

②

$$1234321 \stackrel{1234321}{\equiv} x \pmod{19} \quad (1234321, 19) = 1$$

felh. E-F TÉTEL
 $\varphi(19) = 18$

$$1234321 \equiv 5 \pmod{19}$$

$$1234321 \stackrel{1234321}{\equiv} y \pmod{18} \quad (1234321, 18) = 1 \rightarrow \text{E-F TÉTEL}$$

$$1234321 \equiv 7 \pmod{18}$$

$$\varphi(18) = (2-1)(3^2-3) = 6$$

$$1234321 \equiv 1 \pmod{6}$$

$$1234321 \stackrel{1234321}{\equiv} 5^{7^1} \pmod{19}$$

$$\stackrel{11}{5^7} = 78125 \equiv \underline{\underline{16}} \pmod{19}$$

1) $\varphi(n) = 2^k$

$$n = \prod p_i^{d_i}$$

$$\varphi(n) = \prod (p_i^{d_i} - p_i^{d_i-1}) = \underbrace{(p_1^{d_1} - p_1^{d_1-1}) \cdots (p_r^{d_r} - p_r^{d_r-1})}_{\text{minden tényező két-hatvány (a számelmélet alaptételétől függően)}} = 2^k$$

$$\rightarrow p_i^{d_i} - p_i^{d_i-1} = 2^l \quad l \geq 0 \quad l \in \mathbb{Z}$$

$$\underbrace{p_i^{d_i-1}}_{2^{e-m}} \underbrace{(p_i - 1)}_{2^m} = 2^e$$

I. $p_i = 2 \Rightarrow 2^{d_i-1} \cdot (2-1) = 2^{d_i-1} = 2^e$

II. $p_i^{d_i-1} = 1 \Leftrightarrow \begin{cases} d_i-1=0 \\ d_i=1 \end{cases}$

$$p_i - 1 = 2^l$$

$$p_i = 2^l + 1 \rightarrow \text{Fermat-prím: } 2^{2^l} + 1 \text{ alakú (} l \text{ z-hatvány)}$$

\Rightarrow n kanonikus alakjában minden tényező 2-hatvány vagy Fermat-prím

$$1. \left. \begin{aligned} f(n) + d(n) &= n+1 & f(n) &= \text{azon } k \text{ számok száma, melyekre } 1 \leq k \leq n \text{ és } (k, n) = 1 \\ d(n) &= \text{azon } k \text{ számok száma, melyekre } 1 \leq k \leq n \text{ és } (k, n) = k \end{aligned} \right\}$$

1 megkérhetően szerepel, a többi kám vagy csak az egyikben, vagy ha $(k, n) \neq 1$ és $(k, n) = k$, akkor egyikben sem. Itt nincs olyan k kám, melyet $L(k, n) = 1 = (k, n) = k \Leftrightarrow 1 = k = n$ egyikben sem szerepel, akkor ha az összeg pontos $n+1$, különben $f(n) + d(n) < n+1$

0. eset: $n=1$ $f(n) + d(n) = 1+1 = 2 \checkmark$

I. eset: $n=2^{\alpha}$ 2-hatvány $n=2^{\alpha}$ $f(n) = 2^{\alpha} - 2^{\alpha-1}$ $d(n) = \alpha + 1$ $2^{\alpha} - 2^{\alpha-1} + \alpha + 1 = 2^{\alpha-1} + \alpha + 1$
 $\alpha = 2^{\alpha-1} \Rightarrow \alpha = 1$ vagy $\alpha = 2$, ha $\alpha \geq 3$ akkor $2^{\alpha-1} > \alpha$, bic. teljes indukcióval: $\alpha = 3 : 2 = 4 > 3$
 ha $\alpha = m$ igaz, $\alpha + 1 = m+1$: $\alpha + 1 < \alpha + \alpha = 2 \cdot \alpha < 2 \cdot 2^{\alpha-1} = 2^{\alpha}$, ezért $\alpha > 1$
 $n=2$ vagy $n=4$ $f(2) + d(2) = 1 + 2 = 3 = 2 + 1 \checkmark$ $f(4) + d(4) = 2 + 3 = 5 = 4 + 1 \checkmark$

II. eset: n prím $f(n) = n-1$; $d(n) = 2 \Rightarrow f(n) + d(n) = n+1$ teljesül

III. eset: $n = p \cdot m$, ahol p páratlan prím. Ekkor $1 \leq k = 2m \leq n$ és $(k, n) = m \neq 1$, ezért nem lehet igaz az állítás.

Megoldások: n prím vagy $n=4$ vagy $n=1$.

(2) 100 rész, 100 ór
 d -edik ór eltölje az n -edik részt, ha $d \mid n$.
 Az n -edik részt $d(n)$ -szer tudja el.
 1. eltolás \rightarrow szinglik
 2. eltolás \rightarrow beszámít
 3. eltolás \rightarrow szinglik

\Rightarrow páratlan számú eltolás után lesz újra a cella

\Rightarrow Az n -edik rab hazamehet, ha $d(n)$ páratlan.

ha $n = \prod p_i^{a_i} \Rightarrow d(n) = \prod (a_i + 1)$

ha van olyan L_k , ami páratlan, akkor $L_k + 1$ páros

$\Rightarrow 2 \mid L_k + 1 \Rightarrow 2 \mid d(n) \downarrow$

$\Rightarrow n$ prímtényező felbontásában minden kitevő páros

$\Rightarrow n$ -edik rab hazamehet, ha n négyzetes szám

Ez úgy is belátható, hogy tudjuk, hogy n osztói párosokat

allosztja: $a \mid n \Rightarrow a \sim \frac{n}{a}$

Valójában az osztók száma csak akkor lehet páratlan, ha

van olyan " a ", aminek a párja önmaga:

$a = \frac{n}{a} \Rightarrow n = a^2$

\Downarrow
 n négyzetes szám

\Rightarrow Hazamehet: 1, 4, 9, 16, 25, 36, 49, 64, 81, 100 -as
 számú cellák rabjai.