Introduction to Number Theory

Bui Hong Ha

August 5, 2009

Abstract

Introduction to Number Theory's note. On this note, I summerize many main ideas, important definition, and critical exercises when reading the book: "introduction to number theory " of professor Victor Shoup.

Contents

1 Premilinaries

Some terminology, notation, and simple facts that will bed used throughout the text

Logarithms and exponentials

We write $\log x$ for the natural logarithm, and $\log_b x$ for the logarithm of x to the base b.
We write e^x for the usual exponential function, where $e \approx 2.71828$ is the base of the natural logarithm. $exp[x] \approx e^x$

Sets and families

We use standard set-theoretic notation:

- $\emptyset$ denotes the empty set
- $x \in A$ means that x is an element, or member, of the set A
- For two sets $A, B, A \subset B$ means that A is a subset of B (with A possibly equal to B), and $A \subsetneq B$ means that A is a proper subset of B
- $A \cup B$ denotes the union of A and B
- $A \cap B$ denotes the intersection of A and B
- A/B denotes the set of all elements of A that are not in B
- if A is a set with a finite number of elements, then we write —A— for its **size**, or **cardinality**
- $S_1 \times \ldots \times S_n$ for the **Cartesian product** of sets $S_1, \ldots, S_n$, which is the set of all n-tuples $(a_1, \ldots, a_n)$, where $a_i \in S_i$ for $i = 1, \ldots, n$. We write $S^{\times n}$ for the Cartesian product of n copies of a set S, and for $x \in S$, we write $x^{\times n}$ for the element of $S^{\times n}$ consisting of n copies of x.
- A **family** is a collection of objects, indexed by some set I, called an **index set**. If for each $i \in I$ we have an associated object x_i, the family of all such objects is denoted by $\{x_i\}_{i \in I}$. Unlike a set, a family may contain duplicates,: that is we may have $x_i = x_j$ for some pair of indices i, j with $i \neq j$.

Functions

- $f: A \to B$ indicates that f is a function (also called a **map**) from a set A to a set B
- If $A' \subseteq A$, then $f(A') := \{f(a) : a \in A'\}$ is the **image** of A' undef f, and $f(A)$ is simply referred to as the **image** of f; if $B' \subseteq B$, then $f^{-1}(B') := \{a \in A : f(a) \in B'\}$ is the **pre-image** of B' under f

2 Ideals and greatest common divisors