Math 103A Lecture Notes

1.1 Lecture 1 (1/5/2009)

Notation 1.1 *Introduce* $\mathbb{N} := \{0, 1, 2, \dots\}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, *and* $\mathbb{C}$. *Also let* $\mathbb{Z}_+ := \mathbb{N} \setminus \{0\}$.

- Set notations.
- Recalled basic notions of a function being one to one, onto, and invertible. Think of functions in terms of a bunch of arrows from the domain set to the range set. To find the inverse function you should reverse the arrows.
- Some example of groups without the definition of a group:
  1. $GL(2, \mathbb{R}) = \left\{ g := \begin{bmatrix} a & b \\ c & d \end{bmatrix} : \det g = ad - bc \neq 0 \right\}$.
  2. Vector space with "group" operation being addition.
  3. The permutation group of invertible functions on a set S like $S = \{1, 2, \dots, n\}$.

1.1.1 A Little Number Theory

Axiom 1.2 (Well Ordering Principle) *Every non-empty subset,* S*, of* $\mathbb{N}$ *contains a smallest element.*

We say that a subset $S \subset \mathbb{Z}$ is **bounded below** if $S \subset [k, \infty)$ for some $k \in \mathbb{Z}$ and **bounded above** if $S \subset (-\infty, k]$ for some $k \in \mathbb{Z}$.

Remark 1.3 (Well ordering variations). The well ordering principle may also be stated equivalently as:

1. any subset $S \subset \mathbb{Z}$ which is bounded from below contains a smallest element or
2. any subset $S \subset \mathbb{Z}$ which is bounded from above contains a largest element.

To see this, suppose that $S \subset [k, \infty)$ and then apply the well ordering principle to $S - k$ to find a smallest element, $n \in S - k$. That is $n \in S - k$ and $n \le s - k$ for all $s \in S$. Thus it follows that $n + k \in S$ and $n + k \le s$ for all $s \in S$ so that $n + k$ is the desired smallest element in S.

For the second equivalence, suppose that $S \subset (-\infty, k]$ in which case $-S \subset [-k, \infty)$ and therefore there exist a smallest element $n \in -S$, i.e. $n \le -s$ for all $s \in S$. From this we learn that $-n \in S$ and $-n \ge s$ for all $s \in S$ so that $-n$ is the desired largest element of S.

Theorem 1.4 (Division Algorithm). *Let* $a \in \mathbb{Z}$ *and* $b \in \mathbb{Z}_+$*, then there exists unique integers* $q \in \mathbb{Z}$ *and* $r \in \mathbb{N}$ *with* $r < b$ *such that*

$$a = bq + r.$$

(For example,

$$5\overset{\;2}{\big|\underline{12}}\atop{\;\;\underline{10}\atop\;\;2} \text{ so that } 12 = 2 \cdot 5 + 2.)$$

Proof. Let

$$S := \{k \in \mathbb{Z} : a - bk \ge 0\}$$

which is bounded from above. Therefore we may define,

$$q := \max\{k : a - bk \ge 0\}.$$

As q is the largest element of S we must have,

$$r := a - bq \ge 0 \text{ and } a - b(q + 1) < 0.$$

The second inequality is equivalent to $r - b < 0$ which is equivalent to $r < b$. This completes the existence proof.

To prove uniqueness, suppose that $a = bq' + r'$ in which case, $bq' + r' = bq + r$ and hence,

$$b > |r' - r| = |b(q - q')| = b|q - q'|. \tag{1.1}$$

Since $|q - q'| \ge 1$ if $q \neq q'$, the only way Eq. (1.1) can hold is if $q = q'$ and $r = r'$. ■

Axiom 1.5 (Strong form of mathematical induction) *Suppose that* $S \subset \mathbb{Z}$ *is a non-empty set containing an element* a *with the property that; if* $[a, n) \cap \mathbb{Z} \subset S$ *then* $n \in \mathbb{Z}$*, then* $[a, \infty) \cap \mathbb{Z} \subset S$.

Axiom 1.6 (Weak form of mathematical induction) *Suppose that* $S \subset \mathbb{Z}$ *is a non-empty set containing an element* a *with the property that for every* $n \in S$ *with* $n \ge a$, $n + 1 \in S$*, then* $[a, \infty) \cap \mathbb{Z} \subset S$.

Remark 1.7. In Axioms 1.5 and 1.6 it suffices to assume that $a=0$. For if $a\neq 0$ we may replace S by $S-a:=\{s-a:s\in S\}$. Then applying the axioms with $a=0$ to $S-a$ shows that $[0,\infty)\cap\mathbb{Z}\subset S-a$ and therefore,

$$[a,\infty)\cap\mathbb{Z}=[0,\infty)\cap\mathbb{Z}+a\subset S.$$

Theorem 1.8 (Equivalence of Axioms). *Axioms 1.2 – 1.6 are equivalent. (Only partially covered in class.)*

Proof. We will prove 1.2 $\Longleftrightarrow$ 1.5 $\Longleftrightarrow$ 1.6 $\Longrightarrow$1.2.

1.2$\Longrightarrow$1.5 Suppose $0\in S\subset\mathbb{Z}$ satisfies the assumption in Axiom 1.5. If $\mathbb{N}_0$ is not contained in S, then $\mathbb{N}_0\setminus S$ is a non empty subset of $\mathbb{N}$ and therefore has a smallest element, n. It then follows by the definition of n that $[0,n)\cap\mathbb{Z}\subset S$ and therefore by the assumed property on S, $n\in S$. This is a contradiction since n can not be in both S and $\mathbb{N}_0\setminus S$.

1.5 $\Longrightarrow$1.2 Suppose that $S\subset\mathbb{N}$ does not have a smallest element and let $Q:=\mathbb{N}\setminus S$. Then $0\in Q$ since otherwise $0\in S$ would be the minimal element of S. Moreover if $[1,n)\cap\mathbb{Z}\subset Q$, then $n\in Q$ for otherwise n would be a minimal element of S. Hence by the strong form of mathematical induction, it follows that $Q=\mathbb{N}$ and hence that $S=\emptyset$.

1.5 $\Longrightarrow$1.6 Any set, $S\subset\mathbb{Z}$ satisfying the assumption in Axiom 1.6 will also satisfy the assumption in Axiom 1.5 and therefore by Axiom 1.5 we will have $[a,\infty)\cap\mathbb{Z}\subset S$.

1.6 $\Longrightarrow$1.5 Suppose that $0\in S\subset\mathbb{Z}$ satisfies the assumptions in Axiom 1.5. Let $Q:=\{n\in\mathbb{N}:[0,n)\subset S\}$. By assumption, $0\in Q$ since $0\in S$. Moreover, if $n\in Q$, then $[0,n)\subset S$ by definition of Q and hence $n+1\in Q$. Thus Q satisfies the restrictions on the set, S, in Axiom 1.6 and therefore $Q=\mathbb{N}$. So if $n\in\mathbb{N}$, then $n+1\in\mathbb{N}=Q$ and thus $n\in[0,n+1)\subset S$ which shows that $\mathbb{N}\subset S$. As $0\in S$ by assumption, it follows that $\mathbb{N}_0\subset S$ as desired.

■

1.2 Lecture 2 (1/7/2009)

Definition 1.9. *Given $a,b\in\mathbb{Z}$ with $a\neq 0$ we say that a **divides** b or a is a **divisor** of b (write $a|b$) provided $b=ak$ for some $k\in\mathbb{Z}$.*

Definition 1.10. *Given $a,b\in\mathbb{Z}$ with $|a|+|b|>0$, we let*

$$\gcd(a,b):=\max\{m:m|a \text{ and } m|b\}$$

*be the **greatest common divisor** of a and b. (We do not define $\gcd(0,0)$ and we have $\gcd(0,b)=|b|$ for all $b\in\mathbb{Z}\setminus\{0\}$.) If $\gcd(a,b)=1$, we say that a and b are **relatively prime**.*

Remark 1.11. Notice that $\gcd(a,b)=\gcd(|a|,|b|)\geq 0$ and $\gcd(a,0)=0$ for all $a\neq 0$.

Lemma 1.12 (Euclidean Algorithm). *Suppose that a,b are positive integers with $a<b$ and let $b=ka+r$ with $0\leq r<a$ by the division algorithm. If $r=0$, then $\gcd(a,b)=\gcd(a,r)$. In particular if $r=0$, we have*

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

Proof. Since $b=ka+r$ if d is a divisor of both a and r it is a divisor of b. Similarly, $r=b-ka$ so that if d is a divisor of both a and b then d is also a divisor of r. Thus the common divisors of a and r and a and b are the same and therefore $\gcd(a,b)=\gcd(a,r)$. ■

Example 1.13. Suppose that $a=15=3\cdot 5$ and $b=28=2^2\cdot 7$. In this case it is easy to see that $\gcd(15,28)=1$. Nevertheless, lets use Lemma 1.12 repeatedly as follows;

$$28=1\cdot 15+13 \text{ so } \gcd(15,28)=\gcd(13,15), \tag{1.2}$$
$$15=1\cdot 13+2 \text{ so } \gcd(13,15)=\gcd(2,13), \tag{1.3}$$
$$13=6\cdot 2+1 \text{ so } G\gcd(2,13)=\gcd(1,2), \tag{1.4}$$
$$2=2\cdot 1+0 \text{ so } \gcd(1,2)=\gcd(0,1)=1. \tag{1.5}$$

Moreover making use of Eqs. (1.2–1.4) in reverse order we learn that,

$$\begin{aligned}1&=13-6\cdot 2\\&=13-6\cdot(15-1\cdot 13)=7\cdot 13-6\cdot 15\\&=7\cdot(28-1\cdot 15)-6\cdot 15=7\cdot 28-13\cdot 15.\end{aligned}$$

Thus we have also shown that

$$1=s\cdot 28+t\cdot 15 \text{ where } s=7 \text{ and } t=-13.$$

The choices for s and t used above are certainly not unique. For example we have,

$$0=15\cdot 28-28\cdot 15$$

which added to

$$1=7\cdot 28-13\cdot 15$$

implies,

$$\begin{aligned}1&=(7+15)\cdot 28-(13+28)\cdot 15\\&=22\cdot 28-41\cdot 15\end{aligned}$$

as well.

Example 1.14. Suppose that $a = 40 = 2^3 \cdot 5$ and $b = 52 = 2^2 \cdot 13$. In this case we have $\gcd(40, 52) = 4$. Working as above we find,

$$\begin{aligned} 52 &= 1 \cdot 40 + 12 \\ 40 &= 3 \cdot 12 + 4 \\ 12 &= 3 \cdot 4 + 0 \end{aligned}$$

so that we again see $\gcd(40, 52) = 4$. Moreover,

$$4 = 40 - 3 \cdot 12 = 40 - 3 \cdot (52 - 1 \cdot 40) = 4 \cdot 40 - 3 \cdot 52.$$

So again we have shown $\gcd(a, b) = sa + tb$ for some $s, t \in \mathbb{Z}$, in this case $s = 4$ and $t = 3$.

Example 1.15. Suppose that $a = 333 = 3^2 \cdot 37$ and $b = 459 = 3^3 \cdot 17$ so that $\gcd(333, 459) = 3^2 = 9$. Repeated use of Lemma 1.12 gives,

$$459 = 1 \cdot 333 + 126 \text{ so } \gcd(333, 459) = \gcd(126, 333), \tag{1.6}$$
$$333 = 2 \cdot 126 + 81 \text{ so } \gcd(126, 333) = \gcd(81, 126), \tag{1.7}$$
$$126 = 81 + 45 \text{ so } \gcd(81, 126) = \gcd(45, 81), \tag{1.8}$$
$$81 = 45 + 36 \text{ so } \gcd(45, 81) = \gcd(36, 45), \tag{1.9}$$
$$45 = 36 + 9 \text{ so } \gcd(36, 45) = \gcd(9, 36), \text{ and} \tag{1.10}$$
$$36 = 4 \cdot 9 + 0 \text{ so } \gcd(9, 36) = \gcd(0, 9) = 9. \tag{1.11}$$

Thus we have shown that

$$\gcd(333, 459) = 9.$$

We can even say more. From Eq. (1.11) we have, $9 = 45 - 36$ and then from Eq. (1.11),

$$9 = 45 - 36 = 45 - (81 - 45) = 2 \cdot 45 - 81.$$

Continuing up the chain this way we learn,

$$\begin{aligned} 9 &= 2 \cdot (126 - 81) - 81 = 2 \cdot 126 - 3 \cdot 81 \\ &= 2 \cdot 126 - 3 \cdot (333 - 2 \cdot 126) = 8 \cdot 126 - 3 \cdot 333 \\ &= 8 \cdot (459 - 1 \cdot 333) - 3 \cdot 333 = 8 \cdot 459 - 11 \cdot 333 \end{aligned}$$

so that

$$9 = 8 \cdot 459 - 11 \cdot 333.$$

The methods of the previous two examples can be used to prove Theorem 1.16 below. However, we will two different variants of the proof.

Theorem 1.16. *If $a, b \in \mathbb{Z} \setminus \{0\}$, then there exists (not unique) numbers, $s, t \in \mathbb{Z}$ such that*

$$\gcd(a, b) = sa + tb. \tag{1.12}$$

Moreover if $m \neq 0$ is any common divisor of both a and b then $m | \gcd(a, b)$.

Proof. If m is any common divisor of a and b then m is also a divisor of $sa + tb$ for any $s, t \in \mathbb{Z}$. (In particular this proves the second assertion given the truth of Eq. (1.12).) In particular, $\gcd(a, b)$ is a divisor of $sa + tb$ for all $s, t \in \mathbb{Z}$. Let $S := \{sa + tb : s, t \in \mathbb{Z}\}$ and then define

$$d := \min(S \cap \mathbb{Z}_+) = sa + tb \text{ for some } s, t \in \mathbb{Z}. \tag{1.13}$$

By what we have just said if follows that $\gcd(a, b) | d$ and in particular $d \geq \gcd(a, b)$. If we can snow d is a common divisor of a and b we must then have $d = \gcd(a, b)$. However, using the division algorithm,

$$a = kd + r \text{ with } 0 \leq r < d. \tag{1.14}$$

As

$$r = a - kd = a - k(sa + tb) = (1 - ks)a - ktb \in S \cap \mathbb{N},$$

if r were greater than 0 then $r \geq d$ (from the definition of d in Eq. (1.13) which would contradict Eq. (1.14). Hence it follows that $r = 0$ and $d | a$. Similarly, one shows that $d | b$. ■

Lemma 1.17 (Euclid's Lemma). *If $\gcd(c, a) = 1$, i.e. c and a are relatively prime, and $c | ab$ then $c | b$.*

Proof. We know that there exists $s, t \in \mathbb{Z}$ such that $sa + tc = 1$. Multiplying this equation by b implies,

$$sab + tcb = b.$$

Since $c | ab$ and $c | cb$, it follows from this equation that $c | b$. ■

Corollary 1.18. *Suppose that $a, b \in \mathbb{Z}$ such that there exists $s, t \in \mathbb{Z}$ with $1 = sa + tb$. Then a and b are relatively prime, i.e. $\gcd(a, b) = 1$.*

Proof. If $m > 0$ is a divisor of a and b, then $m | (sa + tb)$, i.e. $m | 1$ which implies $m = 1$. Thus the only positive common divisor of a and b is 1 and hence $\gcd(a, b) = 1$. ■

1.2.1 Ideals (Not covered in class.)

Definition 1.19. *As non-empty subset $S \subset \mathbb{Z}$ is called an **ideal** if S is closed under addition (i.e. $S + S \subset S$) and under multiplication by **any** element of $\mathbb{Z}$, i.e. $\mathbb{Z} \cdot S \subset S$.*

Example 1.20. For any $n \in \mathbb{Z}$, let

$$(n) := \mathbb{Z} \cdot n = n\mathbb{Z} := \{kn : k \in \mathbb{Z}\}.$$

I is easily checked that (n) is an ideal. The next theorem states that this is a listing of all the ideals of $\mathbb{Z}$.

Theorem 1.21 (Ideals of $\mathbb{Z}$). *If $S \subset \mathbb{Z}$ is an ideal then $S = (n)$ for some $n \in \mathbb{Z}$. Moreover either $S = \{0\}$ in which case $n = 0$ for $S \neq \{0\}$ in which case $n = \min(S \cap \mathbb{Z}_+)$.*

Proof. If $S = \{0\}$ we may take $n = 0$. So we may assume that S contains a non-zero element a. By assumption that $\mathbb{Z} \cdot S \subset S$ it follows that $-a \in S$ as well and therefore $S \cap \mathbb{Z}_+$ is not empty as either a or $-a$ is positive. By the well ordering principle, we may define n as, $n := \min S \cap \mathbb{Z}_+$.

Since $\mathbb{Z} \cdot n \subset \mathbb{Z} \cdot S \subset S$, it follows that $(n) \subset S$. Conversely, suppose that $s \in S \cap \mathbb{Z}_+$. By the division algorithm, $s = kn + r$ where $k \in \mathbb{N}$ and $0 \le r < n$. It now follows that $r = s - kn \in S$. If $r > 0$, we would have to have $r \ge n = \min S \cap \mathbb{Z}_+$ and hence we see that $r = 0$. This shows that $s = kn$ for some $k \in \mathbb{N}$ and therefore $s \in (n)$. If $s \in S$ is negative we apply what we have just proved to $-s$ to learn that $-s \in (n)$ and therefore $s \in (n)$. ∎

Remark 1.22. Notice that $a|b$ iff $b = ak$ for some $k \in \mathbb{Z}$ which happens iff $b \in (a)$.

Proof. Second Proof of Theorem 1.16. Let $S := \{sa + tb : s, t \in \mathbb{Z}\}$. One easily checks that $S \subset \mathbb{Z}$ is an ideal and therefore $S = (d)$ where $d := \min S \cap \mathbb{Z}_+$. Notice that $d = sa + tb$ for some $s, t \in \mathbb{Z}$ as $d \in S$. We now claim that $d = \gcd(a, b)$. To prove this we must show that d is a divisor of a and b and that it is the maximal such divisor.

Taking $s = 1$ and $t = 0$ or $s = 0$ and $t = 1$ we learn that both $a, b \in S = (d)$, i.e. $d|a$ and $d|b$. If $m \in \mathbb{Z}_+$ and $m|a$ and $m|b$, then

$$\frac{d}{m} = s\frac{a}{m} + t\frac{b}{m} \in \mathbb{Z}$$

from which it follows that so that $m|d$. This shows that $d = \gcd(a, b)$ and also proves the last assertion of the theorem.

Alternate proof of last statement. If $m|a$ and $m|b$ there exists $k, l \in \mathbb{Z}$ such that $a = km$ and $b = lm$ and therefore,

$$d = sa + tb = (sk + tl)\, m$$

which again shows that $m|d$. ∎

Remark 1.23. As a second proof of Corollary 1.18, if $1 \in S$ (where S is as in the second proof of Theorem 1.16)), then $\gcd(a, b) = \min(S \cap \mathbb{Z}_+) = 1$.

1.3 Lecture 3 (1/9/2009)

1.3.1 Prime Numbers

Definition 1.24. *A number, $p \in \mathbb{Z}$, is **prime** iff $p \ge 2$ and p has no divisors other than 1 and p. Alternatively put, $p \ge 2$ and $\gcd(a, p)$ is either 1 or p for all $a \in \mathbb{Z}$.*

Example 1.25. The first few prime numbers are $2, 3, 5, 7, 11, 13, 17, 19, 23, \dots$.

Lemma 1.26 (Euclid's Lemma again). *Suppose that p is a prime number and $p|ab$ for some $a, b \in \mathbb{Z}$ then $p|a$ or $p|b$.*

Proof. We know that $\gcd(a, p) = 1$ or $\gcd(a, p) = p$. In the latter case $p|a$ and we are done. In the former case we may apply Euclid's Lemma 1.17 to conclude that $p|b$ and so again we are done. ∎

Theorem 1.27 (The fundamental theorem of arithmetic). *Every $n \in \mathbb{Z}$ with $n \ge 2$ is a prime or a product of primes. The product is unique except for the order of the primes appearing the product. Thus if $n \ge 2$ and $n = p_1 \dots p_n = q_1 \dots q_m$ where the p's and q's are prime, then $m = n$ and after renumbering the q's we have $p_i = q_i$.*

Proof. Existence: This clearly holds for $n = 2$. Now suppose for every $2 \le k \le n$ may be written as a product of primes. Then either $n + 1$ is prime in which case we are done or $n + 1 = a \cdot b$ with $1 < a, b < n + 1$. By the induction hypothesis, we know that both a and b are a product of primes and therefore so is $n + 1$. This completes the inductive step.

Uniqueness: You are asked to prove the uniqueness assertion in 0.#25. Here is the solution. Observe that $p_1 | q_1 \dots q_m$. If p_1 does not divide q_1 then $\gcd(p_1, q_1) = 1$ and therefore by Euclid's Lemma 1.17, $p_1 | (q_2 \dots q_m)$. It now follows by induction that p_1 must divide one of the q_i, by relabeling we may assume that $q_1 = p_1$. The result now follows by induction on $n \vee m$. ∎

Definition 1.28. *The least common multiple of two non-zero integers, a, b, is the smallest positive number which is both a multiple of a and b and this number will be denoted by $\operatorname{lcm}(a, b)$. Notice that $m = \min((a) \cap (b) \cap \mathbb{Z}_+)$.*

Example 1.29. Suppose that $a = 12 = 2^2 \cdot 3$ and $b = 15 = 3 \cdot 5$. Then $\gcd(12, 15) = 3$ while

$$\operatorname{lcm}(12, 15) = \left(2^2 \cdot 3\right) \cdot 5 = 2^2 \cdot (3 \cdot 5) = \left(2^2 \cdot 3 \cdot 5\right) = 60.$$

Observe that

$$\gcd(12, 15) \cdot \operatorname{lcm}(12, 15) = 3 \cdot \left(2^2 \cdot 3 \cdot 5\right) = \left(2^2 \cdot 3\right) \cdot (3 \cdot 5) = 12 \cdot 15.$$

This is a special case of Chapter 0.#12 on p. 23 which can be proved by similar considerations. In general if

$$a = p_1^{n_1} \cdot \dots \cdot p_k^{n_k} \text{ and } b = p_1^{m_1} \dots p_k^{m_k} \text{ with } n_j, m_l \in \mathbb{N}$$

then

$$\gcd(a, b) = p_1^{n_1 \wedge m_1} \cdot \dots \cdot p_k^{n_k \wedge m_k} \text{ and } \operatorname{lcm}(a, b) = p_1^{n_1 \vee m_1} \cdot \dots \cdot p_k^{n_k \vee m_k}.$$

Therefore,

$$\begin{aligned}\gcd(a, b) \cdot \operatorname{lcm}(a, b) &= p_1^{n_1 \wedge m_1 + n_1 \vee m_1} \cdot \dots \cdot p_k^{n_k \wedge m_k + n_k \vee m_k} \\ &= p_1^{n_1 + m_1} \cdot \dots \cdot p_k^{n_k + m_k} = a \cdot b.\end{aligned}$$

1.3.2 Modular Arithmetic

Definition 1.30. *Let n be a positive integer and let $a = q_a n + r_a$ with $0 \le r_a < n$. Then we define $a \bmod n := r_a$. (Sometimes we might write $a = r_a \bmod n$ – but I will try to stick with the first usage.)*

Lemma 1.31. *Let $n \in \mathbb{Z}_+$ and $a, b, k \in \mathbb{Z}$. Then:*

1. $(a + kn) \bmod n = a \bmod n$.
2. $(a + b) \bmod n = (a \bmod n + b \bmod n) \bmod n$.
3. $(a \cdot b) \bmod n = ((a \bmod n) \cdot (b \bmod n)) \bmod n$.

Proof. Let $r_a = a \bmod n$, $r_b = b \bmod n$ and $q_a, q_b \in \mathbb{Z}$ such that $a = q_a n + r_a$ and $b = q_b n + r_b$.

1. Then $a + kn = (q_a + k) n + r_a$ and therefore,
$$(a + kn) \bmod n = r_a = a \bmod n.$$
2. $a + b = (q_a + q_b) n + r_a + r_b$ and hence by item 1 with $k = q_a + q_b$ we find,
$$(a + b) \bmod n = (r_a + r_b) \bmod n. = (a \bmod n + b \bmod n) \bmod n.$$
3. For the last assertion,
$$a \cdot b = [q_a n + r_a] \cdot [q_b n + r_b] = (q_a q_b n + r_a q_b + r_b q_a) n + r_a \cdot r_b$$
and so again by item 1. with $k = (q_a q_b n + r_a q_b + r_b q_a)$ we have,
$$(a \cdot b) \bmod n = (r_a \cdot r_b) \bmod n = ((a \bmod n) \cdot (b \bmod n)) \bmod n.$$

■

Example 1.32. Take $n = 4$, $a = 18$ and $b = 7$. Then $18 \bmod 4 = 2$ and $7 \bmod 4 = 3$. On one hand,

$$\begin{aligned}&(18 + 7) \bmod 4 = 25 \bmod 4 = 1 \text{ while on the other,} \\ &(2 + 3) \bmod 4 = 1.\end{aligned}$$

Similarly, $18 \cdot 7 = 126 = 4 \cdot 31 + 2$ so that

$$\begin{aligned}&(18 \cdot 7) \bmod 4 = 2 \text{ while} \\ &(2 \cdot 3) \bmod 4 = 6 \bmod 4 = 2.\end{aligned}$$

Remark 1.33 (Error Detection). Companies often add extra digits to identification numbers for the purpose of detecting forgery or errors. For example the United Parcel Service uses a mod 7 check digit. Hence if the identification number were $n = 354691332$ one would append

$$\begin{aligned}&n \bmod 7 = 354691332 \bmod 7 = 2 \text{ to the number to get} \\ &354691332\_2 \text{ (say).}\end{aligned}$$

See the book for more on this method and other more elaborate check digit schemes. Note,

$$354691332 = 50\,670\,190 \cdot 7 + 2.$$

Remark 1.34. Suppose that $a, n \in \mathbb{Z}_+$ and $b \in \mathbb{Z}$, then it is easy to show

$$(ab) \bmod (an) = a \cdot (b \bmod n).$$

Example 1.35 (Computing $\bmod 10$). We have,

$$\begin{aligned}123456 \bmod 10 &= 6 \\ 123456 \bmod 100 &= 56 \\ 123456 \bmod 1000 &= 456 \\ 123456 \bmod 10000 &= 3456 \\ 123456 \bmod 100000 &= 23456 \\ 123456 \bmod 1000000 &= 123456\end{aligned}$$

so that

$$a_n \ \dots a_2 \ a_1 \bmod 10^k = a_k \ \dots a_2 \ a_1 \text{ for all } k \le n.$$

Solution to Exercise (0.52). As an example, here is a solution to Problem 0.52 of the book which states that $\overbrace{111\dots 1}^{k\text{ times}}$ is not the square of an integer except when $k=1$.

As 11 is prime we may assume that $k \geq 3$. By Example 1.35, $111\dots 1 \bmod 10 = 1$ and $111\dots 1 \bmod 100 = 11$. Hence $1111\dots 1 = n^2$ for some integer n, we must have

$$n^2 \bmod 10 = 1 \text{ and } \left(n^2-1\right) \bmod 100 = 10.$$

The first condition implies that $n \bmod 10 = 1$ or 9 as $1^2 = 1$ and $9^2 \bmod 10 = 81 \bmod 10 = 1$. In the first case we have, $n = k \cdot 10 + 1$ and therefore we must require,

$$\begin{aligned} 10 &= \left(n^2-1\right) \bmod 100 = \left[(k\cdot 10+1)^2 - 1\right] \bmod 100 = \left(k^2 \cdot 100 + 2k\cdot 10\right) \bmod 100 \\ &= (2k\cdot 10) \bmod 100 = 10 \cdot (2k \bmod 10) \end{aligned}$$

which implies $1 = (2k \bmod 10)$ which is impossible since $2k \bmod 10$ is even.

For the second case we must have,

$$\begin{aligned} 10 &= \left(n^2-1\right) \bmod 100 \bmod 100 = \left[(k\cdot 10+9)^2 - 1\right] \bmod 100 \\ &= \left(k^2\cdot 100 + 18k\cdot 10 + 81 - 1\right) \bmod 100 \\ &= ((10+8)\,k\cdot 10 + 8\cdot 10) \bmod 100 \\ &= (8\,(k+1)\cdot 10) \bmod 100 \\ &= 10 \cdot 8k \bmod 10 \end{aligned}$$

which implies which $1 = (8k \bmod 10)$ which again is impossible since $8k \bmod 10$ is even.

1.3.3 Equivalence Relations

Definition 1.36. *A* ***equivalence relation*** *on a set S is a subset, $R \subset S \times S$ with the following properties:*

1. *R* ***is reflexive:*** *$(a,a) \in R$ for all $a \in S$*
2. *R* ***is symmetric:*** *If $(a,b) \in R$ then $(b,a) \in R$.*
3. *R* ***is transitive:*** *If $(a,b) \in R$ and $(b,c) \in R$ then $(a,c) \in R$.*

*We will usually write $a \sim b$ to mean that $(a,b) \in R$ and pronounce this as a is equivalent to b. With this notation we are assuming $a \sim a$, $a \sim b \implies b \sim a$ and $a \sim b$ and $b \sim c \implies a \sim c$. (**Note well:** the book write aRb rather than $a \sim b$.)*

Example 1.37. If $S = \{1,2,3,4,5\}$ then:

1. $R = \{1,2,3\}^2 \cup \{4,5\}^2$ is an equivalence relation.
2. $R = \{(1,1),(2,2),(3,3),(4,4),(5,5),(1,2),(2,1),(2,3),(3,2)\}$ is not an equivalence relation. For example, $1 \sim 2$ and $2 \sim 3$ but 1 is not equivalent to 3, so R is not transitive.

Example 1.38. Let $n \in \mathbb{Z}_+$, $S = \mathbb{Z}$ and say $a \sim b$ iff $a \bmod n = b \bmod n$. This is an equivalence relation. For example, when $s = 2$ we have $a \sim b$ iff both a and b are odd or even. So in this case $R = \{\text{odd}\}^2 \cup \{even\}^2$.

Example 1.39. Let $S = \mathbb{R}$ and say $a \sim b$ iff $a \geq b$. Again not symmetric so is not an equivalence relation.

Definition 1.40. *A* ***partition*** *of a set S is a decomposition, $\{S_\alpha\}_{\alpha\in I}$, by disjoint sets, so S_α is a non-empty subset of S such that $S = \cup_{\alpha\in I} S_\alpha$ and $S_\alpha \cap S_\beta = \emptyset$ if $\alpha \neq \beta$.*

Example 1.41. If $\{S_\alpha\}_{\alpha\in I}$ is a partition of S, then $R = \cup_{\alpha\in I} S_\alpha^2$ is an equivalence relation. The next theorem states this is the general type of equivalence relation.

Theorem 1.42. *Let R or $\sim$ be an equivalence relation on S and for each $a \in S$, let $[a] := \{b \in S : b \sim a\}$ be the* ***equivalence class*** *of a.. Then $S = \cup_{a\in S}[a]$ and $[a] \cap [b] \neq \emptyset$ iff $[a] = [b]$.*

Proof. Because a is reflexive, $a \in [a]$ for all a and therefore, $S = \cup_{a\in S}[a]$.

Suppose that $[a] \cap [b] \neq \emptyset$ in which there exists $c \in [a] \cap [b]$, i.e. $c \sim a$ and $c \sim b$. Because $\sim$ is transitive and reflexive, it follows that $a \sim b$ as well. Thus if $x \in [a]$, i.e. $x \sim a$ we must also have $x \sim b$ (again because $\sim$ is transitive and reflexive), that is $x \in [b]$. This shows that $[a] \subset [b]$. Similarly we can show $[b] \subset [a]$ and thus $[a] = [b]$ as desired. ∎

Exercise 1.1. Suppose that $S = \mathbb{Z}$ with $a \sim b$ iff $a \bmod n = b \bmod n$. Identify the equivalence classes of $\sim$. Answer,

$$\{[0],[1],\dots,[n-1]\}$$

where

$$[i] = i + n\mathbb{Z} = \{i + ns : s \in \mathbb{Z}\}.$$

Exercise 1.2. Suppose that $S = \mathbb{R}^2$ with $\mathbf{a} = (a_1,a_2) \sim \mathbf{b} = (b_1,b_2)$ iff $|\mathbf{a}| = |\mathbf{b}|$ where $|\mathbf{a}| := a_1^2 + a_2^2$. Show that $\sim$ is an equivalence relation and identify the equivalence classes of $\sim$. Answer, the equivalence classes consists of concentric circles centered about the origin $(0,0) \in S$.