1. Find *all* solutions for the given linear diophantine equation, or state why solutions do not exist.

(a) $6x + 51y = 22$

(b) $38x + 14y = 4$

(a) No solution because $(6, 51) = 3$ and $3 \nmid 22$.
(b) Observe that $(38, 14) = 2$ and $2 \mid 4$, so there are solutions.

We first solve $38x + 14y = 2$. By the Euclidean algorithm,
$38 = 14 \cdot 2 + 10$
$14 = 10 \cdot 1 + 4$
$10 = 4 \cdot 2 + 2$
$4 = 2 \cdot 2 + 0.$

Starting with the second to last equation and working backwards,
$2 = 10 - 2 \cdot 4$
$2 = 10 - 2 \cdot (14 - 10) = 3 \cdot 10 - 2 \cdot 14$
$2 = 3 \cdot (38 - 2 \cdot 14) - 2 \cdot 14 = 3 \cdot 38 - 8 \cdot 14.$
Summary: $38(3) + 14(-8) = 2.$

Now multiplying both sides by 2, we get a solution to $38x + 14y = 4$.
$38(6) + 14(-16) = 4.$
Namely, the solution $x_0 = 6, y_0 = -16$.

The general solution to $38x + 14y = 4$ is given by $x = 6 + \frac{14}{(38,14)}t$, $y = -16 - \frac{38}{(38,14)}t$ for any $t \in \mathbb{Z}$.
That is, $x = 6 + 7t$, $y = -16 - 19t$ for any $t \in \mathbb{Z}$

2. (a) You are given two integers whose product is 272484 and whose gcd is 87. What is the lcm of the two integers?

(b) Find the gcd and lcm of p^2q^3 and pqr, where p, q, r are distinct prime numbers.

(a) Let the two integers be a and b. We have $[a, b] = \frac{ab}{(a,b)} = \frac{272484}{87} = 3132.$

(b) $[p^2q^3, pqr] = p^2q^3r$, $(p^2q^3, pqr) = pq$.

3. Every integer n equals $4k + r$ for some $k, r \in \mathbb{Z}$ with $0 \le r < 4$. We know this by division by 4.

(a) List the first ten primes of the form $4k + 1$ for some $k \in \mathbb{Z}$. I will start you off: $5, 13, 17, \ldots$

(b) List the first ten primes of the form $4k + 3$ for some $k \in \mathbb{Z}$. I will start you off: $3, 7, 11, \ldots$

(c) Are there any primes of the form $4k$ for some $k \in \mathbb{Z}$?

(d) Are there any primes of the form $4k + 2$ for some $k \in \mathbb{Z}$?

(a) $5, 13, 17, 29, 37, 41, 53, 61, 73, 89$

(b) $3, 7, 11, 19, 23, 31, 43, 47, 59, 67$

(c) No, because $4k$ is always divisible by 4.

(d) Yes, the prime 2.
$4k+2$ is always even. Apart from 2, this is never a prime.

4. Prove that $\sqrt[3]{7}$ is irrational.

Suppose, for a contradiction that $\sqrt[3]{7} = \frac{a}{b}$, for some positive integers a and b with $(a,b) = 1$.
This implies $7b^3 = a^3$.
Suppose $p|b$ for some prime p. By the equation $7b^3 = a^3$, we get that $p|a^3$. Then by Euclid's Lemma, p must divide a. But this contradicts the assumption $(a,b) = 1$. So there must be no prime p dividing b. But the only way that can be true is if $b = 1$.
If $b = 1$, then $\sqrt[3]{7} = \frac{a}{1} = a \in \mathbb{Z}$. This is a contradiction because the cube of an integer cannot equal 7.

5. Let $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ be the prime factorization of a positive integer n, where $e_k \geq 1$.

We saw in class that every positive divisor d of n must have prime factorization $d = p_1^{f_1} p_2^{f_2} \cdots p_k^{f_k}$ for $0 \leq f_k \leq e_k$.

Find a formula for the *number of positive divisors* of n, in terms of $e_1, e_2, \ldots e_k$.

Hint: The number of possibilities for f_1 is $e_1 + 1$, because f_1 could be $0, 1, 2, \ldots,$ or e_1. Find the number of possibilities for each power f_i. Use this to find the total number of possibilities for d.

The number of possibilities for f_1 is $e_1 + 1$, because f_1 could be $0, 1, 2, \ldots,$ or e_1. The number of possibilities for f_2 is $e_2 + 1$. And so on. So the total number of possible divisors is

$$(e_1 + 1)(e_2 + 1) \cdots (e_k + 1)$$

6. Let a and b be positive integers. Prove that if $(a,b) = 1$, then $(a^2, b^2) = 1$.

Let $a = p_1^{e_1} \cdots p_k^{e_k}$ and $b = q_1^{f_1} \cdots q_l^{f_l}$ be the prime factorizations of a and b. Since a and b are coprime, they do not have any prime factor in common (i.e. $p_i \neq q_j$ for every $1 \leq i \leq k$ and $1 \leq j \leq l$).
Squaring, we get $a^2 = p_1^{2e_1} \cdots p_k^{2e_k}$ and $b^2 = q_1^{2f_1} \cdots q_l^{2f_l}$, the prime factorizations of a^2 and b^2. Since the primes in the two factorizations have not changed, there is no prime factor in common, so $(a^2, b^2) = 1$.

Another way to say the same thing:
Suppose that a^2 and b^2 were not coprime. Then we would have $p|a^2$ and $p|b^2$ for some prime p.
$p|a^2 \implies p|a$ by Euclid's lemma. $p|b^2 \implies p|b$ by Euclid's lemma.
So a common prime factor of a^2 and b^2 is also a common prime factor of a and b, which contradicts the condition $(a,b) = 1$. Therefore, a^2 and b^2 can have no common prime factor. This implies they have no common factor greater than 1.