určitě odhalitelná, pokud platí, že $NSD(w_i - w_{i+2}, k) = 1$. (Gallian, 1996, s.15)

1.7 Dvojitá chyba

Definice 8 (Dvojitá chyba)**.** *Dvojitá chyba typu aa → bb vznikne, pokud v kontrolovaném řetězci vyměníme dvě stejné a_i a a_{i+1} za dvě stejné číslice b_i a b_{i+1} které jsou vedle sebe tak, že platí:*

$$w_1.a_1 + w_2.a_2... + w_{i-1}.a_{i-1} + w_i.a_i + w_{i+1}.a_{i+1} + ... + w_n.a_n \equiv w_1.a_1 + \\ + w_2.a_2... + w_{i-1}.a_{i-1} + w_i.b_i + w_{i+1}.b_{i+1} + ... + w_n.a_n \ (mod\ k)$$
$$a_i = a_{i+1}$$
$$b_i = b_{i+1}$$

(Gallian, 1996, s.15)

Věta 7. *Dvojitou chybu určitě odhalíme, pokud platí podmínka, že $NSD(w_i + w_{i+1}, k) = 1$, kde w_i je váha z vektoru vah a k je modul.*

Dvojitá chyba je odhalena, pokud platí:

$$a_i.w_i + a_{i+1}.w_{i+1} \equiv b_i.w_i + b_{i+1}.w_{i+1} \ (mod\ k)$$

Tuto kongruenční rovnici lze upravit následujícím způsobem:

$$a_i.w_i - b_i.w_i + a_{i+1}.w_{i+1} \equiv 0 \ (mod\ k)$$
$$w_i.(a_i - b_i) + w_{i+1}.(a_i - b_i) \ (mod\ k)$$
$$(a_i - b_i)(w_i + w_{i+1}) \equiv 0 \ (mod\ k)$$

Podobně jako v předchozích odstavcích bude dvojitá chyba určitě odhalitelná, pokud platí, že $NSD(w_i + w_{i+1}, k) = 1$. (Gallian, 1996, s. 15)

1.8 Fonetická chyba

Definice 9 (Fonetická chyba)**.** *Fonetická chyba typu* $a0 \rightarrow 1a$ *vznikne, pokud platí, že*

$$w_1.a_1 + w_2.a_2... + w_{i-1}.a_{i-1} + w_i.a_i + w_{i+1}.0... + w_n.a_n \equiv w_1.a_1 + w_2.a_2$$
$$... + w_{i-1}.a_{i-1} + w_i.1 + w_{i+1}.a_i.... + w_n.a_n \ (mod\ k)$$

(Gallian, 1996, s.15)

Věta 8. *Fonetickou chybu určitě odhalíme, pokud platí podmínka, že* $a_i.(w_i - w_{i+1}) \not\equiv w_i \ (mod\ k)$*, kde* w_i *je váha z vektoru vah a* k *je modul.*

Fonetická chyba je odhalena, pokud platí, že $a_i.w_i + 0.w_{i+1} \equiv 1.w_i + a.w_{i+1} \ (mod\ k)$ Tuto kongruenční rovnici lze upravit následujícím způsobem:

$$a_i.w_i \equiv w_i + a_i.w_{i+1} \ (mod\ k)$$
$$a_i.w_i - a_i.w_{i+1} \equiv w_i \ (mod\ k)$$
$$a_i(w_i - wi + 1) \equiv w_i \ (mod\ k)$$

Podmínka pro neodhalitelnost fonetické chyby bude tedy $a_i.(w_i - w_{i+1}) \not\equiv w_i \ (mod\ k)$. (Gallian, 1996, s.15)

1.9 Skoková dvojitá chyba

Definice 10 (Skoková dvojitá chyba)**.** *Skoková dvojitá chyba typu aca* $\rightarrow$ *bcb vznikne, pokud v kontrolovaném řetězci vyměníme dvě stejné* a_i *a* a_{i+2} *za dvě stejné číslice* b_i *a* b_{i+2}*, že platí:*

$$w_1.a_1 + w_2.a_2... + w_{i-1}.a_{i-1} + w_i.a_i + w_{i+1}.c_{i+1} + w_{i+2}.a_{i+2}... + w_n.a_n \equiv w_1.a_1 +$$
$$+w_2.a_2... + w_{i-1}.a_{i-1} + w_i.b_i + w_{i+1}.c_{i+1} + w_{i+2}.b_{i+2}... + w_n.a_n \ (mod\ k)$$
$$a_i = a_{i+2}$$
$$b_i = b_{i+2}$$

(Gallian, 1996, s.15)

Věta 9. *Skokovou dvojitou chybu určitě odhalíme, pokud platí podmínka, že* $NSD(w_i + w_{i+2}, k) = 1$*, kde* w_i *je váha z vektoru vah a* k *je modul.*

Skoková dvojitá chyba je odhalena, pokud platí:

$$a_i.w_i + c_{i+1}.w_{i+1} + a_{i+2}.w_{i+2} \equiv b_i.w_i + c_{i+1}.w_{i+1} + b_{i+2}.w_{i+2} \ (mod\ k)$$

Tuto kongruenční rovnici lze upravit následujícím způsobem:

$$a_i.w_i + a_{i+2}.w_{i+2} \equiv b_i.w_i + b_{i+2}.w_{i+2} \ (mod\ k)$$
$$a_i.w_i - b_i.w_i + a_{i+2}.w_{i+2} - b_{i+2}.w_{i+2} \equiv 0 \ (mod\ k)$$
$$w_i(a_i - b_i) + w_{i+2}(a_i - b_i) \equiv 0 \ (mod\ k)$$
$$(w_i + w_{i+2}).(a_i - b_i) \equiv 0 \ (mod\ k)$$

Podobně jako v předchozích odstavcích bude skoková dvojitá chyba určitě odhalitelná, pokud platí, že $NSD(w_i + w_{i+2}, k) = 1$.

V tabulce v příloze jsou shrnuty jednotlivé chyby a jejich odvozené podmínky odhalitelnosti. (Gallian, 1996, s.15)

2. Národní identifikační čísla

2.1 Národní identifikační čísla, která mají kontrolní systém založen na modulu 10

Národní identifikační čísla, která mají kontrolní systém založen na modulu 10 budou vždy ve tvaru $(a_1,a_2...a_m).(w_1, w_2..w_n) \equiv p\,(mod\,10)$. Kontrolní číslice budou vždy vycházet jako zbytky po dělení 10. Výhodou je, že díky tomu budou zbytky po dělení číslem 10 jen jednociferná čísla. Takže kontrolní číslice bude vždy jednociferné číslo v rozsahu 0–9. Nevýhodou je to, že číslo 10 není prvočíslo, a proto je větší výskyt neodhalitelných chyb.
Nejdříve se podíváme na jednoduchou chybu. Pokud jsou v jednociferných vahách čísla 2, 4, 5, 6, 8, tak je možné, že v určitých kombinacích násobků kontrolovaných čísel může vyjít po dělení stejný zbytek. Takže potřebujeme vybírat váhy z čísel 1, 3, 7, 9, abychom se vyhnuli jednoduché chybě.
Co se transpozice vedlejších čísel týče, potřebujeme, aby se co nejméně rozdílů vedlejších vah rovnalo číslu, které má společné dělitele s číslem 10. V případě čísel 0–9 to budou znovu čísla 2, 4, 5, 6, 8 a také číslo 0. Pokud se chceme tedy vyhnout jakékoliv transpoziční chybě, musíme vybírat čísla, jejichž rozdíl vyjde 1, 3, 7 a 9. Číslu 9 se to nebude rovnat nikdy, protože bychom museli od číslice 9 odečíst číslo 0 a to nikdy nevybereme jako váhu.
Další čísla, o kterých můžeme uvažovat, jsou čísla kongruentní k těmto číslům. To jsou čísla 9, 7, 3, 1. Číslo 9 nám nevyjde,takže hledáme čísla 1, 3, 7, 1, 3 a 7. Pro číslo 1 to budou dvojice vah (2, 1), (3, 2), (4, 3), (5, 4), (6, 5), (7, 6), (8, 7), (9, 8). Pro 1 to budou stejné dvojice číslic jako u 1, ale vyměníme pořadí první a druhé váhy. Pro číslo 3 to budou číslice (4, 1),(5, 2),(6, 3),(7, 4),(8, 5),(9, 6). Pro číslo 3 to budou stejné dvojice číslic jako u 3, ale zase vyměníme pořadí první a druhé váhy. Pro číslo 7 to budou dvojice číslic (8, 1) a (9, 2). Pro číslo 7 to budou stejné dvojice číslic jako u 7, ale zase vyměníme pořadí první a druhé váhy. Pokud tedy vybereme řetězec, kde budou sousedit jen tyto váhy, bude transpozice vedlejších číslic u tohoto typu kontrolního systému odhalitelná.
U dvojité chyby nás zajímají součty vedlejších vah. Pokud se budou součty vedlejších vah rovnat číslům, která mají společné dělitele s číslem 10, chyby budou neodhalitelné. Jediné číslice, které nebudou mít společné dělitele s číslem 10, budou číslice 1 , 3, 7 a 9. Tím pádem se budeme snažit najít takové dvojice čísel 1–9, že když je sečteme a vydělíme číslem 10, budou mít zbytek po dělení 1, 3, 7 nebo 9. U čísla 1 to budou dvojice (9, 2), (8, 3), (7, 4), (6, 5) a další čtyři dvojice, pokud vyměníme pořadí první a druhé číslice vah. U čísla 3 to budou dvojice čísel (9, 4), (8, 5), (7,6), (2, 1) a další čtyři dvojice, pokud vyměníme pořadí první a druhé číslice vah. U čísla 7 to budou dvojice čísel (6, 1), (5, 2), (3, 4), (9, 8) a další čtyři dvojice, pokud vyměníme pořadí první a druhé číslice vah. U čísla 9 to budou dvojice čísel (8, 1), (7, 2), (6, 3), (5, 4) a další čtyři dvojice, pokud vyměníme pořadí první a druhé číslice vah. Pokud tedy z daných dvojic vytvoříme řetězec takový, že každé dvě vedlejší číslice budou jedny z těchto číslic, budou všechny dvojité chyby v takovém řetězci odhalitelné.
Dále se podíváme na skokové transpozice. U skokové transpozice musíme zajistit, aby se rozdíl vah w_i a w_{i+2} rovnal číslu, které nemá společné dělitele s číslem 10.

To budou stejné dvojice jako u transpozice vedlejších čísel.
Podobně probereme skokové dvojité chyby, kde se součet vah w_i a w_{i+2} rovná číslu, které nemá společné dělitele s číslem 10. To budou stejné dvojice jako u dvojité chyby.
Dále probereme fonetickou chybu. Pokud chceme, aby byla fonetická chyba neodhalitelná, musí platit odvozená podmínka $j.(w_i - w_{i+1} \not\equiv w_i)$. Za čísla w_i a w_{i+1} můžeme dosadit jakoukoliv kombinaci vah, takže nám vyjdou různá čísla od 1 do 9 a od 1 do 9. Tím pádem můžeme vytvořit mnoho rovnic, kde vlastně hledáme, pro jaká čísla má tato rovnice řešení. Protože používáme modulo 10, bude vždy jedno číslo od 1–9, které když dosadíme, bude fonetická chyba neodhalitelná. Pokud chceme, aby byly všechny chyby mezi dvěma vahami odhaleny, musíme zjistit, pro jaká čísla nemá tato rovnice řešení. Pokud rovnice nebude mít řešení, podmínka $j.(w_i - w_{i+1} \not\equiv w_i)$ bude platit pro každé číslo. Podmínkou, aby rovnice $a.j \equiv b\,(mdd\ n)$ měla řešení, je, že b musí být násobkem $NSD(a,n)$ neboli že je číslo b dělitelné číslem $NSD(a,n)$. V našem případě, pokud máme rovnici $j.(w_i - w_{i+1} \equiv w_i)$, tak podmínka, aby rovnice měla řešení, je, aby váha w_i byla dělitelná číslem $NSD((w_i - w_{i+1}, 10)$.

2.1.1 Polsko

Číslo nazvané PESEL je od roku 1979 identifikační číslo pro každého občana Polska.

Číslo je dlouhé jedenáct číslic a je to unikátní identifikátor pro jednu osobu.
Číslo PESEL má formu YYMMDDZZZZQ, kde YYMMDD je poslední dvojčíslí roku narození, měsíc narození a den narození. ZZZZ je unikátní číslo, sudé je určeno pro ženy a liché je určeno pro muže.
Číslo PESEL je vytvořeno, aby vydrželo pět století. Aby se rozeznali lidé narození v jiných století, tak se upravuje druhé dvojčíslí, které značí měsíce. Pro roky narození mezi rokem 1900 a 1999 se žádná změna netvoří, jsou to ty měsíce, které to mají být. Pro roky 2000–2099 se přidá k druhému dvojčíslí dvacet, pro roky 2100–2199 se přidá čtyřicet. Pro 2200–2299 šedesát a pro 1800–1899 osmdesát.
Q je kontrolní číslice. Každou číslici z jedenácti postupně roznásobíme určitými čísly.
Naše dané číslo má formu ABCDEFGHIJ, pak roznásobíme dané číslo postupně čísly 1, 3, 7, 9, 1, 3, 7, 9, 1 a 3 tímto způsobem: $A \times 1 + B \times 3 + C \times 7 + D \times 9 + E \times 1 + F \times 3 + G \times 7 + H \times 9 + I \times 1 + J \times 3$
Na následnou sumu použijeme operaci modulo 10, což znamená, že dané číslo vydělíme číslem deset, a co nám vyjde jako zbytek po dělení, je vlastně modulo. Modulo deseti se značí % daným číslem. Číslo, které nám vyjde po aplikaci operace modula 10, odečteme od čísla 10 a to bude naše kontrolní číslice. (Ministry of Finance of Poland, 2023)
Pro ilustraci vytvoříme příklad polského rodného čísla. Vytvoříme polské rodné číslo pro muže, který se narodil 13. 5. 2002. První dvojčíslí bude 02, protože je to poslední dvojčíslí roku narození.
Rok narození je v rozmezí 2000–2099, takže se k druhému dvojčíslí přičte číslo 20. Druhé dvojčíslí tedy bude číslo 25.
Třetí dvojčíslí bude číslo 13 podle dnu narození.
Další čtyřčíslí zvolíme tak, aby bylo liché a aby vyjadřovalo to, že je daný občan

muž. Zvolíme náhodně číslo 1543.
Číslo PESEL je tedy zatím 0225131643 a poslední, co nám chybí, je kontrolní číslice. Použijeme kontrolní algoritmus a vypočítáme kontrolní číslici: $0 * 1 + 2 * 3 + 2 * 7 + 9 * 5 + 1 * 1 + 3 * 3 + 1 * 7 + 6 * 9 + 1 * 4 + 3 * 3 = 154$. Zbytek po dělení je číslo 4 a kontrolní číslice tedy bude 6. Celé identifikační číslo bude 02251316436.
Systém PESEL byl původně navržen komunistickou vládou Polské lidové republiky, aby mohla sledovat osobní informace o každém občanovi. Jeho založení sahá do 1979, kdy byl tento systém zaveden. Vznik systému PESEL byl reakcí na potřebu rychlého vyhledávání dat, která byla vedena v kartotékovém systému evidence obyvatelstva. PESEL je povinný pro všechny stálé obyvatele Polska a jeho dočasné obyvatele, kteří žijí v Polsku déle než 2 měsíce. (Graczyk, 2019)
Kontrolní systém čísla PESEL má vektor vah (1, 3, 7, 9, 1, 3, 7, 9, 1, 3), kterým se pomocí skalárního součinu vynásobí vektor kontrolovaných číslic $(a_1, a_2 \dots a_{10})$, kde platí, že $(a_1, a_2 \dots a_{10}).(1\ , 3, 7, 9, 1, 3, 7, 9, 1, 3) \equiv p\ (mod\ 10)$. Modulo bude deset a číslo p je jakýkoliv zbytek po dělení deseti.

Jednoduchá chyba Kontrolní systém čísla PESEL odhalí jednoduchou chybu, pokud platí podmínka:

$$NSD(w_i, k) = 1$$

Největší společný dělitel všech číslic vektoru vah a modula k je číslo jedna, což splňuje danou podmínku. Jednoduchá chyba tedy bude ve 100 % případů neodhalitelná.

Transpozice vedlejších čísel Kontrolní systém čísla PESEL odhalí transpozici vedlejších čísel, pokud splňuje odvozenou podmínku o neodhalitelnosti transpozice vedlejších čísel. Podmínka zní:

$$NSD(w_i - w_{i+1}, k) = 1$$

Pokud od sebe postupně odečteme všechny vedlejší číslice z vektoru vah (1, 3, 7, 9, 1, 3, 7, 9, 1, 3), tak zjistíme, že všechna čísla jsou sudá. Pokud totiž odečteme dvě lichá čísla, vždy vyjde číslo sudé. Největší společný dělitel jakéhokoliv sudého čísla a deseti bude vždy jiný než jedna, protože vždy budou mít společného dělitele dvojku.

To znamená, že se nemůžeme spolehnout na kritéria o neodhalitelnosti chyb a musíme se podívat na jednotlivé váhy a čísla. Můžeme složit kongruenční rovnice, které vyjadřují, jakým způsobem se chyba vytváří.

$$\begin{aligned} i + 3j &\equiv j + 3i\ (mod\ 10) \\ 3i + 7j &\equiv 3j + 7i\ (mod\ 10) \\ 7i + 9j &\equiv 7j + 9i\ (mod\ 10) \\ 9i + j &\equiv 9j + i\ (mod\ 10) \end{aligned}$$

Když upravíme dané rovnice, tak nám vyjde.

$$\begin{aligned} 2i &\equiv 2j\ (mod\ 5) \\ 4i &\equiv 4j\ (mod\ 5) \\ 8i &\equiv 8j\ (mod\ 5) \end{aligned}$$

Těmto rovnicím budou odpovídat čísla $i \equiv j + 5 \ (mod\ 10)$ a $i \equiv j \ (mod\ 10)$, ale nepočítáme dvojice jako je 11, 22 atd., protože jejich výměna nebude chyba.

Dvojice čísel (0, 5), (1, 6), (2, 7), (3, 8) a (4, 9) a dvojice čísel, které vzniknou, když vyměníme jejich pořadí, budou neodhalitelné.

To znamená, že máme dohromady 10 dvojic čísel, která budou neodhalitelná u každé dvojice vah.

Počet všech možných kombinací, jak můžeme sestavit dvojciferné číslo je 100. Pokud ale bereme všech 100 možností, znamenalo by to, že dvojice jako jsou 11, 22 atd., zahrnujeme dvakrát. Jednu tuto dvojici odebereme a budeme mít dohromady 90 možností.

U každé dvojice vah budeme mít 10 neodhalitelných chyb a všechny ostatní chyby odhalíme.

Máme dohromady 10 číslic daného identifikačního čísla. Dvojice vah budou tyto (1, 3), (3, 7), (7, 9) , (9, 1) a dohromady jich bude 9.

Počet všech možných chyb tedy bude 810 a počet všech odhalitelných chyb bude 720.

Když vydělíme počet všech možných chyb a počet chyb, které jsou odhalitelné, tak nám vyjde $720/810 * 100 \doteq 88{,}9\ \%$, což znamená, že algoritmus odhalí cca. 88,9 % chyb způsobených výměnou dvou vedlejších číslic.

Skoková transpozice Skoková transpozice je odhalitelná, pokud je splněna následující podmínka:

$$NSD(w_i - w_{i+2}, k) = 1$$

V tomto případě to dopadne úplně stejně jako u transpozice dvou vedlejších čísel. Dvojice vah, které mezi sebou budeme vyměňovat totiž budou stejné .Tím pádem nám vyjde stejná míra detekce chyb skokové transpozice jako u transpozice vedlejších číslic, což je cca. 88,9 %.

Dvojitá chyba Dvojitá chyba je odhalitelná, pokud je splněná odvozená podmínka:

$$NSD(w_i + w_{i+1}, k) = 1$$

Stejně jako u transpozice vedlejších čísel a u skokové transpozice nebude tato podmínka nikdy splněna, protože vektor vah je složen z lichých číslic, a pokud sečteme jakékoliv dvě liché číslice, vznikne z toho sudá. Pokud je číslice sudá, tak určitě bude mít s číslem deset největší společný dělitel jiný než jedna.
Nemůžeme se tedy znovu spolehnout na podmínku a musíme se podívat na jednotlivé váhy a číslice.

$$j + 3j \equiv i + 3i \ (mod\ 10)$$
$$3j + 7j \equiv 3 + 7i \ (mod\ 10)$$
$$7j + 9j \equiv 7i + 9i \ (mod\ 10)$$
$$9j + j \equiv 9i + i \ (mod\ 10)$$

Takže když to upravíme, budeme mít:

$$4j \equiv 4i \,(mod\, 10)$$
$$10j \equiv 10i \,(mod\, 10)$$
$$16j \equiv 16i \,(mod\, 10)$$
$$10j \equiv 10i \,(mod\, 10)$$

U dvojic vah (1, 3) a (7, 9) jsou neodhalitelné dvojice čísel stejné jako u výměny vedlejších číslic, ale u dvojic (3, 7) a (9, 1) jsou neodhalitelné všechny možnosti čísel.

Tím pádem u dvojic (1, 3) a (7, 9) je odhaleno 80 chyb a u dvojic (3, 7) a (9, 1) není odhalena žádná chyba.

Dvojic (1, 3) a (7, 9) je v řetězci 5 a dvojic (3, 7) a (9, 1) je v řetězci 4.

Takže neodhalitelných chyb bude $5 * 10 + 4 * 90 = 410$ a tím pádem bude odhalitelných chyb 400.

Když vydělíme počet všech možných chyb a počet chyb, které jsou odhalitelné, tak nám vyjde $400/810 * 100 \doteq 49{,}4\,\%$, což znamená, že algoritmus odhalí cca. 49,4 % dvojitých chyb.

Fonetická chyba Fonetická chyba lze odhalit, pokud je splněná odvozená podmínka:

$$a(w_i - w_{i+1}) \not\equiv w_i : (mod\, k)$$

Budeme postupně dosazovat do dané podmínky a jako rozdíly daných vah nám vyjdou čísla 2, 4 a 8. Číslo 2 je kongruentní s číslem 8 a číslo 4 je kongruentní s číslem 6 při modulu 10. Takže nám vyšla kombinace takových vah a čísel, že z nich můžeme vytvořit tyto kongruenční rovnice:

$$8a \equiv 1 \,(mod\, 10)$$
$$6a \equiv 3 \,(mod\, 10)$$
$$8a \equiv 9 \,(mod\, 10)$$

Tyto rovnice nemají žádné řešení, protože násobek jakéhokoliv sudého čísla je sudý a ten po dělení deseti nebude mít zbytek, který je lichý. Takže tím pádem se odhalí 100 % chyb.

Skoková dvojitá chyba Skoková dvojitá chyba je odhalitelná, pokud je splněna následující podmínka:

$$NSD(w_i + w_{i+1}, k) = 1$$

Díky sčítání stejných kombinací jako u transpozice vedlejších číslic vyjde míra detekce také stejně, a to 88,9 %. Zde je shrnutí míry detekce jednotlivých chyb. Jednotlivá chyba má míru detekce 100 %, transpozice vedlejších čísel má míru detekce 88,9 %, skoková transpozice má míru detekce 88,9 %, fonetická chyba má míru detekce 100 % a skoková dvojitá chyba má míru detekce 88,9 %.

2.1.2 Rakousko

Rakousko má devítičíselné národní identifikační číslo. Kontrolní systém rakouského rodného čísla má vektor vah (1, 2, 1, 2, 1, 2, 1, 2), kterým se pomocí skalárního součinu vynásobí vektor kontrolovaných číslic
(a_1,
: a_2 ... a_8), kde platí, že (a_1, a_2 ... a_8).(1, 2, 1, 2, 1, 2, 1, 2) $\equiv p\,(mod\,10)$. Modulo je 10 a číslo p je jakýkoliv zbytek po dělení deseti. (TIN Algorithms, 2019, s.8)

Jednoduchá chyba Každá jednoduchá chyba lze odhalit, pokud je pro každou váhu splněna podmínka:

$$NSD(w_i,k)$$

Podmínka je splněna u poloviny všech vah, protože číslo 1 podmínku splňuje, ale číslo 2 ne.

U čísla 2 můžeme sestavit kongruenční rovnici, která nám pomůže zjistit, jaké chyby budou neodhalitelné. Rovnici upravíme následujícím způsobem:

$$2i \equiv 0\,(mod\,10)$$

$$i \equiv 0\,(mod\,5)$$

Tato rovnice bude splněná pro tato čísla:

$$i = 5k\,,\, k \in \mathbb{Z}$$

V našem případě to bude tedy splněno jen pro číslo 5.
U váhy 1 tedy nebude žádná neodhalitelná chyba. U váhy 2 bude 1 neodhalitelná chyba, takže 8 odhalitelných. Vektor vah u rakouského národního identifikačního čísla se skládá z číslic 1 a 2. Číslo 1 je tam zastoupeno čtyřikrát a číslo 2 také. Tím pádem bude 76 odhalitelných chyb z celkových 80. Pravděpodobnost objevení chyby vypočítáme jako 76 / 80 $*$ 100 = 95 %.

Transpozice vedlejších číslic Kontrolní systém rakouského identifikačního čísla odhalí transpozici vedlejších čísel, pokud splňuje podmínku

$$NSD(w_i - w_{i+1} = 1)$$

V našem případě bude rozdíl vah 1 nebo 1. U obou bude největší společný dělitel číslo 1, což znamená, že podmínka je splněna pro všechny váhy a míra detekce je 100 %.

Skoková transpozice Kontrolní systém rakouského identifikačního čísla odhalí skokovou transpozic, pokud platí podmínka:

$$NSD(w_i - w_{i+2}, k) = 1$$

Rozdíl příslušných vah se bude vždy rovnat číslu 0. Číslo 0 má za dělitele všechna čísla, takže největší společný dělitel bude 10. Nemůžeme se tedy spolehnout na podmínku neodhalitelnosti a složíme kongruenční rovnici, která nám to pomůže ověřit:

$$2j + 2i \equiv 2i + 2j\,(mod\,10)$$

Odečteme od obou stran příslušné neznámé a vyjde nám:

$$0 \equiv 0 \,(mod\, 10)$$

To znamená, že rovnice platí vždy.Úplně stejně by to vyšlo u rovnice:

$$i + j \equiv i + j \,(mod\, 10)$$

Kontrolní systém neodhalí žádnou skokovou transpozici, tedy 0 %.

Dvojitá chyba Kontrolní systém rakouského identifikačního čísla odhalí dvojitou chybu, pokud bude splněna podmínka:

$$NSD(w_i + w_{i+1}, k)$$

Když dosadíme příslušné váhy, součet se bude rovnat vždy číslu 3, které je nesoudělné s modulem 10. Míra detekce bude tedy 100 %.

Fonetická chyba Kontrolní systém rakouského identifikačního čísla odhalí fonetickou chybu, pokud je splněna odvozená podmínka:

$$a(w_i - w_{i+1} \not\equiv w_i) \,(mod\, k)$$

Do podmínky budeme dosazovat příslušné váhy. Díky tomu nám vzniknou dvě kongruenční rovnice, jejichž řešení jsou chyby, jež budou neodhalitelné:

$$-j \equiv 1 \,(mod\, 10)$$

To můžeme upravit na:

$$j \equiv -1 \,(mod\, 10)$$

A to lze ekvivalentně přepsat na:

$$j \equiv 9 \,(mod\, 10)$$

Takže u dvojice vah, kde je číslo 1 první a 2 druhé, bude fonetická chyba vzniklá dosazením čísla 9 neodhalitelná. Druhá rovnice je ta, kde první váha je číslo 2 a druhá číslo 1.

$$j \equiv 2 \,(mod\, 10)$$

To znamená, že neodhalitelná fonetická chyba také vznikne dosazením čísla 9.

Tím pádem budou u každé dvojice vah 2 neodhalitelné chyby. Tudíž je u každé váhy 16 chyb, které jsou odhalitelné. Rakouské národní identifikační číslo má 8 číslic, takže je 7 dvojic vah. Odhalitelných chyb je tedy $7 * 16 = 112$.

Pravděpodobnost detekce chyby tedy vypočítáme tak, že vydělíme počet odhalených chyb počtem celkových chyb, tedy $112 \,/\, 126 * 100 \doteq 88{,}9$ %.

Skoková dvojitá chyba Kontrolní systém rakouského identifikačního čísla odhalí skokovou dvojitou chybu, pokud bude splněna podmínka:

$$NSD(w_i + w_{i+2}) = 1$$

Když sečteme příslušné váhy, zjistíme, že vyjde buď číslo 2, nebo číslo 4. Čísla 2 a 4 mají obě největší společný dělitel s číslem 10 číslo 2. Tím pádem není splněna podmínka a my se na ni nemůžeme spolehnout, takže to musíme zkontrolovat jinak. Sestavíme první kongruenční rovnici.

$$i + j \equiv i + j \ (mod\, 10)$$

Když ji upravíme, tak vyjde:

$$0 \equiv 0 \ (mod\, 10)$$

Což znamená, že u vah 1 a 1 nebude odhalena žádná chyba. Další rovnice bude následující:

$$2i + 2j \equiv 2i + 2j \ (mod\, 10)$$

A tato rovnice po úpravě dopadne jako ta předchozí, takže kontrolní systém rakouského identifikačního čísla má míru detekce skokové dvojité chyby 0 %.

Nyní zde uvedu shrnutí míry detekce všech častých chyb u daného identifikačního čísla. Míra detekce jednoduché chyby je 95 %, míra detekce transpozice vedlejších čísel je 100 %, míra detekce skokové transpozice je 0 %, míra detekce dvojité chyby je 100 %, míra detekce fonetické chyby je 100 % a míra detekce skokové dvojité chyby je 0 %.

2.2 Národní identifikační čísla, která mají kontrolní systém založený na modulu 11

Národní identifikační čísla, která mají kontrolní systém založený na modulu 11, budou mít vždy kontrolní systém ve tvaru skalárního součinu dvou vektorů $(a_1, a_2, a_3...a_n).(w_i,w_2, w_3...w_n) \equiv p\,(mod\,11)$. Kontrolní číslice bude vždy nějaký zbytek po dělení 11.
Nevýhodou je to, že kontrolní číslice může vyjít číslo 10, což je dvouciferná číslice odlišná od nuly. Tím pádem je potřeba vymyslet algoritmus nebo speciální znak, který se použije v případě, že tato situace nastane.
V tomto odstavci se podíváme na to, jakým způsobem bude tento algoritmus odhalovat nejčastější chyby. Začneme s jednoduchou chybou.
Jednoduchá chyba je neodhalitelná, pokud existuje společný dělitel modula 11 a váhy z vektoru vah. Pokud budeme předpokládat, že váhy budou jednociferné a nebudou se rovnat 0, není žádná váha, která by měla jakýkoliv společný dělitel s číslem 11 jiný než 1. Tím pádem tedy budou všechny jednoduché chyby u kontrolního algoritmu s modulem 11 vždy odhalitelné, přičemž nezáleží na tom, jakými vahami kontrolovaný řetězec násobíme.
Dále se podíváme na transpozici vedlejších číslic. Transpozice vedlejších číslic bude neodhalitelná v případě, že rozdíl dvou vedlejších vah nám vyjde číslo, které má s číslem 11 jiný společný dělitel než číslo 1. V našem případě bereme v potaz jen jednociferná čísla,takže jedinou možností je číslo 0. To stane jen v případě, že jsou vedle sebe dvě stejné váhy. V jiném případě je transpozice vedlejších čísel vždy odhalitelná.
U skokové transpozice to bude fungovat stejně jako u transpozice vedlejších číslic. Pomocí jednociferných čísel nemůžeme vytvořit číslo, které je dělitelné 11, takže chyba nebude odhalitelná jen v případě, že budou váhy w_i a w_{i+2} stejné číslo.
Dále probereme dvojitou chybu. Dvojitá chyba je neodhalitelná, pokud součet vedlejších vah má s číslem 11 jiného společného dělitele než číslo 1. To se stane jen v případě, že součet daných dvou vah budou násobky 11, 11 nebo 0. Poněvadž sčítáme dvě kladná čísla, tak číslo 0 a násobky čísla 11 nikdy nevyjdou. Číslo 11 vyjde jen v případě dvojic (6, 5), (7, 4), (8, 3), (9, 2). Pokud jsou tyto dvojice čísel ve vektoru vah vedle sebe, tak u nich kontrolní číslice dvojitou chybu neodhalí. Další série čísel, u kterých nelze odhalit dvojitou chybu jsou takové, kdy vyměníme pořadí první a druhé váhy v předchozích dvojicích.
U skokové dvojité chyby to bude fungovat stejně jako u dvojité chyby. Zase budeme mít stejné 4 dvojice čísel, které když dáme za příslušné váhy w_i a w_{i+2}, tak na těchto místech bude skoková dvojitá chyba neodhalitelná.
Dále se podíváme na fonetickou chybu. Aby byla fonetická chyba odhalitelná, tak musí být splněna podmínka pro odhalitelnost fonetické chyby: $(w_i - w_{i+1} \not\equiv w_i\,(mod\,11))$. Za váhy w_i a w_{i+1} můžeme dosadit jakékoliv číslo od 1–9 a jako rozdíl v odvozené podmínce nám vyjdou čísla od 1 do 9 a od 1 do 8. Sestavíme rovnice následujícím způsobem: $a.b \equiv a(\,mod\,11))$, kde a je příslušný rozdíl a přitom jedna z vah a b je číslice z kontrolovaného řetězce. Sestavíme tedy rovnici a ta čísla, která nám vyjdou jako b, budou čísla, pro která je fonetická chyba neodhalitelná.

2.2.1 Česko

České rodné číslo je desetimístné a je beze zbytku dělitelné 11. První dvojčíslí vyznačuje poslední dvě číslice roku narození. Další dvojčíslí vyjadřuje měsíc narození. Pokud je občan žena, tak je druhé dvojčíslí zvýšeno o číslo 50. Třetí dvojčíslí vyjadřuje den narození. Poslední čtyřčíslí vyjadřuje rozdělení občanů narozených ve stejném dnu. Poslední číslice je kontrolní, která je přiřazovaná tak, aby číslo bylo dělitelné číslem 11. (Ministerstvo vnitra, 2023)
Rodná čísla, která byla přidělována občanům před 1. 1. 1954, mají stejnou strukturu, ale nesplňují podmínku dělitelnosti číslem 11. (Ministerstvo vnitra, 2020)
Jako příklad českého rodného čísla uvedeme rodné číslo, které je přiřazeno ženě, která se narodila 12. 5. 1976. Protože se narodila v roce 1976, první dvojčíslí bude 76. Narodila se v květnu, takže druhé dvojčíslí by bylo 05, ale protože je žena, tak přičteme číslo 50, takže druhé dvojčíslí bude 55. Třetí dvojčíslí bude číslo 12, označující den jejího narození. Další trojčíslí je přiřazeno, aby rozlišovalo všechny občany, kteří se narodili ve stejný den, takže například číslo 567. Pak musíme určit kontrolní číslici tak, aby celé číslo bylo dělitelné číslem 11. Zatím máme tedy číslo 765512567. Abychom vypočetli kontrolní číslici, tak použijeme podmínky pro dělitelnost číslem 11. $7\ 6 + 5\ 5 + 1\ 2 + 5\ 6 + 7 = 6$. Abychom získali dělitelnost číslem 11, tak chceme, aby po dělení 11 vyšel zbytek 0. Tím pádem musíme přidat číslo 6. Takže číslo je 7655125676.
Jako rodná čísla jsou brána i čísla, která byla přidělena na území Slovenské republiky před 1. 1. 1993. (Ministerstvo vnitra, 2020) Kontrolní systém českého identifikačního čísla má vektor vah (1, 1, 1, 1, 1, 1, 1, 1, 1) a vektor kontrolovaných číslic (a_1, a_2 ... a_{10}). Platí, že skalární součin těchto vektorů je $(1, 1, 1, 1, 1, 1, 1, 1, 1).(a_1, a_2 ... a_{10}) \equiv p\ (mod\ 11)$.

Jednoduchá chyba Kontrolní systém českého identifikačního čísla odhalí každou jednoduchou chybu, pokud je splněna podmínka:

$$NSD(w_i, k) = 1$$

Tato podmínka je splněna vždy, protože jediná hodnota vah je číslo 1 a společně s číslem 11 má největší společný dělitel právě číslo 1. Takže míra detekce jednoduché chyby bude 100 %.

Transpozice vedlejších číslic Kontrolní systém českého identifikačního čísla odhalí každou jednoduchou chybu, pokud splňuje podmínku:

$$NSD(w_j - w_{j+1}) = 1$$

Pokud od sebe odečteme jakékoliv váhy, tak nám vyjde číslo 0. Všechna čísla jsou dělitelé nuly, takže největší společný dělitel bude 11. Nemůžeme se tedy spolehnout na podmínku a sestavíme kongruenční rovnici:

$$i + j \equiv i + j\ (mod\ 11)$$

Po úpravě nám vyjde:

$$0 \equiv 0\ (mod\ 11)$$

Toto platí vždy, a proto kontrolní systém nenajde žádnou transpozici vedlejších čísel, takže míra detekce je 0 %.

Skoková transpozice Skoková transpozice je odhalitelná vždy, když je splněna podmínka:

$$NSD(w_i - w_{i+2},k) = 1$$

Stejně jako u transpozice vedlejších číslic bude rozdíl příslušných vah vždy číslo 0, takže míra detekce bude 100 %.

Dvojitá chyba Dvojitá chyba je odhalitelná vždy, když je splněná podmínka:

$$NSD(w_i + w_{i+1}, k) = 1$$

Součet dvou vedlejších vah je vždy číslo 2, které je nesoudělné s číslem 11, což znamená, že podmínka je vždy splněna, takže míra detekce je 100 %.

Fonetická chyba Fonetická chyba je odhalitelná vždy, pokud je splněna podmínka

$$a(w_i - w_{i+1}) \not\equiv w_i \,(mod\, k)$$

Všechny váhy jsou číslo 1 a tím pádem nám vyjde $0 \equiv -1 \,(mod\, 11)$. To nikdy kongruentní nebude, takže bude fonetická chyba vždy odhalena, tudíž je míra detekce 100 %.

Skoková dvojitá chyba Skoková dvojitá chyba bude vždy odhalena, pokud je splněna podmínka:

$$NSD(w_i + w_{i+2}, k) = 1$$

Stejně jako u dvojité chyby bude součet vah vždy číslo 2, takže míra detekce bude 0 %.

Nyní zde uvedu míru detekce všech častých chyb u daného identifikačního čísla. Míra detekce jednoduché chyby je 100 %, míra detekce transpozice vedlejších číslic je 0 %, míra detekce skokové transpozice je 0 %, míra detekce dvojité chyby je 100 %. Míra detekce fonetické chyby je 100 % a míra detekce skokové dvojité chyby je 100 %.

2.2.2 Bulharsko

Bulharské národní identifikační číslo je ve zkratce EGN. EGN je přiřazeno každému občanovi při narození, nebo při vydání certifikátu narození.

Skládá se z deseti číslic, z toho je devět identifikačních a jedna kontrolní.

Bulharské národní identifikační číslo je ve tvaru: DDMMYYAAAK.

První šestičíslí se skládá z informačních číslic o daném člověku. První dvě číslice z daného šestičíslí značí poslední dvě číslice roku narození. Další dvě číslice označují měsíc narození. Pro občany narozené mezi rokem 1900 až 1999 značí prostřední číslice pouze měsíc narození a žádné číslo nepřičítáme. Pro občany narozené před rokem 1900 je k měsíci přidáno číslo dvacet. Pro občany, kteří se narodili po roce 2000, je k číslu měsíce narození přičteno číslo čtyřicet. Další dvojčíslí označuje den narození. Dále jsou v bulharském identifikačním čísle tři číslice, díky kterým jdou rozlišit občané, kteří se narodili ve stejný den. Pokud je

toto číslo sudé, jedná se o muže, pokud liché, jedná se o ženu. Poslední číslice je kontrolní. (Kohler a Dimova, 2002, s. 331).

Kontrolní systém bulharského rodného čísla má vektor vah (2, 4, 8, 5, 10, 9, 7, 3, 6), kterým se pomocí skalárního součinu vynásobí vektor kontrolovaných číslic $(a_1, a_2 ... a_9)$, kde platí, že $(a_1, a_2 ... a_8).(2,4,8,5,10,9,7,3,6 \equiv p\,(mod\,11)$. Modulo je 11 a číslo p je jakýkoliv zbytek po dělení deseti. (Unique citizenship number, 2023)

Vytvoříme bulharské identifikační číslo pro ženu, která se narodila 12. 10. v roce 2002. První dvojčíslí bude 02, což je druhé dvojčíslí roku narození. Druhé dvojčíslí bude znamenat měsíc narození, což je 10, a k tomu přičteme číslo 40, takže druhé dvojčíslí bude 50. Třetí dvojčíslí bude 12, protože den narození je 12. 10. Řekněme, že další tři číslice budou 343. Číslo musí být liché, aby z něj šlo vyčíst, že majitelem čísla je žena. Celé číslo bude tedy 025012343. Pak musíme vypočítat poslední číslici, což je kontrolní číslice. To uděláme tím způsobem, že postupně vynásobíme čísla 0∗2+2∗4+5∗8+0∗5+1∗10+2∗9+3∗7+4∗3+3∗6 = 127. Po dělení číslem 11 zůstane zbytek 6, což bude kontrolní číslice. Tím pádem bude dané identifikační číslo 0250123436.

Jednoduchá chyba Kontrolní systém bulharského národního identifikačního čísla odhalí jednoduchou chybu, pokud je splněna následující podmínka o odhalitelnosti dané chyby:

$$NSD(w_i,k) = 1$$

V tomto případě tuto podmínku splňuje se všemi vahami, a tudíž bude míra detekce jednoduché chyby 100 %.

Transpozice vedlejších číslic Kontrolní systém bulharského národního identifikačního čísla odhalí každou transpozici vedlejších číslic, pokud je splněna následující podmínka:

$$NSD(w_j - w_{j+1}) = 1$$

Příslušné rozdíly vyšly jako čísla 2, 4, 3, 5, 1, 2, 4 a 3.

Každý z těchto rozdílů má největší společný dělitel 1, což znamená, že je podmínka vždy splněna a míra detekce je 100 %.

Skoková transpozice Kontrolní systém bulharského národního identifikačního čísla odhalí skokovou transpozici, pokud je splněna následující podmínka:

$$NSD(wi - w_{i+2}) = 1$$

Příslušné rozdíly vyšly jako čísla 6, 1, 2, 4, 3, 6 a 1.

Všechny tyto výsledné číslice mají největší společný dělitel s číslem 11 číslo 1, a proto je míra detekce 100 %.

Dvojitá chyba Kontrolní systém bulharského identifikačního čísla odhalí dvojitou chybu, pokud je splněna následující podmínka:

$$NSD(w_i + w_{i+1}) = 1$$

Příslušné rozdíly vyšly jako čísla 2, 4, 3, 5, 1, 2, 4, 3.

Všechna tato čísla mají jediný společný dělitel s číslem 11 číslo 1, a proto bude míra detekce této chyby 100 %.

Fonetická chyba Fonetická chyba v bulharském národním identifikačním čísle budu odhalena, pokud je splněna následující podmínka:

$$a(w_i - w_{i+1} \not\equiv w_i) \, (mod \, k)$$

Příslušné rozdíly vyjdou 2, 4, 3, 5, 1, 2, 4 a 3.

Vyjdou nám tedy následující rovnice. První rovnicí bude tato:

$$-2a \equiv 2 \, (mod \, 11)$$

Ekvivalentními úpravami upravíme na:

$$-a \equiv 1 \, (mod \, 11)$$

$$a \equiv -1 \, (mod \, 11)$$

$$a \equiv 10 \, (mod \, 11)$$

Tím pádem se tato číslice nesmí rovnat deseti. Ta se ale rovnat 10 nikdy nebude, protože dosazujeme čísla 0–9, takže se tato chyba neprojeví. Druhá rovnice bude tato:

$$-4a \equiv 4 \, (mod \, 11$$

Ta po podobných ekvivalentních úpravách bude vypadat takto:

$$a \equiv 10 \, (mod \, 11)$$

Toto řešení se stejně jako minulé neprojeví. Další rovnice bude ve tvaru:

$$3a \equiv 8 \, (mod \, 11)$$

Což lze upravit na:

$$-8a \equiv 8 \, (mod \, 11)$$

Tím pádem bude řešení znovu deset a také se neprojeví. Další rovnice budou tyto:

$$-5a \equiv 5 \, (mod \, 11)$$

$$a \equiv 10 \, (mod \, 11)$$

$$2a \equiv 9 \, (mod \, 11$$

$$4a \equiv 7 \, (mod \, 11)$$

$$-3q \equiv 3 \, (mod \, 11)$$

U těchto rovnic to dopadne úplně stejně jako u předchozích. Z toho vyvodíme, že daný algoritmus odhalí všechny fonetické chyby a tím pádem bude míra detekce fonetické chyby u bulharského národního identifikačního čísla 100 %.

Skoková dvojitá chyba Skoková dvojitá chyba bude v bulharském národním identifikačním čísle odhalena, pokud bude splněna následující podmínka:

$$NSD(w_i + w_{i+2}, 11) = 1$$

Příslušné rozdíly vah nám vyjdou 10, 9, 18, 14, 17, 12 a 13.

Všechny výsledné součty jsou nesoudělné s 11 a tím pádem bude míra detekce 100 %.

Veškeré časté chyby tedy budou odhaleny, míra detekce bude 100 %.

2.2.3 Lucembursko

Lucembursko má dvě národní identifikační čísla. Jedno je pro právnické osoby, jako jsou společnosti, a druhé je pro občany Lucemburska. Kvůli vhodnějšímu kontrolnímu algoritmu proberu národní identifikační čísla pro právnické osoby. (Tax ID PRO, ©2024)
Lucembursko má pro právnické osoby národní identifikační číslo, které má jedenáct číslic. Z toho je jich deset identifikačních a jedna je kontrolní. V lucemburském národním identifikačním čísle pro právnické osoby jsou všechny číslice určené jen pro identifikační potřeby, nejsou tam uložené informace podobně jako v jiných národních identifikačních číslech.
Tento národní identifikátor je regulovaný od 30. března roku 1979. Od 19. června 2013 je ve funkci nové identifikační číslo, které má 13 číslic, které jsem zmiňoval na začátku dokumentu. (Luxembourg, 2024)
Kontrolní systém lucemburského národního identifikačního čísla pro právnické osoby má vektor vah (5, 4, 3, 2, 7, 6, 5, 4, 3, 2), kterým se pomocí skalárního součinu vynásobí vektor kontrolovaných číslic $(a_1, a_2 \ldots a_{10})$, kde platí, že $(a_1, a_2 \ldots a_{10}).(5, 4, 3, 2, 7, 6, 5, 4, 3, 2) \equiv p\,(mod\,11)$. Modulo je číslo 11 a číslo p je jakýkoliv zbytek po dělení 11.

Jednoduchá chyba Kontrolní systém lucemburského národního identifikačního čísla odhalí jednoduchou chybu, pokud splňuje odvozenou podmínku o neodhalitelnosti jednoduché chyby, která zní:

$$NSD(w_i, k) \;=\; 1)$$

V tomto případě je modulo k číslo 11. Největší společný dělitel čísla 11 a všech číslic vektoru vah je 1. To znamená, že ve všech případech je splněna daná podmínka a jednoduchá chyba bude odhalena ve 100 % případů.

Transpozice vedlejších čísel Kontrolní systém lucemburského národního identifikačního čísla odhalí transpozici vedlejších čísel, pokud splňují podmínku o neodhalitelnosti transpozice vedlejších čísel, která zní:

$$NSD(w_i - w_{i+1}, k) = 1$$

Pokud od sebe odečteme všechny vedlejší číslice ve vektoru vah (5, 4, 3, 2, 7, 6, 5, 4, 3, 2) , tak vyjde buď číslo 1, nebo číslo 5.

To znamená, že je podmínka splněna vždy, protože všechna tato čísla jsou nesoudělná s číslem 11, takže je chyba ve 100 % odhalitelná.

Skoková transpozice Skoková transpozice je odhalitelná, pokud je splněna následující podmínka:

$$NSD(w_{i+2} - w_i, 11) = 1$$

. Pokud od sebe odečteme všechny takové váhy ve vektoru vah
(5, 4, 3, 2, 7, 6, 5, 4, 3, 2), tak nám vyjdou čísla 2, 2 a 4.

To znamená, že podmínka je splněna vždy, protože všechna výsledná čísla jsou nesoudělná s číslicí 11. Míra detekce je tedy 100 %.

Dvojitá chyba Dvojitá chyba lze odhalit, pokud je splněná podmínka:

$$NSD(w_i + w_{i+1}, k) = 1$$

Postupně k sobě přičteme příslušné vedlejší váhy a vyjdou nám čísla 9, 7, 5, 9, 11, 7 a 5.

Jediná dvojice vah, která nesplňuje danou podmínku, je dvojice vah 6 a 5. Můžeme překontrolovat detekci chyb pomocí následující kongruenční rovnice:

$$6j + 5j \equiv 6i + 5i \,(mod\, 11)$$
$$11j \equiv 11i \,(mod\, 11)$$

Z toho vyplývá, že jakákoliv dvojitá chyba, která vznikne u těchto dvou vah, bude neodhalitelná.

Počet číslic v daném identifikačním číslu je 10, takže počet vedlejších číslic bude 9. Z toho 8 bude mít všechny chyby odhalitelné, takže jich bude 90. Zbylá dvojice je dvojice 6 a 5, kde budou všechny chyby neodhalitelné. Tím pádem bude počet odhalitelných chyb 720.

Takže míra detekce se vypočítá: $720/810 * 100 \doteq 88{,}9\,\%$. Národního identifikační číslo Lucemburska tedy odhalí cca. 88,9 % dvojitých chyb.

Fonetická chyba Fonetická chyba je odhalitelná, pokud je splněná odvozená podmínka:

$$a(w_i - w_{i+1}) \not\equiv w_i \,(mod\, k)$$

Budeme postupně dosazovat vedlejší váhy do odvozené podmínky a z toho nám vyjdou následující kongruenční rovnic:

$$a \equiv 5 \,(mod\, 10)$$
$$a \equiv 4 \,(mod\, 10)$$
$$a \equiv 3 \,(mod\, 10)$$
$$-5a \equiv 2 \,(mod\, 10)$$
$$a \equiv 7 \,(mod\, 10)$$
$$a \equiv 6 \,(mod\, 10)$$
$$a \equiv 5 \,(mod\, 10)$$
$$a \equiv 4 \,(mod\, 10)$$
$$a \equiv 3 \,(mod\, 10)$$

Kongruenční rovnici $-5a \equiv 2\,(mod\,10)$ upravíme následujícím způsobem:

$$6a \equiv 2\,(mod\,10)$$
$$3a \equiv 1\,(mod\,10)$$
$$3a \equiv -9\,(mod\,10)$$
$$a \equiv -3\,(mod\,10)$$
$$a \equiv 7\,(mod\,10)$$

Každá vytvořená kongruenční rovnice má jedno řešení. Každé řešení budeme počítat, ale jako dvě možné chyby. Celkový počet fonetických chyb u jedné dvojice vah může být 18, ale u každé dvojice jsou dvě chyby, které jsou neodhalitelné. Vedlejších dvojic bude 9 a u každé bude 16 odhalitelných chyb. Odhalitelných chyb tedy bude $16 * 9 = 144$.

Pravděpodobnost se vypočítá jako podíl počtu odhalitelných chyb a všech možných chyb, takže $144 / 16 * 100 \doteq 88{,}9\,\%$. Míra detekce fonetických chyb u lucemburského národního identifikačního čísla bude cca. 88,9 %.

Skoková dvojitá chyba Skoková dvojitá chyba lze odhalit, pokud je splněna podmínka:

$$NSD(w_i + w_{i+2}, k) = 1$$

Dosadíme do podmínky příslušné váhy. Sčítáme buď dvě sudá, nebo dvě lichá čísla, což znamená, že součet bude vždy sudý. Součty tedy budou nesoudělné s číslem 11. Míra detekce tedy je 100 %.

Zde tedy shrnu veškeré míry detekce u častých chyb. Míra detekce jednoduché chyby bude 100 %, míra detekce transpozice vedlejších číslic bude 100 %, míra detekce skokové transpozice bude 100 %, míra detekce dvojité chyby bude 88,9 %, míra detekce fonetické chyby bude 88,9 % a míra detekce skokové dvojité chyby bude 100 %.

2.2.4 Dánsko

Dánské národní identifikační číslo se skládá z deseti číslic. Od roku 1968 si Dánsko dělalo záznam o všech, kdo bydleli v Dánsku. Tento registr se nazývá Central Person Register neboli CPR. Všichni, kdo jsou registrováni v CPR, mají přiděleno národní identifikační číslo, které se často nazývá CPR number. (Personal identification number, 2024)

Registrace byla zahájena v roce 1968 tím způsobem, že se zkombinovaly všechny národní občanské registry. Nový zkombinovaný registr začal fungovat s královským dekretem od 1. července 1972. V roce 2007 došla osobní identifikační čísla mužům, kteří se narodili 1. ledna. Pokud přišli do země imigranti, kteří neznali přesně datum narození, bylo jim přiděleno fiktivní datum narození právě 1. ledna 1965. Kvůli tomu bylo v registru na 1. ledna větší množství zápisů, takže došly možné číslice, které vyhovují danému kontrolnímu systému. S tímto systémem přidělování fiktivních národních identifikačních čísel se ale před rokem 2023 skončilo. (Nordic Co-Operation, ©2024)

Dánské národní identifikační číslo se tedy skládá z deseti číslic ve tvaru DDMMYYSSSS. DDMMYY je datum narození a tři číslice AAA jsou identifikační část, kdy se přiřazují unikátní čísla, protože se v jeden den narodí více dětí. Poslední číslice je kontrolní. (TIN Algorithms , 2019, s. 16)

Kontrolní systém dánského identifikačního čísla obsahuje vektor vah (4, 3, 2, 7, 6, 5, 4, 3, 2), kterým se pomocí skalárního součinu vynásobí vektor daného identifikačního čísla $(a_1, a_2 \dots a_9)$, kde platí, že $(a_1, a_2 \dots a_9).(4, 3, 2, 7, 6, 5, 4, 3, 2) \equiv p \,(mod\, n)$ kde modulo n je 11 a p je jakékoliv číslo.

Pokud tedy máme například muže, který se narodil 12. ledna v roce 1983, musíme nejdříve složit část, která označuje datum narození. To bude tedy dle vzoru 120183. Pak následuje část, kde se přidává číslo tak, aby se rozeznali lidé, kteří se narodili ve stejný den. Řekněme, že toto číslo je 122. Vybrali jsme číslo tak, aby bylo sudé a říkalo, že daný občan je muž. Zatím bude tedy číslo 120183122. Pak následuje kontrolní číslice.

Kontrolní číslice se vypočítá tak, že vynásobíme číslice postupně vektorem vah.

$$(4,3,2,7,6,5,4,3,2).(1,2,0,1,8,3,1,2,2) = 4*1+3*2+2*0+7*1+6*8+5*3+4*1+3*2+2*2 = 94$$

$$94 \equiv 6 \,(mod\, 11)$$

Takže kontrolní číslice bude 6 a celá národní identifikační číslice dané osoby bude 1201831226.

Jednoduchá chyba Kontrolní systém odhalí jednoduchou chybu, pokud je splněna následující podmínka:

$$NSD(w_i, k) = 1$$

Pokud se podíváme na příslušné váhy, zjistíme, že všechny jsou nesoudělné s modulem 11, a proto bude míra detekce jednoduché chyby 100 %.

Transpozice vedlejších číslic Kontrolní systém odhalí jednoduchou chybu, pokud je splněna následující podmínka:

$$NSD(w_i - w_{i+1}, k) = 1$$

Příslušné rozdíly vah budou buď číslo 1, nebo 5.

Největší společný dělitel těchto čísel a čísla 11 je číslo 1, takže je splněna podmínka odhalitelnosti chyby a míra detekce je 100 %.

Skoková transpozice Kontrolní systém odhalí skokovou transpozici, pokud je splněna následující podmínka:

$$NSD(w_i - w_{i+2}, k) = 1$$

Příslušné rozdíly vah vyjdou buď jako číslo 2, nebo jako číslo 4.

Když se na ně podíváme, tak zjistíme, že všechny jsou nesoudělné s číslem jedenáct a tím pádem je míra detekce skokové transpozice 100 %.

Dvojitá chyba Kontrolní systém odhalí dvojitou chybu, pokud je splněna následující podmínka:

$$NSD(w_i + w_{i+1}, k) = 1$$

Příslušné součty vah budou čísla 7, 5, 9, 13, 11, 9, 7 a 5.

Když se na ně podíváme, tak zjistíme, že všechny kromě jednoho vyšly nesoudělné s číslem jedenáct. U vah 6 a 5 nebyla splněna podmínka, tak musíme pomocí kongrueční rovnice ověřit, jaké chyby jsou neodhalitelné. Sestavíme následující rovnici:

$$6j + 5j \equiv 5i + 6i \,(mod\, 11)$$

To upravíme na následující rovnici.

$$11j \equiv 11i \,(mod\, 11$$

Z toho vyplývá, že jakákoliv dvojitá chyba u této dvojice bude neodhalitelná.

Číslic v identifikačním čísle je 9, takže je 8 dvojic vedlejších vah. U každé dvojice je možné udělat 90 chyb. U 7 dvojic jsou všechny chyby odhalitelné, ale u jedné dvojice jsou všechny neodhalitelné. Z toho vyplývá, že je 720 celkových možných chyb a z toho je 630 odhalitelných.

Abychom získali pravděpodobnost detekce chyby, tak musíme vydělit počet všech možných chyb s počtem všech odhalitelných chyb, tedy 630/720.100 = 87,5 %. Tím pádem bude míra detekce dvojité chyby 87,5 %.

Fonetická chyba Kontrolní systém odhalí fonetickou chybu, pokud je splněna následující podmínka:

$$j.(w_i - w_{i+1} \not\equiv w_i) \,(mod\, k)$$

Dosadíme příslušné číslice do dané podmínky a rozdíly číslo 1, nebo 5.

Díky tomu nám vyjdou následující rovnice k příslušnému řádku vah.

$$j \equiv 4 \,(mod\, 11)$$

$$j \equiv 3 \,(mod\, 11)$$

U těchto dvou rovnic rovnou vidíme řešení. Další rovnici musíme ještě upravit.

$$6j \equiv 2 \,(mod\, 11)$$

$$6j \equiv -9 \,(mod\, 11)$$

$$2j \equiv -3 \,(mod\, 11)$$

$$2j8 \,(mod\, 11)$$

$$j \equiv 4 \,(mod\, 11)$$

Další rovnice vyšly následovně.

$$j \equiv 7 \,(mod\, 11)$$

$$j \equiv 6 \,(mod\, 11)$$

$$j \equiv 5\,(mod\,11)$$

$$j \equiv 4\,(mod\,11)$$

$$j \equiv 3\,(mod\,11)$$

Identifikační číslo má 9 číslic, takže má 8 dvojic vedlejších číslic. Celkový počet chyb u jedné dvojice vedlejších číslic je 16. U každé dvojice jsou neodhalitelné 2 chyby, což znamená, že odhalitelných bude 16. Z toho vyplývá, že celkový počet možných chyb bude 126 a celkový počet odhalitelných chyb bude 112.

Pravděpodobnost detekce fonetické chyby u dánského národního identifikačního čísla vypočítáme tímto způsobem: 112/126 = 88,9 %.

Skoková dvojitá chyba Skokovou dvojitou chybu odhalíme, pokud bude splněna následující podmínka:

$$NSD(w_i + w_{i+2},k) = 1$$

Postupně budeme do této podmínky dosazovat příslušné váhy a jako součty nám vyjdou čísla 6, 10, 8 nebo 12.

Všechny vypočtené součty jsou nesoudělné s 11 a tím pádem budou všechny skokové dvojité chyby odhalené a míra detekce bude 100 %.

Na závěr uvedu shrnutí všech častých chyb a jejich míry detekce. Jednoduchá chyba má míru detekce 100 %, transpozice vedlejších čísel má míru detekce 100 %, skoková transpozice má míru detekce 100 %, dvojitá chyba má míru detekce 87,5 %, fonetická chyba má míru detekce 88,9 % a skoková dvojitá chyba má míru detekce 100 %.

2.2.5 Estonsko

Estonské národní identifikační číslo je vytvořeno z jedenácti číslic.

První číslice značí pohlaví a století, ve kterém byl občan narozený. Pokud je to číslice 1, jedná se o muže narozeného mezi lety 1899 a 1900. Číslice 2 vypovídá o tom, že se jedná o ženu narozenou mezi léty 1899 a 1900. V případě, že to je číslice 3, jde o muže narozeného mezi lety 1900 a 1999, pokud je to číslice 4, tak je to žena narozená mezi roky 1900 až 1999. Jestli je to číslice 5, jedná se o muže narozeného mezi lety 2000–2099, a pokud je to číslice 6, tak se jedná o ženu narozenou mezi lety 2000–2099.

Následují dvojčíslí značí poslední dvě číslice roku narození. To další označuje měsíc narození .
Další dvojčíslí je den narození. Následující trojčíslí značí identifikační kód pro občany, kteří se narodili ve stejný den. Poslední číslicí je kontrolní číslice.
Estonské národní číslo se tedy skládá z jedenácti číslic ve tvaru AYYMMDDSSSK. Kontrolní systém daného čísla se skládá z vektoru vah (1, 2, 3, 4 , 5, 6, 7, 8, 9, 1), kterým se pomocí skalárního součinu vynásobí vektor daného identifikačního čísla $(a_1, a_2 \ldots a_1 0)$, kde platí, že $(a_1, a_2 \ldots a_9).(1, 2, 3, 4, 5, 6, 7, 8, 9, 1) \equiv p\,(mod\,n)$, kde modulo n je 11 a p je jakékoliv číslo. Pokud zbytek po dělení jedenácti vyjde 10, tak se použije tento vektor vah: (3, 4, 5, 6 , 7, 8, 9, 1, 2, 3) a modulo zůstane pořád jedenáct. (TIN Algorithms, 2019, s.18)

Jednoduchá chyba Jednoduchá chyba je odhalena, pokud je splněna následující podmínka:

$$NSD(w_i,k) = 1$$

Protože jsou všechny váhy nesoudělné s číslem jedenáct, tak bude míra detekce estonského národního identifikačního čísla 100 %.

Transpozice vedlejších číslic Transpozice vedlejších číslic bude odhalena, pokud je splněna následující podmínka:

$$NSD(w_i + w_{i+1},k) = 1$$

Pokud budeme postupně dosazovat do tabulky příslušné váhy, příslušné rozdíly vyjdou čísla 1, nebo 8.

Každý takový rozdíl splňuje podmínku $NSD(w_{i+1} - w_i, 11) = 1$, tudíž bude míra detekce transpozice vedlejších číslic 100 %.

Skoková transpozice Podmínkou pro odhalení skokové transpozice je uvedena níže:

$$NSD(w_i - w_{i+2}, k) = 1$$

Postupným dosazením do podmínky nám vyjdou rozdíly 2, nebo 7.

Všechna takováto čísla jsou nesoudělná s číslem jedenáct, a proto bude míra detekce všech skokových transpozicí 100 %.

Dvojitá chyba Dvojitá chyba bude odhalena, pokud bude splněna následující podmínka:

$$NSD(w_i + w_{i+1}, k) = 1$$

Po dosazení příslušných vah do podmínky nám vyjdou součty 3, 5, 7, 9, 11, 13, 15, 17 a 10.

Jediný součet, který má jiné společné dělitele s modulem 11 než číslo 1, je u vah 5 a 6. Tím pádem si vytvoříme kongruenční rovnice.

$$5i + 6i \equiv 5j + 6j \; (mod\, 11)$$

$$11i \equiv 11j \; (mod\, 11)$$

Z toho vyplývá, že každá dvojitá chyba u této dvojice je neodhalitelná, takže míra detekce této chyby je 100 %.

Fonetická chyba Kontrolní systém identifikačního čísla odhalí fonetickou chybu, pokud je splněna následující podmínka:

$$j.(w_i - w_{i+1} \not\equiv w_i) \; (mod\, k)$$

Postupně dosadíme příslušné váhy a složíme následující kongruenční rovnice:

$$-j \equiv 3 \; (mod\, 11)$$

$$-j \equiv 4 \,(mod\, 11)$$
$$-j \equiv 5 \,(mod\, 11)$$
$$-j \equiv 6 \,(mod\, 11)$$
$$-j \equiv 7 \,(mod\, 11)$$
$$-j \equiv 8 \,(mod\, 11)$$
$$-j \equiv 1 \,(mod\, 11)$$
$$-j \equiv 2 \,(mod\, 11)$$

Tyto rovnice mají určitě jedno řešení, ke kterému se dostaneme po jedné úpravě rovnice. Pak nám také u vah 9 a 1 vyjde tato rovnice:

$$8j \equiv 9 \,(mod\, 11)$$

Tuto rovnici upravíme následovně:

$$-3j \equiv 9 \,(mod\, 11)$$
$$-j \equiv 9 \,(mod\, 11)$$
$$j \equiv 9 \,(mod\, 11)$$

Tato rovnice bude mít tedy také jedno řešení.

Celkový počet možných fonetických chyb u dvou vedlejších číslic je 18, z toho 2 jsou neodhalitelné, protože každé řešení kongruenční rovnice se počítá jako 2 chyby.

Máme 10 číslic v identifikačním čísle, takže 9 dvojic vedlejších vah. Z toho vyplývá, že máme celkově 162 možných chyb a z toho 144 lze odhalit. Pravděpodobnost odhalení fonetické chyby v tomto identifikačním čísle vypočítáme takto: $144/162 * 100 = 88{,}9\,\%$

Skoková dvojitá chyba Kontrolní systém estonského identifikačního čísla odhalí skokovou dvojitou chybu, pokud bude splněna podmínka:

$$NSD(w_i + w_{i+2}) = 1$$

Pokud dosadíme příslušné váhy do podmínky, tak nám vyjdou součty 8, 10, 12, 14, 16, 9, 11 a 4.

Jediné číslo, které má společného dělitele s číslem 11, bude číslo 11. Tím pádem budou neodhalitelné chyby u vah 9 a 2. Složíme následující kongruenční rovnice: $9i + 2i \equiv 9j + 2j \,(mod\, 11)$ $11i \equiv 11j \,(mod\, 11)$

Z toho vyplývá, že všechny chyby u dvojice vah 9 a 2 budou neodhalitelné. V estonském identifikačním čísle máme 10 číslic a tím pádem 8 dvojic vah, které jsou vzdálené o 2 číslice. U každé dvojice vah je 90 možných chyb. Víme tedy, že bude 720 možných chyb a z toho 630 bude odhalitelných. Pravděpodobnost odhalení skokové dvojité chyby vypočítáme následujícím způsobem: $630/720 * 100 = 88{,}9\,\%$.

Dále shrnu míru detekce všech častých chyb u estonského identifikačního čísla. Jednoduchá chyba má míru detekce 100 %, transpozice vedlejších číslic má míru detekce 100 %, dvojitá chyba má míru detekce 100 %, skoková transpozice má míru detekce 100 %, fonetická chyba má míru detekce 88,9 % a skoková dvojitá chyba má míru detekce 100 %.

2.3 Národní identifikační čísla, která mají kontrolní systém založen na modulu 23

V následující sekci popíšu, jakým způsobem se tvoří neodhalitelné chyby v kontrolním systému, který používá modulo 23. Je to větší prvočíslo, takže nemá žádné další dělitele kromě sebe a čísla 1. To je velká výhoda pro detekci vzhledem ke kritériím odhalitelnosti. Výhodou modula 23 tedy je, že bude velmi dobře detekovat časté typy chyb.
Nevýhodou je to, že zbytek po dělení číslem 23 může být číslo 0–22, což je tedy 23 čísel a z toho je dost čísel dvojciferných. Tím pádem bude tedy buď kontrolní číslice dvojciferná, nebo to bude nějaký znak, například písmeno.
Jednoduchou chybu odhalí tento algoritmus vždy, nazávisle na vahách. Předpokládáme totiž, že váhy budou jednociferné a jakékoliv jednociferné číslo bude mít největšího společného dělitele s číslem 23 číslo 1. Tím pádem bude mít jednoduchá chyba míru detekce 100 %.
Transpozice vedlejších chyb nebude vždy odhalena, pokud rozdíl vedlejších vah bude mít společného dělitele s číslem 23. Nechceme, aby tento rozdíl vyšel číslo 23, 23 a 0. Předpokládáme, že váhy budou jednociferné. Pomocí rozdílu dvou jednociferných čísel nikdy nevytvoříme číslo 23, nebo 23. Jediným způsobem, jak bychom vytvořili číslo 0, je ten, že bychom vedle sebe měli dvě stejné váhy.
Pokud tedy budeme předpokládat, že všechny váhy budou jednociferné, součtem ani rozdílem nedosáhneme čísla 23. Tím pádem skoková chyba, dvojitá chyba a dvojitá skoková chyba bude neodhalitelná, pokud příslušné váhy nebudou stejné.
Co se týče fonetické chyby, tak zde zase použijeme kritérium pro její odhalení a pomocí kongruenčních rovnic vypočítáme, jaké číslice jsou neodhalitelné. Řešením těchto rovnic budou neodhalitelné chyby.

2.3.1 Irsko

Irské národní identifikační číslo, jinak nazývané Personal Public Service Number, zkráceně PPS. Je to unikátní identifikátor pro občany v Irsku. (Government of Ireland, 2000)

Do roku 1998 bylo známo jako Revenue and Social Insurance number, zkráceně RSI No. V překladu by to znamenalo číslo sociálního pojištění a příjmu.
První RSI čísla byla vydána roku 1979 jako náhrada za tzv. PAYE čísla a Social Welfare Insurance Number, která byla používána pro daň z příjmu a sociální péči.
Všichni občané, kteří byli narozeni v roce 1971, dále mají své PPS číslo. Také lidé, kteří pracovali nebo dostávali sociální péči, mají od roku 1979 své PPS číslo.
Irské národní identifikační číslo PPS je osmičíselný kód, kde poslední číslice je kontrolní. Od roku 1994 bylo stejné číslo používané v Irsku jako studentské identifikační číslo. To způsobilo chaos, takže od roku 2001 bylo studentské identifikační číslo odstraněno a zůstalo jen PPS číslo.
K číslu se někdy přidává další písmeno. Písmeno je buď A pro jednotlivce, nebo H pro společnosti. Někdy je také přidáváno písmeno W, které je přidáno ženám, které dostaly po sňatku stejné PPS číslo jako jejich partner. Od toho se ale odstoupilo v roce 1999 kvůli problémům s rovností žen a mužů. (Personal Public Service Number, 2023)
Irské identifikační číslo má prvních 7 čísel určených pro identifikaci a 8. číslo je

kontrolní číslice.
Tento systém povoluje maximálně 10 milionů čísel, a proto byl v roce 2013 přidán další znak za kontrolní číslici, který vyjadřuje číslo pomocí písmena. Za číslo 1 se přiřadí A, za číslo 2 se přiřadí B a stejným způsobem se přiřazují ostatní čísla k písmenům kromě 0, která je přiřazena k písmenu W.
Kontrolní systém dánského identifikačního čísla obsahuje vektor vah (8, 7, 6, 5, 4, 3, 2, 9), kterým se pomocí skalárního součinu vynásobí vektor daného identifikačního čísla $(a_1, a_2 ... a_8)$, kde platí, že $(a_1, a_2 ... a_8).(8, 7, 6, 5, 4, 3, 2, 9) \equiv p\,(mod\, n)$ kde modulo n je 23 a p je jakékoliv číslo. (TIN Algorithms, 2019, s. 29–30)
Kontrolní číslice vyjde jako číslo, které je v rozmezí 0–23. K číslu A přiřadíme 0, k číslu B přiřadíme 1 a stejným způsobem popořadě přiřadíme písmeno ke každému číslu.
Vytvoříme příklad PPS čísla pro jednotlivce v Irsku. Prvních 7 číslic určíme jako číslo 1472898. Devátou číslici určíme jako číslo 6 a k tomu přiřadíme písmeno F a poté dopočítáme kontrolní číslice. Vynásobíme vektor číslic s vektorem vah a vyjde nám tento výraz: $8*1+4*7+7*6+2*5+8*4+9*3+8*2+6*9 = 217$. Vypočítáme $217\ \%\ 23\ =\ 10$ a tím pádem přiřadíme k číslu 10 písmeno J. Číslo tedy bude ve tvaru 1472898JF.

Jednoduchá chyba Podmínka pro odhalitelnost jednoduché chyby je následující:

$$NSD(w_i, k) = 1$$

Tuto podmínku splňují všechny váhy v irském národním identifikačním čísle, takže míra detekce je 100 %.

Transpozice vedlejších číslic Podmínka pro odhalitelnost transpozice vedlejších je následující:

$$NSD(w_i - w_{i+1}, k) = 1$$

Pokud postupně od sebe odečteme všechny příslušné váhy, tak nám vyjdou čísla 1, nebo 7. U obou těchto čísel vyjde, že největším společným dělitelem těchto čísel a čísla 23 je 1. Tím pádem je míra detekce všech transpozicí vedlejších čísel u irského národního identifikačního čísla 100 %.

Dvojitá chyba Pro odhalení dvojité chyby bude platit následující podmínka:

$$NSD(w_i + w_{i+1}, k) = 1$$

Postupně k sobě přičteme příslušné vedlejší váhy. Vyjdou nám čísla 15, 13, 11, 9, 7 a 5. Tato čísla mají největší společný dělitel s číslem 23 číslo 1, takže míra detekce dvojité chyby u irského národního identifikačního čísla je 100 %.

Skoková transpozice Kontrolní systém odhalí skokovou transpozici, pokud bude splněna následující podmínka:

$$NSD(w_i - w_{i+1}, k) = 1$$

Postupně od sebe odečteme příslušné váhy. Vyjdou nám čísla 2 a 6. Obě tato čísla mají největší společný dělitel s číslem 23 číslo 1, takže míra detekce u skokové transpozice u irského národního identifikačního čísla je 100 %.

Fonetická chyba Podmínka pro odhalitelnost fonetické chyby je následující:

$$a(w_i - w_{i+1} \not\equiv w_i) \ (mod\, k)$$

Příslušné rozdíly vyjdou čísla 1, nebo 7. Z toho nám tedy vyjdou následující kongruenční rovnice.

$$a \equiv 8 \ (mod\, 23)$$
$$a \equiv 7 \ (mod\, 23)$$
$$a \equiv 6 \ (mod\, 23)$$
$$a \equiv 5 \ (mod\, 23)$$
$$a \equiv 4 \ (mod\, 23)$$
$$a \equiv 3 \ (mod\, 23)$$
$$-7a \equiv 2 \ (mod\, 23)$$

U prvních 6 rovnic je jasné, že bude vždy jedno řešení, takže vlastně 2 neodhalitelné chyby z celkových 18. Poslední rovnici upravíme následujícím způsobem:

$$-7a \equiv 2 \ (mod\, 23)$$
$$16a \equiv 2 \ (mod\, 23)$$
$$8a \equiv 1 \ (mod\, 23)$$
$$8a \equiv -22 \ (mod\, 23)$$
$$4a \equiv -11 \ (mod\, 23)$$
$$4a \equiv 12 \ (mod\, 23)$$
$$a \equiv 3 \ (mod\, 23)$$

Každá rovnice má tedy řešení. Číslic v irském národním identifikačním čísle je 8, takže je 7 dvojic vedlejších vah. Každá dvojice vah má 2 neodhalitelné chyby z celkového počtu 18 možných chyb. Celkový počet možných chyb tedy bude 126 a počet odhalitelných chyb bude 112. Pravděpodobnost detekce fonetické chyby tedy bude $112/126 * 100 = 88{,}9$ %.

Skoková dvojitá chyba Skoková dvojitá chyba má následující podmínku pro odhalitelnost:

$$NSD(w_i, w_{i+2}, k) = 1$$

Postupně dosadíme do podmínky příslušné váhy. Vyjdou nám součty 14, 12, 8, 6, 12 a 10. Všechna tato čísla mají největší společný dělitel s číslem 23 číslo 1. Míra detekce skokové dvojité chyby u irského rodného čísla bude 100 %.
Zde shrnu míru detekce všech typů častých chyb u irského národního identifikačního čísla. Míra detekce jednoduché chyby je 100 %, míra detekce transpozice vedlejších číslic je 100 %, míra detekce dvojité chyby je 100 %, míra detekce skokové transpozice je 100 %, míra detekce fonetické chyby je 88,9 % a míra detekce skokové dvojité chyby je 100 %.

3. Relevatní kapitoly z RVP ZV

3.1 Cílové zaměření vzdělávací oblasti z matematiky

V této kapitole budu probírat, jakým způsobem lze zařadit kontrolní číslice a jejich systémy do rámcového vzdělávacího programu a proč vlastně jsou vhodné pro zařazení do výuky 2. stupně základní školy.
Uvedu, jaké kapitoly matematiky se studenti při probírání kontrolních číslic a součtů naučí. Zamyslím se nad tím, pro jaké ročníky bude probírání těchto témat vhodné a jakým způsobem bude tato látka žáky rozvíjet.
Nejdříve se obecně podívám na cílové zaměření vzdělávacích oblastí a vyberu ty, které se nejvíce hodí k tomuto tématu. Nejvíce se dle mého názoru bude hodit tato věta: „rozvíjení spolupráce při řešení problémových a aplikovaných úloh vyjadřujících situace z běžného života a následně k využití získaného řešení v praxi; k poznávání možností matematiky a skutečnosti, že k výsledku lze dospět různými způsoby"(Ministerstvo školství, mládeže a tělovýchovy ČR, 2022, s. 32).
Myslím si, že toto téma bude velmi vhodné na vytvoření pracovních listů, na kterých budou studenti pracovat ve skupinách. Bude to hodně o diskuzi, přemýšlení a zkoušení různých metod a algoritmů metodou pokus omyl.
Jde o to, představit si reálnou situaci v počítačovém systému. Systém pomocí algoritmů kontroluje, jestli je číslo napsáno správně. Jejich úkolem bude pochopit, jak vlastně počítač může zkontrolovat to, co napsal člověk, a jestli počítač vždy odhalí, zda člověk udělá chybu, nebo mu to někdy unikne.
S tímto pochopením velmi souvisí tato věta z RVP ZV: „rozvíjení kombinatorického a logického myšlení, ke kritickému usuzování a srozumitelné a věcné argumentaci prostřednictvím řešení matematických". (Ministerstvo školství, mládeže a tělovýchovy ČR, 2022, s. 32)
Na to, aby student dokázal odhalit funkčnost těchto algoritmů, je potřeba se zamyslet nad tím, kolik je možností různých chyb a kolik jich počítač dle daného algoritmu může odhalit. Na to je potřeba značná dávka logického a kombinatorického přemýšlení, které si budou studenti procvičovat a rozvíjet při probírání tématu kontrolních číslic a součtů.
Také se bude hodit následující cílové zaměření: „provádění rozboru problému a plánu řešení, odhadování výsledků, volba správného postupu k vyřešení problému a vyhodnocování správnosti výsledku vzhledem k podmínkám úlohy nebo problému". (Ministerstvo školství, mládeže a tělovýchovy ČR, s. 32)
Studenti pro pochopení kontrolních systémů a jejich úspěšnost detekce chyb budou muset postupovat velmi systematicky a přemýšlet, jestli jejich návrh a domněnky vlastně fungují a jsou správné.
Určitě se bude velmi hodit toto cílové zaměření – „rozvíjení paměti žáků prostřednictvím numerických výpočtů a osvojování si nezbytných matematických vzorců a algoritmů". (Ministerstvo školství, mládeže a tělovýchovy ČR, 2022, s. 31)
V problematice kontrolních součtů a číslic se používají kontrolní algoritmy, které jsou sled různých matematických operací za sebou, díky kterým se zkontroluje validita kontrolovaného čísla. Dané matematické operace jsou většinou základní jako třeba sčítání, odčítání, násobení a dělení.

Myslím si, že studenti si mohou jak procvičit základní operace, tak pochopit, jak fungují dané alogritmy a proč fungují. Mohou se pokusit zapamatovat si různé kontrolní algoritmy jak Česka, tak dalších zemí a experimentovat, jestli číslo, které jim bylo zadáno, nebo které si vymyslí, je doopravdy identifikační číslo vybrané země.

3.2 Očekávané výstupy z matematiky

Nejdřív se zamyslím nad tím, jak se mohou zařadit kontrolní číslice a součty do RVP základní školy. Projdu očekávané výstupy z RVP ZV a vyberu ty, které se budou rozvíjet a procvičovat při probírání tématu kontrolních číslic a součtů.
Prvním výstupem, který vyberu, bude tento: „M-9-1-0 zaokrouhluje a provádí odhady s danou přesností, účelně využívá kalkulátor". (Ministerstvo školství, mládeže a tělovýchovy ČR, 2022, s. 35)
V tomto tématu se sice nebude vyloženě zaokrouhlovat, ale je nutné provádět odhady v průběhu zkoumání a také je velmi potřebné používat kalkulačku. Bez ní by výpočty byly velmi zdlouhavé a nejsem si jistý, jestli by se to všechno v nějakém adekvátním časovém rozpětí stihlo.
Dalším velmi důležitým výstupem je tento: „M-9-1-03 modeluje a řeší situace s využitím dělitelnosti v oboru přirozených čísel"(Ministerstvo školství, mládeže a tělovýchovy ČR, 2022, s. 35)

Tento výstup je asi nejdůležitější pro toto téma.
V celém tématu kontrolních číslic a součtů se používá dělitelnost různých čísel. Prakticky ve všech identifikačních číslech se jako hlavní nástroj odhalení chyb používá dělení různými čísly.
Je důležité znát pojem prvočíslo a v tomto případě se velmi prakticky používá. U odhalení různých typů chyb kontrolním systémem se používá největší společný dělitel, takže studenti si vyzkouší funkci tohoto konceptu v hodně praktickém kontextu.
Dalším důležitým výstupem je tento: „M-9-1-06 řeší aplikační úlohy na procenta (i pro případ, že procentová část je větší než celek)". (Ministerstvo školství, mládeže a tělovýchovy ČR, 2022, s. 35)
Hojně se využívá v počítání míry detekce různých chyb jednoho kontrolního systému.
Je nutné vypočítat, jaký podíl z celkových chyb, které mohou v identifikačním čísle nastat, dokáže kontrolní algoritmus reálně odhalit.
Dalším velmi důležitým výstupem, který se hodně využívá v tématu kontrolní součty a číslice, je tento: „M-9-4-01 užívá logickou úvahu a kombinační úsudek při řešení úloh a problémů a nalézá různá řešení předkládaných nebo zkoumaných situací". (Ministerstvo školství, mládeže a tělovýchovy ČR, 2022, s. 38)
Ve zkoumání, jak fungují kontrolní algoritmy a jaké procento z celkových chyb dokáží odhalit, je velmi potřebné logické myšlení a kombinační úsudek. Je potřeba promyslet, kolik vlastně celkových chyb jednoho typu může v jednom identifikačním čísle nastat a kolik jich daný kontrolní algoritmus odhalí.

3.3 Cílové zaměření vzdělávací oblasti z informatiky

Téma kontrolní součty a číslice lze také dle mého názoru velmi dobře využívat i v předmětu informatika. Projdu RVP ZV pro tento předmět a pokusím se najít cílové zaměření vzdělávací oblasti, které by se aplikovalo na studium tématu kontrolní číslice a součty.
Prvním takovým cílovým zaměřením vzdělávací oblasti, které se bude aplikovat na téma kontrolní součty a číslice, je toto: „Vzdělávání v dané vzdělávací oblasti směřuje k utváření a rozvíjení klíčových kompetencí tím, že vede žáka k systémovému přístupu při analýze situací a jevů světa kolem něj". (Ministerstvo školství, mládeže a tělovýchovy ČR, 2022, s. 39)
Při zkoumání, jak fungují různé kontrolní systémy a jejich algoritmy, je potřeba velmi systematický přístup.
Je to procedura, která se využívá ve všech zemích ve většině různých internetových formulářích a v mnoha databázích, a je to princip, který se používá v mnoha dalších kódech kromě národních identifikačních čísel.

3.4 Očekávané výstupy z informatiky

V této sekci projdu RVP ZV z informatiky a pokusím se najít očekávané výstupy, které se aplikují na toto téma.
První z takových výstupů je tento: „I-9-1-01 získá z dat informace, interpretuje data, odhaluje chyby v cizích interpretacích dat". (Ministerstvo školství, mládeže a tělovýchovy ČR, 2022, s. 42)
Studenti mohou z různých národních identifikačních čísel získat mnoho informací. Pohlaví, datum narození a jiné důležité informace, které se dají vyčíst z národního identifikačního čísla.
Pak se také na toto téma aplikuje tento výstup: „I-9-2-01 po přečtení jednotlivých kroků algoritmu nebo programu vysvětlí celý postup; určí problém, který je daným algoritmem řešen". (Ministerstvo školství, mládeže a tělovýchovy ČR, 2022, s. 42)
Každý kontrolní algoritmus různých kontrolních systémů národního identifikačního čísla se dělí na více kroků, pomocí kterých dokážeme ověřit, jestli je dané číslo správně napsáno.
Dá se tedy na tomto příkladě zkoumat algoritmus jako takový a k čemu se používá.

Závěr

V této bakalářské práci jsem popsal příklady různých národních identifikačních čísel zemí Evropy. Výběr zemí zahrnoval různé druhy kontrolních systémů, kdy se kontrolní číslice tvořily různými způsoby a používala se dělitelnost různých číslic.
Pomocí další literatury jsem odvodil kritéria pro odhalení nejčastějších typů chyb, které lidé dělají. Tato kritéria jsem aplikoval na všechny vybrané země a pomocí odvozených matematických nástrojů jsem spočítal míru detekce jednotlivých typů nejčastějších chyb.
Testoval jsem, jaký je rozdíl v kontrolních systémech založených na modulu 10, 11 nebo většího čísla, jako je třeba 23. Zjistil jsem, že je značně velký rozdíl míry detekce mezi kontrolními systémy založenými na modulu 10 a ostatními. Kontrolní systémy založené na modulu 10 nemají tak účinnou obranu proti chybám, ale mají jiné výhody. Kontrolní číslice vyjde jen jako jednociferné číslo a tím pádem se nemusí řešit složitější zápis, jako je to u ostatních národních identifikačních čísel.
Kontrolní systémy založené na modulu 11 jsou dobrým kompromisem mezi mírou detekce a složitostí vytvoření identifikačního čísla. Takové kontrolní systémy jsou velmi účinné na detekci častých chyb. Kontrolní číslice vyjde jednociferná, až na zbytek 10, kde se musí použít speciální znak.
Kontrolní systémy založené na větších prvočíselných modulech, jako je třeba 23, mají velmi účinnou detekci proti častým typům chyb. Jejich nevýhodou je to, že kontrolní číslice mohou být dvojciferná čísla a je dost časté, že se nahrazují speciálními znaky, jako jsou písmena.
Zjistil jsem, že toto téma je vhodné pro výuku na základních školách 2. stupně. Aplikuje se na něj mnoho ze součástí RVP základní školy – matematika a informatika 2. stupně. Lze využít znalosti dělitelnosti a kombinatoriky, je třeba používat logické myšlení, rozumět algoritmům a aplikovat je na různé situace.

Literatura

GOVERNMENT OF IRELAND. *Ireland – Information on Tax Identification Numbers*. Online, PDF. OECD, 2000. Dostupné z: <https://www.oecd.org/tax/automatic-exchange/crs-implementation-and-assistance/tax-identification-numbers/Ireland-TIN.pdf>. [cit. 2024-03-12].

GRACZYK, K. *Rejestr PESEL*. Online. In: Ministerstwo Cyfryzacji, 19. 12. 2019. Dostupné z: <https://www.gov.pl/web/cyfryzacja/rejestr-pesel1>. [cit. 2024-03-12].

JOSEPH, A. G. Error Detection Methods. Online. *ACM Comput. Surv.*, 1996, 28(3), 504–517. ISSN 0360-0300. Dostupné z: <https://doi.org/10.1145/243439.243457>. [cit. 2023-06-15].

KOHLER, Iliana a DIMOVA, Mariana. Integrated Information Systém for Demographic Statistics 'ESGRAON-TDS' in Bulgaria. Online. *Demographic research* 2002, 6(12), 325–354. Dostupné z: <https://www.demographic-research.org/articles/volume/6/12/>. [cit. 2024-03-16].

KŘÍŽEK, M.; SOMER, L. a ŠOLCOVÁ, A., 2018. *Kouzlo čísel*. Praha: Academia. ISBN 978-80-200-1610-2. [cit. 2023-05-12].

Luxembourg – Information on Tax Identification Numbers. Online, PDF. Luxembourg: Administration des contributions directes. Dostupné z: <https://www.oecd.org/tax/automatic-exchange/crs-implementation-and-assistance/tax-identification-numbers/Luxembourg-TIN.pdf>. [cit. 2024-03-12].

MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY ČR. *Upravený rámcový vzdělávací program (RVP) pro základní vzdělávání (ZŠ) – 2023*. Dostupné z: <https://www.edu.cz/rvp-ramcove-vzdelavaci-programy/ramcovy-vzdelavacici-program-pro-zakladni-vzdelavani-rvp-zv/>. [cit. 2023-06-15].

MINISTERSTVO VNITRA ČESKÉ REPUBLIKY. *Přidělení rodného čísla*.Online. 12. 9. 2023. Dostupné z: <https://www.mvcr.cz/clanek/prideleni-rodneho-cisla-931400.aspx>. [cit. 2024-03-16].

MINISTERSTVO VNITRA ČESKÉ REPUBLIKY. *Rodné číslo*. Online. 8. 10. 2020. Dostupné z: <https://www.mvcr.cz/clanek/rady-a-sluzby-dokumenty-rodne-cislo.aspx>. [cit. 2024-03-16].

MINISTRY OF FINANCE OF POLAND. *POLAND – Information on Tax Identification Numbers.*. Online, PDF. OECD, 2023. Dostupné z: <https://www.oecd.org/tax/automatic-exchange/crs-implementation-and-assistance/tax-identification-numbers/Poland-TIN.pdf>. [cit. 2024-03-12].

NORDIC CO-OPERATION. *Danish civil registration number (CPR number)*. Online. © 2024. Dostupné z: <https://www.norden.org/en/info-norden/danish-civil-registration-number-cpr-number>. [cit. 2023-06-15].

Personal identification number (Denmark). Online. In: Wikipedia: the free encyclopedia. San Francisco (CA): Wikimedia Foundation, 2001-, 2024. Dostupné z: <https://en.wikipedia.org/wiki/Personal_identification_number_(Denmark)>. [cit. 2024-04-06].

Personal Public Service Number. Online. In: Wikipedia: the free encyclopedia. San Francisco (CA): Wikimedia Foundation, 2001-, 2024. Dostupné z: <https://en.wikipedia.org/wiki/Personal_Public_Service_Number>. [cit. 2024-04-06].

PESEL. Online. In: Wikipedia: the free encyclopedia. San Francisco (CA): Wikimedia Foundation, 2001-, 2023. Dostupné z: https://en.wikipedia.org/wiki/PESEL>. [cit. 2023-08-07].

REGIONAL MINISTER. *The procedure for creating, distributing and issuing personal codes*. Online. In: Riigi Teataja, 28. 1. 2005. Dostupné z: <https://www.riigiteataja.ee/akt/106032012004>. [cit. 2023-06-15].

TAX ID PRO. *Luxembourg Tax ID Numbers*. Online. © 2024. Dostupné z: <https://taxid.pro/docs/countries/luxembourg>. [cit. 2023-06-15].

TIN Algorithms - Public - Functional Specification. Online. DG TAXUD, 27. 3. 2019. Dostupné z: <https://ec.europa.eu/taxation_customs/tin/specs/FS-TIN%20Algorithms-Public.docx?v=1697587200031>. [cit. 2024-03-12].

Unique citizenship number. Online. In: Wikipedia: the free encyclopedia. San Francisco (CA): Wikimedia Foundation, 2001-, 2023. Dostupné z: https://en.wikipedia.org/wiki/Unique_citizenship_number. [cit. 2023-08-16].

Přílohy

1.Typy chyb a jejich relativní frekvence

Typ chyby	Forma	Relativní frekvence
Jednotlivá chyba	$a \to b$	79,1%
Transpozice vedlejších číslic	$ab \to ba$	10,2%
Skoková transpozice	$abc \to cba$	0,8%
Dvojitá chyba	$aa \to bb$	0,5%
Fonetická chyba	$a0 \leftrightarrow 1a$	0,5%
Skoková dvojitá chyba	$aca \to bcb$	0,3%

2.Typy chyb a jejich podmínka odhalitelnosti

Typ chyby	Forma	Podmínka odhalitelnosti
Jednotlivá chyba	$a \to b$	$NSD(w_i, k) = 1$
Transpozice vedlejších číslic	$ab \to ba$	$NSD(w_i - w_{i+1}, k) = 1$
Skoková transpozice	$abc \to cba$	$NSD(w_i - w_{i+2}, k) = 1$
Dvojitá chyba	$aa \to bb$	$NSD(w_i + w_{i+1}, k) = 1$
Fonetická chyba	$a0 \leftrightarrow 1a$	$a_i.(w_i - w_{i+1}) \not\equiv w_i \, (mod\, k)$
Skoková dvojitá chyba	$aca \to bcb$	$NSD(w_i + w_{i+2}, k) = 1$