Number Theory and Cryptography

Muhammad Mustafa[1]*†

Abstract

This document contains a brief smart collection of all the important notes, definitions, facts and various things about Number Theory and Cryptography, the document will be always updated.

1. DIVISIBILITY

- Definition

  1. a (divides, factor of, divisor of) b or b (divisible by, multiple of, dividend of) a, if $(a,b \in \mathbb{Z}) \wedge (a \neq 0) \wedge \exists_{c \in \mathbb{Z}} (b = ac) \wedge (b \bmod a = 0)$ This denoted by $a \mid b$ and $a \nmid b$ otherwise.

- Useful Facts
  Let $(a,b,c \in \mathbb{Z}) \wedge (a \neq 0)$. Then

  1. $(a \mid b) \wedge (a \mid c) \rightarrow (a \mid (b+c))$
  2. $(a \mid b_1) \wedge (a \mid b_2) \wedge ... \wedge (a \mid b_n) \rightarrow a \mid \sum_{i=1}^{n} b_i c_i$ for any integers $c_1, c_2, ..., c_n$
  3. $(a \mid b) \rightarrow \forall_{c \in \mathbb{Z}} (a \mid bc)$
  4. $(a \mid b) \wedge (b \mid c) \rightarrow (a \mid c)$
  5. $(a,b > 0) \wedge (a \mid b) \rightarrow (a \leq b)$
  6. Integers divisible by the positive integer $d \in \{..., -3d, -2d, -d, 0, d, 2d, 3d, ...\}$

2. The Division Algorithm

- Definition

  1. $(a \in \mathbb{Z}) \wedge (d \in \mathbb{Z}_+) \rightarrow \exists!_{q,r \in \mathbb{Z}} [(0 \leq r < d) \wedge (a = dq + r)]$

     a is called the *dividend*, d is called the *divisor*, q is called the *quotient* and r is called the *remainder*.

- Useful Facts

  1. $q = \lfloor \frac{a}{d} \rfloor = a$ **div** d
  2. $r = a - dq = a - d\lfloor \frac{a}{d} \rfloor = a$ **mod** d
  3. The maximum number $\leq a$ and divisible by d equal $a - r$ equal dq

3. PROCEDURE FOR PAPER SUBMISSION

3.1. Selecting a Template (Heading 2)

First, confirm that you have the correct template for your paper size. This template has been tailored for output on the US-letter paper size. Please do not use it for A4 paper since the margin requirements for A4 papers may be different from Letter paper size.

3.2. Maintaining the Integrity of the Specifications

The template is used to format your paper and style the text. All margins, column widths, line spaces, and text fonts are prescribed; please do not alter them. You may note peculiarities. For example, the head margin in this template measures proportionately more than is customary. This measurement and others are deliberate, using specifications that anticipate your paper as one part of the entire proceedings, and not as an independent document. Please do not revise any of the current designations

4. MATH

Before you begin to format your paper, first write and save the content as a separate text file. Keep your text and graphic files separate until after the text has been formatted and styled. Do not use hard tabs, and limit use of hard returns to only one return at the end of a paragraph. Do not add any kind of pagination anywhere in the paper. Do not number text heads-the template will do that for you.

*This work was not supported by any organization

†[1] LinkedIn:muhammad-mustafa-abdalqadir