Notes on Algorithmic Number Theory

Alan Turing

Preface

These notes began as a set of lectures on algorithmic number theory, written for students who already know basic abstract algebra but have not yet seen how those ideas become running code. Each chapter pairs a short piece of theory with the algorithm it justifies.

Acknowledgements

Thanks to the students of the original course for catching more errors in early drafts than the author would like to admit.

Contents

Preface iii

Acknowledgements v

1 Introduction 1

2 Primality 3

Bibliography 5

Chapter 1

Introduction

Modular arithmetic is the setting for most of what follows. Definition 1.1 recalls fast exponentiation, the workhorse behind RSA and Diffie–Hellman alike (Cormen et al., 2009).

Example 1.1 (Fast modular exponentiation). To compute $a^n \bmod m$, write n in binary and square-and-multiply: repeated squaring reduces an $O(n)$-multiplication computation to $O(\log n)$ multiplications modulo m.

Algorithm A.1 makes this precise.

Algorithm A.1 Modular exponentiation by repeated squaring

Input: $a, n, m \in \mathbb{Z}$, $n \geq 0$
Output: $a^n \bmod m$

```
r ← 1
b ← a mod m
while n > 0 do
    if n mod 2 = 1 then
        r ← (r · b) mod m
    end if
    b ← (b · b) mod m
    n ← ⌊n/2⌋
end while
return r
```

Table 1.1 summarises the running time of the operations this chapter introduces.

Table 1.1: Running time of basic modular operations, n-bit inputs

Operation	Bit complexity
Addition mod m	$O(n)$
Multiplication mod m	$O(n^{1.58})$
Exponentiation mod m	$O(n^{2.58})$

Chapter 2

Primality

Example 2.1 (Fermat witness). If $\gcd(a, n) = 1$ and $a^{n-1} \not\equiv 1 \pmod{n}$, then n is composite and a is called a *Fermat witness* for n.

The Miller–Rabin test refines Example 2.1 into a probabilistic algorithm with one-sided error, described in Cormen et al. (2009) and analysed asymptotically in Knuth (1997).

Bibliography

T. H. Cormen, C. E. Leiserson, R. L. Rivest, and C. Stein. *Introduction to Algorithms.* MIT Press, 3 edition, 2009.

D. E. Knuth. *The Art of Computer Programming, Volume 2: Seminumerical Algorithms.* Addison-Wesley, 3 edition, 1997.