Scribe Notes for *Algorithmic Number Theory*
Class 1—May 18, 1998

Scribe: Craig A. Struble

Abstract

This class is an introductory class for *CS6104: Algorithmic Number Theory.* The syllabus and motivations for the class are covered. Following the introductory material, we begin a review of number theory.

1 Introductory Material

Algorithmic number theory approaches number theoretic problems from a computational point of view. We are interested in studying problems, giving algorithms for solving the problems, and classifying how difficult problems are. The syllabus for *CS6104: Algorithmic Number Theory* is available from the class home page, `http://ei.cs.vt.edu/~cs6104/`. Prerequisites for the class include a course in algorithm analysis and a course in probability. A course in abstract algebra covering groups, rings, and fields is also helpful.

The textbook for the course is *Algorithmic Number Theory, Vol. 1: Efficient Algorithms* by Bach and Shallit [1][1]. As the title of the textbook suggests, the main focus of the course is algorithms for problems that can be efficiently solved. Towards the end of the class, other topics not in the text may also be covered. See the syllabus for more details.

Homework will be assigned approximately once a week and will be due approximately one week from when it is assigned. Use of symbolic computation or algebra packages such as *Mathematica, Maple,* or *GAP* may be helpful for solving the problems. Students may collaborate together to solve the problems as long as each student prepares his or her own solutions and credit is given appropriately. Homework submissions must be given in LaTeX.

2 Motivations

The theory of numbers is an interesting topic. It provides fun problems such as those given in Beiler [2]. Also, it is the source of classic problems such as Fermat's "Last Theorem", which was proved recently by A. Wiles and R. Taylor. The statement of Fermat's Theorem is simple, but its proof eluded mathematicians for hundreds of years.

Theorem 2.1 (Fermat's Last Theorem). *There exists no nontrivial integer solutions to* $x^n + y^n = z^n$ *for* $n > 2$.

More recently, number theory plays an important role in cryptography. The RSA [3] public key encryption scheme relies on the assumption that factoring large numbers is a difficult task, even for powerful computers. The connections between algorithmic issues and number theory are

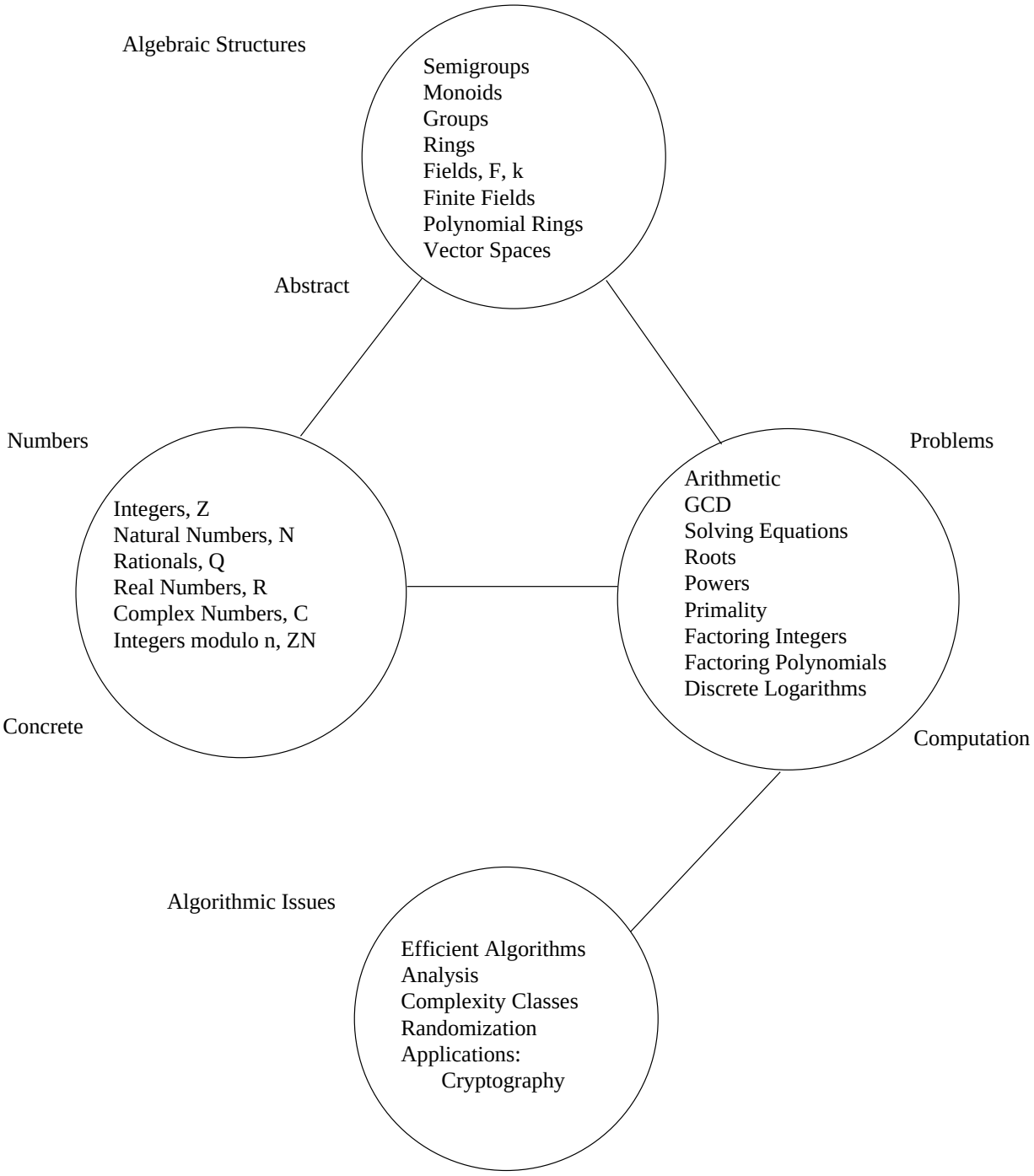

Figure 1: Connections between numbers, algebra, number theory problems, and algorithmic issues.

the motivation behind algorithmic number theory. Figure 1 shows connections between numbers, algebraic structures, number theoretic problems, and algorithmic issues.

The goal of the class is to study number theoretic problems and algorithmic solutions for the problems, if they are known. When the solutions are known, we will attempt to analyze the complexity of the known algorithms. Whether solutions are known or unknown, we will attempt to classify the difficulty of the problems studied.

3 Number Theory

Now, we review some basic number theory. Number theory is a notation rich topic, so notation may not be defined completely in the notes. An index of notation used in the course is on page 487 of the textbook. Also, many theorems are presented without proof. The textbook and references used in the class contains the proofs or proofs are given as exercises. When proofs are given in the textbook, they are referenced in the notes.

3.1 Primes

The integers $\mathbb{Z}$are the focus in number theory. We know how to add, subtract, and multiply integers. While the additive structure of the integers is easily understood, the multiplicative structure is challenging. A **prime** is an integer $p > 1$ whose only positive divisors are 1 and p. An integer $n > 1$ that is not prime is **composite**. We can write every positive integer as a unique product of primes.

Theorem 3.1 (Theorem 2.1.2: Fundamental Theorem of Arithmetic). *Every positive integer n can be expressed as a product of nontrivial powers of distinct primes*

$$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k},$$

*and up to rearrangement of the factors, this **prime factorization** is unique.*

The proof of this theorem is given as Exercise 6 in Chapter 2. The fundamental theorem of arithmetic helps us understand the multiplicative properties of integers.

Example 3.2. The unique prime factorization of 100 is

$$100 = 2^2 \cdot 5^2.$$

Let us count the number of primes less than or equal to a real number x. This value is denoted as $\pi(x)$ and is written

$$\pi(x) = \sum_{p \leq x} 1.$$

The following theorem helps us understand how $\pi(x)$ grows as x approaches infinity.

Theorem 3.3 (Prime Number Theorem). *Asymptotically, the number of primes is given by this limit.*

$$\lim_{x \to \infty} \frac{\pi(x)}{x/\log x} = 1.$$

[1]References to theorems, chapters, exercises, etc., without further attribution always refer to this text.

x	$\pi(x)$	$x/\log x$
1	0	∞
2	1	2.89
3	2	2.73
4	2	2.89
5	3	3.11
10	4	4.34
100	25	21.71

Table 1: Values for $\pi(x)$ and $x/\log x$

The prime number theorem tells us that $\pi(x)$ is approximately $x/\log x$ as x gets large. Intuitively, if we are given a number x, we expect to find a prime by picking $\log x$ random numbers close to x. Table 1 evaluates $\pi(x)$ and $x/\log x$ at some small values.

3.2 Modular Arithmetic

Related to the integers are the integers modulo an integer n, denoted $\mathbb{Z}/(n)$. If a and b are arbitrary integers, we write $a \equiv b \pmod{n}$ when $n \mid a-b$; this notation is read "a is congruent to b, modulo n." Note that $\equiv$ is an equivalence relation on $\mathbb{Z}$.

Example 3.4. Consider $\mathbb{Z}$ modulo $n = 6$, $\mathbb{Z}/(6)$. The equivalence classes of $\mathbb{Z}$ are

$$\begin{array}{lll} a \equiv 0 \pmod 6 & \{..., -12, -6, 0, 6, 12, ...\} \\ a \equiv 1 \pmod 6 & \{..., -11, -5, 1, 7, 13, ...\} \\ a \equiv 2 \pmod 6 & \{..., -10, -4, 2, 8, 14, ...\} \\ a \equiv 3 \pmod 6 & \{..., -9, -3, 3, 9, 15, ...\} \\ a \equiv 4 \pmod 6 & \{..., -8, -2, 4, 10, 16, ...\} \\ a \equiv 5 \pmod 6 & \{..., -7, -1, 5, 11, 17, ...\} \end{array}$$

We can define a function, written $a \bmod n$ that returns a canonical **representative** for the equivalence class containing the integer a as follows:

$$a \bmod n = \begin{cases} a, & \text{if } n = 0; \\ a - n\lfloor \frac{a}{n} \rfloor, & \text{otherwise.} \end{cases}$$

Example 3.5. The unparenthesized "mod" function is applied to three different pairs of numbers.

$$\begin{aligned} 5 \bmod 0 &= 5 \\ 5 \bmod 3 &= 2 \\ 65 \bmod 7 &= 2 \end{aligned}$$

If we define addition, subtraction, and multiplication for $\mathbb{Z}/(n)$ by first performing the operation as if the number is in $\mathbb{Z}$, and then using $a \bmod n$ to give the representative of the equivalence class

for the result, $\mathbb{Z}/(n)$ has the same algebraic operations as $\mathbb{Z}$. Be aware that we may use the same notation to represent objects in two different algebraic structures. For example, 3 may be in $\mathbb{Z}$ or in $\mathbb{Z}/(7)$. Technically, 3 is different in each case, but this abuse of notation is convenient and often clear.

3.3 Greatest Common Divisor

Suppose we have two positive integers m and n. A number d is a **common divisor** of m and n if $d \mid m$ and $d \mid n$. The **greatest common divisor**, denoted $gcd(m, n)$, is the maximum common divisor. We say that m and n are **relatively prime** if $gcd(m, n) = 1$.

Example 3.6. Here are the greatest common divisors for three different pairs of integers.

$$\begin{aligned} \gcd(5, 9) &= 1 \\ \gcd(2, 6) &= 2 \\ \gcd(900, 1200) &= 300 \end{aligned}$$

Exercise 3.7. Try using *Mathematica* or another system to compute $\gcd(10^{100} - 27, 10^{200} + 27)$.

An application of the greatest common divisor is Fermat's Theorem. Fermat's Theorem relates the numbers relatively prime to a prime p and the equivalence class of that number raised to the $p - 1$ power.

Theorem 3.8 (Fermat's Theorem). *If p is a prime and $\gcd(a, p) = 1$, then $a^{p-1} \equiv 1 \pmod{p}$.*

Example 3.9. Suppose that $p = 5$, then $p - 1 = 4$. The following table demonstrates Fermat's theorem.

a	a^4	$a^4 \bmod 5$
0	0	0
1	1	1
2	16	1
3	81	1
4	256	1
5	525	0
6	1296	1

The proof of Fermat's Theorem is given as Exercise 13 in Chapter 2 of the textbook. Fermat's Theorem implies that every non-zero element $\overline{a}$ in $\mathbb{Z}/(p)$ has a multiplicative inverse. Let $\overline{1}$ be the multiplicative identity in $\mathbb{Z}/(p)$. Then the multiplicative inverse of $\overline{a}$ is given by

$$\begin{aligned} \overline{a}^{p-1} &= \overline{1}, \\ \overline{a^{p-2}\overline{a}} &= \overline{1}. \end{aligned}$$

So, $\overline{a^{p-2}}$ is the multiplicative inverse of $\overline{a}$.

4 Next Time

The next class continues the review of number theory, and begins the review of asymptotics.

References

[1] E. Bach and J. Shallit, *Algorithmic Number Theory*, The MIT Press, Cambridge, Massachusetts, 1996.

[2] A. H. Beiler, *Recreations in the Theory of Numbers*, Dover, New York, 1964.

[3] R. L. Rivest, A. Shamir, and L. Adleman, *A method for obtaining digital signatures and public-key cryptosystems*, Comm. ACM, 21 (1978), pp. 120–126.