Sample LaTeX Document

I can't possibly write a whole tutorial on TEX or LATEX (which is what this document uses). The main purpose of this document is to give you some examples that you can draw on and modify in your assignments. Learning TEX is a lifelong experience, and it continues to grow with its user base. There are, of course, innumerable written and/or video tutorials, e.g., `https://youtu.be/Rsoj2YavveE` and its associated blog, `http://quicklatex.blogspot.com/`. A quick reference for the various symbols is also handy, e.g., `https://reu.dimacs.rutgers.edu/Symbols.pdf`. Of course, just about any question you have about how to do something in TEX can be answered almost instantaneously thanks to the "wisdom of the web"; for example, I forgot the command for displaying the backslash character, needed below, so I just googled "What is the LaTeX symbol for backslash?"

A disadvantage with many (most?) tutorials is that they're too general. They include a lot of stuff you won't need for any assignment in this course, and leave out some things you may find useful. My suggestion, based on personal experience: The best way to learn it is to just jump in and start using it. Try beginning with this document. It illustrates a few things, including math symbols, the theorem environment, the proof environment, the symbolic labeling of theorems and equations, and how to reference them. Study the source file (`latexDemo.tex`) and the typeset version you are now reading, and try to understand their relationship. Leave in the "preamble" that you find in the source `latexDemo.tex` (everything up to and including the `\begin{document}`) and, of course, the `\end{document}`. Otherwise, modify what it says to suit your purposes.

Let's start with the theorem and proof environments.

Theorem 1. *("Bézout's Lemma"): Let* $a, b \in \mathbb{Z}$. *Then* $\exists x, y \in \mathbb{Z}$ *such that* $gcd(a, b) = ax + by$.

Proof. Let

$$d = \min_{x,y\in\mathbb{Z}} \{ax + by|ax + by > 0\}.$$

Write $d = ax' + by'$. We first show, for any $x, y \in \mathbb{Z}$, that $d|(ax + by)$.

Let $z = ax + by$ for any $x, y \in \mathbb{Z}$. We divide z by d, i.e., write $z = md + r$, where r is the remainder so $0 \leq r < d$. Suppose now that $r > 0$; we will derive a contradiction. We have $z - md = r$, which implies that $ax + by - md = r$. But then,

$$r = ax + by - md = ax + by - m(ax' + by') = a(x - mx') + b(y - my'). \quad (1)$$

What Eq. (1) says is that r is of the form $ax'' + by''$, where as it happens $x'' = x - mx'$ and $y'' = y - my'$. Since d is the minimum such positive number, and we're assuming that r is positive, it follows that $d \leq r$. However, $r < d$, so this is a contradiction. Therefore, r must equal 0. It follows that $z = ax + by = md$, i.e., $d|(ax + by)$, as we wished to show.

We now know that d is a common divisor of a and b. We need to show it's the *greatest* common divisor to complete the proof. To see that, suppose $c|(ax + by)$, where $ax + by > 0$. Then $c \leq d$, since d is the minimum value that $ax + by$ takes on. Therefore, $d = gcd(a, b)$. □

Theorem 1 is useful, for example, since it leads to an extension of the Euclidean algorithm for finding the inverse of a modulo b, or b modulo a, in the event that $gcd(a, b) = 1$, an important operation in cryptography.

The preamble to this document's source includes a bunch of commands for symbols that will be useful. In particular, we have standard symbols for the natural numbers $\mathbb{N}$, the integers $\mathbb{Z}$, the reals $\mathbb{R}$, the complex numbers $\mathbb{C}$ and so forth. Of great use in this course will be the `\ket`, `\bra`, and `\bracket` commands, which, via expressions like `\ket{\psi}` and the like can be used to form expressions like $|\psi\rangle$ or $|0101\rangle$ or $\langle\varphi|\psi\rangle$ or $\sum_{k=1}^{n} |k\rangle\langle k|$.

Just to illustrate how you use basic but commonly occurring things like fractions, subscripts, exponents/superscripts, the summation sign, and how to align equalities in an array of equations, here's an old boring (but far from useless) theorem that I expect you know well.

Theorem 2. *(Sum of the numbers from* 1 *to* n*): Let* $n \in \mathbb{N}$ *and let*

$$S_n = \sum_{k=1}^{n} k.$$

Then $S_n = \frac{n(n+1)}{2}$.

Proof. We prove this by induction on n.
Base case: Let $n = 1$. Then by definition of the sum, we clearly have $S_n = S_1 = 1$. Furthermore, when $n = 1$, we have $\frac{n(n+1)}{2} = \frac{1(1+1)}{2} = 1$, so the relation follows for $n = 1$.

Induction step: Suppose that $S_n = \frac{n(n+1)}{2}$. Let's break down S_{n+1}:

$$\begin{array}{rcl} S_{n+1} & = & \displaystyle\sum_{k=1}^{n+1} k \\ & = & \displaystyle\sum_{k=1}^{n} k + (n+1) \\ & = & S_n + (n+1) \\ & = & \dfrac{n(n+1)}{2} + (n+1) \\ & = & \dfrac{n(n+1)}{2} + \dfrac{2(n+1)}{2} \\ & = & \dfrac{(n+2)(n+1)}{2}, \end{array}$$

where the fourth equality followed from the induction hypothesis. But $S_{n+1} = \frac{(n+2)(n+1)}{2}$ establishes the original assertion for $n + 1$, so we are done. □

Matrices can be denoted conveniently, as in:

$$\mathsf{H} = \frac{1}{2}\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}, \quad \mathsf{C}_{ij} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}.$$

(the first one, H, being the familiar Hadamard matrix, and C_{ij} is controlled NOT).