1. Let a, b, c be integers such that a and b are not zero.

Prove that if $a|b$ and $b|c$ then $a|c$.

We are given that $a|b$ and $b|c$. So $b = ak$ and $c = bj$ for some $k, j \in \mathbb{Z}$. Thus

$$c = bj = (ak)j = a(kj).$$

This implies that $a|c$, since $kj \in \mathbb{Z}$.

2. Given any two *odd* integers n and m, prove that $n^2 + m^2$ cannot be a perfect square.

First, observe that for any odd integer n, we have that n^2 equals $4q+1$ for some $q \in \mathbb{Z}$. This is because if n is odd, then $n = 2k+1$ for some $k \in \mathbb{Z}$, which implies $n^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 4(k^2 + k) + 1$.

Given any two odd integers n and m, we have that $n^2 + m^2$ is equal to

$$(4q_1 + 1) + (4q_2 + 1) = 4(q_1 + q_2) + 2.$$

Thus $n^2 + m^2$ is always of the form $4q + 2$ for some $q \in \mathbb{Z}$. We saw in class that squares can only be of the form $4q$ or $4q + 1$. Thus $n^2 + m^2$ cannot be a square (remainders when dividing by 4 are unique, so $n^2 + m^2$ cannot be of the form $4q+2$ as well as another form).

3. (a) Use the Euclidean algorithm to show that $(514, 159) = 1$.

(b) Run the Euclidean algorithm backwards to find one pair of integers x and y such that

$$514x + 159y = 1.$$

(c) Use your answer in part (b) to find one pair of integers x and y such that

$$514x + 159y = 100.$$

(d) Find a pair of integers x and y, *different* from the integers you found in part (b), such that

$$514x + 159y = 1.$$

(a)

I. $514 = 3 \cdot 159 + 37$

II. $159 = 37 \cdot 4 + 11$

III. $37 = 11 \cdot 3 + 4$

IV. $11 = 4 \cdot 2 + 3$

V. $4 = 3 \cdot 1 + 1$

VI. $3 = 1 \cdot 3 + 0.$

Therefore, $(514, 159) = (159, 37) = (37, 11) = (11, 4) = (4, 3) = (3, 1) = (1, 0) = 1.$

(b)

$1 = 4 - 3$ (by using equation V)

$1 = 4 - (11 - 2 \cdot 4) = -11 + 3 \cdot 4$ (by equation IV)

$1 = -11 + 3 \cdot (37 - 3 \cdot 11) = 3 \cdot 37 - 10 \cdot 11$ (by equation III)

$1 = 3 \cdot 37 - 10(159 - 4 \cdot 37) = -10 \cdot 159 + 43 \cdot 37$ (by equation II)

$1 = -10 \cdot 159 + 43(514 - 3 \cdot 159) = 43 \cdot 514 - 139 \cdot 159$ (by equation I).

Conclusion: $x = 43, y = -139$.

(c) Take the equation $43 \cdot 514 - 139 \cdot 159 = 1$ from part (b) and multiply through by 100.
Then $4300 \cdot 514 - 13900 \cdot 159 = 10$. So $x = 4300, y = -13900$.

(d) Take the equation $43 \cdot 514 - 139 \cdot 159 = 1$ from part (b) and add on the number $-159 \cdot 514 + 514 \cdot 159 = 0$. Then

$$(43 - 159) \cdot 514 + (-139 + 514) \cdot 159 = 1.$$

So $x = 43 - 159, y = -139 + 514$. Other answers are possible.

4. Let n and m be two integers. Prove that any common divisor of n and m also divides (n, m).

Hint: Use the fact that (n, m) can be written as the linear combination of n and m.

$\exists x, y \in \mathbb{Z}$ such that $nx + my = (n, m)$.
A common divisor of n and m divides both n and m. If $d|n$ and $d|m$ then $n = dq_1,\ m = dq_2$ for some $q_1, q_2 \in \mathbb{Z}$. So $nx+my = (dq_1)x+(dq_2)y = d(q_1x+q_2y)$. Thus d divides $nx + my$. But $nx + my$ equals (n, m). So $d|(n, m)$.

5. Let n and m be two positive integers. Suppose that $n \leq m$ and $n|(m! + 1)$. Prove that $n = 1$.

Hint: Recall that $m! = m \cdot (m - 1) \cdot (m - 2) \cdots 2 \cdot 1$. First, explain why $n \leq m$ implies that $n|m!$. Next, bring into play the assumption $n|(m! + 1)$. What do $n|m!$ and $n|(m! + 1)$ imply?

We are given that $n \leq m$. This implies that n divides $m!$ (because $m!$ is the product of all integers between 1 and m and n is one of these integers). We are also given that n divides $m! + 1$. Therefore n must divide the difference of these two numbers:

$$n|m! \text{ and } n|(m! + 1) \implies n|(m! + 1 - m!) \implies n|1.$$

The only possible value for n is therefore $n = 1$.

Bonus

6. Let n be a positive integer. Use the Euclidean algorithm to find $(4n^2+1, 2n+1)$.

Hint: Polynomial division will enable you to divide $4x^2 + 1$ by $2x + 1$, etc.

Division of $4n^2 + 1$ by $2n + 1$ gives:

$4n^2 + 1 = (2n + 1) \cdot (2n - 1) + 2 \qquad$ (remainder=2).

Thus $(4n^2 + 1, 2n + 1) = (2n + 1, 2)$.
Division of $2n + 1$ by 2 gives:

$2n + 1 = 2 \cdot n + 1 \qquad$ (remainder=1).

Thus $(2n + 1, 2) = (2, 1)$.
Division of 2 by 1 gives:

$2 = 1 \cdot 2 + 0 \qquad$ (remainder=0).

Thus $(2, 1) = (1, 0) = 1$.

So $(4n^2 + 1, 2n + 1) = (2n + 1, 2) = (2, 1) = (1, 0) = 1$.