As any cryptography subfield, Cryptography requires a solid knowledge of Mathematics. While the practical development of cryptographic protocols might not include the need to understand the whole underlying theory, much of it typically still arises. For example, one might need to implement the Elliptic Curve Pairing operation verification in a Zero-Knowledge Proof system, or RSA encryption and decryption methods in Circom circuits. In case you specifically develop the zero-knowledge systems from scratch, there is no need to explain why you need to understand the underlying theory.

This part of the book is dedicated to the mathematical background required for Cryptography. Namely, we will cover essentials specified in Table 1.

Section	Topic	Key Concepts
??	Number Theory	Modular Arithmetic, Ring $\mathbb{Z}_n$ and field $\mathbb{Z}_n^\times$, Fermat's Little Theorem
??	Abstract Algebra	Groups, Subgroups, Fields, Prime field $\mathbb{F}_p$, Isomorphisms, Automorphisms
??	Polynomials	Divisibility, Lagrange Interpolation, Schwartz-Zippel Lemma
??	Linear Algebra Basics	Basic Operations over Vectors and Matrices
??	Fields Extensions	Definition of $\mathbb{F}_{p^m}$, Field Multiplicative Subgroup, Algebraic Closure

Table 1: Topics covered in Part I

This is not the Mathematics book, so we will not prove every mentioned theorem or lemma, but we do provide reasoning for some key facts. We focus on the practical side of the theory, providing examples and exercises for the reader to solve. Moreover, the solutions to the exercises can be found in **??** for the reader to check their understanding.

The reader should already be familiar with very basics of the first four topics, so they will be covered for the sake of completeness and reminding the reader of the key concepts. The last topic, Fields Extensions, is less frequent in the Mathematics curriculum, so we will cover it in more detail.

In case you feel comfortable with the aforementioned topics, feel free to skip them and move to the next part of the book. Finally, if you are unsure about your knowledge, you should open the corresponding section and check whether you can solve exercises in the end without any help.