Discrete Mathematics

Mon 5-7pm, Thur 2-5pm
Room 5, Via Eudossiana

Prof. Stefano Capparelli
Dept SBAI
Università di Roma La Sapienza
Italy
stefano.capparelli@uniroma1.it

Abstract

This is the journal of class activities for Discrete Mathematics 2019 recorded daily. The more current version of this journal is at https://sites.google.com/a/uniroma1.it/stefanocapparelli/insegnamenti/sezione1

1 Monday, Feb 25, Lecture 1,2

A short introduction to the problems and methods of Discrete Mathematics. The student that will attend class regularly will find that it is sufficient to study on my class note Appunti di Matematica Discreta (Esculapio ed. 2019)(referred to as *Notes* below) (an English version is available on Esculapio's cloud https://textincloud.editrice-esculapio.com/product/capparelli-english.

Otherwise, it might be necessary to see one or more of the following textbooks:

a. Baldoni, Ciliberto, Piacentini Cattaneo: Aritmetica, Crittografia e Codici, Springer 2006

b. Biggs, Discrete Mathematics, Oxford, 2002

c. Brualdi, Introductory Combinatorics, Prentice Hall, 1999.

d. Cerasoli, Eugeni, Protasi, Elementi di Matematica Discreta, Zanichelli 1988

e. Knuth, The art of Computer Programming, Vol. I Addison Wesley, 1997

f. Graham, Knuth, Patashnik, Concrete Mathematics, Addison Wesley 1988

g. Schroeder, Number Theory in Science and Communication, Springer 2009

I particularly recommend reading Schroeder's book because it contains a lot of motivations for the study of Number Theory and Discrete Mathematics.

There will be a class test at about the middle of the term and a second one toward the end of the course. Besides these there will be regular exam periods through the academic year.

Let's start with a puzzle.

Consider the sequence of natural numbers:

$$1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, \ldots$$

Let's decide to cross out, for example, every other number, and, of the remaining numbers get the partial sums, thus obtaining a new sequence.

1	~~2~~	3	~~4~~	5	~~6~~	7	~~8~~	9	~~10~~	11
1		4		9		16		25		36

The numbers appearing in the bottom row are the squares of natural numbers. What if we cross out every third number:

1	2	~~3~~	4	5	~~6~~	7	8	~~9~~	10	11	~~12~~
1	~~3~~		7	~~12~~		19	~~27~~		37	~~48~~	
1			8			27			64		

We get cubes.

We do not worry about proofs for now. In general we do: I recommend you take 15 min to watch https://www.ted.com/talks/eduardo_saenz_de_cabezon_math_is_forever#t-569375

Back to our puzzle. Questions:

1. What if we cancel every forth term of the original sequence?
2. If, instead of canceling all terms at a regular distance (1,2,3,etc) as above, we erase those in position 1,3,6,10,15,... what happens then?
3. What if we started with a different sequence, say $\{1, 1, 1, 1, 1, \ldots\}$? or $\{2, 5, 8, 11, 14, 17, \ldots\}$?

If you can, write a program that allows the input of a numerical sequence and then, following the above rules, outputs another sequence as above. Second Puzzle. Start with any number (integer) then if it is even, divide it by 2, while if it is odd multiply it by 3 and add 1. Repeat this procedure a number of times. Try this for small numbers, say less than 30. What happens in the long run?

Equivalence of the Induction Principle and the Well-ordering principle. Proofs by induction

Sections 1.1 and 1.2 of Notes.

2 Monday, Feb 28, Lecture 3,4,5

Euclidean division. Definition of greatest common divisor (gcd) of two integers.

Euclidean algorithm of successive division for the computation of the gcd. Extended Euclidean algorithm also called Bézout identity.

Fundamental Theorem of Arithmetic

Perfect numbers. Mersenne Prime. Theorem (Euclid-Euler): An even number is perfect if and only if it is of the form $2^{p-1}(2^p-1)$ where 2^p-1 is a Mersenne prime.

Nobody knows if there are infinitely many perfect numbers. There is exactly one for each known Mersenne prime. At the time of writing 51 perfect numbers are known. The largest known perfect number has almost 50 million digits. Check: https://en.wikipedia.org/wiki/List_of_perfect_numbers.

An Internet wide search for Mersenne prime is active and anyone can join in:https://www.mersenne.org/

An important corollary to the Fundamental Theorem of Arithmetic: There exist infinitely many prime numbers. Two proofs:

1. The classic Euclid proof, a model of clarity and terseness
2. Euler proof: the series of the reciprocal of prime numbers is divergent,

$$\sum \frac{1}{p} = +\infty$$

Euler's proof is more complicated than Euclid's but it opens a connection between the methods of Calculus and the study of the integers. For more proofs see [1].

Continued fractions: Euclid algorithm can be presented differently with the continued fraction symbolism.

1. Make an educated guess on the possible value of $[2; 1, 2, 1, 1, 4, 1, 1, 6, 1, 1, 8, 1, 1, 10, \ldots]$.
2. Express π as continued fraction.

   Solution. Actually, we can only obtain a partial expression starting form a decimal approximation. Take the integer part of π, i.e., 3. Then the integer part of $\frac{1}{\pi-3}$, i.e., 7. Repeat. Precisely: let $\alpha_0 = \pi$, and let $a_0 = \lfloor \alpha_0 \rfloor$ (the integer part of α_0). Take $a_1 = \lfloor \alpha_1 \rfloor = \lfloor \frac{1}{\alpha_0 - 3} \rfloor = 7$. Repeat $a_2 = \lfloor \alpha_2 \rfloor = \lfloor \frac{1}{\alpha_1 - 7} \rfloor = 15$. After a few steps we get: $\pi = [3; 7, 15, 1, 292, \ldots]$.
3. Write out the continued fraction of $\log_e 2 = 0.693147\ldots$

   Solution. We get $[0; 1, 2, 3, 1, 6, 3, \ldots]$. A fast way to compute this with a pocket calculator is the following:

   (a) type in the decimal value of 0.693147 and make a note of its integer part: 0;

(b) type in the reciprocal of the previous number: 1.442695 and make a note of the integer part: 1;

(c) subtract 1 from the previous and compute the reciprocal: 2.25.... Make a note of the integer part: 2;

(d) subtract 2 and compute the reciprocal: 3.86.... Make a note of the integer part: 3;

(e) and so on.

4. Given a continued fraction $[a; b, c, d, \ldots]$ we want to recover its decimal value.

   Solution. The fast method is to write a table as follows

CF		a	b	c
Num	1	a	ba+1	c(ba+1)+a
Den	0	1	b1+0	c(b1+0)+1

   where each step is obtained from the previous one by multiplying the number on the top by the preceding and adding to this the previous one.

5. Compute the value of $[2; 1, 3, 1, 5, 4]$.

   Solution.

   Start by sketching the table

CF		2	1	3	1	5	4
Num	1	2	3				
Den	0	1	1				

   The first column is fixed: 1 and 0. The second column is obtained by lowering 2 and copying 1. The 3 in the third column is obtained as in the rule described above and so on. One gets

CF		2	1	3	1	5	4
Num	1	2	3	11	14	81	338
Den	0	1	1	4	5	29	121

   The desired value is therefore $\frac{338}{121}$.

6. Compute the value of $[3; 7, 15, 1]$.

   Solution.

CF		3	7	15	1
Num	1	3	22	333	355
Den	0	1	7	106	113

The desired value is therefore $\frac{355}{113}$.

7. Compute the value of $[2; 1, 2, 1, 3, 4, 5]$.

   Solution.

CF		2	1	2	1	3	4	5
Num	1	2	3	8	11	41	175	916
Den	0	1	1	3	4	15	64	335

   The desired value is therefore $\frac{916}{335}$.

8. You have a 5-liter bottle and a 3-liter bottle. You are at a water fountain. How do you measure exactly 4 liters?

   Solution. Since 5 and 3 are coprime you can do this. Indeed, $1 = 2 \times 3 - 5$. So you can

   (a) Fill the 3-liter bottle and pour it in the 5-L bottle.

   (b) Fill the 3-L again and fill up the 5-L, 1 liter remains in 3-L.

   (c) Empty the 5-L and pour the one liter left in the 3-L.

   (d) Fill the 3-L and pour it in the 5-L.

Sections 1.3, 1.4, 1.5, 1.6 of Notes.

3 Monday, Mar 4, Lecture 6,7

Definition of congruence modulo n. The congruence is an equivalence relation. Properties of congruences. Modular arithmetics. Quotient sets: $\mathbb{Z}_4, \mathbb{Z}_5, \mathbb{Z}_6, \mathbb{Z}_7$. Computing the multiplicative inverse of an element of $\mathbb{Z}_n$ using Bézout identity.

Exercises to try.

1. Construct addition and multiplication tables for $\mathbb{Z}_6$. Are there any zero divisors? What are the invertible elements?

2. Construct addition and multiplication tables for $\mathbb{Z}_7$. Are there any zero divisors? What are the invertible elements?

3. Evaluate the following expression:

$$51 \div \{12 + 3 \cdot [2 \cdot 18 - 9 \cdot (24 \div 6 - 2) \div 6] - 60\} + 7$$

   assuming the the numbers are representatives in $\mathbb{Z}_7$.

4. Repeat the evaluation of the previous exercise assuming now the the numbers are representatives in $\mathbb{Z}_6$.

5. Prove that a zero divisor cannot be invertible.

6. Prove that if an integer N has a decimal representation of the form $N = 10b + a_0$, where a_0 is the units digit, then $N \equiv a_0 + 3b \pmod 7$. For example, if $N = 725$ then $N = 10 \times 72 + 5$ so $b = 72$ and $a_0 = 5$ and $725 \equiv 5 + 3 \times 72 \pmod 7$. We can check that $5 + 3 \times 72 = 221$ and the difference $725 - 221 = 504$ is a multiple of 7: $504 = 72 \times 7$. Your job is to prove that this is always the case.

Section 1.7 of Notes.

4 Thursday, Mar 7, Lecture 8,9,10

Condition for the invertibility of an element of $\mathbb{Z}_n$. More properties of the congruence relation. Fermat Little Theorem. Solving congruences. Conditions for solvability of congruences.

Exercise: Solve $87549x \equiv 34761 \pmod{123}$

Section 1.8, 1.9 of Notes.

5 Monday, Mar 11, Lecture 11,12

Exercises on congruences. Proof of divisibility criteria: divisibility by 9,11,7.

Exercise: Solve $17325x \equiv 5880 \pmod{215}$.

The first class test will be on April 11: this test will be reserved to students who are actually attending classes regularly. At the moment this means about 50 students. The date may change if it becomes necessary to find a larger classroom.

See exercises on page 22 and ff, especially numbers 1-13, and 24-30, of Notes.

6 Thursday, Mar 14, Lecture 13,14,15

The Chinese Remainder Theorem (CRT): statement and proof. Examples. How to deal with the case when the moduli are not coprime.

Definition of Euler ϕ-function: definition, properties. A formula for $\phi(n)$.

Solve

$$\begin{cases} x \equiv 10 \pmod{14} \\ x \equiv 2 \pmod{12} \end{cases}$$

An application: the perpetual calendar.

$$f(k,m,S,A) = k + [2.6m - 0.2] - 2S + A + [\frac{A}{4}] + \frac{S}{4}$$

For example, $f(14,1,20,19) = 4$ 14 March 2019 is a Thursday

Compute $f(1,11,20,180$ for January 1, 2019.

A volunteer (or a pair of volunteers) could read the proof of this formula in Notes pp 31-33 (pp 36-38 in the English version) and explain it to the class in the form of a short seminar.

Section 1.10, 1.11, 1.12 of Notes.

7 Monday, Mar 18, Lecture 16,17

Introduction to the concept of GROUP. Definition. Many examples. $(\mathbb{Z},+)$ is an abelian group. $(\mathbb{Z},-)$ is not a group. $(\mathbb{Z}_n,+)$ is an abelian group. $(\mathbb{Z}_n^*,\cdot)$ is an abelian group. The following are also abelian groups: $(\mathbb{Q},+)$, $(\mathbb{R},+)$, $(\mathbb{C},+)$, $(\mathbb{Q}^*,\cdot)$, $(\mathbb{R}^*,\cdot)$, $(\mathbb{C}^*,\cdot)$.

The group $GL_2(\mathbb{R})$ (general linear group) is the set of all invertible 2×2 matrices with respect to the usual row by column operation of matrices. It is a group but it is not abelian.

The group $O_2(\mathbb{R})$ (orthogonal group) of all 2×2 orthogonal matrices is a nonabelian group. It is also a subgroup of $GL_2(\mathbb{R})$.

S_n the set of all permutations of n elements is a nonabelian group with respect to the composition of permutations.

Order of a group. Order of an element of a group.

Cyclic groups and generators of a group.

Exercise: List all elements of S_4. Compute a few operations on this group. Compute the inverse of some elements. Find the order of S_4 and the order of some elements in this group. Is this an abelian group? Why or why not? Is this a cyclic group?

Exercise: Consider the set $Q_8 = \{1,-1,i,-i,j,-j,k,-k\}$ with the operation defined by

$$i\cdot i = j\cdot j = k\cdot k = -1$$

$$i\cdot j = k, j\cdot k = i, k\cdot i = j$$

$$j\cdot i = -k, k\cdot j = -i, i\cdot k = -j$$

check that this is a nonabelian group of order 8. Compute the order of all the elements of Q_8. Is Q_8 cyclic?

Exercise: Consider the set of all complex numbers that satisfy the equation $x^8 = 1$, call this set C_8. Check that they form a cyclic group with respect to the usual multiplication of complex numbers. Draw a picture of the location of these numbers on the Argand plane (the usual plane where we represent complex numbers). Find all generators of C_8.

Exercise: Check that the matrix

$$\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$$

is in $GL_2(\mathbb{R})$ for any $\theta \in \mathbb{R}$. Check that it belongs also to $O_2(\mathbb{R})$. Find the order of this matrix when $\theta = \frac{\pi}{3}$.

Section 2.1, 2.2 of Notes.

8 Thursday, Mar 21, Lecture 18,19,20

Definition of dihedral groups D_n: symmetries of a regular n-gon.

Exercise: Write down all the six elements of D_3 and compute the order of each element. Is D_3 a cyclic group?

Subgroups. Subgroups of cyclic groups are cyclic.

Exercise: Write down all the elements of the group C_8 of the eighth roots of unity. Find the order of each element. What are the primitive 8-th roots of 1?

Lagrange's theorem. Some corollaries. Fermat's little theorem is a corollary of Lagrange's theorem.

Section 2.2 of Notes.

9 Sample test 1

The following is a sample for our first class test that will be held, presumably, on April 11. It is based on last year test. Remember that last year the exam was in Italian so some of the exercises were based on the Italian language. This year it would be modified accordingly. Also, notice that some exercises are based on material not yet covered in class but it will be before the test.

1. Show that $17^{17} + 53^{53}$ is divisible by 385.
2. Find the last three digits of 7^{9810}.
3. Find the smallest positive solution of the system

$$\begin{cases} 2025x \equiv 53120667 \pmod{11} \\ 977x \equiv 5321 \pmod{9} \\ 116334x \equiv 235783 \pmod{7} \end{cases}$$

4. State and prove Lagrange's theorem.

5. Let C_{24} be the cyclic group of 24-th roots of unity and let $\omega = e^{\frac{2\pi i}{24}}$.
   (a) How many are the primitive roots? List them all.
   (b) Write down all the elements of the subgroup generated by ω^6.
   (c) List all the elements in the only subgroup of order 8.
6. Construct a field with 16 elements. Show a nontrivial example of the product of two elements.
7. Using the key word $\mathbf{k} = EULERO$ encrypt the sentence IL DIAVOLO FA LE PENTOLE MA NON I COPERCHI (cifrario di Vigenère).
8. Compute the coincidence index of the following two strings using the formula
$$I.C. = \sum_{i=0}^{25} \frac{f_i(f_i - 1)}{N(N-1)}$$
   where f_i is the fequency of the i-th letter of the alphabet (f_0 corresponds to A, etc.) and N is the length of the string.
   Which of the two strings is more likely an Italian sentence?
   (a) MDNCMSIMIAQATNAAURCEAIASOILSSSI
   (b) FOSURHSAGDTFDPLLFSFSVNCPDDUD
9. Express $\frac{1063}{37}$ as a continued fraction.
10. If $m \in \mathbb{Z}$ and $\gcd(m, n) = 1$, prove that $m^{\phi(n)-1}$ is a multiplicative inverse of m modulo n. Use this observation to compute the multiplicative inverse of 167 modulo 222.

10 Monday, Mar 25, Lecture 21,22

Consequences of Lagranges's Theorem: Fermat's Little Theorem and Euler's Theorem.
Formula for the solution of a system of congruences.
Exercise: Find the last two digits of 7^{50}.
Definition of homomorphism of groups. Isomorphisms.
Exercise: Prove that C_n is isomorphic to Z_n for any n.
Exercise: Prove that Q_8 is not isomorphic to Z_8.
Exercise: Let $K = \{\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \in M_2(\mathbb{R})\}$. Prove that $(K, +)$ is isomorphic to $(\mathbb{C}, +)$.
Prove that $(K^*, \cdot)$ is isomorphic to $(\mathbb{C}^*, \cdot)$.
Section 2.3 of Notes.

11 Thursday, Mar 28, Lecture 23,24,25

Formula for a perpetual calendar. Classification of cyclic groups. Definition of Rings and Fields. Examples. A field of 2×2 matrices isomorphic to $\mathbb{C}$. A field with 9 elements.

Section 2.4 of Notes.

12 Monday, Apr 1, Lecture 26,27

If $\mathbb{F}$ is a field then $\mathbb{F}[x]$ is a Euclidean domain, that is, we can perform the Euclidean division of polynomials. Irreducible polynomials. Irreducibility depends on the field of the coefficients. Theorem of classification of finite fields. Characteristic of a field: $\text{char}(\mathbb{F})$ is a prime number. Fundamental subfield of a field. A finite field must have a number of elements of the form p^k where p is prime and $k \geq 1$ an integer. How to construct a field of 9, 16, 25 elements.

Exercise: Check whether $x^4 + 1$ is irreducible over $\mathbb{Z}_3$, $\mathbb{Z}_2$, $\mathbb{Z}_5$.

Exercise: Find an explicit isomorphism between the two types of fields with 9 elements.

Exercise: Divide $x^3 + 3x^2 + 1$ by $x^2 + 1$ in $\mathbb{Z}_2[x]$.

Section 2.5 of Notes.

(Sections 2.6 and 2.7 are optional and you will not be tested on them)

13 Thursday, Apr 4, Lecture 28,29,30

Exercise: Construct a field with 16 elements: $GF(16) = \mathbb{F}_8$. Find a primitive element of it.

Elements of cryptography. Symmetric cryptography. Classical monoalphabetic ciphers: Caesar's cipher, affine cipher, substitution cipher. Polyalphabetic ciphers: Hill's cipher, Vigénère's cipher.

Exercise: Use the key phrase DISCRETEMATHEMATICSISFUN to encrypt the message "ATTACK AT DAWN" with a substitution cipher.

Exercise: Knowing that the secret message was encrypted with the same key phrase DISCRETEMATHEMATICSISFUN decrypt the message

TGGCUQSFABYGQLSGNABTPROP.

Exercise: Compute the inverse matrix, if possible, of the matrix

$$A = \begin{pmatrix} 2 & -1 \\ -5 & 7 \end{pmatrix}$$

Exercise: Use the Vigénère cipher with key word TIME to encode the message: ATTACK AT DAWN

Project: Decrypt the message https://docs.google.com/a/uniroma1.it/viewer?a=v&pid=sites&srcid=dW5pcm9tYTEuaXR8c3RlZmFub2NhcHBhcmVsbGl8Z3g6ZWQ4ZWYxNDg5Mzg1N2Rk

knowing that it has been encrypted using the Vigénère cipher with a key word of length 4, see also https://docs.google.com/a/uniroma1.it/viewer?a=v&pid=sites&srcid=dW5pcm9tYTEuaXR8c3

Section 3.1 of Notes.

14 Monday, Apr 8, Lecture 31,32

Solution of a substitution cipher from previous lecture: The permutation is the following

$$\begin{pmatrix} A & B & C & D & E & F & G & H & I & J & K & L & M \\ D & I & S & C & R & E & T & M & A & H & F & U & N \end{pmatrix}$$

$$\begin{pmatrix} N & O & P & Q & R & S & T & U & V & W & X & Y & Z \\ B & G & J & K & L & O & P & Q & V & W & X & Y & Z \end{pmatrix}$$

this means, (reading top down): A becomes D, B becomes I, C becomes S, etc.

To decode the secret message

TGGCUQSFABYGQLSGNABTPROP

we must read from the bottom up, so that T goes to G, G goes to O, G goes to O, C goes to D, U goes to L, etc., to form the sentence

GOODLUCKINYOURCOMINGTEST

Cryptanalysis of Vigénère cipher.

We want to analyze the encrypted message

YZYAOYXHNZAXBZYQMPAF TSSRTJSRHLZBRPEAAMSL
KMCQHPRXMPSCTSIXDGIK TFVBSZJQOXWXWJIOBFXQ
HLXXIYXKOXEQTPVQHLXY OZOTADQXDPFVMCQXRVXT
ATRXNOLBTZPATSIQRFXE MLMKLJXEECITADXEIYKP
WSMZHSIPTCIQCSIABFXJ ATRIYSIQOWHQHPXOUELQ
HLXFSYSQHTRDIYISECWB EYEKYMSAYMYQLTIAOYIQ
IXILRLRLTSIO**WTXE**OFXF THEPAFRQPZPIYZVQHPAF
DZALRXEVBPQXRJERNETL LWCQOXWXUYXMOWPVSSIF
SLRAMLVVAYHQHPAFDZAA OFKIADMPAWPQOWHXBZYQ
IYXEAEFLOVAEINLFSXSP TWCXTCYBBZSH**WTXE**SZQB
SEVBTNLBRDEPIDEFDMICOCI

Call this string *message*.

To use Kasiski's test we keep track of repetitions of groups of three or more letters. In the text, for example I highlighted the letters **WTXE** and the letters PAFDZ. The Kasiski's text requires you to count the distance in letters from one repetition to the other. In this case there are 140 letters between the two **WTXE** groups and 56 between PAFDZ. More repetitions are present so that one can get a better estimate. For example, Kasiski tells us the the length of the secret word is a divisor of $GCD(140, 56) = 28$ so it could be $2, 4, 7, 14, 28$. Perhaps by looking at other repetitions some of these options could be excluded.

For the sake of simplicity, let's assume that our guess of the length is 4.

Now we can use Friedman's Coincidence Index: for a string $\mathbf{x}$ of length n of letters the probability that by selecting two letters at random in $\mathbf{x}$ we get two equal letters is

$$I_c(\mathbf{x}) = \sum_{i=0}^{25} \frac{\binom{f_1}{2}}{\binom{n}{2}} = \sum_{i=0}^{25} \frac{f_i(f_i-1)}{n(n-1)}$$

where f_0 is the number of times A appears in the string, f_1 is the number of B, f_2 is the number of C,..., f_{25} is the number of Z.

It is known that for any natural language (English, Italian, etc.) this index is fixed: English has an index of about 0.0667, Italian 0.073. This is computed as

$$\sum_{i=0}^{25} p_i^2$$

where p_i is the probability of finding the i-th letter of the alphabet in a sufficiently long text. For English, the most likely letter is E.

This must be compared with the same probability in a random string of letters. If the string is random then each letter has probability $\frac{1}{26}$ to be picked. For a random string then the index is

$$\frac{1}{26} \approx 0.038$$

The numbers 0.0667 and 0.038 are sufficiently different to allow us to recognize whether a string is from an English text or if it is random.

If we compute the coincidence index of the string *message*, of length 423, we find the number 0.045 which indicates a random string. You can compute that the frequencies are

$$25, 14, 12, 11, 22, 17, 1, 16, 27, 6, 7, 21, 14, 5, 18, 21, 24, 17,\ 25, 23, 2, 11, 13, 35, 21, 15$$

so the index is

$$\frac{1}{423 \times 422}(25(24) + 14(13) + 12(11) + \cdots + 15(14)) \approx 0.045.$$

Assuming a length of 4. We can split the text into groups of four

YZYA OYXH NZAX BZYQ MPAF TSSR TJSR HLZB RPEA AMSL KMCQ HPRX MPSC TSIX DGIK TFVB SZJQ OXWX WJIO BFXQ HLXX IYXK OXEQ TPVQ HLXY OZOT

ADQX DPFV MCQX RVXT ATRX NOLB TZPA TSIQ RFXE MLMK LJXE ECIT ADXE IYKP WSMZ HSIP TCIQ CSIA BFXJ ATRI YSIQ OWHQ HPXO UELQ HLXF SYSQ

HTRD IYIS ECWB EYEK YMSA YMYQ LTIA OYIQ IXIL RLRL TSIO WTXE OFXF THEP AFRQ PZPI YZVQ HPAF DZAL RXEV BPQX RJER NETL LWCQ OXWX UYXM

OWPV SSIF SLRA MLVV AYHQ HPAF DZAA OFKI ADMP AWPQ OWHX BZYQ IYXE AEFL OVAE INLF SXSP TWCX TCYB BZSH WTXE SZQB SEVB TNLB RDEP IDEF

DMIC OCI

If we compute the coincidence index of the string of first letters:

YONBMTTHRAKH...

or of second letters

ZYZZPSJLPMMP...

or of third letters

YXAYASSZESCR...

or of fourth letters

AHXQFRRBALQX...

we get values close to 0.0667 which show that the sequences are not random and our guess of length 4 is correct. If not, we would have to start over, with a different guess for the length.

How can we get to guess the correct four letter word?

We use a similar idea. Define a function

$$M_k = \sum_{i=0}^{25} p_i \frac{f_{i+k}}{n}.$$

This depends on the shift which we imposed on the alphabet. For example, if we take a plain text in English, with no shift, the index would be

$$M_0 = \sum_{i=0}^{25} p_i \frac{f_i}{n} = \sum_{i=0}^{25} p_i^2 \approx 0.0667$$

However, if there is a shift, then M_0 would give a number that is closer to a random value of 0.038. But, if the shift k_0 is exactly the one used, then M_{k_0} would be close to 0.0667 again.

So in practice, we run this function M_k through all possible values from 0 to 25 and when we find a value close to 0.0667 we got our shift.

In our case we get the values:

0.060001, 0.038897, 0.02528, 0.038908, 0.03983, 0.03661, 0.037197, 0.045186, 0.038152, 0.033393, 0.044338, 0.039242, 0.036539, 0.036532, 0.047238, 0.046554, 0.037178, 0.025874, 0.03282, 0.042564, 0.039086, 0.037192, 0.043042, 0.035647, 0.030066, 0.039646

for the first letters. As we can see the "best" value is the first, corresponding to A.

For the second letters we have 0.03213, 0.040498, 0.030093, 0.030204, 0.04034, 0.047173, 0.036449, 0.043234, 0.036237, 0.031359, 0.03819, **0.060452**, 0.039626, 0.02729, 0.036969, 0.039708, 0.031672, 0.040411, 0.045537, 0.036995, 0.038976, 0.043913, 0.037246, 0.036242, 0.042302, 0.040757

corresponding to L

For the third letters we have 0.044759, 0.033554, 0.027816, 0.033825, **0.068231**, 0.039504, 0.033489, 0.032656, 0.040911, 0.035749, 0.039298, 0.036752, 0.036946, 0.033844, 0.033925, 0.047619, 0.042822, 0.041857, 0.032577, 0.046034, 0.040471, 0.033703, 0.035981, 0.045105, 0.032543, 0.029017 corresponding to E and finally the last computation will give you X. So the secret word is ALEX.

Now we can easily recover the message.

YZYA OYXH NZAX BZYQ...

ALEX ALEX ALEX ALEX...

youd ontk nowa bout ...

The text is

You don't know about me without you have read a book by the name of The Adventures of Tom Sawyer; but that ain't no matter. That book was made by Mr. Mark Twain, and he told the truth, mainly. There was things which he stretched, but mainly he told the truth. That is nothing. I never seen anybody but lied one time or another, without it was Aunt Polly, or the widow, or maybe Mary. Aunt Polly – Tom's Aunt Polly, she is – and Mary, and the Widow Douglas is all told about in that book, which is mostly a true book, with some stretchers, as I said before.(The adventures of Huckleberry Finn, page 1, by Mark Twain).

The idea of Public Key Cryptography: One-way trap door functions. Example of discrete logarithm.

Sections 3.2, 3.3 of Notes.

15 Thursday, April 11,Lecture 33,34,35 – Midterm

First Mid-term test, Ver. A

Last Name (please print clearly):_____

First Name :_____

11 April 2019. **There are 10 exercises plus 3 optional ones, please turn the page.**

A	B	C	D	E	F	G	H	I	J
0	1	2	3	4	5	6	7	8	9
K	L	M	N	O	P	Q	R	S	T
10	11	12	13	14	15	16	17	18	19
U	V	W	X	Y	Z				
20	21	22	23	24	25				

1. By using Fermat's Little Theorem find the last two digits of $23^{43} + 47^{47}$.

Solution. To look for the last two digits we study the congruence modulo 100. We use Euler's generalization of Fermat Little Theorem, and compute $\phi(100) = 100(1-\frac{1}{2})(1-\frac{1}{5}) = 40$. We know that, since $gcd(23, 100) = 1$, $23^{40} \equiv 1 \pmod{100}$ and analogously $47^{40} \equiv 1 \pmod{100}$. So

$$\begin{aligned} 23^{43} + 47^{47} &\equiv 23^{40}23^3 + 47^{40}47^7 \equiv 23^3 + 47^7 \pmod{100} \\ &\equiv 23^2 23 + 47^2 47^2 47^2 47 \equiv 29 \cdot 23 + 9 \cdot 9 \cdot 9 \cdot 47 \\ &\equiv 67 + 81 \cdot 9 \cdot 47 \equiv 67 + 29 \cdot 47 \equiv 67 + 63 \equiv 30 \end{aligned}$$

So the last two digits are 30.

2. Write the Bézout identity for $333, 738$

Solution. First, we carry out the Euclidean algorithm of successive divisions:

$$\begin{aligned} 738 &= 333 \cdot 2 + 72 \\ 333 &= 72 \cdot 4 + 45 \\ 72 &= 45 \cdot 1 + 27 \\ 45 &= 27 \cdot 1 + 18 \\ 27 &= 18 \cdot 1 + 9 \\ 18 &= 9 \cdot 2 \end{aligned}$$

Then we proceed from the bottom up to write the last nonzero remainder, which is 9:

$$\begin{aligned} 9 &= 27 - 18 = 27 - (45 - 27) \\ &= -45 + 2 \cdot 27 = -45 + 2(72 - 45) \\ &= -3 \cdot 45 + 2 \cdot 72 \\ &= -3(333 - 4 \cdot 72) + 2 \cdot 72 = -3(333) + 14 \cdot 72 \\ &= -3(333) + 14(738 - 2 \cdot 333) = -31(333) + 14(738) \end{aligned}$$

So finally Bézout identity is

$$\boxed{9 = -31(333) + 14(738)}$$

3. Express $\frac{333}{738}$ as a continued fraction.

Solution. Having carried out the computation in the previous exercise we can immediately write the continued fraction as $[0; 2; 4; 1, 1, 1, 2]$, by looking at the boldface number in the following computation

$$\begin{aligned} 738 &= 333 \cdot \mathbf{2} + 72 \\ 333 &= 72 \cdot \mathbf{4} + 45 \\ 72 &= 45 \cdot \mathbf{1} + 27 \\ 45 &= 27 \cdot \mathbf{1} + 18 \\ 27 &= 18 \cdot \mathbf{1} + 9 \\ 18 &= 9 \cdot \mathbf{2} \end{aligned}$$

preceded by 0 since $\frac{333}{738}$ is less than 1.

In alternative, using a calculator, and a "sufficient" number of decimal digits, we get

$$\begin{aligned}
\frac{333}{738} &\approx 0.4512195121951219 : \mathbf{0} \\
\frac{1}{0.45122} &\approx 2.216216216216216 : \mathbf{2} \\
2.21626 - 2 &= 0.216216216216216 \\
\frac{1}{0.21626} &\approx 4.625 : \mathbf{4} \\
4.62406 - 4 &= 0.625 \\
\frac{1}{0.625} &\approx 1.6 : \mathbf{1} \\
\frac{1}{0.6} &\approx 1.666666666667 : \mathbf{1} \\
\frac{1}{0.666666667} &\approx 1.5 : \mathbf{1} \\
\frac{1}{0.5} &= 2 : \mathbf{2}
\end{aligned}$$

4. Solve using the CRT

$$\begin{cases} 489833x \equiv 750114 \pmod 8 \\ 885731x \equiv 347605 \pmod 9 \\ 603721x \equiv 297857 \pmod{11} \end{cases}$$

Solution. First we simplify the coefficients using the divisibility criteria. Divisibility by 8: since $8 = 2^3$ to compute the residue class of a long number it is equivalent to compute the residue class of the last three digits, so

$$489833 \equiv 833 \equiv 1 \pmod 8$$

$$750114 \equiv 114 \equiv 2 \pmod 8$$

Next, we use the divisibility criterion by 9, so

$$885731 \equiv 8 + 8 + 5 + 7 + 3 + 1 = 32 \equiv 5 \pmod 9$$

$$347605 \equiv 3 + 4 + 7 + 6 + 0 + 5 = 25 \equiv 7 \pmod 9$$

and, finally,

$$603721 \equiv 1 - 2 + 7 - 3 + 0 - 6 = -3 \equiv 8 \pmod{11}$$

$$297857 \equiv 7 - 5 + 8 - 7 + 9 - 2 = 10 \equiv -1 \pmod{11}$$

So our system is equivalent to

$$\begin{cases} x \equiv 2 \pmod 8 \\ 5x \equiv 7 \pmod 9 \\ 8x \equiv -1 \pmod{11} \end{cases}$$

Now notice that the inverse of 5 is 2 (mod 9), so the second congruence becomes $x \equiv 2 \cdot 7 \equiv 5 \pmod 9$; and the inverse of 8 (mod 11) is 7, so the third congruence becomes $x \equiv 4 \pmod{11}$. So the system is

$$\begin{cases} x \equiv 2 \pmod 8 \\ x \equiv 5 \pmod 9 \\ x \equiv 4 \pmod{11} \end{cases}$$

We now use the formula

$$x_0 = 2(9 \cdot 11)^{\phi(8)} + 5(8 \cdot 11)^{\phi(9)} + 4(8 \cdot 9)^{\phi(11)} \pmod{8 \cdot 9 \cdot 11}$$

$$x_0 = 2(99)^4 + 5(88)^6 + 4(72)^{10} \equiv 554 \pmod{792}$$

5. Write the multiplication table for $\mathbb{Z}_9$.

   Solution.

	0	1	2	3	4	5	6	7	8
0	0	0	0	0	0	0	0	0	0
1	0	1	2	2	3	4	5	6	7
2	0	2	4	6	8	1	3	5	7
3	0	3	6	0	3	6	0	3	6
4	0	4	8	3	7	2	6	1	5
5	0	5	1	6	2	7	3	8	4
6	0	6	3	0	6	3	0	6	3
7	0	7	5	3	1	8	6	4	2
8	0	8	7	6	5	4	3	2	1

6. Compute the expression

$$(\frac{1}{4} \cdot \frac{5}{2} - \frac{3}{2} \cdot \frac{1}{4}) \cdot (\frac{6}{3} \cdot \frac{5}{4} + 1) \div (\frac{6}{10} \cdot \frac{5}{2} + 1)$$

   in $\mathbb{Z}_{11}$.

   Solution. The inverse of 4 in $\mathbb{Z}_{11}$ is 3, the inverse of 2 is 6, the inverse of 10 is 10. So the expression can be written as

$$(3 \cdot 5 \cdot 6 - 3 \cdot 6 \cdot 3) \cdot (6 \cdot 4 \cdot 5 \cdot 3 + 1) \div (6 \cdot 10 \cdot 5 \cdot 6 + 1)$$

   which is

$$\begin{aligned} &(4 \cdot 6 - 7 \cdot 3) \cdot (2 \cdot 5 \cdot 3 + 1) \div (5 \cdot 5 \cdot 6 + 1) \\ &= (2 - 10) \cdot (10 \cdot 3 + 1) \div (3 \cdot 6 + 1) \\ &= (-8) \cdot (8 + 1) \div (7 + 1) = 3 \cdot 9 \div 8 \end{aligned}$$

   The inverse of 8 is 7 so:

$$= 3 \cdot 9 \cdot 7 = 5 \cdot 7 = 2$$

7. Compute the permutation as a result of the following product

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix}$$

Solution.

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$$

8. Construct a field with 9 elements and give a nontrivial example of multiplication.

Solution. The construction is possible since $9 = 3^2$. We need to consider $\mathbb{Z}_3[x]$ and find an irreducible polynomial of second degree. We do this by trial and error.

A first possible choice is $x^2 + x + 1$ however, this polynomial has 1 as a root: $1^2 + 1 + 1 = 0$, so it is reducible as it is divisible by $x - 1$. Next, we try $x^2 + 1$ this polynomial has no roots in $\mathbb{Z}_3$:

$$0 + 1 \neq 0, 1 + 1 \neq 0, 4 + 1 = 1 + 1 \neq 0$$

So this is our choice.

Now we consider all possible polynomials of degree less than 2:

$$0, 1, 2, x, x + 1, x + 2, 2x, 2x + 1, 2x + 2$$

A nontrivial multiplication is an example of a multiplication where we need to operate modulo the chosen irreducible polynomial. A trivial multiplication is $1 \cdot x = x$, $0 \cdot 2x + 1 = 0$, etc. A nontrivial multiplication is, for example,

$$(2x)(2x + 1) = 4x^2 + 2x = x^2 + 2x \equiv 2x + 2$$

9. If possible, find the inverse of the matrix

$$A = \begin{pmatrix} 1 & -2 \\ 3 & 5 \end{pmatrix}$$

in $\mathbb{Z}_6$

Solution. The matrix A has determinant equal to $11 \equiv 5 \pmod 6$ and so the matrix is invertible as the determinant is an invertible element of $\mathbb{Z}_6$.

So

$$A^{-1} = 5 \begin{pmatrix} 5 & 2 \\ -3 & 1x \end{pmatrix} = \begin{pmatrix} 1 & 4 \\ 3 & 5 \end{pmatrix}$$

10. Compute the coincidence index of the following two strings:

    (a) PMMLOHNYQGWFJALCYWTD

    (b) TXTFMLOMZTEGDTLFTETLLAKB

Which one is more likely to be a string from an English text?

Solution. In computing the coincidence index of a string, letters that appear once can be discarded. So in the first string we have

$$2M, 2L, 2Y, 2W$$

and there are 20 letters in total so the coincidence index is

$$\frac{2+2+2+2}{20 \cdot 19} = 0.02$$

In the second string, there are 24 letters and there are

$$6T, 2F, 2M, 4L, 2E$$

so the index is

$$\frac{6 \cdot 5 + 2 + 2 + 4 \cdot 3 + 2}{24 \cdot 23} = 0.087$$

The second index is much higher than the random value so it is more likely a permutation of an English sentence.

N.B. The fact that you may or may not remember the exact value of the Index in English is irrelevant, although somewhat surprising. It is not excusable instead to not remember that the index of a random string is close to $\frac{1}{26} \approx 0.038$ because on this observation is based the whole argument of frequency analysis.

The following exercises are optional

11. Show an explicit isomorphism between

$$\mathbb{Z}_{35} \to \mathbb{Z}_7 \times \mathbb{Z}_5$$

(Hint: Use CRT)

Solution. Any element in Z_{35} can be represented by an integer between 0 and 34. Any such

integer can be mapped to its two classes modulo 7 and modulo 5 respectively, as follows:

$$
\begin{aligned}
0 &\mapsto (0,0)\\
1 &\mapsto (1,1)\\
2 &\mapsto (2,2)\\
3 &\mapsto (3,3)\\
4 &\mapsto (4,4)\\
5 &\mapsto (5,0)\\
6 &\mapsto (6,1)\\
7 &\mapsto (0,2)\\
8 &\mapsto (1,3)\\
9 &\mapsto (2,4)\\
10 &\mapsto (3,0)\\
11 &\mapsto (4,1)\\
12 &\mapsto (5,2)\\
13 &\mapsto (6,3)\\
14 &\mapsto (0,4)\\
15 &\mapsto (1,0)\\
16 &\mapsto (2,1)\\
17 &\mapsto (3,2)\\
18 &\mapsto (4,3)\\
19 &\mapsto (5,4)\\
20 &\mapsto (6,0)\\
21 &\mapsto (0,1)\\
22 &\mapsto (1,2)\\
23 &\mapsto (2,3)\\
24 &\mapsto (3,4)\\
25 &\mapsto (4,0)\\
26 &\mapsto (5,1)\\
27 &\mapsto (6,2)\\
28 &\mapsto (0,3)\\
29 &\mapsto (1,4)\\
30 &\mapsto (2,0)\\
31 &\mapsto (3,1)\\
32 &\mapsto (4,2)\\
33 &\mapsto (5,3)\\
34 &\mapsto (6,4)
\end{aligned}
$$

This is a bijection and CRT guarantees that for any pair of classes mod 5 and 7 there is a single element modulo 35 which corresponds to the pair.

Moreover, this is a homomorphism of both addition and multiplication. For example,

$$(2,4)+(5,4)=(0,3)$$

and $(2,4)$ corresponds to 9, $(5,4)$ corresponds to 19 and $(0,3)$ corresponds to 28. and indeed

$$9+19=28$$

and

$$9 \equiv 31 \pmod{35}$$

and

$$(2,4)(5,4)=(10,16)\equiv(3,1)$$

which corresponds to 28.

12. Prove that there are infinitely many prime numbers.

    Solution. Theorem 1.5.1 in Notes.

13. Give the definition of a perfect number.

    Solution. See page 7 in Notes.

First Mid-term test Ver. B

Last Name (please print clearly):_____

First Name :_____

11 April 2019. **There are 10 exercises plus 3 optional ones, please turn the page.**

A	B	C	D	E	F	G	H	I	J
0	1	2	3	4	5	6	7	8	9
K	L	M	N	O	P	Q	R	S	T
10	11	12	13	14	15	16	17	18	19
U	V	W	X	Y	Z				
20	21	22	23	24	25				

1. By using Fermat's Little Theorem find the last two digits of $25^{43} + 38^{47}$.

   Solution. One should notice that $gcd(25, 100) = 25$ so Euler's Theorem does not apply and $gcd(38, 100) = 2$ so we can apply Euler's theorem to 19^{47}.

   For $25^{43} = 25^3(25^2)^{20} \equiv 25$ and $19^{47} \equiv 19^7 \equiv 39$, $2^{47} \equiv 28$. The final answer is : the last two digits are 17.

2. Write the Bézout identity for $342, 423$.

   Solution. $9 = 17 \cdot 423 - 21 \cdot 342$

3. Express $\frac{342}{423}$ as a continued fraction.

   Solution. $[0; 1, 4, 4, 2]$

4. Solve using the CRT

$$\begin{cases} 236019x \equiv 570557 \pmod 8 \\ 831869x \equiv 319034 \pmod 9 \\ 378328x \equiv 928340 \pmod{11} \end{cases}$$

   Solution. $439 \pmod{792}$.

5. Write the multiplication table for $\mathbb{Z}_6$.

6. Compute the expression

$$(\frac{1}{4} \cdot \frac{5}{2} - \frac{3}{2} \cdot \frac{1}{4}) \cdot (\frac{6}{3} \cdot \frac{5}{4} + 1) \div (\frac{6}{10} \cdot \frac{5}{2} + 1)$$

   in $\mathbb{Z}_5$.

   Solution. This cannot be computed as $\frac{6}{10}$ makes no sense: 10 is not invertible.

7. Compute the permutation as a result of the following product

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix}$$

   Solution.

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix}$$

8. Construct a field with 25 elements, compute a nontrivial example of a multiplication.

   Solution. An irreducible polynomial in $\mathbb{Z}_5[x]$ is $x^2 + x + 1$.

9. If possible, find the inverse of the matrix

$$A = \begin{pmatrix} 1 & -2 \\ 3 & 5 \end{pmatrix}$$

   in $\mathbb{Z}_9$

Solution. It is possible because the determinant is invertible in $\mathbb{Z}_9$. The inverse is

$$A^{-1} = \begin{pmatrix} 7 & 1 \\ 3 & 5 \end{pmatrix}$$

10. Compute the coincidence index of the following two strings:

    (a) XWMRIGGKKBUMDXZFSFYC

    (b) CITFOFMITEGWKLTGYIWDAF

    Which one is more likely to be a string from an English text?

    Solution. The first string has index 0.037 the second 0.048 so the second is more likely a string from an English text.

The following exercises are optional

11. Show an explicit isomorphism between

$$\mathbb{Z}_{24} \to \mathbb{Z}_3 \times \mathbb{Z}_8$$

    (Hint: Use CRT)

12. Prove that there are infinitely many prime numbers.

13. Give the definition of a perfect number.

First Mid-term test Ver. C

Last Name (please print clearly):_____

First Name :_____

11 April 2019. **There are 10 exercises plus 3 optional ones, please turn the page.**

A	B	C	D	E	F	G	H	I	J
0	1	2	3	4	5	6	7	8	9
K	L	M	N	O	P	Q	R	S	T
10	11	12	13	14	15	16	17	18	19
U	V	W	X	Y	Z				
20	21	22	23	24	25				

1. By using Fermat's Little Theorem find the last two digits of $28^{43} + 51^{47}$.

   Solution. Euler's theorem can be applied provided that $gcd(a, 100) = 1$. In this case one must observe that $gcd(28, 100) = 4$ so we can apply the theorem to compute the class modulo 100 of 51^{47} and 7^{43} and then compute the class of 4^{43} by reducing as follows, for example

   $$4^{43} = 4^{42}4 = (4^2)^{21}4 \equiv 16^{21}4 \text{ etc.}$$

   In any case the final answer is: the last two digits are 03.

2. Write the Bézout identity for $980, 408$.

   Solution. $4 = 5 \cdot 980 - 12 \cdot 408$

3. Express $\frac{980}{408}$ as a continued fraction.

   Solution. $[2; 2, 2, 20]$

4. Solve using the CRT

   $$\begin{cases} 385133x \equiv 755343 \pmod 8 \\ 202969x \equiv 882452 \pmod 9 \\ 928990x \equiv 304969 \pmod{11} \end{cases}$$

   Solution. $227 \pmod{792}$

5. Write the multiplication table for $\mathbb{Z}_8$.

6. Compute the expression

   $$(\frac{1}{4} \cdot \frac{5}{2} - \frac{3}{2} \cdot \frac{1}{4}) \cdot (\frac{6}{3} \cdot \frac{5}{4} + 1) \div (\frac{6}{10} \cdot \frac{5}{2} + 1)$$

   in $\mathbb{Z}_7$.

   Solution. 0.

7. Compute the permutation as a result of the following product

   $$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix}$$

   Solution.

   $$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}.$$

8. Construct a field with 8 elements, compute a nontrivial example of a multiplication.

   Solution. An irreducible polynomial in $\mathbb{Z}_2[x]$ is $x^3 + x + 1$.

9. If possible, find the inverse of the matrix

$$A = \begin{pmatrix} 1 & -2 \\ 3 & 5 \end{pmatrix}$$

in $\mathbb{Z}_8$.

Solution. It is possible because the determinant is invertible in $\mathbb{Z}_8$. The inverse is

$$A^{-1} = \begin{pmatrix} 7 & 6 \\ 7 & 3 \end{pmatrix}$$

10. Compute the coincidence index of the following two strings:

    (a) CXRCLKWULNDPGUBNFIMY

    (b) YGKGFTHTGHSTMGROLLGSXT

    Which one is more likely to be a string from an English text?

    Solution. The first string has index 0.021 the second 0.082 so the second is more likely a string from an English text.

The following exercises are optional

11. Show an explicit isomorphism between

$$\mathbb{Z}_{30} \to \mathbb{Z}_5 \times \mathbb{Z}_6$$

    (Hint: Use CRT)

12. Prove that there are infinitely many prime numbers.

13. Give the definition of a perfect number.

16 Monday, Apr 15, Lecture 36,37

Public Key Cryptography: trapdoor one-way functions. Discrete logarithm. RSA cipher. Examples. Diffie-Hellman key exchange protocol. Signature authentication.

Exercise. Decrypt

$$3061, 1667, 3031, 2073, 1242, 649, 730, 1932, 908, 2071, 730, 2234$$

knowing that it was sent with the public key $(3233, 17)$.

Exercise. Use a computer to factor $2^{251} - 1$. How long does it take?

Read: https://en.wikipedia.org/wiki/RSA_numbers

Sections 3.4, 3.5, 3.6, 3.7 of Notes.

Next class: Monday April 29. Happy Holidays.

17 Monday, Apr 29, Lecture 38,39

Introduction to coding theory. Definition of a code C on an alphabet F. Hamming distance. Proof of the three main properties of the distance. Minimum distance of a code. The number of errors that a code can detect or correct depends on the minimum distance d. Codes of type (n, M, d).

Sections 4.1, 4.2 of Notes.

Optional Assignment: For those of you who would like to improve your grade average, here is an option. Below is a Project on the Fundamental Theorem of Arithmetic. Study the proof and answer the exercises. The solution to the exercises and any related discussion must be done in writing either by hand or using LaTeX but in any case it must be a clear and clean exposition of the solution or solutions in an essay form. If you want credit for it, it also must be your own personal work and not a collaboration effort. It is due by May 23 at the beginning of class time.

Project

Last Name (please print clearly):_____

First Name :_____

The Fundamental Theorem of Arithmetic looks like it should be an "obvious" theorem and that it is hardly worth a proof. This feeling is likely generated by the great familiarity we have with whole numbers since elementary school so that we mistake familiarity for obviousness. However, deeper understanding is often obtained by reflecting on the most elementary things. The present Project is aimed to induce such a reflection on the Fundamental Theorem of Arithmetic. This theorem essentially says that the set of numbers $\mathbb{N} = \{1, 2, 3, \ldots\}$ has the unique factorization property (UFP), namely, any integer in $\mathbb{N}$ can be factored into prime numbers in a unique way (up to the order of the factors). To be precise we define a prime number one that has exactly two factors: 1 and itself. So, for example, 5 is prime, 6 is not, 1 is not prime. So the set $\mathbb{N}$ is partitioned into three disjoint subsets

$$\mathbb{N} = \{1\} \cup \{\text{prime numbers}\} \cup \{\text{composite numbers}\}$$

Now we are going to consider instead the set

$$S = \{1, 5, 9, 13, 17, \ldots\} = \{4n - 3 | n \in \mathbb{N}\}$$

Exercise. Prove that S is closed under multiplication, namely, prove that if s_1 and s_2 are in S that $s_1 s_2 \in S$.

We now split S into three disjoint subsets as we did for $\mathbb{N}$. The subsets in this case are $\{1\}$, those elements of S which have exactly two factors in S, and all the rest. It makes sense to call the element in the second set S-primes and all the others, except 1, S-composites.

Clearly, any prime in S is also an S-prime.

Exercise. Give some examples of S-primes that are not primes.

Exercise. Are there infinitely many S-primes?

Exercise. Check that $1617 \in S$.

Exercise. Check that $1617 = 33 \times 49 = 77 \times 21$ and that 33,49,77, and 21 are all S-primes.

This last exercise gives an example which shows that S does not have the UFP.

Exercise. Find at least another example of an element of S that has more than one factorization.

Since S is different from $\mathbb{N}$ it is not at all surprising that S does not have the UFP. But then the question is: what exactly is the difference or differences that makes the Fundamental Theorem true in $\mathbb{N}$ but not in S?

To reflect on that, first, let's see which of the many features of $\mathbb{N}$ we actually need to define and talk about the Fundamental Theorem. We are concerned with factors and primes, which clearly have something to do with multiplication, and indeed multiplication is all we need. It is worth spelling this out in detail: in $\mathbb{N}$, we say that a divides b if $b = ka$ for some $k \in \mathbb{N}$, a natural number is called prime if it has exactly two distinct factors, and $\mathbb{N}$ is closed under multiplication. Now go back to the previous sentence, replacing $\mathbb{N}$ by S, factor by S-factor, natural number by S-number, prime by S-prime and you will have analogous definitions and true statements in S.

Since the Fundamental Theorem does not hold for S then if we go through the proof of the Fundamental Theorem for $\mathbb{N}$ something must go wrong when we change the $\mathbb{N}$-words to S-words.

Here is proof of the Fundamental theorem for $\mathbb{N}$.

First, we outline the proof.

Step 1. By contradiction, suppose there is a natural number having more than one prime factorization, and let k be the smallest such number.

Step 2. Deduce from this that a smaller natural number exists with the same property. This clearly contradicts the definition of k, so there is no smallest natural number with more than one factorization, and so the Theorem is true.

In order to get from step 1 to step 2 we need two bridges, B1 and B2. These are

B1: Suppose k has the two factorizations $k = pqr\ldots$ and $k = p'q'r'\ldots$. Then none of the primes $p, q, r, \ldots$ coincides with any of the primes $p', q', r', \ldots$, because otherwise by cancelling the common prime we would get a number smaller than k with two different factorization, while we assumed that k was the smallest.

B2: If a natural number as a unique factorization $p_1 p_2 \cdots p_l$ then n has no other prime factor, otherwise n would not have a UNIQUE factorization.

Then we carry out the main argument.

First, we are free to write the primes in a factorization in any order and for convenience we write them so that $p \leq q \leq r \leq \cdots$ and $p' \leq q' \leq r' \leq \cdots$. Both lists contain at least two members (otherwise the number itself would be prime and it would have a unique factorization).

From this we see that $k \geq p^2$ and $k \geq p'^2$, and since by B1 $p \neq p'$, we have $k > pp'$.

Hence, $k - pp'$ is a natural number less than k and divisible by both p and p'. So by the minimality of k, the number $k - pp'$ must be of the form $pp'QR\cdots$ (or perhaps just pp'), where $Q, R, \ldots$ are further primes.

So

$$k = pp' + pp'QR\cdots$$

That is,

$$pqr\cdots = pp' + pp'QR\cdots$$

so

$$qr\cdots = p' + p'QR\cdots$$

and we see that p' is a factor of $qr\cdots$.

But p' is not equal to any of $q, r, \ldots$ because by B1 the set of prime factors are disjoint. By B2 the number $qr\cdots$ has no unique factorization and it is smaller than k this contradiction tells us that k cannot exist and so all numbers in $\mathbb{N}$ have a unique factorization.

Main Exercise. By going trough this proof and replacing $\mathbb{N}$-words with S-words where will the proof fail? In other words, which property of $\mathbb{N}$ is used which does not hold for S?

18 Thursday, May 2, Lecture 40,41,42

Main problem of coding theory: estimating $A_q(n, d)$. Some easy examples. Notion of equivalence of codes. Weight of a word. A binary code of type (n, M, d), d odd, exists if and only if a code of type $(n+1, M, d+1)$ exists. Spheres. Sphere packing inequality (Hamming inequality). Definition of a perfect code. Fano plane.

Sections 4.3 of Notes.

19 Monday, May 6, Lecture 43,44

Hamming [7,4] code. Linear codes. Minimum weight. Generating matrix. Equivalence of linear codes. Equivalent generating matrices. Standard form of the generating matrix. Encoding with a generating matrix.

Sections 4.4, 4.5 of Notes.

20 Thursday, May 9, Lecture 45,46,47

Dual Code and parity check matrix. Standard form for H. Syndrome decoding.

Recursions. The tower of Hanoi. Fibonacci numbers. Binet formula. Proof of the Binet formula via the method of the vector space.

Sections 4.6, 4.7 of Notes, 4.8 optional. 5.1, 5.2.1

21 Monday, May 13, Lecture 48,49

Proof of the Binet formula using the method of the matrix and, again, using the generating function concept. Solving a general homogeneous linear recurrence of order k.

Sections 5.2.2, 5.2.3, 5.3 of Notes.

In order to fill out the required Student Evaluation of the course (OPIS) you will need one of the following course codes:

EHF5ITLR 10589493 - DISCRETE MATHEMATICS INGEGNERIA DELLE COMUNICAZIONI
W9WUAP0Q 10589493 - DISCRETE MATHEMATICS INGEGNERIA ELETTRONICA
CHEHX4DF 1021828 - MATEMATICA DISCRETA INGEGNERIA DELLE COMUNICAZIONI
CA7X1UKX 1021828 - MATEMATICA DISCRETA INGEGNERIA ELETTRONICA

22 Thursday, May 16, Lecture 50,51,52

An important example of a nonlinear recursion: Catalan numbers. Quadratic recursion. A generating function for the Catalan number sequence. Some objects counted by Catalan numbers: Dyck paths, ballot sequences, parentheses in a nonassociative product, triangulations of a convex polygon. A closed formula for the n-th Catalan number. The ring of formal series. Convolution of sequences. Composition of formal series.

Sections 5.4, 5.5 of Notes.

23 Sample Test

The following is a sample test in preparation for the second Midterm test. To be discussed in class.

Sample Test for Discrete Mathematics

May 2019

1. Write all the words of the binary code C whose generating matrix is

$$G = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \end{pmatrix}$$

   How many words are there? Find the corresponding matrix H.

2. Give the definition of a perfect code. Show that the Hamming $[7, 4]$ code is perfect.

3. There are 2^n binary sequences of length n (with digits 0 and 1).

   (a) How many sequences of length 12 have exactly 6 zeros?

   (b) How many have more zeros than ones?

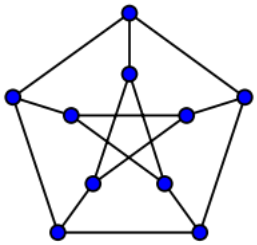
4. Solve the recurrence $a_n = 6a_{n-1} - 11a_{n-2} + 6a_{n-3}, n \geq 4$ with $a_1 = 3, a_2 = 6, a_3 = 14$. What is the value of a_{15}?

5. State and prove (with your favourite method) the convolution identity of Vandermonde.

6. Illustrate in the case $n = 9$ the natural bijection between partitions of 9 into odd parts and partitions of 9 into distinct parts.

7. What is the generating function of the Fibonacci numbers and how do we obtain it?

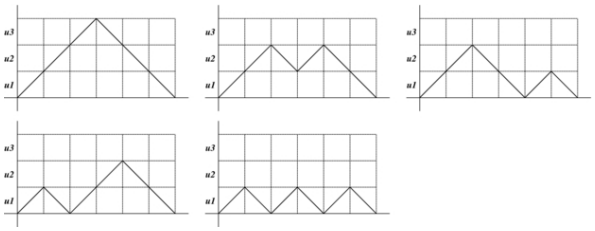
8. Write the adjacency matrix of the following graph (Petersen's graph)



9. Explain whether it is possible to find an Eulerian trail in Petersen's graph.

10. A *Dyck path* is a path on the points of the plane with integer coordinates ("on a graph paper") that, starts from the origin $(0,0)$ and then, using only North-East steps of one unit, and South-East steps, also of one unit, arrives at the point $(2n,0)$ without ever going below the x-axis.

    Find a formula for D_n, the number of Dyck paths with $2n$ steps. (Below you can see the paths with six steps so that $D_3 = 5$).



24 Monday, May 20, Lecture 53,54

Partitions of integers and composition of integers. The number of compositions of an integer n is 2^{n-1}. The number of compositions of an integer n into a fixed number k of parts is $\binom{n-1}{k-1}$.

Much more subtle is the number $p(n)$ of partitions of an integer n.

Euler generating function for the sequence $p(n)$ of partitions: $\prod_{n=1}^{\infty} \frac{1}{1-x^n}$. Euler partition identity: the number of partitions of n into odd parts is the same as the number of partitions of n into distinct parts. Two proofs of Euler's partition identity: a combinatorial proof, giving an explicit bijection, and an analytic proof using the generating function.

Some interesting properties of binomial coefficients. The sum of each row of Pascal's triangle is a power of 2. The alternating sign of each row is zero.

Vandermonde convolution identity: a combinatorial proof and an analytic proof.

Chapter 6 and Section 7.3 of Notes.

25 Thursday, May 23, Lecture 55,56,57

Definition of graph. Graphical representation. Examples. Degree of a vertex. Handshaking lemma. Complete graphs, cycles, hypercubes, bipartite graphs. Adjacency matrix and Incidence matrix.

Connected graphs. Königsberg bridges problem. Eulerian circuit and Eulerian trail. Euler theorem on the necessary and sufficient condition for the existence of an Eulerian circuit. Hamiltonian cycles, sufficient conditions for the existence of a Hamiltonian cycle: Dirac and Ore theorems. Planar graphs. Euler relation $r = e - v + 2$. Graph coloring, chromatic number, Four Color Theorem.

Section 8.1, 8.2 (except pag 162), 8.3, 8.6, 8.7, 8.8 (up to Euler theorem), 8.9 of Notes.

26 Monday, May 27, Lecture 58,59

Solutions of several exercises.

27 Thursday, May 30, Lecture 60,61,62

I regret to notice that in spite of the many repeated requests by me to clearly print your Last Name on the top left corner of the front page of the Problem Sheet, 5 out of 44 students (that's over 11 percent) did not do that: 2 put their first name first, 1 put no name, 2 handed-in no Problem Sheet at all. For the coming year, I will reevaluate whether it is worthwhile on my part to spend so much time on organizing midterms, preparing several different versions of the problems, grading work which sometimes is unreadable, when on your part there is no real effort to help me out in these matters.

The grading of your work will be slow.

I will keep you posted.

28 Second Midterm

Second Mid-term test

30 May 2019

1. Find a generating matrix and a parity-check matrix for the linear code C generated (as a vector space) by

$$S = \{11101, 10110, 01011, 11010\}$$

Solution.

Consider the matrix

$$\begin{pmatrix} 1 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 \end{pmatrix}$$

and reduce to RREF

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Hence the generating matrix is

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \end{pmatrix}$$

which is in standard form; so that the parity check matrix is

$$H = \begin{pmatrix} 0 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 \end{pmatrix}$$

2. Solve $a_n = -a_{n-1} + 8a_{n-2} + 12a_{n-3}, n \geq 3, a_0 = 2, a_1 = -1, a_2 = 0$. What is a_{20}?

   Solution. We can immediately write the characteristic equation of the recursion:

   $$x^3 + x^2 - 8x - 12 = 0$$

   this is clearly solved by -2 and after dividing by $x + 2$ we get $x^2 - x - 6 = (x - 3)(x + 2)$. In other words, the polynomials has a double root -2, and a simple root 3. So the solution is going to be of the form

   $$\alpha_1(-2)^n + \alpha_2 n(-2)^n + \alpha_3 3^n$$

   Substituting the initial conditions we get

   $$\begin{cases} \alpha_1 + \alpha_3 = 2 \\ -2\alpha_1 - 2\alpha_2 + 3\alpha_3 = -1 \\ 4\alpha_1 + 8\alpha_2 + 9\alpha_3 = 0 \end{cases}$$

   Solving this we get

   $$\alpha_1 = \frac{46}{25}, \alpha_2 = -\frac{11}{10}, \alpha_3 = \frac{4}{25},$$

   and $a_{20} = 536746212$.

3. Use a generating function to compute the number of partitions of 10 into even parts.

   Solution. The generating function for partitions into even parts is

   $$\prod_{n>0} \frac{1}{1 - q^{2n}}$$

   and we need to find the coefficient of q^{10} in this function. For this consider the product

   $$(1 + q^2 + q^4 + q^6 + q^8 + q^{10})(1 + q^4 + q^8)(1 + q^6)(1 + q^8)(1 + q^{10})$$

   the coefficient of q^{10} in this product is 7.

4. Compute the generating function for the sequence defined by

$$a_0 = 3, a_1 = -1, a_n = a_{n-1} + a_{n-2}, n \geq 2$$

Solution. Many students seem to confuse the concept of generating function with the closed formula for a recursion. The two are related but different concepts. In this case, we need to mimic the proof of the generating function for the classic Fibonacci formula:

$$\begin{aligned} &a_0 + a_1 t + a_2 t^2 + a_3 t^3 + \cdots \\ &\quad -(a_0 t + a_1 t^2 + \cdots) \\ &\qquad\quad - (a_0 t^2 + \cdots) = f(t) - t f(t) - t^2 f(t) \end{aligned}$$

this gives

$$a_0 + (a_1 - a_0)t = f(t)(1 - t - t^2)$$

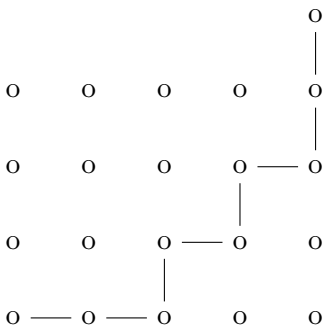
from which

$$f(t) = \frac{a_0 + (a_1 - a_0)t}{1 - t - t^2} = \frac{3 - 4t}{1 - t - t^2}$$

So this is the desired g.f.:

$$\boxed{f(t) = \frac{3 - 4t}{1 - t - t^2}}$$

5. Consider lattice paths that start at $(0, 0)$ and arrive at (m, n) $(m, n > 0)$ and that use only right steps R on 1 unit or up steps U of one unit. For example:



How many such paths are there from $(0, 0)$ to a fixed point (m, n)?

Solution. To reach (m, n) there must be m U steps and n R steps. We need only decide which among the $m + n$ possible steps are the U steps (the other are the R steps). The solution is therefore

$$\binom{m+n}{m} = \binom{m+n}{n}$$

6. What if the path of the previous exercise can touch the line $y = x$ but it is never allowed to go above it; in that case, how many paths are there?

Solution. In this case we assume $m = n$. The desired paths are clearly in a bijection with Dyck paths and are therefore counted by the Catalan number $C_n = \frac{1}{n+1}\binom{2n}{n}$.

7. Prove that if you choose 19 distinct integers in the set

$$S = \{1, 4, 7, 10, 13, 16, ..., 94, 97, 100\}$$

there are at least two distinct integers among them whose sum is 104.

Solution.

There are 16 pairs among these numbers that can add up to 104. E.g., 100 and 4, 97 and 7, etc. Plus the numbers 1 and 52 that cannot be part of such pairs. If we take 19 numbers from that set there is certainly at least one pair that sum up to 104.

8. Prove that if n is an odd integer greater than 1 then the sequence

$$\binom{n}{1}, \binom{n}{2}, \ldots, \binom{n}{\frac{n-1}{2}}$$

contains an odd number of odd numbers.

(Hint: what is the sum of one row of the Pascal triangle?)

Solution. If n is odd then the corresponding row of Pascal's triangle has an even number of coefficients. The sum of that row is 2^n, the sum of half of the row is therefore $\frac{1}{2}2^n = 2^{n-1}$. Our list starts from $\binom{n}{1}$, hence it is missing $\binom{n}{0} = 1$. So the sum of those numbers is

$$2^{n-1} - 1$$

which is an odd number. Therefore there must be an odd number of odd numbers in that list.

9. For the following graph:

   (a) write an adjacency matrix;

   (b) is there an Eulerian circuit?

   (c) is there an Eulerian trail?

Solution. A possible matrix is

$$\begin{pmatrix} 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 2 \\ 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 2 \\ 1 & 2 & 1 & 2 & 0 \end{pmatrix}$$

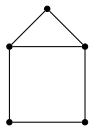
By Euler's theorem there is no Eulerian circuit because there are two odd vertices, there is however an Eulerian trail.

10. For the following graph, determine:

    (a) whether Dirac's theorem can be applied;

    (b) whether Ore's theorem can be applied;

    (c) is there a Hamiltonian cycle?



Solution. The graph has $n = 5$ vertices so $\frac{n}{2} = 2.5$ and there are vertices with degree 2, so Dirac's theorem does not apply.

Also, there are two nonadjacent vertices whose degree is 2 so the sum is $4 < 5$, and so Ore's theorem does not apply.

However, there is clearly a Hamiltonian cycle.

11. How many positive integers not exceeding 2001 are multiples of 3 and 4 but not of 5?

Solution. There are 667 multiples of 3, 500 multiples of 4, 166 multiples of 12, 133 multiples of 15, 100 multiples of 20 and 33 multiples of 60.

The total is 667+500-166-133-100+33=801.

The following exercises are optional

Consider the set

$$S = \{1, 5, 9, 13, 17, \ldots\} = \{4n - 3 | n \in \mathbb{N}\}$$

12. Prove that S is closed under multiplication, namely, prove that if s_1 and s_2 are in S then $s_1 s_2 \in S$.

    Split S into three disjoint subsets : $\{1\}$, those elements of S which have exactly two factors in S, and all the rest. Call the elements in the second set S-primes and all the others, except 1, S-composites.

    Clearly, any prime in S is also an S-prime.

13. Give some examples of S-primes that are not primes.

14. Are there infinitely many S-primes?

15. Show that in S there is no uniqueness of factorization into S-primes.

16. Prove the following theorem.

    Theorem 1. *Let d be an odd positive integer, then a binary code of type (n, M, d) exists if and only if there exist one of type $(n + 1, M, d + 1)$.*

29 Results of the Second Test

The results are out, see below. There will be the grade for the second Test and also a proposed final grade for the whole course. If the final grade is not of your liking you may decide to renounce and instead going to take a final exam in one of the scheduled occasions. The closest date is June 14, the following is July 12 and then again in September, January, February. I would appreciate if you could email me your decision as soon as possible. In any case, for those of you who are content with the result, you MUST register on INFOSTUD (https://stud.infostud.uniroma1.it/Sest/Log/Corpo.html) for the final exam of June 14 so I have an official roster where to record your grade. There is, of course, no final grade for those who passed only one of the two tests.

I want to clarify that if I do not receive any explicit request on your part but you did register for June 14, I assume that you accept the result. This means that your final grade will be recorded as announced. For those who have passed only one of the two midterms, unless you tell me differently, I will assume that you want to be tested only on the missed part. If I get no notice from you and there is no registration for June 14 I assume you want to take the complete final exam at a later date.

WARNING: Please notice that the registration to the test of June 14 is only possible before June 10 at 23:59. If you do not register by then your grade in the midterms will be cancelled.

Email me if something is not clear.

Here you can find the list of grades: https://docs.google.com/a/uniroma1.it/viewer?a=v&pid=sites&srcid=dW5pcm9tYTEuaXR8c3RlZmFub2NhcHBhcmVsbGl8Z3g6NmM1ODI4YzVhNzYzMzcxMg

30 Summary of Syllabus for the whole course.

Natural Numbers. Induction Principle and well ordering principle. Perfect numbers. Mersenne Numbers. (1.1-1.3 Notes) Euclid's formula for even perfect numbers Euler's converse. Greatest common divisor and Bezout identity. Fundamental theorem of arithmetic. Existence of infinitely many primes. Euclid's proof and Euler's proof. Continued fractions and some of their basic properties (Notes 1.4,1.5) Sum of powers of integers. Congruence relations and properties. Modula arithmetic and the quotient set Zn. Ring and field structure in Zn. Invertible elements in Zn. Computation of the inverse using the Bezout identity. Divisibility criteria.

Fermat Little Theorem. Carmichael numbers. (Notes 1.6)

Solution of linear congruences. Applications of congruences. Systems of congruences. Chinese Remainder Theorem. (CRT). (Notes 1.7) Case of moduli not coprime. Definition of Euler ϕ function and its properties. (Notes 1.8)

Formula for ϕ. Euler Theorem Introduction to the concept of group. Definitions and examples. Numerical groups (Z, Q, R, C), matrix groups, permutation groups, dihedral groups. Order of a group and order of an element of a group. Cyclic groups. Lagrange and Euler Theorems. (Notes 2.1, 2.2)

Corollary of Lagrangess theorem. Homomorphisms and isomorphisms. Isomorphism between Cn, the groups of n-th roots of 1 C, and Zn. Classification of cyclic groups. Definition of ring and field. Examples. Finite fields Zp. An example of a field with 9 elements with 2x2 matrices over Z3

. (Notes 2.3, 2.4, 2.5) Finite fields Classification theorem of finite fields. Characteristic of a field. Construction of a field with pn elements. Irreducible polynomials. (Notes 2.5, 2.6)

Perpetual Calendar Primitive elements of F9. Study of irreducibility of a 4th degree polynomial. Construction of a field with 16 elements. First elements of cryptography. Basic definitions. Some classic cibersystems. Caesars cipher and its generalizations. Hills cipher. Permutation cipher. Monoalphabetic and polyalphabetic ciphers. Vignres cipher. Cryptoanalysis of Vignres cipher: Kasiskis test and coincidence index of Friedman. Diffie and Hellman: key exchange protocol.

Public Key cryptography. RSA system: public key and private key. Signature authentication. Elements of Coding theory. Redundancy. Block codes. Repetition code. Hamming distance. Codes of type (n,M,d). Minimum distance d is related top the number of errors the code can detect. Main problem of coding theory. Aq(n,d). Computation of Aq(n,1), Aq(n,n), A2(5,3). Equivalence of codes. (Notes 3.2, 3.3, 3.4, 4.1, 4.2)

Binary codes. Spheres. Hamming inequality. Perfect codes. Construction of a perfect code from Fano plane: Hamming code of type [7,4]. Linear codes. Generating matrix. Weight. (Notes 4.3, 4.4, 4.5) Coding using via a generating matrix of Hamming [7,4]. Equivalent linear codes. Operations on row and column of a generating matrix. Standard form of the generating matrix. Parity check matrix. (Notes 4.6)

Decoding using the standard array and syndrome decoding. Family of Hamming codes Ham(r,q). Sequences defined by recursions. Fibonacci sequence and Binet formula. (Notes 4.7, 4.8, 5.1, 5.2) Vector space method, matric method, generating function method. Generalization. (Notes 5.1, 5.2, 5.3) Ring of formal series. Convolution product of two sequences and composition of series.

Catalan numbers: their generating function, their closed formula. Examples of sets counted by Catalan numbers. (Notes 5.4, 5.5)

Integer partitions. Ferrers diagram. Generating function for the number of partitions p(n) of n. Eulers theorem: Analytic proof and combinatorial proof. Binomial coefficients: some identities. Vandermonde convolution: Analytic proof and combinatorial proof. Pigeonhole principle. (Notes Chapter 6 and 7 (Skip 7.2)) Basic definitions of graph theory. Some special graphs. Eulerian trails and circuits. Adjacency matrix and Incidence matrix of a graph. Hamiltonian cycles: Diracs and Ores theorem. Graph coloring. (Notes Chapter 8 (Skip 8.5, skip 8.10))

References

[1] M. Aigner, G.M. Ziegler, *Proofs from the BOOK*, Springer, 2010.

[2] G. Andrews, K. Eriksson, *Integer Partitions*, Cambridge University Press, 2004

[3] G. Andrews, *Number Theory*, Dover, 1994

[4] G. Andrews, *The Theory of Partitions*, Cambridge University Press, 1984

[5] M.W. Baldoni, C. Ciliberto, G.M. Piacentini Cattaneo, *Aritmetica, Crittografia e Codici*, Springer-Verlag, Milano, 2006

[6] N.L. Biggs, *Discrete Mathematics*, Oxford University Press, 2002.

[7] R.A. Brualdi, *Introductory Combinatorics, 3rd Ed.*, Prentice Hall, 1999.

[8] S. Capparelli, A. Del Fra, Geometria, Esculapio Ed., 2015.

[9] S. Capparelli, P. Maroscia, Alcuni Problemi di Matematica Discreta, Progetto Alice, **39** Vol. XIII, 2012, (379-410)

[10] M. Cerasoli, F. Eugeni, M. Protasi, *Elementi di Matematica Discreta*, Zanichelli 1988

[11] T.S. Chihara, *An Introduction to Orthogonal Polynomials*, Gordon and Breach, New York, London, Paris, 1978

[12] W. Diffie and M. E. Hellman, *New directions in cryptography*, IEEE Transactions on Information Theory **22** (1976), 644-654.

[13] D. S. Dummit, R. M. Foote, *Abstract Algebra*, Wiley, 2003

[14] L. Euler, Solutio problematis ad geometriam situs pertinentis, Commentarii Academiae Scientiarum Imperialis Petropolitanae 8: (128-140), 1736.

[15] L. Euler, Introductio in Analysin infinitorum, Vol.1, Chap. XVI

[16] R. Hill, *A First Course in Coding Theory*, Clarendon Press, Oxford, 1993.

[17] D. E. Knuth, *The Art of Computer Programming, Vol. I, Fundamental Algorithms*, Addison-Wesley, 1997

[18] R. Graham, D. Knuth, O. Patashnik, *Concrete Mathematics*, Addison Wesley 1988

[19] C. T. Long, *Strike it out – add it up*, The Mathematical Gazette, Vol. 66, No. 438, 1982, 273-277.

[20] P. Maroscia, *Geometria e Algebra Lineare*, Zanichelli, 2002.

[21] P. Maroscia, *Introduzione alla Geometria e all'Algebra Lineare*, 2000.

[22] J. Matoušek, J. Nešetřil, *Invitation to Discrete Mathematics*, Clarendon Press, Oxford, 1998

[23] R. A. Mollin, *An Introduction to Cryptography*, Second Edition, Chapman and Hall/CRC Press, 2007

[24] G. M. Piacentini Cattaneo, *Algebra*, Zanichelli, 1996

[25] R. L. Rivest, A. Shamir, and L. Adleman, *A method for obtaining digital signatures and public-key cryptosystems*, Communications of the A.C.M. **21** (1978),120-126.

[26] K. J. Rosen, Discrete Mathematics and its applications, McGraw Hill.

[27] M. R. Schroeder, *Number Theory in Science and Communication*, Fifth Edition, Springer, 2009

[28] D. Shanks, *Solved and Unsolved Problems in Number Theory*, Chelsea, New York 1962

[29] C.J. Stam, J.C. Reijneveld, Graph theoretical analysis of complex networks in the brain, Nonlinear Biomedical Physics, 2007, 1:3

[30] R. Stanley, *Enumerative Combinatorics* Vol.1, Cambridge Studies in Advanced Mathematics, Cambridge Univ. Press, 1999

[31] D. R. Stinson, *Cryptography Theory and Practice*, Second Edition, Chapman and Hall/CRC Press, 2002

[32] R. Sullivan, *Microwave radar: imaging and advanced concepts*, Artech House Radar Library, 2000.

[33] $https://www.ted.com/talks/eduardo\_saenz\_de\_cabezon\_math\_is\_forever\#t-569375$

[34] D. West, *Introduction to Graph Theory*. Upper Saddle River, NJ, Prentice Hall, 1996.

[35] H. S. Wilf, *Generatingfunctionology*, Academic Press, 1990.
