1. (*7 points*) Prove that the open intervals $(1, 3)$ and $(1, 4)$ have the same cardinality, by finding a bijective correspondence between the two sets. Show your work.

We will construct a function f such that

$f(1) = 1$, $f(3) = 4$,

Let $f(x) = kx + l$

$$f(1) = k + l = 1$$
$$f(3) = 3x + l = 4$$
$$-2x = -3$$
$$x = \frac{3}{2} \Rightarrow l = 1 - k = 1 - \frac{3}{2} = -\frac{1}{2}$$

$$\therefore \boxed{f(x) = \frac{3}{2}x - \frac{1}{2}}$$

<u>One-one</u>

Let $f(x_1) = f(x_2)$, $x_1, x_2 \in (1, 3)$

$\Rightarrow \frac{3}{2}x_1 - \cancel{\frac{1}{2}} = \frac{3}{2}x_2 - \cancel{\frac{1}{2}}$

$\Rightarrow x_1 = x_2$

$\therefore$ f is one-one.

$\therefore \boxed{\text{f is bijective}}$

<u>Onto</u>

Let $y \in (1, 4)$

$\Rightarrow y = \frac{3}{2}x - \frac{1}{2}$ for some $x \in \mathbb{R}$.

$\Rightarrow \frac{3}{2}x = y + \frac{1}{2}$

$\Rightarrow x = \frac{2}{3}\left(y + \frac{1}{2}\right)$

Now $1 < y < 4$

$\Rightarrow \frac{3}{2} < y + \frac{1}{2} < \frac{9}{2}$

$\Rightarrow \frac{2}{3} \cdot \frac{3}{2} < \frac{2}{3}\left(y + \frac{1}{2}\right) < \frac{2}{3} \cdot \frac{9}{2}$

$\Rightarrow 1 < \frac{2}{3}\left(y + \frac{1}{2}\right) < 3$

$\Rightarrow 1 < x < 3$

$\therefore x \in (1, 3)$ $\therefore f$ is <u>onto</u>

2. (a) (*7 points*) Using the **Euclidean Algorithm**, find the greatest common divisor (gcd) of

$$a = -1575 \quad \text{and} \quad b = 231.$$

Show your work.

$$-1575 = -7(231) + 42$$
$$231 = 5(42) + 21$$
$$42 = 2(\underbrace{21}_{\text{gcd}}) + 0$$

$$\therefore \boxed{\gcd(-1575, 231) = 21}$$

(b) Now use the **Extended Euclidean Algorithm** to write gcd(−1575, 231) as a linear combination of −1575 and 231. Show your work.

$$21 = 231 - 5(42)$$
$$= 231 - 5(-1575 + 7(231))$$
$$= 231 + 5(1575) - 35(231)$$
$$= 5(1575) - 34(231)$$

$$\boxed{21 = -5(-1575) - 34(231)}$$

3. (*6 points*) Show that a perfect square (an integer that is the square of another integer), always leaves a remainder of 0 or 1, when divided by 4. Show your work.

Any integer is of the form $4k, 4k+1, 4k+2$ or $4k+3$ for some $k \in \mathbb{Z}$.

Case 1 : $n = 4k$. $\Rightarrow n^2 = 16k^2 = 4(4k^2)$ which leaves a remainder 0.

Case 2 : $n = 4k+1 \Rightarrow n^2 = (4k+1)^2 = 16k^2 + 8k + 1$

$= 4\underbrace{(4k^2+2k)}_{\text{integer.}} + 1$

n^2 leaves a remainder of 1.

Case 3 : $n = 4k+2 \Rightarrow n^2 = (4k+2)^2 = 16k^2 + 16k + 4$

$= 4\underbrace{(4k^2 + 4k + 1)}_{\text{integer.}}$

n^2 leaves a remainder 0.

Case 4 : $n = 4k+3 \Rightarrow n^2 = (4k+3)^2 = 16k^2 + 24k + 9$

$= 16k^2 + 24k + 8 + 1$

$= 4\underbrace{(4k^2 + 6k + 2)}_{\text{integer.}} + 1$

n^2 leaves a remainder of 1.

$\therefore$ n^2 always leaves a remainder of 0 or 1 when divided by 4.

4. (a) (*6 points*) Write the prime decomposition of $a = 100$ and $b = 1176$.

$100 = 2 \cdot 50 = 2 \cdot 2 \cdot 25 = 2 \cdot 2 \cdot 5 \cdot 5 = \boxed{2^2 5^2}$

$1176 = 2 \cdot 588 = 2 \cdot 2 \cdot 294 = 2 \cdot 2 \cdot 2 \cdot 147$

$= 2 \cdot 2 \cdot 2 \cdot 3 \cdot 49$

$= 2 \cdot 2 \cdot 2 \cdot 3 \cdot 7 \cdot 7$

$= \boxed{2^3 \cdot 3 \cdot 7^2}$

(b) Using (a) find gcd(100, 1176) and lcm(100, 1176).

$\gcd(100, 176) = 2^{\min(2,3)} \cdot 3^{\min(0,1)} \cdot 5^{\min(2,0)} \cdot 7^{\min(0,2)}$

$= 2^2 \cdot 3^0 \cdot 5^0 \cdot 7^0$

$= \boxed{4}$

$\text{lcm}(100, 176) = 2^{\max(2,3)} \cdot 3^{\max(0,1)} \cdot 5^{\max(2,0)} \cdot 7^{\max(0,2)}$

$= 2^3 \cdot 3^1 \cdot 5^2 \cdot 7^2$

$= \boxed{29400}$

5. (*7 points*) Let $a, b \in \mathbb{Z}^+$ and p be a prime number. Suppose $\gcd(a, p^2) = p$, and $\gcd(b, p^3) = p^2$. Find $\gcd(ab, p^4)$ by giving justification. Show your work. (Hint: Use the prime decompositions of a and b and how it relates to the gcd of the two integers)

$\gcd(a, p^2) = p$

$\Rightarrow p \mid a$ and p is highest power of p that divides a.

$\therefore a = p\alpha$ where $p \nmid \alpha$.

$\gcd(b, p^3) = p^2$

$\Rightarrow p^2 \mid b$ and p^2 is the highest power of p that divides b.

$\Rightarrow b = p^2\beta$ where $p \nmid \beta$.

$\therefore ab = (p\alpha)(p^2\beta)$

$= p^3 \alpha\beta$

As $p \nmid \alpha\beta$ hence, p^3 is the highest power of p that divides ab.

$\therefore \boxed{\gcd(ab, p^4) = p^3}$

6. (*7 points*) Determine whether the following linear congruence has a solution. If so, solve it. Show your work.

$$5x \equiv 12 \pmod{23}$$

$\gcd(5, 23) = 1$
and $1 \mid 12$ so a solution exists which is unique.

$23 = 4(5) + 3$
$5 = 1(3) + 2$
$3 = 1(2) + 1$.
$2 = 2(1) + 0$

$1 = 3 - 2$
$= 3 - (5 - 3)$
$= 2(3) - 5$
$= 2(23 - 4(5)) - 5$
$1 = 2(23) - 9(5)$

$5x \equiv 12 \pmod{23}$ implies that $5x - 12 = 23y$ for some $y \in \mathbb{Z}$.
$\Rightarrow 5x - 23y = 12$ — (1)

We know $-9(5) + 2(23) = 1$
$\Rightarrow -9(5) - 2(-23) = 1$.
$\Rightarrow \underbrace{-108}_{x}(5) - \underbrace{24}_{y}(-23) = 12$

$\therefore$ $x = -108$ which solves equation (1)

$\therefore$ $x \equiv -108 \pmod{23}$
$x \equiv -16 \pmod{23}$
$\boxed{x \equiv 7 \pmod{23}}$