Es 1

Let $\mathbb{Z}_4 \times \mathbb{Z}_5 \to \mathbb{Z}_{20}$ be the isomorphism of CRT. Then

a) $f(x,y) = 5x + 16y$ ✓

b) $f(x,y) = 16x + 5y$

c) $f(x,y) = 13x + 8y$

d) $f(x,y) = 8x + 13y$

Solution: $f(a,b) = af(1,0) + bf(0,1)$

$$\begin{cases} x \equiv 1 \bmod 5 \\ x \equiv 0 \bmod 4 \end{cases} \Rightarrow x = 4y$$

$$4y \equiv 1 \bmod 5$$

$$y = 4$$

Es 2

How many solution does have this equation?

$x^2 \equiv 173 \bmod 291$

a) 3

b) 1

c) $\emptyset$ ✓

d) 4

e) 2

Solution: $291 = 3 \times 97$

$$\begin{cases} x^2 \equiv 2 \bmod 3 \\ x^2 \equiv 76 \bmod 97 \end{cases}$$

Check if they are quadratic residues

$2^{\frac{3-1}{2}} \equiv 1 \bmod 3$? NO

$\Rightarrow$ ZERO SOLUTIONS

Es 3

Find $x \in \mathbb{Z}_{401}$ such that

$x \cdot 56 \equiv 1 \bmod 401$
$5 \cdot x \equiv 308 \bmod 401$

Solution: find $56^{-1} \bmod 401$

$401 = 56 \times 7 + 9$
$56 = 9 \times 6 + 2$
$9 = 2 \times 4 + 1$
$2 = 1 \times 2 + 0$

$p_0 = 0$
$p_1 = 1$
$p_2 = 1 - 7 = 394$
$p_3 = 1 - 394 \times 6 = 43$
$p_4 = 394 - 43 \times 4 = 222$

$222 \cdot 5 = 1110 \equiv 308 \bmod 401$