1. Prove there are an infinite number of primes.

Proof. (by contradiction) Suppose there are a finite number of primes, say $p_1, p_2, \ldots, p_k$. Let $N = p_1 p_2 \cdots p_k + 1$. The number N is either prime or composite.

If N is prime, then we have the contradiction that there are only k primes and there are $k+1$ primes.

Now suppose that N is composite. Thus, N is divisible by at least one of the k primes, $p_1, p_2, \ldots, p_k$, say p_i. So there exists some integer ℓ such that $N = p_i \ell$.

But now the expression $N = p_1 p_2 \cdots p_k + 1$ can be rewritten as

$$1 = N - p_1 p_2 \cdots p_k = p_i(\ell - p_1 p_2 \cdots p_{i-1} p_{i+1} \cdots p_k),$$

which implies that the prime p_i divides 1, a contradiction. □

2. Prove that any two rational numbers x and y can be written in the form $x = \frac{a}{n}$ and $y = \frac{b}{n}$ such that $\gcd(a,b,n) = 1$ but that it is not possible to conclude that $\gcd(a,n) = 1$ or $\gcd(b,n) = 1$.

Informal proof: We know any two rational number can be written as ratios of integers so $x = a/c$ and $y = b/d$ for $a,b,c,d \in \mathbb{Z}$ is possible. Given these ratios, we can find a common denominator, say cd to obtain $x = ad/cd$ and $y = bc/cd$. Let's now simply this to $x = a/n$ and $y = b/n$ (and yes I am overusing the variables a and b.)

Given the integers a,b,n, if they have a common divisor then we can cancel it from all three and still have ratios equal to x and y. So it is possible to suppose that $\gcd(a,b,n) = 1$.

On the other hand, if $x = 9/2$ and $y = 4/3$, then the least common denominator is 6 which would give use $x = 27/6$ and $y = 8/6$ neither or which is in lowest terms. So this is not guaranteed.

3. Statements about even and odd numbers could be rewritten in the language of integers modulo 2. For example, the statement:

$\boxed{\text{If } n \text{ is odd, then } n^2 \text{ is odd}}$ could be rewritten as $\boxed{\text{If } n \equiv 1 \pmod 2\text{, then } n^2 \equiv 1 \pmod 2.}$

Make **conjectures** about what happens when you consider the squares of integers modulo 3 and then prove that you are correct.

Proposition If $n \equiv_3 0$, then $n^2 \equiv_3 0$. If $n \equiv_3 1$ or $n \equiv_3 2$, then $n^2 \equiv_3 1$. (By implication, it is not possible for the square of any integer to be congruent to 2 mod 2.

Informal sketch of proof: For $n = 3k$, $n^2 = 9k^2 = 3(3k^2)$.
For $n = 3k+1$, $n^2 = 9k^2 + 6k + 1 = 3(3k^2 + 2k) + 1$.
For $n = 3k+2$, $n^2 = 9k^2 + 12k + 4 = 3(3k^2 + 4k + 1) + 1$.

4. Make a conjecture about when the sum of two integers can be congruent to 0 modulo 3 and prove that you are correct. Your proposition will look something like the one below:

   Proposition: Let $a,b \in \mathbb{Z}$ such that $a+b \equiv 0 \pmod 3$, then either both are congruent to zero modulo 3 or one is congruent to 1 and the other is congruent to 2.

   Informal sketch of proof: While it's clear that $3k+3\ell \equiv_3 0$ and that $(3k+1)+3\ell+2 \equiv_3 0$, this is not sufficient. We would need to show that no other combinations can be congruent to zero. There are four more. This argument is basically proof by 6 cases.

5. Describe the set of points in the xy-plane that satisfy $x^2+y^2-3=0$.

   It's a circle in the plane with center at the origin and a radius of $\sqrt{3}$.

6. Prove that $x^2+y^2-3=0$ contains no rational points.

   Proof. (by contradiction) Suppose that there exist $(x,y) \in \mathbb{Q} \times \mathbb{Q}$ such that $x^2+y^2-3 \neq 0$. By #2, we can write $x = a/n$ and $y = b/n$ where $\gcd(a,b,n) = 1$. Plugging into the equation we obtain

   $$\frac{a^2}{n^2} + \frac{b^2}{n^2} - 3 = 0.$$

   This is equivalent to $a^2+b^2 = 3n^2$.

   Now, we can conclude that $a^2+b^2 \equiv_3 0$. Using our result in #4, either both a^2 and b^2 are congruent to 0 modulo 3 or one is congruent to 1 and the other to 2. But our result in #3 implies that neither a^2 nor b^2 can be congruent to 2. So we are left with only one possibility – that both a^2 and b^2 are congruent to zero. Using #3 again, we conclude that $a = 3k$ and $b = 3\ell$.

   Now, $3n^2 = 9k^2+9\ell^2 = 3(3k^2+3\ell^2)$ which upon division by 3 gives $n^2 = 3k^2+3\ell^2 = 3(k^2+\ell^2.)$ Thus, we conclude that n is also a multiple of 3.

   Finally we have a contradiction that $\gcd(a,b,n) = 1$ and $\gcd(a,b,n) \geq 3$. □