1. Prove that 7 is the only prime number that precedes a perfect cube. A perfect cube is a number x ∈ N such that there exists n ∈ N and x = n^3. Rewrite the statement using an implication and prove the statement's correctness.

Let P(x) be x is prime.

$$\forall x \in N, \forall n \in N, (P(x) \wedge (x = n^3 - 1)) \rightarrow (x = 7)$$

$$x = n^3 - 1 = (n-1)(n^2 + n + 1)$$

For x to be prime, one of the factors must be equal to 1:

Let n - 1 = 1, therefore n = 2

If n = 2, $(n^2 + n + 1) = 7$

Therefore x = 7 ■

2. A Test for Primality is the following:

   Given an integer n > 1, to test whether n is prime check to see if it is divisible by a prime number less than or equal to its square root. If it is not divisible by any of these numbers then it is prime.

   We will show that this is a valid test.

   a) $\forall n, r, s \in N^+, rs \leq n \rightarrow (r \leq \sqrt{n} \vee s \leq \sqrt{n})$

Contrapositive: $\forall n, r, s \in N^+, (r > \sqrt{n} \wedge s > \sqrt{n}) \rightarrow rs > n$

$$(r > \sqrt{n} \wedge s > \sqrt{n}) \rightarrow rs > \sqrt{n}\sqrt{n} = n$$

   b) $\forall n \in N^{>1}, n \text{ is not prime} \rightarrow \exists p \in N, (p \text{ prime} \wedge (p \leq \sqrt{n}) \wedge p \mid n)$

By the fundamental theorem of arithmetic, all positive non-prime integers can be expressed as a product of primes: this satisfies p is prime and p | n.

Let n = xy, where x and y are integer factors of n.

Let $x \leq y$:

Suppose $x > \sqrt{n}$:

Then: $y \geq x > \sqrt{n}$ and $y > \sqrt{n}$

Which means $yx > \sqrt{n}\sqrt{n} = n$

This contradicts n = xy

Therefore $x \leq \sqrt{n}$ ■

   c) State the contrapositive of the statement of part (b).

$$\forall p \in N, (p \text{ is not prime} \vee (p > \sqrt{n}) \vee p \nmid n) \rightarrow \exists n \in N^+, n \text{ prime}$$

3. Prove that for all natural numbers n, n is either a perfect square or the square root of n is irrational.

$$\forall n \in N, (\sqrt{n} \in N) \vee (\sqrt{n} \notin Q)$$

Assume to the contrary that $\sqrt{n} \in Q$, where n is not a perfect square:

$\sqrt{n} = \frac{p}{q}$ $p, q \in N, q \neq 0$, where $\frac{p}{q}$ is in its most simplified form.

$n = \frac{p^2}{q^2}$

q also cannot be equal to one, as that would make $\sqrt{n}$ an integer, which means it is a perfect square.

Because q^2 cannot be equal to 1, and $\frac{p}{q}$ is in its lowest form, n is not an integer.

This contradicts that n is an element of natural numbers.
Therefore $\sqrt{n} \notin Q$ ■

4. The greatest common divisor c, of a and b, denoted as c = gcd(a, b), is the largest number that divides both a and b. One way to write c is as a linear combination of a and b. Then c is the smallest natural number such that c = ax+by for x, y ∈ Z. We say that a and b are relatively prime iff gcd(a, b) = 1. Prove that a and n are relatively prime if and only if there exists integer s such that sa $\equiv_n$ 1. We call s the inverse of a modulo n.

$(sa) mod n = 1 mod n$
$sa = nq_1 + r$
$1 = nq_2 + r$
$sa - nq_1 = 1 - nq_2$

Prove $\gcd(a, n) = 1 \leftrightarrow$ sa $\equiv_n 1$

Prove: $\gcd(a, n) = 1 \rightarrow$ sa $\equiv_n 1$
Contrapositive: sa$/\equiv_n 1 \rightarrow \gcd(a, n) \neq 1$
$\gcd(a, n) \neq 1 \leftrightarrow 1 \neq \mathrm{ax} + \mathrm{ny}, \quad \mathrm{x}, \mathrm{y} \in \mathrm{Z}$

$(sa) mod n = 1 mod n$
$sa = nq_1 + r$
$1 = nq_2 + r \qquad s, q_1, q_2 \in Z$
$sa - nq_1 \neq 1 - nq_2$
$1 \neq sa + nq_2 - nq_1$
$1 \neq sa + n(q_2 - q_1)$ Let s = x and $(q_2 - q_1)$ = y, because the difference between arbitrary integers is an integer.
$1 \neq ax + ny$

Prove: sa $\equiv_n 1 \rightarrow \gcd(a, n) = 1$
$\gcd(a, n) = 1 \leftrightarrow 1 = \mathrm{ax} + \mathrm{ny}, \quad \mathrm{x}, \mathrm{y} \in \mathrm{Z}$

$(sa) mod n = 1 mod n$
$sa = nq_1 + r$
$1 = nq_2 + r \qquad s, q_1, q_2 \in Z$
$sa - nq_1 = 1 - nq_2$
$1 = sa + nq_2 - nq_1$
$1 = sa + n(q_2 - q_1)$ Let s = x and $(q_2 - q_1)$ = y, because the difference between arbitrary integers is an integer.
$1 = ax + ny$ ■

5. Use simple induction to prove that for all n ≥ 1, $\sum_{i=1}^{n} i(i!) = (n + 1)! - 1$.

Base case, n = 1:
(1+1)! – 1 = 1
$$\sum_{i=1}^{1} i(i!) = 1(1!) = 1$$
Assume S(k) is true for some k ≥ 1
S(k): $\sum_{i=1}^{k} i(i!) = (k+1)! - 1$
Induction step, prove: S(k+1) = (k + 2)! – 1

$$\mathrm{S(k+1)} = \sum_{i=1}^{k+1} i(i!)$$
$$\mathrm{S(k+1)} = \mathrm{(k+1)(k+1)!} + \sum_{i=1}^{k} i(i!)$$
$$\mathrm{S(k+1)} = \mathrm{(k+1)(k+1)!} + (k+1)! - 1$$
$$\mathrm{S(k+1)} = (k+1)!\,(k+1+1) - 1$$
$$\mathrm{S(k+1)} = (k+1)!\,(k+2) - 1$$
$$\mathrm{S(k+1)} = (k+2)! - 1$$

■

6. Suppose that n girls and n boys are distributed around the outside of a circular table. Use mathematical induction to prove that for any integer n ≥ 1, given any such seating plan, it is always possible to find a starting point so that if travel around the table in a clockwise direction the number of girls you pass is never less than the number of boys you have passed. For example, in the diagram below, we use g to denote a girl and b to denote a boy, you should start at the girl in red.

Base case, n = 1:
The only possible orders are gb or bg, in which gb satisfies that the number of g will always be greater than or equal to the number of b's passed.

Hypothesis:
Let S(k) be that there is starting point which the number of g's is always greater than or equal to the number of b's for some k ≥ 1 for which there are k number of b's and k number of g's.

Induction:
Prove S(k+1)

This means there is one more g and b in the circle. Because you need to pass all b's and g's in the circle, there must be, at some point, a g preceding a b. If we take these out, we have the case of S(k) which is true because of the induction hypothesis. If you add back the g preceding a b, then S(k+1) is true, as no matter what S(k) is, adding a g preceding a b will not change the starting point as the increase in the number of b's passed is the same as the number g's passed.

■