

Introduction

MATH2068 Number Theory & Cryptography Week 1 Lecture 1

University of Sydney
NSW 2006
Australia

28 July 2008



1. What is Cryptography?

Cryptography is the science of secret communication.

Starting with a message that anyone could read (the *plaintext*) one disguises or *encrypts* it, so that the resulting message (the *ciphertext*) can only be read by someone who knows how to *decrypt* it.

In mathematical parlance, encryption is a function from the set of possible plaintext messages to the set of possible ciphertexts, and decryption is the inverse function.

2. Basic objectives



Ideally, it should be very quick and easy to encrypt a message, and very quick and easy to decrypt it *if you know how*.

And it should be next to impossible to figure out how to decrypt a message if you have not been told how.

3. Old methods, new methods



People have been encrypting and decrypting messages since ancient times.

Until some 30 years ago, the methods that were employed were such that if you knew how to encrypt a message then you could easily work out how to decrypt one.

But it does not have to be this way: knowing how to compute values of a function does not necessarily tell you how to compute values of the inverse function.

4. Public key cryptosystems



In a public key cryptosystem, telling a person how to encrypt a message does not tell that person how to decrypt a message.

So you can tell everyone in the world how to encrypt messages, and keep the decryption process secret to yourself!

This is useful for banks, law firms, and the like: they can post the details of the encryption process on their web site, and then all their clients can securely transmit confidential information to them. The firm does not have to provide something special for every one of its clients.

In MATH2068 we will learn the theory underlying the two most widely used public key cryptosystems: **RSA** and **Elgamal**.

5. Why Number Theory?



In most cryptosystems, the first step is to convert the plaintext message into some numerical form.

One way is to replace the letters A to Z by the numbers 00 to 25. The message “MEETMETOMORROW” becomes a number: 1204041912041914121417171422.

This process is called *encoding* the message, and should not be confused with encryption.

Encoding is not a secret process: it is a completely open and standard procedure for putting messages into numerical form.

Once the message is a number, you can use number theory to disguise it.

6. Beginning Number Theory



Notation and terminology:

\mathbb{R} = set of all *real numbers*

\mathbb{Z} = set of all *integers*

$\mathbb{Z}^+ = \{1, 2, 3, \dots\}$ = set of all *positive integers*

$\mathbb{N} = \{0, 1, 2, 3, \dots\} = \mathbb{Z}^+ \cup \{0\}$ = set of *natural numbers*

$\mathbb{Q} = \{n/m \mid n \in \mathbb{Z}, m \in \mathbb{Z}^+\}$ = set of all *rational numbers*

Number theory is basically the study of the set \mathbb{N} .

We use braces $\{ \dots \}$ to indicate *sets*.

E.g., $\{3, 7, 9\}$ means the set whose elements are 3, 7 and 9.

7. More set notation



Notation like $\{xxxxx \mid zzzzz\}$ means

the set of all objects given by the formula $xxxxx$ such that the condition $zzzzz$ holds.

The vertical line $|$ means “such that”; $zzzzz$ is called the *membership condition*.

The symbol \in means “is an element of”.

The symbols \cup and \cap mean “union” and “intersection”.

$A \cup B = \{x \mid x \in A \text{ or } x \in B\}$, $A \cap B = \{x \mid x \in A \text{ and } x \in B\}$.

And $A \subseteq B$ means A is a subset of B .

(That is, every element of A is also an element of B .)

8. Peano's Postulates



These five basic properties of the natural numbers were formulated by Giuseppe Peano (1858 – 1932).

They can be regarded as the axioms of number theory.

Ultimately, every theorem of number theory can be proved using only these axioms.

P1: There is a natural number denoted by 0.

P2: Every $a \in \mathbb{N}$ has a “successor” which is also in \mathbb{N} .

P3: The number 0 is not the successor of any natural number.

P4: If $a \neq b$ then (successor of a) \neq (successor of b).

P5: If a subset A of \mathbb{N} has the two properties

(i) $0 \in A$,

(ii) the successor of every element of A is also in A ,
then A equals the whole of \mathbb{N} .

9. Induction



The 5th Postulate is the **Principle of Mathematical Induction** – the basic tool for proving most things about \mathbb{N} .

Suppose that $P(n)$ is some statement about the number n , and we want to prove that $P(n)$ is true for all n .

Define $A = \{ n \in \mathbb{N} \mid P(n) \text{ is true} \}$.

So we want to prove that $A = \mathbb{N}$.

According to P5 it is sufficient to prove

(i) $0 \in A$ (i.e. prove that $P(0)$ is true), and

(ii) $a \in A \Rightarrow (\text{successor of } a) \in A$. (i.e. $P(a) \Rightarrow P(a+1)$.)

10. Least Integer Principle



Every non-empty set of natural numbers has a least element.

This principle is just a reformulation of P5.

Let us use induction to prove the L.I.P.:

Assume $B \subseteq \mathbb{N}$ and B has no least element. (We show $B = \emptyset$.)

We use induction to prove (for all $n \in \mathbb{N}$)

$P(n)$: B does not contain $0, 1, 2, \dots, n$.

If 0 were in B then B would have a least element – since 0 is the least natural number.

This contradicts our hypothesis; so $P(0)$ is true.

Suppose that $P(a)$ is true. Then none of $0, 1, \dots, a$ are in B .

So if $a+1$ were in B then $a+1$ would be the least element of B .

So none of $0, 1, \dots, a+1$ are in B . So $P(a+1)$ is true.

By induction $P(n)$ holds for all n ; hence B is empty.

11. The Division Algorithm



The Least Integer Principle tells us that a decreasing sequence of natural numbers cannot go on forever.

There is no infinite sequence of natural numbers n_1, n_2, n_3, \dots with $n_1 > n_2 > n_3 > \dots$ (for otherwise the set $\{n_1, n_2, n_3, \dots\}$ would have no least element).

This enables us to prove the following theorem:

Theorem: Let $b \in \mathbb{Z}^+$. For every $a \in \mathbb{Z}$ there is a unique integer r such that $0 \leq r < b$ and $a = qb + r$ for some integer q .

We shall call the number r the **residue** of a modulo b (or the **remainder** on division of a by b .)

We give an **algorithm** (i.e. a recipe or procedure) for finding r .

12. Division Algorithm (continued)



Theorem: Let $b \in \mathbb{Z}^+$. For every $a \in \mathbb{Z}$ there is a unique integer r such that $0 \leq r < b$ and $a = qb + r$ for some integer q .

Suppose first that $a \geq 0$, and put $R_0 = a$.

If $R_0 \geq b$ put $R_1 = R_0 - b$. Then $R_1 \geq 0$ and $R_1 = a - b$.

If $R_1 \geq b$ put $R_2 = R_1 - b$. Then $R_2 \geq 0$ and $R_2 = a - 2b$.

If $R_2 \geq b$ put $R_3 = R_2 - b$. Then $R_3 \geq 0$ and $R_3 = a - 3b$.

Continue like this for as long as possible.

Since $R_0 > R_1 > R_2 > \dots$ we have a decreasing sequence of natural numbers. By the L.I.P. it must terminate.

So there is a number q such that $R_q < b$.

Put $r = R_q$. Then we have $0 \leq r < b$ and $r = a - qb$, as required.

(The case $a < 0$ can be done similarly: put $R_1 = a$, $R_2 = a + b$, $R_3 = a + 2b$, etc., continuing so long as $R_i < 0$.)