Introduction to Analytic Number Theory

Tom M. Apostol

newell.jensen@gmail.com

Chapter 1 - The Fundamental Theorem of Arithmetic

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 $(c, d) = 1$. □

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:

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

Therefore, if $(a, b) = (a, c) = 1$, then $(a, bc) = 1$. □

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: Suppose $(a^{n-1}, b^{k-1}) = 1$.

induction step: Let $d = (a^n, b^k)$, then

$$\begin{aligned}d &= a^n x + b^k y \\ &= aa^{n-1} + bb^{k-1}y\end{aligned}$$

From the base case, we know that a and b do not have any common factors as they are relatively prime. Additionally, from the induction hypothesis we know that a^{n-1} and b^{k-1} also do not have any common factors as they are also relatively prime. Thus, the only common divisor for a^n and b^k must be 1.

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

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

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

or

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

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 $d\mid(-3ab)$.

Therefore, each of the prime factors of d must divide 3, a or b. Suppose the prime factor p of d divides a. Then, $p\mid a$ which implies that $p\mid(a+b)-b$ but this contradicts $(a,b)=1$, so we must have that $p\nmid ab$. Therefore, $d\mid 3$ and since 3 is prime its divisors are 1 or 3. $\square$

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

Proof. Since $d\mid(a+b)$ we have that $nd=a+b$ from some integer n. Let $g=(a,d)$.

Then, $nd=a+b\implies b=nd-a$ and since $g\mid a$ and $g\mid d$ we also must have that $g\mid b$. However, since $g\mid a$ and $g\mid b$ we must have that $g\mid(a,b)=1$, showing that $g=(a,d)=1$. The same argument shows that $(b,d)=1$. $\square$

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.

$$\begin{aligned}\frac{a}{b}+\frac{c}{d}&=n\\ \frac{ad+bc}{bd}&=n\\ ad+bc&=nbd\end{aligned}$$

which implies that $b\mid ad, d\mid cb$ but since $(a,b)=(c,d)=1\implies b\mid d$ and $d\mid b$. Therefore, $|b|=|d|$. $\square$

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 $n=a^2b$. $\square$

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 $b^2 = 9 \mid 36$, with $4 < 9$, 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 $n = b^2 d$, where d is squarefree.

Therefore, $n = b^2 d \implies b^2 \mid n$ 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 the greatest common divisor 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 $(m, n) = (x, y)$. □

Note: there is another way to prove this that uses $ad - bc = \pm 1$.

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:

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

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 integers that differ from one another.

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

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. We will prove this inductively using the contrapositive.

base case: If $a \nmid b$ then $a^1 \nmid b^1$.

induction hypothesis: Suppose that if $a \nmid b$ then $a^{n-1} \nmid b^{n-1}$.

induction step: If $a \nmid b$ then

$$a^n \nmid b^n$$
$$aa^{n-1} \nmid bb^{n-1}$$

which we can see is true because $a \nmid b$ and therefore a doesn't divide any power of b. Then, from the induction hypothesis we see that $a^{n-1} \nmid b^{n-1}$ and therefore a^{n-1} doesn't divide any factor of b^{n-1}.

Thus, if $a \nmid b$ then $a^n \nmid b^n$. $\square$

(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 $a \mid b$.

Proof. If a is odd then $(a, 2) = 1$ and then from part (a) we know that $a^n \mid b^n \implies a \mid b$. If a is even then we can write it as $a = 2^r d$ with d odd. Then

$$\begin{aligned} 2b^n &= 2^{nr} d^n k && [k \text{ an integer}] \\ b^n &= 2^{nr-1} d^n k \end{aligned}$$

but since the left side of the equation is raised to the n^{th} power, we know that we can represent the right side of the equation to the n^{th} power as well (i.e., solving for b). This implies that k must be even as 2^{nr-1} is not an n^{th} power. That is, $k = 2t^n$ such that

$$\begin{aligned} b^n &= 2^{nr} d^n t^n && [t \text{ an integer}] \\ &= (2^r d)^n t^n \\ &= a^n t^n \end{aligned}$$

Therefore, we have that $a^n \mid b^n$ and from part (a) we then know that $a \mid b$. $\square$

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

(a) prove that $b = 1$.

Proof. Since a and b are relatively prime we see that

$$\begin{aligned} (a/b)^m &= n \\ \frac{a^m}{b^m} &= n \\ a^m &= nb^m \end{aligned}$$

and this can only be true for $b = 1$ since $(a, b) = 1$. $\square$

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

Proof. Suppose that $n^{1/m}$ is *not* irrational. Thus, it must be rational and of the form

$$\begin{aligned} \frac{a}{b} &= n^{1/m} \\ \left(\frac{a}{b}\right)^m &= (n^{1/m})^m \\ \frac{a^m}{b^m} &= n \\ a^m &= n && [(a, b) = 1 \text{ and part (a) showed } b = 1] \end{aligned}$$

Thus, n is the m^{th} power of a positive integer (this is the negation of the original antecedent).

Therefore, if n is not the m^{th} power of a positive integer, then $n^{1/m}$ is irrational. $\square$

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. By the Fundamental Theorem of Arithmetic we know that

$$\begin{aligned} a &= p_1^{a_1} \cdots p_r^{a_r} \text{ and } b = p_1^{b_1} \cdots p_k^{b_k} \\ c^n &= p_1^{a_1} \cdots p_r^{a_r} \cdot p_1^{b_1} \cdots p_k^{b_k} \\ c &= (p_1^{a_1/n} \cdots p_r^{a_r/n}) \cdot (p_1^{b_1/n} \cdots p_k^{b_k/n}) \end{aligned}$$

which implies that $n \mid a_i$ and $n \mid b_j$ as the primes factors of c must be distinct. Therefore, a and b must be the n^{th} power of some integers. □

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

Proof. Suppose n is even. Let $n = (n-4)+4$, then $n-4$ is also even since

$$\begin{aligned} n-4 &= 2k-4 && [n \text{ is even}] \\ &= 2(k-2) \end{aligned}$$

and therefore n is the sum of two composite numbers.

Suppose n is odd. Let $n = (n-9)+9$, then $n-9$ is even since

$$\begin{aligned} n-9 &= 2k+1-9 && [n \text{ is odd}] \\ &= 2(k-4) \end{aligned}$$

and therefore n is the sum of two composite numbers. □

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

Proof. Suppose that n is *not* prime. Then n is a composite number, say $n = ab$ for some $a > 1$ and $b > 1$. Then

$$2^n - 1 = (2^a)^b - 1 = (2^a - 1)(2^{a(b-1)} + 2^{a(b-2)} + \cdots + 2^a + 1).$$

Since both factors are greater than 1, $2^n - 1$ must be composite. □

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

Proof. Suppose that n is *not* a power of 2, say $n = 2^k b$ with $b > 1$ odd and $a = 2^k$. Then

$$2^n + 1 = (2^a)^b + 1 = (2^a + 1)(2^{a(b-1)} - 2^{a(b-2)} + \cdots + 2^{2a} - 2^a + 1).$$

Thus, $2^n + 1$ is not prime as both factors are greater than 1.

Therefore, if $2^n + 1$ is prime, then n is a power of 2. □

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. Let $d = (A_m, A_n)$. If $m > n$ then

$$\begin{aligned} A_m - 2 = a^{2^m} + 1 - 2 &= a^{2^m} - 1 \\ &= a^{2^n 2^{m-n}} - 1 \\ &= (a^{2^n} + 1)(a^{2^n(2^{m-n}-1)} - a^{2^n(2^{m-n}-2)} + \cdots + a^{2^n} - 1) \\ &= A_n \cdot (a^{2^n(2^{m-n}-1)} - a^{2^n(2^{m-n}-2)} + \cdots + a^{2^n} - 1) \end{aligned}$$

Therefore, $A_n \mid A_m - 2$ showing that $d \mid A_m - 2$ (transitive property of divisibility) as d is a common divisor of A_n and A_m. By linearity, $d \mid 2$. Since $A_n = a^{2^n} + 1$, if a is even then A_n is odd and $d = 1$. If a is odd then $d = 2$. □

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.
base case: $a_1 = a_2 = 1 \implies (a_1, a_2) = 1$.

induction hypothesis: Suppose $(a_{n-1}, a_n) = 1$.

induction step: Let $d = (a_n, a_{n+1})$, then

$$\begin{aligned} d &= a_n x + a_{n+1} y \\ &= a_n x + (a_n + a_{n-1}) y && \text{[recusion relation]} \\ &= a_n(x + y) + a_{n-1} y \\ &= (a_{n-1}, a_n) \\ &= 1 && \text{[induction hypothesis]} \end{aligned}$$

Therefore, $(a_n, a_{n+1}) = 1$ for each n. □

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

Proof.

$$\begin{aligned} 1890 &= 826 \cdot 2 + 238 \\ 826 &= 238 \cdot 3 + 112 \\ 238 &= 112 \cdot 2 + 14 \\ 112 &= 14 \cdot 8 + 0 \end{aligned}$$

Therefore, $d = 14$. Back substituting the remainders in the equations above (this is the extended Euclidean algorithm), we arrive at

$$1890(7) + 826(-16) = 14$$

□

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

Proof. Since we can denote ab as

$$\begin{aligned} ab &= \prod_{i=1}^{\infty} p_i^{a_i} \prod_{i=1}^{\infty} p_i^{b_i} \\ &= \prod_{i=1}^{\infty} p_i^{a_i} p_i^{b_i} \\ &= \prod_{i=1}^{\infty} p_i^{\min\{a_i,b_i\}} p_i^{\max\{a_i,b_i\}} \end{aligned}$$

The gcd (a, b) is constructed from the matching prime powers of a and b. Therefore, the gcd is

$$(a, b) = \prod_{i=1}^{\infty} p_i^{\min\{a_i,b_i\}}$$

Thus, since the lcm is defined to be $[a, b] = |ab|/(a, b)$ if $a \neq 0$ and $b \neq 0$, we see that

$$[a, b] = \prod_{i=1}^{\infty} p_i^{c_i}$$

where $c_i = \max\{a_i, b_i\}$. □

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

Proof. Another way to write this is $[(a, b), c] = ([a, c], [b, c])$. Let $c = \prod_{i=1}^{\infty} p_i^{c_i}$. Then

$$[(a, b), c] = \left[\prod_{i=1}^{\infty} p_i^{\min\{a_i,b_i\}}, \prod_{i=1}^{\infty} p_i^{c_i}\right] = \prod_{i=1}^{\infty} p_i^{\max\{\min\{a_i,b_i\},c_i\}}$$
$$([a, c], [b, c]) = \left(\prod_{i=1}^{\infty} p_i^{\max\{a_i,c_i\}}, \prod_{i=1}^{\infty} p_i^{\max\{b_i,c_i\}}\right) = \prod_{i=1}^{\infty} p_i^{\min\{\max\{a_i,c_i\},\max\{b_i,c_i\}\}}$$

To show that these two are equal we must show that

$$\prod_{i=1}^{\infty} p_i^{\max\{\min\{a_i,b_i\},c_i\}} = \prod_{i=1}^{\infty} p_i^{\min\{\max\{a_i,c_i\},\max\{b_i,c_i\}\}}$$

Let us looks at the possible cases for these exponents:

ordering	$\max\{\min\{a_i,b_i\},c_i\}$	$\min\{\max\{a_i,c_i\},\max\{b_i,c_i\}\}$
$a_i \geq b_i \geq c_i$	b_i	b_i
$a_i \geq c_i \geq b_i$	b_i	b_i
$b_i \geq a_i \geq c_i$	b_i	b_i
$b_i \geq c_i \geq a_i$	a_i	a_i
$c_i \geq a_i \geq b_i$	b_i	b_i
$c_i \geq b_i \geq a_i$	a_i	a_i

This shows $\max\{\min\{a_i,b_i\},c_i\} = \min\{\max\{a_i,c_i\},\max\{b_i,c_i\}\}$ and therefore $(aDb)Mc = (aMc)D(bMc)$. $\square$

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

Proof. Another way to write this is $([a,b],c) = [(a,c),(b,c)]$. Let $c = \prod_{i=1}^{\infty} p_i^{c_i}$. Then

$$([a,b],c) = \left(\prod p_i^{\max\{a_i,b_i\}}, \prod p_i^{c_i}\right) = \prod p_i^{\min\{\max\{a_i,b_i\},c_i\}}$$
$$[(a,c),(b,c)] = \left[\prod p_i^{\min\{a_i,c_i\}}, \prod p_i^{\min\{b_i,c_i\}}\right] = \prod p_i^{\max\{\min\{a_i,c_i\},\min\{b_i,c_i\}\}}$$

To show that these two are equal we must show that

$$\prod p_i^{\min\{\max\{a_i,b_i\},c_i\}} = \prod p_i^{\max\{\min\{a_i,c_i\},\min\{b_i,c_i\}\}}$$

Let us looks at the possible cases for these exponents:

ordering	$\min\{\max\{a_i,b_i\},c_i\}$	$\max\{\min\{a_i,c_i\},\min\{b_i,c_i\}\}$
$a_i \geq b_i \geq c_i$	c_i	c_i
$a_i \geq c_i \geq b_i$	b_i	b_i
$b_i \geq a_i \geq c_i$	c_i	c_i
$b_i \geq c_i \geq a_i$	b_i	b_i
$c_i \geq a_i \geq b_i$	b_i	b_i
$c_i \geq b_i \geq a_i$	b_i	b_i

This shows $\min\{\max\{a_i,b_i\},c_i\} = \max\{\min\{a_i,c_i\},\min\{b_i,c_i\}\}$ and therefore $(aMb)Dc = (aDc)M(bDc)$. $\square$

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

Proof. From Theorm 1.4 (c) if $c > 0$, then we know that $(ac,bc) = c(a,b)$. Let $d = (a,b)$. Then $d \mid a$ and $d \mid b$ such that $a = dn$ and $b = dm$, for integers n,m. Furthermore, we know that $\left(\frac{a}{d},\frac{b}{d}\right) = (n,m) = 1$ since d divides out any common factors that a and b share. Using these facts we see that

$$\begin{aligned}(a+b,[a,b]) &= (a+b,|ab|/d) && \text{[definition of lcm]}\\ &= (dn+dm,\pm dnm) && \text{[substituting } a=dn \text{ and } b=dm\text{]}\\ &= (d(n+m,nm)) && \text{[Theorem 1.4 (c)]}\end{aligned}$$

For this to equal (a,b), we must have that $(n+m,nm) = 1$. We know that $(n,m) = 1$. Suppose that $(n+m,nm) = k$, with $k \neq 1$. Then $k \mid nm$ and $k \mid n+m$, showing that k divides both m and n, which is a contradiction as they are relatively prime. Therefore, $(n+m,nm) = 1$ and we see that $(a+b,[a,b]) = (a,b)$. $\square$

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

Proof. We know that the lcm is

$$\begin{aligned}
[a,b] &= \frac{|ab|}{(a,b)} \\
&= \frac{|ab|}{(a+b,[a,b])} && \text{[Exercise 22]}
\end{aligned}$$

We are given that $[a,b] = 200,340$ and that $a+b$ so this becomes

$$\begin{aligned}
200,340 &= \frac{|ab|}{(5264, 200, 340)} \\
&= \frac{|ab|}{28}
\end{aligned}$$

Therefore, we have that $|ab| = 200,340 \cdot 28 = 5609520$. The factors of 5609520 are: $2^4 \cdot 3^3 \cdot 5 \cdot 7^2 \cdot 53$. Thus, the factors that sum to 5264 are $1484 = 2^2 \cdot 7 \cdot 53$ and $3780 = 2^2 \cdot 3^3 \cdot 5 \cdot 7$. □

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

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

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

Proof. Let $d = (a,b)$ and $l = (h,k)$. Since $d \mid a,\ d \mid b \implies a = dx,\ b = dy$ for integers x and y. Similarly, since $l \mid h,\ l \mid k \implies h = ls,\ k = lt$. Note that $(x,y) = (s,t) = 1$ since, without loss of generality

$$\begin{aligned}
(x,y) &= \left(\frac{a}{d}, \frac{b}{d}\right) \\
&= \frac{1}{d}(a,b) \\
&= \frac{1}{d} \cdot d \\
&= 1
\end{aligned}$$

Thus, we have that

$$\begin{aligned}
(ah, bk) &= (dxls, dylt) \\
&= dl(xs, yt) \\
&= dl(x,t)(s,y) && [(x,y) = (h,k) = 1] \\
&= dl\left(\frac{a}{d}, \frac{k}{l}\right)\left(\frac{b}{d}, \frac{h}{l}\right) && [x = \tfrac{a}{d},\ \text{etc.}] \\
&= (a,b)(h,k)\left(\frac{a}{(a,b)}, \frac{k}{(h,k)}\right)\left(\frac{b}{(a,b)}, \frac{h}{(h,k)}\right).
\end{aligned}$$

Which is the desired result. □

Prove each of the statements in Exercises 25 through 28. All integers are positive.

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

Proof. Since $(a,b)=1$ we have that $as+bt=1$ for integers s and t. Then

$$\begin{aligned}
1 &= as+bt \\
&= as+b(a-y) && [y>0,\ \text{see below for more details}] \\
&= a(s+b)-by && [s+b>0 \text{ since } a>0, b>0, y>0] \\
&= ax-by && [x=s+b>0]
\end{aligned}$$

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

Note: s and t can be either positive or negative and the actual values depend on a and b (these are found via the Extended Euclidean Algorithm). Therefore, when substituting $(a-y)$ for t, if $t<0$ let $y>a$, if $t>0$ let $a>y>0$, and if $a=1$ let $y=1>0$. This last scenario would result in a trivial solution to the equation. □

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. From Exercise 25 we know that if $(a,b)=1$ then there exist $c>0$ and $d>0$ such that $ac-bd=1$. Then

$$\begin{aligned}
x^a &= y^b \\
(x^a)^d &= (y^b)^d \\
x^{ad} &= y^{bd} \\
x^{ad} &= y^{ac-1} && [bd=ac-1] \\
(x^{ad})^{\frac{1}{a}} &= (y^{ac-1})^{\frac{1}{a}} \\
x^d &= y^{c-\frac{1}{a}} \\
x^d &= y^c y^{-\frac{1}{a}} \\
y^{\frac{1}{a}} &= \frac{y^c}{x^d} \\
y &= \left(\frac{y^c}{x^d}\right)^a \\
y &= n^a && \left[\text{Exercise 13 and } n=\frac{y^c}{x^d}\right]
\end{aligned}$$

This shows us that $y=n^a$. There is a similar argument for $x=n^b$

$$\begin{aligned}
x^a &= y^b \\
(x^a)^c &= (y^b)^c \\
x^{ac} &= y^{bc} \\
x^{1+bd} &= y^{bc} && [ac=1+bd] \\
(x^{1+bd})^{\frac{1}{b}} &= (y^{bc})^{\frac{1}{b}} \\
x^{\frac{1}{b}+d} &= y^c \\
x^{\frac{1}{b}}x^d &= y^c \\
x^{\frac{1}{b}} &= \frac{y^c}{x^d}
\end{aligned}$$

$$x = \left(\frac{y^c}{x^d}\right)^b$$

$$x = n^b \qquad \left[\text{Exercise 13 and } n = \frac{y^c}{x^d}\right]$$

This shows us that $x = n^b$.

Therefore, if $(a, b) = 1$ and $x^a = y^b$ then $x = n^b$ and $y = n^a$ from some n. □

27.

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

Proof. From Theorem 1.14 we know that given integers a and b with $b > 0$, there exists a unique pair of integers q and r such that

$$a = bq + r, \quad \text{with } 0 \le r < b$$

Moreover, $r = 0$ if, and only if, $b \mid a$.

Using Theorem 1.14 with the fact that $n > ab,\ a > 0,\ b > 0$, we can write the two equations

$$n = aq_1 + r_1 \tag{1}$$

$$by = aq_2 + r_2 \tag{2}$$

If we subtract (2) from (1) we get

$$n - by = (q_1 - q_2)a + (r_1 - r_2)$$

and since $n - by > 0$ and $a > 0$ we see that $q_1 - q_2 > 0$ and $r_1 - r_2 > 0$. Let $x = q_1 - q_2$ and $r = r_1 - r_2$ so that

$$n - by = ax + r$$

Since $n > ab$ and $(a, b) = 1$, if we take values of $1 \le y \le a$ this equation will give us a conjugacy class mod a with order a (i.e., there are a elements in the conjugacy class mod a). Therefore, there must be an element of this conjugacy class that has remainder zero.

Therefore, 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. Suppose there *are* positive x and y such that $ab = ax + by$. Then $ab \mid a$ and $ab \mid b$ and since $a > 0$ and $b > 0$ we must have positive integers n and m such that $abn = a$ and $abm = b$. This implies that $bn = 1$ and $am = 1$, which would mean that $a = b = n = m = 1$ and therefore $ab = ax + by \implies 1 = x + y$. However, by hypothesis $x > 0$ and $y > 0$ so $1 = x + y$ leads to a contradiction.

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

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

Proof. If $m = n$ this is obviously true. Suppose that $m > n$. Then by Theorem 1.14 we know that there exist unique integers q and r such that $m = nq + r$. Thus,

$$a^m - 1 = a^{nq+r} - 1$$

$$
\begin{aligned}
&= a^r a^{nq} - 1 \\
&= a^r(a^{nq} - 1) + (a^r - 1) \\
&= a^r(a^{q-1} + \cdots + a + 1)(a^n - 1) + (a^r - 1)
\end{aligned}
$$

Since $0 \leq r < n \implies 0 \leq a^r - 1 < a^n - 1$ and therefore, we can perform the Euclidean Algorithm on the above equation to arrive at the gcd $(a^m - 1, a^n - 1)$. However, this process is also performing the Euclidean Algorithm on the *exponents*, namely, (m, n). Therefore, if $a > 1$ then $(a^m - 1, a^n - 1) = a^{(m,n)} - 1$. $\square$

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 $3, 3 \cdot 2, 3 \cdot 2^2, \ldots$, etc.]

Proof. An interesting fact is that any number between $n + 1$ and $2n$ do not divide each other. Therefore, S has at least n elements. From the hint, S contains at most one integer of the form $m2^k$, for each m odd. Since there are exactly n odd numbers between 1 and $2n$, S therefore contains at most n integers. $\square$

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

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

is not an integer.

Proof.
base case: $n = 2$ we have that the sum is $1 + 1/2 = 3/2$, which is not an integer.

induction hypothesis: Suppose

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

is not an integer.

induction step:

$$
\begin{aligned}
\sum_{k=1}^{n} \frac{1}{k} &= \sum_{k=1}^{n-1} \frac{1}{k} + \frac{1}{n} \\
&= \frac{a}{b} + \frac{1}{n} && \text{[induction hypothesis]} \\
&= \frac{an + b}{bn}
\end{aligned}
$$

For $\dfrac{an + b}{bn}$, this would only be an integer if $an + b = bn$. However, this implies $an = b(n-1) \implies \dfrac{a}{b} = \dfrac{n-1}{n}$, which is absurd as $\dfrac{a}{b} > 1$ (Note, even the base case is larger than 1). Therefore, we must have that $an + b \neq bn$, showing us that if $n > 1$ then

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

is not an integer. $\square$