

MAT 7003 : Mathematical Foundations

(for Software Engineering)

J Paul Gibson, A207

`paul.gibson@it-sudparis.eu`

<http://www-public.it-sudparis.eu/~gibson/Teaching/MAT7003/>

The Rest

<http://www-public.it-sudparis.eu/~gibson/Teaching/MAT7003/L10-TheRest.pdf>

Some Revision on:

- Number Theory
- Coding Theory
- Combinatorics

Number Theory - *the study of the integers and functions/relations closed over the integers.*

Divisibility

We say that a *divides* b if there is an integer k such that $ak = b$. This is denoted $a \mid b$.

For example:

$7 \mid 63$ because $7 \cdot 9 = 63$

A consequence of this definition is that every number divides zero since $a \cdot 0 = 0$ for every integer a .

If a divides b , then b is a *multiple of a* . For example, *63 is a multiple of 7.*

Number Theory - number theory is full of questions that are easy to pose, but incredibly difficult to answer

Perfect Numbers

A number is *perfect* if it equals the sum of its positive integral divisors, excluding itself.

For example, $6 = 1+2+3$ and $28 = 1+2+4+7+14$ are perfect numbers. On the other hand, 10 is not perfect because $1+2+5=8$, and 12 is not perfect because $1+2+3+4+6=16$.

Euclid characterized all the even perfect numbers around 300 BC. But is there an odd perfect number? More than two thousand years later, we still don't know! All numbers up to about 10^{300} have been ruled out, but no one has proved that there isn't an odd perfect number waiting just over the horizon.

Number Theory – properties of divisibility

1. If $a \mid b$, then $a \mid bc$ for all c .
2. If $a \mid b$ and $b \mid c$, then $a \mid c$.
3. If $a \mid b$ and $a \mid c$, then $a \mid sb + tc$ for all s and t .
4. For all $c \neq 0$, $a \mid b$ if and only if $ca \mid cb$.

TO DO: Prove these

Number Theory – primes and composites

A number $p > 1$ with no positive divisors other than 1 and itself is called a **prime**.

Every other number greater than 1 is called **composite**.

For example, 2, 3, 5, 7, 11, and 13 are all prime, but 4, 6, 8, and 9 are composite.

The number 1 is considered neither prime nor composite. This is just a matter of definition, but reflects the fact that 1 does not behave like a prime in many contexts, such as the Fundamental Theorem of Arithmetic, which we'll come to shortly.

Number Theory: Division Theorem

Let n and d be integers such that $d > 0$.

Then there exists a unique pair of integers q and r such that $n = qd + r$ and $0 \leq r < d$.

The remainder r in the Division Theorem is denoted $n \text{ rem } d$. In other words, $n \text{ rem } d$ is the remainder when n is divided by d . For example, $32 \text{ rem } 5$ is the remainder when 32 is divided by 5, which is 2. Similarly, $-11 \text{ rem } 7 = 3$, since $-11 = (-2) \cdot 7 + 3$.

There is a remainder operator built into many programming languages. For example, the expression “ $32 \% 5$ ” evaluates to 2 in Java, C, and C++. However, all these languages treat negative numbers strangely

TO DO: Check how your favourite programming language calculates $\%$ with negative parameter values

Number Theory: Division Theorem

There are a couple of naming problems related to the Division Theorem:

- First, the theorem is often called the “Division Algorithm”, even though it is not an algorithm in the modern sense.
- Second, some people use the notation “mod” (which is short for “modulo”) instead of “rem”. This is unfortunate, because “mod” has been used by mathematicians for centuries in a confusingly similar context, which we’ll come to shortly.

Number Theory: Division Theorem

Famous Problems in Number Theory

Fermat's Last Theorem Do there exist positive integers x , y , and z such that

$$x^n + y^n = z^n$$

for some integer $n > 2$? In a book he was reading around 1630, Fermat claimed to have a proof, but not enough space in the margin to write it down. Wiles finally gave a proof of the theorem in 1994, after seven years of working in secrecy and isolation in his attic. His proof did not fit in any margin.

Goldbach Conjecture Is every even integer greater than or equal to 4 the sum of two primes? For example, $4 = 2 + 2$, $6 = 3 + 3$, $8 = 3 + 5$, etc. The conjecture holds for all numbers up to 10^{16} . In 1939 Schnirelman proved that every even number can be written as the sum of not more than 300,000 primes, which was a start. Today, we know that every even number is the sum of at most 6 primes.

Twin Prime Conjecture Are there infinitely many primes p such that $p + 2$ is also a prime? In 1966 Chen showed that there are infinitely many primes p such that $p + 2$ is the product of at most two primes. So the conjecture is known to be *almost* true!

Primality Testing Is there an efficient way to determine whether n is prime? An amazingly simple, yet efficient method was finally discovered in 2002 by Agrawal, Kayal, and Saxena. Their paper began with a quote from Gauss emphasizing the importance and antiquity of the problem even in his time— two centuries ago.

Factoring Given the product of two large primes $n = pq$, is there an efficient way to recover the primes p and q ? The best known algorithm is the "number field sieve", which runs in time proportional to:

$$e^{1.9(\ln n)^{1/3}(\ln \ln n)^{2/3}}$$

This is infeasible when n has a couple hundred digits or more.

Number Theory: The Greatest Common Divisor

The **greatest common divisor** of a and b is the largest number that is a divisor of both a and b . It is denoted $\gcd(a, b)$.

For example, $\gcd(18, 24) = 6$.

The greatest common divisor turns out to be quite useful for reasoning about the integers. Specifically, the quantity $\gcd(a, b)$ is a valuable piece of information about the relationship between the numbers a and b .

Number Theory: Linear combinations and the GCD

An expression of the form $sa + tb$ is called an (integer) **linear combination** of a and b

THEOREM

The greatest common divisor of a and b is equal to the smallest positive linear combination of a and b .

For example:

The greatest common divisor of 52 and 44 is 4.

Also, 4 is a linear combination of 52 and 44: $6 \cdot 52 + (-7) \cdot 44 = 4$

Furthermore, no linear combination of 52 and 44 is equal to a smaller positive integer.

TO DO: Prove the theorem

Number Theory: Properties of the GCD

1. *Every common divisor of a and b divides $\gcd(a, b)$.*
2. *$\gcd(ka, kb) = k \cdot \gcd(a, b)$ for all $k > 0$.*
3. *If $\gcd(a, b) = 1$ and $\gcd(a, c) = 1$, then $\gcd(a, bc) = 1$.*
4. *If $a \mid bc$ and $\gcd(a, b) = 1$, then $a \mid c$.*
5. *$\gcd(a, b) = \gcd(b, a \bmod b)$.*

Number Theory: The Fundamental Theorem of Arithmetic

Theorem (Fundamental Theorem of Arithmetic). *Every positive integer can be written in a unique way as a product of primes*

TO DO: Can you prove this?

HINT: First prove the lemmas –

If p is a prime and $p \mid ab$, then $p \mid a$ or $p \mid b$.

Let p be a prime. If $p \mid a_1 a_2 \dots a_n$, then p divides some a_i

Number Theory: The Prime Number Theorem

The Prime Number Theorem

Let $\pi(x)$ denote the number of primes less than or equal to x . For example, $\pi(10) = 4$ because 2, 3, 5, and 7 are the primes less than or equal to 10. Primes are very irregularly distributed, so the growth of π is similarly erratic. However, the Prime Number Theorem gives an approximate answer:

$$\lim_{x \rightarrow \infty} \frac{\pi(x)}{x / \ln x} = 1$$

Thus, primes gradually taper off. As a rule of thumb, about 1 integer out of every $\ln x$ in the vicinity of x is a prime.

The Prime Number Theorem was conjectured by Legendre in 1798 and proved a century later by de la Vallée Poussin and Hadamard in 1896. However, after his death, a notebook of Gauss was found to contain the same conjecture, which he apparently made in 1791 at age 15. (You sort of have to feel sorry for all the otherwise “great” mathematicians who had the misfortune of being contemporaries of Gauss.)

Number Theory: Modular Arithmetic

Gauss said that a is **congruent** to b **modulo** n if $n \mid (a - b)$. This is denoted $a \equiv b \pmod{n}$.

For example:

$29 \equiv 15 \pmod{7}$ because $7 \mid (29 - 15)$.

Here's another way to think about congruences: *congruence modulo n defines a partition of the integers into n sets so that congruent numbers are all in the same set.* For example, suppose that we're working modulo 3. Then we can partition the integers into 3 sets as follows:

$$\begin{aligned} & \{ \dots, -6, -3, 0, 3, 6, 9, \dots \} \\ & \{ \dots, -5, -2, 1, 4, 7, 10, \dots \} \\ & \{ \dots, -4, -1, 2, 5, 8, 11, \dots \} \end{aligned}$$

Number Theory: Congruences

For all $n > 0$

1. $a \equiv a \pmod{n}$
2. $a \equiv b \pmod{n}$ implies $b \equiv a \pmod{n}$
3. $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$ implies $a \equiv c \pmod{n}$
4. $a \equiv b \pmod{n}$ implies $a + c \equiv b + c \pmod{n}$
5. $a \equiv b \pmod{n}$ implies $ac \equiv bc \pmod{n}$
6. $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$ imply $a + c \equiv b + d \pmod{n}$
7. $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$ imply $ac \equiv bd \pmod{n}$

TO DO: Can you prove these?

Congruences and remainders

1. $a \equiv (a \text{ rem } n) \pmod{n}$
2. $a \equiv b \pmod{n}$ if and only if $(a \text{ rem } n) = (b \text{ rem } n)$

Number Theory: Riemann Hypothesis

Riemann Hypothesis. This conjecture first appeared in a sketchy paper by Bernhard Riemann in 1859 and is now one of the most famous unsolved problem in mathematics. The formula for the sum of an infinite geometric series says:

$$1 + x + x^2 + x^3 + \dots = \frac{1}{1-x}$$

Substituting $x = \frac{1}{2^s}$, $x = \frac{1}{3^s}$, $x = \frac{1}{5^s}$, and so on for each prime number gives a sequence of equations:

$$\begin{aligned}1 + \frac{1}{2^s} + \frac{1}{2^{2s}} + \frac{1}{2^{3s}} + \dots &= \frac{1}{1-1/2^s} \\1 + \frac{1}{3^s} + \frac{1}{3^{2s}} + \frac{1}{3^{3s}} + \dots &= \frac{1}{1-1/3^s} \\1 + \frac{1}{5^s} + \frac{1}{5^{2s}} + \frac{1}{5^{3s}} + \dots &= \frac{1}{1-1/5^s} \\&\text{etc.}\end{aligned}$$

Multiplying together all the left sides and all the right sides gives:

$$\sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p \in \text{primes}} \left(\frac{1}{1-1/p^s} \right)$$

The sum on the left is obtained by multiplying out all the infinite series and applying the Fundamental Theorem of Arithmetic. For example, the term $1/300^s$ in the sum is obtained by multiplying $1/2^{2s}$ from the first equation by $1/3^s$ in the second and $1/5^{2s}$ in the third. Riemann noted that every prime appears in the expression on the right. So he proposed to learn about the primes by studying the equivalent, but simpler expression on the left. In particular, he regarded s as a complex number and the left side as a function, $\zeta(s)$. Riemann found that the distribution of primes is related to values of s for which $\zeta(s) = 0$, which led to his famous conjecture:

The Riemann Hypothesis: Every nontrivial zero of the zeta function $\zeta(s)$ lies on the line $s = 1/2 + ci$ in the complex plane.

Coding Theory

Coding theory, sometimes called algebraic coding theory, deals with the design of error-correcting codes for the reliable transmission of information across noisy channels.

It makes use of classical and modern algebraic techniques involving finite fields, group theory, and polynomial algebra.

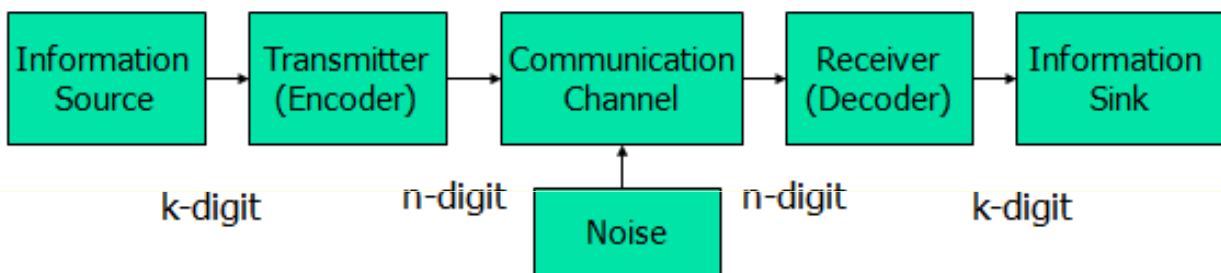
It has connections with other areas of discrete mathematics, especially number theory and the theory of experimental designs

Coding Theory

History: Ode to Shannon

- Clearly everything started with Shannon's paper titled "A Mathematical Theory of Communication".
- Foundations of Information Theory, as well as Coding Theory. Notion of Entropy of Information.
- Two models of communication: Noiseless and Noisy.
- Goal in former: Compress information to take advantage of redundancy in data. Examples such as: Entropy of English.

Coding Theory



Coding Theory

Definitions

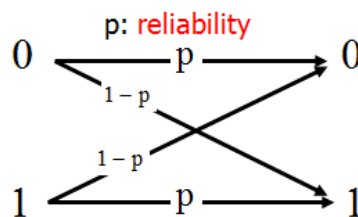
- **Digit** : 0 or 1(binary digit)
- **Word** : a sequence of digits
 - Example : 0110101
- **Binary code** : a set of words
 - Example : 1. {00,01,10,11} , 2. {0,01,001}
- **Block code** : a code having all its words of the same length
 - Example : {00,01,10,11}, 2 is its length
- **Codewords** : words belonging to a given code
- **|C|** : Size of a code C(#codewords in C)

Coding Theory

Assumptions about channel

- $\{0,1\}^n \rightarrow$ **Channel** $\rightarrow \{0,1\}^n$
 1. Receiving word by word
 $011011001 \rightarrow$ **Channel** $\rightarrow 011, 011, 001$
 2. Identifying the beginning of 1st word
 3. The probability of any digit being affected in transmission is the same as the other one.

Binary symmetric channel



In many books, p denotes crossover probability. Here crossover probability(error prob.) is $1-p$

Coding Theory: The effects of error correction and detection

1. No error detection and correction

Let $C = \{0,1\}^{11} = \{00000000000, \dots, 11111111111\}$

Reliability $p = 1 - 10^{-8}$ Transmission rate = 10^7 digits/sec

Then $\Pr(\text{a word is transmitted incorrectly}) = 1 - p^{11} \approx 11 \times 10^{-8}$

$11 \times 10^{-8} (\text{wrong words/words}) \times 10^7 / 11 (\text{words/sec}) = 0.1$ wrong words/sec

1 wrong word / 10 sec

6 wrong words / min

360 wrong words / hr

8640 wrong words / day

Coding Theory: The effects of error correction and detection

2. parity-check digit added (Code length becomes 12)

Any single error can be detected !

(3, 5, 7, ..errors can be detected too !)

$\Pr(\text{at least 2 errors in a word}) = 1 - p^{12} - 12 \times p^{11}(1-p) \approx 66 \times 10^{-16}$

So $66 \times 10^{-16} \times 10^7 / 12 \approx 5.5 \times 10^{-9}$ wrong words/sec

one word error every 2000 days!

**The cost we pay is to reduce a little
information rate + retransmission (after error
detection!)**

Coding Theory: The effects of error correction and detection

3. 3-repetition code

Any single error can be corrected !

Code length becomes 33 and information rate becomes $1/3$

Task : design codes with

- reasonable information rates
- low encoding and decoding costs
- some error-correcting capabilities

Coding Theory: Hamming Codes

In the late 1940's Claude Shannon was developing information theory and coding as a mathematical model for communication.

At the same time, Richard Hamming, a colleague of Shannon's at Bell Laboratories, found a need for error correction in his work on computers.

Parity checking was already being used to detect errors in the calculations of the relay-based computers of the day, and Hamming realized that a more sophisticated pattern of parity checking allowed the correction of single errors along with the detection of double errors.

The codes that Hamming devised marked the beginning of coding theory. These codes remain important to this day, for theoretical and practical reasons as well as historical.

TO DO: Read up on Hamming Codes to get an idea of how they work

Combinatorics – Permutations and Combinations

Many problems in probability theory require that we count the number of ways that a particular event can occur.

For this, we study the topics of *permutations and combinations*.

Classic Example : Birthday Problem

How many people do we need to have in a room to make it a favorable bet (probability of success greater than $1/2$) that two people in the room will have the same birthday?

Combinatorics – Permutations and Combinations

Number of people	Probability that all birthdays are different
20	.5885616
21	.5563117
22	.5243047
23	.4927028
24	.4616557
25	.4313003

TO DO: Verify these probabilities are correct

Combinatorics – Permutations and Combinations

Let A be any finite set. A **permutation** of A is a one-to-one mapping of A onto itself.

The total number of permutations of a set A of n elements is given by $n * (n-1) * \dots * 1$

We call this function **factorial** n , written $n!$

(Stirling's Formula) The sequence $n!$ is asymptotically equal to

$$n^n e^{-n} \sqrt{2\pi n} .$$

Combinatorics – Stirling approximations

n	$n!$	Approximation	Ratio
1	1	.922	1.084
2	2	1.919	1.042
3	6	5.836	1.028
4	24	23.506	1.021
5	120	118.019	1.016
6	720	710.078	1.013
7	5040	4980.396	1.011
8	40320	39902.395	1.010
9	362880	359536.873	1.009
10	3628800	3598696.619	1.008

Combinatorics

Binomial Coefficients

The number of distinct subsets with j elements that can be chosen from a set with n elements is denoted by $\binom{n}{j}$, and is pronounced “ n choose j .” The number $\binom{n}{j}$ is called a *binomial coefficient*. This terminology comes from an application to algebra

For integers n and j , with $0 < j < n$, the binomial coefficients satisfy:

$$\binom{n}{j} = \binom{n-1}{j} + \binom{n-1}{j-1} .$$

Combinatorics

TO DO: Read up on the following (related to statistical analysis) –

- **Bernoulli Trials**
- **Binomial Probabilities**
- **Binomial Distributions**
- **Binomial Expansion**
- **Hypothesis Testing**
- **Inclusion-Exclusion Principle**
- **Choosing a Sample Space**