11 Dokaž, že $\forall a \in \mathbb{Z}$ platí následující:

(i) a^2 dává po dělení čtyřmi zbytek nula nebo jedna

$a = 4k + 0$
1
2
3

$a = 2k$

$a = 2k+1$

$a^2 = 4k^2$

↳ zbytek 0

$a^2 = 4k^2 + 4k + 1$

↳ zbytek 1

(ii) a^3 dává po dělení osmi zbytek 0, 1 nebo 4

$a = 2k$

$a^3 = 4k^2 \rightsquigarrow$ zbytek 0 nebo 4

$a = 2k+1$

$a^3 = 4k(k+1) + 1$

$2 \mid$

$8 \mid$ zbytek 8

(iii) a^4 dává podělením 16 zbytek 0 nebo 1

$a = 2k$

$a^4 = 16k^4$

zbytek 0

$a = 2k+1$

$a^4 = (4k(k+1)+1)^2 =$

$= 16k^2(k+1)^2 + 8\underbrace{k(k+1)}_{\text{sudé}} + 1$

$\underbrace{\underbrace{16|}_{\text{sudé}}}_{16|}$

$\Rightarrow$ zbytek 1

Př. 1.2.1

(i) $\forall n \in \mathbb{N}$ platí: $3 \mid 4^n - 1$

$4^n - 1 = (3+1)^n - 1 =$

$= [3^n + \binom{n}{1}3^{n-1} + \binom{n}{2}3^{n-2} + \dots + n\cdot 3 + 1] - 1$

je dělitelné třemi

(ii) $\forall n \in \mathbb{N}$ platí: $5 \mid n^5 - n$

$n^5 - n = n(n^4 - 1) = n(n^2+1)(n^2-1)$

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

- $n = 5k$
  $n = 5k+1$
  $n = 5k-1$
  $\Big\} \Rightarrow 5 \mid n^5 - n$

- $n = 5k \pm 2 \Rightarrow n^2 + 1 = (25k^2 \pm 10k + 4) + 1$

$\Rightarrow 5 \mid n^2 + 1$

(iii) $\forall n \in \mathbb{N}$ platí: $5 \mid 3^{3n+1} + 2^{n+1}$

Ukážeme indukcí:

- $n = 1 \Rightarrow 3^{3\cdot 1+1} + 2^{1+1} = 3^4 + 2^2 =$

$= 81 + 4 = 85$ dělí 5

- $3^{3(n+1)+1} + 2^{(n+1)+1} =$

$= 3^{3n+1+3} + 2^{n+1+1} =$

$= \underbrace{5^3}_{27} \cdot 5^{3n+1} + 2 \cdot 2^{n+1}$

$= 2\underbrace{\left(5^{3n+1} + 2^{n+1}\right)}_{5|} + \underbrace{2 \cdot 5 \cdot 5^{3n+1}}_{5|}$.

1.3 Určete, pro která přirozená $n \in \mathbb{N}$ je n^3+1 dělitelné číslem $n-1$.

$n^3 + 1 = (n^3 - 1) + 2$

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

$n-1 \mid n^3+1 \iff n-1 \mid 2$

$\Downarrow$

$n-1 = 1$ nebo $n-1 = 2$

$n = 2$ $\qquad$ $n = 3$

Připomenutí: $a, b \in \mathbb{Z}$

(a,b) největší společný dělitel

NV
- Eukleidův alg.
- Bezoutova rovnost

$d := (a,b)$, pak ex. $k, l \in \mathbb{Z}$ t.ž.

$$ka + lb = m$$

PŘ 1.4 (i) $a = 10175$

$b = 2277$ $\quad 4 \cdot 2277 = 9108$

$$10175 = \underbrace{4 \cdot 2277}_{9108} + 1067$$

$$2277 = \underbrace{2 \cdot 1067}_{2134} + 143$$

$$1067 = \underbrace{7 \cdot 143}_{1001} + 66$$

$$143 = \underbrace{2 \cdot 66}_{132} + \underbrace{11}_{= \text{ggT}}$$

$$66 = 6 \cdot 11$$

$$11 = 143 - 2 \cdot 66$$

$$= 143 - 2 \cdot (1067 - 7 \cdot 143)$$

$$= 15 \cdot 143 - 2 \cdot 1067$$

$$= 15 \cdot (2277 - 2 \cdot 1067) - 2 \cdot 1067$$

$$= 15 \cdot 2277 - 32 \cdot 1067$$

$$= 15 \cdot 2277 - 32 \cdot (10175 - 4 \cdot 2277)$$

$$= -32 \cdot 10175 + (15 + 32 \cdot 4)\, 2277$$

$$= -32 \cdot 10175 + 143 \cdot 2277$$

(ii) $a = 2^{49} - 1$, $b = 2^{35} - 1$

$2^{49} - 1 = 2^{14}(2^{35} - 1) + (2^{14} - 1)$

$2^{35} - 1 = 2^{21}(2^{14} - 1) + (2^{21} - 1)$

$= 2^7(2^{14} - 1) + (2^7 - 1)$

$= (2^{21} + 2^7)(2^{14} - 1) + (2^7 - 1)$

$2^{14} - 1 = 2^7(2^7 - 1) + (2^7 - 1) = NSD$

$= (2^7 + 1)(2^7 - 1)$

Bezoutova rovnost

$2^7 - 1 = (2^{35} - 1) + (2^{21} + 2^7)(2^{14} - 1)$

$= (2^{35} - 1) + (2^{21} + 2^7)[(2^{49} - 1) - 2^{14}(2^{35} - 1)]$

$$= \underbrace{(2^{21}+2^7)}_{k}(2^{49}-1) - \underbrace{(2^{35}+2^{21}-1)}_{\ell}(2^{35}-1)$$

Př. 1.5

(i) $a, b \in \mathbb{N}$, $a \neq b$. Ukažte, že existuje nekonečně mnoho čísel $n \in \mathbb{N}$ tak, že $a+n$, $b+n$ jsou nesoudělné.

- Zvolme n tak, že $a+n > b+n$ je provedeno.

Předpokládejme, že $a > b$

(ii) $n \in \mathbb{N}$, $n > 1$ má následující vlastnost: $\forall a, b \in \mathbb{N}$, $a \mid n$, $b \mid n$, $a > 1$, $b > 1$ platí, že $(a, b) > 1$

a, b soudělná

Pak může vzniknout p^k, p prvočíslo

↳ splňuje vlastnost výše

- Naopak: nechť platí vlastnost a spočteme předp. že $p \mid m, q \mid m$ pro prvočísla p, q

$\Rightarrow p = q$

1.6 i) m, n nesoudělné

$\Rightarrow m^2 + mn + n^2, m^2 - mn + n^2$ jsou nesoudělné

- Spočteme: předp. že ex. prvočíslo $p \geq 2$

$p \mid m^2 + mn + n^2 \wedge p \mid m^2 - mn + n^2$

$\Rightarrow p \mid 2mn$

- $p = 2 \Rightarrow m, n$ sudé, spor

- $p \mid m \Rightarrow p \mid m^2 \Rightarrow p \mid m$ spor
- $p \mid m$ . . . . .

- m, M nesoudělná čísla
$\Rightarrow m+2M, m^2+4M^2$ nesoudělná

Sporem: předp., že ex. prvo-
činitel p čísel $\geq$.

$p \mid m+2M$ a $p \mid m^2+4M^2$

$\Downarrow$

$p \mid m^2+4mM+4M^2$

$\Downarrow$

$p \mid 4mM$

- $p=2 \Rightarrow m$ sudé, spor
- $p \mid m \Rightarrow p \mid 2m$, spor
- $p \mid M \Rightarrow p \mid m$, spor