O zajímavosti čísel

Luboš Pick (KMA MFF UK Praha)

OSMA, VŠB Ostrava, 20.11. 2012

Poděkování za podporu

Poděkování za podporu



Svět vědy
CZ 1.07/2.3.00/35.0018

Motto

Motto

O různých typech lidí.

Motto

O různých typech lidí.

Na světě existují tři typy lidí: ti, kteří dovedou počítat, a ti, kteří počítat nedovedou.

Jak nás vidí velikáni

Jak nás vidí velikáni

Propagace matematiky:

Jak nás vidí velikáni

Propagace matematiky:

Matematikové jsou jako Francouzi. Cokoli jim řeknete, přeloží si do svého vlastního jazyka, čímž vznikne něco jiného.

(J.W. Goethe)

Čísla jsou ohromně zajímavá

Čísla jsou ohromně zajímavá

VĚTA 1 (o zajímavosti čísel):

Čísla jsou ohromně zajímavá

VĚTA 1 (o zajímavosti čísel):

Všechna přirozená čísla jsou zajímavá.

Čísla jsou ohromně zajímavá

VĚTA 1 (o zajímavosti čísel):

Všechna přirozená čísla jsou zajímavá.

Důkaz.

Čísla jsou ohromně zajímavá

VĚTA 1 (o zajímavosti čísel):

Všechna přirozená čísla jsou zajímavá.

Důkaz.

Předpokládejme pro spor, že tvrzení věty neplatí.

Čísla jsou ohromně zajímavá

VĚTA 1 (o zajímavosti čísel):

Všechna přirozená čísla jsou zajímavá.

Důkaz.

Předpokládejme pro spor, že tvrzení věty neplatí.
Pak existuje nejmenší nezajímavé přirozené číslo.

Čísla jsou ohromně zajímavá

VĚTA 1 (o zajímavosti čísel):

Všechna přirozená čísla jsou zajímavá.

Důkaz.

Předpokládejme pro spor, že tvrzení věty neplatí.
Pak existuje nejmenší nezajímavé přirozené číslo.
Je to nejmenší číslo s jistou netriviální vlastností.

Čísla jsou ohromně zajímavá

VĚTA 1 (o zajímavosti čísel):

Všechna přirozená čísla jsou zajímavá.

Důkaz.

Předpokládejme pro spor, že tvrzení věty neplatí.
Pak existuje nejmenší nezajímavé přirozené číslo.
Je to nejmenší číslo s jistou netriviální vlastností.
To jej činí zajímavým.

Čísla jsou ohromně zajímavá

VĚTA 1 (o zajímavosti čísel):

Všechna přirozená čísla jsou zajímavá.

Důkaz.

Předpokládejme pro spor, že tvrzení věty neplatí.
Pak existuje nejmenší nezajímavé přirozené číslo.
Je to nejmenší číslo s jistou netriviální vlastností.
To jej činí zajímavým.
Dostáváme spor.

Otázky filosofické a jiné

Otázky filosofické a jiné

- Odkdy lidstvo počítá?

Otázky filosofické a jiné

- Odkdy lidstvo počítá?
- Objevily se nejprve číslovky **základní** nebo **řadové**?

Otázky filosofické a jiné

- Odkdy lidstvo počítá?
- Objevily se nejprve číslovky **základní** nebo **řadové**?

pro **základní**: každodenní potřeby

Otázky filosofické a jiné

- Odkdy lidstvo počítá?
- Objevily se nejprve číslovky **základní** nebo **řadové**?

pro **základní**: každodenní potřeby

pro **řadové**: rituály s daným pořadím prvků

Radikální duchovní skoky v nazírání na čísla

Radikální duchovní skoky v nazírání na čísla

- *rozdíly* nutné pro přežití: jeden vlk nebo smečka vlků?

Radikální duchovní skoky v nazírání na čísla

- *rozdíly* nutné pro přežití: jeden vlk nebo smečka vlků?
- *společné prvky:* dvě ruce, dvě nohy, dvě tělesa na nebi

Tři už jsou dav

Tři už jsou dav

první rozlišení: jeden - dva - mnoho

Tři už jsou dav

první rozlišení: jeden - dva - mnoho

Číslo 3: sumersky: ‘es’ (mnoho)

Tři už jsou dav

první rozlišení: jeden - dva - mnoho

Číslo 3: sumersky: ‘es’ (mnoho)

etnika v Torresově průlivu: dvojková soustava:

Tři už jsou dav

první rozlišení: jeden - dva - mnoho

Číslo 3: sumersky: ‘es’ (mnoho)

etnika v Torresově průlivu: dvojková soustava:
1 = urapun

Tři už jsou dav

první rozlišení: jeden - dva - mnoho

Číslo 3: sumersky: ‘es’ (mnoho)

etnika v Torresově průlivu: dvojková soustava:
1 = urapun
2 = okosa

Tři už jsou dav

první rozlišení: jeden - dva - mnoho

Číslo 3: sumersky: ‘es’ (mnoho)

etnika v Torresově průlivu: dvojková soustava:
1 = urapun
2 = okosa
3 = okosa-urapun

Tři už jsou dav

první rozlišení: jeden - dva - mnoho

Číslo 3: sumersky: ‘es’ (mnoho)

etnika v Torresově průlivu: dvojková soustava:
1 = urapun
2 = okosa
3 = okosa-urapun
4 = okosa-okosa

Tři už jsou dav

první rozlišení: jeden - dva - mnoho

Číslo 3: sumersky: ‘es’ (mnoho)

etnika v Torresově průlivu: dvojková soustava:
1 = urapun
2 = okosa
3 = okosa-urapun
4 = okosa-okosa
5 = ras (= mnoho)

Skok mezi dvojkou a trojkou

Skok mezi dvojkou a trojkou

Ilustrace: **množné číslo a zlomek** v evropských jazycích

Skok mezi dvojkou a trojkou

Ilustrace: **množné číslo a zlomek** v evropských jazycích

tři-třetina	dvě-polovina
three-third	two-half
šaloš-šliš	štajim-hetsi
három-harmad	kettö-fél
trei-treilea	doi-jumate
tair-trydydd	dau-hanner

Oblíbená čísla

Oblíbená čísla

Máte nějaké oblíbené číslo?

Oblíbená čísla

Máte nějaké oblíbené číslo?

A v čem spočívá jeho obliba?

Neoblíbená čísla

Neoblíbená čísla

Nebo snad máte nějaké neoblíbené číslo?

Neoblíbená čísla

Nebo snad máte nějaké neoblíbené číslo?

A v čem spočívá jeho neobliba?

Příklad z vysoké politiky

Příklad z vysoké politiky

Ronald a Nancy Reaganovi si nechali změnit adresu

Příklad z vysoké politiky

Ronald a Nancy Reaganovi si nechali změnit adresu

ze **St. Cloud Road 666**

Příklad z vysoké politiky

Ronald a Nancy Reaganovi si nechali změnit adresu

ze St. Cloud Road 666

na St. Cloud Road 668

Příklad z vysoké politiky

Ronald a Nancy Reaganovi si nechali změnit adresu

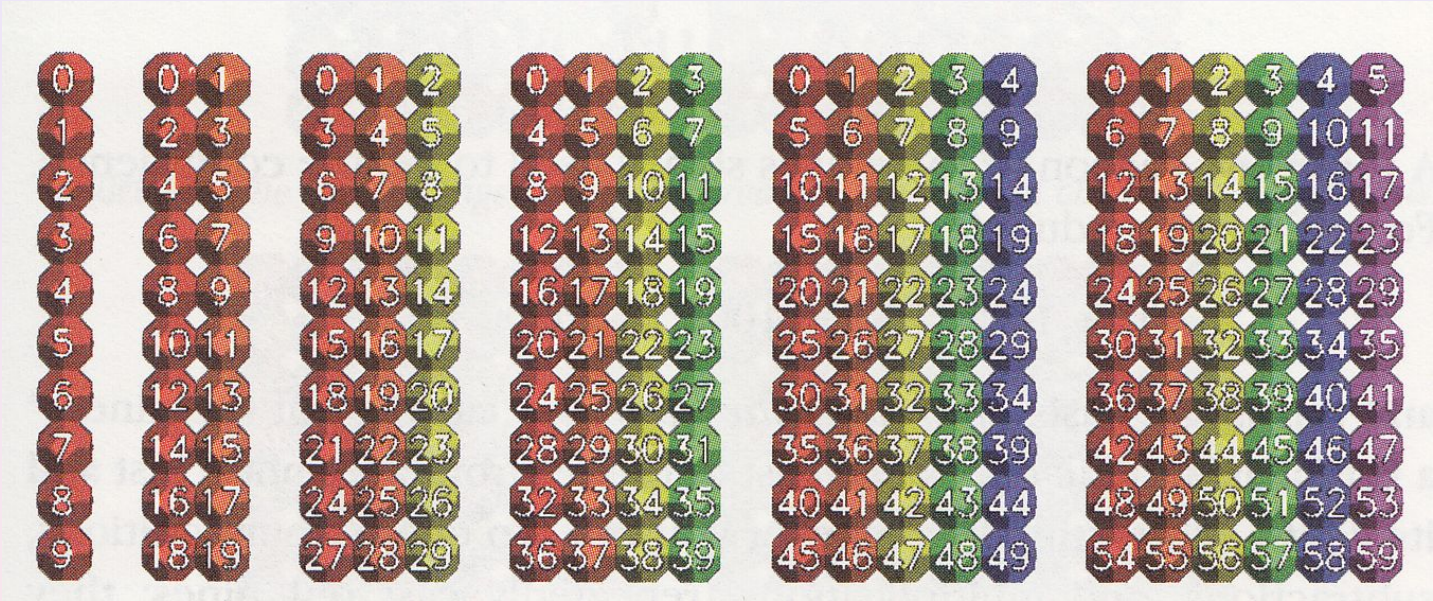
ze St. Cloud Road 666

na St. Cloud Road 668

(na základě přesvědčení, že 666 je ďáblovo číslo).

Residuální třídy - grafické znázornění

Residuální třídy - grafické znázornění



Multiplikační tabulka a kvadráty

Multiplikační tabulka a kvadráty

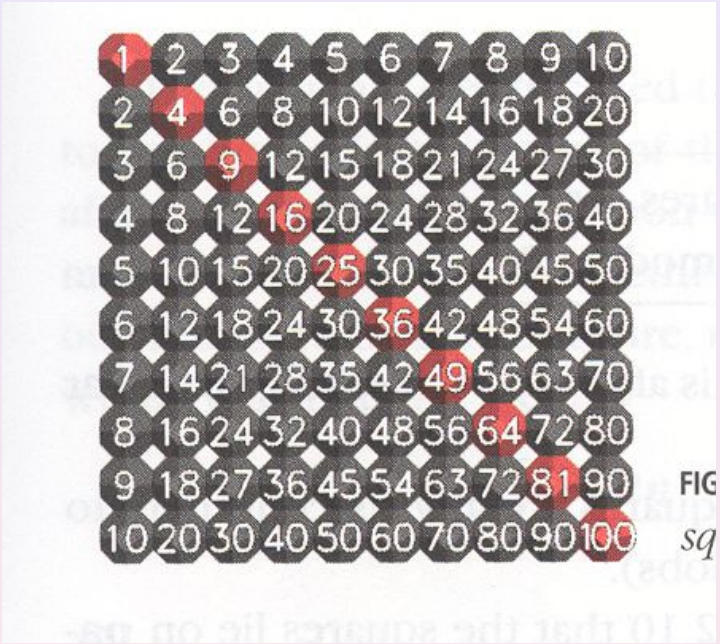
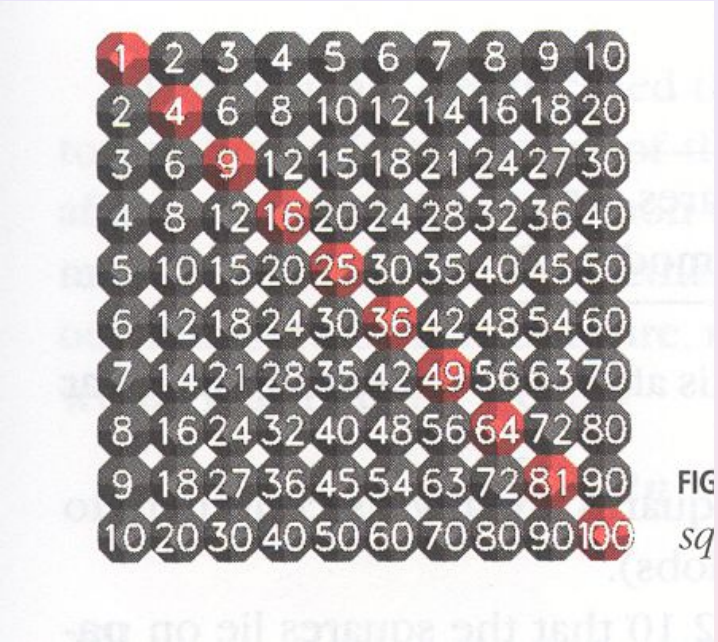


FIG
sq

Multiplikační tabulka a kvadráty



Na multiplikační tabulce jsou kvadráty na diagonále.

Kvadrátická residua

Kvadrátická residua

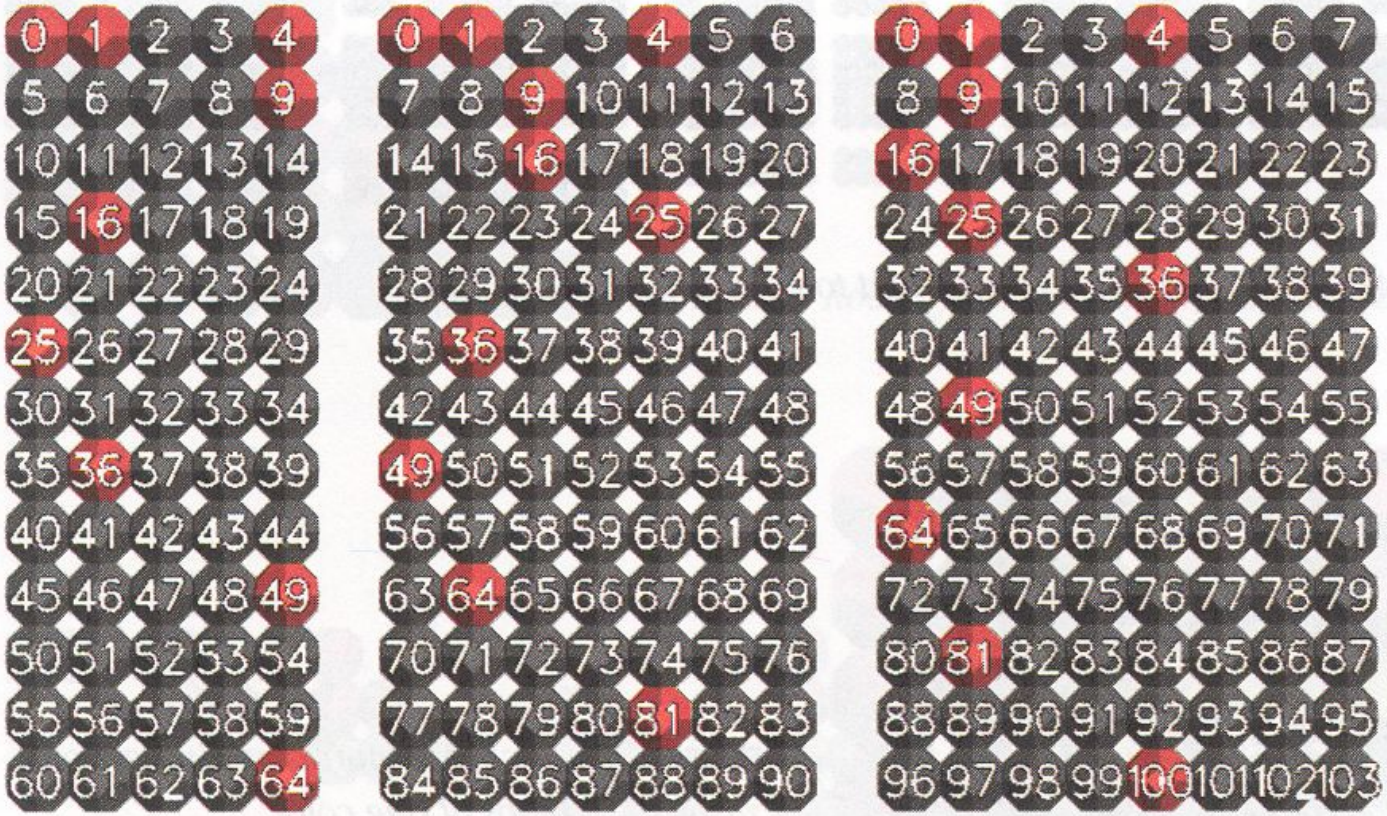


FIGURE 2.10 *Quadratic residues: the residue classes in which the squares lie.*

Kvadrátická residua

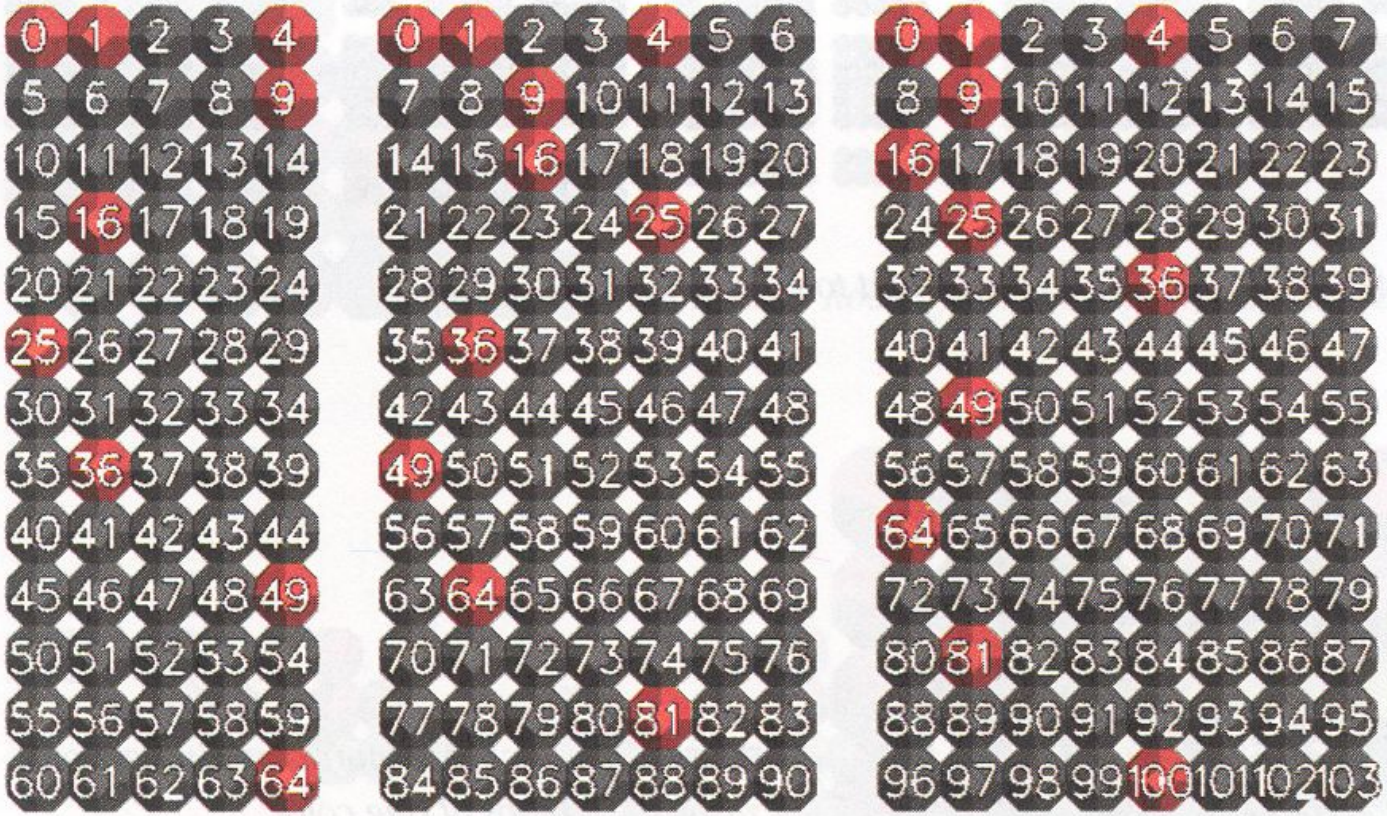


FIGURE 2.10 *Quadratic residues: the residue classes in which the squares lie.*

Na residuálních tabulkách tvoří kvadráty paraboly.

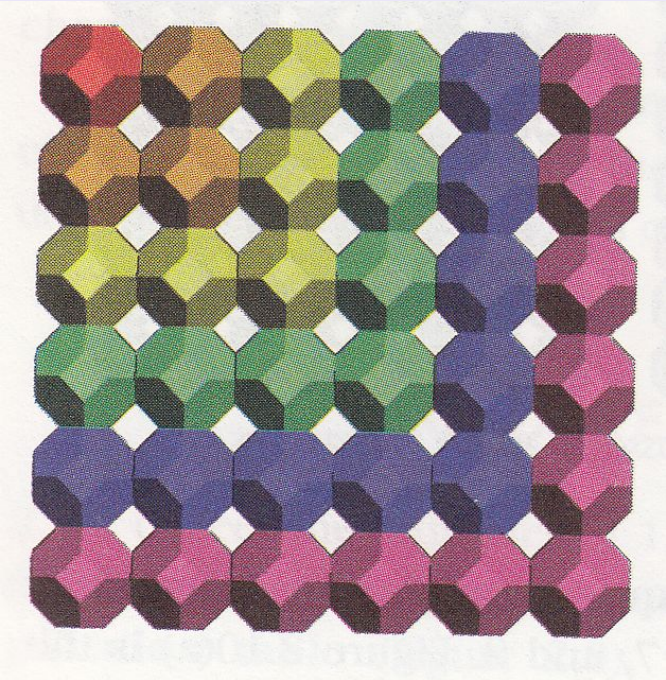
Gnómóny

Gnómóny

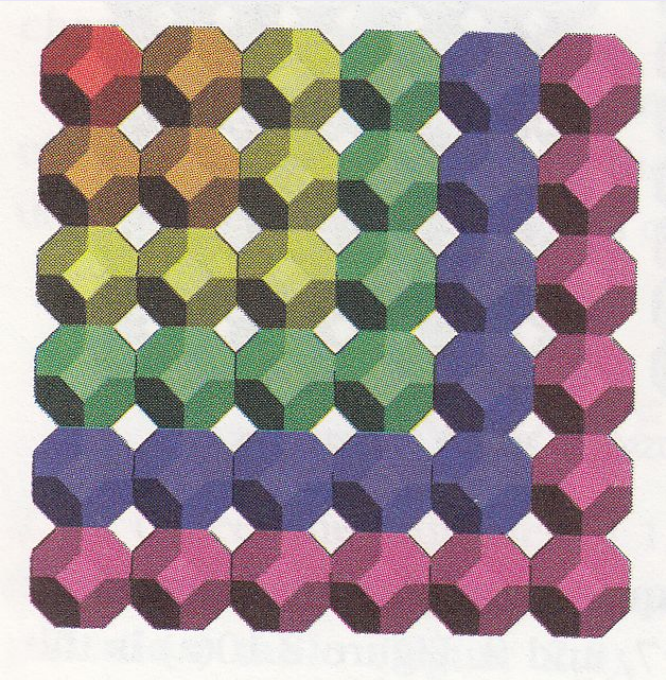
Staří Řekové nazývali **gnómónem** tvar, který je možné přidat ke geometrickému objektu, aby vznikl větší objekt stejného tvaru.

Gnómóny graficky

Gnómóny graficky

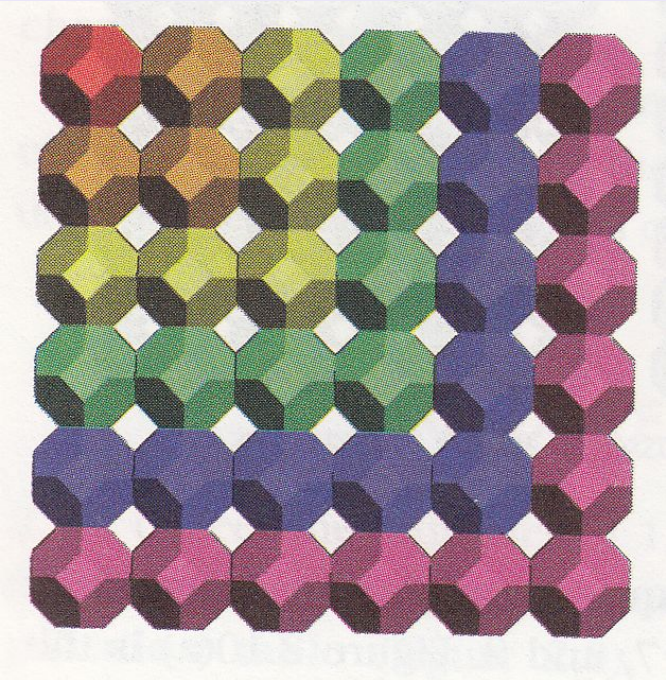


Gnómóny graficky



Každý gnómón obsahuje lichý počet kuliček stejné barvy.

Gnómóny graficky

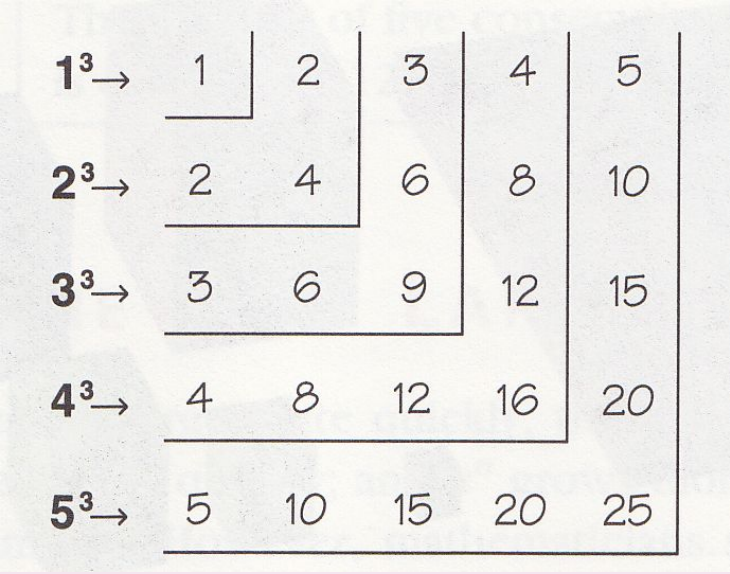


Každý gnómón obsahuje lichý počet kuliček stejné barvy.

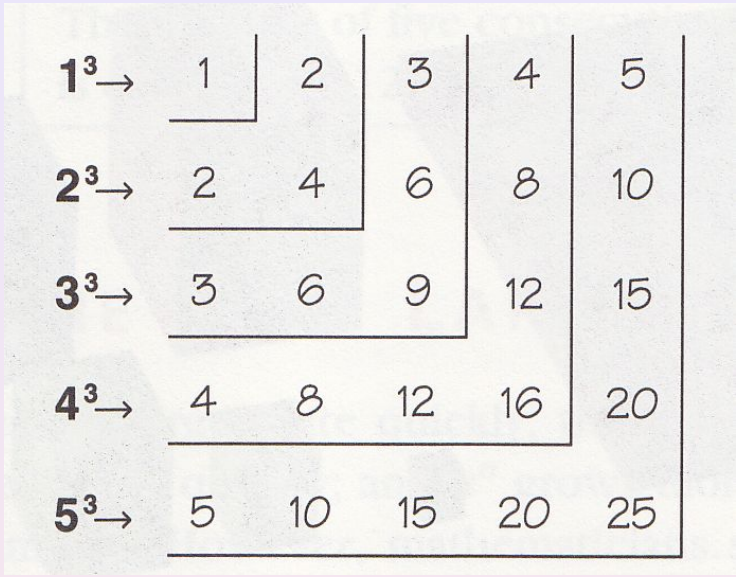
$$n^2 = 1 + 3 + \cdots + 2n - 1$$

Gnómóny znovu

Gnómóny znovu

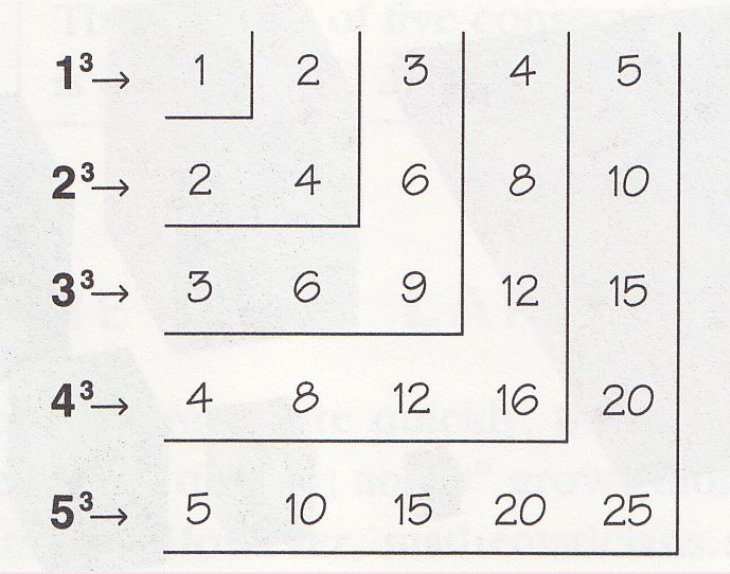


Gnómóny znovu



součty dávají třetí mocniny

Gnómóny znovu

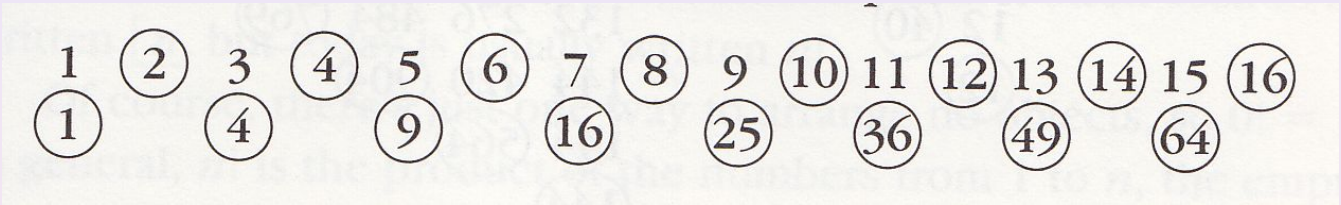


součty dávají třetí mocniny

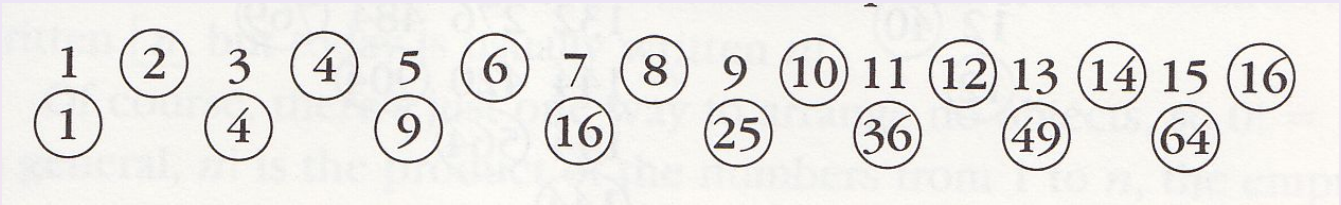
$$1^3 + \cdots + n^3 = (1 + \cdots + n)^2.$$

Moessnerova magie

Moessnerova magie

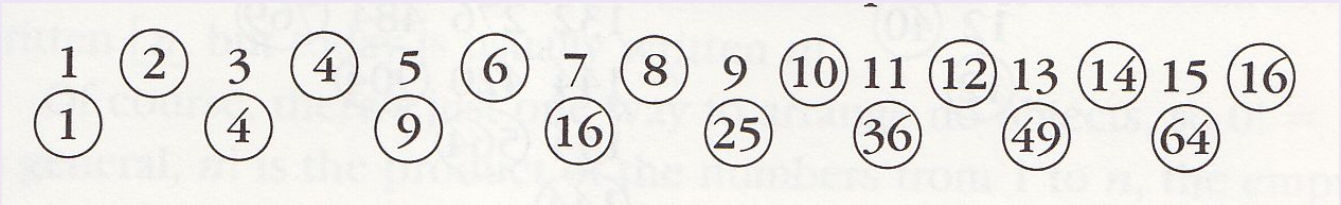


Moessnerova magie



kroužkujeme sudá čísla a pak součty zbylých čísel,

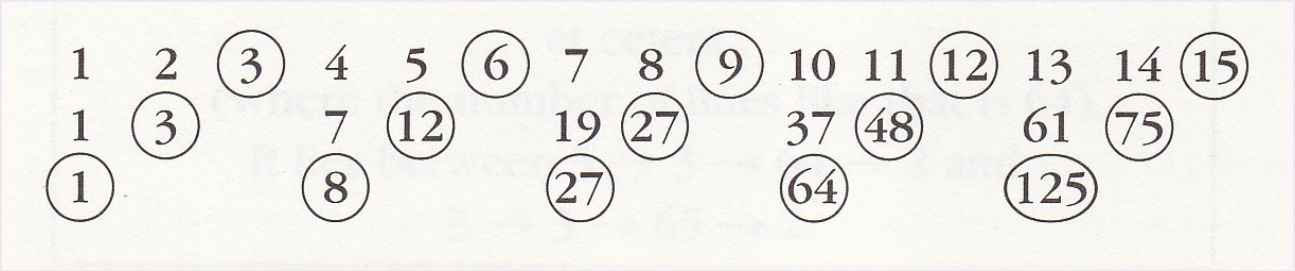
Moessnerova magie



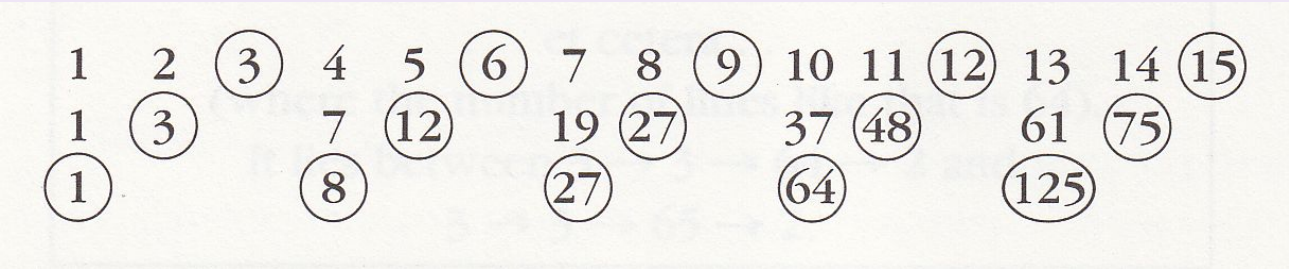
kroužkujeme sudá čísla a pak součty zbylých čísel, dostaneme kvadráty

Moessnerova magie - pokračování

Moessnerova magie - pokračování



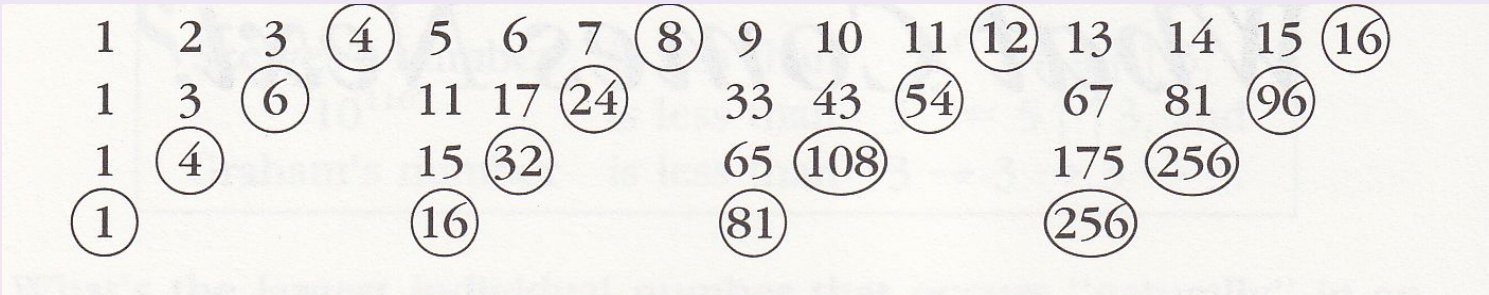
Moessnerova magie - pokračování



obdobný postup pro třetí mocniny

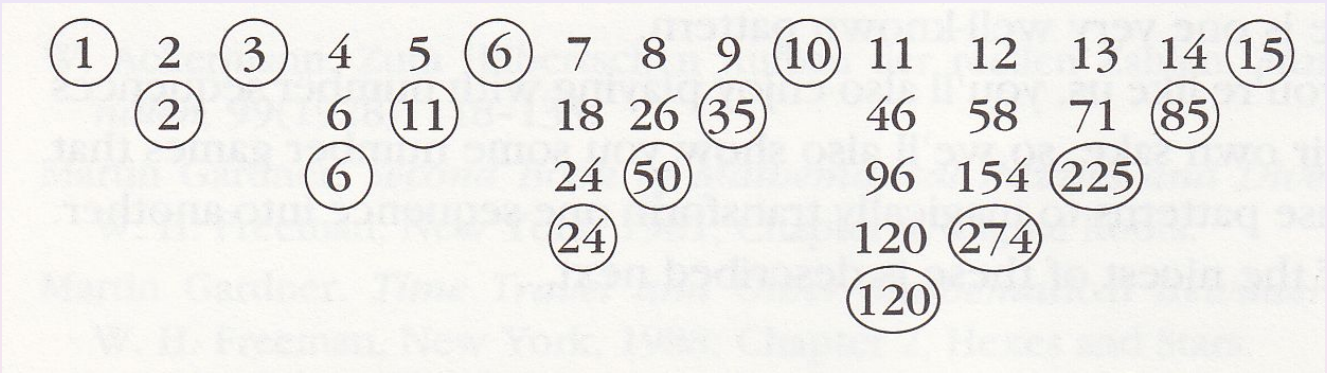
Moessnerova magie - pokračování

Moessnerova magie - pokračování

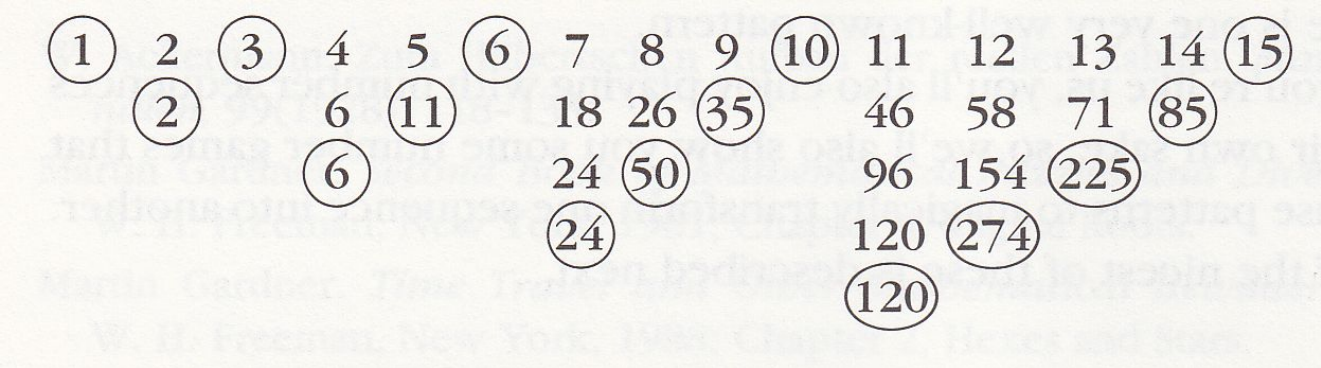


Moessnerova magie - pokračování

Moessnerova magie - pokračování



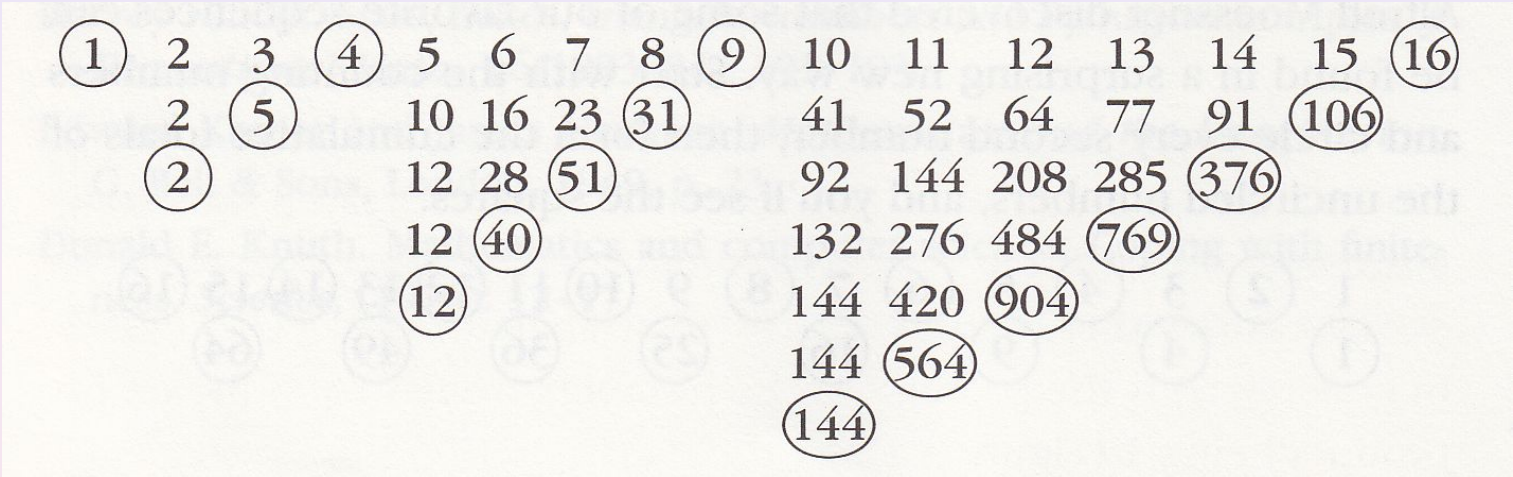
Moessnerova magie - pokračování



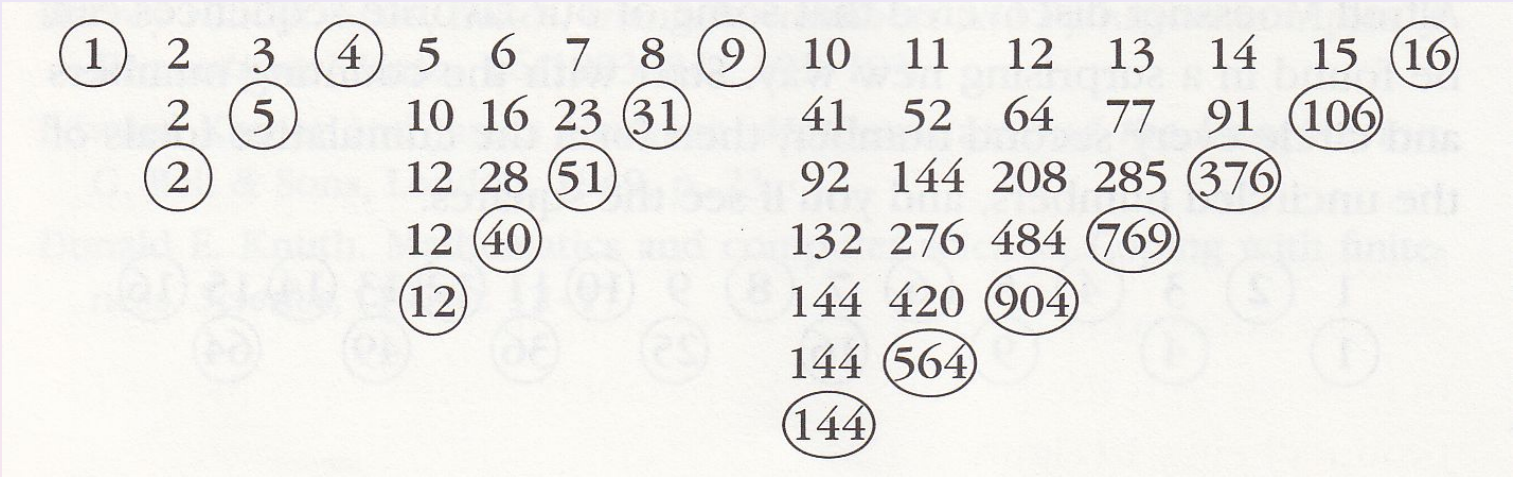
obdobný postup pro faktoriály

Moessnerova magie - pokračování

Moessnerova magie - pokračování



Moessnerova magie - pokračování



co je toto za posloupnost?

Moessnerova magie - pokračování

Moessnerova magie - pokračování

vysvětlení:

Moessnerova magie - pokračování

vysvětlení: kvadráty jsou dány pomocí součtů

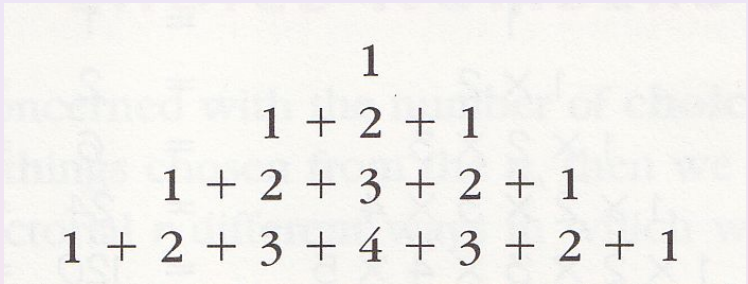
Moessnerova magie - pokračování

vysvětlení: kvadráty jsou dány pomocí součtů

$$1$$
$$1 + 2 + 1$$
$$1 + 2 + 3 + 2 + 1$$
$$1 + 2 + 3 + 4 + 3 + 2 + 1$$

Moessnerova magie - pokračování

vysvětlení: kvadráty jsou dány pomocí součtů



a naše posloupnost splňuje

Moessnerova magie - pokračování

vysvětlení: kvadráty jsou dány pomocí součtů

$$1$$
$$1 + 2 + 1$$
$$1 + 2 + 3 + 2 + 1$$
$$1 + 2 + 3 + 4 + 3 + 2 + 1$$

a naše posloupnost splňuje

$$1$$
$$1 \times 2 \times 1$$
$$1 \times 2 \times 3 \times 2 \times 1$$
$$1 \times 2 \times 3 \times 4 \times 3 \times 2 \times 1$$

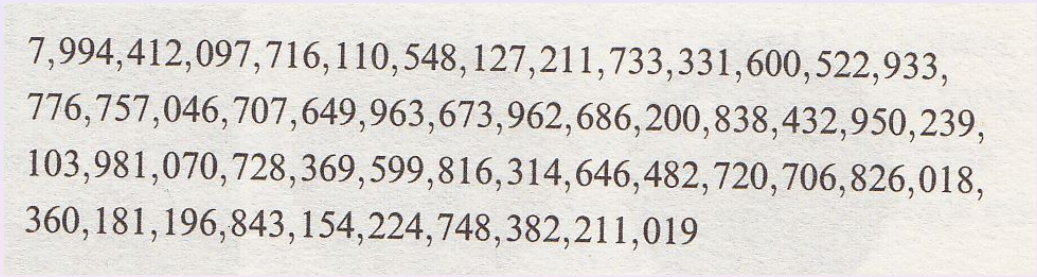
Bacha na věc!

Bacha na věc!

V roce 1994 získal **Roger Schlafly** patent USA číslo 5,373,560 na dvě prvočísla

Bacha na věc!

V roce 1994 získal **Roger Schlafly** patent USA číslo 5,373,560 na dvě prvočísla


7,994,412,097,716,110,548,127,211,733,331,600,522,933,
776,757,046,707,649,963,673,962,686,200,838,432,950,239,
103,981,070,728,369,599,816,314,646,482,720,706,826,018,
360,181,196,843,154,224,748,382,211,019

a

Bacha na věc!

V roce 1994 získal **Roger Schlafly** patent USA číslo 5,373,560 na dvě prvočísla

7,994,412,097,716,110,548,127,211,733,331,600,522,933,
776,757,046,707,649,963,673,962,686,200,838,432,950,239,
103,981,070,728,369,599,816,314,646,482,720,706,826,018,
360,181,196,843,154,224,748,382,211,019

a

103,864,912,054,654,272,074,839,999,186,936,834,171,066,
194,620,139,675,036,534,769,616,693,904,589,884,931,513,
925,858,861,749,077,079,643,532,169,815,633,834,450,952,
832,125,258,174,795,234,553,238,258,030,222,937,772,878,
346,831,083,983,624,739,712,536,721,932,666,180,751,292,
001,388,772,039,413,446,493,758,317,344,413,531,957,900,
028,443,184,983,069,698,882,035,800,332,668,237,985,846,
170,997,572,388,089

Bacha na věc!

V roce 1994 získal **Roger Schlafly** patent USA číslo 5,373,560 na dvě prvočísla

7,994,412,097,716,110,548,127,211,733,331,600,522,933,
776,757,046,707,649,963,673,962,686,200,838,432,950,239,
103,981,070,728,369,599,816,314,646,482,720,706,826,018,
360,181,196,843,154,224,748,382,211,019

a

103,864,912,054,654,272,074,839,999,186,936,834,171,066,
194,620,139,675,036,534,769,616,693,904,589,884,931,513,
925,858,861,749,077,079,643,532,169,815,633,834,450,952,
832,125,258,174,795,234,553,238,258,030,222,937,772,878,
346,831,083,983,624,739,712,536,721,932,666,180,751,292,
001,388,772,039,413,446,493,758,317,344,413,531,957,900,
028,443,184,983,069,698,882,035,800,332,668,237,985,846,
170,997,572,388,089

Bez jeho svolení s nimi nikdo nesmí pracovat!

Palindromatická čísla

Palindromatická čísla

Palindromatické číslo 134 757 431 splňuje:

$$
\begin{aligned}
&= 1^7 + 2^3 + 3^8 + 4^5 + 5^4 + 6^2 + 7^1 + 8^9 + 9^6 \\
&= 1^7 + 2^5 + 3^8 + 4^1 + 5^2 + 6^4 + 7^3 + 8^9 + 9^6 \\
&= 1^7 + 2^8 + 3^4 + 4^2 + 5^3 + 6^5 + 7^1 + 8^9 + 9^6
\end{aligned}
$$

Palindromatická čísla

Palindromatické číslo 134 757 431 splňuje:

$$
\begin{aligned}
&= 1^7 + 2^3 + 3^8 + 4^5 + 5^4 + 6^2 + 7^1 + 8^9 + 9^6 \\
&= 1^7 + 2^5 + 3^8 + 4^1 + 5^2 + 6^4 + 7^3 + 8^9 + 9^6 \\
&= 1^7 + 2^8 + 3^4 + 4^2 + 5^3 + 6^5 + 7^1 + 8^9 + 9^6
\end{aligned}
$$

(každá číslice se vyskytuje vždy právě jednou jako základ a právě jednou jako exponent).

Palindromatická čísla - pokračování

Palindromatická čísla - pokračování

Nejmenší palindromatické číslo obsahující všech deset číslic je 10234567898765432 01.

Palindromatická čísla - pokračování

Nejmenší palindromatické číslo obsahující všech deset číslic je 10234567898765432 01.

Nejmenší palindromatické **prvočíslo** obsahující všech deset číslic je 10234569878965432 01.

Palindromatická čísla - pokračování

Nejmenší palindromatické číslo obsahující všech deset číslic je 10234567898765432 01.

Nejmenší palindromatické **prvočíslo** obsahující všech deset číslic je 10234569878965432 01.

Palindromatické číslo 323323 je součinem po sobě jdoucích prvočísel 7, 11, 13, 17 a 19 a navíc je rovno součtu

$$1^7 + 2^2 + 3^8 + 4^9 + 5^5 + 6^6 + 7^1 + 8^4 + 9^3.$$

Palindromatická čísla - pokračování

Nejmenší palindromatické číslo obsahující všech deset číslic je 10234567898765432 01.

Nejmenší palindromatické **prvočíslo** obsahující všech deset číslic je 10234569878965432 01.

Palindromatické číslo 323323 je součinem po sobě jdoucích prvočísel 7, 11, 13, 17 a 19 a navíc je rovno součtu

$$1^7 + 2^2 + 3^8 + 4^9 + 5^5 + 6^6 + 7^1 + 8^4 + 9^3.$$

Součet druhých mocnin prvních devíti lichých čísel je roven 969.

Palindromatická čísla - pokračování

Palindromatická čísla - pokračování

$$1234321 = 11^2 \cdot 101^2.$$

Palindromatická čísla - pokračování

$$1234321 = 11^2 \cdot 101^2.$$

$$1111 = 11^2 + 12^2 + 13^2 + 14^2 + 15^2 + 16^2.$$

Palindromatická čísla - pokračování

$$1234321 = 11^2 \cdot 101^2.$$

$$1111 = 11^2 + 12^2 + 13^2 + 14^2 + 15^2 + 16^2.$$

$$11111111 = 1234567 \cdot 9 + 8.$$

Palindromatická čísla - pokračování

$$1234321 = 11^2 \cdot 101^2.$$

$$1111 = 11^2 + 12^2 + 13^2 + 14^2 + 15^2 + 16^2.$$

$$11111111 = 1234567 \cdot 9 + 8.$$

$$\frac{2 \cdot 22 \cdot 222 \cdot 2222}{2 \cdot 2 \cdot 2 \cdot 2} = 1356531 = 11 \cdot 123321.$$

Palindromatická čísla - pokračování

$$1234321 = 11^2 \cdot 101^2.$$

$$1111 = 11^2 + 12^2 + 13^2 + 14^2 + 15^2 + 16^2.$$

$$11111111 = 1234567 \cdot 9 + 8.$$

$$\frac{2 \cdot 22 \cdot 222 \cdot 2222}{2 \cdot 2 \cdot 2 \cdot 2} = 1356531 = 11 \cdot 123321.$$

Rozcvička: dokažte, že každé palindromatické číslo o sudém počtu číslic je dělitelné 11.

Hodně velká čísla

Hodně velká čísla

Některé posloupnosti rostou opravdu rychle.

Hodně velká čísla

Některé posloupnosti rostou opravdu rychle. Například n^2,

Hodně velká čísla

Některé posloupnosti rostou opravdu rychle. Například n^2, n^3,

Hodně velká čísla

Některé posloupnosti rostou opravdu rychle. Například n^2, n^3, $n!$,

Hodně velká čísla

Některé posloupnosti rostou opravdu rychle. Například n^2, n^3, $n!$, n^n.

Hodně velká čísla

Některé posloupnosti rostou opravdu rychle. Například n^2, n^3, $n!$, n^n.

Zavedeme symbol $m \uparrow n$.

Hodně velká čísla

Některé posloupnosti rostou opravdu rychle. Například n^2, n^3, $n!$, n^n.

Zavedeme symbol $m \uparrow n$.

Podobně jako $mn = m + m + \cdots + m$ (n kopií),

Hodně velká čísla

Některé posloupnosti rostou opravdu rychle. Například n^2, n^3, $n!$, n^n.

Zavedeme symbol $m \uparrow n$.

Podobně jako $mn = m + m + \cdots + m$ (n kopií), označíme

$$\begin{aligned} m \uparrow n &= mm \cdots m \quad (n \text{ kopií}) \\ m \uparrow\uparrow n &= m \uparrow m \cdots \uparrow m \quad (n \text{ kopií}) \\ m \uparrow\uparrow\uparrow n &= m \uparrow\uparrow m \cdots \uparrow\uparrow m \quad (n \text{ kopií}) \\ m \uparrow\uparrow\uparrow\uparrow n &= m \uparrow\uparrow\uparrow m \cdots \uparrow\uparrow\uparrow m \quad (n \text{ kopií}) \end{aligned}$$

a tak dále.

Ackermannova čísla

Ackermannova čísla

Takto vyzbrojeni, definujeme *n*-té **Ackermannovo číslo** podle modelu

Ackermannova čísla

Takto vyzbrojeni, definujeme ***n*-té Ackermannovo číslo** podle modelu

$$1 \uparrow 1, \quad 2 \uparrow\uparrow 2, \quad 3 \uparrow\uparrow\uparrow 3, \quad 4 \uparrow\uparrow\uparrow\uparrow 4, \quad \ldots$$

Příklady

Příklady

První Ackermannovo číslo je 1.

Příklady

První Ackermannovo číslo je 1.

Druhé Ackermannovo číslo je $2 \uparrow\uparrow 2 = 2 \uparrow 2 = 4$.

Příklady

První Ackermannovo číslo je 1.

Druhé Ackermannovo číslo je $2 \uparrow\uparrow 2 = 2 \uparrow 2 = 4$.

Třetí Ackermannovo číslo je

$$3^{3^{3^{\cdots}}},$$

Příklady

První Ackermannovo číslo je 1.

Druhé Ackermannovo číslo je $2 \uparrow\uparrow 2 = 2 \uparrow 2 = 4$.

Třetí Ackermannovo číslo je

$$3^{3^{3^{\cdots}}},$$

kde počet trojek je roven $3^{3^3} = 7625597484987$.

Příklady

První Ackermannovo číslo je 1.

Druhé Ackermannovo číslo je $2 \uparrow\uparrow 2 = 2 \uparrow 2 = 4$.

Třetí Ackermannovo číslo je

$$3^{3^{3^{\cdots}}},$$

kde počet trojek je roven $3^{3^3} = 7625597484987$.

Má někdo představu, jak velké je čtvrté Ackermannovo číslo?

Velká praktická čísla

Velká praktická čísla

OTÁZKA: Jaké je největší *použitelné* číslo?

Velká praktická čísla

OTÁZKA: Jaké je největší *použitelné* číslo?

Kandidát: **Skewesovo číslo:** $10^{10^{10^{34}}}$.

Velká praktická čísla

OTÁZKA: Jaké je největší *použitelné* číslo?

Kandidát: **Skewesovo číslo:** $10^{10^{10^{34}}}$.

Kde se vzalo?

Hustota prvočísel

Hustota prvočísel

Mezi čísly 1 a 100 se nachází 25 prvočísel.

Hustota prvočísel

Mezi čísly 1 a 100 se nachází 25 prvočísel.

Mezi čísly 10 000 000 a 10 000 100 jsou jen dvě.

Hustota prvočísel

Mezi čísly 1 a 100 se nachází 25 prvočísel.

Mezi čísly 10 000 000 a 10 000 100 jsou jen dvě.

Otázka: Jak se vyvíjí hustota prvočísel $\pi(N)/N$ v závislosti na $N \in \mathbb{N}$?

Hustota prvočísel

Mezi čísly 1 a 100 se nachází 25 prvočísel.

Mezi čísly 10 000 000 a 10 000 100 jsou jen dvě.

Otázka: Jak se vyvíjí hustota prvočísel $\pi(N)/N$ v závislosti na $N \in \mathbb{N}$?

1780 Legendreova domněnka : $\pi(N)/N \approx \frac{1}{\ln N}$.

Hustota prvočísel

Mezi čísly 1 a 100 se nachází 25 prvočísel.

Mezi čísly 10 000 000 a 10 000 100 jsou jen dvě.

Otázka: Jak se vyvíjí hustota prvočísel $\pi(N)/N$ v závislosti na $N \in \mathbb{N}$?

1780 Legendreova domněnka : $\pi(N)/N \approx \frac{1}{\ln N}$.

(Legendreovu domněnku potvrdili Hadamard a Vallée-Poussin v roce 1896.)

Hustota prvočísel - tabulky

Hustota prvočísel - tabulky

up to 100	there are	25	primes, i.e. 1 in	4
10^3		168		6
10^4		1229		8.1
10^5		9592		10.4
10^6		78498		12.7
10^7		664579		15
10^8		5761455		17.3
10^9		50847534		19.8

Hustota prvočísel - tabulky

up to 100	there are	25	primes, i.e. 1 in	4
10^3		168		6
10^4		1229		8.1
10^5		9592		10.4
10^6		78498		12.7
10^7		664579		15
10^8		5761455		17.3
10^9		50847534		19.8

Kolik je prvočísel?

Gaussova domněnka

Gaussova domněnka

1791 Gauss: Legendreova domněnka by se měla upravit do tvaru:

Gaussova domněnka

1791 Gauss: Legendreova domněnka by se měla upravit do tvaru:

$$\pi(N)/N \approx \mathrm{Li}(N).$$

Gaussova domněnka

1791 Gauss: Legendreova domněnka by se měla upravit do tvaru:

$$\pi(N)/N \approx \mathrm{Li}(N).$$

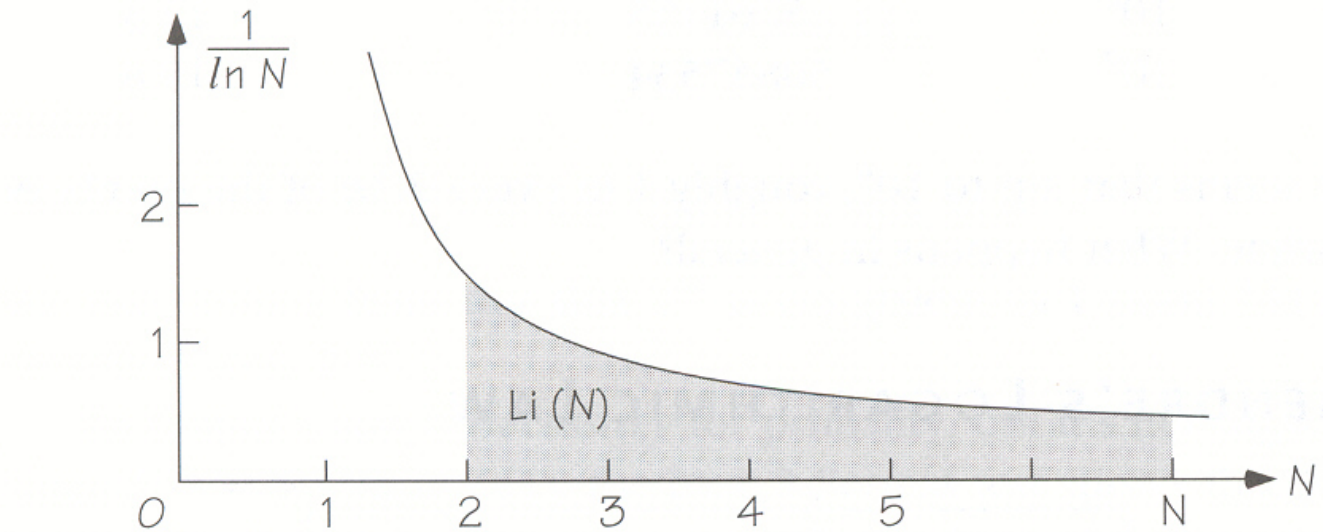


FIGURE 5.2 *Gauss's guess.*

Riemannova domněnka

Riemannova domněnka

1859 Riemann: Legendreova (a Gaussova) domněnka by se měly upravit do tvaru:

Riemannova domněnka

1859 Riemann: Legendreova (a Gaussova) domněnka by se měly upravit do tvaru:

$$\pi(N)/N \approx \mathrm{Li}(N) - \frac{1}{2}Li(N^{\frac{1}{2}}) - \frac{1}{3}Li(N^{\frac{1}{3}}) - \frac{1}{5}Li(N^{\frac{1}{5}}) + \frac{1}{6}Li(N^{\frac{1}{6}}) - \dots$$

Riemannova domněnka

1859 Riemann: Legendreova (a Gaussova) domněnka by se měly upravit do tvaru:

$$\pi(N)/N \approx \mathrm{Li}(N) - \frac{1}{2}Li(N^{\frac{1}{2}}) - \frac{1}{3}Li(N^{\frac{1}{3}}) - \frac{1}{5}Li(N^{\frac{1}{5}}) + \frac{1}{6}Li(N^{\frac{1}{6}}) - \dots$$

Koeficient u $\frac{1}{2}Li(N^{\frac{1}{2}})$ je **Möbiovo číslo** $\mu(n)$, definované předpisem

$$\mu(n) = \begin{cases} 0, & \text{je-li } n \text{ dělitelné nějakým kvadrátem} \\ 1, & \text{má-li } n \text{ sudý počet prvočíselných dělitelů} \\ -1, & \text{má-li } n \text{ lichý počet prvočíselných dělitelů.} \end{cases}$$

Legendre–Gauss–Riemann

Legendre–Gauss–Riemann

N	Number of Primes up to N, $\pi(n)$	... and the errors in: Legendre's Law $\frac{N}{\ln N} - \pi(N)$	Gauss's Guess $\mathrm{Li}(N) - \pi(N)$	Riemann's Refinement $R(N) - \pi(N)$
10	4	0	2	
10^2	25	−3	5	1
10^3	168	−23	10	0
10^4	1229	−143	17	−2
10^5	9592	−906	38	−5
10^6	78498	−6116	130	29
10^7	664579	−44158	339	88
10^8	5761455	−332774	754	97
10^9	50847534	−2592592	1701	−79
10^{10}	455052511	−20758029	3104	−1828
10^{11}	4118054813	−169923159	11588	−2318
10^{12}	37607912018	−1416705183	38263	−1476
10^{13}	346065536839	−11992858452	108971	−5773
10^{14}	3204941750802	−102838308636	314890	−19200
10^{15}	29844570422669	−891604962452	1052619	73218
10^{16}	279238341033925	−7804289844393	3214632	327052

TABLE 5.2 *Errors (to the nearest integer) in formulas for* $\pi(n)$.

Výsledky klání

Výsledky klání

Gaussova domněnka je lepší než Legendreova.

Výsledky klání

Gaussova domněnka je lepší než Legendreova.

Riemannova domněnka je *většinou* ještě o něco lepší (přesně v 99,07%) případech.

Výsledky klání

Gaussova domněnka je lepší než Legendreova.

Riemannova domněnka je *většinou* ještě o něco lepší (přesně v 99,07%) případech.

1914 J.E. Littlewood: Existují případy, kdy je Gaussova domněnka lepší než Riemannova!

Výsledky klání

Gaussova domněnka je lepší než Legendreova.

Riemannova domněnka je *většinou* ještě o něco lepší (přesně v 99,07%) případech.

1914 J.E. Littlewood: Existují případy, kdy je Gaussova domněnka lepší než Riemannova!

Skewes: toto musí nastat alespoň jednou před Skewesovým číslem.

Velká praktická čísla

Velká praktická čísla

Vada na kráse: Skewesovo číslo lze zmenšit, například na 10^{1167}.

Velká praktická čísla

Vada na kráse: Skewesovo číslo lze zmenšit, například na 10^{1167}.

OTÁZKA: Jaké je největší *nezlepšitelné použitelné* číslo?

Velká praktická čísla

Vada na kráse: Skewesovo číslo lze zmenšit, například na 10^{1167}.

OTÁZKA: Jaké je největší *nezlepšitelné použitelné* číslo?

Příklad (kandidát): řád grupy zvané *monster simple group*

Velká praktická čísla

Vada na kráse: Skewesovo číslo lze zmenšit, například na 10^{1167}.

OTÁZKA: Jaké je největší *nezlepšitelné použitelné* číslo?

Příklad (kandidát): řád grupy zvané *monster simple group*

8080 17424 79451 28758 86459 90496 17101 57005 75436 80000 00000.

Richardův paradox

Richardův paradox

V roce 1905 objevil **Jules Richard** zajímavý paradox.

Richardův paradox

V roce 1905 objevil **Jules Richard** zajímavý paradox.

Některé slovní útvary a věty v češtině **definují nějaké číslo**,

Richardův paradox

V roce 1905 objevil **Jules Richard** zajímavý paradox.

Některé slovní útvary a věty v češtině **definují nějaké číslo**, zatímco jiné nikoli.

Richardův paradox

V roce 1905 objevil **Jules Richard** zajímavý paradox.

Některé slovní útvary a věty v češtině **definují nějaké číslo**, zatímco jiné nikoli.

Například výraz *rok nástupu* ***Ferdinanda I. Habsburského*** *na český trůn* definuje číslo

Richardův paradox

V roce 1905 objevil **Jules Richard** zajímavý paradox.

Některé slovní útvary a věty v češtině **definují nějaké číslo**, zatímco jiné nikoli.

Například výraz *rok nástupu* ***Ferdinanda I. Habsburského*** *na český trůn* definuje číslo **1526**.

Richardův paradox

V roce 1905 objevil **Jules Richard** zajímavý paradox.

Některé slovní útvary a věty v češtině **definují nějaké číslo**, zatímco jiné nikoli.

Například výraz *rok nástupu* ***Ferdinanda I. Habsburského*** *na český trůn* definuje číslo **1526**.

Naopak, výraz *historický význam Habsburků na českém trůně*

Richardův paradox

V roce 1905 objevil **Jules Richard** zajímavý paradox.

Některé slovní útvary a věty v češtině **definují nějaké číslo**, zatímco jiné nikoli.

Například výraz *rok nástupu* ***Ferdinanda I. Habsburského*** *na český trůn* definuje číslo **1526**.

Naopak, výraz *historický význam Habsburků na českém trůně* žádné číslo nedefinuje.

Richardův paradox

V roce 1905 objevil **Jules Richard** zajímavý paradox.

Některé slovní útvary a věty v češtině **definují nějaké číslo**, zatímco jiné nikoli.

Například výraz *rok nástupu **Ferdinanda I. Habsburského** na český trůn* definuje číslo **1526**.

Naopak, výraz *historický význam Habsburků na českém trůně* žádné číslo nedefinuje.

Jiný příklad: výraz *rok, ve kterém **Baník** poprvé vyhrál ligu*, definuje číslo

Richardův paradox

V roce 1905 objevil **Jules Richard** zajímavý paradox.

Některé slovní útvary a věty v češtině **definují nějaké číslo**, zatímco jiné nikoli.

Například výraz *rok nástupu **Ferdinanda I. Habsburského** na český trůn* definuje číslo **1526**.

Naopak, výraz *historický význam Habsburků na českém trůně* žádné číslo nedefinuje.

Jiný příklad: výraz *rok, ve kterém **Baník** poprvé vyhrál ligu*, definuje číslo **1976**.

Richardův paradox

V roce 1905 objevil **Jules Richard** zajímavý paradox.

Některé slovní útvary a věty v češtině **definují nějaké číslo**, zatímco jiné nikoli.

Například výraz *rok nástupu* ***Ferdinanda I. Habsburského*** *na český trůn* definuje číslo **1526**.

Naopak, výraz *historický význam Habsburků na českém trůně* žádné číslo nedefinuje.

Jiný příklad: výraz *rok, ve kterém* ***Baník*** *poprvé vyhrál ligu*, definuje číslo **1976**.

Naopak, výraz **Sparta fuj!**

Richardův paradox

V roce 1905 objevil **Jules Richard** zajímavý paradox.

Některé slovní útvary a věty v češtině **definují nějaké číslo**, zatímco jiné nikoli.

Například výraz *rok nástupu **Ferdinanda I. Habsburského** na český trůn* definuje číslo **1526**.

Naopak, výraz *historický význam Habsburků na českém trůně* žádné číslo nedefinuje.

Jiný příklad: výraz *rok, ve kterém **Baník** poprvé vyhrál ligu*, definuje číslo **1976**.

Naopak, výraz **Sparta fuj!** žádné číslo nedefinuje.

Richardův paradox - pokračování

Richardův paradox - pokračování

OTÁZKA:

Richardův paradox - pokračování

OTÁZKA: Které číslo definuje následující slovní spojení?

Richardův paradox - pokračování

OTÁZKA: Které číslo definuje následující slovní spojení?

"Nejmenší číslo, které není možné žádným způsobem definovat pomocí českého slovního útvaru obsahujícího počet slov ostře menší než dvacet."

Richardův paradox - pokračování

OTÁZKA: Které číslo definuje následující slovní spojení?

“Nejmenší číslo, které není možné žádným způsobem definovat pomocí českého slovního útvaru obsahujícího počet slov ostře menší než dvacet.”

Ať je toto číslo jakékoli, právě jsme jej definovali pomocí českého slovního útvaru o pouhých devatenácti slovech.

Číslo skoro celé

Číslo skoro celé

Martin Gardner

Číslo skoro celé

Martin Gardner měl v oblibě

Číslo skoro celé

Martin Gardner měl v oblibě tzv. **Ramanujanovo číslo**

Číslo skoro celé

Martin Gardner měl v oblibě tzv. **Ramanujanovo číslo**

$$e^{\pi\sqrt{163}}.$$

Číslo skoro celé

Martin Gardner měl v oblibě tzv. **Ramanujanovo číslo**

$$e^{\pi\sqrt{163}}.$$

Toto číslo je **"skoro celé"**.

Číslo skoro celé

Martin Gardner měl v oblibě tzv. **Ramanujanovo číslo**

$$e^{\pi\sqrt{163}}.$$

Toto číslo je **"skoro celé"**. Přesněji, je rovno

Číslo skoro celé

Martin Gardner měl v oblibě tzv. **Ramanujanovo číslo**

$$e^{\pi\sqrt{163}}.$$

Toto číslo je **"skoro celé"**. Přesněji, je rovno

$$262\,537\,412\,640\,768\,743,999\,999\,999\,999\,25\ldots \approx 640\,320^3 + 744.$$

Číslo skoro celé

Martin Gardner měl v oblibě tzv. **Ramanujanovo číslo**

$$e^{\pi\sqrt{163}}.$$

Toto číslo je **"skoro celé"**. Přesněji, je rovno

$$262\,537\,412\,640\,768\,743,999\,999\,999\,999\,25\ldots \approx 640\,320^3 + 744.$$

1.4.1975 napsal do *Scientific American*, že je celé, což málem vyvolalo jisté nepokoje.

Další motto

Další motto

O různých typech lidí.

Další motto

O různých typech lidí.

Na světě existuje 10 typů ajťáků:

Další motto

O různých typech lidí.

Na světě existuje 10 typů ajťáků: ti, kteří rozumí binárnímu zápisu čísel, a ti ostatní.

Ještě jedno motto

Ještě jedno motto

O různých typech lidí.

Ještě jedno motto

O různých typech lidí.

Na světě existuje 41 typů lidí: ti, kteří mají nějaké číslo natolik v oblibě, že jej použijí při každé příležitosti, a ti ostatní.

Ještě jedno motto

O různých typech lidí.

Na světě existuje 41 typů lidí: ti, kteří mají nějaké číslo natolik v oblibě, že jej použijí při každé příležitosti, a ti ostatní.

POZNÁMKA: Je to sice pitomost, ale při troše pozornosti odtud můžete zjistit oblíbené číslo autora tohoto příspěvku.

Číslo 41

Číslo 41

ZADÁNÍ:

ZADÁNÍ:

Najděte alespoň jedno **přirozené číslo** $n < 41$ tak, aby

$$n^2 - n + 41$$

nebylo prvočíslo.

Číslo 41 - řešení

Číslo 41 - řešení

Řešení:

Číslo 41 - řešení

Řešení:

Žádné takové číslo neexistuje (!)

Číslo 41 - řešení

Řešení:

Žádné takové číslo neexistuje (!)

Polynom

$$n^2 - n + 41$$

Řešení:

Žádné takové číslo neexistuje (!)

Polynom

$$n^2 - n + 41$$

totiž dává pro $n = 1, \ldots, 40$ následující seznam:

Číslo 41 - řešení

Řešení:

Žádné takové číslo neexistuje (!)

Polynom

$$n^2 - n + 41$$

totiž dává pro $n = 1, \ldots, 40$ následující seznam:

$$41, 43, 47, 53, 61, 71, 83, 97, 113, 131,$$
$$151, 173, 197, 223, 251, 281, 313, 347, 383, 421,$$
$$461, 503, 547, 593, 641, 691, 743, 797, 853, 911,$$
$$971, 1033, 1097, 1163, 1231, 1301, 1373, 1447, 1523, 1601.$$

Číslo 41 - řešení

Řešení:

Žádné takové číslo neexistuje (!)

Polynom

$$n^2 - n + 41$$

totiž dává pro $n = 1, \ldots, 40$ následující seznam:

$$41, 43, 47, 53, 61, 71, 83, 97, 113, 131,$$
$$151, 173, 197, 223, 251, 281, 313, 347, 383, 421,$$
$$461, 503, 547, 593, 641, 691, 743, 797, 853, 911,$$
$$971, 1033, 1097, 1163, 1231, 1301, 1373, 1447, 1523, 1601.$$

POZOROVÁNÍ: *Všechna tato čísla jsou prvočísla.*

Jak se na to dá přijít?

Jak se na to dá přijít?

Pokusíme se nyní vysvětlit, proč tomu tak je.

Jak se na to dá přijít?

Pokusíme se nyní vysvětlit, proč tomu tak je.

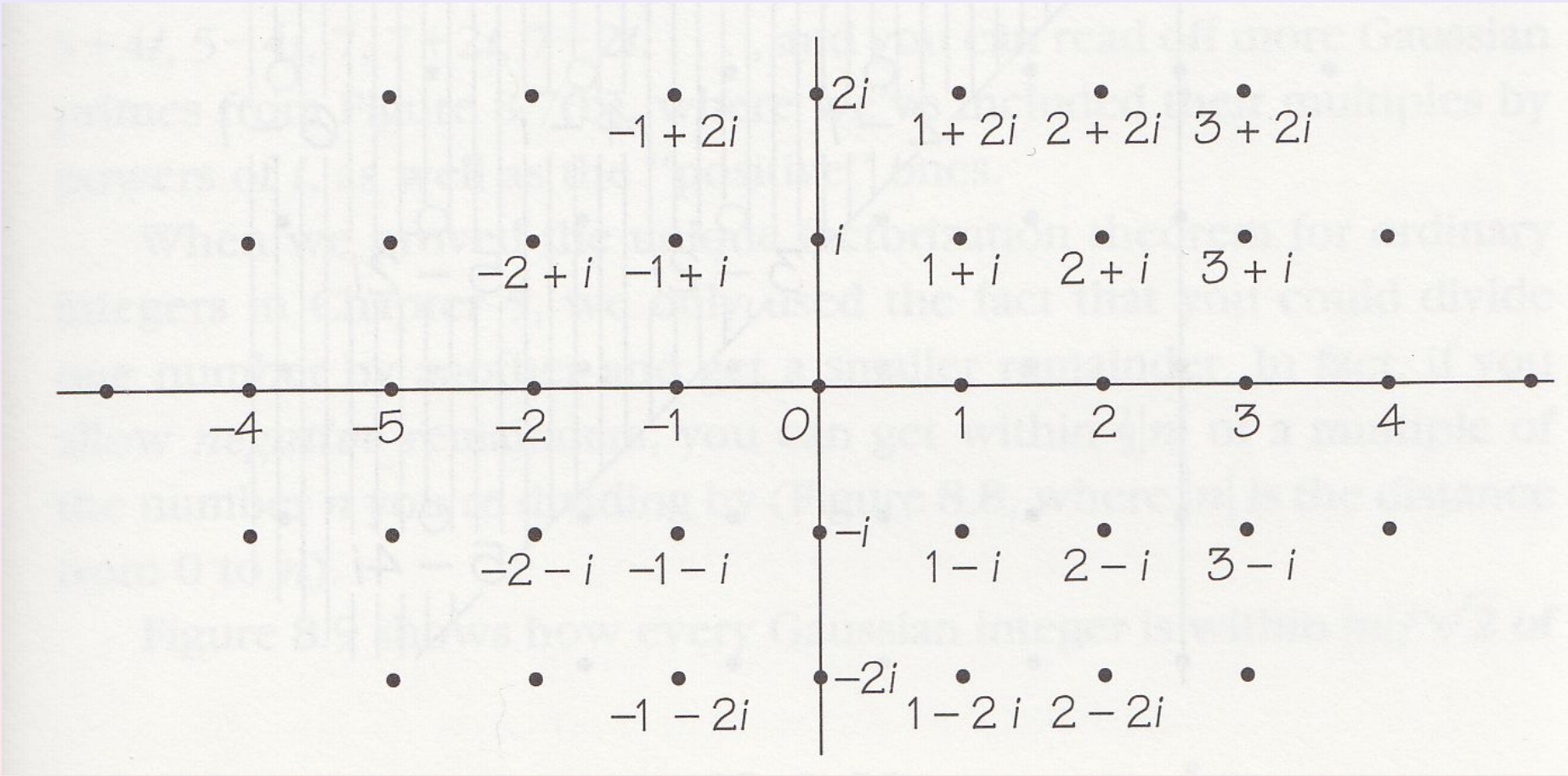
Začneme v komplexní rovině.

Jak se na to dá přijít?

Pokusíme se nyní vysvětlit, proč tomu tak je.

Začneme v komplexní rovině. Nejprve v ní najdeme Gaussova celá čísla.

Gaussova komplexní celá čísla



Gaussova věta

Gaussova věta

Známe: Každé kladné nebo záporné celé číslo lze jednoznačně zapsat ve tvaru součinu nějaké mocniny čísla (-1) a mocnin kladných prvočísel.

Gaussova věta

Známe: Každé kladné nebo záporné celé číslo lze jednoznačně zapsat ve tvaru součinu nějaké mocniny čísla (-1) a mocnin kladných prvočísel.

Gauss: Každé nenulové Gaussovo celé číslo lze jednoznačně zapsat ve tvaru součinu nějaké mocniny čísla i a mocnin *kladných* Gaussových prvočísel.

Gaussova věta

Známe: Každé kladné nebo záporné celé číslo lze jednoznačně zapsat ve tvaru součinu nějaké mocniny čísla (-1) a mocnin kladných prvočísel.

Gauss: Každé nenulové Gaussovo celé číslo lze jednoznačně zapsat ve tvaru součinu nějaké mocniny čísla i a mocnin *kladných* Gaussových prvočísel.

Co je to kladné Gaussovo prvočíslo?

Gaussova věta

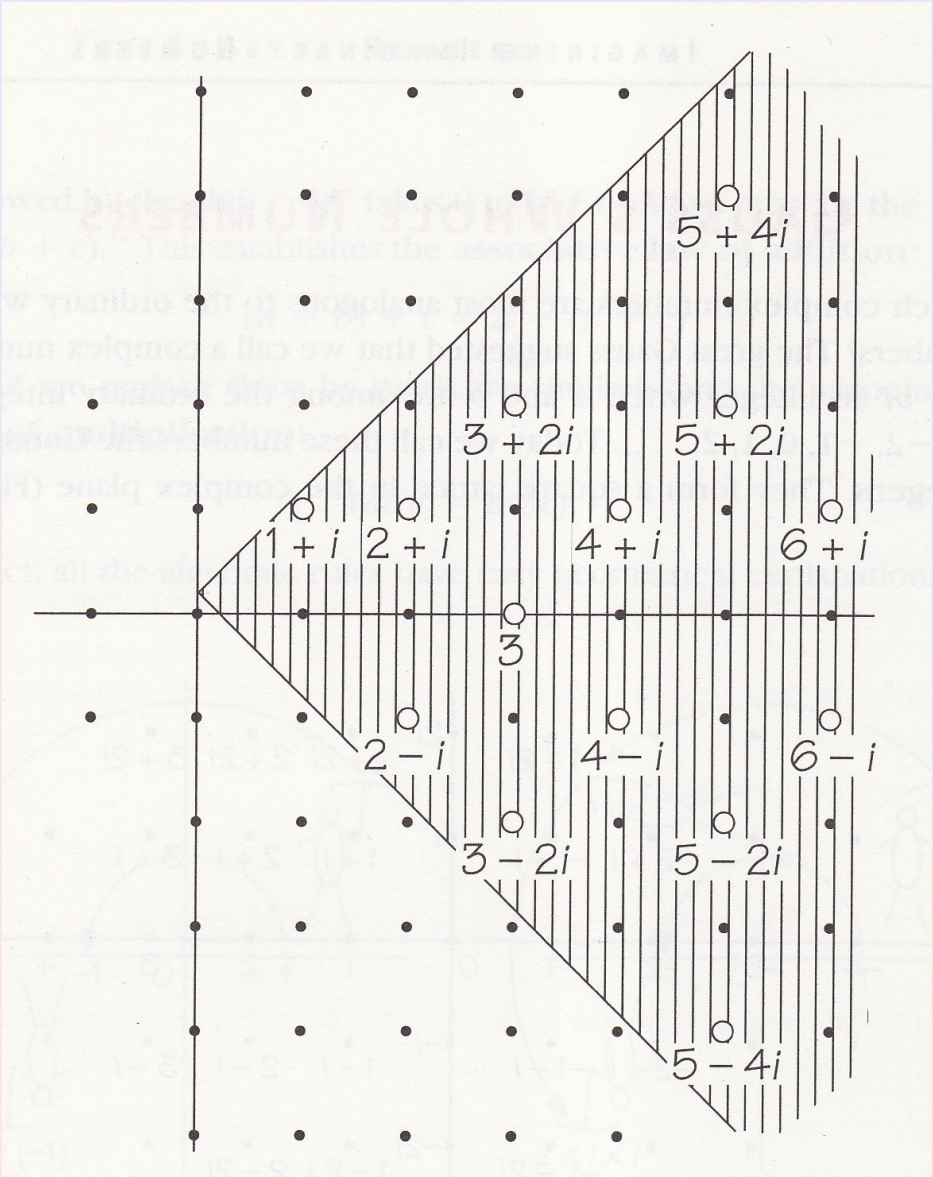
Známe: Každé kladné nebo záporné celé číslo lze jednoznačně zapsat ve tvaru součinu nějaké mocniny čísla (-1) a mocnin kladných prvočísel.

Gauss: Každé nenulové Gaussovo celé číslo lze jednoznačně zapsat ve tvaru součinu nějaké mocniny čísla i a mocnin *kladných* Gaussových prvočísel.

Co je to kladné Gaussovo prvočíslo? Odpovíme obrázkem.

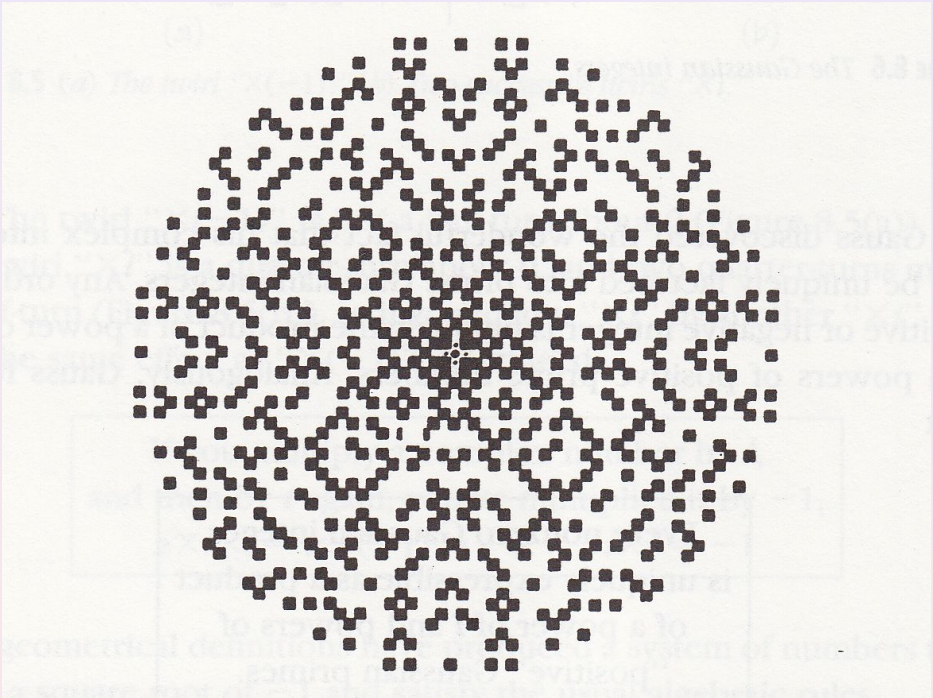
Gaussova kladná prvočísla

Gaussova kladná prvočísla



Gaussova prvočísla, násobená mocninami čísla i

Gaussova prvočísla, násobená mocninami čísla i



Gaussova prvočísla

Gaussova prvočísla

OTÁZKA: Proč není číslo 2 Gaussovým prvočíslem?

Gaussova prvočísla

OTÁZKA: Proč není číslo 2 Gaussovým prvočíslem?

ODPOVĚĎ:

Gaussova prvočísla

OTÁZKA: Proč není číslo 2 Gaussovým prvočíslem?

ODPOVĚĎ: Protože

$$2 = (1+i)(1-i) = 1 - i^2 = 1 + 1 = 2.$$

Modální aritmetika

Modální aritmetika

Číslo m je **kongruentní** číslu n modulo číslo p,

Modální aritmetika

Číslo m je **kongruentní** číslu n modulo číslo p, psáno

$$m \equiv n (\mathrm{mod}\, p),$$

Modální aritmetika

Číslo m je **kongruentní** číslu n modulo číslo p, psáno

$$m \equiv n (\mathrm{mod}\, p),$$

jestliže $m - n$ je dělitelné číslem p.

Modální aritmetika

Číslo m je **kongruentní** číslu n modulo číslo p, psáno

$$m \equiv n (\mathrm{mod}\, p),$$

jestliže $m - n$ je dělitelné číslem p.

POZOROVÁNÍ: V modulárlní aritmetice můžeme sčítat a násobit.

Modální aritmetika

Číslo m je **kongruentní** číslu n modulo číslo p, psáno

$$m \equiv n (\mathrm{mod}\, p),$$

jestliže $m - n$ je dělitelné číslem p.

POZOROVÁNÍ: V modulárlní aritmetice můžeme sčítat a násobit.
Příklady:

Modální aritmetika

Číslo m je **kongruentní** číslu n modulo číslo p, psáno

$$m \equiv n (\mathrm{mod}\, p),$$

jestliže $m - n$ je dělitelné číslem p.

POZOROVÁNÍ: V modulárlní aritmetice můžeme sčítat a násobit.
Příklady: $5 + 3 = 1 (\mathrm{mod}\, 7)$,

Modální aritmetika

Číslo m je **kongruentní** číslu n modulo číslo p, psáno

$$m \equiv n (\mathrm{mod}\, p),$$

jestliže $m - n$ je dělitelné číslem p.

POZOROVÁNÍ: V modulárlní aritmetice můžeme sčítat a násobit.
Příklady: $5 + 3 = 1 (\mathrm{mod}\, 7)$, $2 \cdot 7 = 2 (\mathrm{mod}\, 12)$.

Modální aritmetika

Číslo m je **kongruentní** číslu n modulo číslo p, psáno

$$m \equiv n (\mathrm{mod}\, p),$$

jestliže $m - n$ je dělitelné číslem p.

POZOROVÁNÍ: V modulárlní aritmetice můžeme sčítat a násobit. Příklady: $5 + 3 = 1 (\mathrm{mod}\, 7)$, $2 \cdot 7 = 2 (\mathrm{mod}\, 12)$.

POZOROVÁNÍ: Je-li p prvočíslo, můžeme i dělit a hovořit o zlomcích.

Modální aritmetika

Číslo m je **kongruentní** číslu n modulo číslo p, psáno

$$m \equiv n (\mathrm{mod}\, p),$$

jestliže $m - n$ je dělitelné číslem p.

POZOROVÁNÍ: V modulárlní aritmetice můžeme sčítat a násobit. Příklady: $5 + 3 = 1 (\mathrm{mod}\, 7)$, $2 \cdot 7 = 2 (\mathrm{mod}\, 12)$.

POZOROVÁNÍ: Je-li p prvočíslo, můžeme i dělit a hovořit o zlomcích.

$$\frac{2}{3} = 3,\ \frac{3}{4} = 6,\ \frac{2}{5} = 6,\ \frac{3}{5} = 2,\ \frac{4}{5} = 5,\ \frac{5}{6} = 2\ (\mathrm{mod}\, 7).$$

Modální aritmetika

Číslo m je **kongruentní** číslu n modulo číslo p, psáno

$$m \equiv n (\mathrm{mod}\, p),$$

jestliže $m - n$ je dělitelné číslem p.

POZOROVÁNÍ: V modulárlní aritmetice můžeme sčítat a násobit. Příklady: $5 + 3 = 1 (\mathrm{mod}\, 7)$, $2 \cdot 7 = 2 (\mathrm{mod}\, 12)$.

POZOROVÁNÍ: Je-li p prvočíslo, můžeme i dělit a hovořit o zlomcích.

$$\frac{2}{3} = 3,\ \frac{3}{4} = 6,\ \frac{2}{5} = 6,\ \frac{3}{5} = 2,\ \frac{4}{5} = 5,\ \frac{5}{6} = 2\ (\mathrm{mod}\, 7).$$

Další rozcvička: Co je $\frac{1}{7}\ (\mathrm{mod}\, 7)$?

Modulární dělení

Modulární dělení

Kolik je $\frac{1}{8}$ mod 101?

Modulární dělení

Kolik je $\frac{1}{8}$ mod 101?

Najdeme nejmenší násobek 8, který překročí 101:

Modulární dělení

Kolik je $\frac{1}{8}$ mod 101?

Najdeme nejmenší násobek 8, který překročí 101:

$$8 \times 13 = 104 \equiv 3 (\mathrm{mod} 101).$$

Modulární dělení

Kolik je $\frac{1}{8}$ mod 101?

Najdeme nejmenší násobek 8, který překročí 101:

$$8 \times 13 = 104 \equiv 3 (\mathrm{mod} 101).$$

Najdeme nejmenší násobek 3, který překročí 101:

Modulární dělení

Kolik je $\frac{1}{8}$ mod 101?

Najdeme nejmenší násobek 8, který překročí 101:

$$8 \times 13 = 104 \equiv 3 (\mathrm{mod} 101).$$

Najdeme nejmenší násobek 3, který překročí 101:

$$3 \times 34 = 102 \equiv 1 (\mathrm{mod} 101).$$

Modulární dělení

Kolik je $\frac{1}{8}$ mod 101?

Najdeme nejmenší násobek 8, který překročí 101:

$$8 \times 13 = 104 \equiv 3 (\mathrm{mod} 101).$$

Najdeme nejmenší násobek 3, který překročí 101:

$$3 \times 34 = 102 \equiv 1 (\mathrm{mod} 101).$$

Tedy

$$\frac{1}{8} \equiv 13 \times 34 (\mathrm{mod} 101).$$

Modulární dělění - dokončení výpočtu

Modulární dělění - dokončení výpočtu

To už snadno spočítáme.

Modulární dělění - dokončení výpočtu

To už snadno spočítáme.

Víme: $3 \times 34 \equiv 1$.

Modulární dělění - dokončení výpočtu

To už snadno spočítáme.

Víme: $3 \times 34 \equiv 1$.

Tedy $12 \times 34 \equiv 4$.

Modulární dělění - dokončení výpočtu

To už snadno spočítáme.

Víme: $3 \times 34 \equiv 1$.

Tedy $12 \times 34 \equiv 4$.

Tedy $13 \times 34 \equiv 38$.

Modulární dělění - dokončení výpočtu

To už snadno spočítáme.

Víme: $3 \times 34 \equiv 1$.

Tedy $12 \times 34 \equiv 4$.

Tedy $13 \times 34 \equiv 38$.

Odpověď: $\frac{1}{8} \equiv 38 (\mathrm{mod} 101)$.

Modulární dělění pro neprvočíselné moduly

Modulární dělění pro neprvočíselné moduly

Dělení modulo **neprvočíslo** se může, ale nemusí podařit.

Modulární dělění pro neprvočíselné moduly

Dělení modulo **neprvočíslo** se může, ale nemusí podařit.

Příklad: modulo 15 nelze dělit číslem 3, ačkoli $3 \not\equiv 0 (\mathrm{mod} 15)$.

Modulární dělění pro neprvočíselné moduly

Dělení modulo **neprvočíslo** se může, ale nemusí podařit.

Příklad: modulo 15 nelze dělit číslem 3, ačkoli $3 \not\equiv 0 (\mathrm{mod} 15)$.

Příklad: naším algoritmem postupně vyjde

Modulární dělění pro neprvočíselné moduly

Dělení modulo **neprvočíslo** se může, ale nemusí podařit.

Příklad: modulo 15 nelze dělit číslem 3, ačkoli $3 \not\equiv 0 (\mathrm{mod} 15)$.

Příklad: naším algoritmem postupně vyjde

$$68 \equiv 0 (\mathrm{mod} 102), \quad 5 \equiv 0 (\mathrm{mod} 102).$$

Modulární dělění pro neprvočíselné moduly

Dělení modulo **neprvočíslo** se může, ale nemusí podařit.

Příklad: modulo 15 nelze dělit číslem 3, ačkoli $3 \not\equiv 0 (\mathrm{mod} 15)$.

Příklad: naším algoritmem postupně vyjde

$$68 \equiv 0 (\mathrm{mod} 102), \quad 5 \equiv 0 (\mathrm{mod} 102).$$

Přitom ale:

Modulární dělění pro neprvočíselné moduly

Dělení modulo **neprvočíslo** se může, ale nemusí podařit.

Příklad: modulo 15 nelze dělit číslem 3, ačkoli $3 \not\equiv 0 (\mathrm{mod} 15)$.

Příklad: naším algoritmem postupně vyjde

$$68 \equiv 0 (\mathrm{mod} 102), \quad 5 \equiv 0 (\mathrm{mod} 102).$$

Přitom ale:

zlomek $\frac{1}{68}$ modulo 102 **neexistuje**,

Modulární dělění pro neprvočíselné moduly

Dělení modulo **neprvočíslo** se může, ale nemusí podařit.

Příklad: modulo 15 nelze dělit číslem 3, ačkoli $3 \not\equiv 0 (\mathrm{mod} 15)$.

Příklad: naším algoritmem postupně vyjde

$$68 \equiv 0 (\mathrm{mod} 102), \quad 5 \equiv 0 (\mathrm{mod} 102).$$

Přitom ale:

zlomek $\frac{1}{68}$ modulo 102 **neexistuje**,

zlonmek $\frac{1}{5}$ modulo 102 **existuje** a je roven

Modulární dělění pro neprvočíselné moduly

Dělení modulo **neprvočíslo** se může, ale nemusí podařit.

Příklad: modulo 15 nelze dělit číslem 3, ačkoli $3 \not\equiv 0 (\mathrm{mod} 15)$.

Příklad: naším algoritmem postupně vyjde

$$68 \equiv 0 (\mathrm{mod} 102), \quad 5 \equiv 0 (\mathrm{mod} 102).$$

Přitom ale:

zlomek $\frac{1}{68}$ modulo 102 **neexistuje**,

zlonmek $\frac{1}{5}$ modulo 102 **existuje** a je roven 41 (!).

Příklad

Příklad

OTÁZKA: Proč není číslo 13 Gaussovým prvočíslem?

Příklad

OTÁZKA: Proč není číslo 13 Gaussovým prvočíslem?

Wilsonův test prvočíselnosti:

Příklad

OTÁZKA: Proč není číslo 13 Gaussovým prvočíslem?

Wilsonův test prvočíselnosti:

Číslo p je prvočíslem právě tehdy, když je

$$(p-1)! \equiv -1 \pmod{p}.$$

Odtud plyne, že 13 dělí číslo $12! + 1$.

Odtud plyne, že 13 dělí číslo $12! + 1$. Ale

$$\begin{aligned} 12! + 1 &= 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10 \cdot 11 \cdot 12 + 1 \\ &\equiv 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot (-6) \cdot (-5) \cdot (-4) \cdot (-3) \cdot (-2) \cdot (-1) + 1 \\ &= (6!)^2 + 1 = (6!)^2 - i^2 = (6! + i)(6! - i). \end{aligned}$$

Odtud plyne, že 13 dělí číslo $12! + 1$. Ale

$$\begin{aligned} 12! + 1 &= 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10 \cdot 11 \cdot 12 + 1 \\ &\equiv 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot (-6) \cdot (-5) \cdot (-4) \cdot (-3) \cdot (-2) \cdot (-1) + 1 \\ &= (6!)^2 + 1 = (6!)^2 - i^2 = (6! + i)(6! - i). \end{aligned}$$

Pokud by tedy 13 dělilo $12! + 1$, muselo by dělit i některé z čísel $6! + i$ nebo $6! - i$. Je však zřejmé, že veškeré násobky čísla 13 jsou tvaru $13a + 13bi$, kde $a, b \in \mathbb{Z}$.

Fermatova věta

POZNÁMKA: Zcela analogicky lze dokázat, že *obyčejné* prvočíslo p je možné Gaussovsky faktorizovat právě tehdy, když $p+1$ *není* násobkem čísla 4.

POZNÁMKA: Zcela analogicky lze dokázat, že *obyčejné* prvočíslo p je možné Gaussovsky faktorizovat právě tehdy, když $p+1$ *není* násobkem čísla 4.

FERMATOVA VĚTA O DVOU ČTVERCÍCH:

POZNÁMKA: Zcela analogicky lze dokázat, že *obyčejné* prvočíslo p je možné Gaussovsky faktorizovat právě tehdy, když $p+1$ *není* násobkem čísla 4.

FERMATOVA VĚTA O DVOU ČTVERCÍCH:

Každé prvočíslo p je možné zapsat ve tvaru součtu dvou druhých mocnin právě tehdy, když $p+1$ *není* násobkem čísla 4.

POZNÁMKA: Zcela analogicky lze dokázat, že *obyčejné* prvočíslo p je možné Gaussovsky faktorizovat právě tehdy, když $p+1$ *není* násobkem čísla 4.

FERMATOVA VĚTA O DVOU ČTVERCÍCH:

Každé prvočíslo p je možné zapsat ve tvaru součtu dvou druhých mocnin právě tehdy, když $p+1$ *není* násobkem čísla 4. Tento zápis je jednoznačný.

Fermatova věta v Gaussově světě

Fermatova věta v Gaussově světě

V Gaussově světě vypadá Fermatova věta takto:

Fermatova věta v Gaussově světě

V Gaussově světě vypadá Fermatova věta takto:

$$2 = (1+i)(1-i) = 1^2 + 1^2$$

3 zůstává prvočíslem

$$5 = (2+i)(2-i) = 2^2 + 1^2$$

7 zůstává prvočíslem

11 zůstává prvočíslem

$$13 = (6+i)(6-i) = 3^2 + 2^2$$

Eisensteinovo zobecnění

Eisensteinova celá čísla

Eisensteinovo zobecnění

Eisensteinova celá čísla jsou čísla tvaru $a + b\omega$, kde $\omega = (-1 + i\sqrt{3})/2$.

Eisensteinovo zobecnění

Eisensteinova celá čísla jsou čísla tvaru $a + b\omega$, kde $\omega = (-1 + i\sqrt{3})/2$.

POZNÁMKA: ω je jedním ze tří kořenů rovnice $x^3 = 1$, zbylé dva kořeny jsou 1 a $\omega^2 = (-1 - i\sqrt{3})/2$.

Eisensteinovo zobecnění

Eisensteinova celá čísla jsou čísla tvaru $a + b\omega$, kde $\omega = (-1 + i\sqrt{3})/2$.

POZNÁMKA: ω je jedním ze tří kořenů rovnice $x^3 = 1$, zbylé dva kořeny jsou 1 a $\omega^2 = (-1 - i\sqrt{3})/2$.

POZNÁMKA:

Eisensteinovo zobecnění

Eisensteinova celá čísla jsou čísla tvaru $a + b\omega$, kde $\omega = (-1 + i\sqrt{3})/2$.

POZNÁMKA: ω je jedním ze tří kořenů rovnice $x^3 = 1$, zbylé dva kořeny jsou 1 a $\omega^2 = (-1 - i\sqrt{3})/2$.

POZNÁMKA:
Eisensteinova čísla také mají jednoznačnou prvočíselnou faktorizaci.

Eisensteinovo zobecnění

Eisensteinova celá čísla jsou čísla tvaru $a + b\omega$, kde $\omega = (-1 + i\sqrt{3})/2$.

POZNÁMKA: ω je jedním ze tří kořenů rovnice $x^3 = 1$, zbylé dva kořeny jsou 1 a $\omega^2 = (-1 - i\sqrt{3})/2$.

POZNÁMKA:
Eisensteinova čísla také mají jednoznačnou prvočíselnou faktorizaci. Tentokrát ovšem máme *šest jednotek*: ± 1, $\pm\omega$, $\pm\omega^2$.

Eisensteinovo zobecnění

Eisensteinova celá čísla jsou čísla tvaru $a + b\omega$, kde $\omega = (-1 + i\sqrt{3})/2$.

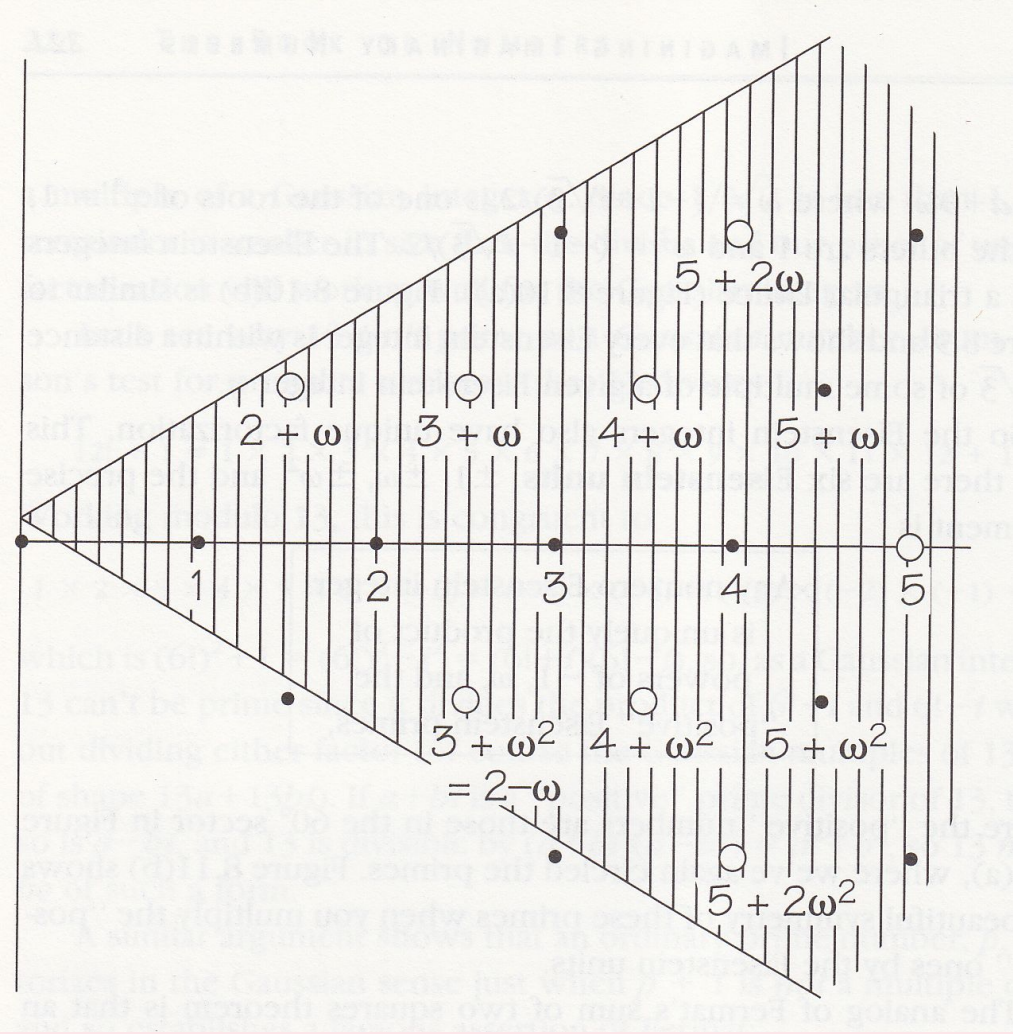
POZNÁMKA: ω je jedním ze tří kořenů rovnice $x^3 = 1$, zbylé dva kořeny jsou 1 a $\omega^2 = (-1 - i\sqrt{3})/2$.

POZNÁMKA:
Eisensteinova čísla také mají jednoznačnou prvočíselnou faktorizaci. Tentokrát ovšem máme *šest jednotek*: ± 1, $\pm\omega$, $\pm\omega^2$.

VĚTA. Každé nenulové Eisensteinovo celé číslo lze jednoznačně zapsat ve tvaru součinu mocnin čísel $-1, \omega$ a mocnin *kladných* Eisensteinových prvočísel.

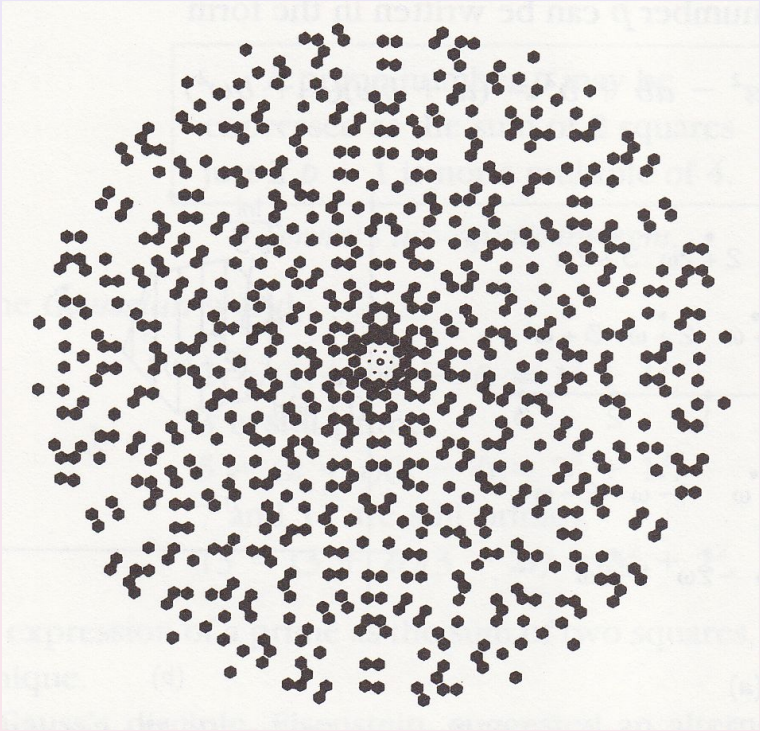
Eisensteinova kladná prvočísla

Eisensteinova kladná prvočísla



Eisensteinova prvočísla, násobená mocninami -1 a ω

Eisensteinova prvočísla, násobená mocninami -1 a ω



Obdoba Fermatovy věty v Eisensteinově systému

Obdoba Fermatovy věty v Eisensteinově systému

VĚTA : Každé prvočíslo p je možné zapsat ve tvaru $a^2 - ab + b^2 = (a + b\omega)(a + b\omega^2)$ právě tehdy, když $p + 1$ *není* násobkem čísla 3.

Obdoba Fermatovy věty v Eisensteinově systému

VĚTA : Každé prvočíslo p je možné zapsat ve tvaru $a^2 - ab + b^2 = (a + b\omega)(a + b\omega^2)$ právě tehdy, když $p + 1$ *není* násobkem čísla 3. Tento zápis je jednoznačný.

Fermatova věta v Eisensteinově světě

Fermatova věta v Eisensteinově světě

V Eisensteinově světě vypadá analogie Fermatovy věty takto:

Fermatova věta v Eisensteinově světě

V Eisensteinově světě vypadá analogie Fermatovy věty takto:

$$
\begin{aligned}
&2 \text{ zůstává prvočíslem} \\
3 &= (2+\omega)(2+\omega^2) = -\omega(2+\omega)^2 \\
&5 \text{ zůstává prvočíslem} \\
7 &= (3+\omega)(2+\omega^2) \\
13 &= (4+\omega)(4+\omega^2) \\
19 &= (5+\omega)(5+\omega^2) \\
31 &= (6+\omega)(6+\omega^2)
\end{aligned}
$$

atd.

Fermatova věta v Eisensteinově světě

V Eisensteinově světě vypadá analogie Fermatovy věty takto:

$$
\begin{aligned}
&2 \text{ zůstává prvočíslem} \\
3 &= (2+\omega)(2+\omega^2) = -\omega(2+\omega)^2 \\
&5 \text{ zůstává prvočíslem} \\
7 &= (3+\omega)(2+\omega^2) \\
13 &= (4+\omega)(4+\omega^2) \\
19 &= (5+\omega)(5+\omega^2) \\
31 &= (6+\omega)(6+\omega^2)
\end{aligned}
$$

atd.

Jsou to právě ta prvočísla, která lze vyjádřit ve tvaru

$$3m^2 + n^2.$$

Jsou další zobecňování možná?

Jsou další zobecňování možná?

POZNÁMKY:

Jsou další zobecňování možná?

POZNÁMKY:

Důkaz jednoznačnosti prvočíselného rozkladu pro *obyčejné* celé číslo není triviální.

Jsou další zobecňování možná?

POZNÁMKY:

Důkaz jednoznačnosti prvočíselného rozkladu pro *obyčejné* celé číslo není triviální.

Důkaz jednoznačnosti prvočíselného rozkladu pro *Gaussova* a *Eisensteinova* čísla (**která v sobě obsahují $\sqrt{-1}$ a $\sqrt{-3}$**) je ještě hlubší a opírá se o geometrické vlastnosti čtverců a rovnostranných trojúhelníků.

Jsou další zobecňování možná?

Jsou další zobecňování možná?

POZNÁMKY:

Jsou další zobecňování možná?

POZNÁMKY:

Pro čísla tvaru $a + b\sqrt{-5}$ věta o jednoznačném rozkladu dokonce **neplatí !!**

Jsou další zobecňování možná?

POZNÁMKY:

Pro čísla tvaru $a + b\sqrt{-5}$ věta o jednoznačném rozkladu dokonce **neplatí !!**

Příklad:

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}),$$

Jsou další zobecňování možná?

POZNÁMKY:

Pro čísla tvaru $a + b\sqrt{-5}$ věta o jednoznačném rozkladu dokonce **neplatí !!**

Příklad:

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}),$$

přičemž žádný ze čtyř faktorů 2, 3, $(1 + \sqrt{-5})$, $(1 - \sqrt{-5})$ nelze dále rozkládat.

Proč to někdy platí a někdy ne?

Proč to někdy platí a někdy ne?

POKUS O VYSVĚTLENÍ:

Proč to někdy platí a někdy ne?

POKUS O VYSVĚTLENÍ:

Při **dělení** v tomto číselném systému ne vždy dostaneme **zbytek menší než dělitel**.

Proč to někdy platí a někdy ne?

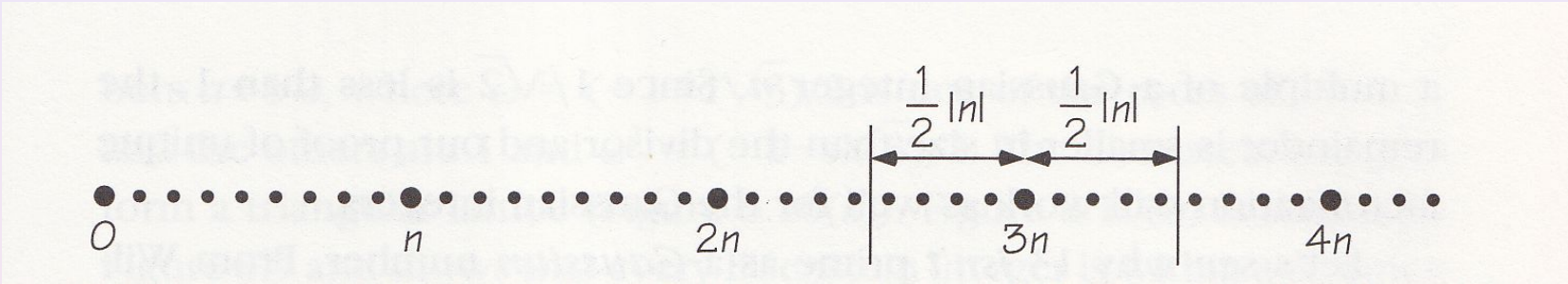
POKUS O VYSVĚTLENÍ:

Při **dělení** v tomto číselném systému ne vždy dostaneme **zbytek menší než dělitel**.

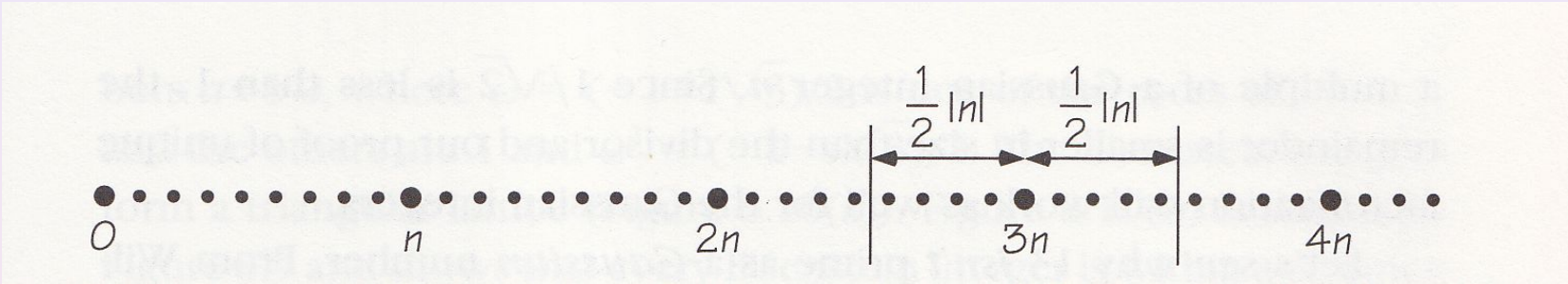
Pokusíme se ilustrovat na obrázcích.

Dělení v obyčejném číselném systému

Dělení v obyčejném číselném systému



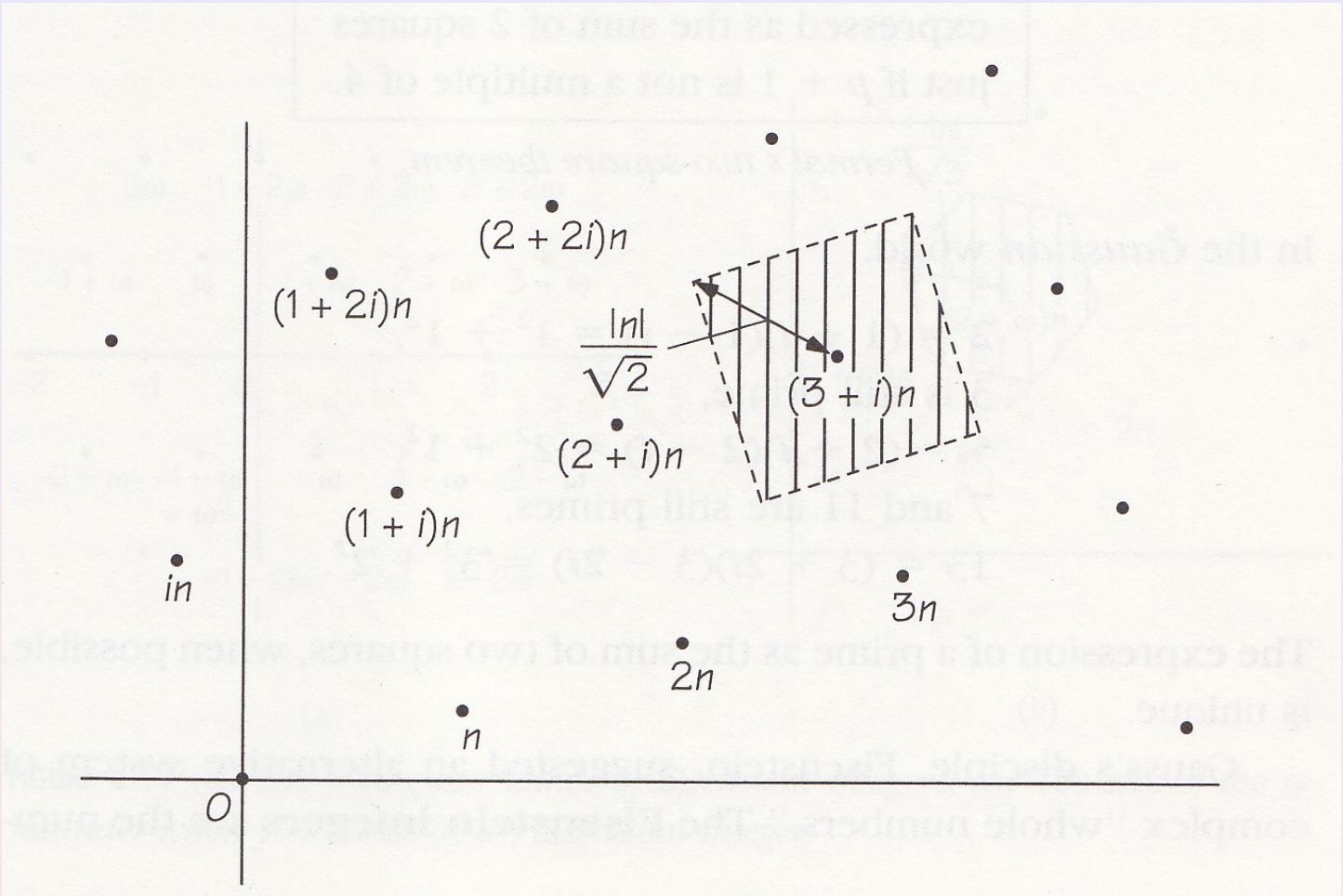
Dělení v obyčejném číselném systému



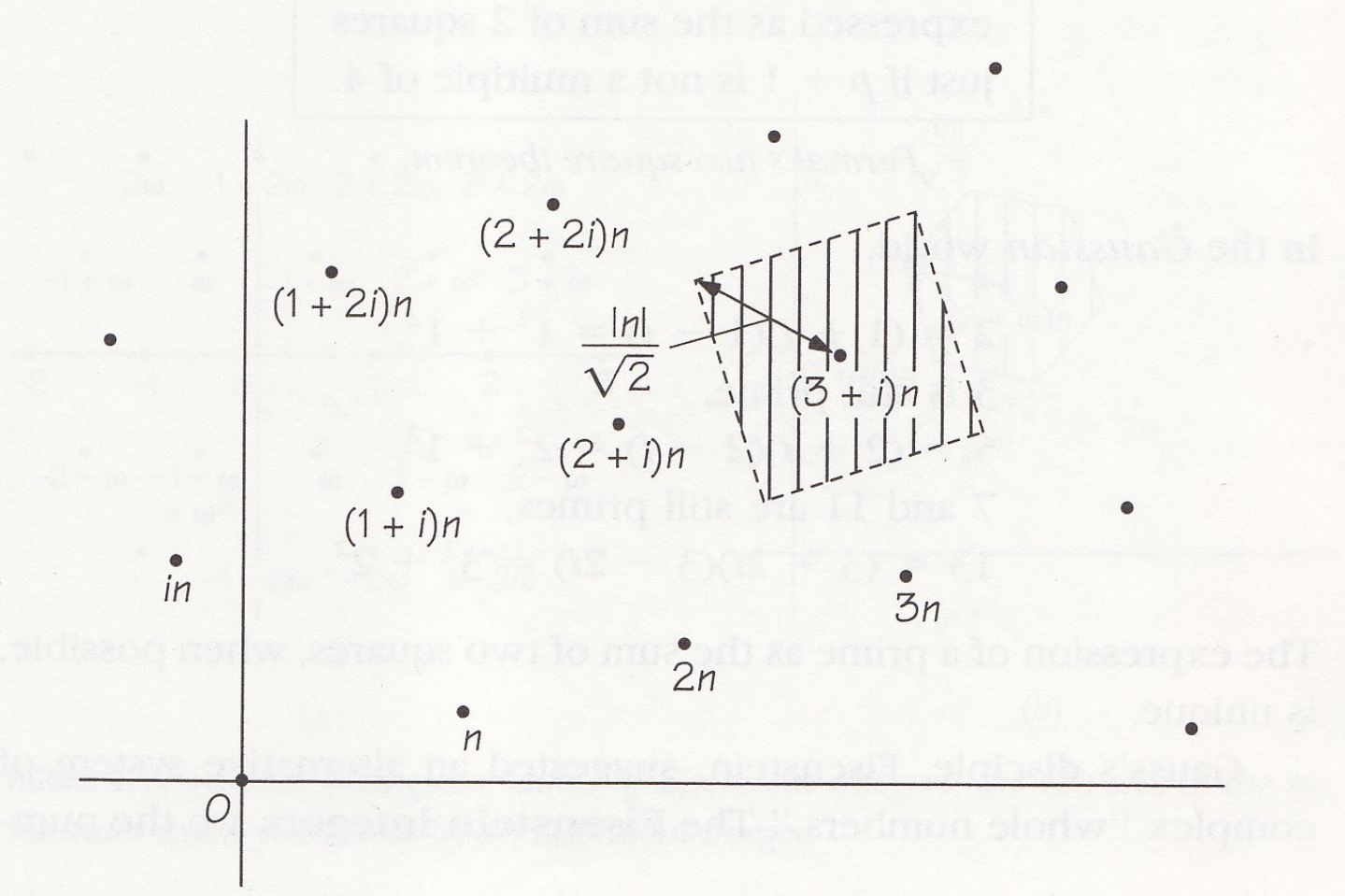
Při obyčejném dělení je zbytek vzdálen od nejbližšího násobku čísla n nejvýše o $\frac{n}{2}$ (pokud připustíme záporné zbytky).

Velikost zbytku při dělení Gaussovým číslem

Velikost zbytku při dělení Gaussovým číslem

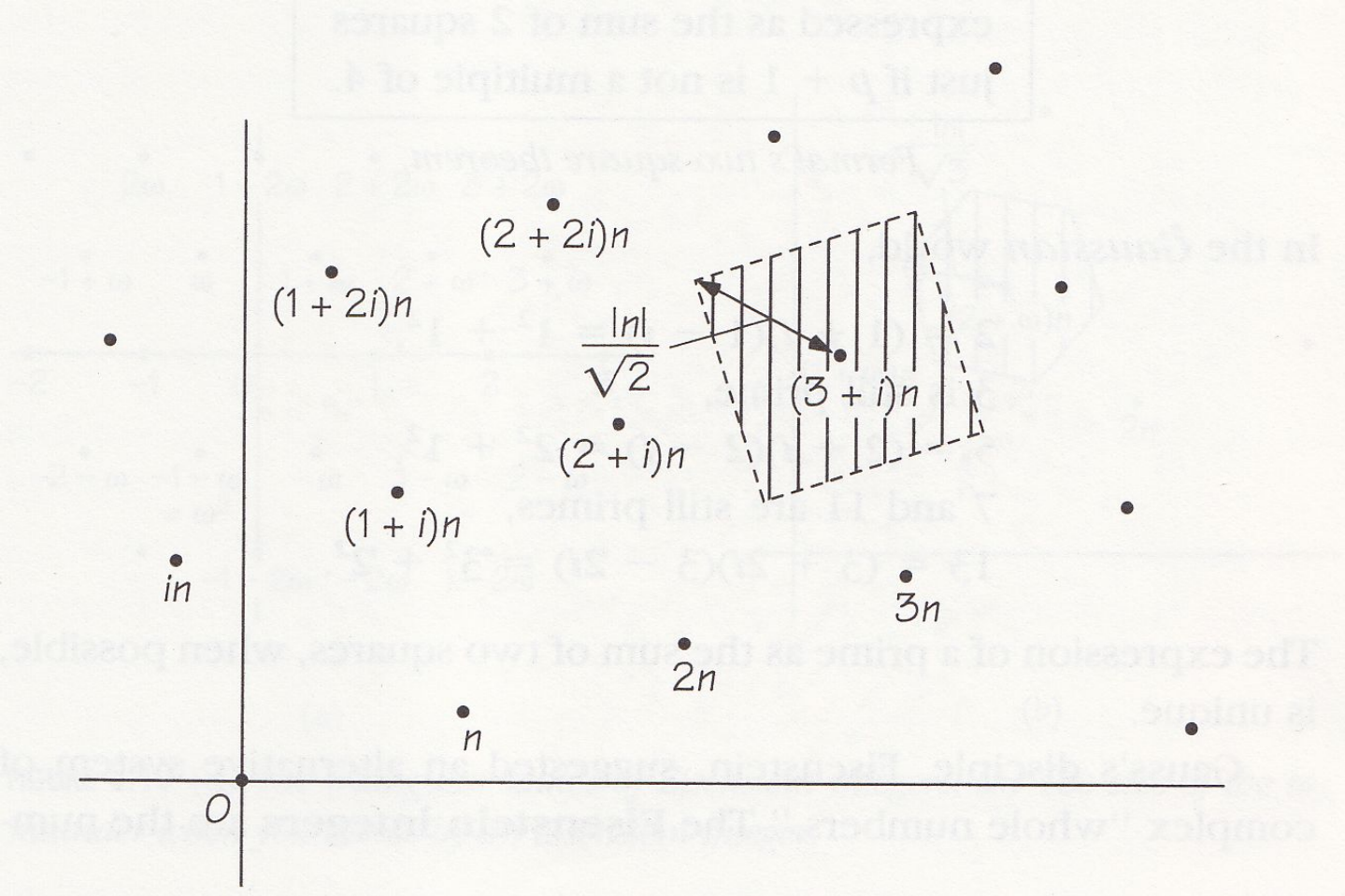


Velikost zbytku při dělení Gaussovým číslem



Při dělení Gaussovým celým číslem má zbytek velikost nejvýše $\frac{n}{\sqrt{2}}$.

Velikost zbytku při dělení Gaussovým číslem

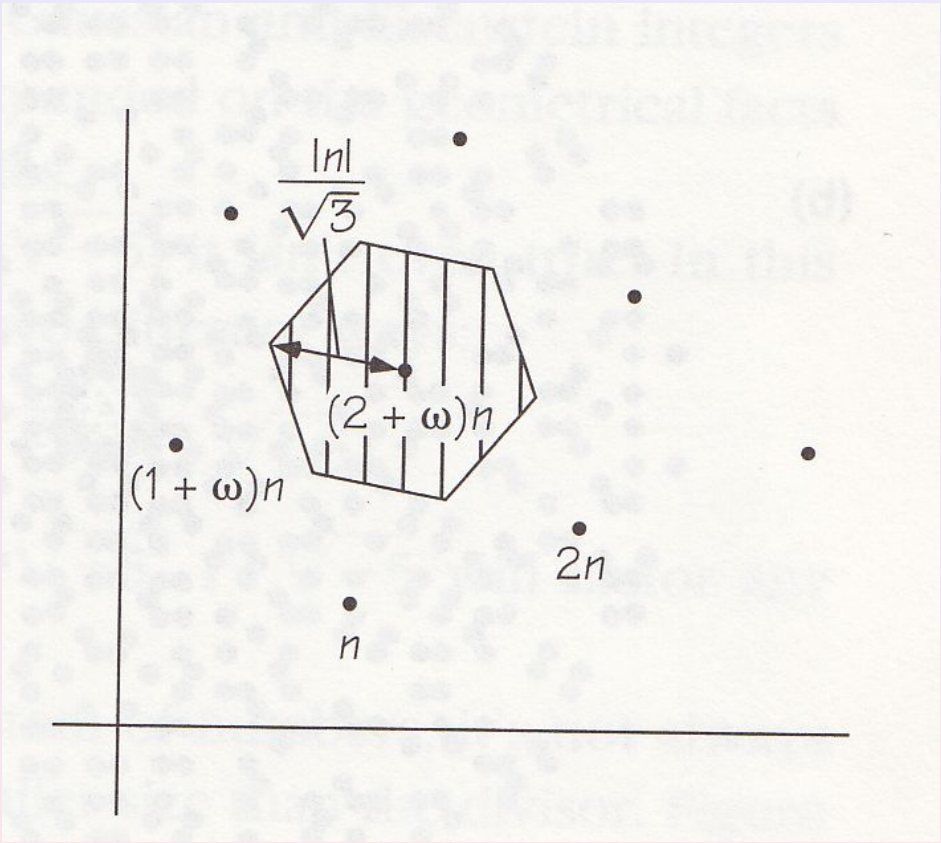


Při dělení Gaussovým celým číslem má zbytek velikost nejvýše $\frac{n}{\sqrt{2}}$.

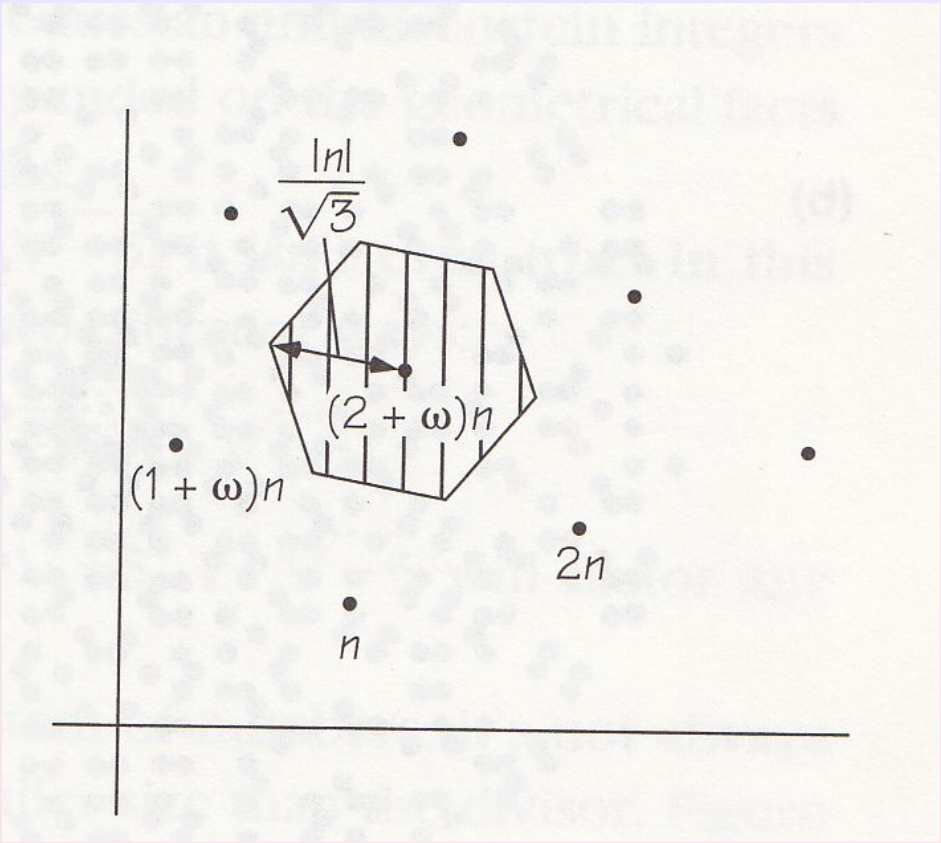
Jednoznačnost rozkladu plyne z toho že $\frac{1}{\sqrt{2}} < 1$.

Velikost zbytku při dělení Eisensteinovým číslem

Velikost zbytku při dělení Eisensteinovým číslem

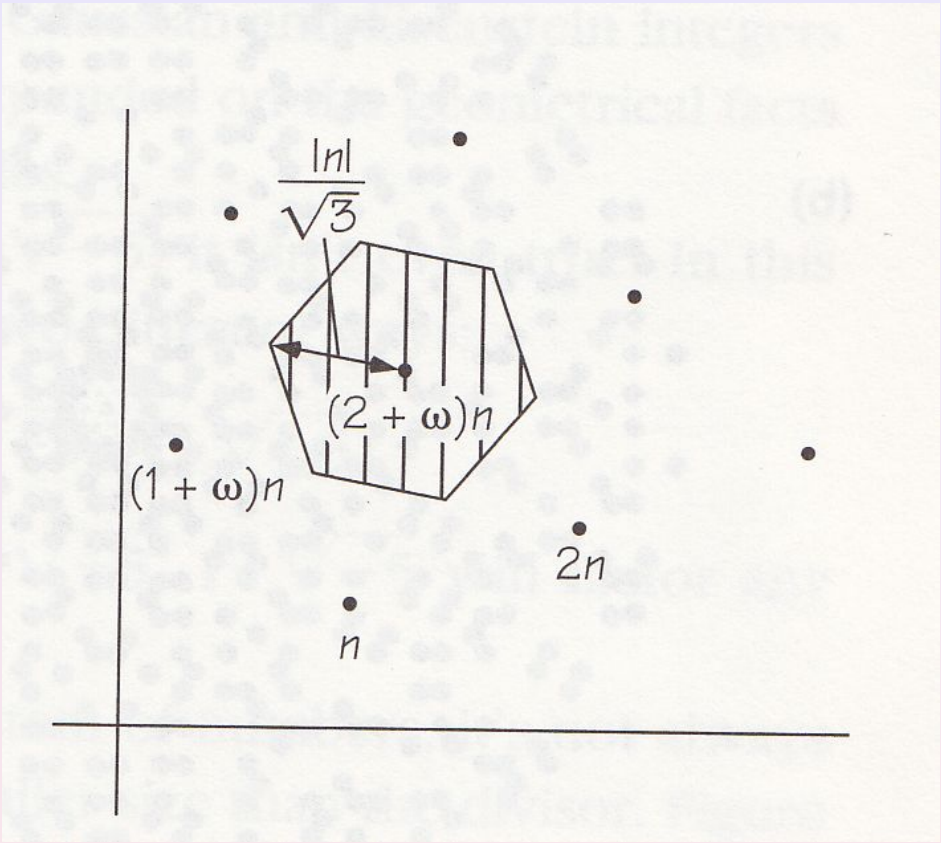


Velikost zbytku při dělení Eisensteinovým číslem



Při dělení Eisensteinovým celým číslem má zbytek velikost nejvýše $\frac{n}{\sqrt{3}}$.

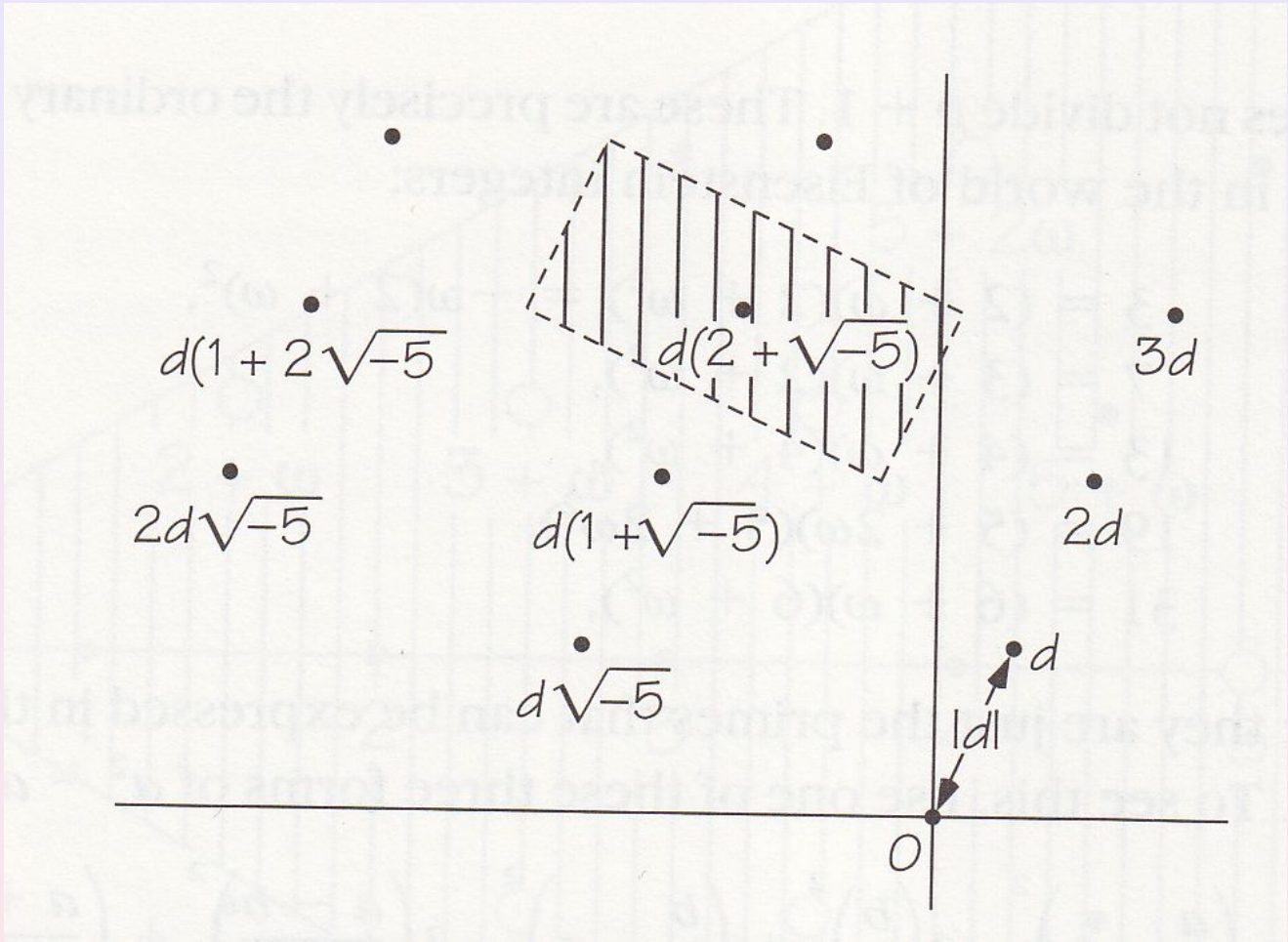
Velikost zbytku při dělení Eisensteinovým číslem



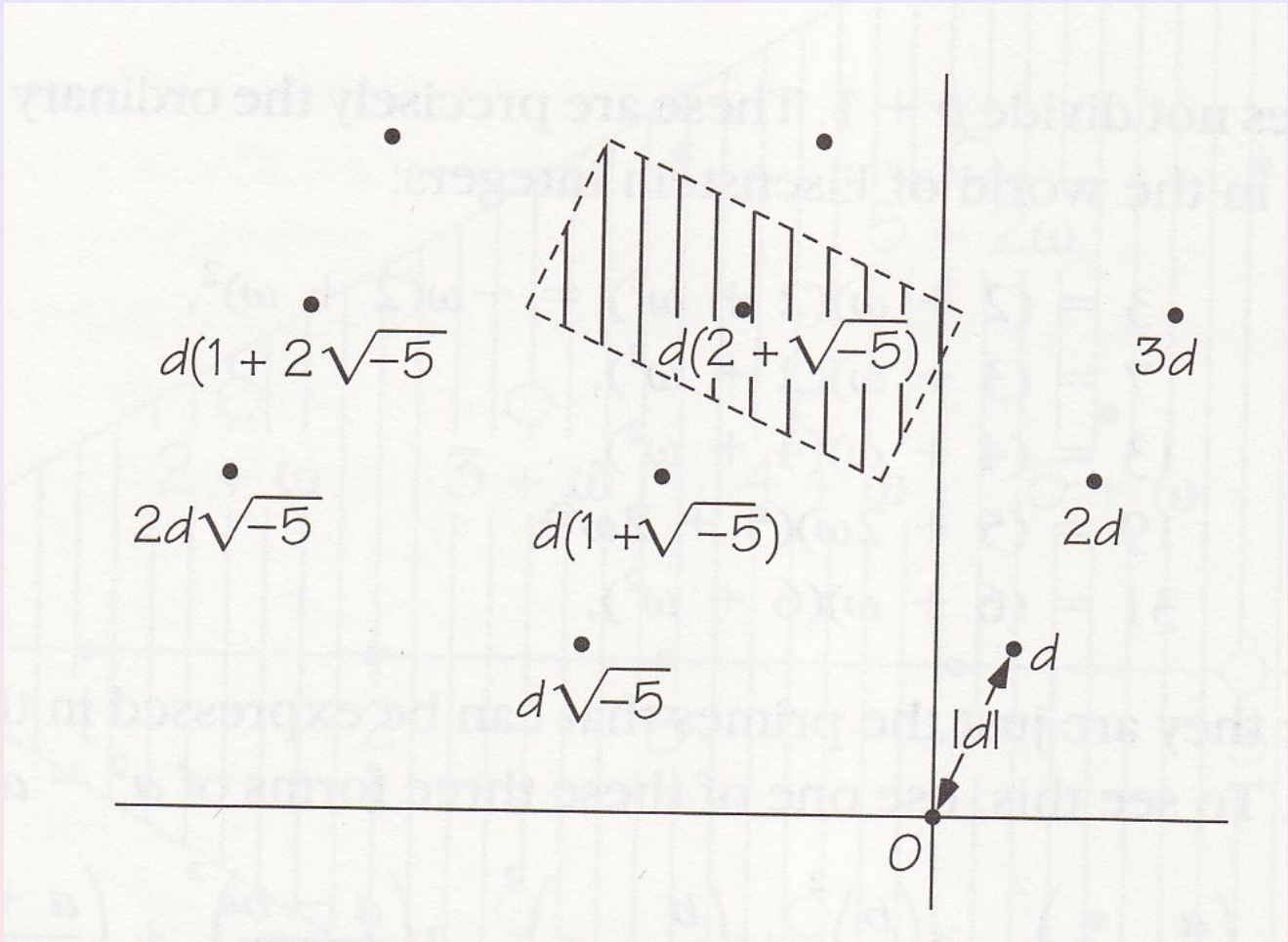
Při dělení Eisensteinovým celým číslem má zbytek velikost nejvýše $\frac{n}{\sqrt{3}}$. Jednoznačnost rozkladu plyne z toho že $\frac{1}{\sqrt{3}} < 1$.

Celočíselné násobky čísla d v číselném systému s $\sqrt{-5}$

Celočíselné násobky čísla d v číselném systému s $\sqrt{-5}$

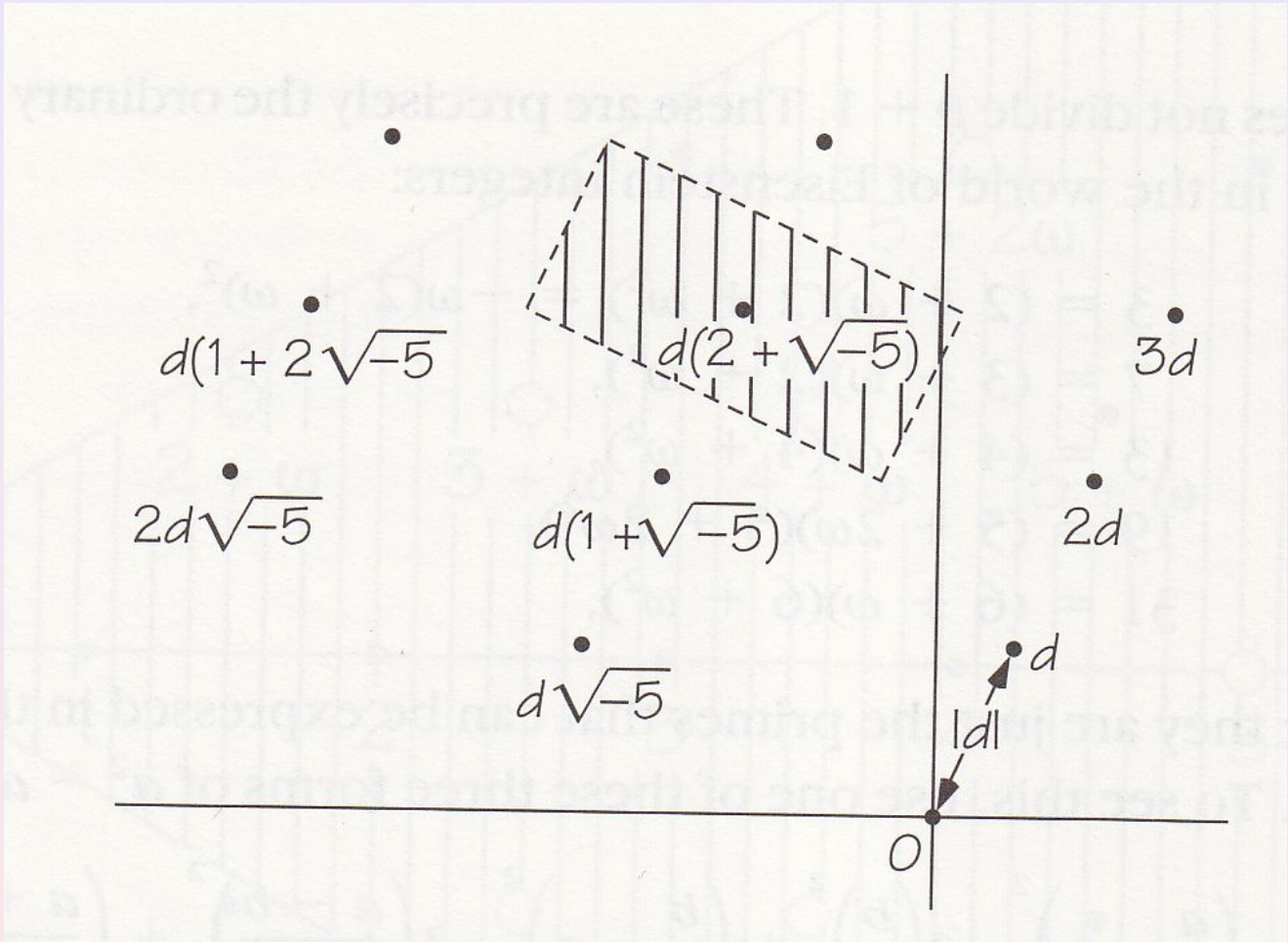


Celočíselné násobky čísla d v číselném systému s $\sqrt{-5}$



Při dělení v tomto systému má ovšem zbytek velikost $d\sqrt{\frac{3}{2}} > d$.

Celočíselné násobky čísla d v číselném systému s $\sqrt{-5}$



Při dělení v tomto systému má ovšem zbytek velikost $d\sqrt{\frac{3}{2}} > d$.

Rozklad tedy nemusí být jednoznačný.

Devět magických diskriminantů

Devět magických diskriminantů

OTÁZKA:

Devět magických diskriminantů

OTÁZKA:

Pro která čísla $-d$ vede $\sqrt{-d}$ na systém s jednoznačnou prvočíselnou faktorizací?

Devět magických diskriminantů

OTÁZKA:

Pro která čísla $-d$ vede $\sqrt{-d}$ na systém s jednoznačnou prvočíselnou faktorizací?

ODPOVĚĎ je hluboce netriviální.

Devět magických diskriminantů

OTÁZKA:

Pro která čísla $-d$ vede $\sqrt{-d}$ na systém s jednoznačnou prvočíselnou faktorizací?

ODPOVĚĎ je hluboce netriviální.

Jsou to takzvaná **Heegnerova čísla**:

Devět magických diskriminantů

OTÁZKA:

Pro která čísla $-d$ vede $\sqrt{-d}$ na systém s jednoznačnou prvočíselnou faktorizací?

ODPOVĚĎ je hluboce netriviální.

Jsou to takzvaná **Heegnerova čísla**:

$$-1,\ -2,\ -3,\ -7,\ -11,\ -19,\ -43,\ -67,\ -163.$$

Trocha historie

Trocha historie

Dlouho nebylo známo, zda existují ještě jiná taková čísla.

Trocha historie

Dlouho nebylo známo, zda existují ještě jiná taková čísla.

Počátek 20. století: pokud existuje další, pak *jen jedno* (!)

Trocha historie

Dlouho nebylo známo, zda existují ještě jiná taková čísla.

Počátek 20. století: pokud existuje další, pak *jen jedno* (!)

Vznikl takzvaný *problém desátého diskriminantu*.

Trocha historie

Dlouho nebylo známo, zda existují ještě jiná taková čísla.

Počátek 20. století: pokud existuje další, pak *jen jedno* (!)

Vznikl takzvaný *problém desátého diskriminantu*.

1936: Heilbronn & Lightfoot: desátý diskriminant by musel být větší než 10^9.

Trocha historie

Dlouho nebylo známo, zda existují ještě jiná taková čísla.

Počátek 20. století: pokud existuje další, pak *jen jedno* (!)

Vznikl takzvaný *problém desátého diskriminantu*.

1936: Heilbronn & Lightfoot: desátý diskriminant by musel být větší než 10^9.

1952: Heegner: první důkaz neexistence desátého diskriminantu (odborníci však pochybují o jeho správnosti).

Trocha historie

Dlouho nebylo známo, zda existují ještě jiná taková čísla.

Počátek 20. století: pokud existuje další, pak *jen jedno* (!)

Vznikl takzvaný *problém desátého diskriminantu*.

1936: Heilbronn & Lightfoot: desátý diskriminant by musel být větší než 10^9.

1952: Heegner: první důkaz neexistence desátého diskriminantu (odborníci však pochybují o jeho správnosti).

1967: Baker & Stark: nový důkaz neexistence desátého diskriminantu a resuscitace Heegnerova důkazu.

A nyní zpět k našemu polynomu

A nyní zpět k našemu polynomu

OTÁZKA:

A nyní zpět k našemu polynomu

OTÁZKA:

Jak to bylo s polynomem $n^2 - n + 41$?

A nyní zpět k našemu polynomu

OTÁZKA:

Jak to bylo s polynomem $n^2 - n + 41$?

ODPOVĚĎ: Rovnice

$$x^2 - x + 41 = 0$$

A nyní zpět k našemu polynomu

OTÁZKA:

Jak to bylo s polynomem $n^2 - n + 41$?

ODPOVĚĎ: Rovnice

$$x^2 - x + 41 = 0$$

má kořeny $\frac{1}{2}(1 \pm \sqrt{-163})$.

A nyní zpět k našemu polynomu

OTÁZKA:

Jak to bylo s polynomem $n^2 - n + 41$?

ODPOVĚĎ: Rovnice

$$x^2 - x + 41 = 0$$

má kořeny $\frac{1}{2}(1 \pm \sqrt{-163})$.

POZOROVÁNÍ: Pro $k > 1$ dává polynom $n^2 - n + k$ prvočíselné hodnoty pro všechna $n = 1, 2, \ldots, k - 1$ právě tehdy, když $1 - 4k$ je Heegnerovo číslo.

A nyní zpět k našemu polynomu

OTÁZKA:

Jak to bylo s polynomem $n^2 - n + 41$?

ODPOVĚĎ: Rovnice

$$x^2 - x + 41 = 0$$

má kořeny $\frac{1}{2}(1 \pm \sqrt{-163})$.

POZOROVÁNÍ: Pro $k > 1$ dává polynom $n^2 - n + k$ prvočíselné hodnoty pro všechna $n = 1, 2, \ldots, k - 1$ právě tehdy, když $1 - 4k$ je Heegnerovo číslo.

DŮSLEDEK: To nastane jedině tehdy, když $k = 2, 3, 5, 11, 17$ nebo $k = 41$.

Hodnoty jednotlivých polynomů pro $n = 1, \ldots, k-1$

Hodnoty jednotlivých polynomů pro $n = 1, \ldots, k-1$

$n^2 - n + 2$: 2

$n^2 - n + 3$: 3 5

$n^2 - n + 5$: 5 7 11 17

$n^2 - n + 11$: 11 13 17 23 31 41 53 67 81 101

$n^2 - n + 17$: 17 19 23 29 37 47 59 73 89 107 127 149 173 199 227 257

Konec

A to je vše, nyní již máte volno!