Základy elementární teorie čísel

Dělení se zbytkem v oboru celých čísel

Ať a, b jsou libovolná celá čísla, $b \neq 0$. Pak existují jednoznačně určená celá čísla q a r taková, že jsou splněny následující dvě podmínky:

1. Platí rovnost $a = q \cdot b + r$.
2. Číslo r splňuje nerovnost $0 \leq r < |b|$.

Důkaz.

Indukcí, tj. rekursivním algoritmem! Viz skripta. ∎

Definice

Jednoznačně určené číslo r z předchozí věty nazveme zbytkem po dělení čísla a číslem b.

Dělení se zbytkem v oboru celých čísel

Ať a, b jsou libovolná celá čísla, $b \neq 0$. Pak existují jednoznačně určená celá čísla q a r taková, že jsou splněny následující dvě podmínky:

1. Platí rovnost $a = q \cdot b + r$.
2. Číslo r splňuje nerovnost $0 \leq r < |b|$.

Důkaz.

Indukcí, tj. rekursivním algoritmem! Viz skripta. ∎

Definice

Jednoznačně určené číslo r z předchozí věty nazveme zbytkem po dělení čísla a číslem b.

Dělení se zbytkem v oboru celých čísel

Ať a, b jsou libovolná celá čísla, $b \neq 0$. Pak existují jednoznačně určená celá čísla q a r taková, že jsou splněny následující dvě podmínky:

1. Platí rovnost $a = q \cdot b + r$.
2. Číslo r splňuje nerovnost $0 \leq r < |b|$.

Důkaz.

Indukcí, tj. rekursivním algoritmem! Viz skripta. ■

Definice

Jednoznačně určené číslo r z předchozí věty nazveme zbytkem po dělení čísla a číslem b.

Definice

Řekneme, že přirozené číslo a dělí přirozené číslo b (značíme $a \mid b$), pokud existuje přirozené číslo n takové, že $b = n \cdot a$.

Řekneme, že celé číslo a dělí celé číslo b, (též značíme $a \mid b$), pokud existuje celé číslo n takové, že $b = n \cdot a$.

Pokud a dělí číslo b (v oboru přirozených čísel nebo celých čísel), pak číslo a nazveme dělitelem čísla b.

Pozor!

Podle definice je

1. číslo 0 dělitelné každým číslem n (i nulou).
2. každé číslo n dělitelné číslem 1.

Definice

Řekneme, že přirozené číslo a dělí přirozené číslo b (značíme $a \mid b$), pokud existuje přirozené číslo n takové, že $b = n \cdot a$.

Řekneme, že celé číslo a dělí celé číslo b, (též značíme $a \mid b$), pokud existuje celé číslo n takové, že $b = n \cdot a$.

Pokud a dělí číslo b (v oboru přirozených čísel nebo celých čísel), pak číslo a nazveme dělitelem čísla b.

Pozor!

Podle definice je

1. číslo 0 dělitelné každým číslem n (i nulou).
2. každé číslo n dělitelné číslem 1.

Definice

Přirozenému číslu p většímu než 1 říkáme prvočíslo, pokud je číslo p dělitelné pouze čísly 1 a p.

Tvrzení

Množina všech prvočísel $\mathbb{P}$ je nekonečná množina.

Důkaz. (Eukleides: 3. století př.n.l.)

Předpokládejme, že $\mathbb{P} = \{p_1, \ldots, p_n\}$. Definujeme přirozené číslo p takto: $p = p_1 \cdot p_2 \cdot \cdots \cdot p_{n-1} \cdot p_n + 1$. Zřejmě $p \notin \mathbb{P}$. Je-li p prvočíslo, jsme hotovi — původní množina $\{p_1, \ldots, p_n\}$ nemohla obsahovat všechna prvočísla. Je-li p složené číslo, musí se v jeho prvočíselném rozkladu vyskytovat prvočíslo, které není v množině $\{p_1, \ldots, p_n\}$. V každém případě množina $\{p_1, \ldots, p_n\}$ neobsahuje všechna prvočísla, množina $\mathbb{P}$ musí být nekonečná. ∎

Definice

Přirozenému číslu p většímu než 1 říkáme prvočíslo, pokud je číslo p dělitelné pouze čísly 1 a p.

Tvrzení

Množina všech prvočísel $\mathbb{P}$ je nekonečná množina.

Důkaz. (Eukleides: 3. století př.n.l.)

Předpokládejme, že $\mathbb{P} = \{p_1, \ldots, p_n\}$. Definujeme přirozené číslo p takto: $p = p_1 \cdot p_2 \cdot \cdots \cdot p_{n-1} \cdot p_n + 1$. Zřejmě $p \notin \mathbb{P}$. Je-li p prvočíslo, jsme hotovi — původní množina $\{p_1, \ldots, p_n\}$ nemohla obsahovat všechna prvočísla. Je-li p složené číslo, musí se v jeho prvočíselném rozkladu vyskytovat prvočíslo, které není v množině $\{p_1, \ldots, p_n\}$. V každém případě množina $\{p_1, \ldots, p_n\}$ neobsahuje všechna prvočísla, množina $\mathbb{P}$ musí být nekonečná. ∎

Definice

Přirozenému číslu p většímu než 1 říkáme prvočíslo, pokud je číslo p dělitelné pouze čísly 1 a p.

Tvrzení

Množina všech prvočísel $\mathbb{P}$ je nekonečná množina.

Důkaz. (Eukleides: 3. století př.n.l.)

Předpokládejme, že $\mathbb{P} = \{p_1, \ldots, p_n\}$. Definujeme přirozené číslo p takto: $p = p_1 \cdot p_2 \cdot \cdots \cdot p_{n-1} \cdot p_n + 1$. Zřejmě $p \notin \mathbb{P}$. Je-li p prvočíslo, jsme hotovi — původní množina $\{p_1, \ldots, p_n\}$ nemohla obsahovat všechna prvočísla. Je-li p složené číslo, musí se v jeho prvočíselném rozkladu vyskytovat prvočíslo, které není v množině $\{p_1, \ldots, p_n\}$. V každém případě množina $\{p_1, \ldots, p_n\}$ neobsahuje všechna prvočísla, množina $\mathbb{P}$ musí být nekonečná. ∎

Základní věta elementární teorie čísel

Pro každé přirozené číslo $x \geq 2$ existuje jednoznačný prvočíselný rozklad.

Příklad

Číslo 1960 má prvočíselný rozklad $2^3 \cdot 5 \cdot 7^2$.
Tudíž číslo 1960 má celkem

$$4 \cdot 2 \cdot 3 = 24$$

různých dělitelů.

Základní věta elementární teorie čísel

Pro každé přirozené číslo $x \geq 2$ existuje jednoznačný prvočíselný rozklad.

Příklad

Číslo 1960 má prvočíselný rozklad $2^3 \cdot 5 \cdot 7^2$.
Tudíž číslo 1960 má celkem

$$4 \cdot 2 \cdot 3 = 24$$

různých dělitelů.

Definice

Řekneme, že přirozené číslo d je největším společným dělitelem přirozených čísel a, b (značení $d = \gcd(a, b)$), pokud jsou splněny následující dvě podmínky:[a]

1. Číslo d je společným dělitelem čísel a, b, tj. platí, $d \mid a$ a současně $d \mid b$ (v oboru přirozených čísel).
2. Číslo d je největším ze všech společných dělitelů čísel a, b, tj. platí následující: je-li c takové přirozené číslo, pro které platí $c \mid a$ a současně $c \mid b$, potom $c \mid d$.

Pokud $\gcd(a, b) = 1$, řekneme, že přirozená čísla a, b jsou nesoudělná.

[a] Anglicky *greatest common divisor*, odtud pochází značení.

Definice

Řekneme, že přirozené číslo d je největším společným dělitelem přirozených čísel a, b (značení $d = \gcd(a, b)$), pokud jsou splněny následující dvě podmínky:[a]

1. Číslo d je společným dělitelem čísel a, b, tj. platí, $d \mid a$ a současně $d \mid b$ (v oboru přirozených čísel).
2. Číslo d je největším ze všech společných dělitelů čísel a, b, tj. platí následující: je-li c takové přirozené číslo, pro které platí $c \mid a$ a současně $c \mid b$, potom $c \mid d$.

Pokud $\gcd(a, b) = 1$, řekneme, že přirozená čísla a, b jsou nesoudělná.

[a] Anglicky *greatest common divisor*, odtud pochází značení.

Definice

Řekneme, že přirozené číslo d je největším společným dělitelem přirozených čísel a, b (značení $d = \gcd(a, b)$), pokud jsou splněny následující dvě podmínky:[a]

1. Číslo d je společným dělitelem čísel a, b, tj. platí, $d \mid a$ a současně $d \mid b$ (v oboru přirozených čísel).
2. Číslo d je největším ze všech společných dělitelů čísel a, b, tj. platí následující: je-li c takové přirozené číslo, pro které platí $c \mid a$ a současně $c \mid b$, potom $c \mid d$.

Pokud $\gcd(a, b) = 1$, řekneme, že přirozená čísla a, b jsou nesoudělná.

[a] Anglicky *greatest common divisor*, odtud pochází značení.

Definice

Řekneme, že přirozené číslo d je největším společným dělitelem přirozených čísel a, b (značení $d = \gcd(a, b)$), pokud jsou splněny následující dvě podmínky:[a]

1. Číslo d je společným dělitelem čísel a, b, tj. platí, $d \mid a$ a současně $d \mid b$ (v oboru přirozených čísel).
2. Číslo d je největším ze všech společných dělitelů čísel a, b, tj. platí následující: je-li c takové přirozené číslo, pro které platí $c \mid a$ a současně $c \mid b$, potom $c \mid d$.

Pokud $\gcd(a, b) = 1$, řekneme, že přirozená čísla a, b jsou nesoudělná.

[a] Anglicky *greatest common divisor*, odtud pochází značení.

Příklad

Pro čísla $a = 1960 = 2^3 \cdot 5 \cdot 7^2$ a $b = 308 = 2^2 \cdot 7 \cdot 11$ je $\gcd(a, b) = 2^2 \cdot 7 = 28$.
Všechna společná prvočísla v maximální společné mocnině.

Prvočíselný rozklad je obecně velmi těžký problém — viz například šifrovací protokol RSA (šifrování s veřejným klíčem).

Lze se při hledání největšího společného dělitele znalosti prvočíselných rozkladů vyhnout?

Příklad

Pro čísla $a = 1960 = 2^3 \cdot 5 \cdot 7^2$ a $b = 308 = 2^2 \cdot 7 \cdot 11$ je $\gcd(a, b) = 2^2 \cdot 7 = 28$.
Všechna společná prvočísla v maximální společné mocnině.

Prvočíselný rozklad je obecně velmi těžký problém — viz například šifrovací protokol RSA (šifrování s veřejným klíčem).

Lze se při hledání největšího společného dělitele znalosti prvočíselných rozkladů vyhnout?

Příklad

Pro čísla $a = 1960 = 2^3 \cdot 5 \cdot 7^2$ a $b = 308 = 2^2 \cdot 7 \cdot 11$ je $\gcd(a, b) = 2^2 \cdot 7 = 28$.
Všechna společná prvočísla v maximální společné mocnině.

Prvočíselný rozklad je obecně velmi těžký problém — viz například šifrovací protokol RSA (šifrování s veřejným klíčem).

Lze se při hledání největšího společného dělitele znalosti prvočíselných rozkladů vyhnout?

Jednoduchý Eukleidův algoritmus

Předpokládejme, že pro přirozená čísla a, b platí $a \geq b > 0$.

Označme $b = b_0$ a dělením se zbytkem vytvořme posloupnost přirozených čísel $b_1, b_2, \ldots$:

$$\begin{aligned} a &= q_0 \cdot b_0 + b_1 \\ b_0 &= q_1 \cdot b_1 + b_2 \\ b_1 &= q_2 \cdot b_2 + b_3 \\ &\vdots \end{aligned}$$

dokud není $b_n = 0$.

Potom $\gcd(a, b) = b_{n-1}$.

Proč by to mělo fungovat? Terminace? Parciální korektnost?

Jednoduchý Eukleidův algoritmus

Předpokládejme, že pro přirozená čísla a, b platí $a \geq b > 0$.

Označme $b = b_0$ a dělením se zbytkem vytvořme posloupnost přirozených čísel $b_1, b_2, \ldots$:

$$\begin{aligned} a &= q_0 \cdot b_0 + b_1 \\ b_0 &= q_1 \cdot b_1 + b_2 \\ b_1 &= q_2 \cdot b_2 + b_3 \\ &\vdots \end{aligned}$$

dokud není $b_n = 0$.

Potom $\gcd(a, b) = b_{n-1}$.

Proč by to mělo fungovat? Terminace? Parciální korektnost?

Příklad

Běh jednoduchého Eukleidova algoritmu pro $a = 427$, $b = 133$.

$$\begin{aligned} 427 &= 3 \cdot 133 + 28 \\ 133 &= 4 \cdot 28 + 21 \\ 28 &= 1 \cdot 21 + 7 \\ 21 &= 3 \cdot 7 + 0 \end{aligned}$$

Proto platí, že $\gcd(427, 133) = 7$.

Tvrzení (Terminace jednoduchého Eukleidova algoritmu)

Existuje n takové, že $b_n = 0$.

Důkaz.

Platí $b_0 > b_1 > b_2 > b_3 > \ldots$. Jde totiž o zbytky při dělení. Proto existuje n takové, že $b_n = 0$. (Princip dobrého uspořádání!) ∎

Zbytky po dělení tvoří variant jednoduchého Eukleidova algoritmu.

Tvrzení (Terminace jednoduchého Eukleidova algoritmu)

Existuje n takové, že $b_n = 0$.

Důkaz.

Platí $b_0 > b_1 > b_2 > b_3 > \dots$. Jde totiž o zbytky při dělení. Proto existuje n takové, že $b_n = 0$. (Princip dobrého uspořádání!) ∎

Zbytky po dělení tvoří variant jednoduchého Eukleidova algoritmu.

Tvrzení (Terminace jednoduchého Eukleidova algoritmu)

Existuje n takové, že $b_n = 0$.

Důkaz.

Platí $b_0 > b_1 > b_2 > b_3 > \dots$. Jde totiž o zbytky při dělení. Proto existuje n takové, že $b_n = 0$. (Princip dobrého uspořádání!) ■

Zbytky po dělení tvoří variant jednoduchého Eukleidova algoritmu.

Tvrzení (Parciální korektnost jednoduchého Eukleidova algoritmu)

Předpokládejme, že pro přirozená čísla a, b platí $a \geq b > 0$. Vydělme číslo a číslem b se zbytkem. Pro nějaká q a r tedy platí

$$a = q \cdot b + r, \ \ kde\ 0 \leq r < b.$$

1. *Je-li $r = 0$, potom b je největším společným dělitelem čísel a, b.*
2. *Je-li $r > 0$, označme jako d jakéhokoli společného dělitele původních čísel a a b. Potom d je společný dělitel čísel b a r.*

Být společným dělitelem tvoří invariant jednoduchého Eukleidova algoritmu.

Tvrzení (Parciální korektnost jednoduchého Eukleidova algoritmu)

Předpokládejme, že pro přirozená čísla a, b platí $a \geq b > 0$. Vydělme číslo a číslem b se zbytkem. Pro nějaká q a r tedy platí

$$a = q \cdot b + r, \ \ kde\ 0 \leq r < b.$$

1. *Je-li $r = 0$, potom b je největším společným dělitelem čísel a, b.*
2. *Je-li $r > 0$, označme jako d jakéhokoli společného dělitele původních čísel a a b. Potom d je společný dělitel čísel b a r.*

Být společným dělitelem tvoří invariant jednoduchého Eukleidova algoritmu.

Příklad

Zpětný běh jednoduchého Eukleidova algoritmu pro $\gcd(427, 133) = 7$:

$$\begin{aligned} 7 &= 1 \cdot \underline{28} - \underline{21} \\ &= 1 \cdot (\boxed{427} - 3 \cdot \boxed{133}) - (\boxed{133} - 4 \cdot \underline{28}) \\ &= 1 \cdot (\boxed{427} - 3 \cdot \boxed{133}) - (\boxed{133} - 4 \cdot (\boxed{427} - 3 \cdot \boxed{133})) \\ &= 5 \cdot \boxed{427} - 16 \cdot \boxed{133} \end{aligned}$$

Zbytky po dělení jsou podtržené, čísla 427 a 133 jsou v rámečku. Tudíž platí:

$$\gcd(427, 133) = 7 = \alpha \cdot 427 + \beta \cdot 133$$

pro $\alpha = 5$, $\beta = -16$.

Důsledek (Bezoutova rovnost)

Ať a a b jsou přirozená čísla. Potom existují celá čísla α, β tak, že platí rovnost

$$\gcd(a, b) = \alpha \cdot a + \beta \cdot b.$$

Důkaz.

Zpětný chod jednoduchého Eukleidova algoritmu. ∎

Zpětný chod je těžkopádný.
Neexistuje lepší způsob hledání čísel α, β?
Ano: rozšířený Eukleidův algoritmus.

Důsledek (Bezoutova rovnost)

Ať a a b jsou přirozená čísla. Potom existují celá čísla α, β tak, že platí rovnost

$$\gcd(a, b) = \alpha \cdot a + \beta \cdot b.$$

Důkaz.

Zpětný chod jednoduchého Eukleidova algoritmu. ∎

Zpětný chod je těžkopádný.
Neexistuje lepší způsob hledání čísel α, β?
Ano: rozšířený Eukleidův algoritmus.

Důsledek (Bezoutova rovnost)

Ať a a b jsou přirozená čísla. Potom existují celá čísla α, β tak, že platí rovnost

$$\gcd(a, b) = \alpha \cdot a + \beta \cdot b.$$

Důkaz.

Zpětný chod jednoduchého Eukleidova algoritmu. ∎

Zpětný chod je těžkopádný.
Neexistuje lepší způsob hledání čísel α, β?
Ano: rozšířený Eukleidův algoritmus.

Důsledek (Bezoutova rovnost)

Ať a a b jsou přirozená čísla. Potom existují celá čísla α, β tak, že platí rovnost

$$\gcd(a, b) = \alpha \cdot a + \beta \cdot b.$$

Důkaz.

Zpětný chod jednoduchého Eukleidova algoritmu. ∎

Zpětný chod je těžkopádný.
Neexistuje lepší způsob hledání čísel α, β?
Ano: rozšířený Eukleidův algoritmus.

Příklad

Rozšířený Eukleidův algoritmus na nalezení Bezoutovy rovnosti

$$\gcd(427, 133) = \alpha \cdot 427 + \beta \cdot 133$$

a	b	q	r	α_2	α_1	β_2	β_1
427	133			1	0	0	1
427	133	3	28	0	1	1	-3
133	28	4	21	1	-4	-3	13
28	21	1	7	-4	5	13	-16
21	7	3	0	5	-19	-16	61
7	0						

Tvrdíme, že $\gcd(427, 133) = 7$ a že Bezoutova rovnost má tvar $7 = 5 \cdot 427 + (-16) \cdot 133$.

Příklad

Rozšířený Eukleidův algoritmus na nalezení Bezoutovy rovnosti

$$\gcd(427, 133) = \alpha \cdot 427 + \beta \cdot 133$$

a	b	q	r	α_2	α_1	β_2	β_1
427	133			1	0	0	1
427	133	3	28	0	1	1	-3
133	28	4	21	1	-4	-3	13
28	21	1	7	-4	5	13	-16
21	7	3	0	5	-19	-16	61
7	0						

Tvrdíme, že $\gcd(427, 133) = 7$ a že Bezoutova rovnost má tvar $7 = 5 \cdot 427 + (-16) \cdot 133$.

Terminace a parciální korektnost

1. Terminace: viz terminace obyčejného Eukleidova algoritmu.
2. Parciální korektnost: na každém řádku platí

$$\alpha_1 \cdot a + \beta_1 \cdot b = r, \quad \text{pro aktuální zbytek } r > 0.$$

To jest: našli jsme invariant rozšířeného Eukleidova algoritmu.