Elementary Numbah Theory

Doctorjay

May 2017

1 Axioms

Axiom 1. $1 \in \mathbb{N}$

Axiom 2. $\forall x \in \mathbb{N}$, $\exists x'$, called the **successor** of x

Axiom 3. 1 is not the successor of any natural number

Axiom 4. $x' = y' \Rightarrow x = y$

Axiom 5. : **Induction Axiom**
Let $S \subseteq \mathbb{N}$ such that

- (1) $1 \in S$
- (2) $x \in S \Rightarrow x' \in S$

Then $S = \mathbb{N}$

Axiom 6. : **Well-Ordering Axiom**
$\forall (S \subseteq \mathbb{N} \ \wedge \ S \neq \emptyset)$, S contains a least element.
That is, $\forall (b \in S)$, $(\exists a \in S) \ : a \leq b$

2 Postulates on $\mathbb{Z}$

Postulate 1. Reflexivity of Equality
$a \in \mathbb{Z} \Rightarrow a = a$

Postulate 2. Symmetry of Equality
$a, b \in \mathbb{Z} \wedge a = b \Rightarrow b = a$

Postulate 3. Transitivity of Equality
$a, b, c \in \mathbb{Z} \wedge a = b \wedge b = c \Rightarrow a = c$

Postulate 4. Transitivity of Inequality
$a, b, c \in \mathbb{Z} \wedge a < b \wedge b < c \Rightarrow a < c$

Postulate 5. Trichotomy
$a, b \in \mathbb{Z} \Rightarrow$ Exactly one of the following is true: (1) $a < b$, (2) $a = b$ or (3) $a > b$

Postulate 6. Binary operations

$\cdot$	Addition	Multiplication
Closure	$(a+b) \in \mathbb{Z}$	$(ab) \in \mathbb{Z}$
Equality	$a = b \Rightarrow a + c = b + c$	$a = b \Rightarrow a \cdot c = b \cdot c$
Associativity	$(a+b)+c = a+(b+c)$	$(ab)c = a(bc)$
Identity	$a + 0 = 0 + a = a$	$a \cdot 1 = 1 \cdot a = a$
Commutativity	$a + b = b + a$	$a \cdot b = b \cdot a$
Inverse	$a + (-a) = 0$	$\{1, -1\}$
Transitivity of Inequality	$a < b \Leftrightarrow a + c < b + c$	$a < b \Leftrightarrow a \cdot \lvert c\rvert < b \cdot \lvert c\rvert$
Distributivity	$a \cdot (b + c) = ab + ac$	

$\mathbb{Z}^+$ is an abelian group and an infinite cyclic group
$\mathbb{Z}^*$ is a commutative monoid

3 Divisibility

Definition 3.1. Let $a, b \in \mathbb{Z}$
$\exists(k \in \mathbb{Z}) : b = ak \Rightarrow a \mid b$
$:= a$ divides b
$:= a$ is a divisor of b

Properties.

Property 3.1. 0 is not a divisor of any integer except 0, since $\neg\exists k \neq 0 : \; 0 \cdot k \neq 0$

Property 3.2. $a \mid 0$ since $0 = 0 \cdot a$

Property 3.3. $1 \mid a$ since $a = 1 \cdot a$

Property 3.4. $a \mid a$ since $a = a \cdot 1$

Property 3.5. $a \mid b \wedge b \neq 0 \Rightarrow |a| \leq |b|$

Proof

1.	$b = ak$ for some $k \in \mathbb{Z}$	(Definition 3.1)
2.	$k \neq 0$ since $b \neq 0$	(Premise)
3.	$\lvert k\rvert \geq 1$	(2)
4.	$\lvert b\rvert = \lvert ak\rvert = \lvert a\rvert \cdot \lvert k\rvert \geq \lvert a\rvert \cdot 1$	(3, Trans. Ineq.) □

Property 3.6. Closure under multiplication
$d \mid a \Rightarrow d \mid ab$

Proof

1	$dk = a$	(Definition 3.1)
2	$dk \cdot b = a \cdot b$	(Trans. Mult.)
2	$d \cdot (kb) = a \cdot b$	(Assoc. Mult.)
4	$d \mid ab$	(Definition 3.1) □

Converse is not necessarily true.

Property 3.7. Transitivity
$a \mid b \wedge b \mid c \Rightarrow a \mid c$

Proof

1	$ak = b$ for some k	(Definition 3.1)
2	$b = ak \mid c$	(Premise)
3	$akk' = c$ for some k'	(Definition 3.1)
4	$a(kk') = c$	(Assoc. Mult.)
5	$a \mid c$	(Definition 3.1) □

Property 3.8. Equality
$a \mid b \Leftrightarrow a \cdot c \mid b \cdot c$

$a \mid b \Rightarrow ak = b \Rightarrow (ac)k = bc \Rightarrow ac \mid bc$
$ac \mid bc \Rightarrow ack = bc \Rightarrow ak = b \Rightarrow a \mid b$

Property 3.9. $a \mid b \wedge b \mid a \Rightarrow |a| = |b|$

Proof
$a \mid b$, so $ak = b$ for some $k \in \mathbb{Z}$
$b \mid a$, so $bk' = a$ for some $k' \in \mathbb{Z}$
$akk' = a \Leftrightarrow (k, -k) \in \{(1, -1), (-1, 1)\}$

4 Common Divisor

Definition 4.1. Let $d \mid a$ and $d \mid b,\ d \in \mathbb{Z}$
$:= d$ is a **common divisor** of a and b

Definition 4.2. A **linear combination** of $a,\ b \in \mathbb{Z}$ is any integer of the form $ra + sb,\ r, s \in \mathbb{Z}$

Theorem 4.1. *Linear Combination*
Let $(a, b, d, r, s) \in \mathbb{Z}$. *Then* $d \mid a \ \wedge\ d \mid b \Rightarrow d \mid (ra + sb)$

Proof

	$d \mid a$	Premise
	$d \mid b$	Premise
(1)	$\exists (e \in \mathbb{Z})\colon a = d \cdot e$	(Definition 3.1)
(2)	$\exists (f \in \mathbb{Z})\colon b = d \cdot f$	(Definition 3.1)
(3)	$ra + sb = rde + sdf = d(re + sf)$	(1, 2)
(4)	$d \mid (ra + sb)$	(3), Definition 3.1 □

Note that the converse is not necessarily true.

Corollary 4.1.1. $d \mid a \wedge d \mid b \Rightarrow d \mid (a + b)$
Set $r = 1, s = 1$

Corollary 4.1.2. $d \mid a \wedge d \mid b \Rightarrow d \mid (a - b)$
Set $r = 1, s = -1$

Corollary 4.1.3. $d \mid a \Rightarrow d \mid ra$
Set $r = 1, s = 0$. Also, see (3.6)

Lemma 4.2. For a, b not both 0, there is a least positive linear combination of a and b.

Proof. WLOG, assume $a \neq 0$. Let $S = \{x : x = (r_0 a + s_0 b)\ \forall (r_0, s_0 \in \mathbb{Z})\}$. Then $a \in S$ for $a > 0$, $r_0 = 1$ and $-a \in S$ for $a < 0$, $r_0 = 1$. Therefore, $S \neq \emptyset$. ■

Lemma 4.3. For a, b not both 0, the least positive linear combination of a and b is a common divisor of a and b.

Proof

(1)	Let d be the least positive linear combination of a and b	(Lemma 4.2)
(2)	Write $a = qd + r,\ 0 \leq r < d$	(Division Algorithm)
(3)	$r = a - qd = a - q(r_0 a + s_0 b) = (1 - qr_0)a + (-qs_0)b$	(2)
(4)	r is also a linear combination of a and b and $r \geq 0$	(2,3)
(5)	If $r > 0$ then (1) is contradicted. Therefore, $r = 0$	(1, 4)
(6)	$a = qd + 0$, Hence $a = qd$ and $d \mid a$	(2)
(7)	Repeat (2)-(6) with b to complete the proof	□

5 Greatest Common Divisor

Definition 5.1. For a, b not both 0, there is a **greatest common divisor** of a and b

Proof. WLOG, assume $a \neq 0$. Let $S = \{x : x \mid a \wedge x \mid b\}$. Then:

Existence	$1 \in S \Rightarrow S \neq \emptyset$	(Property 3.3)
Upper bound	$x \in S \Rightarrow x \mid a \Rightarrow x \leq \|a\|$	(Property 3.5)

■

Properties.

Property 5.1. For a, b not both 0, $gcd(a, b) \geq 1$ since $1 \in S$

Property 5.2. $gcd(a, 0) = a$ since $a \mid 0$ and $a \mid a$

Property 5.3. $c \mid a \wedge c \mid b \Rightarrow c \mid gcd(a, b)$.
This follows directly from Theorem 4.1.

Property 5.4. $gcd(ac, bc) = c \cdot gcd(a, b)$

Proof
Let $d = gcd(a, b)$
Let $d' = gcd(ac, bc)$
(1) Then $d \mid a \wedge d \mid b$ from Definition 4.1
(2) And $dc \mid ac \wedge dc \mid bc$ from Property 3.8
(3) So $dc \mid d'$ from Property 5.3
(4) $d = ra + sb$ for some r and s from (1)
(5) Then $dc = rac + sbc$ (Multiplicative Equality)

(6) $d' \mid ac \wedge d' \mid bc$ by Definition 5.1
(7) $d' \mid (rac + sbc) \Rightarrow d' \mid dc$ from Theorem 4.1, (5)
(8) From (3), $dc \leq d'$, and from (7), $d' \geq dc$
(9) Therefore $d' = dc$ □

Theorem 5.1. ***Bezout's Identity***
$gcd(a, b)$ is the least positive linear combination of a and b

Proof
Let d be the least positive linear combination of a and b.
Then $d \mid a$ and $d \mid b$ from Lemma 4.3
Let $c \mid a$ and $c \mid b$ for some $c \in \mathbb{Z}$
Since d is a linear combination of a and b, $c \mid d$
And $c \leq d$ from Property 3.5
All common divisors c, of $(a,\ b)$ are $\leq d \Rightarrow gcd(a,\ b) = d$ □

Corollary 5.1.1. $c \mid gcd(a, b) \Leftrightarrow c \mid a \wedge c \mid b$

Proof $\Leftarrow$ is restatement of Property 5.3

Proof $\Rightarrow$
$c \mid gcd(a, b)$ by Premise
$gcd(a, b) \mid a$ by Definition 5.1
$c \mid a$ by Property 3.7
$c \mid b$ can be shown by analogous derivation. □

Corollary 5.1.2. $\forall k \in \mathbb{Z},\ \exists\, (r, s) \in \mathbb{Z} : k \cdot gcd(a, b) = ra + sb$
All multiples of $gcd(a, b)$ are a linear combination of a and b

Proof

$gcd(a, b) = r_0 a + s_0 b$	Theorem 5.1
$k \cdot gcd(a, b) = (r_0 k)a + (s_0 k)b$	□

Corollary 5.1.3. $\forall (a, b, r, s \in \mathbb{Z}) : gcd(a, b) \mid (ra + sb)$
All linear combinations of a and b are a multiple of $gcd(a, b)$

Proof
Let $g = gcd(a, b)$
Let $(r,\ s) \in \mathbb{Z}$ be arbitrary integers

$k \cdot g = a$	Definition 5.1
$k' \cdot g = b$	Definition 5.1
$ra + sb = rkg + sk'g = (rk + sk')g$	Substituting
$g \mid (ra + sb)$	□

Corollary 5.1.4. $gcd(ac, bc) = c \cdot gcd(a, b)$

Proof

	Let $d = gcd(a, b)$	
1	$d \mid a \wedge d \mid b$	Definition 4.1
2	$dc \mid ac \wedge dc \mid bc$	Property 3.8
	Let $d' = gcd(ac, bc)$	
3	Then $dc \mid d'$	(2), Property 5.3
4	$d = r_0a + s_0b$	Theorem 5.1
5	$dc = r_0ac + s_0bc$, which is a linear combination of ac, bc	
6	$d' \mid dc$	(5), Corollary 5.1.3
7	$d' = dc$	(3), (6) □

Corollary 5.1.5. $gcd(a, bc) \mid \big(gcd(a, b) \cdot gcd(a, c)\big)$

Proof

Let $gcd(a, b) = r_0a + s_0b$	Theorem 5.1
Let $gcd(a, c) = r_1a + s_1c$	Theorem 5.1
Then $(gcd(a, b) \cdot gcd(a, c) = r_0ar_1a + r_0as_1c + s_0br_1a + s_0bs_1c$	
$= (r_0r_1a + r_0s_1c + s_0s_1b)a + (s_0s_1)bc$	
which is a linear combination of a, bc	
And which $gcd(a, bc)$ is thus a divisor of by Corollary 5.1.3	□

Corollary 5.1.6. $gcd(a + bc) = gcd(a, b)$ for any $c \in \mathbb{Z}$

Proof

	Let $d = gcd(a, b)$ and $d' = gcd(a + bc, b)$	
1	$d' = r(a + bc) + sb = ra + (rc + s)b$	Definition 4.1
2	$d \mid a \wedge d \mid b$	Definition 4.1
3	$d \mid d'$	(2), Theorem 4.1
4	$d' \mid b \Rightarrow d' \mid bc$	Property 3.6
5	$d' \mid (a + bc) \wedge d' \mid bc \Rightarrow d' \mid (a + bc - bc) \Rightarrow d' \mid a$	Corollary 4.1.2
6	$d' \mid a \wedge d' \mid b \Rightarrow d' \mid d$	Property 5.3
7	$d \mid d' \wedge d' \mid d \Rightarrow d = d'$	(3), (6) □

Lemma 5.2.

For a, b not both 0, write $a = bq + r$. Then $gcd(a, b) = gcd(b, r)$

Proof

	Let $d = gcd(a, b)$	
	Let $d' = gcd(b, r)$	
1	$d = sa + tb = s(bq + r) + tb = (sq + t)b + sr$ for some $s, t \in \mathbb{Z}$	
2	Then $d' \mid d$	
3	$d' = s'b + t'r = s'b + t'(a - bq) = t'a + (s - qt')b$ for some $s', t' \in \mathbb{Z}$	
4	Then $d \mid d'$	
	From (2) and (4), $d = d'$	□

6 Euclidean GCD Algorithm

Consider the following sequence of divisions:

$a = bq_0 + r_0$	$0 \leq r_0 < b$	$gcd(a, b) = gcd(b, r_0)$
$b = q_1 r_0 + r_1$	$0 \leq r_1 < r_0$	$gcd(b.r_0) = gcd(r_0, r_1)$
$r_0 = q_2 r_1 + r_2$	$0 \leq r_2 < r_1$	$gcd(r_0, r_1) = gcd(r_1, r_2)$
$r_1 = q_3 r_2 + r_3$	$0 \leq r_3 < r_2$	$gcd(r_1, r_2) = gcd(r_2, r_3)$
...	...	...
...	...	...
$r_{n-2} = q_n r_{n-1} + r_n$	$0 \leq r_n \leq r_{n-1}$	$gcd(r_{n-2}, r_{n-1}) = gcd(r_{n-1}, r_n)$
$r_{n-1} = q_{n+1} r_n + 0$		$gcd(r_{n-1}, r_n) = gcd(r_n, 0) = r_n$

Note that the sequence $r_0, r_1, r_2 ... r_n$ is strictly decreasing.
Therefore, it will eventually yield 0.
Let r_n be the last non-zero remainder. Now:
$r_n \mid r_{n-1}$ from the last term
So $r_n \mid r_{n-2}$ from the term above
Proceeding similarly, $r_n \mid b$ and $r_n \mid a$, so r_n is a common divisor of a and b
Let d be an arbitrary common divisor of a, b. Then:
$d \mid (a - bq_0) \Rightarrow d \mid r_0$
$d \mid (b - q_1 r_0) \Rightarrow d \mid r_1$
$d \mid (r_0 - q_2 r_1) \Rightarrow d \mid r_2$
...
$d \mid (r_{n-2} - q_n r_{n-1}) \Rightarrow d \mid r_n$
Since an arbitrary common divisor of (a, b) divides r_n, $r_n = gcd(a, b)$ (Property 5.3)
$r_n = gcd(a, b)$ can also be observed by noting the sequence in the right hand column, which follows from Lemma 5.2.

7 Coprimality

Definition 7.1. Let $gcd(a, b) = 1$
:= a and b are **coprime**
:= a and b are **relatively prime**
:= 1 is the only common divisor of a and b

Property 7.1. $gcd(a, b) = 1 \Leftrightarrow ra + sb = 1$ for some $r, s \in \mathbb{Z}$
This follows directly from Theorem 5.1

Proposition 7.1. $\frac{a}{gcd(a,b)}$ and $\frac{b}{gcd(a,b)}$ are coprime

Proof

Let $d = gcd(a, b)$

	Let $d = gcd(a,b)$	
1	$d \mid a \Rightarrow dk = a$ for some $k \in \mathbb{Z}$	
2	$d \mid b \Rightarrow dk' = b$ for some $k' \in \mathbb{Z}$	
3	$\frac{a}{d} = k,\ \frac{b}{d} = k'$	(1), (2)
4	Suppose k and k' have a common divisor, d'	
5	Then $k = d'm,\ k' = d'm'$ for some $m, m' \in \mathbb{Z}$	
6	So $a = dd'm$ and $b = dd'm'$, which means dd' is a common divisor of $a,\ b$	
7	But d is the greatest common divisor of a, b, so $d' = 1$	
8	$d' = 1, \Rightarrow k,\ k'$ are relatively prime	(4) □

Theorem 7.1. *Generalized Euclid's Lemma*
$a \mid bc \wedge gcd(a,b) = 1 \Rightarrow a \mid c$

Proof

1	$ak = bc$ for some $k \in \mathbb{Z}$	Definition 3.1
2	$1 = ra + sb$ for some $r, s \in \mathbb{Z}$	Property 7.1
3	$c = rac + sbc = rac + sak = a(rc + sk)$	(1), (2)
4	$a \mid c$	(3) □

Corollary 7.1.1. Euclid's Lemma
For any prime, $p, p \mid bc \Rightarrow p \mid b \vee p \mid c$

Proof
WLOG, assume $p \nmid b$
Then $gcd(p, b) = 1 = rp + sb$ for some $r, s \in \mathbb{Z}$
Multiplying by $c,\ c = (rc)p + (s)bc$
Since $p \mid (rc)p \wedge p \mid (s)bc,\ p \mid c$
The derivation for $p \mid b$ is analogous □

8 Linear Diophantine Equation

Definition 8.1.

A **Linear Diophantine Equation** in 2 variables is an equation of the form $ax + by = c$

Property 8.1. $ax + by = c$ is solvable $\Leftrightarrow gcd(a, b) \mid c$

Proof

Let $ax + by = c$ have a solution	Premise
Then $gcd(a, b) \mid c$	Corollary 5.1.3

Theorem 8.1. *If (x_0, y_0) is a solution of $ax + by = c$, then all solutions are given by* $\left(x_0 + \frac{b}{gcd(a,b)}k,\ y_0 - \frac{a}{gcd(a,b)}k\right)$

Proof $\Rightarrow$

Let $d = gcd(a, b)$
$c = dk$ Property 8.1
$d = ra + sb$ for some $r, s \in \mathbb{Z}$ Theorem 5.1
$c = a(rk) + b(sk)$
So this equation has the solution $(x_0 = rk,\ y_0 = sk)$
Substituting for arbitrary x, y:
$ax + by = a\big(x_0 + \frac{b}{d}k\big) + b\big(y_0 - \frac{a}{d}k\big)$
$= (ax_0 + by_0) + \frac{abk}{d} - \frac{abk}{d} = (ax_0 + by_0)$ □

Proof $\Leftarrow$
Let $x_0, y_0)$ and (x_1, y_1) be solutions of $ax + by = c$
Then $c = ax_0 + by_0 = ax_1 + by_1$
$a(x_1 - x_0) = b(y_0 - y_1)$
$\frac{a}{d}(x_1 - x_0) = \frac{b}{d}(y_0 - y_1)$
$gcd(\frac{a}{d}, \frac{b}{d}) = 1$ Proposition 7.1
Since $\frac{b}{d} \nmid \frac{a}{d},\ \frac{b}{d} \mid (x_1 - x_0)$
Hence, $x_1 - x_0 = \frac{b}{d}k$ for some $k \in \mathbb{Z}$
And $x_1 = x_0 + \frac{b}{d}k$
$a\frac{b}{d}k = b(y_0 - y_1)$
$\frac{a}{d}k = (y_0 - y_1)$
$y_1 = y_0 - \frac{a}{d}k$ □

Corollary 8.1.1. For $gcd(a, b) = 1$, all solutions of $ax + by = 1$ are given by $(x_0 + bk, y_0 - ak)\ \ \forall k \in \mathbb{Z}$, where (x_0, y_0) is one solution.

Substitute 1 for d in Proof above.

9 Congruence

Definition 9.1. If $m \mid (a - b)$:
$:= a \equiv b \mod m$
$:= a$ is **congruent to** $b \mod m$
$:= a$ and b are in the same **congruence class**