3 Divisibility and Prime Numbers

3.1 Divisibility

Important Definition

Definition 3.1 (Divides)**.** For integers a and b, we say that a **divides** b (denoted $a \mid b$) if there exists an integer k such that:

$$b = a \cdot k.$$

For example:

$$3 \mid 15 \quad \text{since } 15 = 3 \times 5.$$

Remark 3.1. If a does not divide a, we write $a \nmid b$.

Properties of Divisibility

For integers a, b, c:

- If $a \mid b$ and $b \mid c$, then $a \mid c$ (Transitivity).
- If $a \mid b$ and $a \mid c$, then $a \mid (b + c)$ and $a \mid (b - c)$.
- If $a \mid b$, then $a \mid kb$ for any integer k.

Theorem 3.1. *For integers a, b, c, the following hold:*

1. $a \mid 0,\ 1 \mid a,\ a \mid a$.
2. $a \mid 1$ *if and only if* $a = \pm 1$.
3. *If* $a \mid b$ *and* $c \mid d$, *then* $ac \mid bd$.
4. $a \mid b$ *and* $b \mid a$ *if and only if* $a = \pm b$.
5. *If* $a \mid b$ *and* $b \neq 0$, *then* $|a| \leq |b|$.
6. *If* $a \mid b$ *and* $a \mid c$, *then* $a \mid (bx + cy)$ *for arbitrary integers* x *and* y.

Division Algorithm

Theorem 3.2. *Let a, b be integers with $a \neq 0$. Then there exist unique integers q and r such that:*

$$b = aq + r, \quad 0 \leq r < |a|.$$

*where q is called the **quotient**, and r is called the **remainder**.*

Remark 3.2. Divisibility Condition: $a \mid b \iff r = 0$

Theorem 3.3. *For any integer $a \neq 0$ and any integer b, there exist unique integers q (quotient) and r (remainder) such that:*

$$b = aq + r, \quad \textit{where } 0 \leq r < |a|. \tag{1}$$

Proof. Let $(q_1, r_1), (q_2, r_2) \in \mathbb{Z}$, such that

$$b = aq_1 + r_1, \quad \text{where } 0 \leq r_1 < |a|, \tag{2}$$

$$b = aq_2 + r_2, \quad \text{where } 0 \leq r_2 < |a|, \tag{3}$$

From (2) and (3) $b = aq_1 + r_1 = aq_2 + r_2 \Rightarrow aq_1 - aq_2 = r_2 - r_1$.

$$a(q_1 - q_2) = r_2 - r_1. \tag{4}$$

Since $-|a| < -r_1 \leq 0, 0 \leq r_2 < |a|$, then

$$-|a| < r_2 - r_1 < |a|. \tag{5}$$

But from (4) $r_2 - r_1 = a(q_1 - q_2) \Rightarrow r_2 - r_1 = 0 \Rightarrow r_2 = r_1$

Since $a \neq 0$, we must have $q_1 - q_2 = 0 \Rightarrow q_1 = q_2$. □

Example 3.1. Prove that

1. $4 \mid 20$
2. $5 \nmid 23$
3. Every even integer n is divisible by 2
4. Every odd integer n is not divisible by 2 **H.W**

Sol. 1. By Division Algorithm, there exists integers q, r such that:

$$20 = 4q + r.$$

We check:

$$20 = 4 \times 5.$$

Since $q = 5$, and $r = 0$, then

$$4 \mid 20.$$

2. By Division Algorithm, there exists integers q, r such that:

$$23 = 5q + r.$$

We check:

$$23 = 5 \times 4 + 3.$$

Since $q = 5$, and $r = 3$, then

$$5 \nmid 23.$$

3. By Division Algorithm, there exists integers q, r such that:

$$n = 2q + r.$$

The only possible values for r are:

$$r = 0 \quad \text{or} \quad r = 1.$$

Case 1: If $r = 0$

Then

$$n = 2q \Rightarrow 2 \mid n.$$

Case 1: If $r = 1$

Then

$$n = 2q + 1 \Rightarrow n \text{ is odd integer } \textbf{C!}$$

$$\therefore 2 \mid n$$

□

3.2 Prime Numbers

Prime Number

Definition 3.2. A prime number is an integer $p > 1$ that has exactly two distinct positive divisors: 1 and itself.

Formally, p is prime if:

$$p > 1 \quad \text{and} \quad \forall d \mid p, \quad d = 1, \ or \ d = p.$$

Examples: $2, 3, 5, 7, 11, 13, 17, 19, 23, \ldots$

Definition 3.3. A **composite number** is an integer greater than 1 that is **not prime**, meaning **it has at least one divisor** other than 1 and itself.

Examples: $4, 6, 8, 9, 10, 12, 14, 15, \ldots$

Lemma 3.1. If n is composite, then there exist integers a and b, such that:

$$n = ab, \quad 1 < a < n, \quad 1 < b < n.$$

Prime Numbers									
2, 3, 5,	151,	271,	409,	557,	683,	839,	997,	1151,	1301,
7, 11,	157,	277,	419,	563,	691,	853,	1009,	1153,	1303,
13, 17,	163,	281,	421,	569,	701,	857,	1013,	1163,	1307,
19, 23,	167,	283,	431,	571,	709,	859,	1019,	1171,	1319,
29, 31,	173,	293,	433,	577,	719,	863,	1021,	1181,	1321,
37, 41,	179,	307,	439,	587,	727,	877,	1031,	1187,	1327,
43, 47,	181,	311,	443,	593,	733,	881,	1033,	1193,	1361,
53, 59,	191,	313,	449,	599,	739,	883,	1039,	1201,	1367,
61, 67,	193,	317,	457,	601,	743,	887,	1049,	1213,	1373,
71, 73,	197,	331,	461,	607,	751,	907,	1051,	1217,	1381,
79, 83,	199,	337,	463,	613,	757,	911,	1061,	1223,	1399,
89, 97,	211,	347,	467,	617,	761,	919,	1063,	1229,	1409,
101,	223,	349,	479,	619,	769,	929,	1069,	1231,	1423,
103,	227,	353,	487,	631,	773,	937,	1087,	1237,	1427,
107,	229,	359,	491,	641,	787,	941,	1091,	1249,	1429,
109,	233,	367,	499,	643,	797,	947,	1093,	1259,	1433,
113,	239,	373,	503,	647,	809,	953,	1097,	1277,	1439,
127,	241,	379,	509,	653,	811,	967,	1103,	1279,	1447,
131,	251,	383,	521,	659,	821,	971,	1109,	1283,	1451,
137,	257,	389,	523,	661,	823,	977,	1117,	1289,	1453,
139,	263,	397,	541,	673,	827,	983,	1123,	1291,	1459,
149,	269,	401,	547,	677,	829,	991,	1129,	1297,	1471

3.3 Exercises of Divisibility and Prime Numbers

Exercises

1. Prove that if x is even, then $x^2 + 2x + 4$ is divisible by 4.
2. Suppose $a \mid b$ and $a \mid c$. Prove the following:
   (a) $a \mid b + c$.
   (b) $a \mid b - c$.
   (c) $a \mid mb$ for all $m \in \mathbb{Z}$.
3. Prove that if $a \mid b$ and $b \mid a$, then $a = b$ or $a = -b$.
4. Show that $5 \mid 25, -19 \mid 38, -5 \nmid 27$ and $2 \mid 98$.
5. List all prime numbers less than 30 and briefly justify why each is prime.
6. Find the prime factorization of 84.