Iowa City Math Circle Handouts
Prime Factorizations and Divisors

Ananth Shyamal, Divya Shyamal, Kevin Yang, and Reece Yang

July 18, 2020

1 Definitions and Basic Theorems

Prime numbers and divisibility play a key part in number theory, so it is imperative that you know the following definitions well.

Definition. Let a and b be two natural numbers. If for some natural numbers a, b, and k such that $a = kb$, then we say that b divides a, or $b|a$, and that b is a *divisor* of a.

From this definition, we have the following propositions.

Proposition 1.1. *If a divides b and b divides c, then a divides c for natural numbers a, b, and c.*

Proof. Since a divides b, $b = ka$ for some natural number k. Additionally, since b divides c, $c = mb$ for some natural number m. Combining these, we have $c = (mk)a$. Since mk is a natural number, we get that a divides c. □

Proposition 1.2. *Let a, b, and c be natural numbers such that a divides both b and c. Then a divides $b + c$.*

Proof. Since a divides b, $b = ka$ for some natural number k. Additionally, since a divides c, $c = ma$ for some natural number m. Combining these, we have $b + c = ka + ma = (m + k)a$. Since $m + k$ is a natural number, we get that a divides $b + c$. □

Definition. Two positive integers are said to be relatively prime if they share no common divisors other than 1.

Definition. Any integer greater than one whose only divisors are itself and 1 is called a *prime number*. The non-prime integers greater than one are called *composite*.

2 is the only even prime, and 2, 3, 5, 7, and 11 are the first 5 prime numbers. Now, you may be wondering how to quickly check if a number is prime or not. One way is to use standard divisibility and modular arithmetic techniques to quickly check divisibility of numbers, but using those techniques blindly forces us to check whether all the numbers less than n (or $\frac{n}{2}$) are divisors.

It turns out that it is sufficient to only check whether the first $\lfloor\sqrt{n}\rfloor$ (i.e. the greatest integer less than or equal to $\sqrt{n}$) numbers for divisibility to determine if n is prime. Why? We pursue a proof by contradiction.

Let suppose that n is not prime (i.e. composite for $n > 1$) and none of the positive integers less than or equal to $\lfloor\sqrt{n}\rfloor$ (besides 1) are divisors. That must mean that there exists an integer m, where $n > m > \sqrt{n}$, such that m is a divisor of n. This implies that there exists a natural number k such that $n = km$. Notice that $k < \sqrt{n}$, because otherwise km would be larger than n. Notice that $n = km$ implies that k is a divisor of n. But since $k < \sqrt{n}$, this contradicts our assumption. Hence, an integer greater than one is composite if and only if it has a divisor (besides 1) that is less than or equal to $\lfloor\sqrt{n}\rfloor$, and it is sufficient to check up until $\lfloor\sqrt{n}\rfloor$ for divisibility to check primality.

So now, we have a reasonable fast way to check for whether a number is prime. Later, we'll see that we can generalize this to find the prime factors of a number quickly. Next, we'll discuss an important result that gives rise to the notion of prime factorizations.

Proposition 1.3. *(Fundamental Theorem of Arithmetic) Every non-prime (composite) positive integer greater than one can be uniquely written as a product of primes. This decomposition of a number is called the number's prime factorization.*

Now, we are ready to prove the following fundamental result regarding primes.

Proposition 1.4. *There are infinitely many primes.*

Proof. First, let's assume that there exist only n primes for the sake of contradiction. Denote the primes by $p_1, p_2, \ldots, p_n$. Now consider the number $p_1 p_2 \cdot \cdots \cdot p_n + 1$. This number is not divisible by any of the existing primes, because when divided by them, there will always be a remainder of 1. Thus, $p_1 p_2 \cdots p_n + 1$ must be prime, which contradicts our assumption. Therefore there are an infinite number of primes. □

Let's take a look at a few more results on prime factorizations.

Proposition 1.5. *Let n be a positive integer with factorization*

$$n = p_1^{a_1} \cdot p_2^{a_2} \cdot \cdots \cdot p_k^{a_k}$$

Let d be a positive integer with prime factorization

$$d = p_1^{b_1} \cdot p_2^{b_2} \cdot \cdots \cdot p_j^{b_j}$$

Then $d|n$ iff $j \leq k$ and $b_i \leq a_i$ for all $1 \leq i \leq j$.

Proof. For the sake of contradiction, suppose that there exists a k such that $b_k > a_k$. Then $p_k^{b_k}$ divides d. In order for $p_k^{b_k}$ to also divide n, we must have that p_k divides $\frac{n}{p_k^{a_k}}$. But since prime numbers are relatively prime, this can't happen. Therefore, the result holds. □

Proposition 1.6. *Let n be a positive integer with prime factorization*

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

where the p_i's are distinct prime numbers and the e_i's are nonnegative integers. Then

1. *The number of divisors of n is*

$$(e_1 + 1)(e_2 + 1) \cdots (e_k + 1).$$

2. *The sum of all the positive divisors of n is*

$$\left(1 + p_1 + p_1^2 + \cdots + p_1^{e_1}\right)\left(1 + p_2 + p_2^2 + \cdots + p_2^{e_2}\right) \cdots \left(1 + p_k + p_k^2 + \cdots + p_k^{e_k}\right).$$

We can simplify each multiplicand of this expression using the formula for the sum of a geometric sequence.

Proof. To prove the first part of Proposition 5.4, we may use Proposition 5.3. All divisors of n must be of the form

$$d = p_1^{b_1} \cdot {}_2^{b_2} \ldots p_k^{b_k}$$

where $b_i \leq e_i$ for $i = 1, 2 \ldots k$. Additionally, all numbers of this form will divide n. Hence, the number of divisors of n is the number of ways we can assign nonnegative, integer values to the b_i's such that $b_i \leq e_i$ for $i = 1, 2 \ldots k$. For each i, b_i can take on values $0, 1 \ldots e_i$. Hence, b_i can take on $e_i + 1$ values. Therefore, the number of divisors of n is

$$\prod_{i=1}^{k}(e_i + 1) = (e_1 + 1)(e_2 + 1) \ldots (e_k + 1)$$

as desired. □

Example 1.1. Consider the number 315. Find its prime factorization, its number of divisors, and the sum of its divisors.

Solution. Notice that

$$315 = 5 \cdot 63 = 5 \cdot 7 \cdot 9 = 3^2 \cdot 5 \cdot 7,$$

so the prime factorization of 315 is $3^2 \cdot 5 \cdot 7$.

By the formula above, the number of divisors is

$$(2 + 1)(1 + 1)(1 + 1) = 12$$

and the sum of divisors is

$$\left(1 + 3 + 3^2\right)(1 + 5)(1 + 7) = 13 \cdot 6 \cdot 8 = 624.$$

△

The above proposition gives us a rather simple but useful fact: the number of divisors of a positive integer is odd if and only if the number is a perfect square.

Checkpoint 1.1. Find the prime factorization of 540. Then, compute its number of divisors and the sum of its divisors.

Checkpoint 1.2. Calculate the number of even and odd divisors of 1200.

Example 1.2. How many positive integers have exactly three proper divisors (positive integral divisors excluding itself), each of which is less than 50? *Source: AIME*

Solution. If a number has exactly 3 proper divisors, then it has 4 divisors in total. This means that the exponents of its prime factorization must satisfy $(e_1+1)(e_2+1)\dots(e_k+1) = 4 = 2^2$. This happens when we have a single exponent of 3, or two exponents of 1. In other words, our number can be written in the form p_1^3 or $p_1 \cdot p_2$. Let us look at the first case: our number is of the form p_1^3. We must have each of our proper divisors, or $1, p_1$,and p_1^2 to be less than 50. This means that we must have $p_1 \leq 7$, giving us that $p_1 = 2, 3, 5$, or 7. So there are 4 numbers for this case.

Our next case is when the number can be written as p_1p_2. The proper divisors of this number are $1, p_1$, and p_2, all of which must be less than 50. Let us denote the number of primes less than 50 as n. We need to choose two primes less than 50, for our values of p_1 and p_2. Therefore, there are $\binom{n}{2}$ numbers for this case, for a total of $4 + \binom{n}{2}$ such numbers.

We can calculate that there are 15 primes less than 50, by listing them out. Therefore, our final answer is $4 + \frac{15 \cdot 14}{2} = \boxed{109}$. △

2 GCD and LCM

We start off with the definitions of the lcm and gcd of two numbers.

Definition. We use the notation $\gcd(a, b)$ to denote the greatest common divisor of a and b. Also, $\text{lcm}(a, b)$ denotes the least common multiple of a and b (i.e. the least natural number whose set of divisors contains a and b).

Note that from the above definitions, if a and b are relatively prime, then $\gcd(a, b) = 1$ and $\text{lcm}(a, b) = ab$. Additionally, if $b|a$ then $\text{lcm}(a, b) = a$.Given the prime factorization of two numbers, we can find their lcm and gcd.

Proposition 2.1. *Let m and n be positive integers with prime factorizations*

$$m = p_1^{a_1} \cdot p_2^{a_2} \cdot \dots \cdot p_i^{a_i}$$

and

$$n = p_1^{b_1} \cdot p_2^{b_2} \cdot \dots \cdot p_j^{b_j},$$

where p_k is the kth prime number, the a_k's and b_k's are nonnegative integers, and p_i and p_j are the largest prime divisors of m and n, respectively. Without loss of generality, let $i \geq j$. For all $k \in \{j+1, j+2, \ldots i\}$, let $b_k = 0$. Then

$$\operatorname{lcm}(m,n) = p_1^{\max(a_1,b_1)} \cdot p_2^{\max(a_2,b_2)} \cdot \cdots \cdot p_i^{\max(a_i,b_i)}$$

and

$$\gcd(m,n) = p_1^{\min(a_1,b_1)} \cdot p_2^{\min(a_2,b_2)} \cdot \cdots \cdot p_j^{\min(a_j,b_j)}.$$

Example 2.1. Find $\gcd(630, 1500)$ and $\operatorname{lcm}(630, 1500)$.

Solution. We first compute the prime factorizations of 630 and 1500 as

$$630 = 2 \cdot 3^2 \cdot 5 \cdot 7$$

and

$$1500 = 2^2 \cdot 3 \cdot 5^3.$$

Using these, we get

$$\begin{aligned} \operatorname{lcm}(630, 1500) &= 2^{\max(1,2)} \cdot 3^{\max(2,1)} \cdot 5^{\max(1,3)} \cdot 7^{\max(1,0)} \\ &= 2^2 \cdot 3^2 \cdot 5^3 \cdot 7 \\ &= 31500 \end{aligned}$$

and

$$\begin{aligned} \gcd(630, 1500) &= 2^{\min(1,2)} \cdot 3^{\min(2,1)} \cdot 5^{\min(1,3)} \\ &= 2 \cdot 3 \cdot 5 \\ &= 30. \end{aligned}$$

△

The previous proposition gives rise to the following proposition, which can be very useful in number theory problems.

Proposition 2.2. *For positive integers m and n,*

$$m \cdot n = \gcd(m,n) \cdot \operatorname{lcm}(m,n).$$

Proof. Let

$$m = p_1^{a_1} \cdot p_2^{a_2} \cdot \cdots \cdot p_i^{a_i}$$

and

$$n = p_1^{b_1} \cdot p_2^{b_2} \cdot \cdots \cdot p_i^{b_i}.$$

We know that

$$\operatorname{lcm}(m,n) = p_1^{\max(a_1,b_1)} \cdot p_2^{\max(a_2,b_2)} \cdot \cdots \cdot p_i^{\max(a_i,b_i)}$$

and

$$\gcd(m,n) = p_1^{\min(a_1,b_1)} \cdot p_2^{\min(a_2,b_2)} \cdot \cdots \cdot p_i^{\min(a_i,b_i)}.$$

Then

$$\gcd(m,n)\cdot\operatorname{lcm}(m,n)=p_1^{\max(a_1,b_1)+\min(a_1,b_1)}\cdot p_2^{\max(a_2,b_2)+\min(a_2,b_2)}\cdot\cdots\cdot p_i^{\max(a_i,b_i)+\min(a_i,b_i)}.$$

Since $\max(a_k,b_k)+\min(a_k,b_k)=a_k+b_k$, this is equal to

$$p_1^{a_1+b_1}\cdot p_2^{a_2+b_2}\cdot\cdots\cdot p_i^{a_i+b_i},$$

which equals $m\cdot n$. □

Now, let's try the following example, which will test your knowledge on the lcm and gcd.

Example 2.2. How many ordered triples (x,y,z) of positive integers satisfy $\operatorname{lcm}(x,y)=72$, $\operatorname{lcm}(x,z)=600$ and $\operatorname{lcm}(y,z)=900$? *Source: AMC 10*

Solution. First let's factorize the numbers in the problem: $72=2^3\cdot3^2$, $600=2^3\cdot3\cdot5^2$, and $900=2^2\cdot3^2\cdot5^2$. The factorizations of these numbers are all in terms of 2, 3, and 5 so let's write $x=2^a3^b5^c$, $y=2^d3^e5^f$, and $z=2^g3^h5^i$, where $a,b,\cdots,i$ are non-negative integers. Notice that x, y, and z can't be multiples of other primes as then those primes wouldn't divide the lcm. From this, we get the following equations.

$$\max(a,d)=3,\quad \max(b,e)=2,\quad \max(a,g)=3,\quad \max(b,h)=1,\quad \max(c,i)=2,$$

$$\max(d,g)=2,\quad \max(e,h)=2,\quad \max(f,i)=2.$$

We can't have $d=3$ as that would contradict the sixth equation. By the first equation, this implies that $a=3$. Furthermore, we can't have $b=2$ as that would contradict the fourth equation. By the second equation, this implies that $e=2$. So now, we've gotten everything out of the equations involving a and e. Since 72 isn't divisible by 5, have that $c=f=0$. This implies that $i=2$.

So now, the only equations we've yet to use fully are the fourth and sixth equations. Hence we take cases. By the fourth equation, $(b,h)=(1,1),(1,0)$, or $(0,1)$ and $(d,g)=(2,2),(2,1),(2,0),(0,2)$, or $(1,2)$. Notice that all these cases satisfy the other equations. Since the cases for (b,h) are independent from those for (d,g), or answer is simply $3\cdot5=\boxed{15}$.

△

Checkpoint 2.1. Compute the least common multiple of 9999 and 100,001. *Source: AoPS*

3 Euclidean Division Algorithm

We start of with a result that is behind the Euclidean division algorithm.

Proposition 3.1. *Let m and n be positive integers with $m > n$ and let r be the remainder when m is divided by n. Then*

$$\gcd(m, n) = \gcd(m - n, n) = \gcd(m - nk, n) = \gcd(r, n).$$

for any integer k.

The Euclidean algorithm repeatedly simplifies the expression $\gcd(m, n)$ using the above result.

Example 3.1. Find $\gcd(1374, 141)$.

Solution. Applying the Euclidean division algorithm multiple times, we get

$$\begin{aligned}
\gcd(1374, 141) &= \gcd(1374 \pmod{141}, 141) \\
&= \gcd(105, 141) \\
&= \gcd(36, 105) \\
&= \gcd(105 \pmod{36}, 36) \\
&= \gcd(33, 36) \\
&= \gcd(3, 33) \\
&= \boxed{3}.
\end{aligned}$$

△

We will now demonstrate the Euclidean division algorithm more generally. Let a and b be integers with $a > b$. Then we may write:

$$\begin{aligned}
a &= bq_1 + r_1 \\
b &= r_1 q_2 + r_2 \\
r_1 &= r_2 q_3 + r_3 \\
&\vdots \\
r_{k-2} &= r_{k-1} q_k + r_k \\
r_{k-1} &= r_k q_{k+1} + r_{k+1}.
\end{aligned}$$

Since all r_n are nonnegative and $r_1 > r_2 > \cdots > r_{k+1}$, there must be some i such that $r_{i+1} = 0$. For this i, $\gcd(a, b) = r_i$.

Example 3.2. The numbers in the sequence 101, 104, 109, 116,... are of the form $a_n = 100 + n^2$, where $n = 1, 2, 3, \ldots$ For each n, let d_n be the greatest common divisor of a_n and a_{n+1}. Find the maximum value of d_n as n ranges through the positive integers. *Source: AIME*

Solution. We are given that

$$\begin{aligned} d_n &= \gcd(a_n, a_{n+1}) \\ &= \gcd(100 + n^2, 100 + (n+1)^2) \\ &= \gcd(100 + n^2, 101 + 2n + n^2). \end{aligned}$$

Now, let's see if we can simplify this using the Euclidean algorithm. We have

$$\begin{aligned} \gcd(100 + n^2, 101 + 2n + n^2) &= \gcd(100 + n^2, (101 + 2n + n^2) - (100 + n^2)) \\ &= \gcd(100 + n^2, 2n + 1). \end{aligned}$$

This doesn't look too nice. However, note that $2n + 1$ is always odd. This means that $\gcd(100 + n^2, 2n + 1) = \gcd(4 \cdot (100 + n^2), 2n + 1)$, because $\gcd(4, 2n + 1) = 1$. The reason we prefer to deal with $400 + 4n^2$ is because now, we can use Euclid's algorithm again! We have

$$\begin{aligned} \gcd(4 \cdot (100 + n^2), 2n + 1) &= \gcd(400 + 4n^2, 2n + 1) \\ &= \gcd(400 + 4n^2 - (2n + 1) \cdot (2n + 1), 2n + 1) \\ &= \gcd(399 - 4n, 2n + 1) \\ &= \gcd(399 - 4n - (2n + 1) \cdot (-2), 2n + 1) \\ &= \gcd(401, 2n + 1). \end{aligned}$$

In this string of simplifications, our goal was to sequentially eliminate the term of highest degree. First, we eliminated n^2, and then we eliminated n in one of the remaining terms. Now, the problem asks us to maximize $\gcd(401, 2n + 1)$. Clearly, this value cannot exceed 401 because any number greater than 401 will not divide 401. But can we find a value of n such that $\gcd(401, 2n + 1) = 401$? We can! Setting $2n + 1 = 401$, or $n = 200$, we have $\gcd(401, 401) = 401$. Therefore, the maximum value d_n can attain is $\boxed{401}$. △

Checkpoint 3.1. What is the greatest common divisor of 1407 and 903? *Source: AoPS*

4 Chicken McNugget Theorem

Proposition 4.1. *(Chicken McNugget Theorem) Let m and n be relatively prime positive integers greater than one. Then*

1. *The greatest positive integer that cannot be written in the form $p \cdot m + q \cdot n$, where p and q are non-negative integers, is $mn - (m + n)$.*
2. *The number of positive integers that cannot be written as a linear combination of m and n is $\frac{(m-1)(n-1)}{2}$.*

Example 4.1. Chicken McNuggets can be purchased in boxes of 5 and 12. Find the largest number of McNuggets that cannot be purchased.

Solution. According to the Chicken McNugget Theorem, the maximum number of McNuggets that cannot be purchased is $5 \cdot 12 - (5 + 12) = 43$. △

Example 4.2. What is the largest integer that cannot be written as a sum of a whole number (possibly zero) of 8.5's and a whole number (possibly zero) of 11's? *Source: MPfG*

Solution. Note that we can not directly apply Chicken McNugget's theorem here, because 8.5 is not an integer. The problem asks for the largest integer that cannot be written in the form $8.5p + 11q$ for whole numbers p and q. However, not all whole number p and q will make $8.5p + 11q$ an integer. Specifically, our expression is integral if and only if p is even. This is because if p is odd, we can write $p = 2k + 1$ for some whole number k, and our expression becomes $8.5(2k+1)+11q = 17k+11q+8.5$. This is not an integer, as $17k + 11q$ is always an integer, but 8.5 is not. Therefore, our p must be even, so we can write $p = 2k$ for some whole number k. Substituting this into our expression, we obtain $8.5(2k) + 11q = 17k + 11q$. 17 and 11 are both integers, so we can use the Chicken McNugget Theorem! We have the largest number that cannot be written in this form is $17 \cdot 11 - (17 + 11) = \boxed{159}$. △

Checkpoint 4.1. The town of Hamlet has 3 people for each horse, 4 sheep for each cow, and 3 ducks for each person. What is the greatest possible number that cannot be the total number of people, horses, sheep, cows, and ducks in Hamlet? *Source: AMC*

5 Problems

1. ⋆ What is the ratio of the least common multiple of 180 and 594 to the greatest common factor of 180 and 594? *Source: AMC 8*

2. ⋆ What is the smallest whole number that can be multiplied by 200 such that the product is a perfect cube? *Source: MATHCOUNTS*

3. ⋆ What is the sum of the three positive integers less than 1000 that have exactly five positive integer divisors. *Source: MATHCOUNTS*

4. ⋆ Prove that the fraction $\frac{21n+4}{14n+3}$ is irreducible for every natural number n. *Source: IMO*

5. ⋆ In how many different ways can 900 be expressed as the product of two (possibly equal) positive integers? Regard $m \cdot n$ and $n \cdot m$ as the same product. *Source: Math Prize For Girls*

6. ⋆⋆ Find the sum of all positive integers whose largest *proper* divisor is 55. *Source: HMMT*

7. ⋆⋆ For how many positive integers $n \leq 100$ is it true that $10n$ has exactly three times as many positive divisors as n has. *Source: HMMT*

8. ⋆⋆ A positive integer divisor of 12! is chosen at random. The probability that the divisor chosen is a perfect square can be expressed as $\frac{m}{n}$, where m and n are relatively prime positive integers. What is $m+n$? *Source: AMC*

9. ⋆⋆ For some positive integer n, the number $110n^3$ has 110 positive integer divisors, including 1 and the number $110n^3$. How many positive integer divisors does the number $81n^4$ have? *Source: AMC 10*

10. ⋆⋆ If n is a positive integer such that $2n$ has 28 positive divisors and $3n$ has 30 positive divisors, then how many positive divisors does $6n$ have? *Source: AHSME*

11. ⋆⋆ What is the largest 2-digit prime factor of the integer $\binom{200}{100}$? *Source: AIME*

12. ⋆⋆ How many ordered pairs (a, b) of positive integers satisfy the equation

$$a \cdot b + 63 = 20 \cdot \text{lcm}(a, b) + 12 \cdot \gcd(a, b).$$

Source: AMC 10

13. ⋆⋆ How many positive integer divisors of 2004^{2004} are divisible by exactly 2004 positive integers? *Source: AIME*

14. ⋆⋆ What is the greatest three-digit positive integer n for which the sum of the first n positive integers is <u>not</u> a divisor of the product of the first n positive integers? *Source: AMC*

15. ⋆⋆ How many positive integer divisors of 201^9 are perfect squares or perfect cubes (or both)? *Source: AMC*

16. ⋆⋆ How many positive three-digit integers have a remainder of 2 when divided by 6, a remainder of 5 when divided by 9, and a remainder of 7 when divided by 11? *Source: AMC 8*

17. ⋆⋆ 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? *Source: AMC*

18. ⋆⋆⋆ Let a, b, c, and d be positive integers such that $\gcd(a, b) = 24$, $\gcd(b, c) = 36$, $\gcd(c, d) = 54$, and $70 < \gcd(d, a) < 100$. Which of the following must be a divisor of a? *Source: AMC*

19. ⋆⋆⋆ The numbers in the sequence 101, 104, 109, 116,... are of the form $a_n = 100 + n^2$, where $n = 1, 2, 3, \ldots$ For each n, let d_n be the greatest common divisor of a_n and a_{n+1}. Find the maximum value of d_n as n ranges through the positive integers. *Source: AIME*

20. ⋆⋆⋆ Find the least positive integer n greater than 1000 for which

$$\gcd(63, n + 120) = 21 \quad \text{and} \quad \gcd(n + 63, 120) = 60.$$

Source: AMC

21. $\star\star\star$ Compute the integer n such that $2009 < n < 3009$ and the sum of the odd positive divisors of n is 1024. *Source: ARML*

22. $\star\star\star$ Let k be the least common multiple of the numbers in the set $\mathcal{S} = \{1, 2, \ldots, 30\}$. Determine the number of positive integer divisors of k that are divisible by exactly 28 of the numbers in the set $\mathcal{S}$. *Source: ARML*