Analytic Number Theory Solutions

Sean Li
Cornell University
sxl6@cornell.edu

Jan. 2013

Introduction

This document is a work-in-progress solution manual for Tom Apostol’s Introduction to Analytic Number Theory. The solutions were worked out primarily for my learning of the subject, as Cornell University currently does not offer an analytic number theory course at either the undergraduate or graduate level. However, this document is public and available for use by anyone. If you are a student using this document for a course, I recommend that you first try work out the problems by yourself or in a group. My math documents are stored on a math blog at www.epicmath.org.

1 The Fundamental Theorem of Arithmetic

1.1. If \((a, b) = 1\) and if \(c|a\) and \(d|b\), then \((c, d) = 1\).

Proof. Suppose \((c, d) = m \neq 1\), so that \(m|c\) and \(m|d\). Since \(c|a\) and \(d|b\), this implies \(m|a\) and \(m|b\), contradicting that \((a, b) = 1\).

1.2. If \((a, b) = (a, c) = 1\), then \((a, bc) = 1\).

Proof. Suppose \((a, bc) = m \neq 1\). Let \(p\) be any prime factor of \(m\). Then \(p|bc\) implies \(p|b\) or \(p|c\), assume by symmetry that \(p|b\). Then \((a, b) = p\).

1.3. If \((a, b) = 1\), then \((a^n, b^k) = 1\) for all \(n \geq 1, k \geq 1\).

Proof. Let \(p_1^{a_1} \cdots p_i^{a_i}\) and \(q_1^{b_1} \cdots q_m^{b_m}\) be the prime factorizations of \(a\) and \(b\)
respectively. Since \((a, b) = 1\), the \(p_i\) are disjoint from the \(q_i\). Since 
\[ a^n = p_1^{\alpha_1 n} \cdots p_l^{\alpha_{ln}} \]
and 
\[ b^k = q_1^{\beta_1 k} \cdots q_m^{\beta_{mk}} , \]
it is clear that the prime factorizations of \(a^n\) and \(b^k\) are disjoint. Hence \((a^n, b^k) = 1\).

1.4. If \((a, b) = 1\), then \((a + b, a - b)\) is either 1 or 2.

Proof. Write \(ax + by = 1\). Note that \(2ax + 2by = 2\), so
\[ 2ax + 2by + bx - bx = (a + b)x + 2by + (a - b)x = 2 \]
and 
\[ 2ax + 2by + ay - ay = (a + b)y + 2ax + (b - a)y = 2 . \]
Adding the two gives \((a + b)(x + y) + 2(ax + by) + (a - b)(x - y) = 4\), but
\[ 2(ax + by) = 2, \]
so that \((a + b)(x + y) + (a - b)(x - y) = 2\).
This implies \((a + b, a - b)|2\), so \((a + b, a - b)\) equals 1 or 2.

1.5. If \((a, b) = 1\), then \((a + b, a^2 - ab + b^2)\) is either 1 or 3.

Proof. Let \(d = (a + b, a^2 - ab + b^2)\). Note that \(a^2 - ab + b^2 = (a + b)^2 - 3ab\), and \(d|(a + b)\) implies \(d|(a + b)^2\). Hence \(d|(-3ab)\). But \((a, b) = 1\) implies \(d \nmid ab\), thus \(d|3\).

1.6. If \((a, b) = 1\) and if \(d|(a + b)\), then \((a, d) = (b, d) = 1\).

Proof. Suppose \((a, d) = m \neq 1\). Then \(a = sm\) and \(d = tm\), where \(s\) and \(t\) are integers. Then the condition that \(d|(a + b)\) implies \((tm)|(sm + b)\), so that \(m|b\). But then \(m|(a, b)\), contradicting \((a, b) = 1\). A symmetric argument works to show \((b, d) = 1\).

1.7. A rational number \(a/b\) with \((a, b) = 1\) is called a reduced fraction. If the sum of two reduced fractions is an integer, say \((a/b) + (c/d) = n\), prove that \(|b| = |d|\).

Proof. Note that \((a/b) + (c/d) = (ad + bc)/(bd)\). This is an integer implies \(bd|(ad + bc)\), which by linearity implies \(d|bc\) and \(b|ad\). However, since \((a, b) = (c, d) = 1\), this implies that \(d|b\) and \(b|d\). Hence \(|b| = |d|\).

1.8. An integer is called squarefree if it is not divisible by the square of any prime. Prove that for every \(n \geq 1\) there exist uniquely determined \(a > 0\) and \(b > 0\) such that \(n = a^2b\), where \(b\) is squarefree.
Proof. Let \( p_1^{\alpha_1} \cdots p_k^{\alpha_k} \) be the prime factorization of \( n \). Let \( a = p_1^{\lceil \alpha_i/2 \rceil} \cdots p_k^{\lceil \alpha_i/2 \rceil} \), where \( \lceil x \rceil \) denotes the largest integer less than or equal to \( x \). Then \( b = n/a^2 \) is the product of \( p_1, \ldots, p_k \) to either power 0 or 1, and is hence squarefree. It is clear that given a prime factorization this is the only way to write \( n = a^2 b \) where \( b \) is squarefree (change any power of the prime factors and either \( b \) has a square divisor or \( n/b \) is not a square), and the prime factorization of \( n \) is unique, so that \( a \) and \( b \) are unique.

1.9. For each of the following statements, either give a proof or exhibit a counterexample.

(a) If \( b^2 | n \) and \( a^2 | n \) and \( a^2 \leq b^2 \), then \( a | b \).

False. Let \( n = 36, a = 2, \) and \( b = 3 \). Then \( 3^2 | 36, \) \( 2^2 | 36, \) and \( 2^2 \leq 3^2 \), but \( 2 \nmid 3 \).

(b) If \( b^2 \) is the largest square divisor of \( n \), then \( a^2 | n \) implies \( a | b \).

True. Let \( p_1^{\alpha_1} \cdots p_k^{\alpha_k} \) be the prime factorization of \( n \). Then \( b = p_1^{\lfloor \alpha_i/2 \rfloor} \cdots p_k^{\lfloor \alpha_i/2 \rfloor} \), and if \( a^2 | n \), then \( a = p_1^{\beta_1} \cdots p_k^{\beta_k} \) with each \( \beta_i \leq \lfloor \alpha_i/2 \rfloor \). Hence \( a | b \).

1.10. Given \( x \) and \( y \), let \( m = ax + by, n = cx + dy \), where \( ad - bc = \pm 1 \). Prove that \((m, n) = (x, y)\).

Proof. Let \( d = (m, n) \), so that \( d = sm + ty \) for some integers \( s \) and \( t \), and let \( d' = (x, y) \). Then \( d = s(ax + by) + t(cx + dy) = x(sa + tc) + y(sb + td) \). Thus \( d|d' \).

The linear transformation by \( \begin{bmatrix} a & b \\ c & d \end{bmatrix} \) is invertible in the integers since \( ad - bc = \pm 1 \), so that we may write \( x \) and \( y \) as linear combinations of \( m \) and \( n \), namely \( x = dm - bn \) and \( y = -cm + an \). There are \( p \) and \( q \) such that \( px + qy = d' \). Thus

\[
\begin{align*}
d' &= px + qy \\
&= p(dm - bn) + q(-cm + an) \\
&= m(pd - qc) + n(-pb + qa)
\end{align*}
\]

Thus \( d'|d \), and hence \((x, y) = (m, n)\).

1.11. Prove that \( n^4 + 4 \) is composite if \( n > 1 \).

Proof. Factor \( n^4 + 4 = (n^2 + 2n + 2)(n^2 - 2n + 2) \). For \( n > 1 \), both of these factors are greater than 1, hence \( n^4 + 4 \) is composite.
1.12.—1.14. In Exercises 12, 13, and 14, \( a, b, c, m, n \) denote positive integers.

1.12. For each of the following statements either give a proof or exhibit a counterexample.

(a) If \( a^n \mid b^n \) then \( a \mid b \).

True. Let \( a = \prod_{i>0} p_i^{\alpha_i} \) and \( b = \prod_{i>0} q_i^{\beta_i} \) be the unique prime factorizations. Suppose \( a \nmid b \), then \( \alpha_k > \beta_k \) for some \( k > 0 \). Then \( q_k^{\alpha_k n} \nmid q_k^{\beta_k n} \), contradicting that \( a^n \mid b^n \).

(b) If \( n^n \mid m^m \) then \( n \mid m \).

False. Consider \( n = 8, m = 12 \). Then \( 8^8 = 2^{24} \cdot 2^{12} = 12^{12} \), but \( 8 \nmid 12 \).

(c) If \( a^n \mid 2b^n \) and \( n > 1 \), then \( a \mid b \).

True. From part (a) we know that if \( a \nmid b \), then \( a^n \nmid b^n \). If \( n > 1 \), it follows that \( a^n \nmid 2b^n \). As in part (a), consider the prime factorizations \( a = \prod_{i>0} p_i^{\alpha_i} \) and \( b = \prod_{i>0} q_i^{\beta_i} \), so that \( \alpha_k > \beta_k \) for some \( k > 0 \). If \( p_k \neq 2 \), then the argument from part (a) works. If \( p_k = 2 \) (i.e. \( k = 1 \)), then note that \( n > 1 \) implies \( \alpha_k n > \beta_k n + 1 \), so that \( a^n \nmid 2b^n \), a contradiction.

1.13.

(a) If \( (a, b) = 1 \) and \( (a/b)^m = n \), prove that \( b = 1 \).

Proof. Let \( a = \prod p_i^{\alpha_i} \) and \( b = \prod q_i^{\beta_i} \) be prime factorizations. Then since \( (a, b) = 1 \), \( \alpha_i \neq 0 \) implies \( \beta_i = 0 \), and \( \beta_i \neq 0 \) implies \( \alpha_i = 0 \). Suppose any of the \( \beta_i \) were greater than 0, then \( q_i^{\beta_i m} \nmid a^m \), so that \( (a/b)^m \) is not an integer.

(b) If \( n \) is not the \( m \)th power of a positive integer, prove that \( n^{1/m} \) is irrational.

Suppose \( n^{1/m} \) is rational, let \( a/b \) be the reduced fraction, so that \( (a, b) = 1 \). By part (a), this implies \( b = 1 \), so \( n = a^m \), a contradiction.

1.14. If \( (a, b) = 1 \) and \( ab = c^n \), prove that \( a = x^n \) and \( b = y^n \) for some \( x \) and \( y \).

Proof. Similarly to the previous problem, let \( a = \prod p_i^{\alpha_i} \) and \( b = \prod q_i^{\beta_i} \) be prime factorizations. Then since \( (a, b) = 1 \), \( \alpha_i \neq 0 \) implies \( \beta_i = 0 \), and \( \beta_i \neq 0 \) implies \( \alpha_i = 0 \). Write the prime factorization of \( c^n \) as \( \prod p_i^{\gamma_i n} \). For each \( i \) such that \( \gamma_i > 0 \), we must have either \( \alpha_i = \gamma_i n \) and \( \beta_i = 0 \), or \( \beta_i > \gamma_i n \) and \( \alpha_i = 0 \). Thus \( a \) and \( b \) can be written as \( x^n \) and \( y^n \) respectively, where \( x = \prod_{\{i|\alpha_i > 0\}} \gamma_i \) and \( y = \prod_{\{i|\beta_i > 0\}} \gamma_i \).

1.15. Prove that every \( n \geq 12 \) is the sum of two composite numbers.
Proof. If \( n \) is even, then \( n = 4 + (n - 4) \), where \( n - 4 = 2m \) for some \( m > 1 \). And if \( n \) is odd, then \( n = 9 + (n - 9) \), where \( n - 9 = 2m \) for some \( m > 1 \).

1.16. Prove that if \( 2^n - 1 \) is prime, then \( n \) is prime.

Proof. Suppose by way of contradiction that \( n = ab \), where \( a, b > 1 \). Then \( 2^n - 1 = 2^{ab} - 1 = (2^a - 1)(2^{a(b-1)} + \cdots + 2^a + 1) \), contradicting that \( 2^n - 1 \) is prime.

1.17. Prove that if \( 2^n + 1 \) is prime, then \( n \) is a power of 2.

Proof. Let \( a = 2^k \) be the highest power of 2 that divides \( n \) and let \( b = n/a \). Note that \( b \) is odd. Suppose \( b > 1 \), then \( 2^n + 1 = 2^{ab} + 1 = (2^a + 1)(2^{a(b-1)} - 2^{a(b-2)} + \cdots - 2^a + 1) \), a contradiction.

1.18. If \( m \neq n \) compute the gcd \( (a^{2^m} + 1, a^{2^n} + 1) \) in terms of \( a \).

Proof. Let \( A_n \) denote \( a^{2^n} + 1 \), let \( A_m \) denote \( a^{2^m} + 1 \), and suppose that \( m > n \). Furthermore, note that \( 2^{m-n} \) is even. Then

\[
A_m - 2 = a^{2^m} - 1 \\
= a^{2^n} a^{m-n} - 1 \\
= (a^{2^n} + 1)(a^{2^n} (a^{m-n-1}) - a^{2^n} (a^{m-n-2}) + \cdots + a^{2^n} - 1)
\]

But \( a^{2^n} + 1 = A_n \), so that \( A_n | (A_m - 2) \).

Denote \( d = (A_n, A_m) \). Then we have \( d | A_m \) and \( d | (A_m - 2) \), so by linearity \( d | 2 \). Moreover, if \( a \) is even, then \( A_m \) and \( A_n \) are odd, so \( d = 1 \), and if \( a \) is odd, then \( A_m \) and \( A_n \) are even, so \( d = 2 \).

1.19. The Fibonacci sequence 1, 1, 2, 3, 5, 8, 13, 21, 34, \ldots is defined by the recursion formula \( a_{n+1} = a_n + a_{n-1} \) with \( a_1 = a_2 = 1 \). Prove that \( (a_n, a_{n+1}) = 1 \) for each \( n \).

Proof. By induction. Clearly \( (a_1, a_2) = 1 \). Now suppose \( (a_n, a_{n-1}) = 1 \). Then

\[
(a_{n+1}, a_n) = (a_n + a_{n-1}, a_n) = (a_{n-1}, a_n) = 1.
\]

1.20. Let \( d = (826, 1890) \). Use the Euclidean algorithm to compute \( d \), then express \( d \) as a linear combination of 826 and 1890.
Solution.

\[ 1890 = 2 \cdot 826 + 238 \]
\[ 826 = 3 \cdot 238 + 112 \]
\[ 238 = 2 \cdot 112 + 14 \]
\[ 112 = 8 \cdot 14 + 0 \]

So \( d = 14 = 7 \cdot 1890 − 16 \cdot 826 \).

1.21. The least common multiple (lcm) of two integers \( a \) and \( b \) is denoted by \([a, b]\) or by \( aMb \), and is defined as follows:

\[ [a, b] = \frac{|ab|}{(a, b)} \quad \text{if } a \neq 0 \text{ and } b \neq 0, \]
\[ [a, b] = 0 \quad \text{if } a = 0 \text{ or } b = 0. \]

Prove that the lcm has the following properties:

(a) If \( a = \prod p_i^{a_i} \) and \( b = \prod p_i^{b_i} \) then \([a, b] = \prod p_i^{c_i} \), where \( c_i = \max\{a_i, b_i\} \).

(b) \((aDb)Mc = (aMc)D(bMc)\).

(c) \((aMb)Dc = (aDc)M(bDc)\).

Proof. For (a), note that \([ab]/(a, b) = \prod p_i^{a_i+b_i - \min\{a_i, b_i\}} = \prod p_i^{\max\{a_i, b_i\}} \). The results for (b) and (c) follow from this, as gcd is a min function and lcm is a max function, and the operations min and max are distributive in the stated properties. Namely, for (b), let \( c = \prod p_i^{c_i} \) and \( d = (aDb)Mc = \prod p_i^{d_i} \). It is evident that \( d_i = \max\{\min\{a_i, b_i\}, c_i\} = \min\{\max\{a_i, c_i\}, \max\{b_i, c_i\}\} \). Switch all the min and max for part (c).

1.22. Prove that \((a, b) = (a + b, [a, b])\).

Proof. Let \( d = (a, b) \), and let \( a = \alpha d \) and \( b = \beta d \). Note that \((\alpha, \beta) = 1\), and as a result \((\alpha + \beta, \alpha\beta) = 1\) (let \( e = (\alpha + \beta, \alpha\beta) \), suppose \( e > 1 \), then \( e|\alpha \) or \( e|\beta \), contradicting that \( e|(\alpha + \beta) \)). Now

\[ (a + b, [a, b]) = (d(\alpha + \beta), |ab|/(a, c)) = (d(\alpha + \beta), \alpha\beta d) = d. \]

1.23. The sum of two positive integers is 5264 and their least common multiple is 200340. Determine the two integers.

First we note that \((5264, 200340) = 28\), so we may simplify the problem to finding two integers who sum to 5264/28 = 188 and multiply to 200340/28 = 7155 (this simplification is valid by the previous exercise). Denoting one of the
numbers as \( n \), we have \( n(188 - n) = 7155 \), which after a quadratic equation yields \( n = 53, 135 \). Multiply by 28 to obtain the original two integers, 1484 and 3780.

**1.24.** Prove the following multiplicative property of the gcf:

\[
(ah, bk) = (a, b)(h, k) \left( \frac{a}{(a, b)} \cdot \frac{k}{(h, k)} \right) \left( \frac{b}{(a, b)} \cdot \frac{h}{(h, k)} \right).
\]

In particular this shows that \((ah, bk) = (a, k)(b, h)\) whenever \((a, b) = (h, k) = 1\).

*Proof.* Let \( d = (a, b) \) and \( l = (h, k) \). The let \( a = \alpha d \), \( b = \beta d \), \( h = \gamma l \), and \( k = \kappa l \). Note that \((\alpha, \beta) = (\gamma, \kappa) = 1\). Then we have

\[
(ah, bk) = (\alpha d \gamma l, \beta d \kappa l) = dl(\alpha \gamma, \beta \kappa) = dl(\alpha, \kappa)(\gamma, \beta)
\]

as desired.

**1.25.–1.28.** Prove each of the statements in Exercises 25 through 28. All integers are positive.

**1.25.** If \((a, b) = 1\) there exist \( x > 0 \) and \( y > 0 \) such that \( ax - by = 1 \).

*Proof.* We know from the gcd theorem that we can write \( 1 = au + bv \) where \( u \) and \( v \) are integers. Since \( a \) and \( b \) are assumed to be positive, we know that \( u \) and \( v \) must have opposite signs, else they would sum to absolute value at least 2. If \( u \) is positive and \( y \) is negative, we have \( x = u \) and \( y = -v \), so that \( ax - by = 1 \). But if \( u \) is negative and \( v \) is positive, i.e. that \( vb + au = 1 \), then note that \((v - a)b + (u + b)a = 1 \), and in general

\[
(v - na)b + (u + nb)a = 1.
\]

Choosing a sufficiently large value for \( n \) makes \( v - na \) negative and \( u + nb \) positive, so that \( x = u + nb \) and \( y = -v + na \).

**1.26.** If \((a, b) = 1\) and \( x^a = y^b \) then \( x = n^b \) and \( y = n^a \) for some \( n \).

*Proof.* First we show \( y^{1/a} \) and \( x^{1/b} \) are integers. Suppose \( y^{1/a} \) is not an integer, then by Exercise 13(b), \( x = y^{b/a} \) is not an integer, which is a contradiction. By symmetry, \( x^{1/b} \) must also be an integer. Then raising both sides of the equation \( x^a = y^b \) to the \( 1/(ab) \) power gives \( x^{1/b} = y^{1/a} \), so they are the same integer, giving \( n \).

**1.27.**
(a) If \((a,b) = 1\) then for every \(n > ab\) there exist positive \(x\) and \(y\) such that 
\[ n = ax + by. \]

Proof. Note that \(n - a, n - 2a, \ldots, n - ba\) all have different remainders when divided by \(b\), as \((a,b) = 1\). Since there are \(b\) of them and there are only \(b\) different remainders when dividing by \(b\), one of these, say \(n - xa\), is a multiple of \(b\), say \(by\). Then \(ax + by = n\), with \(x, y > 0\).

(b) If \((a,b) = 1\) there are no positive \(x\) and \(y\) such that \(ab = ax + by\).

Proof. Suppose \(ab = ax + by\). Clearly \(a\) divides both sides, so that \(a|by\), and \(b\) divides both sides, so that \(b|ax\). Since \((a,b) = 1\), this implies \(a|y\) and \(b|x\), let \(x = bu\) and \(y = av\). Then \(ab = abu + abv\), so that \(1 = u + v\), contradicting that both \(x\) and \(y\) are positive.

1.28. If \(a > 1\) then \((a^m - 1, a^n - 1) = a^{(m,n)} - 1\).

Proof. If \(m = n\) the problem is trivial. Without loss of generality, let \(m > n\). Note that \((a^k, a^j - 1) = 1\), so we may multiply by \(a^{m-n}\) and add to obtain 
\[ (a^m - 1, a^n - 1) = (a^m - 1, a^m - a^{m-n}) = (a^{m-n} - 1, a^n - 1). \]
Repeating the process, this is the Euclidean algorithm on \(m\) and \(n\), ending with \(a^{(m,n)} - 1\).

1.29. Given \(n > 0\), let \(S\) be a set whose elements are positive integers \(\leq 2n\) such that if \(a\) and \(b\) are in \(S\) and \(a \neq b\) then \(a \nmid b\). What is the maximum number of integers that \(S\) can contain?

There are at most \(n\) integers in \(S\). The numbers \(n + 1, \ldots, 2n\) do not divide each other, so the number is at least \(n\). To see it is at most \(n\), note that \(A\) can contain at most one of the integers \(m2^k\) for each odd integer \(m\), and there are precisely \(n\) odd numbers from 1 to \(2n\).

1.30. If \(n > 1\) prove that the sum
\[ \sum_{k=1}^{n} \frac{1}{k} \]
is not an integer.

Proof. Let \(m = 2^l\) be the largest power of 2 that is less than or equal to \(n\). Note that
\[ \sum_{k=1}^{n} \frac{1}{k} = 1 + n! \sum_{k=1}^{n} \frac{n!}{k}. \]
Clearly 2 divides each \(\frac{n!}{k}\) except for \(\frac{n!}{m}\). By linearity, \(\sum_{k=1}^{n} \frac{n!}{k}\) is not divisible by 2, and since \(n \geq 2\), \(\frac{1}{m} \sum_{k=1}^{n} \frac{n!}{k}\) cannot be an integer.