4. Number Theory (Part 2)

Terence Sim

Mathematics is the queen of the sciences and number theory is the queen of mathematics.

Carl Friedrich Gauss,
1777— 1855

Reading

Sections 4.8, 5.2 — 5.4 of Epp.

4.3. Well Ordering Principle

Definition 4.3.1 (Lower Bound)

An integer b is said to be a lower bound for a set $X \subseteq \mathbb{Z}$ if $b \leq x$ for all $x \in X$.

Note that this definition does not require b to be in X.

Moreover, there may be more than one lower bound (ie. the lower bound is not unique).

Examples: Does each of the following sets have a lower bound?

- $A = \{x \in \mathbb{Z} \mid x^2 \leq 38\}$.
- $B = \{x \in \mathbb{Z} \mid x \text{ is a multiple of } 3\}$.
- $C = \{x \in \mathbb{Z} \mid x^2 \leq 100x\}$.

Answer:

- We may list all the elements of the set. $A = \{-6, -5, \ldots, 5, 6\}$. Thus, any integer less than or equal to -6 is a lower bound.
- There is no lower bound. To see this, suppose not; suppose the lower bound is some integer c. Then one of $c-1, c-2, c-3$ must be divisible by 3. But all of them are less than c, contradicting the fact that c is a lower bound.
- If $x^2 \leq 100x$ then $x(x-100) \leq 0$, by basic algebra. Thus C is the set of integers x such that $0 \leq x \leq 100$. Thus any integer $m \leq 0$ is a lower bound.

Theorem 4.3.2 (Well Ordering Principle)

If a non-empty set $S \subseteq \mathbb{Z}$ has a lower bound, then S has a least element.

Proof Sketch

1. Suppose S is a non-empty subset of $\mathbb{Z}$, S has a lower bound, but no least element.
2. Define T to be $\mathbb{Z} - S$, ie. it contains integers not in S.
3. Let b be the lower bound of S. Then $b \notin S$, because otherwise b would be the least element. So $b \in T$.
4. All integers $a < b$ are also lower bounds, so $a \in T$.
5. Suppose $b, b+1, b+2, \ldots k \in T$, then $k+1 \notin S$, because if so, $k+1$ would be the least element in S.
6. Thus $k+1 \in T$, and by Induction, $T = Z$.
7. This means S is empty. Contradiction. ■

Examples: Does each set below have a least element? If so, what is it? If not, explain why there is no violation of the Well Ordering Principle.

- The set of all positive real numbers.
- The set of all non-negative integers n such that $n^2 < n$.
- The set of all non-negative integers of the form $46 - 7k$, where k is any integer.

Answer:

- There is no least (smallest) positive real number. To see this, suppose $x \in \mathbb{R}^+$, then $x/2 \in \mathbb{R}^+$ and $x/2 < x$. There is no violation of the Well Ordering Principle because the principle concerns only sets of integers, not real numbers.
- This set is empty! Thus there is no least element, and no violation of the Well Ordering Principle.
- Now, $46 - 7k \geq 0$ implies $7k \leq 46$, which means $k \leq 6.57$. When $k = 6$, $46 - 7(6) = 4$, which is therefore the least element.

Proposition 4.3.3 (Uniqueness of least element)

If a set S of integers has a least element, then the least element is unique.

The usual way to prove the uniqueness of a solution is to say that if A and B are both solutions, then $A = B$.

First let's define what it means to be a least element:

The least element x of a set S is one that satisfies:

(i) $x \in S$.

(ii) $\forall y \in S,\ x \leq y$.

Proof:

1. Suppose x and z are two least elements in S:
2. Then $\forall y \in S$, $x \leq y$, by definition of least element.
3. Since $z \in S$, this means $x \leq z$ [Universal instantiation].
4. Also, since z is a least element, then $\forall w \in S$, $z \leq w$, by definition of least element.
5. And since $x \in S$, this means $z \leq x$ [Universal instantiation].
6. Now, $(x \leq z) \wedge (z \leq x)$ simplifies to $x = z$, by the distributive and identity laws of logical equivalences.
7. Thus the least element is unique. ■

Well Ordering also states the existence of the greatest (maximum) element too:

Theorem 4.3.2 Well Ordering 2

If a non-empty set $S \subseteq \mathbb{Z}$ has an upper bound, then S has a greatest element.

The definition for upper bound is analogous to that for lower bound, ie. it is an integer that is more than or equal to all elements in the set. The upper bound need not be in the set, and is not unique.

Proposition 4.3.4 (Uniqueness of greatest element)

If a set S of integers has a greatest element, then the greatest element is unique.

The proof is similar to that for Proposition 4.3.3.

4.4. Quotient-Remainder Theorem

Theorem 4.4.1 (Quotient-Remainder Theorem)

Given any integer a and any positive integer b, there exist unique integers q and r such that:

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

The integer q is called the quotient, while r is called the remainder.

Note the limits on r: r lies in the range $0, 1, 2, \ldots, b - 1$.

Proof:

1. Let R be the set of "remainders":
   $R = \{x \in \mathbb{N} \mid a = by + x \text{ for some } y \in \mathbb{Z}\}$.
2. (Claim: R is not empty.)
3. If $a \geq 0$:
4. Then $a = b \cdot 0 + a \geq 0$, and thus $a \in R$.
5. Else $a < 0$:
6. Then $a - ab = a(1 - b) \geq 0$ [because $a < 0$ and $(1 - b) \leq 0$, so their product ≥ 0.]
7. Write $a = ba + a - ab$. Thus $(a - ab) \in R$ by definition of R.
8. In either case, R has at least one element.
9. So R is a non-empty subset of integers.
10. Also, -1 is a lower bound of R.
11. Hence there exists a least element $r \in R$, by the Well Ordering Principle.

...

proof cont'd

12. Then there exists $q \in \mathbb{Z}$ such that $a = bq + r$, since $r \in R$.
13. (We'll prove $0 \leq r < b$ by contradiction.)
14. Suppose $r \geq b$:
15. Re-write: $a = b(q + 1) + (r - b)$ by basic algebra.
16. Thus $(r - b) \in R$, by definition of R.
17. But $r - b < r$, contradicting the fact the r is the least element.
18. Thus, by the Contradiction Rule, $0 \leq r < b$. ■

Note that neither the theorem nor the proof says how to calculate q and r from a, b. They merely say q, r exist.

The above only proved the existence, and not uniqueness, of q, r. Try to prove uniqueness yourself.

Examples: Find the quotient and remainder for each of the following.

- $a = 54, b = 4$
- $a = -54, b = 4$
- $a = 54, b = 70$

- $54 = 4 \times 13 + 2$, so $q = 13, r = 2$.
- $-54 = 4 \times (-14) + 2$, so $q = -14, r = 2$.
- $54 = 70 \times 0 + 54$, so $q = 0, r = 54$.

Most programming languages have built-in operators to compute the quotient and remainder for integers a, b. Example: in C/C++ and Java, the integer division "/" computes the quotient, while "%" computes the remainder.
However, these do not give the correct answer if a is negative, e.g. C gives $q = -13, r = -2$ when $a = -54, b = 4$. Thus some caution is advised.

4.4.1. Representation of Integers

The Quotient-Remainder Theorem provides the basis for writing an integer n as a sequence of digits in a base b.

For example, our usual way of writing the number $n = 3 \cdot 10^2 + 3 \cdot 10^1 + 4 \cdot 10^0$ is: 334. This is in decimal (base 10) because it uses powers of 10. The same number n could be represented using a different base. More generally, given any positive integer n and base b, we may repeatedly apply the Quotient-Remainder Theorem to get:

$$\begin{aligned} n &= bq_0 + r_0 \\ q_0 &= bq_1 + r_1 \\ q_1 &= bq_2 + r_2 \\ &\vdots \\ q_{m-1} &= bq_m + r_m \end{aligned}$$

- Each remainder r_i is one of the integers $0, 1, \ldots, b-1$, and the process stops when $q_m = 0$.
- By eliminating the quotients q_i, we get:

$$n = r_m b^m + r_{m-1} b^{m-1} + \ldots + r_1 b + r_0$$

which may be written more compactly as:

$$n = \sum_{i=0}^{m} r_i b^i$$

- In turn, we may write n more compactly in base b as a sequence of the digits r_i. That is:

$$n = (r_m r_{m-1} \ldots r_1 r_0)_b$$

This positional notation is convenient. When $b = 10$ we usually omit it, which gives us our usual decimal representation for integers.

Note that the summation notation $\sum_{i=a}^{b} f(i)$ is shorthand for:

$$f(a) + f(a+1) + f(a+2) + \ldots + f(b-1) + f(b)$$

The index i increments by 1 starting from the lower limit a and ending at the upper limit b. It is assumed $b \geq a$. If $b < a$, then the sum is empty, which by default equals 0.

Likewise, a product of terms $f(a) \times f(a+1) \times \ldots \times f(b-1) \times f(b)$ is more compactly written as:

$$\prod_{i=a}^{b} f(i)$$

Again, it is assumed $b \geq a$. And if $b < a$ then the product is empty, which by default equals 1.

Example: Express $(109)_{10}$ in base 2.

Answer: Dividing repeatedly by 2 we obtain:

$$\begin{aligned} 109 &= 2 \times 54 + 1 \\ 54 &= 2 \times 27 + 0 \\ 27 &= 2 \times 13 + 1 \\ 13 &= 2 \times 6 + 1 \\ 6 &= 2 \times 3 + 0 \\ 3 &= 2 \times 1 + 1 \\ 1 &= 2 \times 0 + 1 \end{aligned}$$

Hence, by reading the remainders from bottom up, $(109)_{10} = (1101101)_2$. Base 2 (or binary) representation is especially useful for computers to manipulate.

Another useful base for computer manipulation is 16, called hexadecimal.

Here, we need new symbols to represent the decimal digits $10, 11, \ldots, 15$ in base 16. The usual convention is:

$$\text{A=10, B=11, C=12, D=13, E=14, F=15}$$

For the previous example of $(109)_{10}$, we may repeatedly divide by 16 to get: $(109)_{10} = (6D)_{16}$.

But a quicker way is to use the binary notation: starting from the right, take the bits (*b*inary dig*its*) in groups of 4, and convert each group to base 16 using this table:

$0000 = 0$	$0001 = 1$	$0010 = 2$	$0011 = 3$
$0100 = 4$	$0101 = 5$	$0110 = 6$	$0111 = 7$
$1000 = 8$	$1001 = 9$	$1010 = \text{A}$	$1011 = \text{B}$
$1100 = \text{C}$	$1101 = \text{D}$	$1110 = \text{E}$	$1111 = \text{F}$

Thus $(109)_{10} = (0110\ 1101)_2 = (6D)_{16}$.

Now you try:

Convert $(10110101)_2$ to:
(a) decimal (base 10)
(b) octal (base 8)

4.5. Greatest Common Divisor

Definition 4.5.1 (Greatest Common Divisor)

Let a and b be integers, not both zero. The greatest common divisor of a and b, denoted $\gcd(a, b)$, is the integer d satisfying:

(i) $d \mid a$ and $d \mid b$.

(ii) $\forall c \in \mathbb{Z}$, if $c \mid a$ and $c \mid b$ then $c \leq d$.

The greatest common divisor is also called the highest common factor.

Examples: Find $\gcd(72, 63)$ and $\gcd(10^{20}, 6^{30})$.

- Using prime factorization: $72 = 2^3 \cdot 3^2$, and $63 = 3^2 \cdot 7$. The gcd is therefore $3^2 = 9$.
- Using prime factorization: $10^{20} = 2^{20} \cdot 5^{20}$, and $6^{30} = 2^{20} \cdot 2^{10} \cdot 3^{30}$. Thus, gcd is 2^{20}.

More examples:

For any $a \neq 0$, what is $\gcd(a, 0)$?

What is $\gcd(0, 0)$?

The definition of gcd does not guarantee its existence. Hence,

Proposition 4.5.2 (Existence of gcd)

For any integers a, b, not both zero, their gcd exists and is unique.

Proof:

1. Let $D = \{$ all common divisors of a, b $\}$.
2. Clearly, $1 \in D$, and $D \subseteq \mathbb{Z}$.
3. By assumption, one of a, b is non-zero. Let it be a, since $\gcd(a, b) = \gcd(b, a)$ by its definition, so we can swap the numbers to make a the non-zero number.
4. Also, $|a|$ is an upper bound for D, since no common divisor of a, b can be larger than this.
5. Thus by Well Ordering 2, there exists a greatest element d in D.
6. By Proposition 4.3.4, d is unique. ■

4.5.1. Euclid's algorithm

In practice, computing the gcd by prime factorization is too slow, especially when the numbers are large. Luckily, an efficient algorithm was given by Euclid way back in the year 300BC.

The key idea to find $\gcd(a, b)$ is based on two facts:

(i) $\gcd(a, 0) = a$.

(ii) $\gcd(a, b) = \gcd(b, r)$, where r is the remainder of a/b.

Line (i) was explained in the previous slide.

For Line (ii), note that since $a = bq + r$, then any common divisor c of a, b must divide r by Theorem 4.1.1 (r is a linear combination of a, b.) Also, any common divisor of b, r must divide a for the same reason.

So a, b and b, r have the same set of common divisors, and thus their gcd's must be equal.

Euclid's Algorithm for gcd

```
def gcd(I, CAN):
    # assumes I>0, CAN>=0
    # computes gcd using Euclid's algorithmm

    while CAN > 0:
        DOIT = I % CAN
        (I, CAN) = (CAN, DOIT)

    return I
```

Let's trace Euclid's algorithm to calculate $\gcd(330, 156)$.

$$
\begin{array}{lrcll}
 & & & & \gcd(330, 156) \\
\text{(i)} & 330 & = 156 \times 2 + 18 & \leftarrow & \gcd(156, 18) \\
\text{(ii)} & 156 & = 18 \times 8 + 12 & \leftarrow & \gcd(18, 12) \\
\text{(iii)} & 18 & = 12 \times 1 + 6 & \leftarrow & \gcd(12, 6) \\
\text{(iv)} & 12 & = 6 \times 2 + 0 & \leftarrow & \gcd(6, 0)
\end{array}
$$

Thus $\gcd(330, 156) = 6$.

Theorem 4.5.3 (Bézout's Identity)

Let a, b be integers, not both zero, and let $d = gcd(a, b)$. Then there exist integers x, y such that:

$$ax + by = d.$$

In other words, the gcd of two integers is some linear combination of the said numbers.

The proof is cumbersome to write, so we give a sketch instead.

Proof sketch:

Trace the execution of Euclid's algorithm on a, b.
The last line gives the gcd d.
Now work backwards to express d in terms of linear combinations of the quotients and remainders of the previous lines, until you reach the top.

Using the example of $\gcd(330, 156)$, we work as follows:

$$\begin{aligned}
6 &= 18 - 12 \times 1 &&= 18 + 12 \times (-1) && \text{Using (iii)} \\
&= 18 + (156 - 18 \times 8) \times (-1) &&= 156 \times (-1) + 18 \times 9 && \text{Using (ii)} \\
&= 156 \times (-1) + (330 - 156 \times 2) \times 9 &&= 330 \times 9 + 156 \times (-19) && \text{Using (i)}
\end{aligned}$$

Thus $6 = 330 \cdot 9 + 156 \cdot (-19)$.

The above procedure is called the Extended Euclidean Algorithm, for obvious reasons.

Non-uniqueness of Bézout's Identity

There are multiple solutions x, y to the equation $ax + by = d$.

Once a solution pair (x, y) is found, additional pairs may be generated by $(x + \frac{kb}{d}, y - \frac{ka}{d})$, where k is any integer.

Proof sketch: $a(x + \frac{kb}{d}) + b(y - \frac{ka}{d}) = ax + \frac{kab}{d} + by - \frac{kab}{d} = d$.

Aiken & Dueet: A Love Story

Dueet is in trouble. He has been secretly courting Aiken, a pretty farm girl, for the past six months, sneaking into the girl's farm house when her parents were out.

Unfortunately, today he got caught by the girl's no-nonsense father. Father gives Dueet a test: if he passes, he gets to marry the girl; otherwise, never ever step foot on the farm again.

The test is this: fill a large trough in the field with exactly 1 litre of river water. Only two cans are available to scoop water from the river: one is exactly 9 litres when full, the other, 7.

Help Dueet pass the test to win Aiken.


9 litres


7 litres

Since the cans must be completely full or empty when transferring water, Dueet is dealing with multiples of 7 and 9 litres. In other words, Dueet needs to solve the equation:

$$9x + 7y = 1.$$

Note that $\gcd(9, 7) = 1$. Using Bézout's Identity, it is straightforward to get: $9(4) + 7(-5) = 1$.

Thus, Dueet needs to pour in four cans of water into the trough using the 9-litre can, and then scoop out five cans using the 7-litre can.

Definition 4.5.4 (Relatively Prime)

Integers a and b are relatively prime (or coprime) iff $\gcd(a, b) = 1$.

Examples:

- 9 and 7 are coprime (from Aiken & Dueet's puzzle).
- 10 and 100 are not coprime, since $\gcd(10, 100) = 10$.
- In fact, for any integer $a > 1$, a and ka are not coprime for any integer k (because their gcd is a).
- Obviously, any two distinct primes p, q are coprime.

We can now prove this theorem:

Theorem 4.2.3

If p is a prime and $x_1, x_2, \ldots, x_n$ are any integers such that: $p \mid x_1 x_2 \ldots x_n$, then $p \mid x_i$, for some i $(1 \leq i \leq n)$.

Proof: by Induction

1. Let $P(n) = (\ (p \mid x_1 x_2 \ldots x_n) \longrightarrow (p \mid x_i \text{ for some } i \in [1, n])\ )$
2. Base case: $n = 1$
3. Clearly, $P(1)$ is true.

...

proof cont'd

4. Inductive step: For any $k \in \mathbb{Z}^+$:
5. If $P(k)$ ie. $(p \mid x_1 x_2 \dots x_k) \longrightarrow (p \mid x_i \text{ for some } i \in [1, k])$.
6. Consider the case $k + 1$:
7. Suppose $p \mid x_1 x_2 \dots x_{k+1}$:
8. Let $A = x_1 x_2 \dots x_k$, so that $p \mid A x_{k+1}$.
9. If $p \mid A$:
10. Then $p \mid x_i$ for some $i \in [1, k]$ by the Inductive hypothesis. So $P(k + 1)$ is true.

...

proof cont'd

11. Else $p \nmid A$:
12. Then $\gcd(p, A) = 1$, because p is prime and $p \nmid A$.
13. Then there exist integers r, s such that $pr + As = 1$ by Bézout's Identity.
14. Now, $x_{k+1} = 1 \cdot x_{k+1} = (pr + As)x_{k+1}$
$= p(rx_{k+1}) + (Ax_{k+1})s$ by basic algebra.
15. Since p divides both terms, it divides their linear combination by Theorem 4.1.1.
16. Thus, $p \mid x_{k+1}$ and $P(k + 1)$ is true.
17. Hence, by Mathematical Induction, the theorem is true. ■

Proposition 4.5.5

For any integers a, b, not both zero, if c is a common divisor of a and b, then $c \mid gcd(a, b)$.

Proof:

1. Take any two integers a, b, not both zero.
2. Let $d = \gcd(a, b)$.
3. By Bézout's Identity, $d = ax + by$, for some integers x, y.
4. Suppose c is a common divisor of a, b:
5. Then $c \mid a$ and $c \mid b$, by definition of divisibility.
6. Thus $c \mid (ax + by)$ by Theorem 4.1.1
7. Thus $c \mid d$. ■

Example:
$\gcd(30, 45) = 15$.

$30 = 2 \cdot 3 \cdot 5$
$45 = 3^2 \cdot 5$.
Thus the common divisors are $1, 3, 5, 15$.

All these common divisors divide 15.

Optional

Prove that for all positive integers a, b, $a \mid b$ if, and only if, $\gcd(a, b) = a$.

To prove "P iff Q", we need to prove "if P then Q" and "if Q then P".

Proof:

1. (Forward direction: "if P then Q")
2. For any positive integers a, b:
3. Suppose $a \mid b$:
4. Then $b = ak$ for some integer k, by definition of divisibility.
5. Then $\gcd(a, b) = \gcd(a, ak) = a$ because a is the largest common divisor.
6. (Backward direction: "if Q then P")
7. For any positive integers a, b:
8. Suppose $\gcd(a, b) = a$:
9. Then a is a common divisor of a, b, by definition of gcd.
10. Thus, $a \mid b$. ■

Now you try

Prove that if a, b are integers, not both zero, and $d = \gcd(a, b)$, then a/d and b/d are integers with no common divisor that is greater than 1.

4.6. Least Common Multiple

Definition 4.6.1 (Least Common Multiple)

For any non-zero integers a, b, their least common multiple, denoted $\text{lcm}(a, b)$, is the positive integer m such that:

(i) $a \mid m$ and $b \mid m$,

(ii) for all positive integers c, if $a \mid c$ and $b \mid c$, then $m \leq c$.

The lcm of a, b exists because the Well Ordering Principle guarantees the existence of the least element on the set of common multiples of a, b.

Examples: Find

- $\text{lcm}(12, 18)$
- $\text{lcm}(2^2 \cdot 3 \cdot 5,\ 2^3 \cdot 3^2)$
- $\text{lcm}(2800, 6125)$

- $12 = 2 \cdot 2 \cdot 3$, and $18 = 2 \cdot 3 \cdot 3$. The gcd is thus $2 \cdot 3 = 6$. The lcm is made up of the "factors other than the gcd", ie. lcm $= 2 \cdot 2 \cdot 3 \cdot 3 = 36$.
- The two numbers are: $2 \cdot 2 \cdot 3 \cdot 5$, and $2 \cdot 2 \cdot 2 \cdot 3 \cdot 3$. So the gcd $= 2 \cdot 2 \cdot 3 = 12$. And the lcm $= 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 \cdot 5 = 360$.
- $2800 = 2^4 \cdot 5^2 \cdot 7$, and $6125 = 5^3 \cdot 7^2$. Thus gcd $= 5^2 \cdot 7$, and lcm $= 2^4 \cdot 5^3 \cdot 7^2$.

From the above examples, it should be clear that

$$\gcd(a, b) \cdot \operatorname{lcm}(a, b) = ab.$$

Prove this as an exercise. Note that this provides an algorithm to compute the lcm. Write code to do this.

Now you try:

Prove that for all positive integers a and b, $\gcd(a, b) | \operatorname{lcm}(a, b)$.