Introduction to Analytic Number Theory
Chapter 1: The Fundamental Theorem of Arithmetic

newell.jensen@gmail.com

Exercises:

1. If $(a, b) = 1$ and if $c \mid a$ and $d \mid b$, then $(c, d) = 1$.

Proof. If $c \mid a$ and $d \mid b$, then $nc = a$ and $md = b$, for integers n, m.

Therefore, $1 = ax + by = ncx + mdy = c(nx) + d(my)$ showing that $(c, d) = 1$. $\square$

2. If $(a, b) = (a, c) = 1$, then $(a, bc) = 1$.

Proof. If $ax_1 + by_1 = 1$ and $ax_2 + cy_2 = 1$, then multiplying these two together we get:

$$\begin{aligned}(ax_1 + by_1)(ax_2 + cy_2) = 1 &\implies a^2x_1x_2 + acx_1y_2 + abx_2y_1 + bcy_1y_2 = 1\\ &\implies a(ax_1x_2 + cx_1y_2 + bx_2y_1) + (bc)(y_1y_2) = 1\\ &\implies (a, bc) = 1.\end{aligned}$$

$\square$

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

Proof.

base case - $n = k = 1$ is already given via $(a, b) = 1$.

induction hypothesis - Assume $(a^{n-1}, b^{k-1}) = 1$ for all $n \geq 1, k \geq 1$.

induction step - Let $d = (a^n, b^k)$, then $d = (aa^{n-1}, bb^{k-1}) = aa^{n-1}x + bb^{k-1}y$

$$d = a(a^{n-1}x) + b(b^{k-1}y) = 1 \text{ [base case where } (a^{n-1}x), (b^{k-1}y) \in \mathbb{N}]$$

$$d = a^{n-1}(ax) + b^{k-1}(by) = 1 \text{ [induction hypothesis where } (ax), (by) \in \mathbb{N}]$$

Thus, we see we must have $d = 1$.

Therefore, if $(a, b) = 1$, then $(a^n, b^k) = 1$ for all $n \geq 1, k \geq 1$. $\square$

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

Proof. If $(a, b) = 1$ and $d = (a + b, a - b)$, then we have $1 = ax + by$ and $d = (a + b)x + (a - b)y$ so that

$$d = (a + b)x + (a - b)y = a(x + y) + b(x - y) = 1$$

$$d = (a + b)x + (a - b)y = [ay + bx] + [ax + b(-y)] = 1 + 1 = 2$$

Another way to do this is

$$(a + b)(x + y) + (a - b)(x - y) = (ax + ay + bx + by) + (ax - ay - bx + by) = 2ax + 2by = 2(ax + by) = 2$$

which can also be written as

$$2ax + 2by = a(2x) + b(2y) = 1.$$

Therefore $(a + b, a - b)$ is either 1 or 2. $\square$

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

Proof. Let $d=(a+b, a^2-ab+b^2)$.

Since $a^2-ab+b^2=(a+b)^2-3ab$ and $d \mid (a+b) \implies d \mid (a+b)^2$, then $d \mid (-3ab)$.

But $(a,b)=1 \implies d \nmid ab$ therefore $d \mid 3$ and since 3 is prime its only divisors are 1 and itself. ☐

6. If $(a,b)=1$, and if $d \mid (a+b)$, then $(a,d)=(b,d)=1$.

Proof. Since $d \mid (a+b)$ we can write this as $d=a+b \implies a=d-b$ and $b=d-a$.

Therefore, since $(a,b)=1$ we have

$$ax+by=1 \implies (d-b)x+by=1 \implies dx+b(y-x)=1 \implies (d,b)=1 \implies (b,d)=1$$

$$ax+by=1 \implies ax+(d-a)y=1 \implies a(x-y)+dy=1 \implies (a,d)=1.$$

Therefore, $(a,d)=(b,d)=1$. ☐

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. $\frac{a}{b}+\frac{c}{d}=n \implies \frac{ad+bc}{bd}=n \implies ad+bc=nbd \implies b \mid ad, d \mid cb$ but since $(a,b)=(c,d)=1 \implies b \mid d$ and $d \mid b$. Therefore, $|b|=|d|$. ☐

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. From the fundamental theorem of arithmetic we know that any positive integer n can be written as $n=p_1^{a_1}\cdots\ p_r^{a_r}$.

To get this into the form of $n=a^2b$, where b is squarefree we can sort the primes. If the power, a_i, of a particular prime p_i is odd we can take one factor of this prime and add it as a factor for b. Then, we can take *half* of the remaining factors and add them as a factor for a [the other half are represented by the squaring of a]. If the power a_i is not odd, then we simply add half of the factors to a. If we do this for all primes in the unique prime factorization for n, we will arrive at $n=a^2b$. ☐

9. For each of the following statements, either give a proof or exhibit a counter example.

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

Counter example - Let $n=36, a=2, b=3$. Then $a^2=4 \mid 36$ and $b^2=9 \mid 36$ but $2 \nmid 3$.

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

Proof. In Exercise 8 we proved that that for every $n \geq 1$ there exist uniquely determined $b>0$ and $d>0$ such that $n=b^2d$, where d is squarefree (note that we have *relabeled* the equation here to better line up with the variables that we are used in this Exercise).

Therefore, $n=b^2d \implies b^2 \mid n$ as we already know. However, since $a^2 \mid n$ we see that a^2 must be a factor from b^2 as d is squarefree. Therefore, $a^2 \mid b^2 \implies a \mid b$. ☐

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

Proof. From the definition of gcd we know that $(m,n)=ms+nt$ for integers s,t.

$$ms + nt = (ax + by)s + (cx + dy)t = axs + bys + cxt + dyt = x(as + ct) + y(bs + dt)$$

Therefore, since $(as + ct)$ and $(bs + dt)$ are in $\mathbb{Z}$ we have that $(m, n) = (x, y)$. $\square$

Note: there is another way to prove this that uses $ad - bc = \pm 1$ but personally prefer this *algebraic* method.

The other way takes the system of linear equations in m, n and solves for x, y and then uses the fact that $ad - bc = \pm 1$ to simplify. This then shows that x, y are linear combinations in m, n and are also divisible by m, n so that we arrive at the conclusion:

$(x, y) \mid m, (x, y) \mid n$ and $(m, n) \mid x, (m, n) \mid y \implies (x, y) \mid (m, n)$ and $(m, n) \mid (x, y) \implies (m, n) = (x, y)$.

11. Prove that $n^4 + 4$ is composite if $n > 1$.

Proof. $n^4 + 4$ can be factored as $(n^2 + 2n + 2)(n^2 - 2n + 2)$ and for $n > 1$ these two factors are different from one another and belong to $\mathbb{Z}$.

Therefore, $n^4 + 4$ is composite if $n > 1$. $\square$

In exercises 12, 13 and 14, a, b, c, m, n denote *positive* integers.

12. For each of the following statements either give a proof or exhibit a counter example.

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

Proof. If $a^n \mid b^n$ then $a_1 a_2 \cdots a_n \mid b_1 b_2 \cdots b_n$.

TODO: re-check this proof — As each side has n items, if we remove $n - 1$ terms on each side we are left with $a \mid b$. $\square$

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

Counter example - $a = 4, b = 10 \implies 4^4 \mid 10^{10}$ since 10000000000/256=39062500 but $4 \nmid 10$.

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

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

Proof.

Additionally, if n is not the mth power of a positive integer, prove that $n^{1/m}$ is irrational.

14. If $(a, b) = 1$ and $ab = c^n$, prove that $a = x^n$ and $b = y^n$ for some x and y. [*Hint*: Consider $d = (a, c)$.]

Proof.

15. Prove that every $n \geq 12$ is the sum of two composite numbers.

Proof.

16. Prove that if $2^n - 1$ is prime, then n is prime.

Proof.

17. Prove that if $2^n + 1$ is prime, then n is a power of 2.

Proof.

18. If $m \neq n$ compute the gcd$(a^{2^m}+1, a^{2^n}+1)$ in terms of a. [*Hint*: Let $A_n = a^{2^n}+1$ and show that $A_n \mid (A_m - 2)$ if $m > n$.]

Proof.

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.

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

Proof.

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

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

Prove that the lcm has the following properties:

(a) If $a = \Pi_{i=1}^{\infty} p_i^{a_i}$ and $b = \Pi_{i=1}^{\infty} p_i^{b_i}$ then $[a, b] = \Pi_{i=1}^{\infty} p_i^{c_i}$, where $c_i = max a_i, b_i$.

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

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

Proof (a).

Proof (b).

Proof (c).

22. Prove that $(a, b) = (a + b, [a, b])$.

Proof.

23. The sum of two positive integers is 5264 and their least common multiple is 200,340. Determine the two integers.

Proof.

24. Prove that the following multiplicative property of the gcd:

$$(ah, bk) = (a, b)(h, k)\left(\tfrac{a}{(a,b)}, \tfrac{k}{(h,k)}\right)\left(\tfrac{b}{(a,b)}, \tfrac{h}{(h,k)}\right).$$

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

Proof.

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

Proof.

26. If $(a, b) = 1$ and $x^a = y^b$ then $x = n^b$ and $y = n^a$ from some n. [*Hint*: Use Exercises 25 and 13.]

Proof.

27.

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

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

Proof.

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

Proof.

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? [*Hint*: S can contain at most one of the integers $1, 2, 2^2, 2^3, \ldots$, at most one of the $3, 3 \cdot 2, 3 \cdot 2^2, ...$, etc.]

Proof.

30. If $n > 1$ prove that the sum

$$\textstyle\sum_{k=1}^{n} \frac{1}{k}$$

is not an integer.

Proof.