NUMBER THEORY

DIVISIBILITY

WHEN AN INTEGER IS DIVIDED BY A SECOND NONZERO INTEGER, THE QUOTIENT MAY OR MAY NOT BE AN INTEGER. FOR EXAMPLE, 24/8 = 3 IS AN INTEGER. WHILE 17/5 = 3.4 IS NOT. THIS LEADS TO THE FOLLOWING THEOREM:

DEFINITION

IF *a* AND *b* ARE INTEGERS, WE SAY THAT *a DIVIDES b*

(*a* |*b*), IF THERE IS AN INTEGER *c* SUCH THAT $b = ac$.

EXAMPLE: 13 | 182 , -5 | 30, 17 | 289, 7 | 144 (7 does not divide 144)

THEOREM

For integer a, b and c, the following hold: $a \neq 0$

$$(a) \quad a \mid 0, \quad 1 \mid a, \quad -1 \mid a, \quad a \mid a$$

$$(b) \quad If \;\; a \mid b \quad and \quad b \mid a \; then \quad a = \pm b$$

$$(c) \quad If \;\; a \mid b \;\; and \;\; c \mid d \;\; then \;\; ac \mid bd$$

$$(d) \quad If \;\; a \mid b \;\; and \;\; b \mid c \;\; then \;\; a \mid c$$

$$(e) \quad a \mid b \;\; then \;\; a \mid bc$$

$$(f) \quad If \;\; a \mid b \;\; and \;\; a \mid c \;\; then \;\; a \mid (bx + cy) \;\; for \;\; all \;\; x \;\; and \;\; y \in Z$$

THEOREM (DIVISION ALGORITHM)

<u>NUMBER THEORY</u>

LET $a, b \in Z$ WITH $b > 0$. *THEN, THERE* EXIST UNIQUE INTEGERS q AND r SUCH THAT

$$a = bq + r \ , \quad 0 \leq r < b$$