**BI-SPOL-33 Modulární aritmetika, základy teorie čísel, Malá Fermatova věta, diofantické rovnice, lineární kongruence, Čínská věta o zbytcích**

BI-ZDM

## Modulární aritmetika

* Aritmetika definovaná na množině (), kde . V jedno-modulární aritmetice je každé číslo ze Z zobrazeno na číslo *r* z . Číslo *r* je zbytek po dělení čísla *b* číslem *m* (neboli *b* mod *m*)

Obsah obrázku stůl

Popis byl vytvořen automaticky

Obsah obrázku text

Popis byl vytvořen automaticky

**Multiplikativní inverze modulo m**

Obsah obrázku text

Popis byl vytvořen automaticky

**Multiplikativní inverze v prvočíselném modulu**

**Obsah obrázku text

Popis byl vytvořen automaticky**

**„Dělení“**

**Obsah obrázku text

Popis byl vytvořen automaticky**

**Kongruence**

* Máme číslo *a*, to je ekvivalentní (kongruentní) s *b* v modulo *m*. Tzn. *a* bude ve stejném modulu rovno *b*.

**Obsah obrázku text

Popis byl vytvořen automaticky**

* **Vlastnosti**

**Obsah obrázku text

Popis byl vytvořen automaticky**

**Zbytkové třídy**

**Obsah obrázku text

Popis byl vytvořen automaticky**

**Obsah obrázku text

Popis byl vytvořen automaticky**

* Na to, kdy se provede operace modulo m nezáleží

## Základy teorie čísel

* Odvětví matematiky, které se zabývá vlastnostmi čísel
* Uplatnění v kryptografii, kódování, diofantické rovnice, generátory náhodných čísel…

**Dělitelnost**

**Obsah obrázku text

Popis byl vytvořen automaticky**

* relace částečného uspořádání (reflexivní, tranzitivní, antisymetické)

**Obsah obrázku text

Popis byl vytvořen automaticky**

**Obsah obrázku text

Popis byl vytvořen automaticky**

**Dělení se zbytkem**

**Obsah obrázku text

Popis byl vytvořen automaticky**

**r = a mod b**

**Společný dělitel, společný násobek**

**Obsah obrázku text

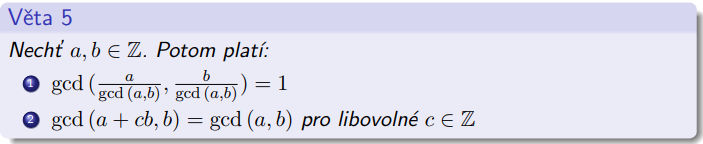
Popis byl vytvořen automaticky**

**Obsah obrázku text

Popis byl vytvořen automaticky**

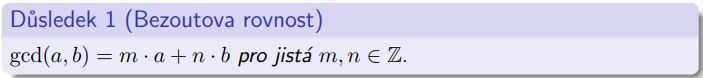
* **GCD i LCM jsou vždy přirozená (tj. nezáporná) čísla**

**Vlastnosti GCD**

****

**Obsah obrázku text

Popis byl vytvořen automaticky**

****

**Euklidův algoritmus**

* Pro hledání *gcd*
* gcd je poslední nenulový zbytek
* vyžaduje nejvýše 5*n* dělení, kde n je počet cifer čísla *b*

Obsah obrázku stůl

Popis byl vytvořen automaticky

**Rozšířený Euklidův algoritmus**

* hledáme *x* a *y* takové, že gcd(*a,b*) = *x \* a* + *y \* b*
* pro výpočet gcd a inverze čísla
* gcd (a,b) = rk, hledáme inverzi 12 v – viz. příklad – inverze 12 = 3

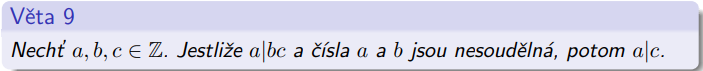
Obsah obrázku text, bílá

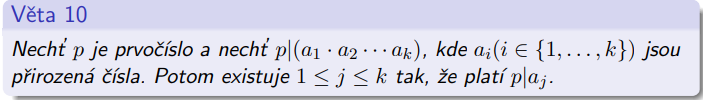
Popis byl vytvořen automatickyObsah obrázku stůl

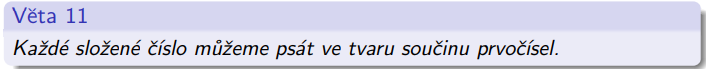
Popis byl vytvořen automaticky

**Prvočísla**

* Číslo je prvočíslo, pokud je dělitelné pouze 1 a samo sebou
* existuje nekonečně mnoho prvočísel
* 1 není prvočíslo







Obsah obrázku text

Popis byl vytvořen automaticky

Obsah obrázku text

Popis byl vytvořen automaticky

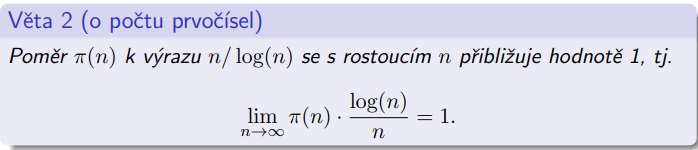
Obsah obrázku text

Popis byl vytvořen automaticky



Obsah obrázku text

Popis byl vytvořen automaticky

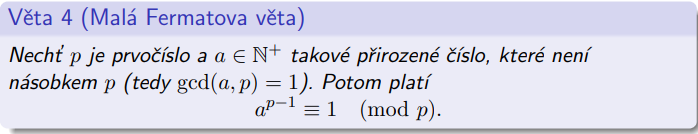


**Pro počítání**

Obsah obrázku text

Popis byl vytvořen automaticky

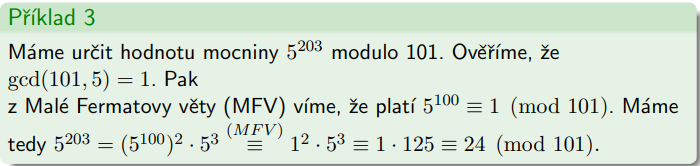
### Malá Fermatova věta



* důkaz sporem z předpokladu, že čísla 1,..., p-1 jsou nesoudělná
* 
* 

**Použití**

* Výpočet mocnin modulo *p*



* Výpočet multiplikativní inverze čísla *a* modulo *p*

Obsah obrázku text

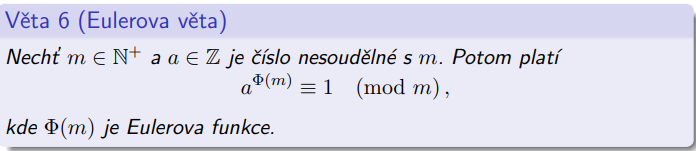
Popis byl vytvořen automaticky

Obsah obrázku text

Popis byl vytvořen automaticky

**Eulerova věta**

* EV je zobecněná MFV



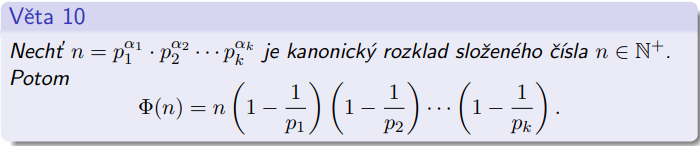
**Eulerova funkce**

Obsah obrázku text

Popis byl vytvořen automaticky



* Pokud nemáme prvočíslo, použijeme prvočíselný rozklad







* pokud je *n* prvočíslo, pak *EF = p-1*
* **Vlastnosti**

Obsah obrázku text

Popis byl vytvořen automaticky



**Použití Eulerovy věty**

* Hledání multiplikativní inverze

**Obsah obrázku text

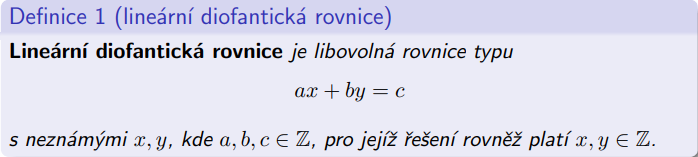
Popis byl vytvořen automaticky**

* Umocňování modulo m

**Obsah obrázku text

Popis byl vytvořen automaticky**

## Diofantická rovnice



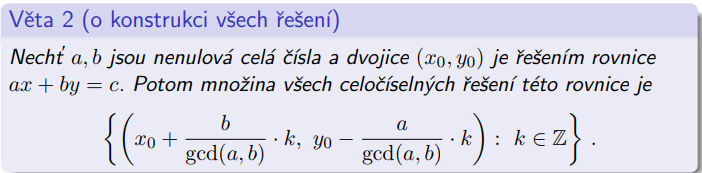
Obsah obrázku text

Popis byl vytvořen automaticky

**Postup řešení rovnice** *ax + by = c*

Obsah obrázku text

Popis byl vytvořen automaticky



* Poznámka:

**Obsah obrázku text

Popis byl vytvořen automaticky**

A

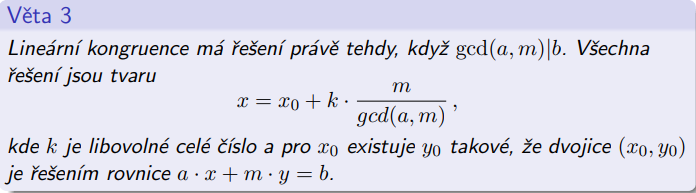
B

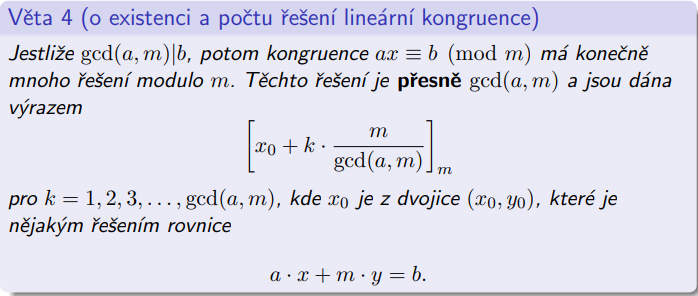
## Lineární kongruence

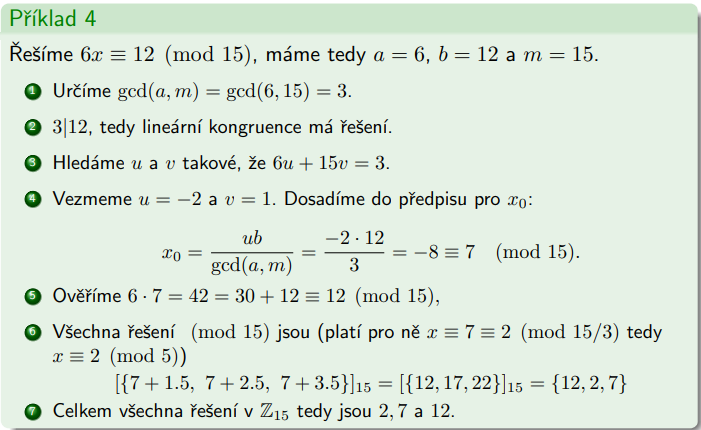
* Máme To můžeme napsat jako *ax + my = b.* Dostáváme diofantickou rovnici, kde hledáme pouze *x*.

Obsah obrázku text

Popis byl vytvořen automaticky



**Existence a počet řešení**

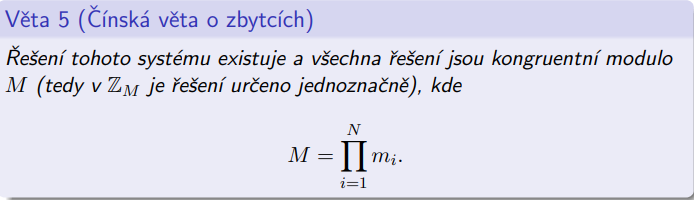


## Čínská věta o zbytcích

* Před x musí být vždy 1. Když není, tak musím tu kongruenci vyřešit, aby tam byla 1\*x
* Když si zvolím modul M jako součin všech modulů, tak řešení existuje v tomto modulu M

Obsah obrázku text

Popis byl vytvořen automaticky



Jak řešit:

Obsah obrázku text

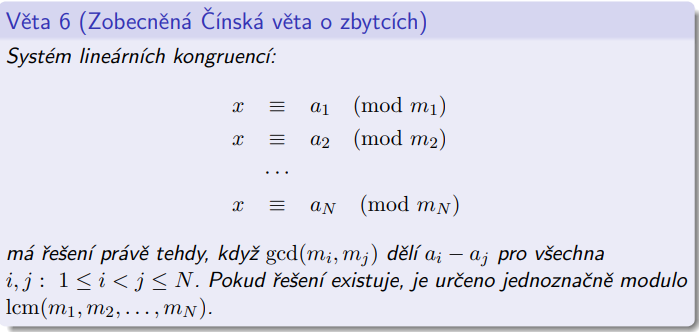
Popis byl vytvořen automaticky

* Když do toho velkého výrazu dáme modulo tak nám vypadnou všechny členy, kromě jednoho – toho co má taky index *i*. Ostatní vypadnou kvůli tomu, že obsahují modulo jako násobek uvnitř
* je inverze k – dáme-li tedy modulo vyleze nám přesně to *a*

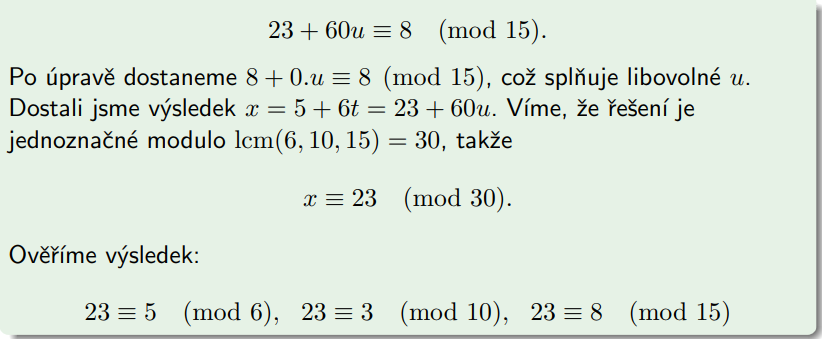
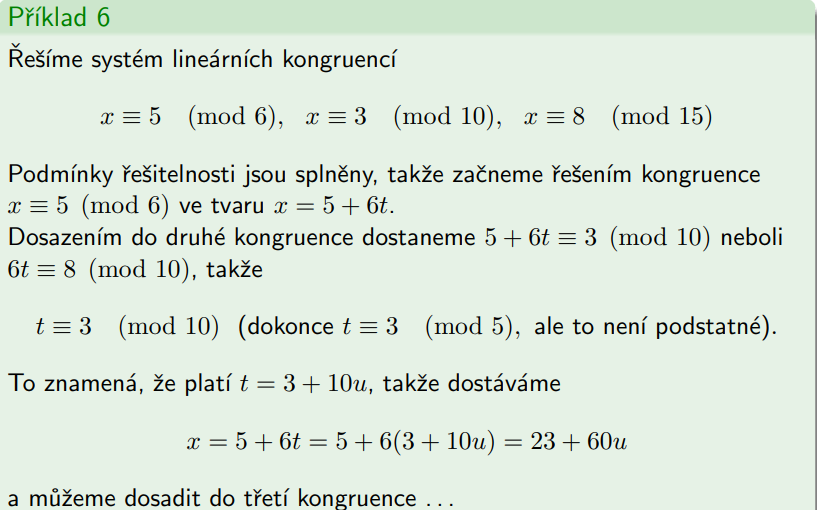
Obsah obrázku text

Popis byl vytvořen automaticky

**Zobecněná čínská věta o zbytcích**

****

* Pro všechny páry kongruence musíme zkontrolovat, že gcd jejich modulů dělí rozdíl zbytků. (tzn. *gcd(m1 , m2 ) | a1 − a2* → pokud ano, pak existuje řešení – jenom jedno).



## Otázky a odpovědi

1. Využití diofantických rovnice, lineární kongruence a ČVOZ?
2. Co vlastně znamená kongruence?
3. Co dokáže řešit ČVOZ?  
   Příklady typu: Mám hromádku kostiček, když je seřadím do věže po 2 zbyde 1, když je seřadím do věže po 3 zbydou 2, když je seřadím do věže po 7 vedle sebe zbydou mi 4. Kolik jich je?  
   Nebo soustava lineárních kongruencí  
   Nebo např. sdílení tajemství. Mám Y lidí a každý dostane nějakou kongruenci. Výsledné „tajemství“ x získáme pouze všichni společně
4. Proč se  rovná   
   Je to vyjádření zbytku po dělení
5. Jak spolu souvisí kongruence a diofantické rovnice?  
   kongruenci lze přepsat do tvaru diofantické rovnice
6. Lineárne diofantické rovnice (predpis, vlasnosti, kedy majú riešenie, uviesť príklad a vypočítať), lineárne kongruencie a ako súvisia s lineárnymi diofantickými rovnicami