"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 11, 2024

Contents

Information and Contacts **1**

1 TODO **2**

1.1 Solved exercises 2

1.1.1 Number theory 2

1.1.2 Induction 3

1.1.3 Continued fractions 4

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

1

TODO

1.1 Solved exercises

1.1.1 Number theory

Problem 1.1.1.1: $n^2 + n$ 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.

$\square$

Problem 1.1.1.2: $4n - 1$ 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. $\square$

Problem 1.1.1.3: 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

$\square$

1.1.2 Induction

Problem 1.1.2.1: 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 1.1.3.1: 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 1.1.3.2: 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

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

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 1.1.3.3: 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. $\square$

Problem 1.1.3.4: 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

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

$\square$

Problem 1.1.3.5: 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 $10 \equiv -3 \pmod{13}$):

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

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

Problem 1.1.3.6: 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:

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

$\square$