EECS 475: Introduction to Cryptography Notes

Noah Peters

March 26, 2023

Abstract

Lecture notes for EECS 475 at the University of Michigan. LaTeXtemplate by Pingbang Hu.

Contents

Chapter 4

Introduction

Lecture 19: Number Theory

We define the set of integers, $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$, and natural numbers, $\mathbb{N} = \mathbb{Z}^+ = \{1, 2, 3, \ldots\}$. 20 Mar. 10:30

Theorem 4.0.1 (Product of primes)**.** Every integer $N > 1$ can be written *uniquely* as a product of (power of) primes.

Lemma 4.0.1 (Division with remainder)**.** Let $a \in \mathbb{Z}, b \in \mathbb{Z}^+$. $\exists$ unique integers q, r such that $a = q.b + r$ where $0 \leq r < b$, and they can be efficiently computed in *polynomial time* relative to the *bit length*: i.e. $\log_2 a + \log_2 b + O(1)$

With the ability to perform division in polynomial time, we are able to find the **greatest common divisor** of two integers a, b:

Definition 4.0.1 (Greatest common divisor)**.** Let $a, b \in \mathbb{Z}^+$. Then, there exists $x, y \in \mathbb{Z}$ such that $\gcd(a, b) = a.x + b.y$. Further, $\gcd(a, b)$ is the smallest positive integer that can be written this way.

Definition 4.0.2 (Natural numbers)**.** We denote the set of *natural numbers* as $\mathbb{N}$.

Lemma 4.0.2 (Useful lemma)**.** Given the axioms of natural numbers $\mathbb{N}$, we have

$$0 \neq 1.$$

An obvious proof. Obvious. ■

Proposition 4.0.1 (Useful proposition)**.** From Lemma 4.0.2, we have

$$0 < 1.$$

Exercise. Prove that $1 < 2$.

Answer. We note the following.

> **Note.** We have Proposition 4.0.1! We can use it iteratively!
>
> With the help of Lemma 4.0.2, this holds trivially. ⊛

Example. We now can have $a < b$ for $a < b$!

Proof. Iteratively apply the exercise we did above. ⊛

Remark. We see that Proposition 4.0.1 is really powerful. We now give an immediate application of it.

Theorem 4.0.2 (Mass-energy equivalence). Given Proposition 4.0.1, we then have

$$E = mc^2.$$

Proof. The blank left for me is too small,[a] hence we put the proof in Appendix A.1. ■

[a] https://en.wikipedia.org/wiki/Richard_Feynman

From Theorem 4.0.2, we then have the following.

Corollary 4.0.1 (Riemann hypothesis). The real part of every nontrivial zero of the Riemann zeta function is $\frac{1}{2}$, where the Riemann zeta function is just

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \frac{1}{1^s} + \frac{1}{2^s} + \frac{1}{3^s} + \cdots.$$

Proof. The proof should be trivial, we left it to you. ■ DIY

As previously seen. We see that Lemma 4.0.2 is really helpful in the proof!

Internal Link

You should see all the common usages of internal links. Additionally, we can use citations as [New26], which just link to the reference page!

4.1 Figures

A simple demo for drawing:

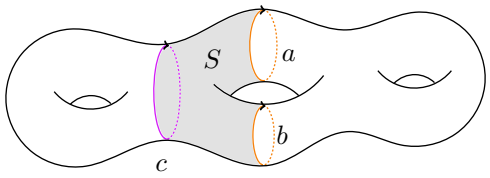


Figure 4.1: A 3-torus.[1]

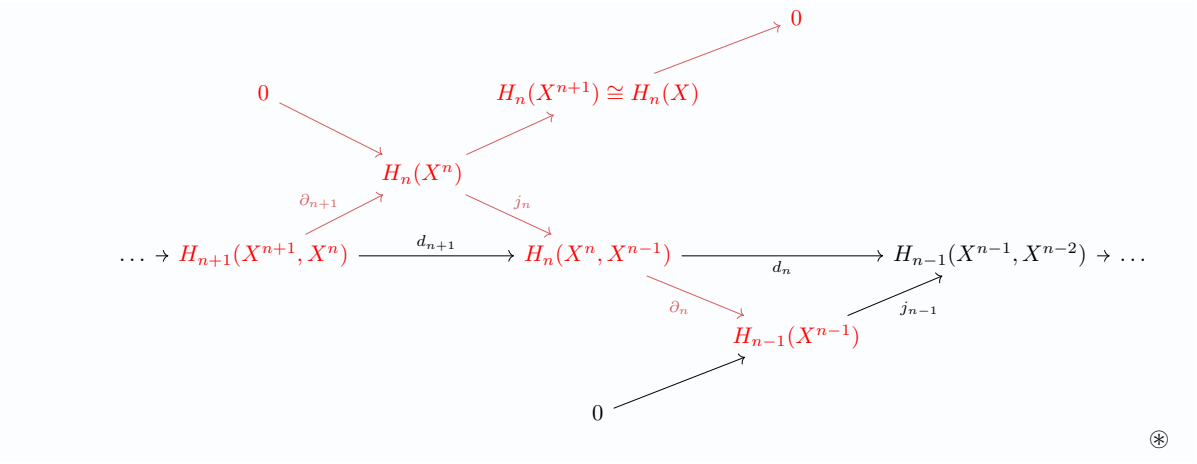
4.2 Commutative Diagram

We can use the package `tikz-cd` to draw some commutative diagram.

Example. The cellular homology agrees with singular homology.

Proof. The following commutative diagram shows everything.

[1] For detailed information, please see https://github.com/sleepymalc/VSCode-LaTeX-Inkscape.



4.3 Fancy Stuffs

With this header, you can achieve some cool things. For example, we can have multiple definitions under a parent environment, while maintains the numbering of definition. This is achieved by `definition*` environment with `definition` inside. For example, we can have the following.

Definition. We have the following number system.

Definition 4.3.1 (Rational number)**.** The set of *rational number*, denote as $\mathbb{Q}$.

Definition 4.3.2 (Real number)**.** The set of *real number*, denote as $\mathbb{R}$.

Definition 4.3.3 (Complex number)**.** The set of *complex number*, denote as $\mathbb{C}$.

Note. And indeed, we can still reference them correctly. For instance, we can use rational numbers to define real numbers and then further use it to define complex numbers.

Furthermore, we can completely control the name of our environments. We already saw we can name definition, lemma, proposition, corollary and theorem environment. In fact, we can also name remark, note, example and proof as follows.

Example (Interesting Example)**.** We note that $1 \neq 2$!

Note (Important note)**.** As a consequence, $2 \neq 3$ also.

Remark (Easy observation)**.** We see that from here, we easily have the following theorem.

Theorem 4.3.1 (Lebesgue Differentiation Theorem)**.** Let $f \in L^1$, then

$$\lim_{r \to 0} \frac{1}{m(B(x,r))} \int_{B(x,r)} |f(y) - f(x)| \, \mathrm{d}y = 0$$

for a.e. x.

An obvious proof of Theorem 4.3.1. Obvious. ■

As we can see, specifically for the `proof` environment, we allow `autoref` and `hyperref`. One can actually allow all example, note and remark environment's name to use reference, but I think that is overkilled.

But this can be achieved by modify the header in an obvious way.[2]

[2]This time I mean it!

Chapter 5

Known Bugs

Lecture 2: Second Lecture

5.1 Introduction

9 Sep. 08:00

Nothing is bugs-free. There are some known bugs which I don't have incentive to solve, or it is hard to solve whatsoever. Let me list some of them.

5.1.1 Footnote Environment

It's easy to let you fall into a situation that you want to keep using `footnote` to add a bunch of unrelated stuffs. However, with our environment there is a known strange behavior, which is following.

Example. Footnote![a]

> **Remark.** Oops! footnote somehow shows up earlier than expect![a]
>
> [a] This is a footnote!
> [a] This is another footnote!

Bugs caught![b]

[b] The final footnote which is ok!

As we saw, the footnote in the `Example` environment should show at the bottom of its own box, but it's caught by `Remark` which causes the unwanted behavior. Unfortunately, I haven't found a nice way to solve this. A potential way to solve this is by using `footnotemark` with `footnotetext` placing at the bottom of the environment, but this is tedious and needs lots of manual tweaking.

Furthermore, not sure whether you notice it or not, but the color box of `Remark` is not quite right! It extends to the right, another trick bug...

5.1.2 Mdframe Environment

Though `mdframe` package is nice and is the key theme throughout this template, but it has some kind of weird behavior. Let's see the demo.

Proof of Theorem 4.0.2. We need to prove the followings.

> **Claim.** $E = mc^2$.

Proof. Nonsense.
Nonsense,
Nonsense,
Nonsense,
Nonsense,
Nonsense. ⊛

■

I expect it should break much earlier, and this seems to be an algorithmic issue of `mdframe`. One potential solution is to use `tcolorbox` instead, but I haven't completely figure it out, hence I can't really say anything right now.

Appendix

Appendix A

Additional Proofs

A.1 Proof of Theorem 4.0.2

We can now prove Theorem 4.0.2.

Proof of Theorem 4.0.2. See here. ■

Bibliography

[New26] I. Newton. *Philosophiae naturalis principia mathematica*. Innys, 1726. URL: https://books.google.com/books?id=WeZO9rjv-1kC.