LEMAT 1

m, n względnie pierwsze

Udowodnię, że $\mathbb{Z}_{mn}$ jest równoliczny z $\mathbb{Z}_m \times \mathbb{Z}_n$.

D: Zdefiniujmy bijekcję $f: \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$

1) f jest różnowartościowa.

dla każdego $a \in \mathbb{Z}_{mn} = \{0, 1, \dots, m(n-1)\}$

$f(a) = (c, d)$ gdzie $c \in \mathbb{Z}_m$ oraz $c \equiv a \pmod{m}$

oraz $d \equiv a \pmod{n}$.

Niech $f(a) = f(b)$. wtedy $a \equiv b \pmod{m}$ oraz

$a \equiv b \pmod{n}$. Z chińskiego tw. o resztach

$a \equiv b \pmod{mn}$. Ponieważ $a, b \in \mathbb{Z}_{mn}$ to

$a = b$. więc f jest różnowartościowa.

2) f jest 1-1: weźmy dowolne $(c, d) \in \mathbb{Z}_m \times \mathbb{Z}_n$

wtedy $c \in \mathbb{Z}_m$, $d \in \mathbb{Z}_n$ z def. funkcji

$\exists a$, $a \equiv c \pmod{m}$, $a \equiv d \pmod{n}$ zatem dla

dowolnego (c, d) istnieje takie a, że $f(a) = (c, d)$. więc f jest 1-1.