Numbers of various sorts

Exercises

1. Prove the following formulas by induction.

(i) $1^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$

Proof. Let $n = 1$. Then $\frac{1(2)(3)}{6} = 1$, so the formula holds. Now assume that the formula is true for some $k \in N$. Then

$$\begin{aligned} 1^2 + \cdots + (k+1)^2 &= 1^2 + \cdots + k^2 + (k+1)^2 = \frac{k(k+1)(2k+1)}{6} + (k+1)^2 \\ &= \frac{k(k+1)(2k+1) + 6(k+1)^2}{6} = \frac{2k^3 + 9k^2 + 13k + 6}{6} \\ &= \frac{(k+1)(k+2)(2(k+1)+1)}{6} \end{aligned}$$

□

(ii) $1^3 + \cdots + n^3 = (1 + \cdots + n)^2$

Proof. Let $n = 1$. Then $1^3 = 1^2$, so the formula holds. Now assume that the formula is true for some $k \in N$. Then

$$\begin{aligned} 1^3 + \cdots + (k+1)^3 &= (1^3 + \cdots + k^3) + (k+1)^3 = (1 + \cdots + k)^2 + (k+1)^3 \\ &= (1 + \cdots + k)^2 + (k+1)^2(k+1) = (1 + \cdots + k)^2 + k(k+1)^2 + (k+1)^2 \\ &= (1 + \cdots + k)^2 + 2\frac{k(k+1)}{2}(k+1) + (k+1)^2 \\ &= (1 + \cdots + k)^2 + 2(1 + \cdots + k)(k+1) + (k+1)^2 \\ &= (1 + \cdots + (k+1))^2 \end{aligned}$$

□

2. Find a formula for

(i) $\sum_{i=1}^{n}(2i-1) = 1 + 3 + 5 + \cdots + (2n-1)$

Proof.

$$\begin{aligned} \sum_{i=1}^{n}(2i-1) &= 1 + 2 + \cdots + 2n - 2(1 + 2 + \cdots + n) = \frac{2n(2n+1)}{2} - 2\frac{n(n+1)}{2} \\ &= n(2n+1) - n(n+1) = 2n^2 + n - n^2 - n = n^2. \end{aligned}$$

□

(ii) $\sum_{i=1}^{n}(2i-1)^2 = 1^2 + 3^2 + 5^2 + \cdots + (2n-1)^2$

Proof.

$$\sum_{i=1}^{n}(2i-1)^2 = 1^2+2^2+\cdots+(2n)^2 - 4(1^2+2^2+\cdots+n^2) = \frac{2n(2n+1)(4n+1)}{6} - 4\frac{n(n+1)(2n+1)}{6}$$
$$= \frac{8n^3-2n}{6} = \frac{2n(2n-1)(2n+1)}{6}$$

□

3. If $0 \le k \le n$, the "binomial coefficient" $\binom{n}{k}$ is defined by

$$\binom{n}{k} = \frac{n!}{k!(n-k)!} = \frac{n(n-1)\dots(n-k+1)}{k!}\textbf{, if } k \neq 0, n$$

$$\binom{n}{0} = \binom{n}{n} = 1 \textbf{ (a special case of the first formula if we define 0! = 1)},$$

and for $k < 0$ or $k > n$ we just define the binomial coefficient to be 0.

(a) Prove that

$$\binom{n+1}{k} = \binom{n}{k-1} + \binom{n}{k}$$

Proof.

$$\binom{n}{k-1} + \binom{n}{k} = \frac{n!}{(k-1)!(n-(k-1))!} + \frac{n!}{k!(n-k)!} = \frac{kn!}{k!(n+1-k)!} + \frac{(n+1-k)n!}{k!(n+1-k)!}$$
$$= \frac{n!(k+n+1-k)}{k!(n+1-k)!} = \frac{(n+1)!}{k!(n+1-k)!} = \binom{n+1}{k}$$

□

(b) Notice that all the numbers in Pascal's triangle are natural numbers. Use part (a) to prove by induction that $\binom{n}{k}$ is always a natural number.

Proof. Let $n = 1$. Then $\binom{1}{0} = 1$ and $\binom{1}{1} = 1$, so the binomial coefficient is always a natural number. Next, suppose that for some number n, and $0 \le k \le n$, $\binom{n}{k}$ is always a natural number. Then if $k = 0$ or $k = n+1$, then $\binom{n+1}{k} = 1$, which is a natural number. Otherwise,

$$\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1}, \text{ and } 1 \le k \le n, 0 \le k-1 \le n-1,$$

so $\binom{n+1}{k}$ is a sum of two natural numbers, and is therefore also a natural number. □

(c) Give another proof that $\binom{n}{k}$ is a natural number by showing that $\binom{n}{k}$ is the number of sets of exactly k integers chosen from $1, \dots, n$.

Proof. The number of k-tuples of integers chosen from $1, \dots, n$ is $n(n-1)\dots(n-k+1)$, because there is n choices for the first element, $n-1$ choices for the second, etc. Now, for each k-tuple, it can be arranged in $k(k-1)\dots(1) = k!$ different ways, so to get the number of sets of size k, with elements chosen from $1, \dots, n$, we have $\frac{n(n-1)\dots(n-k+1)}{k!} = \binom{n}{k}$. □

(d) Prove the "binomial theorem": If a and b are any numbers and n is a natural number, then

$$\begin{aligned}(a+b)^n &= a^n + \binom{n}{1}a^{n-1}b + \binom{n}{2}a^{n-2}b^2 + \cdots + \binom{n}{n-1}ab^{n-1} + b^n \\ &= \sum_{j=0}^{n}\binom{n}{j}a^{n-j}b^j.\end{aligned}$$

Proof. Let $n = 1$. Then

$$(a+b)^1 = a + b = a^1 + b^1 = \sum_{j=0}^{1}\binom{n}{j}a^{n-j}b^j,$$

so the statement holds true.

Next, suppose that the statement is true for some $n \geq 1$. Then

$$\begin{aligned}(a+b)^{n+1} &= (a+b)(a+b)^n = (a+b)\sum_{j=0}^{n}\binom{n}{j}a^{n-j}b^j \\ &= \sum_{j=0}^{n}\binom{n}{j}a^{n+1-j}b^j + \sum_{j=0}^{n}\binom{n}{j}a^{n-j}b^{j+1} \\ &= \sum_{j=0}^{n}\binom{n}{j}a^{n+1-j}b^j + \sum_{j=1}^{n+1}\binom{n}{j-1}a^{n+1-j}b^j \\ &= a^{n+1} + \sum_{j=1}^{n}(\binom{n}{j} + \binom{n}{j-1})a^{n+1-j}b^j + b^{n+1} \\ &= a^{n+1} + \sum_{j=1}^{n}\binom{n+1}{j}a^{n+1-j}b^j + b^{n+1} \\ &= \sum_{j=0}^{n+1}a^{n+1-j}b^j.\end{aligned}$$

□

(e) Prove that

(i)

$$\sum_{j=0}^{n}\binom{n}{j} = \binom{n}{0} + \cdots + \binom{n}{n} = 2^n$$

Proof. Let $n = 1$. Then

$$\sum_{j=0}^{n}\binom{n}{j} = 1 + 1 = 2 = 2^1,$$

so the formula holds.

Next, suppose that for some $n \geq 1$, $\sum_{j=0}^{n} = 2^n$. Then

$$\sum_{j=0}^{n+1} \binom{n+1}{j} = \sum_{j=0}^{n+1} \left(\binom{n}{j} + \binom{n}{j-1} \right) = \binom{n}{0} + \sum_{j=1}^{n} \binom{n}{j} + \sum_{j=1}^{n} \binom{n}{j-1} + \binom{n}{n}$$
$$= \sum_{j=0}^{n} \binom{n}{j} + \sum_{j=0}^{n} \binom{n}{j} = 2^n + 2^n = 2^{n+1}.$$

□

Proof. (alternative)

$$2^n = (1+1)^n = \sum_{j=0}^{n} 1^{n-j} 1^j \binom{n}{j} = \sum_{j=0}^{n} \binom{n}{j}$$

□

(ii)

$$\sum_{j=0}^{n} (-1)^j \binom{n}{j} = \binom{n}{0} - \binom{n}{1} + \cdots \pm \binom{n}{n} = 0$$

Proof.

$$0 = (1 + (-1))^n = \sum_{j=0}^{n} 1^{n-j} (-1)^j \binom{n}{j} = \sum_{j=0}^{n} (-1)^j \binom{n}{j}.$$

□

(iii)

$$\sum_{l \text{ odd}} \binom{n}{l} = \binom{n}{1} + \binom{n}{3} + \cdots = 2^{n-1}$$

Proof.

$$0 = \sum_{l=0}^{n} (-1)^l \binom{n}{l} = \sum_{l \text{ even}} \binom{n}{l} - \sum_{l \text{ odd}} \binom{n}{l},$$

so

$$\sum_{l \text{ even}} \binom{n}{l} = \sum_{l \text{ odd}} \binom{n}{l}.$$

Then

$$2^n = \sum_{l=0}^{m} \binom{n}{l} = \sum_{l \text{ even}} \binom{n}{l} + \sum_{l \text{ odd}} \binom{n}{l} = 2 \sum_{l \text{ odd}} \binom{n}{l},$$

so

$$\sum_{l \text{ odd}} = \frac{2^n}{2} = 2^{n-1}$$

□

(iv)

$$\sum_{l \text{ even}} \binom{n}{l} = \binom{n}{0} + \binom{n}{2} + \cdots = 2^{n-1}$$

Proof. It follows from proof of (iii). □

5.

(a) Prove by induction on n that

$$1 + r + r^2 + \cdots + r^n = \frac{1 - r^{n+1}}{1 - r}$$

if $r \neq 1$.

Proof. Let $n = 1$. Then $1 + r = \frac{(1+r)(1-r)}{1-r} = \frac{1-r^2}{1-r}$, so the formula holds.
Next, suppose that the formula is true for some $n \geq 1$. Then

$$\begin{aligned} 1 + r + r^2 + \cdots + r^{n+1} &= \frac{1 - r^{n+1}}{1 - r} + r^{n+1} = \frac{1 - r^{n+1}}{1 - r} + \frac{r^{n+1}(1 - r)}{1 - r} \\ &= \frac{1 - r^{n+1} + r^{n+1} - r^{n+2}}{1 - r} = \frac{1 - r^{n+2}}{1 - r} \end{aligned}$$

□

(b) Derive this result by setting $S = 1 + r + \cdots + r^n$, multiplying this equation by r, and solving the two equations for S.

Proof.

$$S = 1 + r + \cdots + r^n \text{ and } Sr = r + r^2 + \cdots + r^{n+1}.$$

Then

$$S(1 - r) = 1 + r + \cdots + r^n - r - r^2 - \cdots - r^{n+1} = 1 - r^{n+1},$$

so

$$S = \frac{1 - r^{n+1}}{1 - r}$$

□

6. The formula for $1^2 + \cdots + n^2$ can be derived as follows. We begin with the formula

$$(k + 1)^3 - k^3 = 3k^2 + 3k + 1.$$

Writing this formula for $k = 1, \ldots, n$ and adding, we obtain

$$2^3 - 1^3 = 3 \cdot 1^2 + 3 \cdot 1 + 1$$

$$3^3 - 2^3 = 3 \cdot 2^2 + 3 \cdot 2 + 1$$

$$\vdots$$

$$\frac{(n+1)^3 - n^3 = 3n^2 + 3n + 1}{(n+1)^3 - 1 = 4[1^2 + \cdots + n^2] + 3[1 + \cdots + n] + n.}$$

Thus we can find $\sum_{k=1}^{n} k^2$ if we already know $\sum_{k=1}^{n} k$. Use this method to find

(i) $1^3 + \cdots + n^3$.

Proof. We begin with

$$(k+1)^4 - k^4 = 4k^3 + 6k^2 + 4k + 1$$

Then we have

$$(n+1)^4 - 1 = 4\sum_{j=1}^{n} j^3 + 6\sum_{k=1}^{n} k^2 + 4\sum_{l=1}^{n} l + n$$

so

$$\begin{aligned}
\sum_{j=1}^{n} j^3 &= \frac{(n+1)^4 - 1 - 6\sum_{k=1}^{n} k^2 - 4\sum_{l=1}^{n} l - n}{4} \\
&= \frac{n^4 + 4n^3 + 6n^2 + 4n + 1 - 1 - 6\frac{n(n+1)(2n+1)}{6} - 4\frac{n(n+1)}{2} - n}{4} \\
&= \frac{n^4 + 4n^3 + 6n^2 + 3n - 2n^3 - 3n^2 - n - 2n^2 - 2n}{4} \\
&= \frac{n^4}{4} + \frac{n^3}{2} + \frac{n^2}{4}
\end{aligned}$$

□

(ii) $1^4 + \cdots + n^4$.

Proof. We begin with

$$(k+1)^5 - k^5 = 5k^4 + 10k^3 + 10k^2 + 5k + 1$$

Then we have

$$(n+1)^5 - 1 = 5\sum_{i=1}^{n} i^4 + 10\sum_{j=1}^{n} j^3 + 10\sum_{k=1}^{n} k^2 + 5\sum_{l=1}^{n} l + n$$

so

$$\begin{aligned}
\sum_{i=1}^{n} i^4 &= \frac{(n+1)^5 - 1 - 10\sum_{j=1}^{n} j^3 - 10\sum_{k=1}^{n} k^2 - 5\sum_{l=1}^{n} l - n}{5} \\
&= \frac{n^5 + 5n^4 + 10n^3 + 10n^2 + 5n - 5\left(\frac{n^4}{4} + \frac{n^3}{2} + \frac{n^2}{4}\right) - 10\frac{n(n+1)(2n+1)}{6} - 5\frac{n(n+1)}{2} - n}{5} \\
&= \frac{n^5}{5} + \frac{n^4}{2} + \frac{n^3}{3} - \frac{n}{30}
\end{aligned}$$

□

(iii) $\frac{1}{1\cdot 2} + \frac{1}{2\cdot 3} + \cdots + \frac{1}{n(n+1)}$.

Proof. We begin with

$$\frac{1}{k} - \frac{1}{k+1} = \frac{1}{k(k+1)}$$

Then we have

$$\sum_{j=1}^{n} \frac{1}{n(n+1)} = 1 - \frac{1}{n+1}$$

□

(iv) $\frac{3}{1^2\cdot 2^2} + \frac{5}{2^2\cdot 3^2} + \cdots + \frac{2n+1}{n^2(n+1)^2}$.

Proof. We begin with

$$\frac{1}{(k+1)^2} - \frac{1}{k^2} = \frac{2k+1}{k^2(k+1)^2}$$

Then we have

$$\sum_{j=1}^{n} \frac{2j+1}{j^2(j+1)^2} = \frac{1}{(n+1)^2} - 1$$

□

8. Prove that every natural number is either even or odd.

Proof. Since $1 = 2 \cdot 0 + 1$, 1 is obviously an odd number. Now suppose that some natural number n is either odd or even. We consider two cases:

Case 1: n is odd. Then $n = 2k + 1$ for some integer k, and $n + 1 = 2k + 2 = 2(k + 1)$. Since $k + 1$ is an integer, $n + 1$ is even.

Case 2: n is even. Then $n = 2k$ for some integer k, and $n + 1 = 2k + 1$, so $n + 1$ is odd. □

9. Prove that if a set A of natural numbers contains n_0 and contains $k + 1$ whenever it contains k then A contains all natural number $\geq n_0$.

Proof. Suppose that a set A of natural numbers contains n_0 and contains $k+1$ whenever it contains k, and that there is some smallest element i, such that $i \notin A$ and $i > n_0$. Then $i - 1 \in A$, or else i would not be the smallest such element. Since $i - 1 \in A$, $(i - 1) + 1 \in A$, so $i \in A$, which is a contradiction. □

10. Prove the principle of mathematical induction from the well-ordering principle.

Proof. Suppose that for some statement P, A is the set of all natural numbers, for which P is true, and that if $k \in A$, then $k+1 \in A$. Then A has a least member n_0, and contains all natural numbers $\geq n_0$, so if $1 \in A$, then A is the set of all natural numbers, and therefore P is true for all natural numbers. □

11. Prove the principle of complete induction from the ordinary principle of induction. Hint: If A contains 1 and A contains $n+1$ whenever it contains $1,\ldots,n$, consider the set B of all k such that $1,\ldots,k$ are all in A.

Proof. Suppose that for some statement P, A is the set of all natural numbers for which P is true, $1 \in A$, and whenever $1,\ldots,n$ are all in A, then $n+1 \in A$. Let B be the set of all k such that $1,\ldots,k$ are all in A. Then obviously $1 \in B$. Now suppose that for some element k, $1,\ldots,k$ are all in A, and therefore $k \in B$. Since $1,\ldots,k$ are all in A, then $k+1 \in A$, so $1,\ldots,k+1$ are all in A, and therefore $k+1 \in B$. Then $B = N$, so $A = N$, and thus P is true for all natural numbers. □

12.

(a) If a is rational and b is irrational, is $a+b$ necessarily irrational? What if a and b are both irrational?

Proof. Suppose that for some rational number a and some irrational b, $a+b$ is rational. Then $a+b = \frac{x}{y}$ with x, y being integers. Then $b = \frac{x}{y} - a = \frac{x-ay}{y}$ so b is rational, which is a contradiction. □

(b) If a is rational and b is irrational, is ab necessarily irrational?

Proof. For some rational number a and irrational b, ab is rational if $a = 0$, since $0b = 0$ is rational. Suppose that $a \neq 0$ and ab is rational. Then $ab = \frac{x}{y}$ for some integers x, y, so $b = \frac{x}{ay}$, which would imply that b is rational, which is a contradiction. □

(c) Is there a number a such that a^2 is irrational but a^4 is rational?

Proof. Consider $a = \sqrt{\sqrt{2}}$. Then $a^2 = \sqrt{2}$ but $a^4 = 2$. □

(d) Are there two irrational numbers whose sum and product are both rational?

Proof. Consider consider $a + \sqrt{2}$ and $a - \sqrt{2}$ with a rational. Then $a + \sqrt{2} + a - \sqrt{2} = 2a$ which is rational, and $(a+\sqrt{2})(a-\sqrt{2}) = a^2 - 2$ which is rational. □

13.

(a) Prove that $\sqrt{3}, \sqrt{5}$ and $\sqrt{6}$ are irrational. Hint: To treat $\sqrt{3}$ for example, use the fact that every integer is of the form $3n, 3n+1$ or $3n+2$. Why doesn't this proof work for $\sqrt{4}$.

Proof. Since

$$(3n+1)^2 = 3(3n^2+2n)+1$$
$$(3n+2)^2 = 3(3n^2+4n+1)+1$$

and

$$(3n)^2 = 3(3n)^2,$$

it follows that if k^2 is divisible by 3, then k is also divisible by 3. Suppose that $\sqrt{3}$ is rational, that is, there exist some integers x, y, $y \neq 0$ with no common divisor, such that $\sqrt{3} = \frac{x}{y}$. Then $(\frac{x}{y})^2 = 3$, so $x^2 = 3y^2$, so x must be divisible by 3. Then $x = 3z$ for some integer z, so $3y^2 = 9z^2$, and thus $y^2 = 3z^2$, which means that y is divisible by 3, which contradicts x and y having no common divisor, which means that $\sqrt{3}$ can not be rational. □

Proof. Since

$$(5n+1)^2 = 5(5n^2+2n)+1$$
$$(5n+2)^2 = 5(5n^2+4n)+4$$
$$(5n+3)^2 = 5(5n^2+6n+1)+4$$
$$(5n+4)^2 = 5(5n^2+8n+3)+1$$

and

$$(5n)^2 = 5(5n^2),$$

it follows that if k^2 is divisible by 5, then k is also divisible by 5. Suppose that $\sqrt{5}$ is rational, that is, there exist some integers x, y, $y \neq 0$ with no common divisor, such that $\sqrt{5} = \frac{x}{y}$. Then $(\frac{x}{y})^2 = 5$, so $x^2 = 5y^2$, so x must be divisible by 5. Then $x = 5z$ for some integer z, so $5y^2 = 25z^2$, and thus $y^2 = 5z^2$, which means that y is divisible by 5, which contradicts x and y having no common divisor, so $\sqrt{5}$ can not be rational. □

Proof. Since

$$(6n+1)^2 = 6(6n^2+2n)+1$$
$$(6n+2)^2 = 6(6n^2+4n)+4$$
$$(6n+3)^2 = 6(6n^2+6n+1)+3$$
$$(6n+4)^2 = 6(6n^2+8n+2)+4$$
$$(6n+5)^2 = 6(6n^2+10n+4)+1$$

and

$$(6n)^2 = 6(6n^2)$$

it follows that if k^2 is divisible by 6, then k is also divisible by 6. Suppose that $\sqrt{6}$ is rational, that is, there exist some integers x, y, $y \neq 0$ with no common divisor, such that $\sqrt{6} = \frac{x}{y}$. Then $(\frac{x}{y})^2 = 6$ so $x^2 = 6y^2$, so x must be divisible by 6. Then $x = 6z$ for some integer z, so $6y^2 = 36z^2$, and thus $y^2 = 6z^2$, which means that y is divisible by 6, which contradicts x and y having no common divisor, so $\sqrt{6}$ can not be rational. □

This proof doesn't work for $\sqrt{4}$ because

$$(4n+2)^2 = 4(4n^2+4n+1)$$

so k^2 being divisible by 4 does not imply k is divisible by 4.

(b) Prove that $\sqrt[3]{2}$ and $\sqrt[3]{3}$ are irrational.

Proof. Since

$$(2n+1)^3 = 2(4n^3+6n^2+3n)+1$$

and

$$(2n)^3 = 2(4n^3),$$

it follows that if k^3 is even, then k is even. Suppose that $\sqrt[3]{2}$ is rational, that is, there exist some integers x, y, $y \neq 0$ with no common divisor, such that $\sqrt[3]{2} = \frac{x}{y}$. Then $(\frac{x}{y})^3 = 2$, so $x^3 = 2y^3$, which means that x is even. Then $x = 2z$ for some integer z, so $2y^3 = 8z^3$, so $y^3 = 2(2z^3)$, which means that y is also even, which contradicts x and y having no common divisor, so $\sqrt[3]{2}$ can not be rational. □

Proof. Since

$$(3n+1)^3 = 3(9n^3+9n^2+n)+1$$
$$(3n+2)^3 = 3(9n^3+18n^2+12n+2)+2$$

and

$$(3n)^3 = 3(9n^3)$$

it follows that if k^3 is divisible by 3, then k is divisible by 3. Suppose that $\sqrt[3]{3}$ is rational, that is, there exist some integers x, y, $y \neq 0$ with no common divisor, such that $\sqrt[3]{3} = \frac{x}{y}$. Then $(\frac{x}{y})^3 = 3$, so $x^3 = 3y^3$, which means that x is divisible by 3. Then $x = 3z$ for some integer z, so $3y^3 = 27z^3$, so $y^3 = 3(3z^3)$, which means that y is also divisible by 3, which contradicts x and y having no common divisor, so $\sqrt[3]{3}$ can not be rational. □

17. It seems likely that $\sqrt{n}$ is irrational whenever the natural number n is not the square of another natural number. Although the method of problem 13 may actually be used to treat any particular case, it is not clear in advance that it will always work, and a proof for the general case requires some extra information. A natural number p is called a prime number if it is impossible to write $p = ab$ for natural numbers a and b unless one of these is p and the other 1; for conveniece we also agree that 1 is not a prime number. The first few prime numbers are $2, 3, 5, 7, 11, 13, 17, 19$. If $n > 1$ is not a prime, then $n = ab$, with a and b both $< n$; if either a or b is not a prime, it can be factored similarly; continuing in this way proves that we can write n as a product of primes. For example, $28 = 4 * 7 = 2 * 2 * 7$.

(a) Turn this argument into a rigorous proof by complete induction.

Proof. Let A be the set of non-prime natural numbers bigger than 1. Then the smallest element $a_0 = 4$, and $4 = 2 \cdot 2$, so it can be written as a product of primes.

Next, suppose that $a_0, a_1, \ldots, a_n$ are all consecutive elements of A and can be written as products of primes. Then $a_{n+1} \in A$ is a non-prime natural number, so it can be written as $a_{n+1} = ab$ with $a, b < a_{n+1}$. Then either a, b are prime, so a_{n+1} can be written as a product of primes, or if any of a, b are not prime, then since they are smaller than a_{n+1}, they themselves can be written as a product of primes, so a_{n+1} can be written as a product of primes. □

A fundamental theorem about integers, states that this factorization is unique, except for the order of the factors. Thus, for example, 28 can never be written as a product of primes one of which is 3, nor can it be written in a way that involves 2 only once.

(b) Using this fact, prove that $\sqrt{n}$ is irrational unless $n = m^2$ for sume natural number m.

Lemma. *A natural number y is a square of another natural number x if and only if each prime in its factorization appears an even number of times.*

Let x be some natural number. Then x can be written as a unique product of primes, say $p_1, p_2, \ldots, p_n$. Then

$$x^2 = x \cdot x = (p_1 \cdot p_2 \cdot \cdots \cdot p_n)(p_1 \cdot p_2 \cdot \cdots \cdot p_n) = {p_1}^2 \cdot {p_2}^2 \cdot \cdots \cdot {p_n}^2$$

so each prime in the factorization of x^2 appears an even number of times.

Now suppose that for some natural number y, each prime in its factorization appears an even number of times. Then

$$y = p_1^2 \cdot p_2^2 \cdot \cdots \cdot p_n^2 = (p_1 \cdot p_2 \cdot \cdots \cdot p_n)(p_1 \cdot p_2 \cdot \cdots \cdot p_n),$$

so y is the square of a natural number $x = (p_1 \cdot p_2 \cdot \cdots \cdot p_n)$.

Proof. Suppose that for some natural number n, $\sqrt{n}$ is rational. Then $\sqrt{n} = \frac{a}{b}$ for some natural numbers a and b, and $nb^2 = a^2$. Then the factorization of nb^2 is the same as the factorization of a^2, and in the factorizations of a^2 and b^2 each prime appears an even number of times. Then in the factorization of n each prime also appears an even number of times, so n is the square of another natural number. □

(c) Prove more generally that $\sqrt[k]{n}$ is irrational unless $n = m^k$.

Lemma. *A natural number y is the k-th power of another natural number x if and only if each prime in its factorization appears a factor of k times.*

Let x be some natural number. Then x can be written as a unique product of primes, say $p_1, p_2, \ldots, p_n$. Then

$$x^k = (p_1 \cdot p_2 \cdot \cdots \cdot p_n)^k = {p_1}^k \cdot {p_2}^2 \cdot \cdots \cdot {p_n}^k$$

so each prime in the factorization of x^k appears a factor of k times.

Now suppose that for some natural number y, each prime in its factorization appears a factor of k times. Then

$$y = {p_1}^k \cdot {p_2}^k \cdot \cdots \cdot {p_n}^k = (p_1 \cdot p_2 \cdot \cdots \cdot p_n)^k$$

so y is the k-th power of a natural number $x = (p_1 \cdot p_2 \cdot \cdots \cdot p_n)$.

Proof. Suppose that for some natural number n, $\sqrt[k]{n}$ is rational. Then $\sqrt[k]{n} = \frac{a}{b}$ for some natural numbers a and b, and $nb^k = a^k$. Then the factorization of nb^k is the same as the factorization of a^k, and in the factorizations of a^k and b^k each prime appears a factor of k times. Then in the factorization of n each prime also appears an even number of times, so n is the k-th power of another natural number. □

(d) No discussion of prime numbers should fail to allude to Euclid's beautiful proof that there are infinitely many of them. Prove that there cannot be only finitely many prime numbers $p_1, p_2, \ldots, p_n$ by considering $p_1 \cdot p_2 \cdot \cdots \cdot p_n + 1$.

Proof. Suppose that there are only finitely many prime numbers $p_1, p_2, \ldots, p_n$. The number

$$x = p_1 \cdot p_2 \cdot \cdots \cdot p_n + 1$$

is not divisible by any of $p_1, p_2, \ldots, p_n$ (it would result in a remainder of 1), so either x is itself a prime $> p_n$, or it is a factor of primes bigger than p_n, which contradicts p_n being the biggest prime number. □