Divisors Handout

Maximillian Roach

1 Introduction

Divisors are one of the most important parts of number theory. Each number has special characteristics because of the divisors it has, so investigating what numbers divide a given number can lead to important insights on a problem. In this handout, we'll learn about prime factorizations, the greatest common divisor, least common multiple, and some ways to apply these concepts.

2 What is a Divisor?

Definition 1 (Divisor)**.** Let a, b be integers. If we can write $a = bk$, where k is also an integer, then we can say b is a divisor of k.

This definition is a little difficult to understand, so consider $6 = 2 \cdot 3$. Because you can multiply 2 by an integer to get 6, we know 2 is a divisor of 6. Moreover, 3 is a divisor of 6.

However, we know 4 isn't a divisor of 6 because $6 = 4 \cdot 1.5$ and 1.5 isn't an integer.

Example 1. How many divisors does 12 have?

Solution: We can go through all the integers less than 12 and see which ones can be multiplied by another integer to get a product of 12. We don't have to consider integers greater than 12 since any number greater than 12 will have to be multiplied by a number between 0 and 1 to produce 12.
We then have $\{1, 2, 3, 4, 6, 12\}$ as the set of divisors of 12.

3 Prime Numbers

Definition 2 (Prime)**.** An integer is said to be prime if its only divisors are 1 and itself.

Definition 3 (Composite)**.** An integer is composite if it can be written as a product of two integers that are not 1 or itself. That is, it has divisors besides 1 and itself.

There is often a conflict about whether 1 is prime or not. It can be written as a product of 1 and itself ($1 \cdot 1 = 1$), since "itself" is 1. However, 1 is not considered prime because this product is not one of two **distinct** integers.

Example 2. What are the prime numbers less than 20?

Solution: We can test each of the number less than 20 see if it has divisors besides 1 and itself. This gives $\{2, 3, 5, 7, 11, 13, 17, 19\}$.

Theorem 1 (Fundamental Theorem of Arithmetic)**.** Every integer greater than 1 can be represented uniquely as a product of prime numbers, up to the order of the factors.

This represents one of the most important theorems in number theory. More simply, it says that we can represent every integer greater than 1 as a product of prime numbers. Moreover, there is only one of these representations for an integer.

The "order of the factors" means that when we write the integer as a product of primes, it doesn't matter if we change the order of the primes in the product. For instance, $2 \cdot 3 \cdot 2$ is the same as $2 \cdot 2 \cdot 3$.

The Fundamental Theorem of Arithmetic (FTA for short) introduces an essential problem solving technique: finding the prime factorization of a number.

Definition 4 (Prime Factorization)**.** The representation of an integer as a product of only prime numbers.

Example 3. The prime factorization of 84 is $2^2 \cdot 3 \cdot 7$ since $42 = 2^2 \cdot 3 \cdot 7$ and 2,3 and 7 are all prime numbers. The FTA tells us that this is the only prime factorization of 42.

The prime factorization of a number reveals a lot of information. Above, we know that 2, 3, and 7 all divide 84. We also know 84 has exactly 2 powers of 2 in its product.

Note that there is no clear way to find the prime factorization of a number. Generally, you can try testing smaller primes to see if they divide the number. For instance, I might try to see if the number is divisible by 2, then 3, and so on...

Theorem 2. There exist infinitely many primes.

Proof. Suppose by way of contradiction that there are finitely many primes $p_1, p_2, \ldots, p_n$, where n is a positive integer. Consider the integer

$$Q = p_1 p_2 \cdots p_n + 1$$

Because $Q > 1$, Q must have at least one prime divisor, call it q. If we prove that q is not one of the primes listed then we obtain a contradiction. Suppose q is one of the primes listed, say $q = p_i$ for $i \leq i \leq n$. Therefore, q divides $p_1 p_2 \cdots p_n$. Because q divides Q and q divides $p_1 p_2 \cdots p_n$, we know q divides $Q - p_1 p_2 \cdots p_n = 1$. However, there is not prime that divides 1. Hence, we have a contradiction and q is not one of the primes listed. $\square$

It might seem intuitive that there are infinitely many prime numbers. But how do we determine where primes occur? Sometimes prime numbers appear very close to each other, like 11 and 13, or 101 and 103. These are called twin primes. But often there are large gaps between one prime number and the next smallest prime. It is still unknown how to predict the size of these gaps between primes.

Definition 5 (Relatively Prime)**.** Two integers a and b are said to be relatively prime if they share no common divisors besides 1.

For example, 3 and 7 are relatively prime because the only common factor they share is 1. However, 5 and 10 are not relatively prime because they both have 5 as a factor. Relatively prime integers become more important as you explore number theory deeper because it is often the case that special properties are true only when the integers involved are relatively prime.

4 Greatest Common Divisor

Definition 6 (Greatest Common Divisor)**.** Given two integers a and b, the greatest common divisor of a and b, denoted by $\gcd(a, b)$, is the greatest of all divisors of both a and b.

Example 4. Consider the following GCD calculations:
$\gcd(5, 10) = 5$
$\gcd(3, 7) = 1$
$\gcd(16, 24) = 4$

There are two GCD calculations that are important to know when performing procedures such as the Euclidean Algorithm (by the time you're reading this you might be able to find a handout on the Euclidean Algorithm under Number Theory in Resources at desmoinesmathcircle.org).

First, $\gcd(a, 1) = 1$ for any integer a. This is because the only divisor of 1 is 1, so the greatest common divisor between any integer and 1 is also 1.
Second, $\gcd(a, 0) = a$ for any integer a. This is because any integer can be interpreted as a factor of 0 since $0 = a \cdot 0$. Therefore, a is a divisor of a and 0. It should also be apparent that a is the greatest divisor of a.

<u>How to Find the GCD of Two Numbers</u>
To obtain a general way to find the greatest common divisor, we can first consider a concrete example. Suppose we want to find $\gcd(48, 56)$. First, we find the prime factorizations of 24 and 56:

$$48 = 2^4 \cdot 3^1$$

$$56 = 2^3 \cdot 7^1$$

We can try to construct the PF (prime factorization) of $\gcd(48, 56)$. Any prime that is in the PF of $\gcd(48, 56)$ must be in 48's PF and 56's PF. 3 can't be in $\gcd(48, 56)$ since it's only a divisor of 48. The same reasoning works for why 7 can't be in $\gcd(48, 56)$. It might seem obvious, but a prime that is not in either 48 nor 56 cannot be in the PF of $\gcd(48, 56)$. Therefore, a prime such as 13 isn't a part of the GCD.
Now we have to keep in my mind that we want the **greatest** common divisor. Hence, for a given prime in the PF, it must be raised to the highest power common in both

48 and 46. For instance, 2^3 will be in the PF of $\gcd(48, 56)$. We can't use 2^4 since 2^4 is not a divisor of 56. We don't want to use 2^0, 2^1, or 2^2 because these are all less than 2^3 and wouldn't result in the largest common divisor.

Using the above logic, we can conclude $\gcd(48, 56) = 2^3 = 8$. Now we're ready to construct a general procedure.

Let a and b be two positive integers. To find $\gcd(a, b)$, perform the following steps:

1. Find the prime factorizations of a and b. Then
$$a = p_1^{e_1} \cdot p_2^{e_2} \cdots p_k^{e_k}$$
$$b = p_1^{f_1} \cdot p_2^{f_2} \cdots p_k^{f_k}$$
where e_i and f_i, for $1 \leq i \leq k$ are the powers p_i are raised to in a and b, respectively.

2. Consider only the primes that are present in **both** the PF of a and the PF of b.

3. In the prime factorization of $\gcd(a, b)$, p_i is raised to $\min(e_i, f_i)$. That is, each prime is raised to the minimum power it is raised to in the PF of a and b. Hence,
$$\gcd(a, b) = p_1^{\min(e_1, f_1)} \cdot p_2^{\min(e_2, f_2)} \cdots p_k^{\min(e_k, f_k)}$$

Put simply, to find the GCD of two numbers, you want to find the numbers' prime factorizations then take the minimum powers of the primes presents in both PFs.

Example 5. Find $\gcd(72, 156)$.

Solution: We first find the prime factorizations of 72 and 156:

$$72 = 2^3 \cdot 3^2$$
$$156 = 2^2 \cdot 3^1 \cdot 13^1$$

The primes present in both are 2 and 3. The minimum power 2 is raised to is 2 and the minimum power 3 is raised to is 1. Therefore, $\gcd(72, 156) = 2^2 \cdot 3^1 = 12$.

5 Least Common Multiple

First, we should define what a multiple of a number is. Don't worry, Multiplies are very similar to divisors.

Definition 7 (Multiple)**.** If a and b are integers, then a is a multiple of b if a can be written as $a = bk$, where k is an integer.

Notice the similarity between divisors and multiples. We can say that if a is a divisor of b, then b is a multiple of a. For instance, 3 is a divisor of 12 and 12 is a multiple of 3.

Definition 8 (Least Common Multiple)**.** Let a and b be integers. Then consider the set of all common multiples of a and b. Then the least common multiple of a and b is the smallest of all these common multiples.

Example 6. Consider the following LCM calculations:
$\text{lcm}(5, 10) = 10$
$\text{lcm}(3, 7)\ 21$
$\text{lcm}(24, 10) = 120$

How to Find the LCM of Two Numbers
To derive a general method to finding the least common multiple of two numbers, we find consider a tangible example. Suppose we want to find $\text{lcm}(60, 122)$. We first find the prime factorizations of 60 and 122:

$$60 = 2^2 \cdot 3^1 \cdot 5^1$$

$$122 = 2^1 \cdot 61^1$$

We can try to construct the prime factorization of $\text{lcm}(a, b)$. For a number to be a multiple of 60, the smallest power of 2 it can have in it's prime factorization is 2^2. Similarly, the smallest power of 3 and 5 it can have are 3^1 and 5^1, respectively. You can apply similar reasoning for 122.
Additionally, if a prime is present in the prime factorization of 60 or 122, it must present in $\text{lcm}(a, b)$. Then we want 2^2, 3^1, 5^1, and 61^1 so that the prime factorization is $\text{lcm}(a, b) = 2^2 \cdot 3^1 \cdot 5^1 \cdot 61^1$. Now we can determine a general method.

Let a and b be two positive integers. To $\text{lcm}(a, b)$, perform the following steps:

1. Find the prime factorizations of a and b. Then

$$a = p_1^{e_1} \cdot p_2^{e_2} \cdots p_k^{e_k}$$

$$b = p_1^{f_1} \cdot p_2^{f_2} \cdots p_k^{f_k}$$

   where e_i and f_i, for $1 \leq i \leq k$ are the powers p_i are raised to in a and b, respectively.

2. Consider all primes that are present in either the PF of a or the PF of b.

3. In the prime factorization of $\text{lcm}(a, b)$, p_i is raised to $\max(e_i, f_i)$. That is, each prime is raised to the maximum power it is raised to in the PF of a and b. Hence,

$$\text{lcm}(a, b) = p_1^{\max(e_1, f_1)} \cdot p_2^{\max(e_2, f_2)} \cdots p_k^{\max(e_k, f_k)}$$

Put simply, $\text{lcm}(a, b)$ has every prime present in either the prime factorization of a or the prime factorization of b. For a given prime in the PF of $\text{lcm}(a, b)$, it is raised to the maximum power it is raised to in a and b. For instance, if 2 is raised to the second power in a and the third power in b, we take 2^3.

Example 7. Find $\text{lcm}(42, 98)$.

Solution: First we find the prime factorizations of 42 and 98:

$$42 = 2^1 \cdot 3^1 \cdot 7^1$$

$$98 = 2^1 \cdot 7^2$$

We know some power of 2, 3, and 7 will be present in the prime factorization of $\text{lcm}(42, 98)$. These powers will be $2^1, 3^1, 7^2$. Note that 7^2 is chosen because $7^2 > 7^1$. Therefore, $\text{lcm}(42, 98) = 2^1 \cdot 3^1 \cdot 7^2 = 294$.

6 Special Functions

There are three well-known functions that can be used to get information about the divisors of a number. First, there is $\tau(n)$ which outputs the number of divisors of n. $\tau(n)$ is likely the most useful of the three functions we'll cover. Then there is $\sigma(n)$, which outputs the sum of the divisors of n. Finally, $d(n)$ outputs the product of the divisors of n.

Theorem 3 (Number of Divisors)**.** Let the positive integer n have prime factorization

$$n = p_1^{e_1} \cdot p_2^{e_2} \cdots p_k^{e_k}$$

Then the number of divisors of n is given by

$$\tau(n) = (e_1 + 1)(e_2 + 1)(e_3 + 1) \cdots (e_k + 1)$$

We can see this in action by finding the number of divisors of 12. The prime factorization of 12 is $12 = 2^2 \cdot 3^1$, which means $\tau(12) = (2 + 1)(1 + 1) = 6$. Indeed, the 6 divisors of 12 are 1, 2, 3, 4, 6, and 12.

The derivation for $\tau(n)$ is relatively simple and follows from a combinatorial argument. Notice in the example above with 12, the possible powers of 2 for a divisor of 12 are $2^0, 2^1,$ and, 2^2. So there are 3 possibilities for the power of 2. Similarly there are 2 possibilities for the power of 3. Then by the Fundamental Principle of Counting (if you don't know what this is, read the Introductory Counting handout at desmoinesmathcircle.org), there are $3 \cdot 2 = 6$ divisors of 12.

By the same reasoning, we can say for a given prime p_i, there are $e_i + 1$ choices for the power p_i is raised to so that you get a divisor of n. These are $0, 1, 2, \ldots, e_i - 1, e_i$. Then we multiply the number of choices for each power to get the total number of divisors, $(e_1 + 1)(e_2 + 1) \cdots (e_k + 1)$.

Theorem 4 (Sum of Divisors)**.** Let the positive integer n have prime factorization

$$n = p_1^{e_1} \cdot p_2^{e_2} \cdots p_k^{e_k}$$

Then the number of divisors of n is given by

$$\sigma(n) = (1 + p_1^2 + \cdots p_1^{e_1})(1 + p_2^2 + \cdots p_2^{e_2}) \cdots (1 + p_k^2 + \cdots p_k^{e_k})$$

Now we can try to find the sum of the divisors of 12.

$$\sigma(12) = (1 + 2 + 2^2)(1 + 3) = (7)(4) = 28$$

Indeed, $1 + 2 + 3 + 4 + 6 + 12 = 28$. It might seem like this expression can become difficult to evaluate when n is much larger, but each sum can be evaluated simply using the geometric series formula.

The reason this formula works is because if you expand the product you get the sum of every divisor of n. If you expand the expression given by $\sigma(12)$ you'll get the sum of the every divisor of 12.

Theorem 5 (Product of Divisors)**.** Let the positive integer n have prime factorization

$$n = p_1^{e_1} \cdot p_2^{e_2} \cdots p_k^{e_k}$$

Then the product of the divisors of n is given by

$$d(n) = n^{\tau(n)/2}$$

We can now calculate the product of the divisors of 12. From above, we know $\tau(12) = 6$. Therefore, $d(12) = 12^{6/2} = 12^3$. We can get this same product by direct computation, $(1)(2)(3)(4)(6)(12) = [(1)(12)][(2)(6)][(3)(4)] = (12)(12)(12) = 12^3$.

Notice the method we used above to compute $(1)(2)(3)(4)(6)(12)$. We paired up the divisors of 12 into pairs that multiplied to 12. This is how we'll find a closed form for $d(n)$. Every divisor of n can be paired with another divisor so that their product is n. There are $\tau(n)$ divisors, so we can create $\tau(n)/2$ pairs. Each pair multiplies to n, so the entire product is $d(n) = n^{\tau(n)/2}$. However, this logic only works if n isn't a perfect square, because if n is a perfect square, then what are we supposed to pair $\sqrt{n}$ with? What we can do is find the product of all the numbers that can be paired up, then multiply that product by $\sqrt{n}$ to get the product of the divisors of n. If n is a perfect square, then there are $\tau(n) - 1$ divisors that aren't perfect squares. Hence, there are $(\tau(n)-1)/2$ pairs and the product of the non-$\sqrt{n}$ divisors is $n^{\tau(n)-1)/2}$. After we multiply by $\sqrt{n}$, we get $d(n) = n^{\tau(n)-1)/2} \cdot \sqrt{n} = n^{\tau(n)-1)/2} \cdot n^{1/2} = n^{\tau(n)/2}$. We get the same formula!

Note that we are assured $(\tau(n) - 1)/2$ is an integer because $\tau(n)$ must be odd when n is a perfect square. This is because if n is a perfect square, then the power each prime in the prime factorization is raised to must be even. Thus, $\tau(n)$ is equal to the product of only odd factors and must be odd.

7 Problem-Solving

Example 8. When a positive two-digit number m is multiplied by a positive three-digit number n the result is 21210. Find all possible pairs (m, n). (CEMC)

Solution: The prime factorization of 21210 is $21210 = 2 \cdot 3 \cdot 5 \cdot 6 \cdot 101$. Since m is a two-digit number, it cannot have 101 as a divisor. Therefore, n is a multiple of 101. The prime factorization of n can include at most one 2, at most one 3, at most one 5, and at most one 7.
Since n is a three-digit number, the possible values for n are 101, 202, 303, 505, 606, and 707. The corresponding values for m are 210, 105, 70, 42, 35, and 30, respectively.

Since m is a two-digit number, 210 and 105 are not possible. Therefore, the possible pairs (m, n) are (70,303), (42, 505), (35,606), and (30, 707).
(Solution from CEMC Properties of Numbers)

Example 9. Find $\gcd(6, 24, 39)$

Solution: Finding the GCD of two numbers is the same as finding the GCD of three numbers. First, we find the prime factorization of each number: $6 = 2^1 \cdot 3^1, 24 =$

$2^3 \cdot 3^1, 39 = 3^1 \cdot 13^1$. The only prime that is present in all three PFs is 3 and the minimum power 3 is raised to is 3^1. Hence, $\gcd(6, 24, 39) = 3^1 = \boxed{3}$.

Example 10. There are 10 horses, named Horse 1, Horse 2, ..., Horse 10. They get their names from how many minutes it takes them to run one lap around a circular race track. Horse k runs one lap in exactly k minutes. At time 0 all the horses are together at the starting point on the track at their constant speeds. The least time $S > 0$, in minutes, at which all 10 horses will again simultaneously be at the starting point is $S = 2520$. Let $T > 0$ be the least time, in minutes, such that at least 5 of the horses are again at the starting point. What is the sum of the digits of T?
(2017 AMC 10A)

Solution: Observe that $2520 = \text{lcm}(1, 2, 3, 4, 5, 6, 7, 8, 9, 10)$. This is because the LCM of all the completion rates should be the first time every horse is at the starting simultaneously. This realization should inspire how we should find T. We want to find 5 distinct numbers from $\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$ such that the LCM of the five numbers is as small as possible. By inspection, we find that $\text{lcm}(1, 2, 3, 2 \cdot 2, 2 \cdot 3) = 12$. Therefore $T = 12$, and the sum of the digits is $1 + 2 = \boxed{3}$.
The following identity will be used in the next problem.

Theorem 6. For all positive integers a and b we have

$$\text{lcm}[a, b] \cdot \gcd(a, b) = ab$$

This theorem makes sense given the processes we use to find the GCD and LCM. For a given prime, the GCD takes the least power and the LCM takes the greatest power. Hence, both instances of that prime in prime factorizations of a and b are taken. So, the product of the LCM should have the product the two instances of that prime, just as ab does. This works for every prime in the PFs.

Example 11. If r is a positive integer such that

$$\text{lcm}[r, 100] \cdot \gcd(r, 100) = 13200$$

then what is $\text{lcm}[r, 100]$?
(Alcumus)

Solution: Theorem 6 says

$$13200 = \text{lcm}[r, 100] \cdot \gcd(r, 100) = r \cdot 100$$

Solving the equation yields $r = 132$. We want the value of $\text{lcm}[132, 100]$ so we find the prime factorizations of 132 and 100. $132 = 2^2 \cdot 3 \cdot 11$ and $100 = 2^2 \cdot 5^2$. Then we take the maximum exponent of each prime present in either prime factorization to obtain

$$\text{lcm}[132, 100] = 2^2 \cdot e \cdot 5^2 \cdot 11 = \boxed{3300}$$

Example 12. How many positive integers n are there such that n is a multiple of 5, and the least common multiple of $5!$ and n equals 5 times the greatest common divisor of $10!$ and n?
(2020 AMC 12A)

Solution: We receive the equation

$$\text{lcm}(5!, n) = 5\gcd(10!, n)$$

Then we find the prime factorization of 5! and 10! and the equation becomes

$$\text{lcm}(2^3 \cdot 3 \cdot 5, n) = 5\gcd(2^8 \cdot 3^4 \cdot 5^2 \cdot 7, n)$$

We can now be certain that the only possible prime divisors of n are 2,3,5, and 7. Now we determine the restraints on the powers of the prime factors of n. We do this by considering what values allow the equation to remain true. If the prime factorization of n is

$$n = 2^a \cdot 3^b \cdot 5^c \cdot 7^d$$

we have $a \in [3, 8]$, $b \in [1, 4]$, and $5 \in [0, 1]$. Determining the powers of 5 that are allowed is a little more difficult. The power of 5 on the left side of the initial equation will be 5^1 or c. However, the power of 5 on the right side of the equation is $c + 1$ if $c < 2$ and 3 if $n \geq 2$. Hence, the power of 5 on both sides must be 5^3 and we have $c = 5^3$. This gives 6 choices for a, 4 choices for b, 1 choice for c, and 2 choices for d, giving $6 \cdot 4 \cdot 1 \cdot 2 = \boxed{48}$ possibilities for n.

8 Exercises

Problem 1. A number has exactly eight positive divisors, including one and the number itself. If two of the divisors are 35 and 77, what is the sum of all eight positive divisors?
(CEMC)

Problem 2. Find $\gcd(12, 40, 68)$.

Problem 3. Find $\text{lcm}(4, 35, 39)$

Problem 4. Find the smallest positive integer k such that $504k$ is a perfect square
(CEMC)

Problem 5. What is the least number you can multiply 180 by so that the product is a perfect cube? (Hint: If a number is a perfect nth power, then the exponent of every prime in its prime factorization is a multiple of n)

Problem 6. Let $N = 34 \cdot 34 \cdot 63 \cdot 270$. What is the ratio of the sum of the odd divisors of N to the sum of the even divisors of N?
(2021 AMC 12B)

Problem 7. Let $n = 2^{31}3^{38}$. How many positive integer divisors of n^2 are less than n but do not divide n?
(1995 AIME)

Problem 8. A positive integer n is *nice* if there is a positive integer m with exactly four positive divisors such that the sum of the four divisors is equal to n. How many numbers in the set $\{2010, 2011, 2012, \ldots 2019\}$ are nice?
(2013 AMC 10B)

Problem 9. What is the sum of the exponents of the prime factors of the square root of the largest perfect square that divides 12!?
(2013 AMC 12B)

Problem 10. Let S be the set of all positive integer divisors of 100,000. How many numbers are the product of two distinct elements of S?
(2019 AMC 10B)