Zadanie 9

Pokaż, że jeśli n i m są względnie pierwsze, to $\varphi(nm) = \varphi(n) \cdot \varphi(m)$

Najpierw udowodnię 2 lematy

Lemat 1: Dla dowolnych a, b, n zachodzi

$$(a \perp n) \wedge (a \equiv_n b) \Rightarrow (b \perp n)$$

Załóżmy nie wprost, że tak nie jest

$b = c \cdot k$

$n = d \cdot k \qquad k \neq 1$

Jeśli $b \equiv_n a$, to $b = a + r \cdot n$

$b = c \cdot k$

$ck = a + r \cdot n$

$a = ck - rn \qquad // \; n = dk$

$a = ck - rdk$

$a = k(c - rd)$

a skoro $n = dk$ to dostrzegamy do

sprzeczności

Lemat 2 Jeśli $(a \not\perp n) \wedge (a \equiv_n b)$, to $(b \not\perp n)$

Skoro $a \not\perp n$, to $a = ck$

$n = dk \qquad k \neq 1$

$a \equiv_n b$

$ck \equiv_n b$

$b = ck + r_n = ck + rdk = k(c + rd)$

$n = k(d)$

sprzeczność

Z tych lematów wynika, że dla a, b, n t. i. $a \equiv_n b$ zachodzi

$$(a \perp n) \Leftrightarrow (b \perp n)$$

Rozpatrzmy liczby od 1 do $n \cdot m$

Każdą można zapisać jako $k + ml$, $k \in \{1, 2, \dots, m\}$

$l \in \{0, 1, \dots, n-1\}$

Pokażę, że dla dowolnego k oraz $l_1 \neq l_2$

otrzymujemy $k + ml_1 \not\equiv_n k + ml_2$

Załóżmy nie wprost, że taka równość zachodzi

$$k + ml_1 \equiv_n k + ml_2$$

$$ml_1 \equiv_n ml_2$$

$$m(l_1 - l_2) \equiv_n 0$$

Skoro $n \perp m$ oraz $m(l_1 - l_2)$ jest wielokrotnością n, to

$(l_1 - l_2)$ jest wielokrotnością n

$$n > l_1 \geq l_2 \geq 0$$

$$n > l_1 - l_2 \geq 0$$

więc $l_1 = l_2$

Sprzeczność

Dla danego k oraz $l_1 \neq l_2$ mamy

$$k + ml_1 \not\equiv_n k + ml_2$$

takich liczb jest n, więc dla każdego n_1 t.ż. $0 \leq n_1 < n$

istnieje l t.ż.

$$n_1 \equiv_n k + ml$$

Niech $a = n_1$, $b = k + ml$,

$$a \equiv_n b$$

2 lematów $a \perp n \iff b \perp n$

Takich liczb a, że $a \perp n$, jest z definicji $\varphi(n)$

Zatem dla dowolnego k istnieje dokładnie $\varphi(n)$ liczb

postaci $k+ml$ t.z. $k+ml \perp n$

Liczby te się nie powtórzą, ponieważ każda z nich

daje inną resztę przy dzieleniu przez n

Zauważmy, że dla dowolnego k mamy

$$k+ml \equiv_m k$$

$$\underbrace{(k+ml \perp m)} \iff \underbrace{(k \perp m)}$$

Zatem dla $\varphi(m)$ takich k jest $\varphi(m)$

wartości k i dowolnego l.

powyższe równanie jest spełnione

Rozpatrując tylko takie k (jest ich $\varphi(m)$) że $k+ml \perp m$:

dla dowolnego takiego k jest dokładnie $\varphi(n)$ różnych l t.z.

$k+ml \perp n$

Łącząc powyższe jest dokładnie ~~$\varphi(m)$~~ $\varphi(n)\varphi(m)$ par k,l

t.z. $k+ml \perp nm$, czyli

$$\varphi(nm) = \varphi(n) \cdot \varphi(m)$$

$\varphi(p^k) = ?$

Oczywiście dla $b = pa$ $b \not\perp p^k$ bo

$$pa \not\perp p^k$$

$$1 \leq pa < p^k$$

$1 \leq p^a$ $\qquad$ $p^a < p^k$

$a > 0$ $\qquad$ $a < p^{k-1}$

czyli $\quad a \in \{1, 2, \dots, p^{k-1}\}$

$A = \{1, 2, \dots, p^{k-1} - 1\} \qquad |A| = p^{k-1} - 1$

Pokaże, że dla $b \neq pa$ $\quad (tj. \neg \exists_a \; b = pa)$

$b \perp p^k$. Jedynym dzielnikiem pierwszym p^k jest p. Skoro

~~Gdy~~ $p \nmid b$, to b oraz p^k nie posiadają żadnego wspólnego

dzielnika pierwszego, a zatem też żadnego wspólnego dzielnika poza 1

Mamy więc $\quad (b \neq pa) \Leftrightarrow (b \perp p^k)$

↑

takich b jest $(p^k - 1) - |A| = p^k - p^{k-1}$

$A \leq b < p^k$

$\varphi(p_1^{d_1} \cdot p_2^{d_2} \cdot \dots \cdot p_k^{d_k}) = ?$

Oczywiście dla $p_i, p_j \in \mathbb{P}$ t.i. $p_i \neq p_j$

$p_i^{\lambda_i} \perp p_j^{d_j}$

2 własności (. pierwszych $\quad p_i^{\lambda_i} \nmid p_j^{d_j} \Rightarrow p_i = p_j$

Zatem z $\varphi(nm) = \varphi(n)\varphi(m)$

$\varphi(p_1^{d_1} \cdot p_2^{d_2} \cdot \dots \cdot p_k^{d_k}) = \varphi(p_1^{d_1}) \varphi(p_2^{d_2}) \dots \varphi(p_k^{d_k})$ z własności $\varphi(p^k) = p^k - p^{k-1}$

$= (p_1^{d_1} - p_1^{d_1-1})(p_2^{d_2} - p_2^{d_2-1}) \dots (p_k^{d_k} - p_k^{d_k-1})$