Teorie čísel

Milan Radojčić

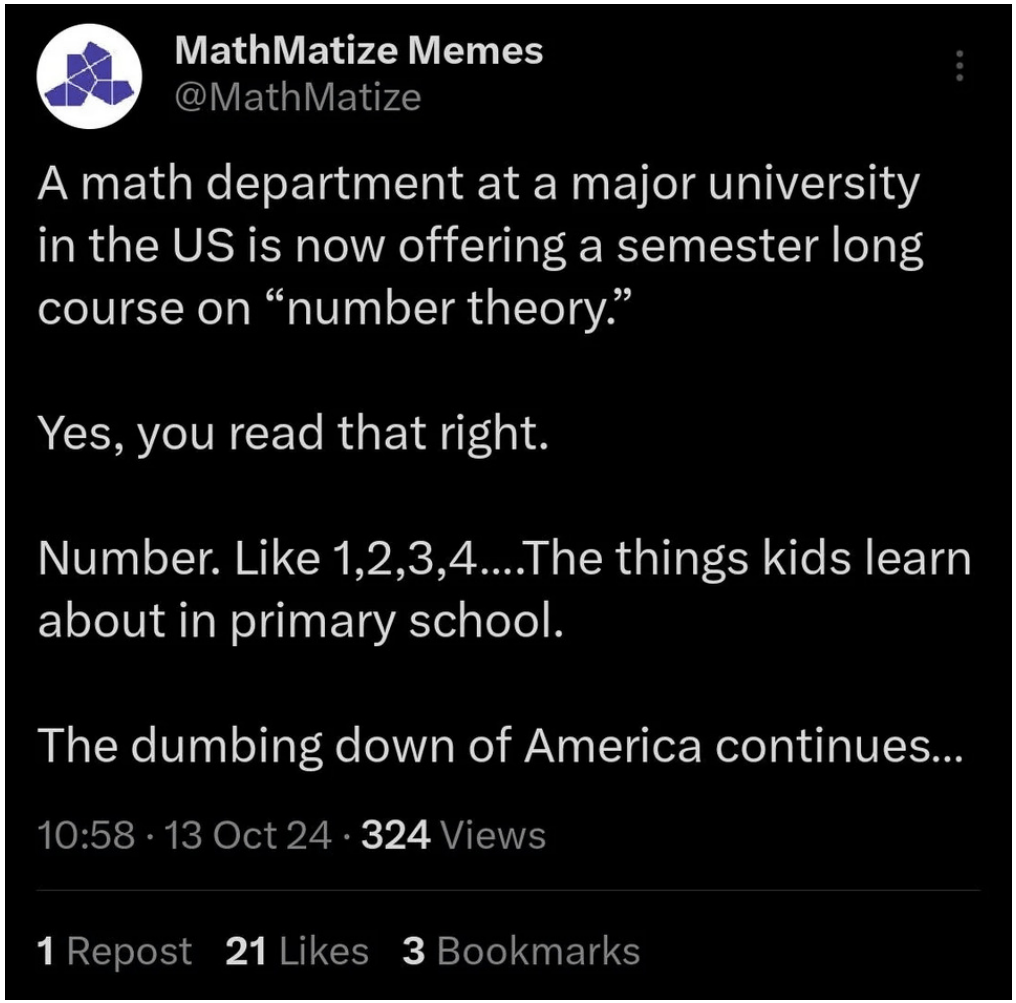
SSPŠaG

2024

Hlavní body

Hlavní body

Úvod


MathMatize Memes
@MathMatize
A math department at a major university in the US is now offering a semester long course on “number theory.”
Yes, you read that right.
Number. Like 1,2,3,4....The things kids learn about in primary school.
The dumbing down of America continues...
10:58 · 13 Oct 24 · 324 Views
1 Repost 21 Likes 3 Bookmarks

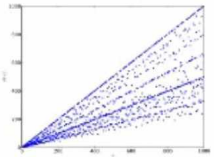
Úvod

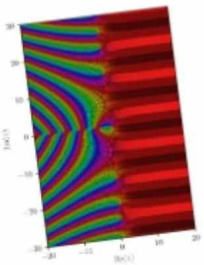
What I expected from Number Theory:

1 + 2 = 3

What I got:

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$





$$\sum_{n=0}^{\infty} p(n)x^n = \prod_{k=1}^{\infty}\left(\frac{1}{1-x^k}\right)$$

Úvod

- Teorie čísel se zabývá vlastnostmi (hlavně celých) čísel.
- Jedná se o jednu z nejstarších matematických disciplín vedle algebry, aritmetiky a geometrie.
- Poznatky jsou v současné době používány v asymetrické kryptografii (RSA, pseudonáhodné generátory).

Hlavní body

Dělitelnost

Definice

Mějme $a, b \in \mathbb{Z}$, platí, že a **dělí** b, značíme $a \mid b$, právě tehdy, když: $(\exists k \in \mathbb{Z})(a \cdot k = b)$.

Definice

Číslo $c \in \mathbb{N}_0$ je **největším společných dělitelem** čísel $a, b \in \mathbb{Z}$, značíme $c = \gcd(a, b)$, pokud je jejich společný dělitel a zároveň je celočíselným násobkém každého jiného jejich společného dělitele.

Definice

Čísla $a, b \in \mathbb{Z}$ nazýváme **nesoudělná** právě tehdy, když $\gcd(a, b) = 1$.

Definice prvočísla

Definice

Přirozené číslo $n \geq 2$ nazýváme **prvočíslem** právě tehdy, když má jen dva dělitele: 1 a sebe sama.

Definice

Přirozené číslo $n \geq 2$ nazýváme **složeným číslem** právě tehdy, když není prvočíslem (má jiného dělitele než 1 a sebe sama).

Z těchto definic je patrné, že číslo 1 nepatří ani do čísel složených ani do prvočísel a tvoří samotnou skupinu.

Základní věta aritmetiky

Věta

Každé $c \in \mathbb{N}, c \geq 2$ lze vyjádřit ve tvaru:

$$c = p_1^{m_1} \cdot p_2^{m_2} \cdot \ldots \cdot p_n^{m_n} = \prod_{i=1}^{n} p_i^{m_i}$$

kde $p_1, \ldots, p_n$ jsou prvočísla a $m_1, \ldots, m_n$ jsou celá čísla. Tento zápis také nazýváme **prvočíselným rozkladem**.

Příklad

$36 = 4 \cdot 9 = 2 \cdot 2 \cdot 3 \cdot 3 = 2^2 \cdot 3^2$

Základní věta aritmetiky

Problém faktorizace je předpokládán za velice obtížný. Není znám obecný algoritmus co by dokázal faktorizovat v polynomiálním čase a předpokládá se, že takový algoritmus neexistuje.

Na tomto principu funguje RSA.

Hlavní body

Kongruence modulo n

Definice

Mějme $a, b, n \in \mathbb{N}$ a $n \geq 2$. Říkáme, že a je **kongruentní** s b modulo n, značíme

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

právě tehdy, když $n \mid (a - b)$.

Příklad

$11 \equiv 7 \equiv 3 \pmod{4}$

Věta

Následující tvrzení jsou ekvivalentní:

- $a \equiv b \pmod{n}$
- $a \mod n = b \mod n$
- $(\exists l \in \mathbb{N})(b = a + l \cdot n)$

Úpravy v kongruencích modulo n

- Můžeme nejprve zmodulovat čísla a pak s nimi dále počítat (u sčítání, odčítání, násobení a dělení).
- Můžeme obě strany rovnic vynásobit stejným číslem. Také můžeme od nich stejné čísla odečítat nebo přičítat.
- Nemůžeme modulovat čísla v exponentech. Tzn. provádět úpravy typu: $4^7 \not\equiv 4^2 \pmod 5$
- Nemůžeme jednoduše dělit obě strany rovnice číslem. Např.: $4x \equiv 12 \pmod{20}$ a $x \equiv 3 \pmod{20}$ nejsou stejné rovnice. První rovnice platí pro $x = 8$, ale druhá ne.

Krácení rovnic v kongruencích modulo n

Věta

Mějme $a, b, c, n \in \mathbb{N}$ a $n \geq 2$, pak platí:

$$ac \equiv bc \pmod{n} \Leftrightarrow a \equiv b \pmod{\frac{n}{\gcd(c,n)}}$$

Příklad

$$\begin{aligned} 4x &\equiv 8 \pmod{18} \div 4 \\ 4x &\equiv 8 \pmod{18} \div 4,\ \gcd(18,4) = 2 \\ x &\equiv 2 \pmod{9} \end{aligned}$$

Zjednodušte tak, aby se na levé straně nacházelo jen x

$8 + 5x \equiv 18 \pmod{15}$	$x \equiv 2 \pmod{3}$
$18 + 12x \equiv 78 \pmod{9}$	$x \equiv 2 \pmod{3}$
$9 + 12x \equiv 225 \pmod{30}$	$x \equiv 3 \pmod{5}$
$2 + 8x \equiv 39 \pmod{29}$	$x \equiv 1 \pmod{29}$
$9 + 5x \equiv 49 \pmod{17}$	$x \equiv 8 \pmod{17}$
$6 + 12x \equiv 42 \pmod{15}$	$x \equiv 3 \pmod{5}$

Hlavní body

Algoritmus *Square and Multiply*

Algoritmus *Square and Multiply* (česky algoritmus binárního umocňování, ale používá se častěji anglický název) je nejjednodušší a nejobecnější metoda pro krácení exponentů, která funguje když máme vypočíst $a^b \mod n$ pro libovolné $a, b, n \in \mathbb{N}$.

Funguje na tom principu, že exponent krátit nemůžeme, ale základ mocniny ano. Takže například výraz $a^{2b} \mod n$, jsme schopni přepsat jako: $(a^2)^n \mod n$. Nyní pokud a^2 vyjde větší než n, tak jsme si ulehčili práci a můžeme mezivýsledek zmodulovat a nyní budeme mocnit menší číslo.

Ukázka *Square and Multiply*

Ukažme si *Square and Multiply* na příkladě. Zkusme vypočítat 2^{15} mod 5.

Jako první si rozdělme 2^{15} na $2^1 \cdot 2^2 \cdot 2^4 \cdot 2^8$.

A nyní už jen vypočítejme jednotlivé mocniny:

$$2^1 \equiv 2 \pmod 5, \quad 2^2 \equiv (2^1)^2 \equiv 2^2 \equiv 4 \pmod 5$$
$$2^4 \equiv (2^2)^2 \equiv 4^2 \equiv 16 \equiv 1 \pmod 5$$
$$2^8 \equiv (2^4)^2 \equiv 1^2 \equiv 1 \pmod 5$$

$$2^{15} \equiv 2 \cdot 4 \cdot 1 \cdot 1$$

Popis Square and Multiply

1. Rozdělíme naši mocninu na součin tak, aby v exponentech byly jen mocniny dvojek.
2. Postupně vypočítáme od nejmenšího exponentu všechny mocniny v našem součinu tak, že využijeme výsledek z té předchozí.
3. Vypočítáme naši mocninu ze součinu mocnin.

- Ve skriptech je pseudokód.

Příklady

Zjednodušte následující výrazy

$2^{16} \pmod 8$
$3^{31} \pmod{10}$
$6^{64} \pmod 7$
$7^{7} \pmod 8$

Malá Fermatova věta

Věta

Pro každé prvočíslo p a každé $a \in \mathbb{Z}$ platí:

$$a^p \equiv a \pmod{p}$$

Z této věty také plyne: $a^{p-1} \equiv 1 \pmod{p}$.

Příklad

Podle Malé Fermatovy věty má platit: $3^4 \equiv 1 \pmod{5}$. Ověřme pomocí algoritmu Square and Multiply.

$3^2 \equiv 9 \equiv 4 \pmod{5}$, $3^4 \equiv 4^2 \equiv 16 \equiv 1 \pmod{5}$

Příklady

Zjednodušte následující výrazy

$7^{26} \pmod{13}$
$8^{20} \pmod{17}$
$5^{16} \pmod{16}$
$26^{50} \pmod{23}$

Eulerova věta je zobecněním malé Fermatovy věty pro p, které není prvočíslem. Pro ukázání Eulerovy věty si ale musíme říct co je **Eulerova funkce**.

Definice

Eulerova funkce (značíme $\varphi(n)$) je počet všech $k \in \mathbb{N}$ takových, že $1 \leq k \leq n$ a $\gcd(k, n) = 1$.

Slovně: **Eulerova funkce** nám udává počet čísel menší než n, která jsou s ním **nesoudělná**.

Vlastnosti Eulerovy funkce

Pro výpočet se nám budou často hodit tyto vlastnosti Eulerovy funkce:

- $\varphi(p) = p - 1$, kde p je prvočíslo (plyne přímo z definice prvočísla)
- $\varphi(p^a) = (p-1) \cdot p^{a-1}$, pro prvočíslo p a kladné celé a
- Pro nesoudělná x, y platí: $\varphi(x \cdot y) = \varphi(x) \cdot \varphi(y)$

Z těchto vlastností a ze základní věty aritmetiky (prvočíselný rozklad) nám plyne:

Věta

Pro $c \in \mathbb{N}$ platí, že pokud: $c = p_1^{m_1} \cdot p_2^{m_2} \cdot \ldots \cdot p_n^{m_n}$, tak platí:

$$\varphi(c) = (p_1 - 1) \cdot p_1^{m_1 - 1} \cdot (p_2 - 1) \cdot p_2^{m_2 - 1} \cdot \ldots \cdot (p_n - 1) \cdot p_n^{m_n - 1}$$

Eulerova věta

Věta

Pro každé $n \in \mathbb{N}$ a každé $a \in \mathbb{N}$ takové, že $\gcd(n, a) = 1$, platí:

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

Příklady

Zjednodušte následující výrazy

$3^5 \pmod 8$

$8^6 \pmod 9$

$3^5 \pmod 9$

$7^{17} \pmod{15}$