Solutions to Elementary Number Theory (Second Edition) by David M. Burton

Samy Lahlou

November 16, 2025

Preface

The goal of this document is to share my personal solutions to the exercises in the Second Edition of Elementary Number Theory by David M. Burton during my reading. To make my solutions clear, for each exercise, I will assume nothing more than the content of the book and the results proved in the preceding exercises. Moreover, it should be noted that a lot of the exercises can be done very easily using a calculator or using a computer program. It is for this reason that I chose to do every exercise with **no calculator and without writing any computer program**. I took this decision because I believe that I will learn more in this way.

As a disclaimer, the solutions are not unique and there will probably be better or more optimized solutions than mine. Feel free to correct me or ask me anything about the content of this document at the following address:

samy.lahloukamal@mail.mcgill.ca

Contents

Chapter 1

Euler's Generalization of Fermat's Theorem

1.1 Leonhard Euler

There are no exercices in this section.

1.2 Euler's Phi-Function

1. Calculate $\phi(1001)$, $\phi(5040)$, and $\phi(36,000)$.

Solution Since $1001 = 7 \cdot 11 \cdot 13$, then

$$\phi(1001) = \phi(7)\phi(11)\phi(13) = 6 \cdot 10 \cdot 12 = 720.$$

Since $5040 = 2^4 \cdot 3^2 \cdot 5 \cdot 7$, then

$$\phi(5040) = 2^3(2-1) \cdot 3(3-1) \cdot (5-1) \cdot (7-1) = 1152.$$

Since $36,000 = 2^5 \cdot 3^2 \cdot 5^3$, then

$$\phi(36,000) = 2^4(2-1) \cdot 3(3-1) \cdot 5^2(5-1) = 9600.$$

2. Verify that the equality $\phi(n) = \phi(n+1) = \phi(n+2)$ holds when $n = 5186$.

Solution When $n = 5186$, we have $n = 2 \cdot 2593$, $n+1 = 3 \cdot 7 \cdot 13 \cdot 19$, and $n+2 = 2^2 \cdot 1297$. Hence:

$$\begin{aligned} \phi(n) &= (2-1)(2593-1) = 2592 \\ \phi(n+1) &= (3-1)(7-1)(13-1)(19-1) = 2592 \\ \phi(n+2) &= 2(2-1)(1297-1) = 2592. \end{aligned}$$

3. Show that the integers $m = 3^k \cdot 568$ and $n = 3^k \cdot 638$, where $k \geq 0$, satisfy simultaneously

$$\tau(m) = \tau(n),\ \sigma(m) = \sigma(n),\ \phi(m) = \phi(n).$$

Solution Since $m = 2^3 \cdot 3^k \cdot 71$ and $n = 2 \cdot 3^k \cdot 11 \cdot 29$, then

$$\tau(m) = (3+1)(k+1)(1+1) = (1+1)(k+1)(1+1)(1+1) = \tau(n)$$
$$\sigma(m) = (1+2+2^2+2^3)\sigma(3^k)(1+71) = 1080\sigma(3^k) = (1+2)\sigma(3^k)(1+11)(1+29) = \sigma(n)$$
$$\phi(m) = 2^2(2-1)\phi(3^k)(71-1) = 280\phi(3^k) = (2-1)\phi(3^k)(11-1)(29-1) = \sigma(n)$$

which proves the claim.

4. Establish each of the assertions below:

(a) If n is an odd integer, then $\phi(2n) = \phi(n)$.

(b) If n is an even integer, then $\phi(2n) = 2\phi(n)$.

(c) $\phi(3n) = 3\phi(n)$ if and only if $3 \mid n$.

(d) $\phi(3n) = 2\phi(n)$ if and only if $3 \nmid n$.

(e) $\phi(n) = n/2$ if and only if $n = 2^k$ for some $k \geq 1$. [*Hint:* Write $n = 2^k N$, where N is odd, and use the condition $\phi(n) = n/2$ to show that $N = 1$.]

Solution

(a) If n is odd, then $\gcd(2, n) = 1$, and so it follows that $\phi(2n) = \phi(2)\phi(n) = \phi(n)$.

(b) If n is even, then we can write $n = 2^k m$ where $k \geq 1$ and m such that $\gcd(2, m) = 1$. Hence, by multiplicativity:

$$\phi(2n) = \phi(2^{k+1}m) = \phi(2^{k+1})\phi(m) = 2^k\phi(m) = 2\phi(2^k)\phi(m) = 2\phi(n).$$

(c) Write $n = 3^k m$ where $\gcd(3, m) = 1$. If $3 \mid n$, then $k \geq 1$ which implies that $3^k(3-1) = 3 \cdot 3^{k-1}(3-1)$, and hence, that $\phi(3^{k+1})\phi(m) = 3\phi(3^k)\phi(m)$. Equivalently, this means that $\phi(3n) = 3\phi(n)$. Conversely, if $3 \nmid n$, then $k = 0$, and hence, $\phi(3n) = \phi(3)\phi(n) = 2\phi(n) \neq 3\phi(n)$.

(d) We showed in the previous part that $3 \nmid n$ implies that $\phi(3n) = 2\phi(n)$. Conversely, when $3 \mid n$, we know that $\phi(3n) = 3\phi(n)$, and hence, $\phi(3n) \neq 2\phi(n)$.

(e) If $n = 2^k$ for some $k \geq 1$, then

$$\phi(n) = \phi(2^k) = 2^{k-1} = n/2.$$

Conversely, suppose that $\phi(n) = n/2$ and write $n = p_1^{k_1} \cdots p_r^{k_r}$, then we can rewrite the equation as

$$n\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_r}\right) = \frac{n}{2}.$$

Rearranging the equation gives us

$$2(p_1 - 1) \cdots (p_r - 1) = p_1 \cdots p_r.$$

Since the left hand side is even, then one of the primes in the right hand side must be 2, and hence, $p_1 = 2$. The equation becomes

$$(p_2 - 1) \cdots (p_r - 1) = p_2 \cdots p_r.$$

But this equation is impossible (the left hand side is clearly strictly less than the right hand side) when $r \geq 2$, if $r = 1$, this equation is simply $1 = 1$. Hence, $r = 1$, and hence, $n = p_1^{k_1} = 2^{k_1}$ for some $k_1 \geq 1$.

5. Prove that the equation $\phi(n) = \phi(n + 2)$ is satisfied by $n = 2(2p - 1)$ whenever p and $2p - 1$ are both odd primes.

Solution Simply notice that

$$\phi(n) = \phi(2)\phi(2p - 1) = 2p - 2$$

and

$$\phi(n + 2) = \phi(4p) = \phi(4)\phi(p) = 2(p - 1).$$

Hence, it follows that $\phi(n) = \phi(n + 2)$.

6. Show that there are infinitely many integers n for which $\phi(n)$ is a perfect square. [*Hint:* Consider the integers $n = 2^{k+1}$ for $k = 1, 2, \ldots$.]

Solution Let k be an arbitrary integer and $n = 2^{2k+1}$, then $\phi(n) = 2^{2k} = (2^k)^2$. Since $(2^k)^2 \neq (2^q)^2$ for $k \neq q$, then there are infinitely many n such that $\phi(n)$ is a square since there are infinitely many k's.

7. Verify the following:

(a) For any positive integer n, $\frac{1}{2}\sqrt{n} \leq \phi(n) \leq n$. [*Hint:* Write $n = 2^{k_0} p_1^{k_1} \cdots p_r^{k_r}$, so $\phi(n) = 2^{k_0 - 1} p_1^{k_1 - 1} \cdots p_r^{k_r - 1}(p_1 - 1) \cdots (p_r - 1)$. Now, use the inequalities $p - 1 > \sqrt{p}$ and $k - \frac{1}{2} \geq k/2$ to obtain $\phi(n) \geq 2^{k_0 - 1} p_1^{k_1/2} \cdots p_r^{k_r/2}$.]

(b) If the integer $n > 1$ has r distinct prime factors, then $\phi(n) \geq n/2^r$.

(c) If $n > 1$ is a composite number, then $\phi(n) \leq n - \sqrt{n}$. [*Hint:* Let p be the smallest prime divisor of n, so that $p \leq \sqrt{n}$. Then $\phi(n) \leq n(1 - 1/p)$.]

Solution

(a) Let $n = 2^{k_0} p_1^{k_1} \cdots p_r^{k_r}$, then $\phi(n) = 2^{k_0 - 1} p_1^{k_1 - 1} \cdots p_r^{k_r - 1}(p_1 - 1) \cdots (p_r - 1)$. Since $(p_i - 1) \geq \sqrt{p_i}$, then we get that $\phi(n) \geq \frac{1}{2} \cdot 2^{k_0} p_1^{k_1 - \frac{1}{2}} \cdots p_r^{k_r - \frac{1}{2}}$. Next, since $k_0 \geq k_0/2$ and $k_i - \frac{1}{2} \geq k_i/2$, then $\phi(n) \geq \frac{1}{2} 2^{k_0/2} p_1^{k_1/2} \cdots p_r^{k_r} = \frac{1}{2}\sqrt{n}$. Finally, the inequality $\phi(n) \leq n$ follows from the definition of ϕ.

(b) Let $n = p_1^{k_1} \cdots p_r^{k_r}$, then

$$\frac{n}{\phi(n)} = \frac{n}{n\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_r}\right)} = \frac{p_1}{p_1 - 1} \cdots \frac{p_r}{p_r - 1} \leq 2^r$$

which we can rearrange into $\phi(n) \geq n/2^r$.

(c) Let p be a prime dividing n, since n is composite, then $p \leq \sqrt{n}$, hence, $p\sqrt{n} \leq n$. It follows that the numbers p, $2p$, ..., $\lfloor\sqrt{n}\rfloor p$ are all less than n, and not relatively prime to n. There are $\lfloor\sqrt{n}\rfloor$ such numbers. If we let q be a second prime divisor of n (if n is a power of p, then the statement is clear from the formula for $\phi(p^k)$ and the inequality $k - 1 \geq k/2$ for $k \geq 2$), then we know that q is a number distinct from p, $2p$, ..., $\lfloor\sqrt{n}\rfloor$ that is not relatively prime to n. Hence, we have found $\lfloor\sqrt{n}\rfloor + 1$ numbers less than n which are not relatively prime to it. Therefore, $\phi(n) \leq n - (\lfloor\sqrt{n}\rfloor + 1) \leq n - \sqrt{n}$.

8. Prove that if the integer n has r distinct odd prime factors, then $2^r \mid \phi(n)$.

Solution Write $n = 2^{k_0} p_1^{k_1} \cdots p_r^{k_r}$ where $k_0 \geq 0$ and $k_i \geq 1$ for $1 \leq i \leq r$, then

$$\phi(n) = \phi(2^{k_0}) p_1^{k_1 - 1} \cdots p_r^{k_r - 1}(p_1 - 1) \cdots (p_r - 1).$$

Since all the factors $p_i - 1$ are even, and there are r such factors, then 2^r divides $\phi(n)$.

9. Prove that:

(a) If n and $n + 2$ are a pair of twin primes, then $\phi(n + 2) = \phi(n) + 2$; this also holds for $n = 12$, 14, and 20.

(b) If p and $2p + 1$ are both odd primes, then $n = 4p$ satisfies $\phi(n + 2) = \phi(n) + 2$.

Solution

(a) For any prime p, we have that $\phi(p) = p - 1$. It follows that

$$\phi(n + 2) = n + 1 = (n - 1) + 2 = \phi(n) + 2$$

when both n and $n + 2$ are prime. When $n = 12$:

$$\phi(n + 2) = \phi(2)\phi(7) = 6 = \phi(2^2)\phi(3) + 1 = \phi(n) + 2.$$

When $n = 14$:

$$\phi(n + 2) = \phi(2^4) = 8 = \phi(2)\phi(7) + 2 = \phi(n) + 2.$$

When $n = 20$:

$$\phi(n + 2) = \phi(2)\phi(11) = 10 = \phi(2^2)\phi(5) + 2 = \phi(n) + 2.$$

(b) Suppose that p and $2p+1$ are odd primes, then for $n = 4p$, we have

$$\phi(n+2) = \phi(4p+2) = \phi(2)\phi(2p+1) = 2p$$

and

$$\phi(n) + 2 = \phi(4p) + 2 = \phi(4)\phi(p) + 2 = 2(p-1) + 2 = 2p$$

which proves that $\phi(n+2) = \phi(n) + 1$.

10. If every prime that divides n also divides m, establish that $\phi(nm) = n\phi(m)$; in particular, $\phi(n^2) = n\phi(n)$ for every positive integer n.

Solution Write $n = p_1^{k_1} \cdots p_r^{k_r}$ and $m = p_1^{t_1} \cdots p_r^{t_r} q_1^{s_1} \cdots q_u^{s_u}$, then

$$\begin{aligned}
\phi(nm) &= \phi(p_1^{k_1+t_1} \cdots p_r^{k_r+t_r} q_1^{s_1} \cdots q_u^{s_u}) \\
&= p_1^{k_1+t_1-1}(p_1-1) \cdots p_r^{k_r+t_r-1}(p_r-1)\phi(q_1^{s_1} \cdots q_u^{s_u}) \\
&= [p_1^{k_1} \cdots p_r^{k_r}] \cdot p_1^{t_1-1}(p_1-1) \cdots p_r^{t_r-1}(p_r-1)\phi(q_1^{s_1} \cdots q_u^{s_u}) \\
&= n\phi(p_1^{t_1} \cdots p_r^{t_r})\phi(q_1^{s_1} \cdots q_u^{s_u}) \\
&= n\phi(m).
\end{aligned}$$

11.

(a) If $\phi(n) \mid n-1$, prove that n is a square-free integer. [*Hint:* Assume that n has the prime factorization $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$, where $k_1 \geq 2$. Then $p_1 \mid \phi(n)$, whence $p_1 \mid n-1$, which leads to a contradiction.]

(b) Show that if $n = 2^k$ or $n = 2^k 3^j$, with k and j positive integers, then $\phi(n) \mid n$.

Solution

(a) Let p be a prime divisor of n and let k be the exponent of p in the prime factorization of n, then $\phi(n) = \phi(p^k)\phi(n/p^k) = p^{k-1}(p-1)\phi(n/p^k)$. When $k \geq 2$, we have that $p \mid \phi(n)$ using the expression above, but since $\phi(n) \mid n-1$, then $p \mid n-1$. This is impossible because $p \mid n$. Thus, $k = 1$, and hence, n is square-free.

(b) Let $n = 2^k 3^k$ with $k \geq 1$. If $j = 0$, then $\phi(n) = 2^{k-1} \mid 2^k = n$. When $j \geq 1$, we get $\phi(n) = 2^{k-1}3^{j-1}(3-1) = 2^k 3^{j-1} \mid 2^k 3^j = n$.

12. If $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$, derive the inequalities

(a) $\sigma(n)\phi(n) \geq n^2(1-1/p_1^2)(1-1/p_2^2) \cdots (1-1/p_r^2)$ and

(b) $\tau(n)\phi(n) \geq n$. [*Hint:* Show that $\tau(n)\phi(n) \geq 2^r \cdot n(1/2)^r$.]

Solution

(a) First, notice that

$$\begin{aligned}\sigma(n) &= (1 + \cdots + p_1^{k_1-1} + p_1^{k_1}) \cdots (1 + \cdots + p_r^{k_r-1} + p_r^{k_r}) \\ &\geq (p_1^{k_1} + p_1^{k_1-1}) \cdots (p_r^{k_r} + p_r^{k_r-1}) \\ &= p_1^{k_1} \cdots p_r^{k_r}(1 + 1/p_1) \cdots (1 + 1/p_r) \\ &= n(1 + 1/p_1) \cdots (1 + 1/p_r).\end{aligned}$$

Multiplying the resulting inequality by

$$\phi(n) = n(1 - 1/p_1) \cdots (1 - 1/p_r)$$

gives us

$$\sigma(n)\tau(n) \geq n^2(1 - 1/p_1^2) \cdots (1 - 1/p_r^2).$$

(b) Since

$$\begin{aligned}\tau(n) &= (k_1 + 1)(k_2 + 1) \cdots (k_r + 1) \\ &\geq \left(1 - \frac{1}{p_1}\right)^{-1} \left(1 - \frac{1}{p_2}\right)^{-1} \cdots \left(1 - \frac{1}{p_r}\right)^{-1} \\ &= \frac{n}{\phi(n)},\end{aligned}$$

then $\tau(n)\phi(n) \geq n$.

13. Assuming that $d \mid n$, prove that $\phi(d) \mid \phi(n)$. [*Hint:* Work with the prime factorizations of d and n.]

Solution Let $d = p_1^{k_1} \cdots p_r^{k_r}$ and $n = p_1^{t_1} \cdots p_r^{t_r} q_1^{s_1} \cdots q_u^{s_u}$ with $k_i \leq t_i$, then $p_i^{k_i-1} \mid p_i^{t_i-1}$. It follows that $\prod_{i=1}^r p_i^{k_i-1} \mid \prod_{i=1}^r p_i^{t_i-1}$. Using the rules of divisibility, we get that $\phi(d)$, which is equal to $\prod_{i=1}^r p_i^{k_i-1}(p_i - 1)$ divides $\prod_{i=1}^r p_i^{t_i-1}(p_i - 1)$, which in turns divides $\prod_{i=1}^r p_i^{t_i-1}(p_i - 1) \prod_{i=1}^u q_i^{s_i-1}(q_i - 1) = \phi(n)$. Therefore, $\phi(d) \mid \phi(n)$.

14. Obtain the following two generalizations of Theorem 7-2:

(a) For positive integers m and n,

$$\phi(m)\phi(n) = \phi(mn)\phi(d)/d,$$

where $d = \gcd(m, n)$.

(b) For positive integers m and n,

$$\phi(m)\phi(n) = \phi(\gcd(m, n))\phi(\text{lcm}(m, n)).$$

Solution

(a) Let $m = p_1^{k_1} \cdots p_r^{k_r} a$ and $n = p_1^{t_1} \cdots p_r^{t_r} b$ where the p_i's are the prime common to m and n, and where a and b are prime relative to the p_i's, then $d = \gcd(m, n)$ is also formed of the primes p_1, ..., p_r. It follows that

$$\begin{aligned}
\phi(mn)\frac{\phi(d)}{d} &= \phi\left(ab\prod_i p_i^{k_i+t_i}\right)\prod_i\left(1-\frac{1}{p_i}\right) \\
&= \phi(a)\phi(b)\prod_i p_i^{k_i+t_i-1}(p_i-1)\prod_i\frac{p_i-1}{p_i} \\
&= \left[\phi(a)\prod_i p_i^{k_i-1}(p_i-1)\right]\left[\phi(b)\prod_i p_i^{t_i-1}(p_i-1)\right] \\
&= \phi(m)\phi(n).
\end{aligned}$$

(b) First, recall that $mn = \gcd(m, n)\,\mathrm{lcm}(m, n)$. Moreover, since $\gcd(m, n) \mid mn$, then

$$\phi(mn) = \gcd(m, n)\phi\left(\frac{mn}{\gcd(m, n)}\right) = \gcd(m, n)\phi(\mathrm{lcm}(m, n))$$

by Problem 10. Therefore, using part (a):

$$\phi(m)\phi(n) = \phi(mn)\frac{\phi(\gcd(m, n))}{\gcd(m, n)} = \phi(\gcd(m, n))\phi(\mathrm{lcm}(m, n)).$$

15. Prove that:

(a) There are infinitely many integers n for which $\phi(n) = n/3$. [*Hint:* Consider $n = 2^k 3^j$, where k and j are positive integers.]

(b) There are no integers n for which $\phi(n) = n/4$.

Solution

(a) **TODO**

(b) **TODO**

1.3 Euler's Theorem

TODO

1.4 Some Properties of the Phi-Function

TODO

1.5 An Application to Cryptography

TODO