Faculty of Engineering Chulalongkorn University

DISCRETE MATHEMATICS
PART: Number Theory

The elementary theory of numbers should be one of the very best subjects for early mathematical instruction. It demands very little pervious knowledge, its subject matter is tangible and familiar; the processes of reasoning which it employs are simple, general and few; and it is unique among the mathematical sciences in its appeal to natural human curiosity.

G. H. Hardy (1877-1947)

PROLOQUE
BACKGROUND

CONTENTS

1. Floor and Ceiling functions

Let us recall two integral functions that are used in this section.

Definition 1: Floor function of a real numbers x, *denoted by* $\lfloor x \rfloor$, *is a function x to the greatest integer that is less than or equal to the number x.*

Definition 2: Ceiling function of a real numbers x, *denoted by* $\lceil x \rceil$, *is a function x to the smallest integer that is greater than or equal to the number x.*

Express those two functions by mathematical formula.

Floor function
Ceiling function

Exercise 1 (Prove or disprove these statements)

1.1 For any real number x, it is obtained that $\lfloor x \rfloor \leq x$.

1.2 For any real number x, it is obtained that $x - 1 < \lfloor x \rfloor$.

1.3 For any real number x, it is obtained that $x \leq \lceil x \rceil$.

1.4 For any real number x, it is obtained that $\lceil x \rceil < x + 1$.

1.5 For any real number x, any integer n, $x < n$ if and only if $\lfloor x \rfloor < n$.

1.6 For any real number x, any integer n, $n < x$ if and only if $n < \lfloor x \rfloor$.

1.7 For any real number x, any integer n, $x \leq n$ if and only if $\lceil x \rceil \leq n$.

1.8 For any real number x, any integer n, $n \leq x$ if and only if $n \leq \lceil x \rceil$.

1.9 For any real number x, any integer n, $n > x$ if and only if $n > \lceil x \rceil$.

Exercise 2 (Prove or disprove these statements and their inverses.

For any integers a and b,

2.1 if $a \leq b$ then $\lfloor a \rfloor \leq \lfloor b \rfloor$.

2.2 if $a \leq b$ then $\lceil a \rceil \leq \lceil b \rceil$.

Theorem 3: *Given an integer n and real numbers x and y, the following statements are tautology.*

1. $n = \lfloor n \rfloor = \lceil n \rceil$.
2. $\lceil x \rceil - \lfloor x \rfloor = 1$.
3. $\lfloor -x \rfloor = -\lceil x \rceil$.
4. $\lceil -x \rceil = -\lfloor x \rfloor$.
5. $\lfloor x \rfloor + n = \lfloor x + n \rfloor$.
6. $\lfloor x \rfloor + \lfloor y \rfloor \leq \lfloor x + y \rfloor$
7. $\lceil x + y \rceil \leq \lceil x \rceil + \lceil y \rceil$.

Exercise 3 Prove theorem 3.

Theorem 4: *Let F be a continuous and monotonically increasing function. If F satisfies the following condition:*

F(x) is an integer only if x is an integer,

then $\lfloor F(x) \rfloor = \lfloor F(\lfloor x \rfloor) \rfloor$ *and* $\lceil F(x) \rceil = \lceil F(\lceil x \rceil) \rceil$.

Proof:

For instance, the square root function of a real number satisfies the condition of the theorem and the function is a continuous & monotonically increasing, then it is concluded that

$$\sqrt{\lfloor x \rfloor} = \sqrt{\lfloor x \rfloor} \text{ and } \sqrt{\lceil x \rceil} = \sqrt{\lceil x \rceil}.$$

There is another way for identifying the floor and ceiling functions using their property.

Definition 5: Floor function of a real numbers x, *denoted by* $\lfloor x \rfloor$, *is a function x to integer n where there is a real number* ε *such that* $0 \le \varepsilon < 1$ *and x can be expressed as* $n + \varepsilon$.

Definition 6: Ceiling function of a real numbers x, *denoted by* $\lceil x \rceil$, *is a function x to integer m where there is a real number* δ *such that* $0 \le \delta < 1$ *and x can be expressed as* $m - \delta$.

2. Divisibility

This section, we introduce some notations for defining the divisibility of integers.

Definition 7: *For any integers m and n, where m is not zero, m* divides *n, denoted by* $m \mid n$ *(or n is divisible by m), if there is an integer c such that*

$$m \times c = n.$$

m is called a factor *of n, and*
n is said to be a multiple *of m.*

Theorem 8: *Let a, b, and c be three integers, then*

1. *if* $a \mid b$ *and* $a \mid c$ *then* $a \mid (b + c)$
2. *if* $a \mid b$ *then* $a \mid bc$ *for all integer c,*
3. *if* $a \mid b$ *and* $b \mid c$ *then* $a \mid c$ *(b is not zero).*

Proof:

3. Modularity

Definition 9: *A* modulo *n function, where n is a positive integer, is a function from an integer m to the remainder of m over n. This is usually denoted by m mod n.*

Express the modulo function by mathematical formula.

$m \bmod n =$

Theorem 10: *Let m and n be integers where n is positive,* $0 \leq m \bmod n < n$.

Proof:

Exercise 4 Prove these statements

4.1 For integers m, n, and c where m is not zero, if $m \mid nc$ and $\gcd(m, n) = 1$ then $m \mid c$.

4.2 For integers m, n, c, and d, if $m \mid c$ and $n \mid d$ then $mn \mid cd$.

4.3 For integers m, n and c, if $mc \mid nc$ then $m \mid n$.

LESSON 1
INTRODUCTION

Mathematics is the Queen of the sciences,
and number theory is the Queen of mathematics.
C.F.GAUSS (1777-1855)

CONTENTS

1.1. Introduction

We give you here a brief review of the fundamental ideas of number theory. We present some mathematical preliminaries of elementary number theory including the basic concepts and its results.

Number theory, in mathematics, is primarily the theory of *properties* of integers such as parity, divisibility, primality, additivity and multiplicativity etc. To appreciate the intrinsic mathematical beauty of the theory of numbers, we first investigate some of the properties of the integers.

1.2. Parity

It seem to be that parity (odd or even) is the simplest property of an integer. An integer is even, by definition, if it is divisible by 2, otherwise it is odd. In the binary representation, only the rightmost digit of the integer presents its parity, oddness is indicated by 1 or

evenness is indicated by 0. Euclid[1], about 350 B.C., has been proposed some well-known results about the parity property of integers which are as follows:

1. The sum of n even numbers is even, the sum of n odd numbers is even if n is even and the sum of n odd numbers is odd if n is odd.
2. The difference of n even numbers is even, the difference if n odd numbers is even if n is even and the difference of n odd numbers is odd if n is odd.

The parity property of integers has important applications in error detection and correction codes that are useful in computer design and communications.

Example 1.2.1: *Parity check* for error detection and correction code.
Let $x_1x_2x_3...x_n$ be a codeword (bit string) to be send from the main memory to the central processing unit of a computer. Of course, this code is no way an error detection and correction code. However, if an additional bit 1 (respect to 0) is added to the end of the codeword when the number of 1's in the codeword is odd (respect to even), then this new code is error detecting. For instance, if after transmission a codeword X becomes 1011101001010, then we know there is an error in the transmitted code. Of course, the new codes are still not error correction codes. However, if we arrange data in a rectangle and use parity bits for each row and column, then a single bit error can be corrected.

1	0	0	1	0	1	1	0	0
1	0	1	1	1	0	1	1	0
1	1	0	0	0	0	0	1	1
0	1	1	0	0	1	0	0	1
0	0	0	1	1	0	0	0	0
1	0	1	0	1	0	1	0	1
0	1	**0**	0	0	0	0	0	1
1	0	0	1	1	0	1	0	0
1	1	0	0	0	0	0	0	0

Figure 1.2.1: *Two-dimensional error checking by adding one additional bit into each codeword and one additional codeword. This can be verified that the third bit of the seventh codeword is wrong.*

[1] Euclid (about 350 B.C.) was the author of the most successful mathematical textbook ever written, namely his thirteen books of Elements, which has appeared in over a thousand different editions from ancient to modern times. It provides an introduction to plane and solid geometry as well as number theory. For example, some properties of the parity of integers are given in Propositions 21-29 of Book IX, Euclid's algorithm for computing the greatest common divisor of two and three positive integers is found in Book VII Proposition 2 and Proposition 3, respectively, and his proofs for the infinittude of primes and a sufficient condition for even number to be perfect are found in Book IX Proposition 20 and Proposition 36, respectively. The "Axiom-Definition-Theorem-Proof" style of Euclid's work has become the standard for formal mathematical writing up to the present day.

1.3. Primality

We first start by recalling the definition of prime and composite.

Definition 1.3.1: *A positive integer (greater than 1) that has only two distinct factors, 1 and itself is called* prime*; otherwise, it is called* composite*.*

For instance, 2, 3, 5, 7, 11, 13, 17, 19… are prime numbers. It is interesting to note that primes thin out: there are eight prime numbers between 1 and 20, but only three prime numbers between 80 and 100, namely 83, 89 and 97. This might lead one to suppose that there are only finitely many primes. However as Euclid proved 2000 years ago there are infinitely many primes. It is also interesting to note that

1. 2 is the only even prime, all the rest are odd.
2. (3, 5), (5, 7) and (11, 13) are the twin primes of the form (p, p+2) where p and p+2 are primes; two of the largest known twin primes (both found in 1995) are
    1. $570918348 \times 10^{5120} \pm 1$ with 5129 digits.
    2. $242206083 \times 2^{38880} \pm 1$ with 11713 digits.

    It has been proved by Chen that there are infinitely many pairs of integers (p, p+2), with p prime and p+2 a product of at most two primes.
3. There is only one prime triple of the form (p, p+2, p+4), namely (3, 5, 7).
4. The prime triples (5, 7, 11), (11, 13, 17), (17, 19, 23), (41, 43, 47), (101, 103, 107), (107, 109, 113), (191, 193, 197), (227, 229, 233), (311, 313, 317) and (347, 349, 353) are all of the form (p, p+2, p+6).
5. We do not know whether or not there are infinitely many prime triples of the form (p, p+4, p+6); the first ten triples of this form are as follows: (7, 11, 13), (13, 17, 19), (37, 41, 43), (67, 71, 73), (97, 101, 103), (103, 107, 109), (193, 197, 199), (223, 227, 229), (277, 281, 283) and (307, 311, 313).

The ancient Chinese mathematicians, even before Fermat [2](1601-1665), seem to have known that

$$p \in \text{Primes} \Rightarrow p \mid 2^p - 2.$$

However, there are some composites n that are not prime but satisfy this condition; for instance, $n = 341 = 11 \times 31$ is not prime, but $341 \mid 2^{341} - 2$. It is not an easy task to decide wherther or not a large number is prime.

---

[2] The great amateur French scientist Pierre de Fermat (1601-1665) led a quiet life practicing law in Toulouse, and producing high quality work in number theory and other areas of mathematics as a hobby. He published almost nothing, revealing most of his results in his extensive correspondence with friends, and generally kept his proofs to himself. Probably the most remarkable reference to his work is his *last Theorem* (called Fermat's Last Theorem), which asserts that if $n > 2$, the equation $x^n + y^n = z^n$ cannot be solved in integers x, y, z with $xyz \neq 0$. He claimed in a margin of his copy of Diophantus's book that he had found a beautiful proof of this theorem, but the margin was too small to contain his proof. Later on mathematicians everywhere in the world struggled to find a proof for this theorem but without success. The theorem remained open for more than 300 years and was finally settled in June 1995 by two English number theorists, Andrew Wiles, currently Professor at Princeton University, and Richard Taylor, a former student of Wiles and currently Professor at Harvard University; the original result of Wiles (with a hole in it) was first announced on 23 June 1993 at the Isaac Newton Institute in Cambridge.

In order to test that n is prime, one might test all the numbers (or just the primes) up to $n^{1/2}$. The number n has about log n bits in binary representation, then this would require about exp((1/2)log n). The current best algorithm for primality testing needs at most

$$(\log n)^{c \log\log\log n}$$

bit operations, where c is real positive constant.

Some results concerning primality properties:

- For all integers $n \geq 1$, there is a prime p such that $n < p \leq n!+1$.
- For a real number $x \geq 1$, there exists a prime between x and $2x$.
- If n is a composite, n has a prime divisor p such that $p \leq n^{1/2}$.

The Sieve of Eratosthenes[3]

This is an algorithm for finding all primes up to an integer n. Create a list of integers from 2 to n. For prime p,

- from 2 up to n, delete all multiples $p < pm \leq n$.
- Print the integers remaining in the list.

For instance, find primes up to 36.

	2	3	~~4~~	5	~~6~~
7	~~8~~	~~9~~	~~10~~	11	~~12~~
13	~~14~~	~~15~~	~~16~~	17	~~18~~
19	~~20~~	~~21~~	~~22~~	23	~~24~~
~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~

Figure 1.3.1: *Prime numbers that are less than 36 are 2, 3, 5, 7, 11, 13, 17, 19, 23, 29 and 31.*

1.4. Multiplicativity

Any positive integer $n > 1$ can be written uniquely in the following *prime factorization form*;

$$n = p_1^{\alpha 1} p_2^{\alpha 2} p_3^{\alpha 3} \ldots p_k^{\alpha k},$$

where $p_1 < p_2 < p_3 < \ldots < p_k$ are primes, and $\alpha_1, \alpha_2, \alpha_3, \ldots, \alpha_k$ are positive integers. This is the famous Fundamental Theorem of Arithmetic; it was possibly known to Euclid, but it was first clearly stated and proved by Gauss (1777-1855).

Example 1.4.1:

1999	=	1999	2000	=	24×53
2001	=	$3 \times 23 \times 29$	2002	=	$2 \times 7 \times 11 \times 13$
2003	=	2003	2004	=	$22 \times 3 \times 167$
2005	=	5×401	2006	=	$2 \times 17 \times 59$
2007	=	32×223	2008	=	23×251

[3] Eratosthenes of Cyrene (274-194 B.C.), librarian of the great library in Alexandria, was an ancient Greek astronomer and mathematician. He was the first to calculate the size of the Earth by making measurements of the angle of the Sun at two different places a known distance apart. His other achievements include measuring the tilt of the Earth's axis. But number theorists will always remember his wonderful prime sieve.

Fundamental Theorem of Arithmetic
An interesting theorem concerning the factors of any positive integer is recalled.

Theorem 1.4.2: *Every positive integer $n > 1$ can be written uniquely as the product of primes.*

Proof: The proof is separated into two parts. The first part is to show that there exists a product of primes corresponding to each positive integer greater than 1. The second part is to show that such product is unique.

1.5. Additivity

Some interest conjectures proposed by Ch. Goldbach 1690-1764 are as follows:

- Every odd integer > 7 is the sum of 3 odd primes.
- Every even integer > 4 is the sum of 2 odd primes.

For instance,

6 = 3+3	8 = 3+5
9 = 3+3+3	10 = 3+7 = 5+5
11 = 3+3+5	12 = 5+7
13 = 3+3+7 = 3+5+5	14 = 3+11
15 = 3+5+7 = 5+5+5	16 = 3+13 = 5+11.

It is obvious that the second conjecture implies the first.

1.6. Some interesting results

- *Carmichael* number, 1912 (CONJECTURED)
  A composite number n that satisfies $b^{n-1} \bmod n = 1$ for every positive integer b such that $\gcd(b,n) = 1$.

- There are infinitely many *Carmichael* numbers. (CONJECTURED)
  This conjecture was proved in 1992, by W.Alford, G. Granville and C.Pomerance. For instance, Carmichael numbers are 561, 1105, 1729, 2465, 2821, …

- The *Hardy-Ramanujan taxi* number
  Hardy and Ramanujan[4] have found that 1729 is the smallest positive integer expressible as a sum of two positive cubes in exactly two different ways, namely
  $$1729 = 1^3 + 12^3 = 9^3 + 10^3.$$
  (1729 is also the third smallest *Carmichael* number). Fourth powers, known to Euler (1707-1783), is
  $$635318657 = 59^4 + 158^4 = 133^4 + 134^4.$$

[4] Srinivasa Ramanujan (1887-1920) was one of India's greatest mathematical geniuses. He made substantial contributions to the analytical theory of numbers and worked on elliptic functions, continued fractions, and infinite series. Despite his lack of a formal education, he was well-known as a mathematical genius in Madras (the place where he lived) and his friends suggested that he should send his results to professors in England. Ramanujan first wrote to two Cambridge mathematicians E.W. Hobson and H.F. Baker trying to interest them in his results but neither replied. In January 1913 Ramanujan then wrote to Hardy a long list of unproved theorems, saying that "I have had no university education but I have undergone the ordinary school course. After leaving school I have been employing the spare time at my disposal to work at mathematics." It did not take long time for Hardy and Littlewood to conclude that Ramanujan was a man of exceptional ability in mathematics and decided to bring him to Cambridge. Ramanujan arrived in Cambridge in April 1914. Hardy was soon convinced that, in terms of natural talent, Ramanujan was in the class of Euler and Gausse. He worked with Hardy and made a series of outstanding breakthroughs in mathematics, and elected a Fellow on the Royal Society at the age of just 31. It was Littlewood who said that every positive integer was one of Ramanujan's personal friends. But sadly, in May 1917, Ramanujan fell ill; he returned to India in 1919 and died in 1920, at the early age of 33.

LESSON 2
THEORY OF DIVISIBILITY

We might call Euclid's method the granddaddy of all algorithms,
because it is the oldest nontrivial algorithm
that has survived to the present day.
D. E. Knuth

CONTENTS

2.1. Introduction

Divisibility has been studied for at least three thousand years. From before the time of *Pythagoras*, the Greeks considered questions about even and odd numbers, perfect and amicable numbers, and the primes, among many others; even today a few of these questions are still unanswered.

2.2. Greatest common divisor and Least common multiple

Definition 2.2.1: *Let a,b be integers, not both zero. The largest divisor d such that d|a and d|b is called the* greatest common divisor *of a and b, denoted by gcd(a,b).*

Integers a and b are called *relatively prime* if gdc(a,b) = 1. Integers $n_1,n_2,\ldots,n_k$ are called *pairwise relatively prime* if, whether $i \neq j$, we have gcd(n_i,n_j) = 1. If $a \mid bc$ and gcd(a,b) = 1, then $a \mid c$.

Definition 2.2.2: *Let a,b be integers, not both zero. The smallest multiple d such that d is a multiple of a and d is a multiple of b is called* the least common multiple *of a and b, denoted by lcm(a,b).*

Theorem 2.2.3: *Let a, b be integers, not both zero and let m = gcd(a, b). Suppose that x is a common divisor of a, b. Then x | m. (Every common divisor of a and b is a factor of the greatest common divisor.)*

Proof:

Theorem 2.2.4: *Let a, b be integers, not both zero and let m = lcm(a, b). Suppose that x is a common multiple of a, b. Then m|x. (Every common multiple of a and b is a multiple of the least common multiple.)*

Proof: Similar to the proof of Theorem 2.2.3. ■

Example 2.2.5: *Find gcd(1800, 420).*
Since $1800 = 2 \times 2 \times 2 \times 3 \times 3 \times 5 \times 5$ and $420 = 2 \times 2 \times 3 \times 5 \times 7$.
$\gcd(1800,420) = 2 \times 2 \times 3 \times 5 = 60$. That is $60 \mid 420$ and $60 \mid 1800$.
There is not any integer $m > 60$ and $m \mid 420$ and $m \mid 1800$.

Example 2.2.6: *Find lcm(1800,420).*
$\text{lcm}(1800,420) = 2 \times 2 \times 2 \times 3 \times 3 \times 5 \times 5 \times 7 = 12600$.
That is $1800 \mid 12600$ and $420 \mid 12600$.
There is not any integer $n < 12600$ and $1800 \mid n$ and $420 \mid n$.

Theorem 2.2.7: *Let a, b be integers, $a \times b = lcm(a, b) \times gcd(a, b)$.*

Proof: by definition of greatest common divisor and least common multiple. ■

2.3. Euclid's algorithm
In this section, we consider in Euclid's algorithm for the greatest common divisor. We start by recalling a definition of residue. We denote $r = a \bmod n$, for integer a and n, for

$$r = a - \lfloor a/n \rfloor n.$$

- Then r is the *residue* of a modulo n. It is clear that r is also an integer.

Theorem 2.3.1: *Given two integers a and b, where $b > 0$, there exist unique integers q and r such tha*

$a = bq + r$ where $0 \le r < b$.

Proof: Brief, the proof can be separated into two parts:
1. Show that there exist two integers q and r satisfying $0 \le r < b$.
2. Show that q and r are unique.

Exercise 5: Prove the following statement

Given two integers a and b where $b > 0$. From Euclid's division theorem, there exist two integers q and r, $a = bq + r$ and $0 \le r < b$.

5.1. Show that $r = a \bmod b$.

5.2. Show that $\gcd(a, b) = \gcd(b, r)$.

Given a, b two integers, find the *greatest common divisor* of a and b, $\gcd(a,b)$. For non-negative integers $a > b$, compute:

Let $r_0 = b$.

$r_1 = a \bmod b$.
i.e., $r_1 = a - q_0 r_0$.
We have that $\gcd(a,b) = \gcd(a \bmod b, b)$.
(If $r_1 = 0$, then $\gcd(a,b) = b$.)

$r_2 = b \bmod r_1$.
i.e., $r_2 = b - q_1 r_1$.
We also have that $\gcd(b,r_1) = \gcd(b \bmod r_1, r_1) = \gcd(a,b)$
if $r_2 = 0$, then $\gcd(a,b) = r_1$.

$r_3 = r_1 \bmod r_2$.
i.e., $r_3 = r_1 - q_2 r_2$.
We also have that $\gcd(r_1,r_2) = \gcd(r_3,r_2) = \gcd(a,b)$.
if $r_3 = 0$, then $\gcd(a,b) = r_2$.

…

$r_{n+1} = 0$. Thus $\gcd(a,b) = r_n$.

Example 2.3.2: *Using this algorithm for finding gcd(273,462).*

Let $a = 462$ and $b = 273 = r_0$.

i	r_i	q_{i-1}
	$a = 462$	
0	$b = 273$	
1	189	1
2	84	1
3	**21**	2
4	0	4

Then gcd(462,273) = 21.

Exercises 6:

6.1.Find gcd(340,250) by using Euclid's algorithm.

6.2.Find gcd(34,55) by using Euclid's algorithm.

2.4. Simple Continued Fraction

From the Euclid's algorithm, a and b are two integers, $a > b$, a can be represented as

$$\begin{aligned}
a &= q_0 r_0 + r_1 \\
a/b &= q_0 + (r_1 / r_0) && : b = r_0. \\
&= q_0 + r_1 / (q_1 r_1 + r_2) && : r_0 = q_1 r_1 + r_2. \\
&= q_0 + 1 / q_1 + (r_2/r_1) \\
&= q_0 + 1 / q_1 + (r_2/ q_2 r_2 + r_3) && : r_1 = q_2 r_2 + r_3. \\
&= q_0 + 1 / q_1 + (1/ q_2 + (r_3/r_2)) \\
&\ldots \\
&= q_0 + 1 / q_1 + (1/ q_2 + (1/ \ldots (1/q_n + 1/(r_{n+1}/r_n))\ldots))
\end{aligned}$$

Since $r_{n+1} = 0$, a/b can be illustrated as the following equation:

$$(a/b) = q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cfrac{1}{\ldots + \cfrac{1}{q_{n-1} + \cfrac{1}{q_n}}}}}$$

The simple continued fraction of a/b is usually denoted by

$$[q_0,q_1,q_2,\ldots,q_n].$$

Here we will give some interesting results:

Theorem 2.7.1: *Any rational number can be expressed as a finite simple continued fraction.*

Theorem 2.7.2: *Any irrational number can be expressed uniquely as an infinite simple continued fraction.*

An infinite simple continued fraction is said to be *periodic* if there exists integers k and m such that $q_{i+m} = q_i$ for all $i \geq k$, and k is called the *period* of the expansion. The periodic continued fraction is denoted by

$$[q_0, q_1, \ldots, q_k, \overline{q_{k+1}, \ldots, q_{k+m}}].$$

Theorem 2.7.3: *Any* periodic *simple continued fraction is a quadratic irrational.*

2.8. Continued Fraction Algorithm
The simple continued fraction of a real number x can be computed by

Let $x_0 = x$.

q_0	$=\lfloor x_0 \rfloor$	$x_1 = 1/(x_0-q_0)$
q_1	$=\lfloor x_1 \rfloor$	$x_2 = 1/(x_1-q_1)$
q_2	$=\lfloor x_2 \rfloor$	$x_3 = 1/(x_2-q_2)$
…		
q_n	$=\lfloor x_n \rfloor$	$x_{n+1} = 1/(x_n-q_n)$
q_{n+1}	$=\lfloor x_{n+1} \rfloor$	$x_{n+2} = 1/(x_{n+1}-q_{n+1})$

The algorithm stops when $q_{n+1} = x_{n+1}$.

Example 2.8.1: *Expand 1281/243 as a finite simple continued fraction.*
Let $x_0 = 1281/243$. Then we have

q_0	$=\lfloor 1281/243 \rfloor$	$= 5$	x_1	$= 1/(x_0-5) = 243/66$
q_1	$=\lfloor 243/66 \rfloor$	$= 3$	x_2	$= 1/(x_1-3) = 66/45$
q_2	$=\lfloor 66/45 \rfloor$	$= 1$	x_3	$= 1/(x_2-1) = 45/21$
q_3	$=\lfloor 45/21 \rfloor$	$= 2$	x_4	$= 1/(x_3-2) = 21/3$
q_4	$=\lfloor 21/3 \rfloor$	$= 7 = x_4$.		

The simple continued fraction of 1281/243 = [5, 3, 1, 2, 7].
That is

$$1281/243 = 5 + \cfrac{1}{3 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{7}}}}.$$

Example 2.8.2: *Expand $\sqrt{3}$ as a simple continued fraction.*

Let $x_0 = \sqrt{3}$. Then we have

$q_0 = \lfloor \sqrt{3} \rfloor = 1$
$x_1 = 1/(\sqrt{3}-1) = (\sqrt{3}+1)/2.$

$q_1 = \lfloor (\sqrt{3}+1)/2 \rfloor = 1$
$x_2 = 1/((\sqrt{3}-1)/2) = 2(\sqrt{3}+1)/(\sqrt{3}-1)(\sqrt{3}+1) = \sqrt{3}+1.$

$q_2 = \lfloor \sqrt{3}+1 \rfloor = 2$
$x_3 = 1/(\sqrt{3}+1-2) = 1/(\sqrt{3}-1) = \mathbf{(\sqrt{3}+1)/2}.$

$q_4 = \lfloor (\sqrt{3}+1)/2 \rfloor = 1$

$x_4 = 1/((\sqrt{3}-1)/2) = 2(\sqrt{3}+1)/(\sqrt{3}-1)(\sqrt{3}+1) = \mathbf{\sqrt{3}+1}$.

$q_5 = \lfloor \sqrt{3}+1 \rfloor = 2$
$x_5 = 1/(\sqrt{3}+1-2) = 1/(\sqrt{3}-1) = \mathbf{(\sqrt{3}+1)/2}$.
…

So, for $n = 1, 2, 3 \ldots$ we have that $q_{2n-1} = 1$ and $q_{2n} = 2$. Thus the *period* of the continued fraction expansion of $\sqrt{3}$ is 2. Finally, we get

$$\sqrt{3} = 1 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{\ddots}}}}}$$

The simple continued fraction of $\sqrt{3} = [1, \overline{1, 2}]$.

Exercises:

1. *Find the simple continued fraction of 34/55.*
2. *Find the simple continued fraction of √7.*

2.9. The Convergent of the Continued Fraction

Now, we define the n^{th} convergent term C_k of the expansion of a/b is as follow:

$$C_k = q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cfrac{1}{\ldots + \cfrac{1}{q_{k-1} + \cfrac{1}{q_k}}}}}$$

Let $C_0=q_0$.
Let $C_1=q_0+1/(q_1)$.
Let $C_2=q_0+1/(q_1+1/(q_2))$.
Let $C_k=q_0+1/(q_1+\ldots 1/(q_k))$

C_k is called the k^{th} *convergent* of a/b. Let us express C_k in the form of P_k and Q_k defined by

$C_0 = P_0/Q_0 = q_0/1$
$C_1 = P_1/Q_1 = (q_0q_1+1)/q_1$
$C_2 = P_2/Q_2 = (q_2(q_0q_1+1)+q_0)/(q_2q_1+1) = (q_2P_1+P_0)/(q_2Q_1+Q_0)$

…

$C_k = P_k/Q_k = (q_kP_{k-1}+P_{k-2})/(q_kQ_{k-1}+Q_{k-2})$.

That is $P_k = q_kP_{k-1}+P_{k-2}$, and
$Q_k = q_kQ_{k-1}+Q_{k-2}$.

Example 2.9.1: *Find the convergent terms of 1281/243.*
Since the continued fraction of 1281/243 = [5, 3, 1, 2, 7].
Then

$C_0 = P_0/Q_0$	$= q_0/1$	$= 5/1$
$C_1 = P_1/Q_1$	$= (q_0q_1+1)/q_1$	$= 16/3$
$C_2 = P_2/Q_2$	$= (q_2P_1+P_0)/(q_2Q_1+Q_0)$	$= 21/4$
$C_3 = P_3/Q_3$	$= (q_3P_2+P_1)/(q_3Q_2+Q_1)$	$= 58/11$
$C_4 = P_4/Q_4$	$= (q_4P_3+P_2)/(q_4Q_3+Q_2)$	$= 427/81 = 1281/243$.

Exercises:

3. *Find the simple continued fraction of (34/55), and write its C_n in the form of P_n/Q_n.*
4. *How can you explain the sequence of C_n.*

For any rational number a/b, it can be represented by a *finite* sequence of all convergent terms C_n, where $C_n=(a/b)$.

We can see for all $i > j$, C_i is closer to a/b than C_j. From the example above, $C_1 = 16/3 = 1296/243$ that is closer to 1281/243 than $C_0 = 1215/243$. In fact, the sequence of all convergent terms satisfy the condition that

- If $C_j < C_n$, then $C_{j+1} \geq C_n$.
- If $C_j > C_n$, then $C_{j+}1 \leq C_n$.

For instance, the i^{th} convergent term of 1281/243 can be expressed as

- C_0 = 53460/10692 $< C_4$ +2904/10692
- C_1 = 57024/10692 $> C_4$ -660/10692
- C_2 = 56133/10692 $< C_4$ +231/10692
- C_3 = 56376/10692 $> C_4$ -12/10692
- C_4 = 56364/10692 $< C_4$

LESSON 3
DIOPHANTINE EQUATIONS

I consider that I can understand an equation when,
I can predict the properties of its solutions,
Without actually solving it.
PAUL. A. M. DIRAC (1902-1984)

CONTENTS

3.1. Diophantine Equations

We consider the linear equation of two variables of the form

$$ax + by = c,$$

where a, b and c are all integers. We are interested in the integral solutions (*i.e.*, the solution that x and y are both integers). Some interesting results are recalled below.

Theorem 3.1.1: *Let a, b, c be integers. For the equation ax - by = c where c = gcd(a,b), we have that* $x=(-1)^{n-1}Q_{n-1}$ *and* $y=(-1)^{n-1}P_{n-1}$ *is the integral solution.*

Theorem 3.1.2: *Let a, b, c be integers. For the equation ax + by = c and gcd(a,b) = d and d | c, if* x_0 *and* y_0 *are the integral solution, other solutions are of the form*

$$x = x_0 + (b/d)t \text{ and } y = y_0 - (a/d)t$$

for any integers t.

Example 3.1.3: *Find the integral solution of 364x - 227y = 1.*

The simple continued fraction of 364/227 is [1, 1, 1, 1, 1, 10, 1, 3] see below:

$137 = 364 \bmod 227, \quad r_1 = 137 \quad q_0 = 1$
$90 = 227 \bmod 137, \quad r_2 = 90 \quad q_1 = 1$
$47 = 137 \bmod 90, \quad r_3 = 47, \quad q_2 = 1$
$43 = 90 \bmod 47, \quad r_4 = 43, \quad q_3 = 1$
$4 = 47 \bmod 43, \quad r_5 = 4, \quad q_4 = 1$
$3 = 43 \bmod 4, \quad r_6 = 3, \quad q_5 = 10$
$1 = 4 \bmod 3, \quad r_7 = 1, \quad q_6 = 1$
$1 = 3 \bmod 1, \quad r_8 = 0 \quad q_7 = 3.$

That is gcd(364,227) is 1.

Since 364/227 can be represented by a *finite* sequence of convergent terms as

C_0	C_1	C_2	C_3	C_4	C_5	C_6	C_7
1	2	3/2	5/3	8/5	85/53	93/58	364/227

The solution is $x = (-1)^6 58 = 58$, and $y = (-1)^6 93 = 93$.

That is $364(58) - 227(93) = 1$.

In the case that $ax + by = c$, where $d = \gcd(a,b)$ and $d \mid c$. This solution can be solved by finding the solution of $a_0x + b_0y = 1$ where $a = a_0 \times d$, $b = b_0 \times d$.

Since $d \mid c$, there exists an integer e such that $c = d \times e$. Rewrite

$$ax + by = c$$
$$a_0dx + b_0dy = d \times e$$
$$a_0x + b_0y = e$$

We have that $\gcd(a_0,b_0) = 1$, then the solution of $a_0x + b_0y = 1$ can be solved. Let x_0 and y_0 be the solution of $a_0x + b_0y = 1$. We also have that $a_0(e \times x_0) + b_0(e \times y_0) = e$. That is $x = e \times x_0$ and $y = e \times y_0$ are also the solution of $ax + by = c$.

Example 3.1.4: *Find the integral solution of 33x + 15y = 22.*

Since the greatest common divisor of 33 and 15 is 3, but 3 is not a divisor of 22, we can conclude that this equation does not has an integral solution. This can be proved by supposing that x and y are two integers satisfied the equation. Since 3 is the greatest common divisor of 33 and 15, then $11x+5y = 22/3$. This contradicts the supposition that x and y are both integers.

Example 3.1.5: *Find the solution of 24x – 15y = 21.*

Since gcd(24,15) = 3, we are going to solve the solution $24x – 15y = 3$.

$9 = 24 \bmod 15, \quad r_1 = 9, \quad q_0 = 1$
$6 = 15 \bmod 9, \quad r_2 = 6, \quad q_1 = 1$
$3 = 9 \bmod 6, \quad r_3 = 3, \quad q_2 = 1$

$0 = 6 \bmod 3$, $r_4 = 0$, $q_3 = 2$.

The simple continued fraction of 24/15 is [1, 1, 1, 2]. That is

$$24/15 = 1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{2}}}$$

Then 24/15 can be represented by the sequence of all convergent terms as follow:

C_0	C_1	C_2	C_3
1	2	3/2	8/5

The solution of $24x - 15y = 3$ is $x = (-1)^2 \times 2 = 2$ and $y = (-1)^2 \times 3 = 3$.
That is $24(2) - 15(3) = 3$.
The solution of $24x - 15y = 21$ is $x = 2(7) = 14$ and $y = 3(7) = 21$. That is $24(14) - 15(21) = 21$.
Then $x = 14$ and $y = 21$ is the integral solution of $24x - 15y = 21$.

Example 3.1.6: *Find the solution of $5x + 2y = 3$.*

Since gcd(2,5) =1 and the simple continued fraction of 5/2 is [2, 2]. Since $C_0 = 2$ and $C_1 = 5/2$, we have that $x = (-1)^0 \times 1$ and $y = (-1)^0 \times 2$ are the solution of $5x - 2y = 1$. We can conclude that $x = (-1)^0 \times 3 = 3$ and $y = (-1)^1 \times 6 = -6$ is the solution of $5x + 2y = 3$.
The other solutions are of the form

$$x = 3 + 2n \text{ and } y = -6 - 5n, \text{ for any integer } n.$$

Example 3.1.7: *Find the solution of $2x + 3y + 4z = 5$.*

This solution can be solved by first consider only x and y. The equation can be rewritten as

$$2x + 3y = 5 - 4z.$$

Since gcd(2,3) = 1, the solution of $2x + 3y = 1$ is

$$x = (-1)^1 = -1 \text{ and } y = (-1)^0 = 1.$$

Then for any integers z and n, $x = -1(5 - 4z) - 3n$ and $y = 1(5 - 4z) + 2n$ are all solutions of the equation.

Exercises:

5. *Find the solution of $1353x - 55y = 451$.*
6. *Find the solution of $7x + 21y + 35z = 8$.*

LESSON 4
THEORY OF CONGRUENCES

As with everything else, so with a mathematical theory:
beauty can be perceived, but not explained.
A. CAYLEY (1821-1895)

CONTENTS

4.1. Theory of Congruences

The relation of congruence has many properties in common with the relation of equality.

Theorem 4.1.1: *Let n be a positive integer. Then the congruence modulo n is*

- *Reflexive:* $a \equiv a \pmod{n}$ *for all a in* $\mathbb{Z}$.
- *Symmetric: If* $a \equiv b \pmod{n}$ *for all a, b in* $\mathbb{Z}$, *then* $b \equiv a \pmod{n}$.
- *Transitive: If* $a \equiv b \pmod{n}$ *and* $b \equiv c \pmod{n}$ *for all a, b and c in* $\mathbb{Z}$, *then* $a \equiv c \pmod{n}$.

The set of all integers x that $x \equiv a \pmod{n}$ is called the *residue class of a modulo n*, denoted by $[a]_n$.

The set of all residue classes modulo n is denoted by $\mathbb{Z}/n\mathbb{Z}$. For example, $\mathbb{Z}/4\mathbb{Z} = \{ [0]_4, [1]_4, [2]_4, [3]_4 \}$.

A *complete system of residues modulo n* is a set that contains exactly one element of each residue class modulo *n*. For instance, a complete system of residues modulo 4 is a set { 0, 1, 2, 3 }.

4.2. Modular Arithmetic

Let *a*, *b* and *n* be integers. For any integers *x* and *y*, if $x \equiv a \pmod{n}$ and $y \equiv b \pmod{n}$, we have that

- *x* can be represented as $sn + a$, with an integer *s*.
- *y* can be represented as $tn + b$, with an integer *t*.

Consider $x + y = (s + t)n + (a + b)$, or $x + y \equiv (a + b) \pmod{n}$. This implies that addition of integer in $[a]_n$ with an integer in $[b]_n$, is must be an element of the residue class $[a + b]_n$. *(It is similar for subtraction and multiplication.)* Then we can define arithmetic operations on $\mathbb{Z}/n\mathbb{Z}$ for any integer *n*.

$$[a]_n \ +_n \ [b]_n = [a + b]_n$$
$$[a]_n \ -_n \ [b]_n = [a - b]_n$$
$$[a]_n \ \times_n \ [b]_n = [a \times b]_n \qquad \text{for all integers } a, b.$$

Example 4.2.1: *Find the complete system of residues modulo 3.*

The congruence classes is

$[0]_3$ = { …, -9, -6, -3, 0, 3, 6, 9, …}
$[1]_3$ = { …, -8, -5, -2, 1, 4, 7, 10, … }
$[2]_3$ = { …, -7, -4, -1, 2, 5, 8, 11, … }

Consider $23 \in [2]_3$ and $12 \in [0]_3$, $23 + 12 = 35 \in [2]_3$.
$23 - 12 = 11 \in [2]_3$.
$23 \times 12 = 276 \in [0]_3$.

Let *a*, *b*, *c* and *d* be integers such that $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, we can conclude that

- $(a + c) \equiv (b + d) \pmod{n}$
- $(a - c) \equiv (b - d) \pmod{n}$
- $(a \times c) \equiv (b \times d) \pmod{n}$
- $(a)^n \equiv (b)^n \pmod{n}$

Example 4.2.2: *Show that $3 \mid (2^n - 1)$ if n is an even number.*

Since 2 and -1 are in the same residue class modulo 3.
We have $2 \equiv -1 \pmod{3}$. That is $2^n \equiv (-1)^n \pmod{3}$. If *n* is an even number, $(-1)^n = 1$, and $2^n \equiv 1 \pmod{3}$ or $2^n - 1 \equiv 0 \pmod{3}$.

Exercises:

7. *Find an integer x such that $2^{33} \equiv x \pmod{7}$.*

LESSON 5
DISTRIBUTION OF PRIME NUMBERS

I know numbers are beautiful. If they aren't beautiful, nothing is.
Paul Erdös (1913-1996)

CONTENTS

5.1. Introduction

In fact, the theory of numbers is essentially the theory of prime numbers. In this section, we shall introduce some important results about the distribution of prime numbers. More specifically, we shall study some functions of a real or complex variable that are related to te distribution of prime numbers. We start by introduce some basic concepts and results on primes.

5.2. Mersenne Primes and Fermat Numbers

Some basic results on Mersenne[5] primes.

Definition 5.2.1: *A number is call* Mersenne *number if it is of the form* $M_p = 2^p - 1$, *where p is a prime. If a Mersenne number is a prime, it is called* Mersenne prime.

For instance, the following numbers are all Mersenne numbers as well as Mersenne primes, but $2^{11} - 1$ is only a Mersenne number, not a Mersenne prime, since $2^{11} - 1 = 2047 = 23 \times 89$ is a composite.

- p = 2 $2^2 - 1 = 3$
- p = 3 $2^3 - 1 = 7$
- p = 5 $2^5 - 1 = 31$
- p = 7 $2^7 - 1 = 127$
- p = 11 $2^{11} - 1 = 2047$
- p = 13 $2^{13} - 1 = 8191$
- p = 17 $2^{17} - 1 = 131071$.

There are some probabilistic estimates for the distribution of Mersenne primes; for example, in 1983, Wagstaff proposed the following conjecture:

Conjecture 5.2.2: *Let the number of Mersenne primes less than x be* $\pi_M(x)$, *then*

$$\pi_M(x) \approx (e^\gamma / \ln 2) \times \log \log x = (2.5695\ldots) \ln \ln x,$$

where $\gamma = 0.5772\ldots$ *is Euler's constant.*

Conjecture 5.2.3: *The expected number of Mersenne primes* M_q *with* $x < q < 2x$ *is about*

$$e^\gamma = 1.7806\ldots .$$

Conjecture 5.2.4: *The probability that* M_q *is a prime is about*

$$(e^\gamma / \ln 2) \times (\ln aq / \ln 2),$$

where a is 2 if $q \equiv 3 \pmod 4$ *or a is 6 if* $q \equiv 1 \pmod 4$.

Conjecture 5.2.5: *Let q be the* n^{th} *prime such that* M_q *is a Mersenne prime. Then*

$$q \approx (3 / 2)^n.$$

---

[5] Marin Mersenne (1588-1648) was a French monk, philosopher and mathematician who provided a valuable channel of communication between such contemporaries as Descartes, Fermat, Galileo and Pascal: "to inform Mersenne of a discovery is to publixh it throughout the whole of Europe". Mersenne stated in *Cognitata Physico-Mathematica* but without proof that M_p is prime for $p = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257$ qnd for no other primes $p < 257$. Of course, Mersenne's list is not quite correct. It took over 300 years to totally settle this claim made by Mersenne, and finally in 1947, it was shown that Mersenne made five errors in his work; namely, M_{67} and M_{257} are composite and hence should be deleted from the list, whereas M_{61}, M_{89} and M_{107} are all primes and hence should be added to the list.

No.	p	Digits in M_p	discoverer
8	31	10	Euler, 1772
35	1398269	420921	Armengard & Woltman, 1996
36	2976221	895932	Spence & Woltman, 1997
37	3021377	909526	Clarkson, Woltman, Kurowski et al, 1998

Figure 3.2.1: *Until now, there are 37 known Mersenne primes.*

Definition 5.2.6: *Numbers of the form* $F_n = ((2)^2)^n + 1$*, whether prime or composite, are called* Fermat numbers. *A Fermat number is called* prime Fermat number *if it is prime. A Fermat number is called a* composite Fermat number *if it is composite.*

These special numbers obey the simple recursion:

$$F_{n+1} = (F_n - 1)^2 + 1 \text{ or } F_{n+1} - 2 = F_n(F_n - 2)$$

which leads to the interesting product;

$$F_{n+1} - 2 = F_0F_1F_2\ldots F_n.$$

In other words, $F_{n+1} - 2$ is divisible by all lower Fermat numbers:

$$F_{n-k} \mid (F_{n+1} - 2), \text{ where } 1 \le k \le n.$$

Fermat in 1640 conjectured, in a letter to Mersenne, that all numbers of the form F_n were primes after he had verified it up to $n = 4$; but Euler in 1732 found that the fifth Fermat number is not a prime, since F_5 is the product of two primes 641 and 6700417. Later, it was found that F_6, F_7, and many others are not primes. To date, the Fermat numbers until F_{11} have been completely factored. The smallest Fermat numbers which are not known to be prime or composite are F_{24} and F_{28}.

There are still many open problems related to the Fermat numbers; some of them are the following;

- Are there infinitely many *prime* Fermat numbers?
- Are there infinitely many *composite* Fermat numbers?
- Is every Fermat number *square-free*?

5.3. Euler's function

Let us first introduce Euler's (totient) function proposed by Euler[6].

Definition 5.3.1: *Let n be a positive number. Euler's function, ϕ-function, $\phi(n)$ is defined to be the number of positive integers k less than n which are relatively prime to n:*

$$\phi(n) = \sum_{1 \le k < n \text{ where } gcd(k,n)=1} 1.$$

For example, we have, by definition, the following Euler's function:

n	$\phi(n)$
1	1
2	1
3	2
4	2
5	4
6	2
7	6
8	4
9	6
10	4
100	40
101	100
102	32
103	102

Figure 3.3.1: *Example of $\phi(n)$*

Theorem 5.3.2: *Let n be a positive integer. Then $\phi(n)$ is multiplicative. i.e.,*

$$\phi(mn) = \phi(m)\phi(n).$$

Theorem 5.3.3: *If p is a prime, then $\phi(p) = p - 1$. More generally, if n is a prime power, p^u, then $\phi(p^u) = p^u - p^{u-1}$. If n is a composite, then*
$\phi(n) = p_1^{u1}(1-(1/p_1))p_2^{u2}(1-(1/p_2)) \times \ldots \times p_k^{uk}(1-(1/p_k))$
with $n = p_1^{u1}p_2^{u2}\ldots p_k^{uk}$ (prime factorization form).

---

[6] Leonhard Euler (1707-1783), a key figure in 18th century mathematics, was the son of a minister from the vicinity of Basel, Switzerland, who, besides theology, also studied mathematics. He spent most of his life in the Imperial Academy in St. Peterburg, Russia (1727-1741 and 1766-1783). "Prolific" is the word most often applied to Euler, from whom gushed forth a steady flow of work from the age of 19 on, even though he was blind for the last 17 years of his life. (He also had 13 children.) Mainly known for his work in analysis, Euler wrote a calculus textbook and introduced the present-day symbols for e, ϕ and i. Among Euler's discoveries in number theory is the law of quadratic reciprocity, which connects toe solbability of the congruences $x^2 \equiv p \pmod{q}$ and $y^2 \equiv q \pmod{p}$, where p and q are distinct primes, although it remained for Gauss to provide the first proof. Euler also gave a marvelous proof of the existence of infinitely many primes based on the divergence of the harmonic series $\sum n^{-1}$.

Theorem 5.3.4: *If n is a composite, then*

$$\phi(n) = p_1^{u1}(1-(1/p_1))p_2^{u2}(1-(1/p_2)) \times \ldots \times p_k^{uk}(1-(1/p_k))$$

with $n = p_1^{u1}p_2^{u2}\ldots p_k^{uk}$ *(prime factorization form).*

Suppose that n is known to be the product of two distinct primes p and q. Then knowledge of p and q is equivalent to knowledge of $\phi(n)$, since $\phi(n) = (p-1)(q-1)$. However, there is no known efficient method to compute $\phi(n)$ if the prime factorization of n is not known. This interesting fact is useful in the RSA public-key cryptography, which will be studied in detail later.

5.4. Carmichael's function

The following function, first proposed by the American mathematician Carmichael[7], is a very useful number theoretic function.

Definition 5.4.1: *Let n be a positive integer. Carmichael's λ-function, λ(n) is defined as follows*:

- $\lambda(n) = \phi(n)$ *if n is a prime.*
- $\lambda(p^u) = \phi(p^u)$ *for* $p = 2$ *and* $u \leq 2$ *and for* $p \geq 3$.
- $\lambda(2^u) = \phi(2^u)/2$ *for* $u \geq 3$
- $\lambda(n) = lcm(\lambda(p_1^{u1}), \lambda(p_2^{u2}), \ldots, \lambda(p_k^{uk}))$, *with* $n = p_1^{u1}p_2^{u2}\ldots p_k^{uk}$.

For example, we have, by definition, the following Carmichael's function:

n	$\phi(n)$
1	1
2	1
3	2
4	2
5	4
6	2
7	6
8	2
9	6
10	4
100	20
101	100
102	16
103	102

Figure 3.4.1: *Example of λ (n)*

[7] Robert D. Carmichael (1879-1967) was born in Goodwater, Alabama. He received his BA from Lineville College in 1898 and his Ph.D. in 1911 from Princeton University. His thesis, written under G.D. Birkhoff, was considered the first significant American contribution to differential equations. Perhaps best known in number theory for his Carmichael numbers, Carmichael's function, and Carmichael's theorem, Carmichael worked in a wide range of areas, including real analysis, differential equations, mathematical physics, group theory, and number theory. It is also worthwhile mentioning that Carmichael published two very readable little books about number theory: *Theory of Numbers* in 1914 and *Diophantine Analysis* in 1915, both published by John Wiley & Sons., New York.

Example 5.4.2: *Let* $n = 65520 = 2^4 \times 3^2 \times 5 \times 7 \times 13$, *and* $a = 11$. *Then* $\gcd(n,a) = 1$ *and we have*
$\phi(n) = 8 \times 4 \times 6 \times 12 = 13824$.
$\lambda(n) = \text{lcm}(4, 6, 4, 6, 12) = 12$.

5.5. Prime distribution function

We first investigate the occurrence of the prime numbers among the positive integers. The following are some counting results of the number of primes in each hundred positive integers.

- From 1 to 100, there are 25 prime numbers:
  2 3 5 7
  11 13 17 19
  23 29
  31 37
  41 43 47
  53 59
  61 67
  71 73 79
  83 89
  97
- From 1 to 1000, each 100 contains
  25-21-16-16-17-14-16-14-15-14
- From 106 to 106+1000, each 100 contains
  6-10-8-8-7-7-10-5-6-8
- From 1012 to 1012+1000, each 100 contains
  4-6-2-4-2-4-3-5-1-6

Except 2 and 3, any two consecutive primes must have a distance that is at least equal to 2. Pairs of primes with this shortest distance are called *twin primes*. Of the positive integers less than or equal to 100, there are eight twin primes, namely, (3, 5), (5, 7), (11, 13), (17, 19), (29, 31), (41, 43), (59, 61), (71, 73). There are however arbitrarily long distances between two consecutive primes, that is, there are arbitrarily long sequences of consecutive composite numbers.

Theorem 5.5.1: *For an arbitrary positive number* $n > 1$, *the following* $n-1$ *numbers*
$n!+2, n!+3, n!+4, \ldots, n!+n$
are all composite numbers.

The occurrence of primes is very irregular. However, when the large scale distribution of primes is considered, it appears in many ways quite regular and obey simple laws. In the study of these laws, a central question is "How many primes are there less than or equal to x"? The answer to this question leads to a famous expression, $\pi(x)$, which is defined as follows:

Definition 5.5.2: *Let x be a positive real number ≥ 1. Then π(x), is defined as follows:*

$$\pi(x) = \sum_{p \le x,\ p \text{ prime}} 1.$$

That is $\pi(x)$ is the number of primes less than or equal to x; it is also called the *prime counting function* or the *prime distribution function*.

For example, the following table shows the value of $\pi(x)$ and $\pi(x) / x$.

x	$\pi(x)$	$\pi(x) / x$
10	4	0.4
10^2	25	0.25
10^3	68	0.168
10^4	1229	0.1229
10^5	9692	0.9692
10^6	78498	0.78498
10^7	664579	0.664579
10^8	5761455	0.5761455
10^9	50847534	0.50847534
10^{10}	455052511	0.455052511
…	…	…
10^{20}	2220819602560918840	0.02220819602560918840

Figure 5.5.1: *Prime Distribution Function*

The numerical values of the ratio $\pi(x) / x$ suggest that

$$\lim_{x \to \infty} (\pi(x) / x) = 0.$$

It must be, however, pointed out that even though almost all positive integers are composites, there are infinitely many prime numbers, as proved by Euclid 2000 years ago. So, in term of $\pi(x)$, Euclid's theorem on the infinitude of prime numbers can then be re-formulated as follows:

$$\lim_{x \to \infty} \pi(x) = \infty.$$

Some interesting results concerning the distribution of prime numbers are showed as follows:

1789 Legendre proposed (using the sieve of Eratosthenes)

$$\pi(x) = \pi(\sqrt{x}) - 1 + \Sigma\ \mu(d) \lfloor n/d \rfloor$$

where the sum is over all divisors d of the product of all primes $p \le x$, and $\mu(d)$ is the *Mobius* function.

1808 Legendre proposed $\pi(x) \approx x / (\ln x - A(x))$ with for large x, $A(x) = 1.08366\ldots$

1850 Chebyshev shown that $\lim_{x \to \infty} A(x) = 1.08366\ldots$ and

$$0.92129 (x / \ln x) < \pi(x) < 1.1056 (x / \ln x)$$

for large x.

1892 Sylvester shown that

$$0.95695 (x / \ln x) < \pi(x) < 1.04423 (x / \ln x)$$

for every sufficiently large x.

5.6. Approximation of $\pi(x)$

Although the distribution of prime numbers among the integers is very irregular, the prime distribution function is surprising well behaved. Let us see the following table.

x	$\pi(x)$	$x / \ln x$	$\pi(x)/(x/\ln x)$
10	4	4.3…	0.93…
10^2	25	21.7…	1.15…
10^3	68	144.8…	1.16…
10^4	1229	1085.7…	1.13…
10^5	9692	8685.8…	1.13…
10^6	78498	72382.5…	1.08…
10^7	664579	620420.5…	1.07…
10^8	5761455	5428680.9…	1.06…
10^9	50847534	48254942.5…	1.05…
10^{10}	455052511	434294481.9…	1.04…
…	…	…	…
10^{20}	2220819602560918840	2171472409516259138.2…	1.02…

Figure 5.6.1: *Approximation of the prime distribution function*

It can be easily seem from the table above that the approximation $x / \ln x$ gives reasonably accurate estimates of $\pi(x)$. In fact, the study of this approximation leads to the following famous theorem of number theory, and indeed of all mathematics.

Theorem 5.6.1: (Prime number theorem, postulated by Gauss[8]) *$\pi(x)$ is asymptotic to $x/\ln x$. That is*

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

5.7. Fermat's Little Theorem

We shall introduce some important results in linear congruence equation. Our first result will be Fermat's Little Theorem.

Theorem 5.7.1: (Fermat's Little theorem) *Let a be a positive integer, and p be a prime number. If gcd(a, n) = 1 then*

$$a^{p-1} \equiv 1 \pmod{p}.$$

Proof: First note that the residues modulo p of a, $2a$, $3a$, …, $(p-1)a$ are 1, 2, 3, …,$(p-1)$ in some order, because no two of them can be equal. So, if we multiply them together, we get

[8] Carl Friedrich Gauss (1777-1855), the greatest mathematician of all time (Prime of Mathematics), waqs the son of a German bricklayer. It was quickly apparent that he was a child prodigy. In fact, at the age of three he corrected an error in his father's payroll. Gauss made fundamental contributions to astronomy including calculating the orbit of the asteroid Ceres. On the basis of this calculation, Gauss was appointed director of the Gottingen Observatory. He laid the foundations of modern number theory with his book *Disquisitiones Arithmeticae* in 1801. Gauss conceived most of his discoveries before the age of 20, but spent the rest of his life polishing and refining them.

$$a \times 2a \times 3a \times \ldots \ (p-1)a \equiv 1 \times 2 \times 3 \times \ldots \times (p-1) \pmod{p}$$
$$\equiv (p-1)! \pmod{p}$$

This means that

$$(p-1)! \times a^{p-1} \equiv (p-1)! \pmod{p}$$

or

$$a^{p-1} \equiv 1 \pmod{p}.$$

There is a more convenient and more general form of Fermat's Little Theorem:

$$a^{p} \equiv a \pmod{p},$$

for any positive integer a. The very important consequence for compositeness is as follows:

Corollary 5.7.2: (Converse of Fermat's Little theorem, 1640) *Let n be an odd positive integer. If gcd(a, n) = 1 and*

$$a^{n-1} \text{ not} \equiv 1 \pmod{n},$$

then n is composite.

Remark 5.7.3: *F_5 (5^{th} Fermat number) is composite. This can be proved by using the converse of his theorem.*

Let $a = 3$ and let $n = F_5$. Since $2^{32} = 4294967296$ and $F_5 = 2^{32} + 1$, and since we have that

$$3^{4294967296} \text{ not} \equiv 1 \pmod{4294967297},$$

we can conclude that F_5 is composite (in fact, F_5 is composed of 641 and 670417).

5.8. Euler's Theorem

Based on Fermat's Little Theorem, Euler established a more general result in 1760:

Theorem 5.8.1: (Euler's theorem) *Let a and n be positive integers with gcd(a, n) = 1. Then*

$$a^{\phi(n)} \equiv 1 \pmod{n}, \text{ where } \phi(n) \text{ is Euler's function.}$$

Example 5.8.2: *Find 11^8 mod 24.*
Let $a = 11$ and $n = 24$. Since all relatively primes < 24 of 24 are 1, 5, 7, 11, 13, 17, 19 and 23. Then $\phi(24) = 8$. We can conclude that $11^8 \equiv 1 \pmod{24}$. That is $11^8 \bmod 24 = 1$.

5.9. Carmichael's Theorem

The smallest integer r such that $a^{r} \equiv 1 \pmod{n}$ is called the *order* of an element a modulo n. It can be difficult to find the order of an element a modulo n but sometimes it is possible to improve the theorem by proving that every integer a modulo n must have an order smaller than the $\phi(n)$. This order is actually the number $\lambda(n)$.

Theorem 5.9.1: (Carmichael's theorem) *Let a and n be positive integers with gcd(a, n) = 1. Then*

$$a^{\lambda(n)} \equiv 1 \pmod{n}, \text{ where } \lambda(n) \text{ is Carmichael's function.}$$

Example 5.9.2: *Find 11^8 mod 24.*
Let $a = 11$ and $n = 24$. Since $\lambda(24) = 2$. We can conclude that $11^2 \equiv 1 \pmod{24}$. That is $11^8 \bmod 24 = 1 = (11^2)^4 \bmod 24$.

LESSON 6
CRYPTOGRAPHY

Cryptography relies heavily on number-theoretic tools.
In particular, systems based on (assumed) hardness of problems
In number theory, such as factoring and discrete log,
form an important part of modern cryptography.
R. MOTWANI & P. RAQGHAVAN

CONTENTS

6.1. Introduction

Cryptologo is composed of two domains of study. *Cryptography* (from the Greek *Kryptos*, "hidden", and *graphein*, "to write") is the study of the principles and techniques by which information can be concealed in cyphertexts and later revealed by legitimate users employing the secret key, but in which it is either impossible or computationally infeasible for an unauthorized person to do so. Cryptanalysis (from the Greek *kryptos* and *analyein*, "to loosen") is the science of recovering information from ciphertexts without knowledge of the key. Both terms are subordinate to the more general term cryptology. That is

$$\text{Cryptology} =^{\text{def}} \text{Cryptography} + \text{Cryptanalysis},$$

and

$$\text{Cryptology} =^{\text{def}} \text{Encryption} + \text{Decryption}.$$

Modern cryptography, however, is the study of "mathematical" systems for solving the following two main types of security problems:

- Privacy
- Authentication

Privacy: A privacy system prevents the extraction of information by unauthorized parties from messages transmitted over a public and often insecure channel, thus assuring the sender of a message that it will only be read by the intended receiver.

Authentication An authentication system prevents the unauthorized injection of messages into a public channel, assuring the receiver of a message of the legitimacy of its sender.

Some notations that we use in cryptography described as the followings:

- *Message space* $\mathcal{M}$: A set of strings (plaintext messages) over some alphabet, that needs to be encrypted.
- *Ciphertext space* $\mathcal{C}$: A set of strings (ciphertexts) over some alphabet, that has been encrypted.
- *Key space* $\mathcal{K}$: A set of strings (keys) over some alphabet, which includes the encryption key e_k and the decryption key d_k.
- *The encryption process*: E: $E_{ek}(M) = C$.
- *The decryption process*: D: $D_{dk}(C) = M$.
- The algorithm E and D must have the property that $D_{dk}(C) = D_{dk}(E_{ek}(M)) = M$.

There are essentially two different types of cryptographic systems: *Secrete-key* (or symmetric cryptosystems) and *Public-key* (asymmetric cryptosystems).

6.2. Secret-key cryptosystems

In a conventional secret-key cryptosystem, the same key ($e_k = d_k = k$) called the *secret-key* is used in both encryption and decryption; this is why we call it secret-key cryptosystem, or symmetric cryptosystem.

The sender uses an invertible transformation E_k defined by $E_k : \mathcal{M} \to \mathcal{C}$. To produce the cipher text. That is for $M \in \mathcal{M}$ and for $C \in \mathcal{C}$, we have $C = E_k(M)$, and transmits it over the public insecure to the receiver. The key should be transmitted to the legitimate receiver for decryption but via a secure channel. Since legitimate receiver knows the key k, he can decrypt C by a transformation $D_k = (E_k)^{-1}$ defined by $D_k : \mathcal{C} \to \mathcal{M}$, and obtain $D_k(C) = M$. The problem is illustrated by the following figure.

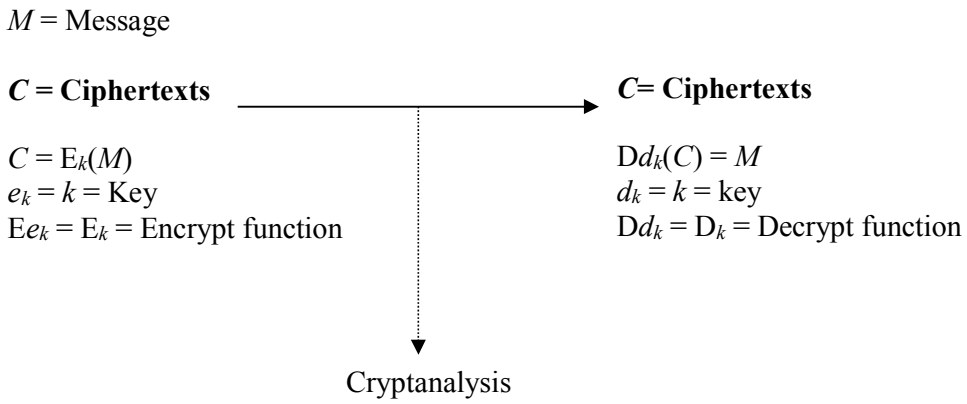

Figure 6.2.1: *Secret-key cryptosystem*

6.2.1. Stream (bit) ciphers

In this technique, the message units are bits, and the key is usually produced by a random bit generator. The plaintext is encrypted on a bit-by-bit basis.

Let k = Random string
M = Message
C = Ciphertexts

- Encryption algorithm = $M \oplus k \rightarrow C$
- Decryption algorithm = $C \oplus k \rightarrow M$.

6.2.2. Monographic (character) ciphers

Earily ciphers were based on transforming each letter of the plaintext into a different letter to produce the ciphertext. First of all, let us define the numerical equivalents of the 26 English letters, since our operations will be on the numerical equivalents of letters, rather than the letters themselves. The following is a typical character ciphers, used by Caesar[9].

- Encryption algorithm: $C \equiv M + k \pmod{26}$, where $0 \le M < 26$
- Decryption algorithm: $M \equiv C - k \pmod{26}$, where $0 \le C < 26$

Other techniques are of the form:

- Encryption algorithm: $C \equiv aM + b \pmod{26}$, where $0 \le M < 26$
- Decryption algorithm: $M \equiv a^{-1}(C - b) \pmod{26}$, where $0 \le C < 26$

6.2.3. Polygraphic (block) ciphers

[9] Julius Caesar (100-44 BC) was a celebrated Roman general and statesman. The Caesar cipher was apparently used by Caesar, but he was also supposed to have invented the cipher himself.

Monographic ciphers can be made more secure by splitting the plaintext into groups of letters (rather than a single letter) and then performing the encryption and decryption on these groups of letters. This block technique is called *block ciphering*. Block cipher is also called a *polygraphic cipher*. Block ciphers may be described as follows:

Let M_i = the i^{th} block message ($n \times 1$ matrix)
A = $n \times n$ matrix
B = secret key = $(B_1, B_2, B_3, \ldots, B_n)^T$
A^{-1} = inverse matrix of A.
Encryption algorithm : $C_i \equiv AM_i + B \pmod N$.
Decryption algorithm: $M_i \equiv A^{-1} (C_i - B) \pmod N$.
Then $C = (c_1, c_2, c_3, \ldots, c_n)^T$.

6.2.4. Exponentiation ciphers

The exponentiation cipher, invented by Pohlig and Hellman in 1976, may be described as follows:

Let p be a prime number,
M the numerical equivalent of the plaintext, where each letter of the plantext is replaced by its two digit equivalent.

Subdivide M into blocks M_i such that $0 < M_i < p$. Let k be an integer with $0 < k < p$ and $\gcd(k,p-1) = 1$. Then the encryption transformation for M_i is defined by

$$C_i \equiv E_k (M_i) \equiv (M_i)^k \pmod p,$$

and the decryption transformation for C_i is defined by

$$M_i = D_{k'} (C_i) \text{ c } C_i^{k'} \equiv (M_i^k)^{k'} \equiv M_i \pmod p,$$

where $k \times k' \equiv 1 \pmod p$.

6.3. Public-key cryptosystems

In their famous paper "*New Directions in Cryptography*", the electrical engineers Diffie and Hellman, both in the Department of Electrical Engineering at Standford University at the time, proposed a seminal idea to solve the key-exchange problem which led to the birth of public-key cryptography. In a public-key cryptosystem, the encryption key e_k and decryption key d_k are different.

Since e_k is only used for encryption, it can be made public: only d_k must be kept a secret for decryption. To distinguish public-key cryptosystems fro secret-key cryptosystems, e_k is called the *public-key* and d_k is called the *private-key*: only yhe key used in secret-key cryptosystems is called the *secret-key*. The implementation of public-key cryptosystems is based on *trapdoor one-way functions.*

Definition 6.3.1: *Let S and T be finite sets. A one-way function f: S→T is an invertible function satisfying*

1. *f is easy to compute, that is given $x \in S$, $y = f(x)$ is easy to compute.*
2. *f^1 the inverse function of f, is difficult to compute, that is, given $y \in T$, $x = f^1(y)$ is difficult to compute.*

3. *f^{-1} is easy to compute when a secret string of information associated with the function becomes available.*

Example 6.3.2: *The following functions are one-way functions:*

1. *$f: pq \rightarrow n$ where p and q are prime numbers. The computation of f^{-1} is an extremely difficult problem (this is well-known difficult integer factorization problem); there is no efficient algorithm to determine p and q from their product pq, the fastest algorithm is Number Field Seive (NFS).*
2. *$f_{g,N}$: $x \rightarrow g^x \bmod N$. This function is easy to compute since the modular exponentiation $g^x \bmod N$ can be performed. The computation of $f^{-1}$is an extremely difficult problem (this is a well-known difficult discrete logarithm problem).*
3. *$f_{k,N}$: $x \rightarrow x^k \bmod N$, where $N = pq$ with p and q are prime numbers, and $kk' \equiv 1 \pmod{\phi(N)}$. The computation of f^{-1} (i.e., the k^{th} root of x modulo N) is difficult. However, if k' is given, f can be easily inverted, since $(x^k \bmod N)^{k'} \bmod N = x$.*

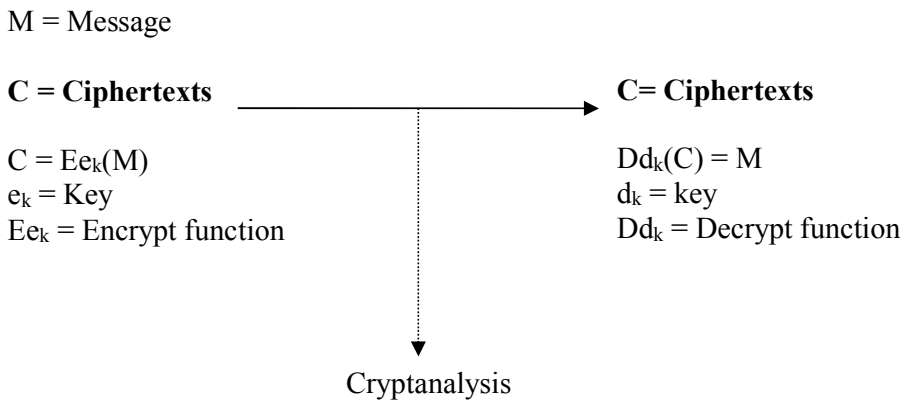

Figure 6.3.1: *Public-key cryptosystem*

6.4. RSA Public-key Cryptosystem

In 1978, three MIT researchers Rivest, Shamir and Adleman proposed the first practical public-key cryptosystem, now widely known as the RSA public-key cryptosystem. The RSA cryptosystem is based on the following assumption:

> *It is not so difficult to find two large prime numbers, but it is very difficult to factor a large composite into its prime factorization form.*

An example of the one-way function if the form used in the RSA cryptosystem is as follows:

$$f(x) \equiv x^k \pmod{N}$$

where $N = pq$ (p and q are two large primes),
$k > 1$, and $\gcd(k, \lambda(N)) = 1$.
$\lambda(N) = \text{lcm}(p-1, q-1) = (p-1)(q-1) / \gcd(p-1, q-1)$.

We assume that k and N are publicly known, but p, q and $\lambda(N)$ are not. In the RSA cryptosystem, we are essentially only interested in the case where the modulus $N = pq$. In general, instead of considering the modulus $N = pq$, we can consider an arbitrary integer N, which is larger than any number representing a message block.

The inverse function of $f(x)$ is defined by

$$f^{-1}(y) \equiv y^{k'} \pmod{N} \text{ with } kk' \equiv 1 \pmod{\lambda(N)}.$$

It should be easy to compute $f^{-1}(y) \equiv y^{k'} \pmod{N}$ if k' is known, provided that $f^{-1}(y)$ exists. The assumption underlying the RSA cryptosystem is that it is hard to compute $f^{-1}(y)$ without knowing k.

We use an useful result:

Theorem 6.4.1: *If N is a product of two distinct primes, then for all a,*

$$a^{\lambda(N)+1} \equiv a \pmod{N}.$$

Example 6.4.2: *Let $p = 2$ and $q = 3$, we have that $\lambda(6) = \text{lcm}(1,2) = 2$. That is for all integers a,*

$$a^3 \equiv a \pmod{6}.$$

For instance, $a = 2$, $8 \equiv 2 \pmod 6$,
$a = 3$, $27 \equiv 3 \pmod 6$,
$a = 4$, $64 \equiv 4 \pmod 6$, etc…
Now, let us introduce $N = 3 \times 4$ (i.e., $p = 3$ and $q = 4$), then

$$\begin{aligned} \lambda(12) &= \text{lcm}(\lambda(3), \lambda(4)) \\ &= \text{lcm}(3-1, \phi(4)) \\ &= 2. \end{aligned}$$

That is $a^3 \equiv a \pmod{12}$ for all integers a. But this is not true, since $10^3 \equiv 4 \pmod{12}$.

Let k and N have been chosen suitably as follows:
$N = pq$ with p and q distinct primes
$a^{kk'} \equiv a \pmod N$, for all a, k and k' are both integers.
From the theorem, it follows immediately that
$a^{m\lambda(N)+1} \equiv a \pmod N$,
what is exactly the form needed for RSA cryptosystem.

6.5. Example of RSA Public-key Cryptosystem

The first step is to select two prime numbers.

- $p = 47$ and $q = 71$ are two primes used in the RSA cryptosystem.

The second step is to compute:

- $N = 47 \times 71 = 3337$.
- $\lambda(3337) = \text{lcm}(46,70) = 3220$.

The third step is to determine the public-key and private key:

- We try to factorize $m\lambda(3220)+1$ for $m = 1, 2, 3, \ldots$ until we find a "good" factorization that can be used to obtain suitable k and k'.
- for $m = 25$, $25\lambda(3220)+1 = 80501 = 79 \times 1019$
  and $1019 = (79)^{-1} \bmod 3220$.
- Then $k = 79$ and $k' = 1019$.

Note: The public key is $N = 3337$
The public-key is $k = 79$
The private-key is $k' = 1019$

To encrypt the number:

- (The number must be less than 3337.)
- For example, we want to encrypt the number 688, then
- Compute $688^{79} \bmod 3337 = 1570$.

To decrypt the number:

- The number can be decrypted by the private-key 1019,
- that is compute $1570^{1019} \bmod 3337 = 688$.
- So the original number is obtained.

Note 6.5.1: *The most recent record of NFS, by a group led by Herman te Riele in August 1999 of random 155 digit number RSA-155 (512 bits) which can be written as the product of two 78-digit primes.*

Conjecture 6.5.2: ***(RSA-CONJECTURE)*** *Any method of breaking the RSA cryptosystem must be as difficult as factoring. There are some other possible attacks on the RSA cryptosystem, which include:*

1. *Wiener's attack on the short RSA private-key (k'). It is important that the private-key should be large (nearly as many bits as the modulus N); otherwise, there is an attack due to Wiener and based on properties of continued fractions, that can be find the private-key in time polynomial in the length of the modulus N, and hence decrypt the message.*

2. *Iterated encryption or fixed-point attack (Meijer and Pinch): Suppose k has order r in the multiplicative group modulo λ(N). Then* $x = k^r \equiv 1 \pmod{\lambda(N)}$, *so*
3. $M^x \equiv M \pmod{\lambda(N)}$.
4. *This is just the* r^{th} *iterate of the encryption of M. So we must ensure that r is large.*