O tajných zprávách, šifrách a prvočíslech

OSMA, VŠB TU, Ostrava!!!

Mirko Rokyta

(. . . devátá, s ódou na prvočísla, **5.3.2024**)

KMA MFF UK Praha

0. Úvod

... aneb

"Taweje blajmezhe blu Uzno."

0. Úvod

... aneb

"Taweje blajmezhe blu Uzno."

"Dobrá kniha neprozradí své tajemství najednou." (Stephen King)

0. Úvod

... aneb

"Taweje blajmezhe blu Uzno."

"Dobrá kniha neprozradí své tajemství najednou." (Stephen King)

Motto:

"Je vůbec k něčemu matematika v reálném životě?"

(Typická reakce běžného občana.)

... aneb

"Taweje blajmezhe blu Uzno."

"Dobrá kniha neprozradí své tajemství najednou." (Stephen King)

Motto:

"Je vůbec k něčemu matematika v reálném životě?"

(Typická reakce běžného občana.)

Krátká verze přednášky: Většinou ani moc ne.

Děkuji za pozornost.

0. Úvod

... aneb

"Taweje blajmezhe blu Uzno."

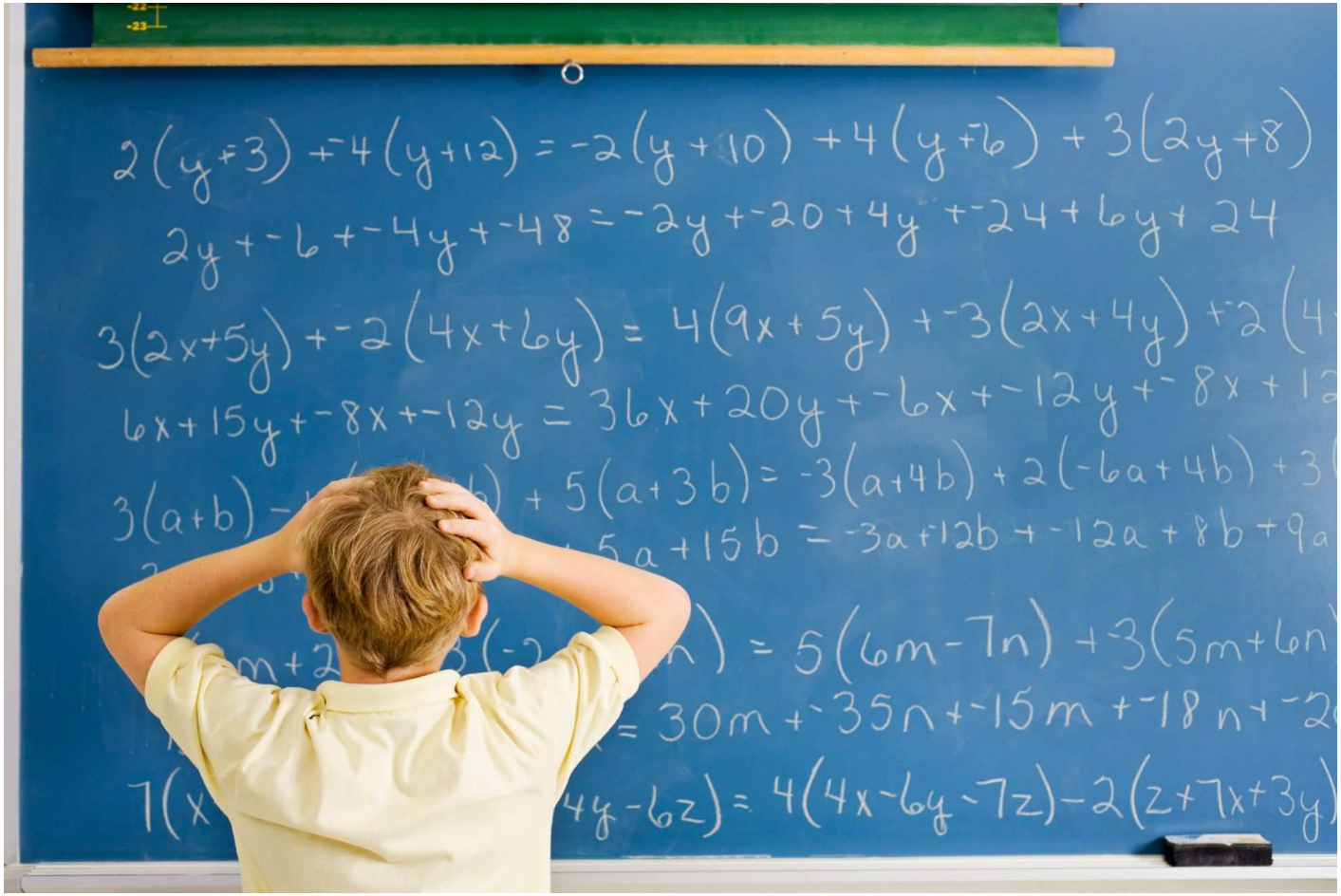
"Dobrá kniha neprozradí své tajemství najednou." (Stephen King)

Motto 2:

"Je vůbec k něčemu matematika v reálném životě?"

(Typická reakce běžného občana.)

Delší verze přednášky: Docela ano.



Dnes to sice bude o matematice, která k "něčemu je", ale kromě toho se seznámíme se spoustou výsledků, které lze označit jako "čistě teoretické" či dokonce "krásné".

Šifra?

Šifra?

- Z čeho vzniklo slovo "šifra"?

Šifra?

- Z čeho vzniklo slovo "šifra"? Ze slova "cifra".

Šifra?

- Z čeho vzniklo slovo "šifra"? Ze slova "cifra".
- "Šifrovat" ("cifrovat") v jisté době znamenalo "nahradit písmena číslicemi".

Šifra?

- Z čeho vzniklo slovo "šifra"? Ze slova "cifra".
- "Šifrovat" ("cifrovat") v jisté době znamenalo "nahradit písmena číslicemi".
- *Z čeho vzniklo slovo "cifra"?*

Šifra?

- Z čeho vzniklo slovo "šifra"? Ze slova "cifra".
- "Šifrovat" ("cifrovat") v jisté době znamenalo "nahradit písmena číslicemi".
- *Z čeho vzniklo slovo "cifra"? Z arabského slova "as-sifr", majícího svůj původ v sanskrtu*

Šifra?

- Z čeho vzniklo slovo "šifra"? Ze slova "cifra".
- "Šifrovat" ("cifrovat") v jisté době znamenalo "nahradit písmena číslicemi".
- *Z čeho vzniklo slovo "cifra"? Z arabského slova "as-sifr", majícího svůj původ v sanskrtu a označujícího nejtajemnější ze všech čísel, a sice*

Šifra?

- Z čeho vzniklo slovo "šifra"? Ze slova "cifra".
- "Šifrovat" ("cifrovat") v jisté době znamenalo "nahradit písmena číslicemi".
- *Z čeho vzniklo slovo "cifra"? Z arabského slova "as-sifr", majícího svůj původ v sanskrtu a označujícího nejtajemnější ze všech čísel, a sice číslo* ***nula****.*

Šifrování nebo kódování?

Šifrování nebo kódování?

- Šifrování je proces změny informace (typicky převod otevřeného textu na šifrovaný) tak, aby k nim neměly přístup neoprávněné osoby.

Šifrování nebo kódování?

- Šifrování je proces změny informace (typicky převod otevřeného textu na šifrovaný) tak, aby k nim neměly přístup neoprávněné osoby. Cílem šifrování je uchování tajemství

Šifrování nebo kódování?

- Šifrování je proces změny informace (typicky převod otevřeného textu na šifrovaný) tak, aby k nim neměly přístup neoprávněné osoby. Cílem šifrování je uchování tajemství (tj. získat původní informaci má být těžké).

Šifrování nebo kódování?

- Šifrování je proces změny informace (typicky převod otevřeného textu na šifrovaný) tak, aby k nim neměly přístup neoprávněné osoby. Cílem šifrování je uchování tajemství (tj. získat původní informaci má být těžké).
- Kódování i šifrování mají společné to, že mění podobu textu.

Šifrování nebo kódování?

- Šifrování je proces změny informace (typicky převod otevřeného textu na šifrovaný) tak, aby k nim neměly přístup neoprávněné osoby. Cílem šifrování je uchování tajemství (tj. získat původní informaci má být těžké).
- Kódování i šifrování mají společné to, že mění podobu textu. Cílem kódování však není utajení, pouze spolehlivý záznam či přenos zprávy

Šifrování nebo kódování?

- Šifrování je proces změny informace (typicky převod otevřeného textu na šifrovaný) tak, aby k nim neměly přístup neoprávněné osoby. Cílem šifrování je uchování tajemství (tj. získat původní informaci má být těžké).
- Kódování i šifrování mají společné to, že mění podobu textu. Cílem kódování však není utajení, pouze spolehlivý záznam či přenos zprávy(např. převod zvuku či obrazu "do nul a jedniček").

- První šifrovací přístroj: starořecká **skytalé**.

- První šifrovací přístroj: starořecká **skytalé**. (Válec, na který se navinul kožený proužek).

- První šifrovací přístroj: starořecká **skytalé**. (Válec, na který se navinul kožený proužek).

- První šifrovací přístroj: starořecká **skytalé**. (Válec, na který se navinul kožený proužek).

Snadné **"prolomení šifry"**: navinuli proužek na kužel.

- První šifrovací přístroj: starořecká **skytalé**. (Válec, na který se navinul kožený proužek).

  Snadné **"prolomení šifry"**: navinuli proužek na kužel.

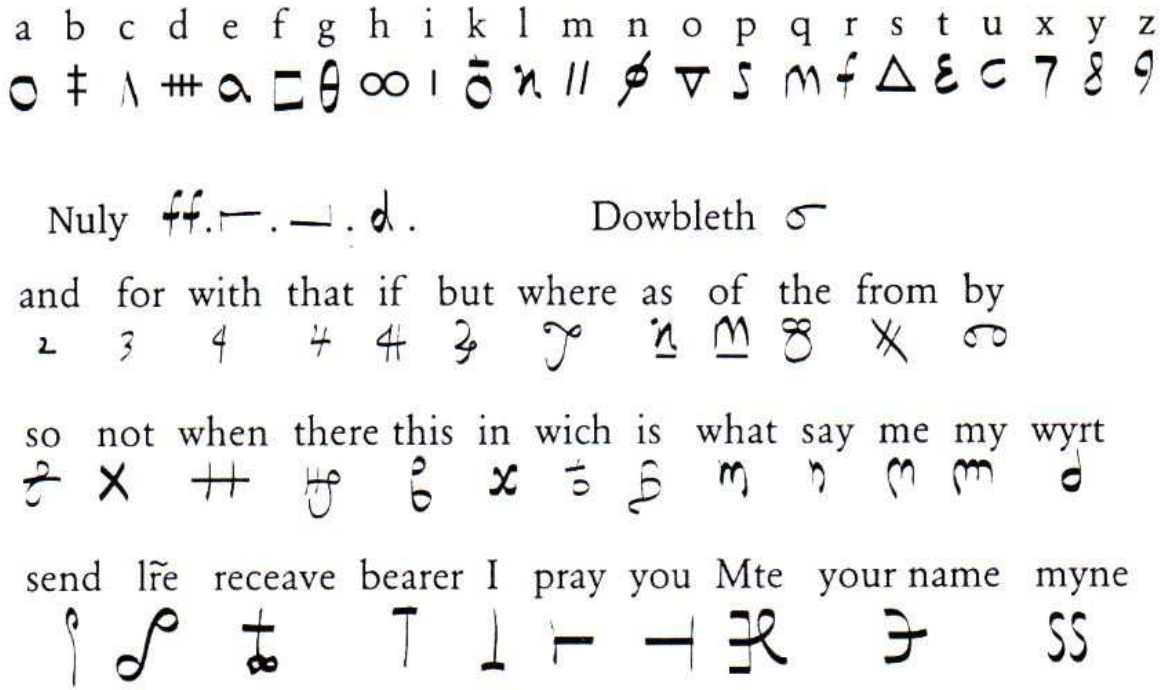
- Další historie šifrování se víceméně vždy opírala o náhradu konkrétního znaku jiným znakem. . .

- Jeden z prvních: Césarova šifra (ano, Gaius Julius...):

- Jeden z prvních: Césarova šifra (ano, Gaius Julius...): každé písmeno zprávy nahradil písmenem, které bylo v abecedě o tři místa dále.

- Jeden z prvních: Césarova šifra (ano, Gaius Julius...): každé písmeno zprávy nahradil písmenem, které bylo v abecedě o tři místa dále.
- Šifra Marie Stuartovny:

- Jeden z prvních: Césarova šifra (ano, Gaius Julius...): každé písmeno zprávy nahradil písmenem, které bylo v abecedě o tři místa dále.
- Šifra Marie Stuartovny:



Jedna z klasických šifrovacích tabulek (cca 1976. . .)

A = E	J = D	S = Z
B = P	K = H	T = C
C = T	L = R	U = O
D = J	M = N	V = W
E = A	N = M	W = V
F = G	O = U	X = Q
G = F	P = B	Y = I
H = K	Q = X	Z = S
I = Y	R = L	

Jedna z klasických šifrovacích tabulek (cca 1976. . .)

A = E	J = D	S = Z
B = P	K = H	T = C
C = T	L = R	U = O
D = J	M = N	V = W
E = A	N = M	W = V
F = G	O = U	X = Q
G = F	P = B	Y = I
H = K	Q = X	Z = S
I = Y	R = L	

Jupli jam, deh za neca? Nena jmaz jutare kashi.

Jedna z klasických šifrovacích tabulek (cca 1976. . .)

A = E	J = D	S = Z
B = P	K = H	T = C
C = T	L = R	U = O
D = J	M = N	V = W
E = A	N = M	W = V
F = G	O = U	X = Q
G = F	P = B	Y = I
H = K	Q = X	Z = S
I = Y	R = L	

Jupli jam, deh za neca? Nena jmaz jutare kashi.

Dobry den, jak se mate? Mame dnes docela hezky.

Jedna z klasických šifrovacích tabulek (cca 1976. . .)

A = E	J = D	S = Z
B = P	K = H	T = C
C = T	L = R	U = O
D = J	M = N	V = W
E = A	N = M	W = V
F = G	O = U	X = Q
G = F	P = B	Y = I
H = K	Q = X	Z = S
I = Y	R = L	

Jupli jam, deh za neca? Nena jmaz jutare kashi.

Dobry den, jak se mate? Mame dnes docela hezky.

Taweje blajmezhe blu Uzno.

Jedna z klasických šifrovacích tabulek (cca 1976. . .)

A = E	J = D	S = Z
B = P	K = H	T = C
C = T	L = R	U = O
D = J	M = N	V = W
E = A	N = M	W = V
F = G	O = U	X = Q
G = F	P = B	Y = I
H = K	Q = X	Z = S
I = Y	R = L	

Jupli jam, deh za neca? Nena jmaz jutare kashi.

Dobry den, jak se mate? Mame dnes docela hezky.

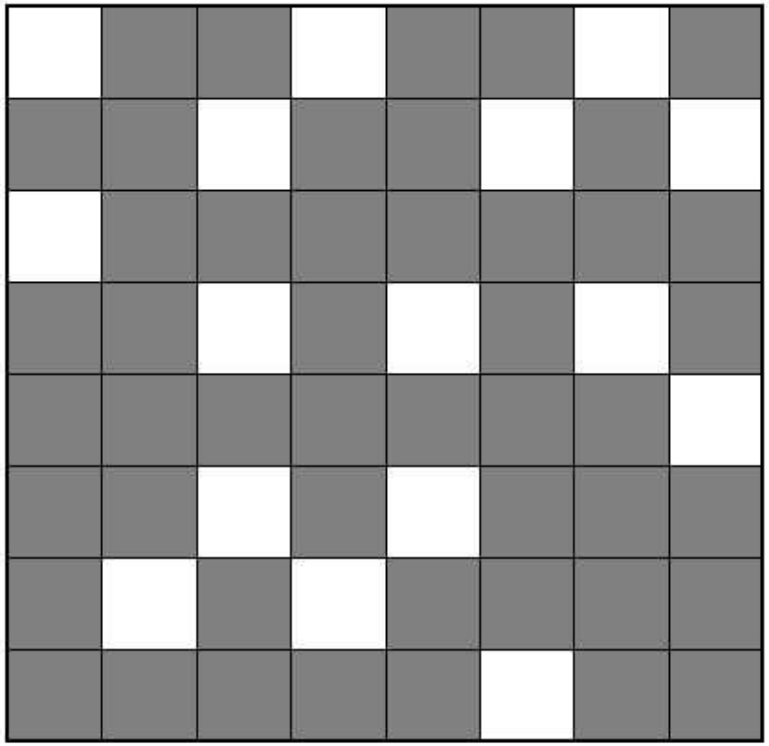
Taweje blajmezhe blu Uzno.

Devata prednaska pro Osmu.

Šifrování pomocí šifrovací mřížky

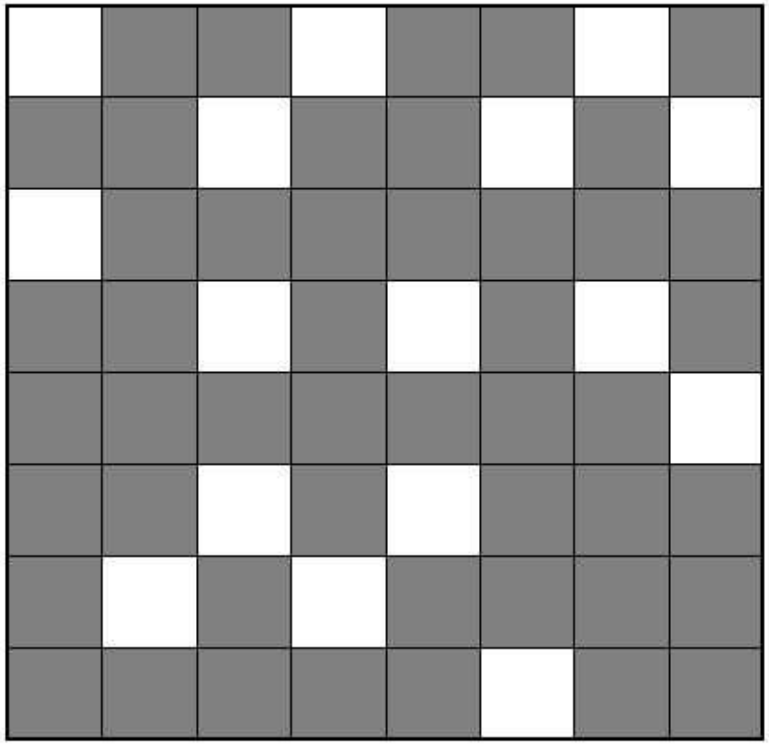
K	A	E	O	V	M	P	S
E	M	E	N	S	J	E	P
O	I	R	N	K	A	E	Š
CH	M	D	T	N	Ě	E	N
A	Á	A	Z	M	Í	H	J
Í	U	V	S	Y	T	S	V
E	Š	L	Š	T	K	Ý	Ě
K	É	EŘ	K	M	Í	D	R

Šifrování pomocí šifrovací mřížky



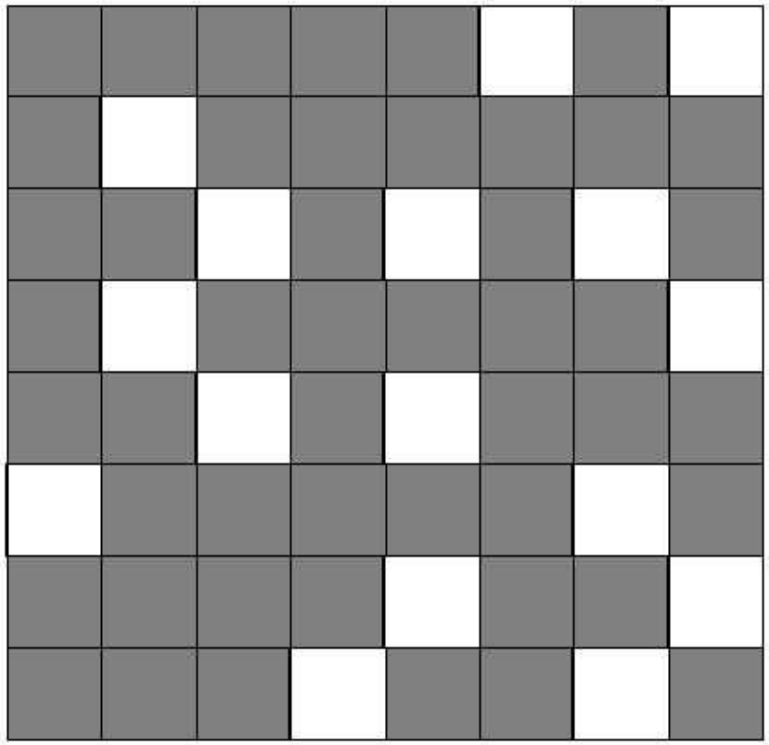
K	A	E	O	V	M	P	S
E	M	E	N	S	J	E	P
O	I	R	N	K	A	E	Š
CH	M	D	T	N	Ě	E	N
A	Á	A	Z	M	Í	H	J
Í	U	V	S	Y	T	S	V
E	Š	L	Š	T	K	Ý	Ě
K	É	EŘ	K	M	Í	D	R

Šifrování pomocí šifrovací mřížky



K	A	E	O	V	M	P	S
E	M	E	N	S	J	E	P
O	I	R	N	K	A	E	Š
CH	M	D	T	N	Ě	E	N
A	Á	A	Z	M	Í	H	J
Í	U	V	S	Y	T	S	V
E	Š	L	Š	T	K	Ý	Ě
K	É	EŘ	K	M	Í	D	R

Šifrování pomocí šifrovací mřížky



K	A	E	O	V	M	P	S
E	M	E	N	S	J	E	P
O	I	R	N	K	A	E	Š
CH	M	D	T	N	Ě	E	N
A	Á	A	Z	M	Í	H	J
Í	U	V	S	Y	T	S	V
E	Š	L	Š	T	K	Ý	Ě
K	É	EŘ	K	M	Í	D	R

Šifrování pomocí šifrovací mřížky

1	2	3	4	13	9	5	1
5	6	7	8	14	10	6	2
9	10	11	12	15	11	7	3
13	14	15	16	16	12	8	4
4	8	12	16	16	15	14	13
3	7	11	15	12	11	10	9
2	6	10	14	8	7	6	5
1	5	9	13	4	3	2	1

Šifrování pomocí šifrovací mřížky

1	2	3	4	13	9	5	1
5	6	7	8	14	10	6	2
9	10	11	12	15	11	7	3
13	14	15	16	16	12	8	4
4	8	12	16	16	15	14	13
3	7	11	15	12	11	10	9
2	6	10	14	8	7	6	5
1	5	9	13	4	3	2	1

1	2	3	4	13	9	5	1
5	6	7	8	14	10	6	2
9	10	11	12	15	11	7	3
13	14	15	16	16	12	8	4
4	8	12	16	16	15	14	13
3	7	11	15	12	11	10	9
2	6	10	14	8	7	6	5
1	5	9	13	4	3	2	1

Šifrování pomocí šifrovací mřížky

1	2	3	4	13	9	5	1
5	6	7	8	14	10	6	2
9	10	11	12	15	11	7	3
13	14	15	16	16	12	8	4
4	8	12	16	16	15	14	13
3	7	11	15	12	11	10	9
2	6	10	14	8	7	6	5
1	5	9	13	4	3	2	1

Šifrování pomocí šifrovací mřížky

1	2	3	4	13	9	5	1
5	6	7	8	14	10	6	2
9	10	11	12	15	11	7	3
13	14	15	16	16	12	8	4
4	8	12	16	16	15	14	13
3	7	11	15	12	11	10	9
2	6	10	14	8	7	6	5
1	5	9	13	4	3	2	1

K	A	E	O	V	M	P	S
E	M	E	N	S	J	E	P
O	I	R	N	K	A	E	Š
CH	M	D	T	N	Ě	E	N
A	Á	A	Z	M	Í	H	J
Í	U	V	S	Y	T	S	V
E	Š	L	Š	T	K	Ý	Ě
K	É	EŘ	K	M	Í	D	R

Enigma - nejslavnější šifrovací přístroj

Enigma - nejslavnější šifrovací přístroj

- Patentován 1918.

Enigma - nejslavnější šifrovací přístroj

- Patentován 1918.
- Proměnné nastavení, které lze měnit, náhrada znaku znakem zůstává.

Enigma - nejslavnější šifrovací přístroj

- Patentován 1918.
- Proměnné nastavení, které lze měnit, náhrada znaku znakem zůstává.
- Používán Němci ve 2. světové válce.

Enigma - nejslavnější šifrovací přístroj

- Patentován 1918.
- Proměnné nastavení, které lze měnit, náhrada znaku znakem zůstává.
- Používán Němci ve 2. světové válce.
- Prolomen týmem matematiků a inženýrů vedených Alanem Turingem (film *Kód Enigmy*).

Enigma - nejslavnější šifrovací přístroj

- Patentován 1918.
- Proměnné nastavení, které lze měnit, náhrada znaku znakem zůstává.
- Používán Němci ve 2. světové válce.
- Prolomen týmem matematiků a inženýrů vedených Alanem Turingem (film *Kód Enigmy*).

"Úspěch v prolomení Enigmy byl dán třemi faktory: strachem, špionáží a matematikou." (Simon Singh)

- Zásadní otázka: Co je nejkritičtějším momentem při procesu posílání tajných zpráv a jak tento prvek co nejvíce eliminovat?

- Zásadní otázka: Co je nejkritičtějším momentem při procesu posílání tajných zpráv a jak tento prvek co nejvíce eliminovat?
- Zásadní odpověď: Lidský faktor - vyzrazení principu šifry, ať už náhodné, úmyslné nebo neobratné.

- Zásadní otázka: Co je nejkritičtějším momentem při procesu posílání tajných zpráv a jak tento prvek co nejvíce eliminovat?
- Zásadní odpověď: Lidský faktor - vyzrazení principu šifry, ať už náhodné, úmyslné nebo neobratné.
- Odvážná myšlenka: Vymyslet šifrovací systém, který by pro zašifrování a dešifrování používal natolik odlišný "proces", že by **nevadilo, kdyby byl princip zašifrování vyzrazen.**

- Zásadní otázka: Co je nejkritičtějším momentem při procesu posílání tajných zpráv a jak tento prvek co nejvíce eliminovat?
- Zásadní odpověď: Lidský faktor - vyzrazení principu šifry, ať už náhodné, úmyslné nebo neobratné.
- Odvážná myšlenka: Vymyslet šifrovací systém, který by pro zašifrování a dešifrování používal natolik odlišný "proces", že by **nevadilo, kdyby byl princip zašifrování vyzrazen.**
- Další zásadní otázka: Je něco takového teoreticky vůbec možné?

- Zásadní otázka: Co je nejkritičtějším momentem při procesu posílání tajných zpráv a jak tento prvek co nejvíce eliminovat?
- Zásadní odpověď: Lidský faktor - vyzrazení principu šifry, ať už náhodné, úmyslné nebo neobratné.
- Odvážná myšlenka: Vymyslet šifrovací systém, který by pro zašifrování a dešifrování používal natolik odlišný "proces", že by **nevadilo, kdyby byl princip zašifrování vyzrazen.**
- Další zásadní otázka: Je něco takového teoreticky vůbec možné?
- Konec 70. let 20. století: Ano!

- Zásadní otázka: Co je nejkritičtějším momentem při procesu posílání tajných zpráv a jak tento prvek co nejvíce eliminovat?
- Zásadní odpověď: Lidský faktor - vyzrazení principu šifry, ať už náhodné, úmyslné nebo neobratné.
- Odvážná myšlenka: Vymyslet šifrovací systém, který by pro zašifrování a dešifrování používal natolik odlišný "proces", že by **nevadilo, kdyby byl princip zašifrování vyzrazen.**
- Další zásadní otázka: Je něco takového teoreticky vůbec možné?
- Konec 70. let 20. století: Ano! – šifrovací systém RSA

- Zásadní otázka: Co je nejkritičtějším momentem při procesu posílání tajných zpráv a jak tento prvek co nejvíce eliminovat?
- Zásadní odpověď: Lidský faktor - vyzrazení principu šifry, ať už náhodné, úmyslné nebo neobratné.
- Odvážná myšlenka: Vymyslet šifrovací systém, který by pro zašifrování a dešifrování používal natolik odlišný "proces", že by **nevadilo, kdyby byl princip zašifrování vyzrazen.**
- Další zásadní otázka: Je něco takového teoreticky vůbec možné?
- Konec 70. let 20. století: Ano! – šifrovací systém RSA (Rivest, Shamir, Adleman)

- Zásadní otázka: Co je nejkritičtějším momentem při procesu posílání tajných zpráv a jak tento prvek co nejvíce eliminovat?
- Zásadní odpověď: Lidský faktor - vyzrazení principu šifry, ať už náhodné, úmyslné nebo neobratné.
- Odvážná myšlenka: Vymyslet šifrovací systém, který by pro zašifrování a dešifrování používal natolik odlišný "proces", že by **nevadilo, kdyby byl princip zašifrování vyzrazen.**
- Další zásadní otázka: Je něco takového teoreticky vůbec možné?
- Konec 70. let 20. století: Ano! – šifrovací systém RSA (Rivest, Shamir, Adleman) . . . aneb "i prvočísla mohou mít praktické uplatnění".

Popis fungování RSA (zatím bez velkých detailů):

Popis fungování RSA (zatím bez velkých detailů):

- Vezmi dvě velká prvočísla p, q (typicky mající stovky cifer) a vynásob je: $n = p \cdot q$.

Popis fungování RSA (zatím bez velkých detailů):

- Vezmi dvě velká prvočísla p, q (typicky mající stovky cifer) a vynásob je: $n = p \cdot q$.
- Pomocí tohoto n a tzv. exponentu E zašifruj svou zprávu algoritmem "RSA".

Popis fungování RSA (zatím bez velkých detailů):

- Vezmi dvě velká prvočísla p, q (typicky mající stovky cifer) a vynásob je: $n = p \cdot q$.
- Pomocí tohoto n a tzv. exponentu E zašifruj svou zprávu algoritmem "RSA".
- Nejen zašifrovaná zpráva, ale i ona čísla n a E mohou být klidně zveřejněna, protože je to tak chytře vymyšleno, že:

Popis fungování RSA (zatím bez velkých detailů):

- Vezmi dvě velká prvočísla p, q (typicky mající stovky cifer) a vynásob je: $n = p \cdot q$.
- Pomocí tohoto n a tzv. exponentu E zašifruj svou zprávu algoritmem "RSA".
- Nejen zašifrovaná zpráva, ale i ona čísla n a E mohou být klidně zveřejněna, protože je to tak chytře vymyšleno, že:
- Pro dešifrování zprávy je potřeba umět rozložit (nebo znát rozklad) n zpátky na součin jeho dvou prvočinitelů p, q.

První obava: Je to bezpečné?

První obava: Je to bezpečné?

Totiž: co když někdo bude umět rychle rozložit veřejně známé číslo n na součin oněch dvou prvočísel p, q, a tím prolomí naši šifru?

■ První obava: Je to bezpečné?

Totiž: co když někdo bude umět rychle rozložit veřejně známé číslo n na součin oněch dvou prvočísel p, q, a tím prolomí naši šifru?

■ Druhá obava

Pro důležité šifrování se používají čísla o 300 a více cifrách, tj. součiny prvočísel o cca 150 cifrách. Je jich dost? Nevyčerpáme je po nějaké konečné době? Nebude tím někdo mít v ruce úplný seznam možností, který pak bude stačit jen projít?

■ První obava: Je to bezpečné?

Totiž: co když někdo bude umět rychle rozložit veřejně známé číslo n na součin oněch dvou prvočísel p, q, a tím prolomí naši šifru?

■ Druhá obava

Pro důležité šifrování se používají čísla o 300 a více cifrách, tj. součiny prvočísel o cca 150 cifrách. Je jich dost? Nevyčerpáme je po nějaké konečné době? Nebude tím někdo mít v ruce úplný seznam možností, který pak bude stačit jen projít?

To jsou nejen zajímavé, ale i velice důležité otázky – takže se k nim ještě vrátíme, až budeme umět trochu zacházet s . . .

■ První obava: Je to bezpečné?

Totiž: co když někdo bude umět rychle rozložit veřejně známé číslo n na součin oněch dvou prvočísel p, q, a tím prolomí naši šifru?

■ Druhá obava

Pro důležité šifrování se používají čísla o 300 a více cifrách, tj. součiny prvočísel o cca 150 cifrách. Je jich dost? Nevyčerpáme je po nějaké konečné době? Nebude tím někdo mít v ruce úplný seznam možností, který pak bude stačit jen projít?

To jsou nejen zajímavé, ale i velice důležité otázky – takže se k nim ještě vrátíme, až budeme umět trochu zacházet s . . . prvočísly a tzv. modulární aritmetikou.

2. Prvočísla a některé jejich vlastnosti

2. Prvočísla a některé jejich vlastnosti

Prvočíslo: přirozené číslo větší než 1 dělitelné jen sebou samým a jedničkou (tj. 1 není prvočíslo).

Prvočíslo: přirozené číslo větší než 1 dělitelné jen sebou samým a jedničkou (tj. 1 není prvočíslo).

Známá posloupnost:

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31 \ldots$$

Prvočíslo: přirozené číslo větší než 1 dělitelné jen sebou samým a jedničkou (tj. 1 není prvočíslo).

Známá posloupnost:

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31 \ldots$$

Základní otázky: Kolik je prvočísel a jak jsou rozložena mezi ostatními přirozenými čísly?

Prvočíslo: přirozené číslo větší než 1 dělitelné jen sebou samým a jedničkou (tj. 1 není prvočíslo).

Známá posloupnost:

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31 \ldots$$

Základní otázky: Kolik je prvočísel a jak jsou rozložena mezi ostatními přirozenými čísly?

Věta (Eukleidés)

Prvočísel je nekonečně mnoho.

Prvočíslo: přirozené číslo větší než 1 dělitelné jen sebou samým a jedničkou (tj. 1 není prvočíslo).

Známá posloupnost:

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31 \ldots$$

Základní otázky: Kolik je prvočísel a jak jsou rozložena mezi ostatními přirozenými čísly?

Věta (Eukleidés)

Prvočísel je nekonečně mnoho.

Pozor, $x = p_1 \cdot p_2 \cdots p_n + 1$ nemusí být prvočíslo:

Prvočíslo: přirozené číslo větší než 1 dělitelné jen sebou samým a jedničkou (tj. 1 není prvočíslo).

Známá posloupnost:

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31 \ldots$$

Základní otázky: Kolik je prvočísel a jak jsou rozložena mezi ostatními přirozenými čísly?

Věta (Eukleidés)

Prvočísel je nekonečně mnoho.

Pozor, $x = p_1 \cdot p_2 \cdots p_n + 1$ nemusí být prvočíslo:

$$2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 = 30031$$

Prvočíslo: přirozené číslo větší než 1 dělitelné jen sebou samým a jedničkou (tj. 1 není prvočíslo).

Známá posloupnost:

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31 \ldots$$

Základní otázky: Kolik je prvočísel a jak jsou rozložena mezi ostatními přirozenými čísly?

Věta (Eukleidés)

Prvočísel je nekonečně mnoho.

Pozor, $x = p_1 \cdot p_2 \cdots p_n + 1$ nemusí být prvočíslo:

$$2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 = 30031 = 59 \cdot 509$$

O **rozložení prvočísel mezi ostatními čísly** hovoří tzv. **prvočíselná věta**.

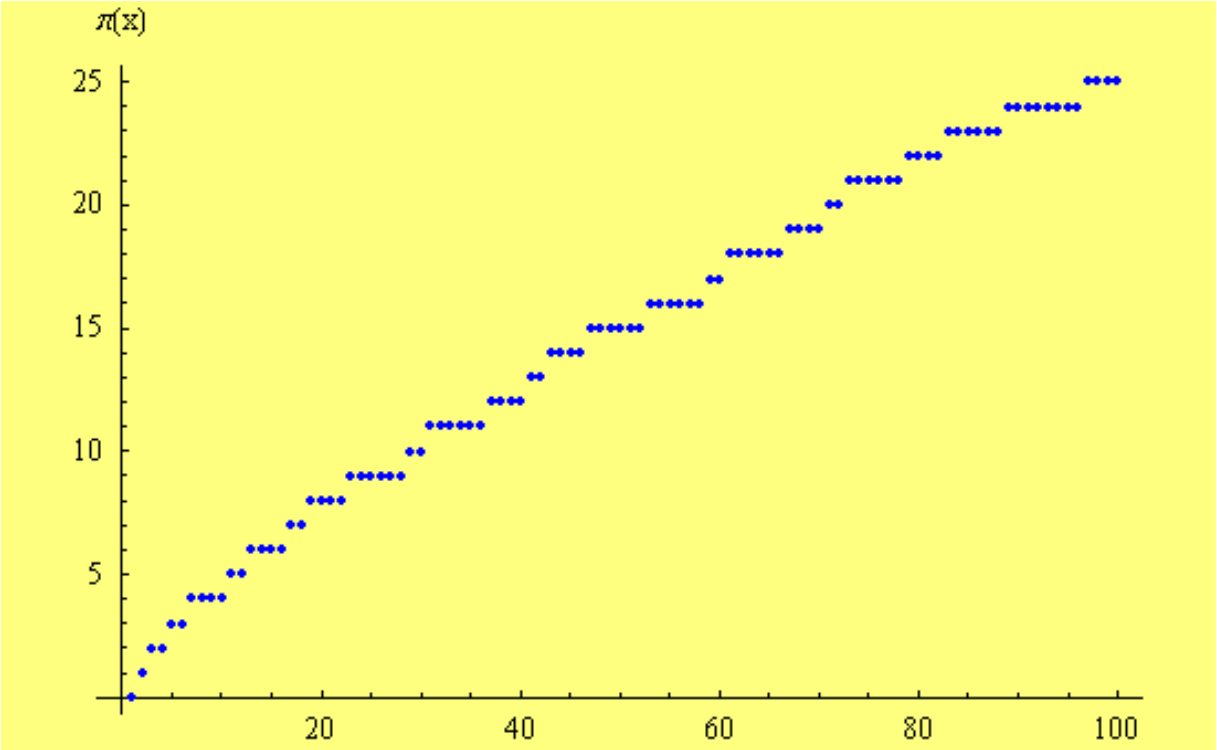
O **rozložení prvočísel mezi ostatními čísly** hovoří tzv. **prvočíselná věta**. Označme

O **rozložení prvočísel mezi ostatními čísly** hovoří tzv. **prvočíselná věta**. Označme

$$\pi(x) = \text{počet prvočísel, menších než } x.$$

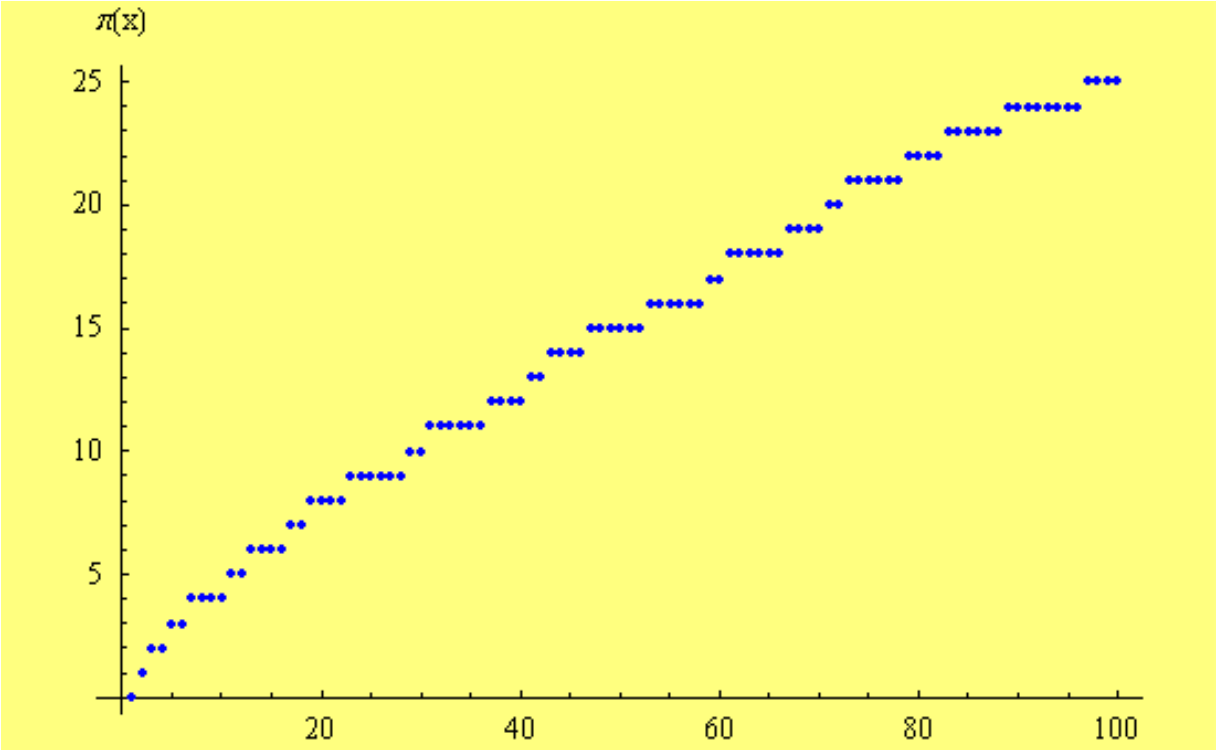
O **rozložení prvočísel mezi ostatními čísly** hovoří tzv. **prvočíselná věta**. Označme

$$\pi(x) = \text{počet prvočísel, menších než } x.$$



O **rozložení prvočísel mezi ostatními čísly** hovoří tzv. **prvočíselná věta**. Označme

$$\pi(x) = \text{počet prvočísel, menších než } x.$$



Prvočíselná věta $\approx$ uměli bychom tím proložit "co nejpřesněji" křivku, popsanou pomocí "známých" funkcí?

R. **1792**, ve věku 15 let (!), vyslovil *C. F. Gauss* (bez důkazu) domněnku (dnes známou jako **prvočíselná věta**):

R. **1792**, ve věku 15 let (!), vyslovil *C. F. Gauss* (bez důkazu) domněnku (dnes známou jako **prvočíselná věta**):

$$\pi(x) \approx \frac{x}{\ln x}\,.$$

R. **1792**, ve věku 15 let (!), vyslovil *C. F. Gauss* (bez důkazu) domněnku (dnes známou jako **prvočíselná věta**):

$$\pi(x) \approx \frac{x}{\ln x}\,.$$

Gaussův odhad se zdá být "geniálně uhodnutý", přitom však není zas tak obtížné (pokud jsme všímaví) odhad $\pi(x) \approx \frac{x}{\ln x}$ zpozorovat.

Prvočíselnou větu dokázali až v r. 1896 (nezávisle na sobě) *Jacques Hadamard* a *Charles de la Vallée Poussin*.

Prvočíselnou větu dokázali až v r. 1896 (nezávisle na sobě) *Jacques Hadamard* a *Charles de la Vallée Poussin*.

$$\pi(x) \approx \frac{x}{\ln x} \quad \text{pro } x \to \infty\,,$$

Prvočíselnou větu dokázali až v r. 1896 (nezávisle na sobě) *Jacques Hadamard* a *Charles de la Vallée Poussin*.

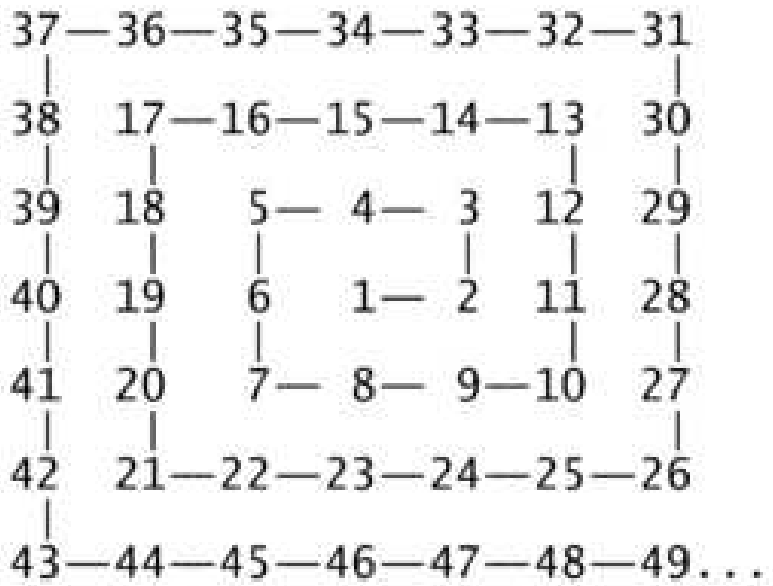
$$\pi(x) \approx \frac{x}{\ln x} \quad \text{pro } x \to \infty\,,$$

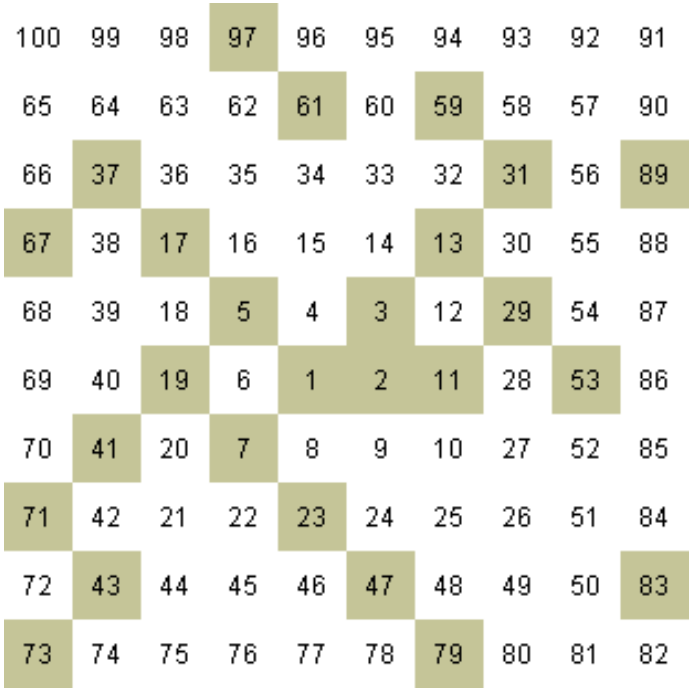
v tomto smyslu:

$$\lim_{x\to\infty} \frac{\pi(x)}{\frac{x}{\ln x}} = 1.$$

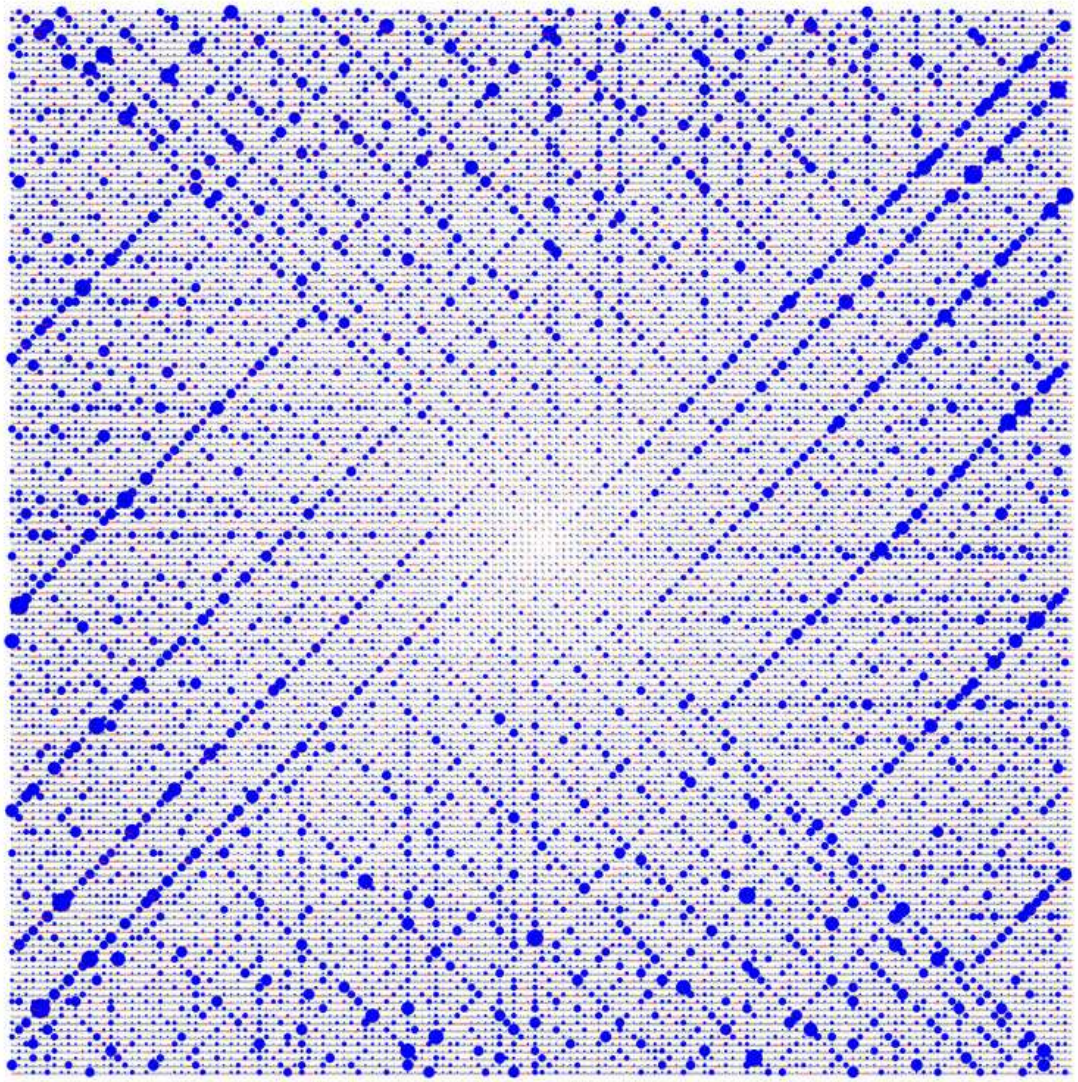
3. Jeden z dalších příspěvků k tématu "krása matematiky"

3. Jeden z dalších příspěvků k tématu "krása matematiky"





Ulamova prvočíselná spirála - vznik



Ulamova prvočíselná spirála

Otázka: Jaké je největší prvočíslo?

Otázka: Jaké je největší prvočíslo?

(...ale vždyť ...)

Otázka: Jaké je největší prvočíslo?

(. . . ale vždyť . . .)

Dobře, tak jaké je největší **známé** prvočíslo?

Otázka: Jaké je největší prvočíslo?

(... ale vždyť ...)

Dobře, tak jaké je největší **známé** prvočíslo?

Nejvetší k dnešnímu datu známé prvočíslo (bylo nalezeno v prosinci 2018) je

$$2^{82\,589\,933} - 1\,,$$

Otázka: Jaké je největší prvočíslo?

(... ale vždyť ...)

Dobře, tak jaké je největší **známé** prvočíslo?

Nejvetší k dnešnímu datu známé prvočíslo (bylo nalezeno v prosinci 2018) je

$$2^{82\,589\,933} - 1\,,$$

má 24 862 048 dekadických cifer.

Otázka: Jaké je největší prvočíslo?

(. . . ale vždyť . . .)

Dobře, tak jaké je největší **známé** prvočíslo?

Nejvetší k dnešnímu datu známé prvočíslo (bylo nalezeno v prosinci 2018) je

$$2^{82\,589\,933} - 1\,,$$

má 24 862 048 dekadických cifer.

(Při 30 řádcích a 60 znacích na řádek by bylo potřeba asi 13 800 stran papíru na jeho vytištění.)

Proč se to vlastně počítá?

Proč se to vlastně počítá?

1. Číselně-teoretické vlastnosti: hustota a rozložení prvočísel. . .

Proč se to vlastně počítá?

1. Číselně-teoretické vlastnosti: hustota a rozložení prvočísel. . .
2. Touha být držitelem rekordu. . .

Proč se to vlastně počítá?

1. Číselně-teoretické vlastnosti: hustota a rozložení prvočísel. . .
2. Touha být držitelem rekordu. . .
3. Test počítačových procesorů (asi nejdůležitější současný důvod).

Proč se to vlastně počítá?

1. Číselně-teoretické vlastnosti: hustota a rozložení prvočísel. . .
2. Touha být držitelem rekordu. . .
3. Test počítačových procesorů (asi nejdůležitější současný důvod). Je schopen náš nový hardware bezchybně počítat dlouhé hodiny či dny a týdny a dostat stejný výsledek jako konkurence? Případně ještě lepší výsledek nebo rychleji spočtený výsledek?

"Nejlepší" prvočíslo?

"Nejlepší" prvočíslo?

"Nejlepším číslem je číslo 73. Je to v pořadí 21. prvočíslo. Jeho zrcadlově obrácené číslo (37) je 12. prvočíslem, což je zrcadlový obraz pořadí čísla 73. Navíc oněch 21 je součinem cifer 7 a 3. V dvojkovém zápisu je 73 rovno 1001001, což je palindrom (jeho zrcadlový obraz je totéž číslo)"

"Nejlepší" prvočíslo?

"Nejlepším číslem je číslo 73. Je to v pořadí 21. prvočíslo. Jeho zrcadlově obrácené číslo (37) je 12. prvočíslem, což je zrcadlový obraz pořadí čísla 73. Navíc oněch 21 je součinem cifer 7 a 3. V dvojkovém zápisu je 73 rovno 1001001, což je palindrom (jeho zrcadlový obraz je totéž číslo)"

[Sheldon Cooper, TBBT, s04e10]

"Nejlepší" prvočíslo?

"Nejlepším číslem je číslo 73. Je to v pořadí 21. prvočíslo. Jeho zrcadlově obrácené číslo (37) je 12. prvočíslem, což je zrcadlový obraz pořadí čísla 73. Navíc oněch 21 je součinem cifer 7 a 3. V dvojkovém zápisu je 73 rovno 1001001, což je palindrom (jeho zrcadlový obraz je totéž číslo)"

[Sheldon Cooper, TBBT, s04e10]

Zajímavé prvočíslo:

3141592653589793238462643383346264832397853562951413

"Nejlepší" prvočíslo?

"Nejlepším číslem je číslo 73. Je to v pořadí 21. prvočíslo. Jeho zrcadlově obrácené číslo (37) je 12. prvočíslem, což je zrcadlový obraz pořadí čísla 73. Navíc oněch 21 je součinem cifer 7 a 3. V dvojkovém zápisu je 73 rovno 1001001, což je palindrom (jeho zrcadlový obraz je totéž číslo)"

[Sheldon Cooper, TBBT, s04e10]

Zajímavé prvočíslo:

3141592653589793238462643383346264832397853562951413

(Vidíte, čím je zajímavé? Nápověda: π, 26.)

Prvočíselný vzorec?

Existuje vzorec, který pro každé n dá prvočíslo?

Prvočíselný vzorec?

Existuje vzorec, který pro každé n dá prvočíslo? Odpověď vhodná pro přednášku, přednesenou 1. dubna:

Prvočíselný vzorec?

Existuje vzorec, který pro každé n dá prvočíslo? Odpověď vhodná pro přednášku, přednesenou 1. dubna:

$$p_n = 1 + 1^n .$$

Prvočíselný vzorec?

Existuje vzorec, který pro každé n dá prvočíslo? Odpověď vhodná pro přednášku, přednesenou 1. dubna:

$$p_n = 1 + 1^n .$$

Dobře, tak existuje vzorec, který pro každé n dá **n-té prvočíslo**?

Prvočíselný vzorec?

Existuje vzorec, který pro každé n dá prvočíslo? Odpověď vhodná pro přednášku, přednesenou 1. dubna:

$$p_n = 1 + 1^n .$$

Dobře, tak existuje vzorec, který pro každé n dá **n-té prvočíslo**? Překvapení: Ano!

$$p_n = 1 + \sum_{m=1}^{2^n} \left\lfloor \sqrt[n]{\left\lfloor \frac{n}{1 + \sum_{j=1}^{m} \left(\left\lfloor \frac{(j-1)!+1}{j} \right\rfloor - \left\lfloor \frac{(j-1)!}{j} \right\rfloor \right)} \right\rfloor} \right\rfloor$$

Prvočíselný vzorec?

Existuje vzorec, který pro každé n dá prvočíslo? Odpověď vhodná pro přednášku, přednesenou 1. dubna:

$$p_n = 1 + 1^n .$$

Dobře, tak existuje vzorec, který pro každé n dá **n-té prvočíslo**? Překvapení: Ano!

$$p_n = 1 + \sum_{m=1}^{2^n} \left\lfloor \sqrt[n]{\left\lfloor \frac{n}{1 + \sum_{j=1}^{m} \left(\left\lfloor \frac{(j-1)!+1}{j} \right\rfloor - \left\lfloor \frac{(j-1)!}{j} \right\rfloor \right)} \right\rfloor} \right\rfloor$$

viz

P. Ribenboim: *The new book of prime number records*, 3rd edition, Springer-Verlag, New York, NY, 1995.

5. Co je to ta modulární aritmetika?

Definice

Uvažujme celá čísla a, b a přirozené n (tj. $a, b \in \mathbb{Z}$, $n \in \mathbb{N}$) a označme symbolem "$a \bmod n$" zbytek při dělení čísla a číslem n.

5. Co je to ta modulární aritmetika?

Definice

Uvažujme celá čísla a, b a přirozené n (tj. $a, b \in \mathbb{Z}$, $n \in \mathbb{N}$) a označme symbolem "$a \bmod n$" zbytek při dělení čísla a číslem n. Řekneme, že a je **kongruentní** s b **modulo** n,

5. Co je to ta modulární aritmetika?

Definice

Uvažujme celá čísla a, b a přirozené n (tj. $a, b \in \mathbb{Z}$, $n \in \mathbb{N}$) a označme symbolem "$a \bmod n$" zbytek při dělení čísla a číslem n. Řekneme, že a je **kongruentní** s b **modulo** n, pokud je $a \bmod n = b \bmod n$, tedy pokud je zbytek při dělení a/n a b/n tentýž.

Definice

Uvažujme celá čísla a, b a přirozené n (tj. $a, b \in \mathbb{Z}$, $n \in \mathbb{N}$) a označme symbolem "$a \bmod n$" zbytek při dělení čísla a číslem n. Řekneme, že a je **kongruentní** s b **modulo** n, pokud je $a \bmod n = b \bmod n$, tedy pokud je zbytek při dělení a/n a b/n tentýž. Píšeme:

$$a \equiv b \pmod{n}.$$

Definice

Uvažujme celá čísla a, b a přirozené n (tj. $a, b \in \mathbb{Z}$, $n \in \mathbb{N}$) a označme symbolem "$a \bmod n$" zbytek při dělení čísla a číslem n. Řekneme, že a je **kongruentní** s b **modulo** n, pokud je $a \bmod n = b \bmod n$, tedy pokud je zbytek při dělení a/n a b/n tentýž. Píšeme:

$$a \equiv b \pmod{n}.$$

Příklady:

Definice

Uvažujme celá čísla a, b a přirozené n (tj. $a, b \in \mathbb{Z}$, $n \in \mathbb{N}$) a označme symbolem "$a \bmod n$" zbytek při dělení čísla a číslem n. Řekneme, že a je **kongruentní** s b **modulo** n, pokud je $a \bmod n = b \bmod n$, tedy pokud je zbytek při dělení a/n a b/n tentýž. Píšeme:

$$a \equiv b \pmod{n}.$$

Příklady:

$$11 \equiv 1 \pmod{2},$$

Definice

Uvažujme celá čísla a, b a přirozené n (tj. $a, b \in \mathbb{Z}$, $n \in \mathbb{N}$) a označme symbolem "$a \bmod n$" zbytek při dělení čísla a číslem n. Řekneme, že a je **kongruentní** s b **modulo** n, pokud je $a \bmod n = b \bmod n$, tedy pokud je zbytek při dělení a/n a b/n tentýž. Píšeme:

$$a \equiv b \pmod{n}.$$

Příklady:

$$11 \equiv 1 \pmod{2}, \qquad 53 \equiv 4 \pmod{7},$$

Definice

Uvažujme celá čísla a, b a přirozené n (tj. $a, b \in \mathbb{Z}$, $n \in \mathbb{N}$) a označme symbolem "$a \bmod n$" zbytek při dělení čísla a číslem n. Řekneme, že a je **kongruentní** s b **modulo** n, pokud je $a \bmod n = b \bmod n$, tedy pokud je zbytek při dělení a/n a b/n tentýž. Píšeme:

$$a \equiv b \pmod{n}.$$

Příklady:

$$11 \equiv 1 \pmod{2}, \qquad 53 \equiv 4 \pmod{7},$$
$$22 \equiv 71 \pmod{7},$$

Definice

Uvažujme celá čísla a, b a přirozené n (tj. $a, b \in \mathbb{Z}$, $n \in \mathbb{N}$) a označme symbolem "$a \bmod n$" zbytek při dělení čísla a číslem n. Řekneme, že a je **kongruentní** s b **modulo** n, pokud je $a \bmod n = b \bmod n$, tedy pokud je zbytek při dělení a/n a b/n tentýž. Píšeme:

$$a \equiv b \pmod{n}.$$

Příklady:

$$11 \equiv 1 \pmod{2}, \qquad 53 \equiv 4 \pmod{7},$$
$$22 \equiv 71 \pmod{7}, \qquad 10 \equiv -1 \pmod{11}.$$

Definice

Uvažujme celá čísla a, b a přirozené n (tj. $a, b \in \mathbb{Z}$, $n \in \mathbb{N}$) a označme symbolem "$a \bmod n$" zbytek při dělení čísla a číslem n. Řekneme, že a je **kongruentní** s b **modulo** n, pokud je $a \bmod n = b \bmod n$, tedy pokud je zbytek při dělení a/n a b/n tentýž. Píšeme:

$$a \equiv b \pmod{n}.$$

Příklady:

$$11 \equiv 1 \pmod 2, \qquad 53 \equiv 4 \pmod 7,$$
$$22 \equiv 71 \pmod 7, \qquad 10 \equiv -1 \pmod{11}.$$

Platí:

$$a \equiv b \pmod n \iff n \text{ dělí } (a - b).$$

Modulární aritmetika . . . je počítání s kongruencemi.

Modulární aritmetika . . . je počítání s kongruencemi.

- Dobrá zpráva č.1:

Modulární aritmetika . . . je počítání s kongruencemi.

- Dobrá zpráva č.1: s modulárním počítáním se setkáváme odmalička:

Modulární aritmetika . . . je počítání s kongruencemi.

- Dobrá zpráva č.1: s modulárním počítáním se setkáváme odmalička:

Modulární aritmetika . . . je počítání s kongruencemi.

- Dobrá zpráva č.1: s modulárním počítáním se setkáváme odmalička:

hodiny, týdny, roky . . .

Modulární aritmetika . . . je počítání s kongruencemi.

- Dobrá zpráva č.1: s modulárním počítáním se setkáváme odmalička:

hodiny, týdny, roky . . . $14 \equiv 2 \pmod{12}$,

Modulární aritmetika . . . je počítání s kongruencemi.

- Dobrá zpráva č.1: s modulárním počítáním se setkáváme odmalička:

hodiny, týdny, roky . . . $14 \equiv 2 \pmod{12}$,
$730 \equiv 0 \pmod{365}$,. . .

Modulární aritmetika . . . je počítání s kongruencemi.

- Dobrá zpráva č.1: s modulárním počítáním se setkáváme odmalička:

hodiny, týdny, roky . . . $14 \equiv 2 \pmod{12}$,
$730 \equiv 0 \pmod{365}$,. . .

- Dobrá zpráva č.2:

Modulární aritmetika . . . je počítání s kongruencemi.

- Dobrá zpráva č.1: s modulárním počítáním se setkáváme odmalička:

hodiny, týdny, roky . . . $14 \equiv 2 \pmod{12}$,
$730 \equiv 0 \pmod{365}$,. . .

- Dobrá zpráva č.2: sčítání, odečítání, násobení i umocnění kongruencí je snadné:

Tvrzení

$a_1, a_2, b_1, b_2, c \in \mathbb{Z}$, $n, k \in \mathbb{N}$:

$$a_1 \equiv b_1 \pmod{n}$$

Tvrzení

$a_1, a_2, b_1, b_2, c \in \mathbb{Z}$, $n, k \in \mathbb{N}$:

$$a_1 \equiv b_1 \pmod{n}$$
$$a_2 \equiv b_2 \pmod{n}$$

Tvrzení

$a_1, a_2, b_1, b_2, c \in \mathbb{Z}$, $n, k \in \mathbb{N}$:

$$a_1 \equiv b_1 \pmod{n}$$
$$a_2 \equiv b_2 \pmod{n}$$

$$\Downarrow$$

Tvrzení

$a_1, a_2, b_1, b_2, c \in \mathbb{Z}$, $n, k \in \mathbb{N}$:

$$a_1 \equiv b_1 \pmod{n}$$
$$a_2 \equiv b_2 \pmod{n}$$

$$\Downarrow$$

$$ca_1 \equiv cb_1 \pmod{n}$$

Tvrzení

$a_1, a_2, b_1, b_2, c \in \mathbb{Z}$, $n, k \in \mathbb{N}$:

$$a_1 \equiv b_1 \pmod{n}$$
$$a_2 \equiv b_2 \pmod{n}$$

$$\Downarrow$$

$$ca_1 \equiv cb_1 \pmod{n}$$
$$(a_1 + a_2) \equiv (b_1 + b_2) \pmod{n}$$

Tvrzení

$a_1, a_2, b_1, b_2, c \in \mathbb{Z}$, $n, k \in \mathbb{N}$:

$$a_1 \equiv b_1 \pmod{n}$$
$$a_2 \equiv b_2 \pmod{n}$$

$$\Downarrow$$

$$\begin{aligned} ca_1 &\equiv cb_1 \pmod{n} \\ (a_1 + a_2) &\equiv (b_1 + b_2) \pmod{n} \\ (a_1 - a_2) &\equiv (b_1 - b_2) \pmod{n} \end{aligned}$$

Tvrzení

$a_1, a_2, b_1, b_2, c \in \mathbb{Z}$, $n, k \in \mathbb{N}$:

$$a_1 \equiv b_1 \pmod{n}$$
$$a_2 \equiv b_2 \pmod{n}$$

$$\Downarrow$$

$$\begin{aligned} ca_1 &\equiv cb_1 \pmod{n} \\ (a_1 + a_2) &\equiv (b_1 + b_2) \pmod{n} \\ (a_1 - a_2) &\equiv (b_1 - b_2) \pmod{n} \\ (a_1 \cdot a_2) &\equiv (b_1 \cdot b_2) \pmod{n} \end{aligned}$$

Tvrzení

$a_1, a_2, b_1, b_2, c \in \mathbb{Z}$, $n, k \in \mathbb{N}$:

$$a_1 \equiv b_1 \pmod{n}$$
$$a_2 \equiv b_2 \pmod{n}$$

$$\Downarrow$$

$$\begin{aligned} ca_1 &\equiv cb_1 \pmod{n} \\ (a_1 + a_2) &\equiv (b_1 + b_2) \pmod{n} \\ (a_1 - a_2) &\equiv (b_1 - b_2) \pmod{n} \\ (a_1 \cdot a_2) &\equiv (b_1 \cdot b_2) \pmod{n} \\ a_1^k &\equiv b_1^k \pmod{n} \end{aligned}$$

Příklady:

Příklady:

- $14 \equiv 2 \pmod{12}$,

Příklady:

- $14 \equiv 2 \pmod{12}$, $23 \equiv 11 \pmod{12}$

Příklady:

- $14 \equiv 2 \pmod{12}, \;\; 23 \equiv 11 \pmod{12}$
  $\Rightarrow \quad 14 + 23 \equiv 2 + 11 \pmod{12}$

Příklady:

- $14 \equiv 2 \pmod{12}$, $23 \equiv 11 \pmod{12}$
  $\Rightarrow \quad 14 + 23 \equiv 2 + 11 \pmod{12}$
  $\Rightarrow \quad 37 \equiv 13 \equiv 1 \pmod{12}$

Příklady:

- $14 \equiv 2 \pmod{12}$, $23 \equiv 11 \pmod{12}$
  $\Rightarrow \quad 14 + 23 \equiv 2 + 11 \pmod{12}$
  $\Rightarrow \quad 37 \equiv 13 \equiv 1 \pmod{12}$
- $14 \equiv 2 \pmod{12}$,

Příklady:

- $14 \equiv 2 \pmod{12}, \ 23 \equiv 11 \pmod{12}$
  $\Rightarrow \quad 14 + 23 \equiv 2 + 11 \pmod{12}$
  $\Rightarrow \quad 37 \equiv 13 \equiv 1 \pmod{12}$
- $14 \equiv 2 \pmod{12}, \ 23 \equiv 11 \pmod{12}$

Příklady:

- $14 \equiv 2 \pmod{12}, \;\; 23 \equiv 11 \pmod{12}$
  $\Rightarrow \quad 14 + 23 \equiv 2 + 11 \pmod{12}$
  $\Rightarrow \quad 37 \equiv 13 \equiv 1 \pmod{12}$
- $14 \equiv 2 \pmod{12}, \;\; 23 \equiv 11 \pmod{12}$
  $\Rightarrow \quad 14 \cdot 23 \equiv 22 \pmod{12}$

Příklady:

- $14 \equiv 2 \pmod{12}, \;\; 23 \equiv 11 \pmod{12}$
  $\Rightarrow \quad 14 + 23 \equiv 2 + 11 \pmod{12}$
  $\Rightarrow \quad 37 \equiv 13 \equiv 1 \pmod{12}$
- $14 \equiv 2 \pmod{12}, \;\; 23 \equiv 11 \pmod{12}$
  $\Rightarrow \quad 14 \cdot 23 \equiv 22 \pmod{12}$
- $123^{17} \equiv ? \pmod{3233}$

Příklady:

- $14 \equiv 2 \pmod{12}, \;\; 23 \equiv 11 \pmod{12}$
  $\Rightarrow \quad 14 + 23 \equiv 2 + 11 \pmod{12}$
  $\Rightarrow \quad 37 \equiv 13 \equiv 1 \pmod{12}$
- $14 \equiv 2 \pmod{12}, \;\; 23 \equiv 11 \pmod{12}$
  $\Rightarrow \quad 14 \cdot 23 \equiv 22 \pmod{12}$
- $123^{17} \equiv ? \pmod{3233}$ $\qquad (123^{17} \approx 3.38 \cdot 10^{35})$

Příklady:

- $14 \equiv 2 \pmod{12}, \;\; 23 \equiv 11 \pmod{12}$
  $\Rightarrow \quad 14 + 23 \equiv 2 + 11 \pmod{12}$
  $\Rightarrow \quad 37 \equiv 13 \equiv 1 \pmod{12}$
- $14 \equiv 2 \pmod{12}, \;\; 23 \equiv 11 \pmod{12}$
  $\Rightarrow \quad 14 \cdot 23 \equiv 22 \pmod{12}$
- $123^{17} \equiv ? \pmod{3233}$ $\qquad (123^{17} \approx 3.38 \cdot 10^{35})$

$$123 \cdot 123 \equiv 2197 \pmod{3233}$$

Příklady:

- $14 \equiv 2 \pmod{12}, \;\; 23 \equiv 11 \pmod{12}$
  $\Rightarrow \quad 14 + 23 \equiv 2 + 11 \pmod{12}$
  $\Rightarrow \quad 37 \equiv 13 \equiv 1 \pmod{12}$
- $14 \equiv 2 \pmod{12}, \;\; 23 \equiv 11 \pmod{12}$
  $\Rightarrow \quad 14 \cdot 23 \equiv 22 \pmod{12}$
- $123^{17} \equiv ? \pmod{3233}$ $\qquad (123^{17} \approx 3.38 \cdot 10^{35})$

$$123 \cdot 123 \equiv 2197 \pmod{3233} \qquad (123^2)$$

Příklady:

- $14 \equiv 2 \pmod{12}, \;\; 23 \equiv 11 \pmod{12}$
  $\Rightarrow \quad 14 + 23 \equiv 2 + 11 \pmod{12}$
  $\Rightarrow \quad 37 \equiv 13 \equiv 1 \pmod{12}$
- $14 \equiv 2 \pmod{12}, \;\; 23 \equiv 11 \pmod{12}$
  $\Rightarrow \quad 14 \cdot 23 \equiv 22 \pmod{12}$
- $123^{17} \equiv ? \pmod{3233}$ $\qquad (123^{17} \approx 3.38 \cdot 10^{35})$

$$\begin{aligned} 123 \cdot 123 &\equiv 2197 \pmod{3233} \qquad (123^2) \\ 2197 \cdot 2197 &\equiv 60 \pmod{3233} \end{aligned}$$

Příklady:

- $14 \equiv 2 \pmod{12}, \;\; 23 \equiv 11 \pmod{12}$
  $\Rightarrow \quad 14 + 23 \equiv 2 + 11 \pmod{12}$
  $\Rightarrow \quad 37 \equiv 13 \equiv 1 \pmod{12}$
- $14 \equiv 2 \pmod{12}, \;\; 23 \equiv 11 \pmod{12}$
  $\Rightarrow \quad 14 \cdot 23 \equiv 22 \pmod{12}$
- $123^{17} \equiv ? \pmod{3233}$ $\qquad (123^{17} \approx 3.38 \cdot 10^{35})$

$$\begin{aligned} 123 \cdot 123 &\equiv 2197 \pmod{3233} && (123^2) \\ 2197 \cdot 2197 &\equiv 60 \pmod{3233} && (123^4) \end{aligned}$$

Příklady:

- $14 \equiv 2 \pmod{12}, \;\; 23 \equiv 11 \pmod{12}$
  $\Rightarrow \quad 14 + 23 \equiv 2 + 11 \pmod{12}$
  $\Rightarrow \quad 37 \equiv 13 \equiv 1 \pmod{12}$
- $14 \equiv 2 \pmod{12}, \;\; 23 \equiv 11 \pmod{12}$
  $\Rightarrow \quad 14 \cdot 23 \equiv 22 \pmod{12}$
- $123^{17} \equiv ? \pmod{3233}$ $\qquad (123^{17} \approx 3.38 \cdot 10^{35})$

$$\begin{aligned} 123 \cdot 123 &\equiv 2197 \pmod{3233} && (123^2) \\ 2197 \cdot 2197 &\equiv 60 \pmod{3233} && (123^4) \\ 60 \cdot 60 &\equiv 367 \pmod{3233} \end{aligned}$$

Příklady:

- $14 \equiv 2 \pmod{12}, \;\; 23 \equiv 11 \pmod{12}$
  $\Rightarrow \quad 14 + 23 \equiv 2 + 11 \pmod{12}$
  $\Rightarrow \quad 37 \equiv 13 \equiv 1 \pmod{12}$
- $14 \equiv 2 \pmod{12}, \;\; 23 \equiv 11 \pmod{12}$
  $\Rightarrow \quad 14 \cdot 23 \equiv 22 \pmod{12}$
- $123^{17} \equiv ? \pmod{3233}$ $\qquad (123^{17} \approx 3.38 \cdot 10^{35})$

$$\begin{aligned} 123 \cdot 123 &\equiv 2197 \pmod{3233} && (123^2) \\ 2197 \cdot 2197 &\equiv 60 \pmod{3233} && (123^4) \\ 60 \cdot 60 &\equiv 367 \pmod{3233} && (123^8) \end{aligned}$$

Příklady:

- $14 \equiv 2 \pmod{12}, \;\; 23 \equiv 11 \pmod{12}$
  $\Rightarrow \quad 14 + 23 \equiv 2 + 11 \pmod{12}$
  $\Rightarrow \quad 37 \equiv 13 \equiv 1 \pmod{12}$
- $14 \equiv 2 \pmod{12}, \;\; 23 \equiv 11 \pmod{12}$
  $\Rightarrow \quad 14 \cdot 23 \equiv 22 \pmod{12}$
- $123^{17} \equiv ? \pmod{3233}$ $\qquad (123^{17} \approx 3.38 \cdot 10^{35})$

$$\begin{aligned} 123 \cdot 123 &\equiv 2197 \pmod{3233} && (123^2) \\ 2197 \cdot 2197 &\equiv 60 \pmod{3233} && (123^4) \\ 60 \cdot 60 &\equiv 367 \pmod{3233} && (123^8) \\ 367 \cdot 367 &\equiv 2136 \pmod{3233} \end{aligned}$$

Příklady:

- $14 \equiv 2 \pmod{12}, \;\; 23 \equiv 11 \pmod{12}$
  $\Rightarrow \quad 14 + 23 \equiv 2 + 11 \pmod{12}$
  $\Rightarrow \quad 37 \equiv 13 \equiv 1 \pmod{12}$
- $14 \equiv 2 \pmod{12}, \;\; 23 \equiv 11 \pmod{12}$
  $\Rightarrow \quad 14 \cdot 23 \equiv 22 \pmod{12}$
- $123^{17} \equiv ? \pmod{3233}$ $\qquad (123^{17} \approx 3.38 \cdot 10^{35})$

$$
\begin{aligned}
123 \cdot 123 &\equiv 2197 \pmod{3233} && (123^2)\\
2197 \cdot 2197 &\equiv 60 \pmod{3233} && (123^4)\\
60 \cdot 60 &\equiv 367 \pmod{3233} && (123^8)\\
367 \cdot 367 &\equiv 2136 \pmod{3233} && (123^{16})
\end{aligned}
$$

Příklady:

- $14 \equiv 2 \pmod{12}, \;\; 23 \equiv 11 \pmod{12}$
  $\Rightarrow \quad 14 + 23 \equiv 2 + 11 \pmod{12}$
  $\Rightarrow \quad 37 \equiv 13 \equiv 1 \pmod{12}$
- $14 \equiv 2 \pmod{12}, \;\; 23 \equiv 11 \pmod{12}$
  $\Rightarrow \quad 14 \cdot 23 \equiv 22 \pmod{12}$
- $123^{17} \equiv ? \pmod{3233}$ $\qquad (123^{17} \approx 3.38 \cdot 10^{35})$

$$
\begin{aligned}
123 \cdot 123 &\equiv 2197 \pmod{3233} && (123^2)\\
2197 \cdot 2197 &\equiv 60 \pmod{3233} && (123^4)\\
60 \cdot 60 &\equiv 367 \pmod{3233} && (123^8)\\
367 \cdot 367 &\equiv 2136 \pmod{3233} && (123^{16})\\
2136 \cdot 123 &\equiv 855 \pmod{3233}
\end{aligned}
$$

Příklady:

- $14 \equiv 2 \pmod{12}$, $23 \equiv 11 \pmod{12}$
  $\Rightarrow \quad 14 + 23 \equiv 2 + 11 \pmod{12}$
  $\Rightarrow \quad 37 \equiv 13 \equiv 1 \pmod{12}$
- $14 \equiv 2 \pmod{12}$, $23 \equiv 11 \pmod{12}$
  $\Rightarrow \quad 14 \cdot 23 \equiv 22 \pmod{12}$
- $123^{17} \equiv ? \pmod{3233}$ $\qquad (123^{17} \approx 3.38 \cdot 10^{35})$

$$
\begin{aligned}
123 \cdot 123 &\equiv 2197 \pmod{3233} && (123^2)\\
2197 \cdot 2197 &\equiv 60 \pmod{3233} && (123^4)\\
60 \cdot 60 &\equiv 367 \pmod{3233} && (123^8)\\
367 \cdot 367 &\equiv 2136 \pmod{3233} && (123^{16})\\
2136 \cdot 123 &\equiv 855 \pmod{3233} && (123^{17})
\end{aligned}
$$

Příklady:

- $14 \equiv 2 \pmod{12}, \quad 23 \equiv 11 \pmod{12}$
  $\Rightarrow \quad 14 + 23 \equiv 2 + 11 \pmod{12}$
  $\Rightarrow \quad 37 \equiv 13 \equiv 1 \pmod{12}$
- $14 \equiv 2 \pmod{12}, \quad 23 \equiv 11 \pmod{12}$
  $\Rightarrow \quad 14 \cdot 23 \equiv 22 \pmod{12}$
- $123^{17} \equiv ? \pmod{3233}$ $\qquad (123^{17} \approx 3.38 \cdot 10^{35})$

$$
\begin{aligned}
123 \cdot 123 &\equiv 2197 \pmod{3233} && (123^2)\\
2197 \cdot 2197 &\equiv 60 \pmod{3233} && (123^4)\\
60 \cdot 60 &\equiv 367 \pmod{3233} && (123^8)\\
367 \cdot 367 &\equiv 2136 \pmod{3233} && (123^{16})\\
2136 \cdot 123 &\equiv 855 \pmod{3233} && (123^{17})\\
123^{17} &\equiv 855 \pmod{3233}
\end{aligned}
$$

Dělitelnost třemi:

Dělitelnost třemi:

- $10 \equiv 1 \pmod 3$

Dělitelnost třemi:

- $10 \equiv 1 \pmod 3$
  $\Rightarrow \quad 10^k \equiv 1^k \pmod 3, \qquad k \in \mathbb{N},$

Dělitelnost třemi:

- $10 \equiv 1 \pmod 3$
  $\Rightarrow \quad 10^k \equiv 1^k \pmod 3, \qquad k \in \mathbb{N},$
  $\Rightarrow \quad a_k 10^k \equiv a_k \pmod 3, \quad a_k \in \{0, \ldots, 9\},$

Dělitelnost třemi:

- $10 \equiv 1 \pmod 3$

  $\Rightarrow \quad 10^k \equiv 1^k \pmod 3, \qquad k \in \mathbb{N},$

  $\Rightarrow \quad a_k 10^k \equiv a_k \pmod 3, \quad a_k \in \{0, \ldots, 9\},$

  $\Rightarrow \quad \boxed{\sum_{k=0}^{n} a_k 10^k \equiv \sum_{k=0}^{n} a_k \pmod 3.}$

Dělitelnost třemi:

- $10 \equiv 1 \pmod 3$

  $\Rightarrow \quad 10^k \equiv 1^k \pmod 3, \qquad k \in \mathbb{N},$

  $\Rightarrow \quad a_k 10^k \equiv a_k \pmod 3, \quad a_k \in \{0, \ldots, 9\},$

  $\Rightarrow \quad \boxed{\sum_{k=0}^{n} a_k 10^k \equiv \sum_{k=0}^{n} a_k \pmod 3.}$

Dělitelnost jedenácti:

Dělitelnost třemi:

- $10 \equiv 1 \pmod 3$

  $\Rightarrow \quad 10^k \equiv 1^k \pmod 3, \qquad k \in \mathbb{N},$

  $\Rightarrow \quad a_k 10^k \equiv a_k \pmod 3, \quad a_k \in \{0, \ldots, 9\},$

  $\Rightarrow \quad \boxed{\sum_{k=0}^{n} a_k 10^k \equiv \sum_{k=0}^{n} a_k \pmod 3.}$

Dělitelnost jedenácti:

- $10 \equiv -1 \pmod{11}$

Dělitelnost třemi:

- $10 \equiv 1 \pmod 3$

  $\Rightarrow \quad 10^k \equiv 1^k \pmod 3, \qquad k \in \mathbb{N},$

  $\Rightarrow \quad a_k 10^k \equiv a_k \pmod 3, \quad a_k \in \{0, \ldots, 9\},$

  $\Rightarrow \quad \boxed{\sum_{k=0}^{n} a_k 10^k \equiv \sum_{k=0}^{n} a_k \pmod 3.}$

Dělitelnost jedenácti:

- $10 \equiv -1 \pmod{11}$

  $\Rightarrow \quad 10^k \equiv (-1)^k \pmod{11}, \qquad k \in \mathbb{N},$

Dělitelnost třemi:

- $10 \equiv 1 \pmod 3$

  $\Rightarrow \quad 10^k \equiv 1^k \pmod 3, \qquad k \in \mathbb{N},$

  $\Rightarrow \quad a_k 10^k \equiv a_k \pmod 3, \quad a_k \in \{0, \ldots, 9\},$

  $\Rightarrow \quad \boxed{\sum_{k=0}^{n} a_k 10^k \equiv \sum_{k=0}^{n} a_k \pmod 3.}$

Dělitelnost jedenácti:

- $10 \equiv -1 \pmod{11}$

  $\Rightarrow \quad 10^k \equiv (-1)^k \pmod{11}, \qquad k \in \mathbb{N},$

  $\Rightarrow \quad a_k 10^k \equiv a_k (-1)^k \pmod{11}, \quad a_k \in \{0, \ldots, 9\},$

Dělitelnost třemi:

- $10 \equiv 1 \pmod 3$

  $\Rightarrow \quad 10^k \equiv 1^k \pmod 3, \qquad k \in \mathbb{N},$

  $\Rightarrow \quad a_k 10^k \equiv a_k \pmod 3, \quad a_k \in \{0, \ldots, 9\},$

  $\Rightarrow \quad \boxed{\sum_{k=0}^{n} a_k 10^k \equiv \sum_{k=0}^{n} a_k \pmod 3.}$

Dělitelnost jedenácti:

- $10 \equiv -1 \pmod{11}$

  $\Rightarrow \quad 10^k \equiv (-1)^k \pmod{11}, \qquad k \in \mathbb{N},$

  $\Rightarrow \quad a_k 10^k \equiv a_k (-1)^k \pmod{11}, \quad a_k \in \{0, \ldots, 9\},$

  $\Rightarrow \quad \boxed{\sum_{k=0}^{n} a_k 10^k \equiv \sum_{k=0}^{n} a_k (-1)^k \pmod{11}.}$

Opakování principu fungování RSA:

Opakování principu fungování RSA:

- Vezmi dvě velká prvočísla p, q (typicky stovky cifer) a vynásob je: $n = p \cdot q$.

Opakování principu fungování RSA:

- Vezmi dvě velká prvočísla p, q (typicky stovky cifer) a vynásob je: $n = p \cdot q$.
- Pomocí tohoto n a tzv. exponentu E zašifruj svou zprávu algoritmem "RSA".

Opakování principu fungování RSA:

- Vezmi dvě velká prvočísla p, q (typicky stovky cifer) a vynásob je: $n = p \cdot q$.
- Pomocí tohoto n a tzv. exponentu E zašifruj svou zprávu algoritmem "RSA".
- Nejen zašifrovaná zpráva, ale i ona čísla n a E mohou být klidně zveřejněna, protože:

Opakování principu fungování RSA:

- Vezmi dvě velká prvočísla p, q (typicky stovky cifer) a vynásob je: $n = p \cdot q$.
- Pomocí tohoto n a tzv. exponentu E zašifruj svou zprávu algoritmem "RSA".
- Nejen zašifrovaná zpráva, ale i ona čísla n a E mohou být klidně zveřejněna, protože:
- Pro dešifrování zprávy je potřeba umět rozložit (nebo znát rozklad) n zpátky na součin jeho dvou prvočinitelů p, q.

Opakování principu fungování RSA:

- Vezmi dvě velká prvočísla p, q (typicky stovky cifer) a vynásob je: $n = p \cdot q$.
- Pomocí tohoto n a tzv. exponentu E zašifruj svou zprávu algoritmem "RSA".
- Nejen zašifrovaná zpráva, ale i ona čísla n a E mohou být klidně zveřejněna, protože:
- Pro dešifrování zprávy je potřeba umět rozložit (nebo znát rozklad) n zpátky na součin jeho dvou prvočinitelů p, q.

A jak to teda doopravdy funguje? Jaká matematika je za tím schovaná?

Věta (Malá Fermatova věta)

$a \in \mathbb{N}$,

Věta (Malá Fermatova věta)

$a \in \mathbb{N}$, $p \in \mathcal{P}$,

Věta (Malá Fermatova věta)

$a \in \mathbb{N}$, $p \in \mathcal{P}$, $(a, p) = 1$.

Věta (Malá Fermatova věta)

$a \in \mathbb{N}$, $p \in \mathcal{P}$, $(a, p) = 1$. *Potom*

$$a^{p-1} \equiv 1 \ mod \ p$$

Věta (Malá Fermatova věta)

$a \in \mathbb{N}$, $p \in \mathcal{P}$, $(a, p) = 1$. *Potom*

$$a^{p-1} \equiv 1 \mod p \qquad \text{resp.} \qquad a^{k(p-1)} \equiv 1 \mod p$$

pro všechna $k \in \mathbb{N}$.

Věta (Malá Fermatova věta)

$a \in \mathbb{N}$, $p \in \mathcal{P}$, $(a, p) = 1$. Potom

$$a^{p-1} \equiv 1 \mod p \qquad \text{resp.} \qquad a^{k(p-1)} \equiv 1 \mod p$$

pro všechna $k \in \mathbb{N}$.

Příklad: zkoumejme výsledky modulo $p = 5$ při umocňování čísla $a = 2$ na $m = 1, 2, 3 \ldots$:

Věta (Malá Fermatova věta)

$a \in \mathbb{N}$, $p \in \mathcal{P}$, $(a, p) = 1$. Potom

$$a^{p-1} \equiv 1 \mod p \qquad \text{resp.} \qquad a^{k(p-1)} \equiv 1 \mod p$$

pro všechna $k \in \mathbb{N}$.

Příklad: zkoumejme výsledky modulo $p = 5$ při umocňování čísla $a = 2$ na $m = 1, 2, 3 \ldots$:

$$2^1 \quad 2^2 \quad 2^3 \quad 2^4 \quad 2^5 \quad 2^6 \quad 2^7 \quad 2^8 \quad 2^9 \quad 2^{10}$$

Věta (Malá Fermatova věta)

$a \in \mathbb{N}$, $p \in \mathcal{P}$, $(a, p) = 1$. Potom

$$a^{p-1} \equiv 1 \mod p \qquad \text{resp.} \qquad a^{k(p-1)} \equiv 1 \mod p$$

pro všechna $k \in \mathbb{N}$.

Příklad: zkoumejme výsledky modulo $p = 5$ při umocňování čísla $a = 2$ na $m = 1, 2, 3 \ldots$:

2^1	2^2	2^3	2^4	2^5	2^6	2^7	2^8	2^9	2^{10}
2	4	8	16	32	64	128	256	512	1024

Věta (Malá Fermatova věta)

$a \in \mathbb{N}$, $p \in \mathcal{P}$, $(a, p) = 1$. *Potom*

$$a^{p-1} \equiv 1 \mod p \qquad \text{resp.} \qquad a^{k(p-1)} \equiv 1 \mod p$$

pro všechna $k \in \mathbb{N}$.

Příklad: zkoumejme výsledky modulo $p = 5$ při umocňování čísla $a = 2$ na $m = 1, 2, 3 \ldots$:

2^1	2^2	2^3	2^4	2^5	2^6	2^7	2^8	2^9	2^{10}
2	4	8	16	32	64	128	256	512	1024
2									

Věta (Malá Fermatova věta)

$a \in \mathbb{N}$, $p \in \mathcal{P}$, $(a, p) = 1$. *Potom*

$$a^{p-1} \equiv 1 \mod p \qquad \text{resp.} \qquad a^{k(p-1)} \equiv 1 \mod p$$

pro všechna $k \in \mathbb{N}$.

Příklad: zkoumejme výsledky modulo $p = 5$ při umocňování čísla $a = 2$ na $m = 1, 2, 3 \ldots$:

2^1	2^2	2^3	2^4	2^5	2^6	2^7	2^8	2^9	2^{10}
2	4	8	16	32	64	128	256	512	1024
2	4								

Věta (Malá Fermatova věta)

$a \in \mathbb{N}$, $p \in \mathcal{P}$, $(a, p) = 1$. Potom

$$a^{p-1} \equiv 1 \mod p \qquad \text{resp.} \qquad a^{k(p-1)} \equiv 1 \mod p$$

pro všechna $k \in \mathbb{N}$.

Příklad: zkoumejme výsledky modulo $p = 5$ při umocňování čísla $a = 2$ na $m = 1, 2, 3 \ldots$:

2^1	2^2	2^3	2^4	2^5	2^6	2^7	2^8	2^9	2^{10}
2	4	8	16	32	64	128	256	512	1024
2	4	3							

Věta (Malá Fermatova věta)

$a \in \mathbb{N}$, $p \in \mathcal{P}$, $(a, p) = 1$. Potom

$$a^{p-1} \equiv 1 \mod p \qquad \text{resp.} \qquad a^{k(p-1)} \equiv 1 \mod p$$

pro všechna $k \in \mathbb{N}$.

Příklad: zkoumejme výsledky modulo $p = 5$ při umocňování čísla $a = 2$ na $m = 1, 2, 3 \ldots$:

2^1	2^2	2^3	2^4	2^5	2^6	2^7	2^8	2^9	2^{10}
2	4	8	16	32	64	128	256	512	1024
2	4	3	1						

Věta (Malá Fermatova věta)

$a \in \mathbb{N}$, $p \in \mathcal{P}$, $(a, p) = 1$. Potom

$$a^{p-1} \equiv 1 \mod p \qquad \text{resp.} \qquad a^{k(p-1)} \equiv 1 \mod p$$

pro všechna $k \in \mathbb{N}$.

Příklad: zkoumejme výsledky modulo $p = 5$ při umocňování čísla $a = 2$ na $m = 1, 2, 3 \ldots$:

2^1	2^2	2^3	2^4	2^5	2^6	2^7	2^8	2^9	2^{10}
2	4	8	16	32	64	128	256	512	1024
2	4	3	1	2					

Věta (Malá Fermatova věta)

$a \in \mathbb{N}$, $p \in \mathcal{P}$, $(a, p) = 1$. Potom

$$a^{p-1} \equiv 1 \mod p \qquad \text{resp.} \qquad a^{k(p-1)} \equiv 1 \mod p$$

pro všechna $k \in \mathbb{N}$.

Příklad: zkoumejme výsledky modulo $p = 5$ při umocňování čísla $a = 2$ na $m = 1, 2, 3 \ldots$:

2^1	2^2	2^3	2^4	2^5	2^6	2^7	2^8	2^9	2^{10}
2	4	8	16	32	64	128	256	512	1024
2	4	3	1	2	4				

Věta (Malá Fermatova věta)

$a \in \mathbb{N}$, $p \in \mathcal{P}$, $(a, p) = 1$. Potom

$$a^{p-1} \equiv 1 \mod p \qquad \text{resp.} \qquad a^{k(p-1)} \equiv 1 \mod p$$

pro všechna $k \in \mathbb{N}$.

Příklad: zkoumejme výsledky modulo $p = 5$ při umocňování čísla $a = 2$ na $m = 1, 2, 3 \ldots$:

2^1	2^2	2^3	2^4	2^5	2^6	2^7	2^8	2^9	2^{10}
2	4	8	16	32	64	128	256	512	1024
2	4	3	1	2	4	3			

Věta (Malá Fermatova věta)

$a \in \mathbb{N}$, $p \in \mathcal{P}$, $(a, p) = 1$. Potom

$$a^{p-1} \equiv 1 \mod p \qquad \text{resp.} \qquad a^{k(p-1)} \equiv 1 \mod p$$

pro všechna $k \in \mathbb{N}$.

Příklad: zkoumejme výsledky modulo $p = 5$ při umocňování čísla $a = 2$ na $m = 1, 2, 3 \ldots$:

2^1	2^2	2^3	2^4	2^5	2^6	2^7	2^8	2^9	2^{10}
2	4	8	16	32	64	128	256	512	1024
2	4	3	1	2	4	3	1		

Věta (Malá Fermatova věta)

$a \in \mathbb{N}$, $p \in \mathcal{P}$, $(a, p) = 1$. Potom

$$a^{p-1} \equiv 1 \mod p \qquad \text{resp.} \qquad a^{k(p-1)} \equiv 1 \mod p$$

pro všechna $k \in \mathbb{N}$.

Příklad: zkoumejme výsledky modulo $p = 5$ při umocňování čísla $a = 2$ na $m = 1, 2, 3 \ldots$:

2^1	2^2	2^3	2^4	2^5	2^6	2^7	2^8	2^9	2^{10}
2	4	8	16	32	64	128	256	512	1024
2	4	3	1	2	4	3	1	2	

Věta (Malá Fermatova věta)

$a \in \mathbb{N}$, $p \in \mathcal{P}$, $(a, p) = 1$. Potom

$$a^{p-1} \equiv 1 \mod p \qquad \text{resp.} \qquad a^{k(p-1)} \equiv 1 \mod p$$

pro všechna $k \in \mathbb{N}$.

Příklad: zkoumejme výsledky modulo $p = 5$ při umocňování čísla $a = 2$ na $m = 1, 2, 3 \ldots$:

2^1	2^2	2^3	2^4	2^5	2^6	2^7	2^8	2^9	2^{10}
2	4	8	16	32	64	128	256	512	1024
2	4	3	1	2	4	3	1	2	4

Věta (Malá Fermatova věta)

$a \in \mathbb{N}$, $p \in \mathcal{P}$, $(a, p) = 1$. *Potom*

$$a^{p-1} \equiv 1 \ mod\ p \qquad resp. \qquad a^{k(p-1)} \equiv 1 \ mod\ p$$

pro všechna $k \in \mathbb{N}$.

Příklad: zkoumejme výsledky modulo $p = 5$ při umocňování čísla $a = 2$ na $m = 1, 2, 3 \ldots$:

2^1	2^2	2^3	2^4	2^5	2^6	2^7	2^8	2^9	2^{10}
2	4	8	16	32	64	128	256	512	1024
2	4	3	1	2	4	3	1	2	4

Při pohybu "dokola kolem hodin" (při umocňování), se na ciferníku o prvočíselném počtu hodin občas dostaneme zpátky k jedničce. A umíme říci, kdy.

Věta (Malá Fermatova věta)

$a \in \mathbb{N}$, $p \in \mathcal{P}$, $(a, p) = 1$. *Potom*

$$a^{p-1} \equiv 1 \mod p \qquad \text{resp.} \qquad a^{k(p-1)} \equiv 1 \mod p$$

pro všechna $k \in \mathbb{N}$.

Příklad: zkoumejme výsledky modulo $p = 5$ při umocňování čísla $a = 2$ na $m = 1, 2, 3 \ldots$:

2^1	2^2	2^3	2^4	2^5	2^6	2^7	2^8	2^9	2^{10}
2	4	8	16	32	64	128	256	512	1024
2	4	3	1	2	4	3	1	2	4

Při pohybu "dokola kolem hodin" (při umocňování), se na ciferníku o prvočíselném počtu hodin občas dostaneme zpátky k jedničce. A umíme říci, kdy. Ale taky (po přenásobení a): $\boxed{a^p \equiv a \mod p}$

Věta (Eulerovo zobecnění Malé Fermatovy věty)

$a \in \mathbb{N}$,

Věta (Eulerovo zobecnění Malé Fermatovy věty)

$a \in \mathbb{N}$, $p, q \in \mathcal{P}$,

Věta (Eulerovo zobecnění Malé Fermatovy věty)

$a \in \mathbb{N}, p, q \in \mathcal{P}, n = p \cdot q,$

Věta (Eulerovo zobecnění Malé Fermatovy věty)

$a \in \mathbb{N}$, $p, q \in \mathcal{P}$, $n = p \cdot q$, $(a, n) = 1$. *Potom*

$$a^{(p-1)(q-1)} \equiv 1 \mod n$$

Věta (Eulerovo zobecnění Malé Fermatovy věty)

$a \in \mathbb{N}$, $p, q \in \mathcal{P}$, $n = p \cdot q$, $(a, n) = 1$. *Potom*

$$a^{(p-1)(q-1)} \equiv 1 \mod n \qquad \text{resp.} \qquad a^{k(p-1)(q-1)} \equiv 1 \mod n$$

pro všechna $k \in \mathbb{N}$.

Věta (Eulerovo zobecnění Malé Fermatovy věty)

$a \in \mathbb{N}$, $p, q \in \mathcal{P}$, $n = p \cdot q$, $(a, n) = 1$. *Potom*

$$a^{(p-1)(q-1)} \equiv 1 \mod n \qquad \text{resp.} \qquad a^{k(p-1)(q-1)} \equiv 1 \mod n$$

pro všechna $k \in \mathbb{N}$.

Drobné úpravy Eulerova vztahu:

$$a^{(p-1)(q-1)+1} \equiv a \mod n$$

Věta (Eulerovo zobecnění Malé Fermatovy věty)

$a \in \mathbb{N}$, $p, q \in \mathcal{P}$, $n = p \cdot q$, $(a, n) = 1$. *Potom*

$$a^{(p-1)(q-1)} \equiv 1 \ mod\ n \qquad resp. \qquad a^{k(p-1)(q-1)} \equiv 1 \ mod\ n$$

pro všechna $k \in \mathbb{N}$.

Drobné úpravy Eulerova vztahu:

$$a^{(p-1)(q-1)+1} \equiv a \bmod n$$

$$a^{R} \equiv a \bmod n \quad \text{pro} \quad R = (p-1)\cdot(q-1) + 1$$

Věta (Eulerovo zobecnění Malé Fermatovy věty)

$a \in \mathbb{N}$, $p, q \in \mathcal{P}$, $n = p \cdot q$, $(a, n) = 1$. *Potom*

$$a^{(p-1)(q-1)} \equiv 1 \mod n \qquad \text{resp.} \qquad a^{k(p-1)(q-1)} \equiv 1 \mod n$$

pro všechna $k \in \mathbb{N}$.

Drobné úpravy Eulerova vztahu:

$$a^{(p-1)(q-1)+1} \equiv a \mod n$$

$$a^{R} \equiv a \mod n \quad \text{pro} \quad R = (p-1)\cdot(q-1) + 1$$

$$a^{R} \equiv a \mod n \quad \text{pro} \quad R \equiv 1 \mod (p-1)\cdot(q-1)$$

Věta (Eulerovo zobecnění Malé Fermatovy věty)

$a \in \mathbb{N}$, $p, q \in \mathcal{P}$, $n = p \cdot q$, $(a, n) = 1$. *Potom*

$$a^{(p-1)(q-1)} \equiv 1 \mod n \qquad \text{resp.} \qquad a^{k(p-1)(q-1)} \equiv 1 \mod n$$

pro všechna $k \in \mathbb{N}$.

Drobné úpravy Eulerova vztahu:

$$a^{(p-1)(q-1)+1} \equiv a \mod n$$

$$a^{R} \equiv a \mod n \quad \text{pro} \quad R = (p-1)\cdot(q-1) + 1$$

$$a^{R} \equiv a \mod n \quad \text{pro} \quad R \equiv 1 \mod (p-1)\cdot(q-1)$$

I když to možná ještě není jasné, před očima máme podstatu RSA šifrování, jen R hledáme ve tvaru $E \cdot D$:

Věta (Eulerovo zobecnění Malé Fermatovy věty)

$a \in \mathbb{N}$, $p, q \in \mathcal{P}$, $n = p \cdot q$, $(a, n) = 1$. *Potom*

$$a^{(p-1)(q-1)} \equiv 1 \mod n \qquad \text{resp.} \qquad a^{k(p-1)(q-1)} \equiv 1 \mod n$$

pro všechna $k \in \mathbb{N}$.

Drobné úpravy Eulerova vztahu:

$$a^{(p-1)(q-1)+1} \equiv a \mod n$$

$$a^{R} \equiv a \mod n \quad \text{pro} \quad R = (p-1)\cdot(q-1) + 1$$

$$a^{R} \equiv a \mod n \quad \text{pro} \quad R \equiv 1 \mod (p-1)\cdot(q-1)$$

I když to možná ještě není jasné, před očima máme podstatu RSA šifrování, jen R hledáme ve tvaru $E \cdot D$:

$$a^{E\cdot D} \equiv a \mod n, \quad \text{pokud} \quad E \cdot D \equiv 1 \mod (p-1)\cdot(q-1),$$

Věta (Eulerovo zobecnění Malé Fermatovy věty)

$a \in \mathbb{N}$, $p, q \in \mathcal{P}$, $n = p \cdot q$, $(a, n) = 1$. *Potom*

$$a^{(p-1)(q-1)} \equiv 1 \ mod\ n \qquad resp. \qquad a^{k(p-1)(q-1)} \equiv 1 \ mod\ n$$

pro všechna $k \in \mathbb{N}$.

Drobné úpravy Eulerova vztahu:

$$a^{(p-1)(q-1)+1} \equiv a \bmod n$$
$$a^{R} \equiv a \bmod n \quad \text{pro} \quad R = (p-1)\cdot(q-1) + 1$$
$$a^{R} \equiv a \bmod n \quad \text{pro} \quad R \equiv 1 \bmod (p-1)\cdot(q-1)$$

I když to možná ještě není jasné, před očima máme podstatu RSA šifrování, jen R hledáme ve tvaru $E \cdot D$:

$$a^{E\cdot D} \equiv a \bmod n, \quad \text{pokud} \quad E\cdot D \equiv 1 \bmod (p-1)\cdot(q-1),$$
$$(a^{E})^{D} \equiv a \bmod p\cdot q, \quad \text{pokud} \quad E\cdot D \equiv 1 \bmod (p-1)\cdot(q-1).$$

Ještě jednou:

Ještě jednou: $n = p \cdot q$, $\varphi(n) = (p-1) \cdot (q-1)$.

$$(a^E)^D \equiv a \bmod n, \quad \text{pokud} \quad E \cdot D \equiv 1 \bmod \varphi(n).$$

Ještě jednou: $n = p \cdot q$, $\varphi(n) = (p-1) \cdot (q-1)$.

$$(a^E)^D \equiv a \bmod n, \quad \text{pokud} \quad E \cdot D \equiv 1 \bmod \varphi(n).$$

Podstata šifrování:

Ještě jednou: $n = p \cdot q$, $\varphi(n) = (p-1) \cdot (q-1)$.

$$(a^E)^D \equiv a \bmod n, \quad \text{pokud} \quad E \cdot D \equiv 1 \bmod \varphi(n).$$

Podstata šifrování:

- Zvol dvě (velká) prvočísla p, q a vynásob je: $n = p \cdot q$.

Ještě jednou: $n = p \cdot q$, $\varphi(n) = (p-1) \cdot (q-1)$.

$$(a^E)^D \equiv a \bmod n, \quad \text{pokud} \quad E \cdot D \equiv 1 \bmod \varphi(n).$$

Podstata šifrování:

- Zvol dvě (velká) prvočísla p, q a vynásob je: $n = p \cdot q$.
- Spočti si $\varphi(n) = (p-1) \cdot (q-1)$.

Ještě jednou: $n = p \cdot q$, $\varphi(n) = (p-1) \cdot (q-1)$.

$$(a^E)^D \equiv a \bmod n, \quad \text{pokud} \quad E \cdot D \equiv 1 \bmod \varphi(n).$$

Podstata šifrování:

- Zvol dvě (velká) prvočísla p, q a vynásob je: $n = p \cdot q$.
- Spočti si $\varphi(n) = (p-1) \cdot (q-1)$.
- Zvol tzv. šifrovací exponent E;

Ještě jednou: $n = p \cdot q$, $\varphi(n) = (p-1)\cdot(q-1)$.

$$(a^E)^D \equiv a \bmod n, \quad \text{pokud} \quad E \cdot D \equiv 1 \bmod \varphi(n).$$

Podstata šifrování:

- Zvol dvě (velká) prvočísla p, q a vynásob je: $n = p \cdot q$.
- Spočti si $\varphi(n) = (p-1)\cdot(q-1)$.
- Zvol tzv. šifrovací exponent E; teorie: pokud má existovat D s vlastnostmi výše, pak musí nutně $E < n$ a zároveň E nesoudělné s $\varphi(n)$.

Ještě jednou: $n = p \cdot q$, $\varphi(n) = (p-1) \cdot (q-1)$.

$$(a^E)^D \equiv a \bmod n, \quad \text{pokud} \quad E \cdot D \equiv 1 \bmod \varphi(n).$$

Podstata šifrování:

- Zvol dvě (velká) prvočísla p, q a vynásob je: $n = p \cdot q$.
- Spočti si $\varphi(n) = (p-1) \cdot (q-1)$.
- Zvol tzv. šifrovací exponent E; teorie: pokud má existovat D s vlastnostmi výše, pak musí nutně $E < n$ a zároveň E nesoudělné s $\varphi(n)$.

Zašifruj:

zpráva A

Ještě jednou: $n = p \cdot q$, $\varphi(n) = (p-1)\cdot(q-1)$.

$$(a^E)^D \equiv a \bmod n, \quad \text{pokud} \quad E \cdot D \equiv 1 \bmod \varphi(n).$$

Podstata šifrování:

- Zvol dvě (velká) prvočísla p, q a vynásob je: $n = p \cdot q$.
- Spočti si $\varphi(n) = (p-1)\cdot(q-1)$.
- Zvol tzv. šifrovací exponent E; teorie: pokud má existovat D s vlastnostmi výše, pak musí nutně $E < n$ a zároveň E nesoudělné s $\varphi(n)$.

Zašifruj:

$$\text{zpráva } A \quad \rightsquigarrow \quad \text{zpráva } B = A^E \bmod n$$

Ještě jednou: $n = p \cdot q$, $\varphi(n) = (p-1)\cdot(q-1)$.

$$(a^E)^D \equiv a \bmod n, \quad \text{pokud} \quad E \cdot D \equiv 1 \bmod \varphi(n).$$

Podstata šifrování:

- Zvol dvě (velká) prvočísla p, q a vynásob je: $n = p \cdot q$.
- Spočti si $\varphi(n) = (p-1)\cdot(q-1)$.
- Zvol tzv. šifrovací exponent E; teorie: pokud má existovat D s vlastnostmi výše, pak musí nutně $E < n$ a zároveň E nesoudělné s $\varphi(n)$.

Zašifruj:

$$\text{zpráva } A \quad \rightsquigarrow \quad \text{zpráva } B = A^E \bmod n$$

Dešifrování:

- Spočti exponent D tak, aby $E \cdot D \equiv 1 \bmod \varphi(n)$

Ještě jednou: $n = p \cdot q$, $\varphi(n) = (p-1)\cdot(q-1)$.

$$(a^E)^D \equiv a \bmod n, \quad \text{pokud} \quad E \cdot D \equiv 1 \bmod \varphi(n).$$

Podstata šifrování:

- Zvol dvě (velká) prvočísla p, q a vynásob je: $n = p \cdot q$.
- Spočti si $\varphi(n) = (p-1)\cdot(q-1)$.
- Zvol tzv. šifrovací exponent E; teorie: pokud má existovat D s vlastnostmi výše, pak musí nutně $E < n$ a zároveň E nesoudělné s $\varphi(n)$.

Zašifruj:

$$\text{zpráva } A \quad \rightsquigarrow \quad \text{zpráva } B = A^E \bmod n$$

Dešifrování:

- Spočti exponent D tak, aby $E \cdot D \equiv 1 \bmod \varphi(n)$ (zde hraje roli nesoudělnost E a $\varphi(n)$).

Ještě jednou: $n = p \cdot q$, $\varphi(n) = (p-1)\cdot(q-1)$.

$$(a^E)^D \equiv a \bmod n, \quad \text{pokud} \quad E \cdot D \equiv 1 \bmod \varphi(n).$$

Podstata šifrování:

- Zvol dvě (velká) prvočísla p, q a vynásob je: $n = p \cdot q$.
- Spočti si $\varphi(n) = (p-1)\cdot(q-1)$.
- Zvol tzv. šifrovací exponent E; teorie: pokud má existovat D s vlastnostmi výše, pak musí nutně $E < n$ a zároveň E nesoudělné s $\varphi(n)$.

Zašifruj:

$$\text{zpráva } A \quad \rightsquigarrow \quad \text{zpráva } B = A^E \bmod n$$

Dešifrování:

- Spočti exponent D tak, aby $E \cdot D \equiv 1 \bmod \varphi(n)$ (zde hraje roli nesoudělnost E a $\varphi(n)$).

$$\text{zpráva } B$$

Ještě jednou: $n = p \cdot q$, $\varphi(n) = (p-1)\cdot(q-1)$.

$$(a^E)^D \equiv a \bmod n, \quad \text{pokud} \quad E \cdot D \equiv 1 \bmod \varphi(n).$$

Podstata šifrování:

- Zvol dvě (velká) prvočísla p, q a vynásob je: $n = p \cdot q$.
- Spočti si $\varphi(n) = (p-1)\cdot(q-1)$.
- Zvol tzv. šifrovací exponent E; teorie: pokud má existovat D s vlastnostmi výše, pak musí nutně $E < n$ a zároveň E nesoudělné s $\varphi(n)$.

Zašifruj:

$$\text{zpráva } A \quad \rightsquigarrow \quad \text{zpráva } B = A^E \bmod n$$

Dešifrování:

- Spočti exponent D tak, aby $E \cdot D \equiv 1 \bmod \varphi(n)$ (zde hraje roli nesoudělnost E a $\varphi(n)$).

$$\text{zpráva } B \quad \rightsquigarrow \quad \text{zpráva } A = B^D \bmod n$$

Údaje pro zašifrování lze sdělit veřejně: $n =$ součin dvou velkých prvočísel p, q a $E =$ exponent, např.:

Údaje pro zašifrování lze sdělit veřejně: $n =$ součin dvou velkých prvočísel p, q a $E =$ exponent, např.:

$$
\begin{aligned}
n := \; & 845271249817064394163743655866426570430155 \\
& 721657794435404737134442678244090759775159 \\
& 067609420251500631479031989211405945460126 \\
& 098124464706839595878134450352504117725020 \\
& 988379763560756131117402470008945360895199 \\
& 006475651620544108061441769747900359915806
\end{aligned}
$$

Údaje pro zašifrování lze sdělit veřejně: $n =$ součin dvou velkých prvočísel p, q a $E =$ exponent, např.:

$$
\begin{aligned}
n := \; & 845271249817064394163743655866426570430155 \\
& 721657794435404737134442678244090759775159 \\
& 067609420251500631479031989211405945460126 \\
& 098124464706839595878134450352504117725020 \\
& 988379763560756131117402470008945360895199 \\
& 006475651620544108061441769747900359915806 \\
& 34344053284137960 67, \\
E := \; & 586642657043015572165779443540473713444267 \\
& 824409075977515906760942025150 01.
\end{aligned}
$$

Údaje pro zašifrování lze sdělit veřejně: $n =$ součin dvou velkých prvočísel p, q a $E =$ exponent, např.:

$$
\begin{aligned}
n := \; & 845271249817064394163743655866426570430155 \\
& 721657794435404737134442678244090759775159 \\
& 067609420251500631479031989211405945460126 \\
& 098124464706839595878134450352504117725020 \\
& 988379763560756131117402470008945360895199 \\
& 006475651620544108061441769747900359915806 \\
& 34344053284137960 67, \\
E := \; & 586642657043015572165779443540473713444267 \\
& 824409075977515906760942025150 01.
\end{aligned}
$$

Zpráva A se zašifruje pomocí výpočtu $B = A^E \bmod n$.

Údaje pro zašifrování lze sdělit veřejně: $n =$ součin dvou velkých prvočísel p, q a $E =$ exponent, např.:

$$
\begin{aligned}
n := \; & 845271249817064394163743655866426570430155 \\
& 721657794435404737134442678244090759775159 \\
& 067609420251500631479031989211405945460126 \\
& 098124464706839595878134450352504117725020 \\
& 988379763560756131117402470008945360895199 \\
& 006475651620544108061441769747900359915806 \\
& 343440532841379606 7, \\
E := \; & 586642657043015572165779443540473713444267 \\
& 824409075977515906760942025150 01.
\end{aligned}
$$

Zpráva A se zašifruje pomocí výpočtu $B = A^E \bmod n$.
Dešifrovat bude schopen jen ten, kdo si umí spočíst exponent D pro výpočet $A = B^D \bmod n$.

Údaje pro zašifrování lze sdělit veřejně: $n =$ součin dvou velkých prvočísel p, q a $E =$ exponent, např.:

$$
\begin{aligned}
n := \; & 845271249817064394163743655866426570430155 \\
& 721657794435404737134442678244090759775159 \\
& 067609420251500631479031989211405945460126 \\
& 098124464706839595878134450352504117725020 \\
& 988379763560756131117402470008945360895199 \\
& 006475651620544108061441769747900359915806 \\
& 343440532841379606 7, \\
E := \; & 586642657043015572165779443540473713444267 \\
& 824409075977515906760942025150 01.
\end{aligned}
$$

Zpráva A se zašifruje pomocí výpočtu $B = A^E \bmod n$. Dešifrovat bude schopen jen ten, kdo si umí spočíst exponent D pro výpočet $A = B^D \bmod n$. Exponent D může najít jen ten, kdo zná $\varphi(n) = (p-1)\cdot(q-1)$,

Údaje pro zašifrování lze sdělit veřejně: $n =$ součin dvou velkých prvočísel p, q a $E =$ exponent, např.:

$$
\begin{aligned}
n := \; & 845271249817064394163743655866426570430155 \\
& 721657794435404737134442678244090759775159 \\
& 067609420251500631479031989211405945460126 \\
& 098124464706839595878134450352504117725020 \\
& 988379763560756131117402470008945360895199 \\
& 006475651620544108061441769747900359915806 \\
& 343440532841379606 7, \\
E := \; & 586642657043015572165779443540473713444267 \\
& 824409075977515906760942025150 01.
\end{aligned}
$$

Zpráva A se zašifruje pomocí výpočtu $B = A^E \bmod n$. Dešifrovat bude schopen jen ten, kdo si umí spočíst exponent D pro výpočet $A = B^D \bmod n$. Exponent D může najít jen ten, kdo zná $\varphi(n) = (p-1)\cdot(q-1)$, tj. kdo zná p, q.

Je jasné, že potřebujeme dva efektivní algoritmy:

Je jasné, že potřebujeme dva efektivní algoritmy:

1. Počítání velkých mocnin velkých čísel modulo něco:

Je jasné, že potřebujeme dva efektivní algoritmy:

1. Počítání velkých mocnin velkých čísel modulo něco: při šifrování $B = A^E \bmod n$

Je jasné, že potřebujeme dva efektivní algoritmy:

1. Počítání velkých mocnin velkých čísel modulo něco: při šifrování $B = A^E \bmod n$ i při dešifrování $A = B^D \bmod n$.

Je jasné, že potřebujeme dva efektivní algoritmy:

1. Počítání velkých mocnin velkých čísel modulo něco: při šifrování $B = A^E \bmod n$ i při dešifrování $A = B^D \bmod n$. (Částečně jsme si ukázali.)

Je jasné, že potřebujeme dva efektivní algoritmy:

1. Počítání velkých mocnin velkých čísel modulo něco: při šifrování $B = A^E \bmod n$ i při dešifrování $A = B^D \bmod n$. (Částečně jsme si ukázali.)
2. Počítání "modulární inverze":

Je jasné, že potřebujeme dva efektivní algoritmy:

1. Počítání velkých mocnin velkých čísel modulo něco: při šifrování $B = A^E \bmod n$ i při dešifrování $A = B^D \bmod n$. (Částečně jsme si ukázali.)
2. Počítání "modulární inverze": spočíst D tak, aby $E \cdot D \equiv 1 \bmod \varphi(n)$.

Je jasné, že potřebujeme dva efektivní algoritmy:

1. Počítání velkých mocnin velkých čísel modulo něco: při šifrování $B = A^E \bmod n$ i při dešifrování $A = B^D \bmod n$. (Částečně jsme si ukázali.)
2. Počítání "modulární inverze": spočíst D tak, aby $E \cdot D \equiv 1 \bmod \varphi(n)$.

Na obojí jsou počítačové softwary, založené (např.) na:

Je jasné, že potřebujeme dva efektivní algoritmy:

1. Počítání velkých mocnin velkých čísel modulo něco: při šifrování $B = A^E \bmod n$ i při dešifrování $A = B^D \bmod n$. (Částečně jsme si ukázali.)
2. Počítání "modulární inverze": spočíst D tak, aby $E \cdot D \equiv 1 \bmod \varphi(n)$.

Na obojí jsou počítačové softwary, založené (např.) na:

1. Redukci velkých mocnin pomocí zobecněné Malé Fermatovy věty.

Je jasné, že potřebujeme dva efektivní algoritmy:

1. Počítání velkých mocnin velkých čísel modulo něco: při šifrování $B = A^E \bmod n$ i při dešifrování $A = B^D \bmod n$. (Částečně jsme si ukázali.)
2. Počítání "modulární inverze": spočíst D tak, aby $E \cdot D \equiv 1 \bmod \varphi(n)$.

Na obojí jsou počítačové softwary, založené (např.) na:

1. Redukci velkých mocnin pomocí zobecněné Malé Fermatovy věty.
2. Zobecněném Eukleidově algoritmu a Bézoutově identitě.

Malá smršť čísel, sloužící jako příklad.

Malá smršť čísel, sloužící jako příklad.

Příprava:

Malá smršť čísel, sloužící jako příklad.

Příprava:

- $p = 53$, $q = 61$,

Malá smršť čísel, sloužící jako příklad.

Příprava:

- $p = 53$, $q = 61$, $n = 53 \cdot 61 = 3233$.

Malá smršť čísel, sloužící jako příklad.

Příprava:

- $p = 53$, $q = 61$, $n = 53 \cdot 61 = 3233$.
- $\varphi(n) = (p-1)(q-1) = 3120$.

Malá smršť čísel, sloužící jako příklad.

Příprava:

- $p = 53$, $q = 61$, $n = 53 \cdot 61 = 3233$.
- $\varphi(n) = (p-1)(q-1) = 3120$.
- $E = 17$;

Malá smršť čísel, sloužící jako příklad.

Příprava:

- $p = 53$, $q = 61$, $n = 53 \cdot 61 = 3233$.
- $\varphi(n) = (p-1)(q-1) = 3120$.
- $E = 17$; je menší než $n = 53 \cdot 61 = 3233$

Malá smršť čísel, sloužící jako příklad.

Příprava:

- $p = 53$, $q = 61$, $n = 53 \cdot 61 = 3233$.
- $\varphi(n) = (p-1)(q-1) = 3120$.
- $E = 17$; je menší než $n = 53 \cdot 61 = 3233$ a je nesoudělný s $\varphi(n) = 3120$.

Malá smršť čísel, sloužící jako příklad.

Příprava:

- $p = 53$, $q = 61$, $n = 53 \cdot 61 = 3233$.
- $\varphi(n) = (p-1)(q-1) = 3120$.
- $E = 17$; je menší než $n = 53 \cdot 61 = 3233$ a je nesoudělný s $\varphi(n) = 3120$.

Šifrování:

Malá smršť čísel, sloužící jako příklad.

Příprava:

- $p = 53$, $q = 61$, $n = 53 \cdot 61 = 3233$.
- $\varphi(n) = (p-1)(q-1) = 3120$.
- $E = 17$; je menší než $n = 53 \cdot 61 = 3233$ a je nesoudělný s $\varphi(n) = 3120$.

Šifrování:

- Zpráva $A = 123$.

Malá smršť čísel, sloužící jako příklad.

Příprava:

- $p = 53$, $q = 61$, $n = 53 \cdot 61 = 3233$.
- $\varphi(n) = (p-1)(q-1) = 3120$.
- $E = 17$; je menší než $n = 53 \cdot 61 = 3233$ a je nesoudělný s $\varphi(n) = 3120$.

Šifrování:

- Zpráva $A = 123$.
- Zašifrovaná zpráva $B = 123^{17} = 855 \bmod 3233$.

Malá smršť čísel, sloužící jako příklad.

Příprava:

- $p = 53$, $q = 61$, $n = 53 \cdot 61 = 3233$.
- $\varphi(n) = (p-1)(q-1) = 3120$.
- $E = 17$; je menší než $n = 53 \cdot 61 = 3233$ a je nesoudělný s $\varphi(n) = 3120$.

Šifrování:

- Zpráva $A = 123$.
- Zašifrovaná zpráva $B = 123^{17} = 855 \bmod 3233$.
- Klidně sdělím tzv. klíč $n = 3233$, exponent $E = 17$, zašifrovanou zprávu $B = 855$.

Malá smršť čísel, sloužící jako příklad.

Příprava:

- $p = 53$, $q = 61$, $n = 53 \cdot 61 = 3233$.
- $\varphi(n) = (p-1)(q-1) = 3120$.
- $E = 17$; je menší než $n = 53 \cdot 61 = 3233$ a je nesoudělný s $\varphi(n) = 3120$.

Šifrování:

- Zpráva $A = 123$.
- Zašifrovaná zpráva $B = 123^{17} = 855 \bmod 3233$.
- Klidně sdělím tzv. klíč $n = 3233$, exponent $E = 17$, zašifrovanou zprávu $B = 855$.

Dešifrování:

Malá smršť čísel, sloužící jako příklad.

Příprava:

- $p = 53$, $q = 61$, $n = 53 \cdot 61 = 3233$.
- $\varphi(n) = (p-1)(q-1) = 3120$.
- $E = 17$; je menší než $n = 53 \cdot 61 = 3233$ a je nesoudělný s $\varphi(n) = 3120$.

Šifrování:

- Zpráva $A = 123$.
- Zašifrovaná zpráva $B = 123^{17} = 855 \bmod 3233$.
- Klidně sdělím tzv. klíč $n = 3233$, exponent $E = 17$, zašifrovanou zprávu $B = 855$.

Dešifrování:

- $D = 2753$;

Malá smršť čísel, sloužící jako příklad.

Příprava:

- $p = 53$, $q = 61$, $n = 53 \cdot 61 = 3233$.
- $\varphi(n) = (p-1)(q-1) = 3120$.
- $E = 17$; je menší než $n = 53 \cdot 61 = 3233$ a je nesoudělný s $\varphi(n) = 3120$.

Šifrování:

- Zpráva $A = 123$.
- Zašifrovaná zpráva $B = 123^{17} = 855 \bmod 3233$.
- Klidně sdělím tzv. klíč $n = 3233$, exponent $E = 17$, zašifrovanou zprávu $B = 855$.

Dešifrování:

- $D = 2753$; protože je $E \cdot D = 17 \cdot 2753 \equiv 1 \bmod 3123$.

Malá smršť čísel, sloužící jako příklad.

Příprava:

- $p = 53$, $q = 61$, $n = 53 \cdot 61 = 3233$.
- $\varphi(n) = (p-1)(q-1) = 3120$.
- $E = 17$; je menší než $n = 53 \cdot 61 = 3233$ a je nesoudělný s $\varphi(n) = 3120$.

Šifrování:

- Zpráva $A = 123$.
- Zašifrovaná zpráva $B = 123^{17} = 855 \bmod 3233$.
- Klidně sdělím tzv. klíč $n = 3233$, exponent $E = 17$, zašifrovanou zprávu $B = 855$.

Dešifrování:

- $D = 2753$; protože je $E \cdot D = 17 \cdot 2753 \equiv 1 \bmod 3123$.
- Dešifrování $855^{2753} = 123 \bmod 3233$.

7. Dodatek: Rozptylování obav

7. Dodatek: Rozptylování obav

- **Naše první obava byla: Je to bezpečné?** Co když někdo bude umět rychle rozložit veřejně známé číslo n na součin oněch dvou prvočísel p, q?

7. Dodatek: Rozptylování obav

- **Naše první obava byla: Je to bezpečné?** Co když někdo bude umět rychle rozložit veřejně známé číslo n na součin oněch dvou prvočísel p, q?

(Zatím) je to zcela bezpečné.

7. Dodatek: Rozptylování obav

- **Naše první obava byla: Je to bezpečné?** Co když někdo bude umět rychle rozložit veřejně známé číslo n na součin oněch dvou prvočísel p, q?

(Zatím) je to zcela bezpečné. Je totiž (zatím) nesmírně obtížné (a časově velmi náročné) rozložit číslo o 200+ cifrách na prvočinitele.

7. Dodatek: Rozptylování obav

- **Naše první obava byla: Je to bezpečné?** Co když někdo bude umět rychle rozložit veřejně známé číslo n na součin oněch dvou prvočísel p, q?

(Zatím) je to zcela bezpečné. Je totiž (zatím) nesmírně obtížné (a časově velmi náročné) rozložit číslo o 200+ cifrách na prvočinitele. (Nejsou efektivní algoritmy.)

7. Dodatek: Rozptylování obav

- **Naše první obava byla: Je to bezpečné?** Co když někdo bude umět rychle rozložit veřejně známé číslo n na součin oněch dvou prvočísel p, q?

(Zatím) je to zcela bezpečné. Je totiž (zatím) nesmírně obtížné (a časově velmi náročné) rozložit číslo o 200+ cifrách na prvočinitele. (Nejsou efektivní algoritmy.)

RSA - výzvy (vypsány slušné ceny: 10^4 **i** 10^5 **USD - za 309 cifer, např.)**

7. Dodatek: Rozptylování obav

- **Naše první obava byla: Je to bezpečné?** Co když někdo bude umět rychle rozložit veřejně známé číslo n na součin oněch dvou prvočísel p, q?

(Zatím) je to zcela bezpečné. Je totiž (zatím) nesmírně obtížné (a časově velmi náročné) rozložit číslo o 200+ cifrách na prvočinitele. (Nejsou efektivní algoritmy.)

RSA - výzvy (vypsány slušné ceny: 10^4 **i** 10^5 **USD - za 309 cifer, např.)**

- RSA-250 (250 cifer), rozloženo 2020, výpočet: několik měsíců.

7. Dodatek: Rozptylování obav

- **Naše první obava byla: Je to bezpečné?** Co když někdo bude umět rychle rozložit veřejně známé číslo n na součin oněch dvou prvočísel p, q?

(Zatím) je to zcela bezpečné. Je totiž (zatím) nesmírně obtížné (a časově velmi náročné) rozložit číslo o 200+ cifrách na prvočinitele. (Nejsou efektivní algoritmy.)

RSA - výzvy (vypsány slušné ceny: 10^4 **i** 10^5 **USD - za 309 cifer, např.)**

- RSA-250 (250 cifer), rozloženo 2020, výpočet: několik měsíců.
- RSA-260 (260 cifer) dosud nebylo rozloženo.

- **Naše první obava byla: Je to bezpečné?** Co když někdo bude umět rychle rozložit veřejně známé číslo n na součin oněch dvou prvočísel p, q?

(Zatím) je to zcela bezpečné. Je totiž (zatím) nesmírně obtížné (a časově velmi náročné) rozložit číslo o 200+ cifrách na prvočinitele. (Nejsou efektivní algoritmy.)

RSA - výzvy (vypsány slušné ceny: 10^4 **i** 10^5 **USD - za 309 cifer, např.)**

- RSA-250 (250 cifer), rozloženo 2020, výpočet: několik měsíců.
- RSA-260 (260 cifer) dosud nebylo rozloženo.
- RSA-768B (768 bitů = 232 dekadických cifer) - rozloženo,

- **Naše první obava byla: Je to bezpečné?** Co když někdo bude umět rychle rozložit veřejně známé číslo n na součin oněch dvou prvočísel p, q?

(Zatím) je to zcela bezpečné. Je totiž (zatím) nesmírně obtížné (a časově velmi náročné) rozložit číslo o 200+ cifrách na prvočinitele. (Nejsou efektivní algoritmy.)

RSA - výzvy (vypsány slušné ceny: 10^4 **i** 10^5 **USD - za 309 cifer, např.)**

- RSA-250 (250 cifer), rozloženo 2020, výpočet: několik měsíců.
- RSA-260 (260 cifer) dosud nebylo rozloženo.
- RSA-768B (768 bitů = 232 dekadických cifer) - rozloženo, výpočet: 2 roky na propojených paralelních počítačích.

- **Naše první obava byla: Je to bezpečné?** Co když někdo bude umět rychle rozložit veřejně známé číslo n na součin oněch dvou prvočísel p, q?

(Zatím) je to zcela bezpečné. Je totiž (zatím) nesmírně obtížné (a časově velmi náročné) rozložit číslo o 200+ cifrách na prvočinitele. (Nejsou efektivní algoritmy.)

RSA - výzvy (vypsány slušné ceny: 10^4 **i** 10^5 **USD - za 309 cifer, např.)**

- RSA-250 (250 cifer), rozloženo 2020, výpočet: několik měsíců.
- RSA-260 (260 cifer) dosud nebylo rozloženo.
- RSA-768B (768 bitů = 232 dekadických cifer) - rozloženo, výpočet: 2 roky na propojených paralelních počítačích. Ekvivalent výpočtu na PC (2,2 GHz AMD Opteron): cca 2000 let.

- **Naše druhá obava byla:** Pro důležité šifrování se používají čísla o 300 a více cifrách, tj. součiny prvočísel o cca 150 cifrách. Je jich dost?

- **Naše druhá obava byla:** Pro důležité šifrování se používají čísla o 300 a více cifrách, tj. součiny prvočísel o cca 150 cifrách. Je jich dost? Nevyčerpáme je po nějaké konečné době? Nebude tím někdo mít v ruce úplný seznam možností, který pak bude stačit jen projít?

- **Naše druhá obava byla:** Pro důležité šifrování se používají čísla o 300 a více cifrách, tj. součiny prvočísel o cca 150 cifrách. Je jich dost? Nevyčerpáme je po nějaké konečné době? Nebude tím někdo mít v ruce úplný seznam možností, který pak bude stačit jen projít?

Pomůže Gauss - odhad počtu prvočísel, menších než x:

- **Naše druhá obava byla:** Pro důležité šifrování se používají čísla o 300 a více cifrách, tj. součiny prvočísel o cca 150 cifrách. Je jich dost? Nevyčerpáme je po nějaké konečné době? Nebude tím někdo mít v ruce úplný seznam možností, který pak bude stačit jen projít?

Pomůže Gauss - odhad počtu prvočísel, menších než x: $\pi(x) \approx \frac{x}{\ln x}$;

- **Naše druhá obava byla:** Pro důležité šifrování se používají čísla o 300 a více cifrách, tj. součiny prvočísel o cca 150 cifrách. Je jich dost? Nevyčerpáme je po nějaké konečné době? Nebude tím někdo mít v ruce úplný seznam možností, který pak bude stačit jen projít?

Pomůže Gauss - odhad počtu prvočísel, menších než x: $\pi(x) \approx \frac{x}{\ln x}$; tj. odhad počtu prvočísel o 150 cifrách:

- **Naše druhá obava byla:** Pro důležité šifrování se používají čísla o 300 a více cifrách, tj. součiny prvočísel o cca 150 cifrách. Je jich dost? Nevyčerpáme je po nějaké konečné době? Nebude tím někdo mít v ruce úplný seznam možností, který pak bude stačit jen projít?

Pomůže Gauss - odhad počtu prvočísel, menších než x: $\pi(x) \approx \frac{x}{\ln x}$; tj. odhad počtu prvočísel o 150 cifrách:

$$\pi(10^{150})$$

- **Naše druhá obava byla:** Pro důležité šifrování se používají čísla o 300 a více cifrách, tj. součiny prvočísel o cca 150 cifrách. Je jich dost? Nevyčerpáme je po nějaké konečné době? Nebude tím někdo mít v ruce úplný seznam možností, který pak bude stačit jen projít?

Pomůže Gauss - odhad počtu prvočísel, menších než x: $\pi(x) \approx \frac{x}{\ln x}$; tj. odhad počtu prvočísel o 150 cifrách:

$$\pi(10^{150}) - \pi(10^{149})$$

- **Naše druhá obava byla:** Pro důležité šifrování se používají čísla o 300 a více cifrách, tj. součiny prvočísel o cca 150 cifrách. Je jich dost? Nevyčerpáme je po nějaké konečné době? Nebude tím někdo mít v ruce úplný seznam možností, který pak bude stačit jen projít?

Pomůže Gauss - odhad počtu prvočísel, menších než x: $\pi(x) \approx \frac{x}{\ln x}$; tj. odhad počtu prvočísel o 150 cifrách:

$$\pi(10^{150}) - \pi(10^{149}) \approx \frac{10^{150}}{\ln 10^{150}}$$

- **Naše druhá obava byla:** Pro důležité šifrování se používají čísla o 300 a více cifrách, tj. součiny prvočísel o cca 150 cifrách. Je jich dost? Nevyčerpáme je po nějaké konečné době? Nebude tím někdo mít v ruce úplný seznam možností, který pak bude stačit jen projít?

Pomůže Gauss - odhad počtu prvočísel, menších než x: $\pi(x) \approx \frac{x}{\ln x}$; tj. odhad počtu prvočísel o 150 cifrách:

$$\pi(10^{150}) - \pi(10^{149}) \approx \frac{10^{150}}{\ln 10^{150}} - \frac{10^{149}}{\ln 10^{149}}$$

- **Naše druhá obava byla:** Pro důležité šifrování se používají čísla o 300 a více cifrách, tj. součiny prvočísel o cca 150 cifrách. Je jich dost? Nevyčerpáme je po nějaké konečné době? Nebude tím někdo mít v ruce úplný seznam možností, který pak bude stačit jen projít?

Pomůže Gauss - odhad počtu prvočísel, menších než x: $\pi(x) \approx \frac{x}{\ln x}$; tj. odhad počtu prvočísel o 150 cifrách:

$$\pi(10^{150}) - \pi(10^{149}) \approx \frac{10^{150}}{\ln 10^{150}} - \frac{10^{149}}{\ln 10^{149}} \approx 2{,}6 \cdot 10^{147}.$$

- **Naše druhá obava byla:** Pro důležité šifrování se používají čísla o 300 a více cifrách, tj. součiny prvočísel o cca 150 cifrách. Je jich dost? Nevyčerpáme je po nějaké konečné době? Nebude tím někdo mít v ruce úplný seznam možností, který pak bude stačit jen projít?

Pomůže Gauss - odhad počtu prvočísel, menších než x: $\pi(x) \approx \frac{x}{\ln x}$; tj. odhad počtu prvočísel o 150 cifrách:

$$\pi(10^{150}) - \pi(10^{149}) \approx \frac{10^{150}}{\ln 10^{150}} - \frac{10^{149}}{\ln 10^{149}} \approx 2{,}6 \cdot 10^{147}.$$

To je obrovské číslo.

- **Naše druhá obava byla:** Pro důležité šifrování se používají čísla o 300 a více cifrách, tj. součiny prvočísel o cca 150 cifrách. Je jich dost? Nevyčerpáme je po nějaké konečné době? Nebude tím někdo mít v ruce úplný seznam možností, který pak bude stačit jen projít?

Pomůže Gauss - odhad počtu prvočísel, menších než x: $\pi(x) \approx \frac{x}{\ln x}$; tj. odhad počtu prvočísel o 150 cifrách:

$$\pi(10^{150}) - \pi(10^{149}) \approx \frac{10^{150}}{\ln 10^{150}} - \frac{10^{149}}{\ln 10^{149}} \approx 2{,}6 \cdot 10^{147}.$$

To je obrovské číslo. Počet atomů ve vesmíru $\approx 10^{80}$.

- **Naše druhá obava byla:** Pro důležité šifrování se používají čísla o 300 a více cifrách, tj. součiny prvočísel o cca 150 cifrách. Je jich dost? Nevyčerpáme je po nějaké konečné době? Nebude tím někdo mít v ruce úplný seznam možností, který pak bude stačit jen projít?

Pomůže Gauss - odhad počtu prvočísel, menších než x: $\pi(x) \approx \frac{x}{\ln x}$; tj. odhad počtu prvočísel o 150 cifrách:

$$\pi(10^{150}) - \pi(10^{149}) \approx \frac{10^{150}}{\ln 10^{150}} - \frac{10^{149}}{\ln 10^{149}} \approx 2{,}6 \cdot 10^{147}.$$

To je obrovské číslo. Počet atomů ve vesmíru $\approx 10^{80}$.

Každý atom ve vesmíru může mít $10^{67} \cdot 10^{67}$ "svých" dvojic prvočísel o 150 cifrách pro své vlastní šifrovací potřeby.

8. Závěr

"Matematika je jediný skutečně zaručený způsob, jak přijít o zdravý rozum."

Albert Einstein

8. Závěr

"Matematika je jediný skutečně zaručený způsob, jak přijít o zdravý rozum."

Albert Einstein

(Přednášející věří, že se tak ještě nestalo, ale chápe, že nic se nemá přehánět.)

8. Závěr

"Matematika je jediný skutečně zaručený způsob, jak přijít o zdravý rozum."

Albert Einstein

(Přednášející věří, že se tak ještě nestalo, ale chápe, že nic se nemá přehánět.)

Děkuji za pozornost.

Mirko Rokyta
KMA MFF Praha
Sokolovská 83
Praha 8 - Karlín

mirko.rokyta@mff.cuni.cz