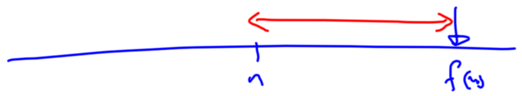
1, 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, ...

$p_1 \cdot p_2 \cdots p_k + 1 = N$



$[n, n!]$ $n > 2$ $p \mid (n! - 1)$

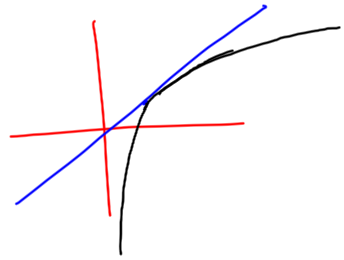
a) $p \leq n \Rightarrow p \mid n! \Rightarrow p \nmid (n! - 1)$

b) $p > n$

3 3-14:09

$$\underbrace{(n+1)!+2,\ (n+1)!+3,\ \ldots,\ (n+1)!+(n+1)}_{n \text{ čísel}}$$

$k = \{2, 3, \ldots, n+1\}$ $k \mid (n+1)! \Rightarrow k \mid (n+1)! + k$



3 3-14:23

$\tau(n)$ - počet dělitelů

$\sigma(n)$ - součet dělitelů

$\varphi(n)$ - počet čísel nesoudělných s n mezi 0 a n.

$\varphi(2) = 1$ $\varphi(4) = 2$

$\varphi(3) = 2$

$\mu(n)$

n ... dělitel $d \mid n$ $\sum_{d \mid n} \mu(d) = 0$

$\mu(6) = (-1)^2 = 1$

$$\boxed{\begin{array}{ll} \mu(3) = -1 & \mu(6) = 1 \\ \mu(2) = -1 & \mu(1) = 1 \end{array}}$$

$(1 + (-1))^k$

$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k}$

$(\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_k + 1) = \tau$

3 3-14:32

$(f \circ I)(n) = \sum_{d \mid n} I(d) f\left(\frac{n}{d}\right) = f(n)$

$(f \circ 1)(n) = \sum_{d \mid n} 1(d) f\left(\frac{n}{d}\right) = \sum_{d \mid n} \underbrace{1\left(\frac{n}{d}\right)}_{1} f(d) = \sum_{d \mid n} f(d)$

$F(n) = \sum_{d \mid n} f(d) = f \circ 1$

$\Rightarrow f(n) = F \circ \mu$

3 3-14:49

$\underbrace{n}_{F(n)} = \sum_{d \mid n} \varphi(d) \Rightarrow \varphi(n) = \sum_{d \mid n} \mu(d) \underbrace{\frac{n}{d}}_{F\left(\frac{n}{d}\right)}$

$\varphi(n) = n \cdot \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_k}\right)$

$n = p^\alpha$

$$\boxed{\begin{aligned} \varphi(n) &= p^\alpha \cdot \left(1 - \frac{1}{p}\right) \\ &= p^{\alpha - 1}(p - 1) \end{aligned}}$$

$\varphi(4) = 2 \cdot 1$

$\varphi(81) = 27 \cdot 2$

3 3-15:03

$p = 7$ $\{0, 1, 2, 3, 4, 5, 6\} = \mathbb{Z}_7$

$3^6 = 729 \equiv 1 \mod 7$

$\boxed{a^{p-1} \equiv 1}$ mod p $p \nmid a$

$\boxed{a^p \equiv a \mod p \quad \forall a}$

$\mathbb{Z}_7 = \{-3, -2, -1, 0, 1, 2, 3\}$

$n = 8$ $\boxed{3^2 \equiv 1 \equiv 5^2 \equiv 7^2 \mod 8}$

$\varphi(8) = \underline{\underline{4}}$

3 3-15:21

$(a^r)^s = a^{r \cdot s} \equiv 1 \pmod m$

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

$\boxed{a^n \equiv 1 \pmod m \iff r \mid n}$

3 3-15:39