An example of Latex in action

S. D. Galbraith

1 February 2005

Abstract

This article gives an example of how to write mathematical documents using the LaTeX package.

1 Introduction

Everyone learns Latex by borrowing someone else's document. That's what this is for. There are also books, articles and lots of web pages which explain valuable things. A good place to look for help on the web is here:

`http://www-h.eng.cam.ac.uk/help/tpl/textprocessing/`

You can write text in **bold face** or *italics (emphasised)* or sans serif font or in `typewriter style`.

You can write text in large letters or larger letters or even larger letters or the hugest letters.

2 Formulae

The best thing about Latex is that it makes nice mathematical formulae for you. Possibly the three most important tools are superscripts, subscripts and fractions, for example:

$$x_1^{77} \qquad a_{1,2}^{2^8} \qquad \frac{2+x}{x^2+1} \qquad \tfrac{1}{2}.$$

Formulae can be written as part of the line, such as $\int_0^2 e^x dx$, or in display mode like

$$\frac{\sin(x)}{x^2+e^x+23}.$$

The above equation does not have an equation number. Giving equations numbers is easy, and they can be referred to in the following way: see equation (1) below

$$\sum_{i=0}^{N_3} \binom{N_4}{i} \frac{x^i}{i!} \tag{1}$$

You can do equations on several lines, such as

$$f(x) = (x+1)(x+2)(x+3) \quad (2)$$
$$= x^3 + 6x^2 + 11x + 6 \quad (3)$$

or without numbers as

$$\begin{aligned} f(x) &= (x+1)(x+2)(x+3) \\ &= x^3 + 6x^2 + 11x + 6. \end{aligned}$$

References are done like this [2].

Greek letters are obtained in mathematics mode, for example $\alpha, \beta, \gamma, \Gamma, \delta, \Delta, \ldots$. Other fonts are available for mathematics, such as calligraphic $\mathcal{A}, \mathcal{B}$ and blackboard bold $\mathbb{A}, \mathbb{R}$. One can do underlining and overlining

$$\underline{x} \in \overline{\mathbb{Q}}.$$

There are lots of built-in symbols such as $\Rightarrow, \rightarrow, \in, <, \leq, \subset, \subseteq, |, \dagger, \star, \oplus, \times, \pounds, \S, \perp$.

There are several ways to write modular arithmetic. For example $a \equiv 23 \bmod 78$ or $a \equiv 23 \pmod{78}$.

Operations can be negated, for example:

$$a \neq b, \quad a \not\equiv b \bmod c.$$

The operations \left and \right are useful for making braces the right size:

$$\left\{0, \frac{1}{2}, 1\right\}, \quad \left(\sum_{i=1}^{3}(i^2+2)\right), \quad \left[1 + \frac{1}{2 + \frac{2}{4+\frac{1}{5}}}\right].$$

Here is a table:

N	Information about N
2	A prime
3	A prime
4	A square
5	A prime
6	Half a dozen

In the next section you will find Theorem 3.1.

If you want to start on a new page then do this:

3 A theorem

Theorem 3.1 *Let E/F be an elliptic curve defined over a number field F. Let $End(E) = \mathcal{O}$ be an order of discriminant D. Let p be a prime for which E has good and supersingular reduction. Let $\wp$ be a prime ideal of F above p. Let $\tilde{E}$ over $k = \mathbb{F}_{p^m}$ be the reduction mod $\wp$ of E. Let π be the p^m-Frobenius map on $\tilde{E}$. Suppose $r \mid \#\tilde{E}(\mathbb{F}_{p^m})$ is a prime such that $r > 3$ and $r \nmid pD$.*

Let $d \in \mathbb{N}$ be such that $\sqrt{-d} \in \mathcal{O}$. Let $\Psi \in End(E)$ satisfy $\Psi^2 = -d$. Let $\psi \in End_{\mathbb{F}_p}(\tilde{E})$ be the reduction mod $\wp$ of Ψ. Then ψ is a suitable distortion map for points $P \in \tilde{E}[r]$ which lie in a π-eigenspace.

Proof. You don't want to see the proof. □

4 More things

4.1 Subsections

This is subsection 4.1.

4.2 Spot the difference

Experts in Latex find that they like things a certain way, for example:

- “quotes” rather than ”quotes”.
- $a \mid b$ and $a \nmid b$ rather than $a|b$ and $a \not| b$.

Doing references the right way is also important. Some examples are given below.

References

[1] D. Boneh, The decision Diffie-Hellman problem, in J. Buhler (ed.), ANTS III, Springer LNCS 1423 (1998) 48–63.

[2] H. Cohen, *A course in computational algebraic number theory*, Springer GTM 138 (1993).

[3] B. H. Gross, Heights and special values of L-series, CMS proceedings, **7**, AMS (1986), 115–187.

[4] J. Vélu, Isogénies entre courbes elliptiques, C. R. Acad. Sci. Paris, Série A, 273 (1971) 238–241.