Euclid’s infinitude of primes

Theorem 78  The set of primes is infinite.

Proof:
Sets
Objectives

To introduce the basics of the theory of sets and some of its uses.
Abstract sets

It has been said that a set is like a mental “bag of dots”, except of course that the bag has no shape; thus,

\[
\begin{array}{cccccc}
(1,1) & (1,2) & (1,3) & (1,4) & (1,5) \\
(2,1) & (2,2) & (2,3) & (2,4) & (2,5)
\end{array}
\]

may be a convenient way of picturing a certain set for some considerations, but what is apparently the same set may be pictured as

\[
\begin{array}{cccccc}
(1,1) & (2,1) & (1,2) & (2,2) & (1,3) & (2,3) & (1,4) & (2,4) & (1,5) & (2,5)
\end{array}
\]

or even simply as

\[
\begin{array}{cccccccccccc}
\bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet
\end{array}
\]

for other considerations.
Naive Set Theory

We are not going to be formally studying Set Theory here; rather, we will be *naively* looking at ubiquitous structures that are available within it.
Extensionality axiom

Two sets are equal if they have the same elements.

Thus,

\[ \forall \text{ sets } A, B. \ A = B \iff ( \forall x. x \in A \iff x \in B ) \]

Example:

\[ \{0\} \neq \{0, 1\} = \{1, 0\} \neq \{2\} = \{2, 2\} \]
Subsets and supersets
Separation principle

For any set $A$ and any definable property $P$, there is a set containing precisely those elements of $A$ for which the property $P$ holds.

\[ \{ x \in A \mid P(x) \} \]
Russell’s paradox
Empty set

\[ \emptyset \quad \text{or} \quad \{ \} \]

defined by

\[ \forall x. x \notin \emptyset \]

or, equivalently, by

\[ \neg (\exists x. x \in \emptyset) \]
Cardinality

The *cardinality* of a set specifies its size. If this is a natural number, then the set is said to be *finite*.

Typical notations for the cardinality of a set \( S \) are \(#S\) or \(|S|\).

**Example:**

\[
#\emptyset = 0
\]
Powerset axiom

For any set, there is a set consisting of all its subsets.

\[ \forall X. X \in \mathcal{P}(U) \iff X \subseteq U. \]
Hasse diagrams
Proposition 81  \textit{For all finite sets} $\mathcal{U}$,

\[
\# \mathcal{P}(\mathcal{U}) = 2^{\# \mathcal{U}}.
\]

\textbf{Proof Idea:}