$n = p_1^{n_1} \cdots p_l^{n_l}$ $\quad n_j \geq 1$

$(m,n) = 1$ Každé nesoudělné ... p_i

3 7 11 15 19 23 ...

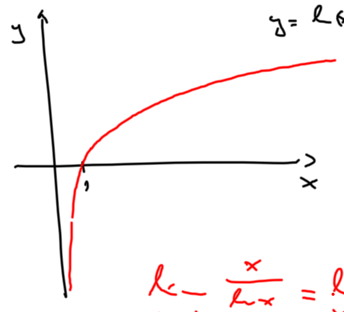
$p_1, p_2, \dots, p_N$ všechna prvočísla

$M = p_1 \cdots p_N + 1$ ... nemůže být prvočíslo

$\Rightarrow p_i \mid M$ a zároveň $p_i \mid M-1 \Rightarrow$ SPOR!

$(7,14) \ni 11, 13 \quad (30,60) \ni$

bře 5-14:06



$\ln'(x) = \frac{1}{x}$

$y = \ln(x)$

$\lim_{x\to\infty} \frac{x}{\ln x} = \lim_{x\to\infty} \frac{1}{\frac{1}{x}} = \infty$

$\sum_{p \text{ prvočíslo}} \frac{1}{p} = \infty$

bře 5-14:23

Aritmetické funkce:

$f: \mathbb{N} \to \mathbb{Z}$ (případně $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \dots$)

$\varphi(n)$ = počet nesoudělných čísel mezi 0 a n

n	φ
2	1
3	2
4	2
5	4
6	2
7	6
8	4
9	6

p prvočíslo $\varphi(p) = p-1$

$\varphi(p^\alpha) = p^{\alpha-1}(p-1)$

[1 2][3 4][5 6][7 8] $\quad 2 \cdot 1$

[1 2 3][4 5 6][7 8 9] $\quad 3 \cdot 2 = 6$

bře 5-14:31

$12 = 2 \cdot 2 \cdot 3$ $\quad$ 1 2 3 4 5 6 7 8 9 10 11 12

$\tau(12) = 3 \cdot 2 = 6$

$(p_1^0 + p_1^1 + \dots + p_1^{n_1})(p_2^0 + p_2^1 + \dots + p_2^{n_2}) \dots$

$= \frac{p_1^{n_1+1} - 1}{p_1 - 1}$

$\tau(n)$, $\sigma(n)$ multiplikativní!

$a = p_1^{n_1} \cdots p_k^{n_k}$ $\quad b = q_1^{m_1} \cdots q_l^{m_l}$ $\quad (a,b) = 1$

$a \cdot b = p_1^{n_1} \cdots p_k^{n_k} q_1^{m_1} \cdots q_l^{m_l}$ $\quad \tau(ab) = (n_1+1)\cdots(n_k+1)(m_1+1)\cdots(m_l+1)$ $= \tau(a)\tau(b)$

bře 5-14:45

$\forall n \in \mathbb{N} \quad \sum_{d \mid n} \varphi(d) = n$

1 2 3 4 5 6 7 8 9 10 11 12 / $\frac{1}{12}$

$\frac{1}{12}, \frac{1}{6}, \frac{1}{4}, \frac{1}{3}, \frac{5}{12}, \frac{1}{2}, \frac{7}{12}, \frac{2}{3}, \frac{3}{4}, \frac{5}{6}, \frac{11}{12}, 1$

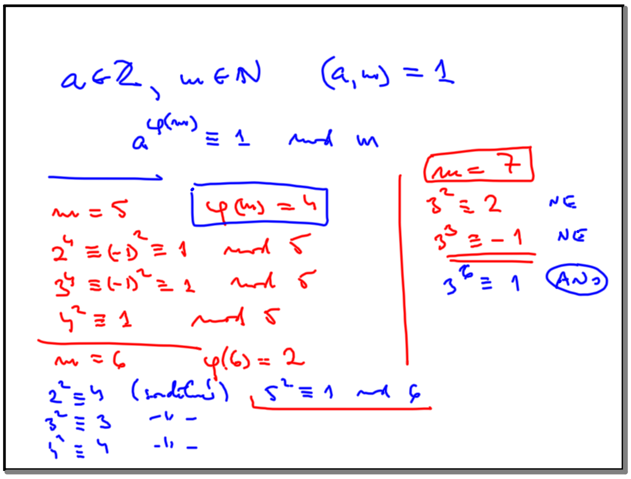
bře 5-15:05

$n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$

$\varphi(n) = p_1^{\alpha_1}\left(1 - \frac{1}{p_1}\right) p_2^{\alpha_2}\left(1 - \frac{1}{p_2}\right) \cdots$

$= p_1^{\alpha_1 - 1}(p_1 - 1) \cdot p_2^{\alpha_2 - 1}(p_2 - 1) \cdots$

bře 5-15:19


a ∈ ℤ, m ∈ ℕ (a, m) = 1
a^φ(m) ≡ 1 mod m
m = 5
φ(m) = 4
2^4 ≡ (-1)^2 ≡ 1 mod 5
3^4 ≡ (-1)^2 ≡ 1 mod 5
4^2 ≡ 1 mod 5
m = 6
φ(6) = 2
2^2 ≡ 4 (sudé čísla)
3^2 ≡ 3 -"-
4^2 ≡ 4 -"-
5^2 ≡ 1 mod 6
m = 7
3^2 ≡ 2 NE
3^3 ≡ -1 NE
3^6 ≡ 1 ANO

bře 5-15:28