Tut 10 solutions

1. $1764 = 225 \times 7 + 189$
$225 = 189 \times 1 + 36$
$189 = 36 \times 5 + 9$
$36 = 9 \times 4 + 0$ $\longrightarrow \gcd(1764, 225) = 9.$

Since $\gcd(1764, 225) \neq 1$, the multiplicative inverse of 225 (mod 1764) does not exist.

$1764 = 652 \times 2 + 514$
$652 = 514 \times 1 + 111$
$514 = 111 \times 4 + 70$
$111 = 70 \times 1 + 41$
$70 = 41 \times 1 + 29$
$41 = 29 \times 1 + 12$
$29 = 12 \times 2 + 5$
$12 = 5 \times 2 + 2$
$5 = 2 \times 2 + 1$
$2 = 1 \times 2 + 0$ $\longrightarrow \gcd(1764, 625) = 1.$

Since $\gcd(1764, 625) = 1$, the multiplicative inverse of 625 (mod 1764) exists:

$$1 = 5 - 2\times 2 = (1)5 + (-2)2$$

$$= 5 - 2(12 - 5\times 2) = (-2)12 + (5)5$$

$$= (-2)12 + 5(29 - 12\times 2) = (5)29 + (-12)12$$

$$= (5)29 - 12(41 - 29\times 1) = (-12)41 + (17)29$$

$$= (-12)41 + 17(70 - 41\times 1) = (17)70 + (-29)41$$

$$= (17)70 - 29(111 - 70\times 1) = (-29)111 + (46)70$$

$$= (-29)111 + 46(514 - 111\times 4) = (46)514 + (-213)111$$

$$= (46)514 - 213(625 - 514\times 1) = (-213)625 + (259)514$$

$$= (-213)625 + 259(1764 - 625\times 2) = (259)1764 + (-731)625$$

So, $1 = (259)1764 + (-731)625$

and therefore $1 \equiv (-731)\times 625 \pmod{1764}$.

It follows that the multiplicative inverse of 625 (mod 1764) is 1033.

2. Since $1764 = 2^2 \times 3^2 \times 7^2$,

$\phi(1764) = 1764\left(\frac{1}{2}\right)\left(\frac{2}{3}\right)\left(\frac{6}{7}\right) = 504$

Since 503 is prime, $\phi(503) = 502$.

3. Since $x \equiv 9 \pmod{14}$,

$x = 9 + 14k$ for some integer k.

Since $x \equiv 1 \pmod{15}$,

$1 \equiv 9 + 14k \pmod{15}$.

Therefore $-8 \equiv -k \pmod{15}$

and therefore $k = 8$, and so

$x = 9 + 14 \times 8 = 121$.

Now $121 \in \mathbb{Z}_{210}^*$,

$121 \equiv 9 \pmod{14}$ and $121 \equiv 1 \pmod{15}$.

4. Suppose that $a \equiv b \pmod{mn}$.

Then $a - b = cmn$ for some integer c.

Since $a - b = (cn)m$, $a \equiv b \pmod{m}$,

and since $a - b = (cm)n$, $a \equiv b \pmod{n}$.

Suppose $a \equiv b \pmod{m}$ and $a \equiv b \pmod{n}$.

Then $a - b = km$ for some integer k

and $a - b = ln$ for some integer l.

Therefore $km = ln$. Since $\gcd(m,n) = 1$,

it follows that n divides k, that is,

$k = cn$ for some integer c.

Therefore $a - b = cnm$, and

therefore $a \equiv b \pmod{mn}$. ∎