"Sapienza" University of Rome
Faculty of Information Engineering,
Informatics and Statistics
Department of Computer Science

Discrete Mathematics

Lecture notes integrated with the book "TODO",
Author TODO, ...

Author
Alessio Bandiera

March 25, 2024

Contents

Information and Contacts

Personal notes and summaries collected as part of the *Discrete Mathematics* course offered by the degree in Computer Science of the University of Rome "La Sapienza".

Further information and notes can be found at the following link:
https://github.com/aflaag-notes. Anyone can feel free to report inaccuracies, improvements or requests through the Issue system provided by GitHub itself or by contacting the author privately:

- Email: **alessio.bandiera02@gmail.com**
- LinkedIn: **Alessio Bandiera**

The notes are constantly being updated, so please check if the changes have already been made in the most recent version.

Suggested prerequisites:

- Differential Calculus
- Integral Calculus

Licence:

1

TODO

1.1 Solved exercises

1.1.1 Number theory

Problem 1: $n^2 + n$ is even

Show that for every $n \in \mathbb{N}$, $n^2 + n$ is an even number.

Proof. Note that $n^2 + n = n \cdot (n+1)$, hence:

- if n is even, then
$$\exists k \in \mathbb{N} \mid n = 2k \implies n(n+1) = 2k(2k+1) = 4k^2 + 2k = 2(k^2 + k)$$
which is an even number;
- if n is odd, then
$$\exists k \in \mathbb{N} \mid n = 2k+1 \implies n(n+1) = (2k+1)(2k+2) = 4k^2+6k+2 = 2(2k^2+3k+1)$$
which is an even number.

□

Problem 2: $4n - 1$ is not prime

Show that there are infinitely many numbers of the form $4n-1$ that are not prime.

Proof. Note that
$$\forall x^2 \in \mathbb{N} - \{0\} \quad 4x^2 - 1 = (2x+1)(2x-1)$$
which is a proper factorization of $4x^2 - 1$, hence every perfect square yields a number of the form $4n - 1$ which is not a prime number. Note that the number of perfect squares is

infinite since the set of perfect square has the same cardinality of $\mathbb{N}$ since it's possibile to construct a bijective function as follows:

$$f : \mathbb{N} \to \mathbb{N} : x \mapsto x^2$$

Also, note that this proof does not show *every non-prime number of the form* $4n - 1$, since that is outside the scope of the problem. □

Problem 3: The $4n - 3$ set

Consider the following set:

$$S := \{4n - 3 \mid n \in \mathbb{N}\}$$

1. Show that S closed under multiplication.
2. A number p is said to be S-*prime* if and only if p is the product of exactly two factors of S; for example, even though $3^2 = 9 \notin \mathbb{P}$ we have that $9 = 1 \cdot 9$, and since $1 = 4 \cdot 1 - 3 \in S$ and $9 = 4 \cdot 3 - 3 \in S$, then 9 is S-prime. Is the set of S-prime numbers infinite?
3. TODO

Proof.

1. To show that S is closed under multiplication, it suffices to show that

$$\forall a, b \in \mathbb{N} \quad (4a - 3)(4b - 3) = 16ab - 12a - 12b + 9 = 4(4ab - 3a - 3b + 3) - 3 \in S$$

2. TODO

□

1.1.2 Induction

Problem 4: Cardinality of the power set

Show that for every given set S such that $n := |S|$ it holds that $|\mathcal{P}(S)| = 2^n$.

Proof. The statement will be shown by induction over n, the number of elements contained into S.

Base case. $n = 0 \implies S = \varnothing \implies \mathcal{P}(S) = \mathcal{P}(\varnothing) = \{\varnothing\} \implies |\mathcal{P}(S)| = 1 = 2^0 = 2^n$.

Inductive hypothesis. Assume that the statement is true for some fixed integer n.

Inductive step. It must be shown that, for a given set of elements S such that $|S| = n + 1$, it holds true that $|\mathcal{P}(S)| = 2^{n+1}$. Consider a subset $S' \subseteq S$ such that $|S'| = |S| - 1 = n + 1 - n = n$, hence for the inductive hypothesis we have that

$|\mathcal{P}(S')| = 2^n$. Thus, to get the cardinality of $\mathcal{P}(S)$ the $(n+1)$-th element inside $S - S'$ must be paired with every of the sets contained inside $\mathcal{P}(S')$, hence

$$\mathcal{P}(S) = 2 \cdot \mathcal{P}(S') = 2 \cdot 2^n = 2^{n+1}$$

□

1.1.3 Continued fractions

Problem 5: Limits of continued fractions

1. What is the value that the following limit approaches?

$$\lim_{n \to +\infty} [2; 1, 4, n]$$

2. Consider the following sequence:

$$\frac{25}{16}, \frac{49}{36}, \frac{81}{64}, \frac{121}{100}, \ldots$$

   Compute the continued fractions of these ratios; what is the limit of this sequence?

Proof.

1. By using the CFA, we get the following table:

C.F.		2	1	4	n
N	1	2	3	14	$14 \cdot n + 3$
D	0	1	1	5	$5 \cdot n + 1$

   which means that

$$[2; 1, 4, n] = \frac{14n + 3}{5n + 1} \implies \lim_{n \to +\infty} \frac{14n + 3}{5n + 1} = \frac{14}{5}$$

2. We can convince ourselves that the sequence is

$$\left(\frac{2k + 1}{2k}\right)^2$$

   for some $k \in \mathbb{N}$. Thus we can compute the continued fractions of the given ratios (calculations omitted) and get the following results:

$$\begin{aligned}
k=2 &\implies \left(\frac{2\cdot 2+1}{2\cdot 2}\right)^2 = \left(\frac{5}{4}\right)^2 = \frac{25}{16} = [1;1,1,3,2]\\
k=3 &\implies \left(\frac{2\cdot 3+1}{2\cdot 3}\right)^2 = \left(\frac{7}{6}\right)^2 = \frac{49}{36} = [1;2,1,3,3]\\
k=4 &\implies \left(\frac{2\cdot 4+1}{2\cdot 4}\right)^2 = \left(\frac{9}{8}\right)^2 = \frac{81}{64} = [1;3,1,3,4]\\
k=5 &\implies \left(\frac{2\cdot 5+1}{2\cdot 5}\right)^2 = \left(\frac{11}{10}\right)^2 = \frac{121}{100} = [1;4,1,3,5]
\end{aligned}$$

and we can easily prove that

$$\left(\frac{2k+1}{2k}\right)^2 = [1;k-1,1,3,k]$$

by using the CFA and constructing the following table:

C.F.		1	$k-1$	1	3	k
N	1	1	k	$k+1$	$4k+3$	$4k^2+4k+1$
D	0	1	$k-1$	k	$4k-1$	$4k^2$

Ultimately, the limit approaches

$$\lim_{k\to+\infty} \frac{4k^2+4k+1}{4k^2} = \frac{4}{4} = 1$$

□

Problem 6: Binomial coefficients

Prove that

$$\forall p \in \mathbb{P}, k \in \mathbb{N} \mid p > k > 1 \quad \binom{p}{k} \equiv 0 \pmod{p}$$

Proof. Note that

$$\binom{p}{k} = \frac{p!}{k!(p-k)!} = p \cdot \frac{(p-1)!}{k!(p-k)!} \implies p \Bigg| \binom{p}{k}$$

and note that, since $p \in \mathbb{P}$, p can't be simplified with any of the factors of the denominator (since $p > k$ and $p > p-k$ because $k > 1$), hence

$$\binom{p}{k} \equiv 0 \pmod{p}$$

□

Problem 7: Systems of congruence equations

Solve the following system:

$$\begin{cases} x + 2y \equiv 4 \pmod 7 \\ 4x + 3y \equiv 4 \pmod 7 \end{cases}$$

Are there any solutions in $\mathbb{Z}_5$?

Proof. Note that

$$x + 2y \equiv 4 \pmod 7 \iff x = 4 - 2y \pmod 7$$

that we can substitute x in the second equation as follows

$$4 \cdot (4 - 2y) + 3y \equiv 16 - 8y + 3y \equiv 2 - 5y \equiv 4 \pmod 7 \iff$$
$$\iff -5y \equiv 2 \pmod 7 \iff 2y \equiv 2 \pmod 7 \iff y \equiv 1 \pmod 7$$

and then

$$x + 2 \cdot 1 \equiv 4 \pmod 7 \iff x \equiv 2 \pmod 7$$

Instead, if we try to solve the following system

$$\begin{cases} x + 2y \equiv 4 \pmod 5 \\ 4x + 3y \equiv 4 \pmod 5 \end{cases}$$

and we substitute x in the second equation, we get that

$$16 - 8y + 3y \equiv 1 - 5y \equiv 4 \pmod 5 \iff -5y \equiv 5 \pmod 5$$

but since $\gcd(-5, 5) = -5 \neq 1$ then $[5] \notin \mathbb{Z}_5^*$, which means that the system has no solutions. □

Problem 8: Quadratic congruence equations

Solve the following equation in $\mathbb{Z}_{11}$

$$x^2 + 3x + 4 \equiv 0 \pmod{11}$$

Proof. By solving for x in $\mathbb{Z}_{11}$ we get that

$$x_{1,2} \equiv \frac{-3 \pm \sqrt{9 - 4 \cdot 4}}{2} \equiv \frac{-3 \pm \sqrt{-7}}{2} \equiv \frac{-3 \pm \sqrt{4}}{2} \equiv \frac{-3 \pm 2}{2} \equiv \frac{8 \pm 2}{2} \implies \begin{cases} x \equiv 5 \pmod{11} \\ x \equiv 3 \pmod{11} \end{cases}$$

□

Problem 9: Divisibility criterion for 13

Given $n = n_1 \dots n_k$, prove that n is a multiple of 13 if and only if $n_1 \dots n_{k-1} + 4n_k$ is a multiple of 13. Is 2024 a multiple of 13?

Proof. Since

$$4 \cdot 10 \equiv 40 \equiv 1 \pmod{13} \iff 10^{-1} \equiv 4 \pmod{13}$$

we can apply the following steps:

$$n \equiv 0 \pmod{13}$$
$$\sum_{i=1}^{k} n_i \cdot 10^{k-i} \equiv 0 \pmod{13}$$
$$\sum_{i=1}^{k-1} n_i \cdot 10^{k-i} + n_k \cdot 10^0 \equiv 0 \pmod{13}$$
$$10 \cdot \sum_{i=1}^{k-1} n_i \cdot 10^{k-i-1} + n_k \equiv 0 \pmod{13}$$
$$\sum_{i=1}^{k-1} n_i \cdot 10^{k-i-1} + 4n_k \equiv 0 \pmod{13}$$

Applying this formula to 2024 recursively, we can check that

$$202 + 4 \cdot 4 = 202 + 16 = 218$$
$$21 + 4 \cdot 8 = 21 + 32 = 53$$
$$5 + 4 \cdot 3 = 5 + 12 = 17$$

and since 17 is prime, it can't be a multiple of 13, which means that 2024 is not a multiple of 13. □

Problem 10: Divisibility criterion for 13

By imitating the divisibility criterion for 7, invent a divisibility criterion for 13.

Proof. By imitating the divisibility criterion for 7, to check if a number is divisible by 13 the following procedure can be applied (remembering that $10 \equiv -3 \pmod{13}$):

$$n_1 \ldots n_k \equiv \sum_{i=1}^{k} n_i \cdot 10^{k-i} \equiv n_1 10^{k-1} + \ldots + n_{k-1}10^1 + n_k 10^0 \equiv$$
$$\equiv 10 \cdot \left(n_1 10^{k-2} + \ldots + n_{k-1}10^0\right) + n_k \equiv -3 \cdot \left(n_1 10^{k-2} + \ldots + n_{k-1}10^0\right) + n_k \equiv: n' \pmod{13}$$

and the same process can be repeated for n' recursively, until the number can be trivially checked. □

Problem 11: Quadratic equations in $\mathbb{Z}_6$

Invent a quadratic equation in $\mathbb{Z}_6$ that has more than 2 solutions. Could the quadratic formula be used in this situation?

Proof. Consider the following quadratic equation:

$$x^2 + 3x + 2 \equiv 0 \pmod{6}$$

this equation is satisfied by the following two values for x:

$$\begin{cases} x_1 \equiv 2 \pmod{6} \implies 2^2 + 3 \cdot 2 + 2 \equiv 4 + 6 + 2 \equiv 4 + 2 \equiv 6 \equiv 0 \pmod{6} \\ x_2 \equiv 4 \pmod{6} \implies 4^2 + 3 \cdot 4 + 2 \equiv 16 + 12 + 2 \equiv 4 + 2 \equiv 6 \equiv 0 \pmod{6} \end{cases}$$

But this equation is also satisfied by the following two values for x:

$$\begin{cases} x_1 \equiv 1 \pmod{6} \implies 1^2 + 3 \cdot 1 + 2 \equiv 1 + 3 + 2 \equiv 6 \equiv 0 \pmod{6} \\ x_2 \equiv 5 \pmod{6} \implies 5^2 + 3 \cdot 5 + 2 \equiv 25 + 15 + 2 \equiv 1 + 3 + 2 \equiv 6 \equiv 6 \equiv 0 \pmod{6} \end{cases}$$

Note that the quadratic formula couldn't be used in this situation, because the product

$$\left(-b \pm \sqrt{b^2 - 4ac}\right) \cdot (2a)^{-1}$$

requires a product by 2^{-1}, which is not defined in $\mathbb{Z}_6$ since $\gcd(2, 6) = 2 \neq 1$. □

Problem 12: Remainders

Find the remainder of the division by 9 and by 10 of the number

$$325437^{759}$$

Proof. We can compute the remainder of the division by 9 by doing the following:

$$325437^{759} \equiv 6^{759} \equiv 6^{9 \cdot 84 + 3} \equiv 10077696^{8}4 \cdot 216 = 0 \pmod{9}$$

Likewise, we can compute the remainder of the division by 10 by doing the following:

$$\begin{gathered} 325437^{759} \equiv 7^{759} \equiv 7^{9 \cdot 84 + 3} \equiv 40353607^{84} \cdot 343 = 7^{84} \cdot 3 \equiv 7^{8 \cdot 10 + 4} \cdot 3 \equiv \\ \equiv 282475249^{10} \cdot 7^4 \cdot 3 \equiv 9^{10} \cdot 1 \cdot 3 \equiv 3486784401 \cdot 3 \equiv 1 \cdot 3 \equiv 3 \pmod{10} \end{gathered}$$

□

Problem 13: Congruence systems

1. Find the smallest positive solution for the following system

$$\begin{cases} 35841x \equiv 874569 \pmod{9} \\ 4573x \equiv 78654 \pmod{14} \\ 3528 \equiv 85911 \pmod{5} \end{cases}$$

2. If

$$\begin{cases} 325x \equiv 875 \pmod{12} \\ 621x \equiv 377 \pmod{14} \end{cases}$$

is solvable, find a solution.

Proof.

1. First, we can evaluate the smallest class representatives for the given equations in their respective moduli:

$$\begin{cases} 6x \equiv 3 \pmod 9 \\ 9x \equiv 2 \pmod{14} \\ 3x \equiv 1 \pmod 5 \end{cases}$$

Then, in the second and third equation we can remove the x coefficients since

$$\gcd(9, 14) = 1 \implies \exists [9]^{-1} \in \mathbb{Z}_{14}$$
$$\gcd(3, 5) = 1 \implies \exists [3]^{-1} \in \mathbb{Z}_5$$

and in fact

$$9 \cdot 11 \equiv 99 \equiv 1 \pmod{14} \implies [9]^{-1} = [11]$$
$$3 \cdot 2 \equiv 6 \equiv 1 \pmod 5 \implies [3]^{-1} = [2]$$

But since the x coefficient of the first equation is 6, which is not invertible in $\mathbb{Z}_9$, to eliminate the 6 in front of the x we can use the following property

$$\begin{cases} ac \equiv bc \pmod n \\ d := \gcd(c, n) \end{cases} \implies a \equiv b \left(\bmod \frac{n}{d}\right)$$

applied as follows

$$\begin{cases} 3 \cdot 2x \equiv 3 \pmod 9 \\ \gcd(3, 9) = 3 \end{cases} \implies 2x \equiv 1 \pmod 3$$

and since

$$\gcd(2, 3) = 1 \implies \exists [2]^{-1} \in \mathbb{Z}_3$$

we have that

$$2 \cdot 2 \equiv 4 \equiv 1 \pmod 3$$

thus the system becomes

$$\begin{cases} x \equiv 1 \cdot 2 \equiv 2 \pmod 3 \\ x \equiv 2 \cdot 11 \equiv 22 \equiv 8 \pmod{14} \\ x \equiv 1 \cdot 2 \equiv 2 \pmod 5 \end{cases}$$

Now, since 3, 14 and 5 are mutually coprime, we can solve the system by using the CRT, by first getting the following partial results

$$R := 3 \cdot 14 \cdot 5 = 210 \implies \begin{cases} R_1 = \frac{R}{r_1} = 70 \\ R_2 = \frac{R}{r_2} = 45 \\ R_3 = \frac{R}{r_3} = 126 \end{cases}$$

and then solving the following congruence equations

$$R_1 x_1 \equiv c_1 \pmod{r_1} \iff 70x_2 \equiv 2 \pmod 3 \iff 7x_1 \equiv 2 \pmod 3 \iff x_1 \equiv 2 \cdot 4 \equiv 8 \equiv 2 \pmod 3$$
$$R_2 x_2 \equiv c_2 \pmod{r_2} \iff 45x_2 \equiv 8 \pmod{14} \iff 3x_2 \equiv 8 \pmod{14} \iff x_2 \equiv 8 \cdot 5 \equiv 40 \equiv 12 \pmod{14}$$
$$R_3 x_3 \equiv c_3 \pmod{r_3} \iff 126x_3 \equiv 2 \pmod 5 \iff x_3 \equiv 2 \pmod 5$$

Finally, the result of the system is

$$x \equiv R_1 x_1 + R_2 x_2 + R_3 x_3 = 70 \cdot 2 + 45 \cdot 12 + 126 \cdot 2 \equiv 932 \equiv 92 \pmod{210}$$

2. Note that the given system can be rewritten as

$$\begin{cases} x \equiv 11 \pmod{12} \\ 5x \equiv 13 \pmod{14} \end{cases} \iff \begin{cases} x \equiv 11 \pmod{12} \\ x \equiv 13 \cdot 3 \equiv 39 \equiv 11 \pmod{14} \end{cases}$$

which means that TODO prove that it's solvable, and also wyd when 12 and 14?

□

Problem 14: TODO

TODO

Proof. TODO □

Problem 15: Group theory

1. Prove that the only homomorphism between $\mathbb{Z}_{15}$ and $\mathcal{D}_4$ is the trivial homomorphism.
2. Prove that $\mathcal{D}_3$ and $\mathcal{S}_3$ as isomorphic.
3. Show that the kernel of a group homomorphism $f : G \to G'$ is a subgroup of G.
4. With the notations of the previous exercise, show that the image $\operatorname{im} f$ of a group homomorphism is a subgroup of G'.
5. Check that the 24 permutations in $\mathcal{S}_4$ split into two subsets: 12 are even and 12 are odd. Call $\mathcal{A}_n$ the subset of even permutations; check that $\mathcal{A}_4$ is a subgroup of $\mathcal{S}_4$.

Proof.

1. Let

$$f : \mathbb{Z}_{15} \to \mathcal{D}_4$$

be a homomorphism between $(\mathbb{Z}_{15}, +)$ and $(\mathcal{D}_4, \cdot)$; since f is a homomorphism, we have that

$$f([0]) = r_0$$

which means that

$$\forall k \in \mathbb{N} \quad r_0 = f([0]) = f(15k) = f(\underbrace{k + \ldots + k}_{15 \text{ times}}) = \underbrace{f(k) \cdot \ldots \cdot f(k)}_{15 \text{ times}} = f^{15}(k)$$

and in particular, this equation shows that $f(k)$ can't be a symmetry – since no symmetry raised to an odd power, namely 15, can yield r_0 – $f(k)$ must be a rotation, which means that

$$\forall k \in \mathbb{N} \quad r_0 = f^{15 \pmod 4}(k) = f^3(k) \implies f(k) = r_0$$

hence for every $k \in \mathbb{N}$, we have that $f(k) = r_0$. Finally, since this argument doesn't involve any particular characteristic of f – other than f being a homomorphism – this means that every homomorphism must be the trivial homomorphism.

2. TODO

3. To show that $\ker f \leqslant G$, we must show the following properties:

   - since f is a homomorphism, we have that
   $$f(1_G) = 1_{G'}$$
   which means that
   $$1_G \in \ker f$$
   hence $\ker f$ has the identity element;

   - to show the closure under the group operation, we show that
   $$\forall x, y \in \ker f \quad f(x) = f(y) = 1_{G'} \implies f(x \cdot y) = f(x) \cdot f(y) = 1_{G'} \cdot 1_{G'} = 1_{G'}$$
   thus $x \cdot y \in \ker f$

   - note that
   $$\forall x \in \ker f \quad f(x) = 1_{G'} \iff f(x)^{-1} = 1_{G'}^{-1} = 1_{G'}$$
   and since f is a homomorphism, we have that
   $$1_{G'} = f(x)^{-1} = f\left(x^{-1}\right) \implies x^{-1} \in \ker f$$

4. To show that $\operatorname{im} f \leqslant G$, we must show the following properties:

   - note that
   $$f(1_G) = 1_{G'} \implies 1_G \in \operatorname{im} f$$

   - to show the closure under the group operation, we show that
   $$\forall x, y \in \operatorname{im} f \quad \exists a, b \in G \mid \begin{cases} x = f(a) \\ y = f(b) \end{cases}$$
   meaning that
   $$x \cdot y = f(a) \cdot f(b) = f(a \cdot b) \implies \exists a \cdot b \in G \mid x \cdot y = f(a \cdot b) \implies x \cdot y \in \operatorname{im} f$$

   - note that
   $$\forall x \in \operatorname{im} f \quad \exists a \in G \mid f(a) = x \iff$$
   $$\iff f(a)^{-1} = x^{-1} \iff f\left(a^{-1}\right) = x^{-1} \implies x^{-1} \in \operatorname{im} f$$

$\square$