

(1)

WRITING MATHEMATICS

- * Write in _____
- * Use mathematical symbols where _____.
- Any new mathematical symbols or variables _____

Introduction

Let $\mathbb{Z}$ _____
 $\mathbb{Z} = \{ \quad \quad \quad \}$

Read pp. 1-2.

Chapter 1 Divisibility & Factorization1.1 Divisibility

Definition Let $a, b \in \mathbb{Z}$. We say a divides b (denoted by _____) if _____

Examples

(1) $6 \mid 30$ since _____

(2) $3 \nmid 7$ since _____

Here $a \nmid b$ means " _____ "

NOTE: (1) $a \mid b$ does not mean " _____ "

(2) If $a \in \mathbb{Z}$ then $a \mid 0$.

This is true since _____

(2)

(3) If $a \in \mathbb{Z}$ and $0 \mid a$ then _____

Proof Suppose _____ then _____

□

Proposition Let $a, b, c \in \mathbb{Z}$. If $a \mid b$ and $b \mid c$
then _____

Example: _____

Proof of Prop: Suppose $a, b, c \in \mathbb{Z}$, $a \mid b$ and $b \mid c$

Proposition Let $a, b, c, m, n \in \mathbb{Z}$. If $c \mid a$ and $c \mid b$
then _____

Proof:

(3)

The Greatest Integer Function

Let $x \in \mathbb{R}$. The greatest integer function of x denoted by $\lfloor x \rfloor$ is the greatest integer less than or equal to x .

Examples $\lfloor \frac{7}{3} \rfloor =$

$\lfloor -\frac{7}{3} \rfloor =$



Lemma Let $x \in \mathbb{R}$. Then

$$\lfloor x \rfloor \leq x < \lfloor x \rfloor + 1$$

Proof:

Theorem (Division Algorithm)

Let $a, b \in \mathbb{Z}$, $b > 0$. Then there exist integers q and r such that

$a = bq + r$ and $0 \leq r < b$.

Proof: Suppose $a, b \in \mathbb{Z}$, $b > 0$.

Let $q = \lfloor \frac{a}{b} \rfloor$, and $r = a - bq$.

(4)

To show uniqueness we suppose

Examples (1) $a = 13$, $b = 5$.

(2) $a = -13$, $b = 5$.

(5)

Ex 10(a) Let $n \in \mathbb{Z}$. Then $3 \mid (n^3 - n)$.

PROOF. Suppose $n \in \mathbb{Z}$. Then by the Division Algorithm
 $n =$

Definition Let $n \in \mathbb{Z}$. n is even if $\dots$
 n is odd if

NOTE: By the Division Alg.
 $n =$

Lemma Let $x \in \mathbb{R}$, $d \in \mathbb{Z}$ with $d \geq 1$. Then
 $(x^d - 1) =$

PROOF:

(6)

Corollary Let $a \in \mathbb{Z}$, $n = md$ where m, d
are positive integers. Then

PROOF.

Suggested HW Ex 1.1 (pp. 9-10).

1(a), (c), (d), 2, 3(a)(c), 5, 6, 7, 9,
10(a)(b)(c), 14(a)(b)(c).

(7)

Corollary Let $a, b \in \mathbb{Z}$ with $b > 0$.

By Division Algorithm, there are unique integers q, r :

$$a = bq + r, \text{ and } 0 \leq r < b.$$

$b \mid a$ if and only if $r = 0$.

1.2 Prime Numbers

Definition p is a prime (or a prime number) if $p > 1$, $p \in \mathbb{Z}$ and the only positive divisors of p are 1 and p . If $n > 1$, $n \in \mathbb{Z}$ and n is not prime, we say n is composite.

Example

The primes are 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, ...

The composites are 4, 6, 8, 9, 10, 12, 14, 15, 16, 18, 20, 21, 22, 24, 25, 26, 27, 28, 30, 32, 33, 34, 35, 36, 38, 39, 40, 42, 44, 45, 46, 48, 49, 50, 51, 52, 54, 55, 56, 57, 58, 60, 62, 63, 64, 65, 66, 68, 69, 70, 72, 74, 75, 76, 77, 78, 80, 81, 82, 84, 85, 86, 87, 88, 90, 91, 92, 93, 94, 95, 96, ...

Lemma If $a, b \in \mathbb{Z}$, $a \mid b$ and $b \neq 0$, then $|a| \leq |b|$.

PROOF Suppose $a, b \in \mathbb{Z}$, $a \mid b$ & $b \neq 0$.

(8)

The Well-Ordering Principle

Every -----
-----.

Lemma Every integer greater than 1 has
a -----.

PROOF: Assume by way of contradiction that there is
some integer $n > 1$ that has no prime divisor.

Theorem (Euclid)

There are ----- primes.

PROOF: Suppose by way of contradiction that

(9)

Proposition Let n be composite. Then
 n must have prime divisor $p \leq \sqrt{n}$.

PROOF: Let n be composite. Then $n > 1$ and
 $n = ab$

for

Example $n = 51$
 $\sqrt{51} \approx 7.14$.

(10)

The Sieve of Eratosthenes

As an example we find all primes ≤ 100 .

By Prop. any composite ≤ 100 must have a prime divisor $p \leq \sqrt{100} = 10$ i.e. $p =$ _____

& any $1 < n \leq 100$ is composite iff it is a _____

We _____ What _____ are the primes we seek.

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Eliminate

--- 4, 6, 8, ..., 98, 100

---, 9, 15, 21, 27, 33, 39, 45, 51, 57,

---,

(11)

Prop. For any positive integer n there are at least n consecutive

PROOF Suppose n is a positive integer.

Consider the following sequence of n consecutive integers:

$(n+1)! + 2, (n+1)! + 3, \dots, \dots$

The Twin Prime Conjecture

There are infinitely many primes p for which

Examples:

Prime Gap Theorem (Zhang, Maynard, POLYMATH 2014)

There are infinitely many primes p such that the gap to the next prime is $\leq$

(12)

x	pi(x)	x/log(x)	pi(x)*log(x)/x
[2,	1,	2.885390082,	.3465735903]
[3,	2,	2.730717679,	.7324081927]
[4,	2,	2.885390082,	.6931471805]
[5,	3,	3.106674674,	.9656627472]
[6,	3,	3.348663760,	.8958797345]
[7,	4,	3.597288397,	1.111948657]
[8,	4,	3.847186775,	1.039720771]
[9,	4,	4.096076521,	.9765442563]
[10,	4,	4.342944819,	.9210340372]
[100,	25,	21.71472410,	1.151292546]
[1000,	168,	144.7648273,	1.160502887]
[10000,	1229,	1085.736205,	1.131950832]
[100000,	9592,	8685.889642,	1.104319810]
[1000000,	78498,	72382.41364,	1.084489948]
[10000000,	664579,	620420.6885,	1.071174789]
[100000000,	5761455,	5428681.025,	1.061299232]
[1000000000,	50847534,	48254942.43,	1.053726964]
[10000000000,	455052511,	434294481.9,	1.047797128]

Definition Let $x > 0$, $x \in \mathbb{R}$.

$\pi(x)$ is — — — — —.

Example There — — — primes ≤ 10 namely — — — — —.

So $\pi(10) = \dots$

The Prime Number Theorem (Hadamard & de la Vallée Poussin, 1896)

Note This means when x is large, $\pi(x) \approx$

Goldbach's Conjecture (1742)Every even integer — — — — —
— — — — —
— — — — —Example

$$74 = _ + _.$$

PROPOSITION (#26, p.18).Let $p \in \mathbb{Z}$, $p > 1$.If $2^p - 1$ is prime then p is — — — — —.PROOF:

Pg

(14)

A Mersenne prime is a prime of the form _____.

Examples

$$2^2 - 1$$

$$2^3 - 1$$

$$2^5 - 1$$

$$2^7 - 1$$

$$2^{11} - 1$$

$$2^{13} - 1$$

Largest known Mersenne prime is

Conjecture There are _____.

Lemma If $n \geq 1$ is odd then

$$x^n + 1 = \text{_____}$$

PROOF (EX)

Proposition: Let $n \in \mathbb{Z}$, $n \geq 1$.

If $2^n + 1$ is prime then n is _____.

PROOF:

Definition A Fermat prime is

Example

$$F_0 =$$

$$F_1 =$$

$$F_2 =$$

$$F_3 =$$

$$F_4 =$$

$$F_5 =$$

Conjecture :

1.3 Greatest Common Divisor

Definition: Let $a, b \in \mathbb{Z}$, a, b not both zero.
The greatest common divisor of a, b denoted by $\text{gcd}(a, b)$ is the

If $\text{gcd}(a, b) = 1$ we say a, b are coprime.

Example

① Find $\text{gcd}(10, 6)$

The divisors of 10 are

... .. 6 are

The common divisors are

$$\text{gcd}(10, 6) = \text{Greatest Common Divisor} = 2$$

② $\text{gcd}(6, 55) =$

Proposition Let $a, b \in \mathbb{Z}$ (not both zero), & let $d = \text{gcd}(a, b)$. Then

$$\left(\frac{a}{d}, \frac{b}{d} \right) = 1.$$

Proof: Suppose $d = \text{gcd}(a, b)$ where $a, b \in \mathbb{Z}$ & a, b not both zero.

Example $(10, 6) = \dots$ and $(\dots) = (\dots) = 1$.

Proposition Let $a, b \in \mathbb{Z}$ (not both zero). Then

$$(a, b) = \dots \left\{ \dots : \dots \right\}.$$

Proof: Let $a, b \in \mathbb{Z}$ (not both zero).

Let

$$S = \left\{ \dots : \dots \right\}.$$

S is non-empty since ^{at least} one of $\dots \in S$.

By The Well-Ordering Property,

(18)

Ex 42(a) Let $a, b, c \in \mathbb{Z}$ with $(a, b) = (a, c) = 1$
Then $(a, bc) = 1$.

PROOF:

Ex 43(a) Let $(a, b) = 1$. If $a \mid c$ & $b \mid c$ then $ab \mid c$

PROOF.

(19)

Ex 44(a) If $(a, b) = 1$ & $a \mid bc$ then $a \mid c$.

Proof:

1.4 The Euclidean Algorithm

Lemma: Let $a, b \in \mathbb{Z}$, $a \geq b > 0$ with
 $a = bq + r$

we $q, r \in \mathbb{Z}$. Then $(a, b) = \underline{\hspace{2cm}}$.

PROOF: Suppose c is a common divisor of a, b .

Theorem (Euclidean Algorithm)

Let $a, b \in \mathbb{Z}$, $a \geq b > 0$. By the Division alg.

we exist $q_1, r_1 \in \mathbb{Z}$:

$$a =$$

If $r_1 > 0$, we then exist $q_2, r_2 \in \mathbb{Z}$:

$$b =$$

If $r_2 > 0$, we then exist $q_3, r_3 \in \mathbb{Z}$:

$$r_1 =$$

(21)

We continue this process until some $r_n = \underline{\hspace{2cm}}$

If $n > 1$ then $(a, b) = \underline{\hspace{2cm}}$

If $n = 1$ then $(a, b) = \underline{\hspace{2cm}}$

PROOF:

Example (#54ff) Use the Euclidean Alg. to find
(42722, 25174).

(22)

Example Express 82 as an integral linear combination of $a = 42722$ & $b = 25174$.

1.5 The Fundamental Theorem of Arithmetic

Lemma (Euclid)

Let $a, b, p \in \mathbb{Z}$ with p prime.

If $p \mid (ab)$ then _____

PROOF:

Corollary

Let $a_1, a_2, \dots, a_n, p \in \mathbb{Z}$ with p prime.

If $p \mid (a_1 a_2 \dots a_n)$ then $p \mid a_i$ for _____

PROOF: We proceed by induction on _____

(24).

Theorem (Fundamental Theorem of Arithmetic)

PROOF:

Example Find the prime factorization of 1692.

Theorem

Theorem Let $a = p_1^{a_1} p_2^{a_2} \dots p_n^{a_n}$
 $b = p_1^{b_1} p_2^{b_2} \dots p_n^{b_n}$

be prime factorizations of a & b where each $a_i, b_i \geq 0$.

Then $a \mid b$ if and only if _____.

PROOF:

(26)

Definition Let a, b be positive integers.

The least common multiple of a & b denoted by $\text{lcm}(a, b)$ is

Example Find $[8, 12]$.

Proposition

$$\text{Let } a = p_1^{e_1} p_2^{e_2} \cdots p_n^{e_n},$$

$$b = p_1^{f_1} p_2^{f_2} \cdots p_n^{f_n},$$

be prime factorizations where each p_i is a prime. Then

$$(a, b) =$$

$$[a, b] =$$

PROOF:

(28)

Example Let $a=90$, $b=924$. Find (a,b) & $[a,b]$

Dirichlet's Theorem

Let a, b be _____

Then the _____ progression:

a ,
contains

Examples ① $a=1, b=2$

② $a=3, b=4$.

Lemme Let a, b be integers of the form $4n+1$ (where $n \in \mathbb{Z}$). Then ab is

PROOF:

Theorem There are infinitely many primes of the form $4n+3$ where n is a nonnegative integer.

PROOF:

Lemma Let $x, y \in \mathbb{R}$. Then
 $\max\{x, y\} + \min\{x, y\} = \underline{\hspace{1cm}}.$

PROOF:

Theorem Let $a, b \in \mathbb{Z}$ with $b > 0$. Then
 $(a, b)[a, b] = \underline{\hspace{1cm}}.$

(31)