Solutions and Proofs: Elementary Introduction to Number Theory by Calvin Long

Winter 2022

Abstract

This document will contain answers to selected exercises and important proofs from the book, "Elementary Introduction to Number Theory" by Calvin Long. I think this is a very good book for beginners who want to learn Number Theory. The prerequisites are minimal, it is my opinion that decent knowledge of high-school mathematics and a lot of patience are more than enough. For the more interested kind, I recommend complementing the book with the Theory of Numbers YouTube lecture series by 1998 Fields Medallist Richard E. Borcherds.

Exercises that I found difficult will be on the document, so do not expect this to be a full fledged solution manual. The book itself offers solutions to select questions in the end and the reader should look at those. Proofs on the other hand, are mostly included here, as they are very important to my understanding of the subject. Some ideas or methods might be inaccurate or plain wrong, please send corrections and feedback here.

I don't want to number all the sections as they appear in the book since that would look very confusing with the automatic numbering that LaTeXdoes for us. There aren't many problems per section, so finding the question from the title of the section should be straightforward. If there are better ways to do this, I would love to hear from you.

Disclaimer: This document is a work in progress, and progress will be slow.

Contents

1 Preliminary Considerations

1.1 Summation and Multiplication Notation

1. Evaluate $\sum_{i=1}^{n}(a_i - a_{i-1})$ given that $a_0 = 0$.

Let S_n be the value of the sum for $n \in \mathbb{N}$. We can easily see that $S_1 = a_1$. Now, we will write the following sum values and add them up.

$$S_1 = a_1 - a_0$$

$$S_2 = a_2 - a_1$$
$$S_3 = a_3 - a_2$$
$$\ddots$$
$$S_n = a_n - a_{n-1}$$

Adding all the equations gives $S_n = a_n$.

2. Use the result of exercise 1 to prove that $\sum_{i=1}^{n} i = n(n+1)/2$.

Let $a_k = k(k+1)/2$, we need to somehow obtain the LHS of the required equation and our problem is solved.

$$a_k - a_{k-1} = \frac{k(k+1)}{2} - \frac{(k-1)k}{2} = k.$$

This shows us that $\sum_{i=1}^{n}(a_i - a_{i-1}) = \sum_{i=1}^{n} i = a_n = n(n+1)/2$. By using the result from exercise 1.

3. Use the result of exercise 1 to prove that $\sum_{i=1}^{n} i(i+1) = n(n+1)(n+2)/3$.

In a similar manner to how we solved the second question, we say that $a_k = k(k+1)(k+2)/3$, and get the LHS that we need.

$$a_k - a_{k-1} = \frac{k(k+1)(k+2)}{3} - \frac{(k-1)k(k+1)}{3} = k(k+1).$$

This shows us that $\sum_{i=1}^{n}(a_i - a_{i-1}) = \sum_{i=1}^{n} i(i+1) = a_n = n(n+1)(n+2)/3$. By using the result from exercise 1.

1.2 Mathematical Induction

1. Discover a formula for the following sum and prove that it is correct for every positive integer n: $\sum\limits_{i=1}^{n}(-1)^{i-1}f_i$

Definition 1 (Fibonacci Sequence)**.** The *Fibonacci Sequence*, named after Leonardo of Pisa (1170?-1250?) who was nicknamed Fibonacci, is defined by the equations $f_1 = 1, f_2 = 1$, and $f_n = f_{n-1} + f_{n-2}$ for $n \geq 3$.

To solve this problem of finding a formula, we will look for a pattern that we can deduce, for a value of n, the sum is denoted by S_n:

n	1	2	3	4	5	6	7	8
S_n	1	0	2	-1	4	-4	9	-12

The pattern that stood out to me was $S_n = (-1)^{n-1}f_{n-1} + 1$, obviously, we need to define $f_0 = 0$ for this to work. Now we have to prove the formula using induction. For $n = 1, S_n = 1$ using both the sum and the formula. Let us assume the formula is correct for some $n = k$. Then the value if the sum for $k+1$ can be expressed as:

$$\begin{aligned} S_{k+1} &= \left[(-1)^{k-1}f_{k-1} + 1\right] + (-1)^k f_{k+1} \\ &= (-1)^k\left[f_{k+1} - f_{k-1}\right] + 1 \\ &= (-1)^k\left[f_k + \cancelto{0}{f_{k-1} - f_{k-1}}\right] + 1 \end{aligned}$$

$$\implies S_{k+1} = (-1)^k f_k + 1$$

■

2. Use I$_2$ to prove that $\alpha^{n-2} \leq f_n \leq \alpha^{n-1}$ for every positive integer n

Definition 2 (Second form of the principle of mathematical induction)**.** Any set of positive integers which contains the integer 1 and which contains $k+1$ whenever it contains the positive integers $1, 2, \ldots, k$, contains all positive integers.

Definition 3 (α and β)**.** Let $\alpha = (1+\sqrt{5})/2$ and $\beta = (1-\sqrt{5})/2$, so that α and β are the roots of $x^2 = x+1$.

For $n = 1$, we have $\alpha^{-1} \leq f_1 \leq \alpha^0$, and for $n = 2$, we have $\alpha^0 \leq f_2 \leq \alpha^1$. Both hold true, we now assume that the inequality holds for all $n = 2$ to k. To prove the inequality for $n = k+1$, we will state the inequality for the last two cases and add them up.

$$\begin{aligned} \alpha^{k-3} &\leq f_{k-1} \leq \alpha^{k-2} \\ \alpha^{k-2} &\leq f_k \quad \leq \alpha^{k-1} \end{aligned}$$

On adding up the equations, we get this rather convenient form of inequality:

$$\alpha^{k-3} + \alpha^{k-2} \leq f_k + f_{k-1} \leq \alpha^{k-1} + \alpha^{k-2}$$

The answer should be obvious by now, if not, the reader is required to work out the result $1 + \alpha = \alpha^2$ and then try again.

$$\alpha^{k-1} \leq f_{k+1} \leq \alpha^{k+1}$$

■

1.3 The Division Algorithm

Theorem 1. For all $a, b \in \mathbb{Z}$, with $b > 0$, there exists unique $q, r \in \mathbb{Z}$ such that $a = bq + r$ with $0 \leq r < b$

Proof. Basically, q is the quotient and r is the remainder. Consider the set $S = \{a - bx | x \in \mathbb{Z}, a - bx \geq 0\}$. For this set, we will first choose a, b and vary x to get elements of the set. In general, to find the smallest element r in S, we have to argue that the set S is not empty.

Claim: $S \neq \phi$
Case 1: $a \geq 0$, we set $x = 0$, so that we get $a - b(0) = a \in S$. The set is not empty
Case 2: $a < 0$, we will set $x = a$, so that $a - ba = a(1 - b) \geq 0$. The set is not empty

Let r be the minimum value of S and q be the corresponding quotient for this value of r. We have $r = a - bq$. Towards the contradiction, assume that $r \geq b$:
$r = a - bq \geq b$
$r - b = a - b(q + 1) \geq b - b \geq 0$

This means that $r - b \in S$ because $r - b = a - b(q')$ where $q' = q + 1$. But on the other hand, $r - b < r$ which contradicts our assumption that r is the minimum value of S. This implies that $0 \leq r < b$

Now, all that is left is to prove the uniqueness of q and r. Suppose that q, q', r, r' are such that $a = bq + r = bq' + r'$. Assume $r' \geq r$ (this assumption can work either ways). We have $b(q - q') = r' - r$. The LHS is a multiple of b and the RHS follows the inequality $o \leq r' - r < b$. The only way both can be true is if LHS=RHS=0. This implies that $q = q'$ and $r = r'$. ■

2 Divisibility Properties of Integers

2.1 Basic Properties

1. If $m\big|(35n+26), m\big|(7n+3)$, and $m>1$, prove that $m=11$.

From the question, we can write that $m\alpha = 35n+26$ and $m\beta = 7n+3$ for some $\alpha, \beta \in \mathbb{Z}$. If we multiply the second equation with 5 and subtract it from the first equation, we get

$$m(\alpha - 5\beta) = 11.$$

11 is a prime which means that the only divisors are 1 and itself. Since $m>1$, we can conclude that $m=11$.

■

2.2 The Euclidean Algorithm

Theorem 2. Suppose $a, b \in \mathbb{N}$, if we repeatedly perform the division algorithm:

$$a = bq_1 + r_1$$

$$b = r_1 q_2 + r_2$$

$$\dots$$

$$r_{n-2} = r_{n-1}q_n + 0;$$

then $r_{n-1} = gcd(a,b)$.

Proof. There are three steps to this proof:

- We need to show that this algorithm halts:
The set $\{r_1, r_2, \dots, r_{n-2}, r_{n-1}\} \in \mathbb{N}$ and is strictly decreasing, this means that the set will truncate somewhere.

- Show that the algorithm halts with a common divisor
We know $r_{n-1}\big|r_{n-2}$, this implies that $r_{n-1}\big|r_{n-3}$ and so on. All the dominoes fall from this. Finally, $r_{n-1}\big|b$ and $r_{n-1}\big|a$.

- Show that r_{n-1} is the GCD
Suppose there is a d such that $d\big|a$ and $d\big|b$, we just have to prove that $d\big|r_{n-1}$ for r_{n-1} to be the GCD.
From the first equation, $d\big|a - bq \implies d\big|r_1 \implies d\big|r-2 \implies \cdots \implies d\big|r_{n-1}$. ■

Theorem 3. $(a,b)=1$ if and only if there exist integers x and y such that $1 = ax+by$.

1. If $(a,c)=1$, prove that $(a,bc)=(a,b)$.

Let $(a,bc)=d_1$ and $(a,b)=d_2$, we need to show that $d_1 = d_2$. The way we will do it is by proving that $d_2\big|d_1$ and $d_1\big|d_2$. Proving the former is easier, because we already know that $d_2\big|a$ and $d_2\big|b$. This implies that $d_2\big|bc$ which makes it a common divisor for both a and bc. Thus, we have $d_2\big|d_1$.

Similarly for the second part, we just have to prove that $d_1\big|b$ because we anyway know that $d_1\big|a$. We can then use the common divisor rule and conclude that $d_1\big|d_2$. We are given that $(a,c)=1$, from that, we can write the following:

$$ax + cy = 1,$$

$$abx + bcy = b.$$

Since $d_1 \big| a$ and $d_1 \big| bc$, we can also write $d_1 \big| abx$ and $d_1 \big| bcy$.

$$\implies d_1 \big| (abx + bcy),$$

$$\implies d_1 \big| b.$$

As d_1 is a common divisor to both a and b, it also divides d_2. Thus, $d_1 = d_2$.

■

2. If $(a, b) = 1$, prove that $(a + b, a - b) = 1$ or 2

We have $(a, b) = 1$ and $(a + b, a - b) = d$. This means that d divides both $(a + b)$ and $(a - b)$. The implication is that $a + b = rd$ and $a - b = sd$ for some $r, s \in \mathbb{Z}$. Adding up the equations, we get $2a = (r + s)d$ and $2b = (r - s)d$. Thus, $d \big| 2a$ and $d \big| 2b$.

From the question, we know that the GCD of a and b is 1. If there is a d that divides $2a$ and $2b$, it has to be either 1 or 2.

■

3. If $d \big| mn$ and $(m, n) = 1$, prove that $d = d_1 d_2$ where $d_1 \big| m, d_2 \big| n$, and $(d_1, d_2) = 1$.

Let $d_1 = (d, m)$, we then automatically have $d_1 \big| m$ and $d_2 = d/d_1 \implies d_1 d_2 = d$. All that we have to prove now is $d_2 \big| n$. Because $m = Md_1$ and $d = d_2 d_1$, we can write $(M, d_2) = 1$ using Theorem 1. From hypothesis, $d \big| mn$:

$$\begin{aligned} &\implies dq = mn, \\ &\implies d_1 d_2 q = M d_1 n \\ &\implies d_2 \big| Mn \\ &\implies d_2 \big| n \qquad \because (M, d_2) = 1 \end{aligned}$$

■

4. If $(a, b) = (c, d) = 1, b > 0, d > 0$, and $\frac{a}{b} + \frac{c}{d}$ is an integer, prove that $b = d$.

Both the fractions are in reduced form and if we assume that the sum is equal to n, we can write:

$$\frac{a}{b} + \frac{c}{d} = n \implies \frac{a}{b} = \frac{dn - c}{d}.$$

Because both are in reduced form, they are unique, and hence $b = d$. If there was a p that divided d and $dn - c$, it would also have to divide c which contradicts the hypothesis $(c, d) = 1$.

■