4 Induction and the Integers

In this chapter we cover all sections of Chapter 4 of the text. We also add some material about the 'modulo' function. The topics covered are

- Inductive proofs
- Recursive definitions
- The Fibonacci numbers
- Divisibility and the Division Algorithm
- Prime numbers
- The (Reverse) Euclidean Algorithm and GCD
- The Fundamental Theorem of Arithmetic
- The integers modulo m.

4.1 Induction

A *proof by induction* proceeds as follows. For a open statement $S(n)$ where the universe for n is the set of positive integers, we can prove that $S(n)$ is true for all n by proving the following two statements.

1. $S(1)$ is true.
2. For all $k \geq 2$, if $S(k-1)$ is true, then $S(k)$ is true.

Having done this, the principle of induction impies that $S(n)$ is true for all n.

Statement 1. is called the 'basis step' and 2. is called the 'induction step'. The assumption that $S(k-1)$ is true, in the induction step, is called the 'induction hypothesis'.

In practice, the universe for n may vary.

Example 4.1. Use induction to show that

$$\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$$

for all positive integers n.

Sol:

Let $S(n)$ be the statement that $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$.

Basis step $S(1)$**:** $\sum_{i=1}^{1} i = 1 = \frac{1(2)}{2}$, so $S(1)$ is true.

Induction Step: Assume that $S(k-1)$ is true, we show that $S(k)$ is true.

$$\begin{aligned}\sum_{i=1}^{k} i &= (\sum_{i=1}^{k-1} i) + k \\ &= \frac{(k-1)(k)}{2} + k \text{ by induction hypothesis} \\ &= \frac{(k-1)(k)+2k}{2} \\ &= \frac{k(k+1)}{2}\end{aligned}$$

This is $S(k)$. By the principle of induction, $S(n)$ is true for all positive integers n.

In the next example our universe for n is $\mathbb{N}$ instead of $\mathbb{Z}^+$. The principle of induction still applies here, indeed, we could replace every occurence of n with $n-1$ and 'shift' our argument to the universe $\mathbb{Z}^+$.

Example 4.2. Show that for any finite set A, $|\mathscr{P}(A)| = 2^{|A|}$.

Sol:

We prove this by induction on $|A|$. *(We are implicitly saying that $n = |A|$, so our statement $S(n)$ would be that for sets A with $|A| = n$ the equality holds. It is common to write up an induction proof like this, not making these definitions explicit.)*

Indeed, the equality is true if $|A| = 0$ because then $\mathscr{P}(A) = \{\emptyset\}$ so $|\mathscr{P}(A)| = 1 = 2^0 = 2^{|A|}$.

Now assume the equality is true for sets of size $k-1$ and let $|A| = k$. Let $a_0 \in A$ and let $A' = A \setminus a_0$.

Then

$$\begin{aligned}\mathscr{P}(A) &= \{B \mid B \subset A\} \\ &= \{B \mid B \subset A'\} \cup \{B \cup \{a_0\} \mid B \subset A'\}\end{aligned}$$

The sets $\{B \mid B \subset A'\}$ and $\{B \cup \{a_0\} \mid B \subset A'\}$ disjoint and both have size $|\mathscr{P}(A')|$ which by the induction hypothesis is 2^{k-1} so $|\mathscr{P}(A)| = 2^{k-1} + 2^{k-1} = 2^k$. The equality follows by induction.

4.1.1 Strong induction

Sometime it is useful strenghen our induction assumption, and assume that a statement $S(n)$ has been proved for more values of n.

Example 4.3. Show that for all $n \geq 14$, n can be written as a sum of '3's and '8's.

Sol:

We show this by induction on n. As our basis step, we show that it is true for $n = 14, 15$ and 16. Indeed $14 = 8 + 3 + 3$, $15 = 3 + 3 + 3 + 3 + 3$, and $16 = 8 + 8$. Now assume we have proved the claim for $n = k - 3, k - 2$ and $k - 1$; we prove it for $n = k$. Indeed $k = (k-3)+3$, and by the induction hypothesis $k-3$ can be written as a sum of '3's and '8's. So k can be as well. The claim follows by induction.

4.2 Recursive Definitions

We can define things using a process similar to induction. This process is called recursion, it consists of a base step, and a recursion step.

The following three definitions are by recursion.

Definition 4.4. Let the notation $n!$ be defined as follows.

- Base Step: $0! = 1$
- Recursion Step: For $n \geq 1$, $n! = (n-1)! \cdot n$.

Definition 4.5. Let the general union $A_1 \cup A_2 \cup \cdots \cup A_n$ be defined for all $n \geq 2$ as follows.

- $A_1 \cup A_2 = \{x \mid x \in A_1 \vee x \in A_2\}$
- $A_1 \cup A_2 \cup \cdots \cup A_n = (A_1 \cup A_2 \cup \cdots \cup A_{n-1}) \cup A_n$

In any course in which recursion is defined, one must have the following example.

Definition 4.6. The n^{th} Fibonacci number F_n is defined for all $n \geq 0$ as follows.

- $F_0 = 1$ and $F_1 = 1$.
- For $i \geq 2$, $F_n = F_{n-2} + F_{n-1}$.

Recursive definitions lend to inductive proofs.

Problem 4.1. Show $\overline{\cup_{i=1}^{n} A_i} = \cap_{i=1}^{n} \overline{A_i}$. (General DeMorgan.)

Sol:

We know it is true for $n = 2$. We proceed by induction on n. Assume it is true for $n - 1$ sets. Then

$$\begin{aligned}
\overline{\cup_{i=1}^{n} A_i} &= \overline{(\cup_{i=1}^{n-1} A_i) \cup A_n} \\
&= \overline{(\cup_{i=1}^{n-1} A_i)} \cap \overline{A_n} \quad \text{by } n = 2 \text{ case} \\
&= (\cap_{i=1}^{n-1} \overline{A_i}) \cap \overline{A_n} \quad \text{by } n - 1 \text{ case} \\
&= \cap_{i=1}^{n} \overline{A_i}
\end{aligned}$$

Problem 4.2. Where F_i is the i^{th} Fibonacci number, show that the following is true for all $n \geq 2$.

$$F_0 + F_1 + \cdots + F_n = F_{n+2} - 1.$$

Sol:

For the base step, observe that $F_0 = 1 = 2-1 = F_2-1$. Now assume that the result has been proved for all $n < k$, we prove if for $n = k$. Indeed, by the induction hypothesis $F_0 + F_1 + \cdots + F_{k-1} + F_k = F_k + F_{k+1} - 1$ and this is $F_{k+1} - 1$, by definition.

As a final example, observe that

$$\binom{n+1}{r} = \binom{n}{r} + \binom{n}{r-1}.$$

(Give a combinatorial argument for this identity.) This allows us to define the binomial co-efficients recursively as follows.

Definition 4.7. The binomial coefficients are defined by:

- $\binom{0}{0} = 1$
- $\binom{n}{r} = 0$ if $r > n$ or $r < 0$
- $\binom{n+1}{r} = \binom{n}{r} + \binom{n}{r-1}$ otherwise

Problem 4.3. Use the recursive definition of the binomial coefficients to calculate $\binom{4}{2} = 6$.

4.3 The Division Algorithm

Definition 4.8. For integers a and b, we say 'a *divides* b', and write $a \mid b$, if there is some integer x such that $ax = b$. In this case, we also say a is a *divisor* or *factor* of b, and b is a *multiple* of a.

Example 4.9. Accoring to this definition we have that: $3 \mid 9$, $-2 \mid 12$, $2 \mid -12$, $7 \mid 0$, '$0 \mid a \Rightarrow a = 0$'.

Further we have $a \mid 0 \Rightarrow a = 0$. This is an important property of the integers. It is the property of having 'no zero divisors', and doesn't hold in such number systems as $\mathbb{Z}_{12}$: the integers modulo 12. This is introduced in Chapter 14 of the text. We will not look at $\mathbb{Z}_m$, but in the end of this chapter look at something very similar.

Anyways, without this property, we would not be able to cancel:

$$ab = ac \Rightarrow b = c$$

and many of the properties we prove in this chapter would not be true.

Let's record/prove a couple easy properties dealing with divisiblity.

Theorem 4.10. *For all integers a, b, and c the following hold.*

a) $1 \mid a$, $-1 \mid a$, *and* $a \mid 0$.

b) If $a \mid b$ *and* $b \mid a$, *then* $a = \pm b$.

c) If $a \mid b$ *and* $b \mid c$, *then* $a \mid c$.

d) If $a \mid b$ *then* $a \mid xb$ *for all integers* x.

e) If $x + y = z$ *and* a *divides two of* x, y *and* z, *then* a *divides all of* x, y, *and* z.

f) If a *divides* c_i *for* $i = 1, \ldots, d$, *then* a *divides any* linear combination *of the* c_i, *that is:*

$$a \mid x_1c_1 + x_2c_2 + \cdots + x_dc_d$$

for any integers $x_1, \ldots, x_d$.

Proof. You should be able to prove all of these, but we prove only b) and e).

To see b), assume that $a \mid b$ and $b \mid a$. By definition, there are integers x and x' such that $ax = b$ and $bx' = a$, and so $a = bx' = (ax)x' = a(xx')$. This implies that $xx' = 1$, but both x and x' are integers so $x = x' = \pm 1$. From $a = x'b$ this give $a = \pm b$.

For e), there are three cases to prove, for the first, we assume that a divides x and z and show that it divides y also. The proofs of the other cases (what are they?) are essentially the same, so we omit them. Assuming that a divides x and z, we have that $ax' = x$ and $az' = z$ for some integers x' and z'. Now $y = z - x = az' - ax' = a(z' - x') = ay'$ where $y' = (z' - x')$ is an integer. So a divides y. □

The following two problems use the above rules.

Problem 4.4. Do there exist integers x, y and z such that

$$7x + 14y + 49z = 100?$$

Sol:

No. We know that 7 divides all of $7, 14$, and 49, so it divides the left side of the equation, but it doesn't divide the right side: 100.

Problem 4.5. Suppose that $13 \mid 3a + 4b$. Show that $13 \mid 7a + 5b$.

Sol:

From Theorem 4.10 d) we have that

$$13 \mid -2(3a + 4b) = -6a - 8b.$$

From the fact that $13 \mid 13$, we have using Theorem 4.10 that

$$13 \mid 13a + 13b.$$

Thus by Theorem 4.10 b),

$$13 \mid 13a + 13b - 6a - 8b = 7a + 5b,$$

as needed.

Definition 4.11. An integer $p \geq 2$ is *prime* if its only positive divisors are 1 and p. It is *composite* if it isn't prime.

Note that 1 is neither prime or composite. Also note that by definition any composite number n can be expressed as the product of two integers greater than 1. In fact with a bit of work we can say that a can assumed to be prime.

Lemma 4.12. *Let $n \geq 2$ be an integer. Then there is some prime p such that $p \mid n$.*

Proof. Our proof is by strong induction. For $n = 2$ we have $2 \mid 2$, and 2 is prime, so we are done. Assume the lemma has been proved for all values less then n. If n is prime, then $n \mid n$ and we are done, so we may assume that n is composite. Then $n = ab$ for some integers a and b less than n. By the induction hypothesis, $p \mid a$ for some prime p. But then $p \mid ab = n$ by Theorem 4.10. □

This lemma helps us prove the following old theorem of Euclid.

Theorem 4.13. *There are infinitely many primes.*

Proof. Towards condtradiction, assume that there are finitely many primes: $p_1, \ldots, p_n$. Let $N = p_1 p_2 \ldots p_n + 1$. By Lemma 4.12 there is some prime q such that $q \mid N$. Since it is prime, $q = p_i$ for some i, so $q \mid p_1 p_2 \ldots p_n$. By Theorem 4.10 we have that $q \mid 1$. But this implies that $q = 1$, a contradiction. □

Theorem 4.14 (The Division Algorithm)**.** *For $a, b \in \mathbb{Z}$ with $b > 0$, there exist unique $q, r \in \mathbb{Z}$ with $0 \leq r < b$ such that $a = qb + r$.*

Proof. We split the proof up into two parts: the existence of q, r, and their uniqueness.

For existence, we first prove the theorem for $a \geq 0$ by induction on a. For $0 \leq a < r$ and any b, $q = 0$ and $r = a$ make the equation true. This is our base case. Now fix $b \geq 0$ and let $a \geq r$. Assume that for any non-negative integer a' less then a we have $a = bq' + r'$ for integers q' and r' with $0 \leq r' < b$. Then because $a > r$, we have that $a - r = q'b + r'$, and so $a = (q' + 1)b + r'$.

Now for $a < 0$, $-a = q'b + r'$ for some q' and $0 \leq r' < b$, and so $a = -q'b - r'$. If $r' = 0$ we are done, otherwise, $a = (-q' - 1)b + b - r' = (-q' - 1)b + r$ where $r = b - r'$ is in $\{1, 2, \ldots, b - 1\}$.

To see that q and r are unique, for given a and b, we assume that $qb + r = a = q'b + r'$ are two such representations, and show that $q = q'$ and $r = r'$. Indeed, assume wlog that $q \geq q'$. Rearranging $qb + r = q'b + r'$ we get $r' - r = b(q - q')$. As $r' < b$ and r is positive, $b > r' - r$. So $q - q' < 1$. But q and q' are integers with $q \geq q'$ so $q = q'$. By $r' - r = b(q - q')$, this implies that $r = r'$, as needed. □

Although the above theorem is not an algorithm, it is usually called 'The Division Algorithm'. The inductive proof of existence suggests an algorithm for finding q and r when a is positive: subtract b repeatedly from a until you are left with $r < b$. The number of times you did this is q. Our proof ensures that this process terminates, and that the result is unique.

4.3.1 Integers in other bases

Definition 4.15. For integer $b \geq 2$ and $d_0, \ldots d_n \in \{0, 1, \ldots b-1\}$, the *base b integer* $(d_n d_{n-1} \ldots d_1 d_0)_b$ represents the the integer

$$d_n b^n + d_{n-1} b^{n-1} + \ldots d_2 b^2 + d_1 b + d_0.$$

So, for example, the number 99, which is represented in base 10, can be represented in base 7 as $(201)_7$, or in base 2 as $(1100011)_2$. In base 16, we need extra digits. It is standard that $(A)_{16}, (B)_{16}, \ldots, (F)_{16}$ are used for $10, 11, \ldots, 15$ respectively. Thus $90 = (5A)_{16}$.

The division algortihm ensures that any integer has a unique base b representation for any $b \geq 2$. Further, it suggests how to find it.

Example 4.16. To represent 131 in base 7 we repeatedly apply the division algorithm by dividing 7 into 131:

$$\begin{aligned} 131 &= 18(7) + 5 \\ 18 &= 2(7) + 4 \\ 4 &= 0(7) + 2 \end{aligned}$$

Reading up the column on the right, we get that $(245)_7 = 131$. Indeed $131 = 7(18)+5 = 7\,(7(2)+4)+5$, which gives that $131 = 2{\cdot}7^2+4{\cdot}7+5 = (245)_7$.

4.4 GCD and the Euclidean Algorithm

You have probably seen that the 'greatest common divisor', or the 'gcd' of two numbers is the greatest integer c that divides them both. However, our formal definition will use a more useful condition in place of 'greatest'.

Definition 4.17. For two non-zero integers a and b, $\gcd(a, b)$ is the unique positive integer c satisfying all of the following conditions.

i) $c|a$

ii) $c|b$

iii) If $d|a$ and $d|b$, then $d|c$.

It is clear that there are integers c satisfying items i) and ii) indeed 1 does, but not so clear that there is one that satisfies iii) as well. I think we believe it but we haven't talked about the prime decomposition of an integer yet, so it isn't fair to use this.

Theorem 4.18. *For non-zero integers a and b, $\gcd(a, b)$ exists.*

Proof. Consider the set S of poitive integers that can be written as $xa + yb$ for integers x and y. Let $c = x_0a + y_0b$ be the smallest integer in S. We claim $c = \gcd(a, b)$. First we show that $c \mid a$. Assume $c \nmid a$. Then $a = qc+r$ for integers q and r where $r < c$. So $r = a - qc = a - q(x_0a + y_0b) = (1 - qx_0)a + (-qy)b$ is in S. This contradicts the fact that c was the smallest element of S. So $c \mid a$. The proof that $c \mid b$ is the same. Now proving item iii) is easy. If $d \mid a$ and $d \mid b$ then $d \mid xa + yb$ for any integers x and y. In particular, $d \mid x_0a + y_0b = c$. □

Now to find the GCD of two numbers, we can list out the divisors of each number, and scan the lists:

Example 4.19. Finding $\gcd(18, 30)$.
Positive divisors of 18: $1, 2, 3, 6, 9, 18$
Positive divisors or 30: $1, 2, 3, 5, 6, 10, 15, 30$
By inspection, we have $\gcd(18, 30) = 6$.

However, this gets to be a lot of work for large numbers. We look at an algorithm to do it quickly, based on the following lemma.

Lemma 4.20. *If $a = bq + r$ then $\gcd(a, b) = \gcd(b, r)$.*

Proof. Let $a = bq + r$. We show that $\gcd(a, b) \mid \gcd(b, r)$ and that $\gcd(b, r) \mid \gcd(a, b)$. The lemma follows because $(x \mid y) \wedge (y \mid x) \Rightarrow x = \pm y$, and gcd are always positive.

By definition, $\gcd(a, b)$ divides a and b. So it also divides $r = a - bq$. As it divides b and r, the definition of $\gcd(b, r)$ implies that $\gcd(a, b) \mid \gcd(b, r)$. The proof that $\gcd(b, r) \mid \gcd(a, b)$ is similar. □

With this lemma in hand, we have a nice algorithm for finding the gcd of two integers. It is called the Euclidean Algorithm, and we introduce it by example.

Example 4.21. The Euclidean Algorithm to find $\gcd(132, 55)$.

Observe that

$$\begin{aligned} 132 &= 2(55) + 22 \\ 55 &= 2(22) + 11 \\ 22 &= 2(11) + 0 \end{aligned}$$

Thus by the lemma, $\gcd(132, 55) = \gcd(55, 22) = \gcd(22, 11) = \gcd(11, 0) = 11$.

In fact, one can take the algorithm further and find the integers x and y such that $\gcd(a, b) = xa + yb$. We proved such integers existed in the proof of Theorem 4.18.

Example 4.22. The Reverse Euclidean Algorithm.

From the calculations of the last example, we have that

$$\begin{aligned} 11 &= 55 - 2(22) \\ &= 55 - 2(132 - 2(55)). \end{aligned}$$

Collecting terms on the right, we have $11 = (-2)132 + (5)55$.

Problem 4.6. Find $\gcd(288, 89)$ and write it as a linear combination of 288 and 89.

By far the most important application of this algorithm is in defusing bombs, as we saw when Bruce Willis and Samuel L. Jackson's characters had to defuse a bomb in Die Hard: With A Vengeance. Essentially, their problem was this:

Problem 4.7. You have 2 containers, one measures 132ml and the other 55ml. How do you use these containers to measure out 11ml? 22ml? What quantities can you measure with these two containers? (See Example 4.37 of text.)

Definition 4.23. Integers a and b are *relatively prime* if $\gcd(a, b) = 1$.

Equivalently, a and b are relatively prime if and only if there exists integers x and y such that $ax = by = 1$. To determine if two integers are relatively we can use the Euclidean Algorithm.

Example 4.24. Prove that for all integers n, $13n + 5$ and $5n + 2$ are relatively prime.

Sol:

$$\begin{aligned} 13n + 5 &= 2(5n + 2) &&+(3n + 1) \\ 5n + 2 &= (3n + 1) &&+(2n + 1) \\ 3n + 1 &= (2n + 1) &&+n \\ 2n + 1 &= 2(n) &&+1 \end{aligned}$$

So $\gcd(13n + 5, 5n + 2) = 1$.

Recall that a real number r is *rational* if if can be expressed as a fraction of integers: $r = \frac{a}{b}$. Otherwise it is *irrational*.

Problem 4.8. For an integer n, show that if $\sqrt{n}$ rational then n is a perfect square.

Sol:

Assume that $\sqrt{n} = a/b$ for some integers a and b. We may assume that $\gcd(a, b) = 1$, because if it isn't, we can replace a and b by

$a/\gcd(a,b)$ and $b/\gcd(a,b)$ respectively. Now $n = a^2/b^2$, so $nb^2 = a^2$.

We show that $b = 1$ and so $n = a^2$, a perfect square. Towards contradiction, assume that $p \mid b$ for some prime p. Then $p^2 \mid b^2 n = a^2$, so $p \mid a$. This contradicts the fact that $\gcd(a,b) = 1$.

As a consequence, we have that, for example, $\sqrt{2}$ is irrational.

4.4.1 Least Common Multiple

Dual to the GCD is the LCM, or least common multiple.

Definition 4.25. The least common multiple $\text{lcm}(a,b)$ of integers a and b, is the is the unique positive integer c satisfying all of the following conditions.

i) $a \mid c$

ii) $b \mid c$

iii) If $a \mid d$ and $b \mid d$, then $c \mid d$.

Problem 4.9. Mimic the proof of Theorem 4.18 to show that the lcm of two integers does indeed exists. (See Thm 4.9 of text.)

Theorem 4.26.

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

Proof. We'll prove this in the next section. □

4.5 The Fundamental Theorem of Arithmetic

Theorem 4.27 (The Fundamental Theorem of Arithmetic)**.** *Every integer $n \geq 2$ can be written uniquely (up to order of the factors) as a product of primes.*

This unique representation of a number of a product of primes is called its *prime factorisation.* For example, the prime factorisation of 124 is

$$124 = 2 \cdot 2 \cdot 31.$$

The proof of the Theorem 4.27 consists of two parts. The first parts is an exercise:

Problem 4.10. Using Lemma 4.12 and induction, show that every integer has a representation as a product of primes.

We finish the proof of Theorem 4.27 by showing uniqueness. We start with a lemma.

Lemma 4.28. *Let a and b be positive integers, and p a prime. If $p \mid ab$, then either $p \mid a$ or $p \mid b$,*

We prove this below, but lets first look at our approach. Let r, s and t be the statements '$p \mid ab$', '$p \mid a$' and '$p \mid b$'. The theorem is the sentence $r \to s \vee t$. What we actully show is $(r \wedge \neg s) \to t$. Prove to yourself that these are logically equivalent.

Proof. If $p \mid a$ then we are done, so we assume that $p \nmid a$ and show that $p \mid b$.

As $p \nmid a$, a and p are relatively prime, so there exist x and y such that $xp + ya = 1$. Multiplying by b we get $p(xb) + y(ab) = b$. But p divides $p(xb)$, and it divides $y(ab)$ (because it divides ab), so p divides b, as needed. □

Using indution on the previous lemma, we can show

Corollary 4.29. *For all positive integers $a_1, \ldots, a_n$, and all prime p, if*

$$p \mid a_1 a_2 \ldots a_n,$$

then $p \mid a_i$ for some $i = 1, \ldots, n$.

Now we prove the uniqueness part of Theorem 4.27.

Proof of uniqueness in Thm. 4.27. The proof is trivially true if $n = 2$. Assume it is true for $n < k$, we show it is true for $n = k$.

Assume that k has two representations as a product of primes:

$$p_1 p_2 \ldots p_m = k = q_1 q_2 \ldots q_n.$$

We want to show that as multisets $\{p_1, p_2, \ldots, p_m\} = \{q_1, \ldots q_n\}$.

Now $p_1 \mid k = q_1 q_2 \ldots q_n$, so by Corollary 4.29, $p_1 | q_i$ for some i in $1, \ldots, n$. As they are both prime, $p_1 = q_i$. By the induction hypothesis, the theorem is true for k/p_1, and so the multisets $\{p_2, p_3, \ldots, p_m\}$ and $\{q_1 q_2 \ldots q_{i-1} q_{i+1} \ldots q_n\}$ are equal. Adding $p_1 = q_i$ to each, they are still the same. □

In the prime factorisation of an integer such as $124 = 2 \cdot 2 \cdot 31$ where a prime occurs more than once, we usually write the factorisation as

$$124 = 2^2 \cdot 31$$

and say the prime 2 has *power* 2 in the factorisation of 124.

If $p^d \mid a$, for some prime p, then $a = p^d \cdot x$ for some integer x and $a = p^d(p_1^{d_1} p_2^{d_2} \ldots p_m^{d_m})$ where the bracketed part is the prime factorisation of x. This is a prime factorisation of a, and so the power of p in the factorisation of a is at least d.

With this we can prove the following:

Lemma 4.30. *Let a and b be integers. For some prime p, let d_a be the power of p in the prime factorisation of a and d_b be the power of p in the prime factorisation of b. Then*

a) The power of p in ab is $d_a + d_b$.

b) The power of p in $\gcd(a,b)$ is $\min(d_a, d_b)$.

c) The power of p in $\text{lcm}(a,b)$ is $\max(d_a, d_b)$.

Proof. We prove b). (The other parts can be an exercise.) Let d be the power of p in $\gcd(a,b)$. Then $p^d \mid \gcd(a,b)$. So $p^d \mid a$ and $p^d \mid b$. □

With this lemma, we are easily able to prove Theorem 4.26 which states that $\text{lcm}(a,b) \cdot \gcd(a,b) = ab$.

Proof. For any prime p in the prime factorisation of ab the power of p in ab is $d_a + d_b = \min(d_a, d_b) + \max(d_a, d_b)$. On the other hand, the power of p in $\text{lcm}(a,b) \cdot \gcd(a,b)$ is the power of p in $\text{lcm}(a,b)$ plus the power in $\gcd(a,b)$, so is $\min(d_a, d_b) + \max(d_a, d_b)$.

This is true for any p dividing ab so the prime factorisations of ab and $\text{lcm}(a,b) \cdot \gcd(a,b)$ are the same. We conclude that they are equal. □

Definition 4.31. Let $d(n)$ be the number of positive divisors of n.

Problem 4.11. Find $d(2^3 \cdot 3^5 \cdot 7^2)$.

Sol:

> Each positive divisor of $2^3 \cdot 3^5 \cdot 7^2$ is of the form $2^a \cdot 3^b \cdot 7^c$ where $a \in \{0,1,2,3\}, b \in \{0,1,\ldots,5\}$, and $c \in \{0,1,2\}$. So there are $4 \times 6 \times 3$ different ones.

In a similar way one could show that where an integer n has prime decomposition

$$n = p_1^{d_1} \cdot p_2^{d^2} \cdot \ldots \cdot p_r^{d_r},$$

we have $d(n) = (d_1 + 1)(d_2 + 1)\ldots(d_r + 1)$.

4.6 Integers Modulo m (or clock numbers)

The following material is similar to that covered in Section 14.3 of the text, but fundamentally different. We are not defining a new number system here, simply a function of the integers.

For integers a and m, the division algorithm gives us unique integers q and r such that $a = qm + r$ with $0 \leq r \leq m - 1$. There is a lot that we can do only with the value r, throwing away the q. We denote this r by $a \mod m$, saying 'a is equal to r modulo m We write $a \equiv_m b$ to mean $(a \mod m) = (b \mod m)$. Equivalently,

Definition 4.32. For integers a, b and m, we write

$$a \equiv_m b$$

to mean that $m \mid a - b$. We say 'a is congruent to b modulo m'.

For example $7 \mod 4 = 3$, and $-9 \equiv_{10} 1 \equiv_{10} 11$.
The following alternate definition of $a \equiv_m b$ should be clear.

Fact 4.33. *We have $a \equiv_m b$ if and only if there is some integer k such that $a = b + mk$.*

Problem 4.12. Show that $4^n \equiv_9 3n + 1$ for all $n \geq 1$.

Sol:

This is clear if $n = 1$, indeed $4^1 = 3(1) + 1$. Assume it has been proved for $n = k - 1$, that is , that $4^{k-1} \equiv_9 3(k-1) + 1 + 9c$ for some integer c. Then

$$\begin{aligned} 4^k &= 4(4^{k-1}) \\ &= 4(4^{k-1}) \\ &= 4\left((3(k-1)+1)+9c)\right) \text{ by the induction hypothesis} \\ &= (3+1)(3(k-1)+1) + 4 \cdot 9c \\ &= 3(k-1) + 9(k-1) + 3 + 1 + 9(4c) \\ &= 3k + 1 + 9(k - 1 + 4c) \\ &\equiv_9 3k + 1 \end{aligned}$$

The following rules would simplify the above proof.

Theorem 4.34. *If $a \equiv_m b$ and $c \equiv_m d$, then*

i) $a + c \equiv_m b + d$

ii) $a - c \equiv_m b - d$

iii) $ac \equiv bd$

Proof. We do only ii). The other proofs are similar. As $a \equiv_m b$ and $c \equiv_m d$, we have by definition that $m \mid a - b$ and $m \mid c - d$. So $m \mid (a - b) - (c - d) = (a - c) - (b - d)$. By definition we get ii). □

Cancelation doesn't for work in general in the integers modulo m, because for example $2(1) \equiv_6 2(4)$ but $1 \not\equiv_6 4$. But it does work sometimes.

Theorem 4.35. *If $ac \equiv_m bc$ and $\gcd(c, m) = 1$, then $a \equiv_m b$.*

Proof. If $ac \equiv_m bc$ then $m \mid ac - bc = c(a - b)$, so $m \mid c$ or $m \mid (a - b)$. If we also have that $\gcd(c, m) = 1$, then $m \nmid c$, and so $m \mid a - b$. That is $a \equiv_m b$. □

Problem 4.13. Show that 3 divide n if and only if 3 divides the sum of the digits of n.

Sol:

Let $n = d_r(10^r) + d_{r-1}(10^{r-1} + \ldots d_0$. Since $10 \equiv_3 1$ we have

$$\begin{aligned} n &= d_r(10^r) + d_{r-1}(10^{r-1} + \ldots d_0 \\ &\equiv_3 d_r(1^r) + d_{r-1}(1^{r-1}) + \ldots d_0 \\ &= d_r + d_{r-1} + \ldots d_0 \end{aligned}$$

Problem 4.14. Find the last digit of 7^{100}.

Sol:

$7^2 = 49 \equiv_{10} -1$, so $7^{100} \equiv_{10} -1^{50} = 1$.

Problem 4.15. Find $15(17) - 19 \mod 7$.