Number Theory

Martina Tscheckl

January 4, 2016

Please send feedback to martina@tscheckl.eu.

Contents

Organizatorial stuff

Dates (in TUGrazOnline):

Mon	14:15–15:45	C208	Exercises (starting 19.10. first exercise class)
Tue	14:15–15:45	C307	Lecture (starting 20.10. first (real) lecture)
Wed	08:15–09:45	C208	Lecture

From now until 15.12. lectures by Martin Widmer. Then C. Frei.
End: oral exams
Exercises: Find details on website of the instructor Dijana Kreso. math.tugraz.at/~kreso

0 Basics

$$\mathbb{N} = \{1, 2, \dots\} \tag{1}$$
$$\mathbb{N}_0 = \mathbb{N} \cup \{0\} \tag{2}$$
$$\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\} \tag{3}$$

0.1 Divisibility

Definition 0.1.1. *Let $a, b \in \mathbb{Z}$. a divides b (written $a \mid b$) if $\exists q \in \mathbb{Z} : b = qa$.*
Some properties: Let $a, b, c \in \mathbb{Z}$. Then the following statements hold:

$$a \mid b \Rightarrow ac \mid bc \tag{4}$$
$$a \mid b \wedge b \mid c \Rightarrow a \mid c \tag{5}$$
$$a \mid b \wedge b \mid a \Leftrightarrow a = b \tag{6}$$
$$a \mid b \wedge a \mid c \Rightarrow a \mid (b + c) \tag{7}$$

Definition 0.1.2 (Remainder)**.** *Let $a \in \mathbb{Z}$, $b \in \mathbb{N}$. Then there are unique $q, r \in \mathbb{Z}$ such that*

$$a = qb + r \text{ and } 0 \le r < b.$$