Divisibility and Prime Factorization

Chirag Samantaroy

July 15, 2021

Thank you to **Vincent Cheng** for helping me with the handout, specifically writing solutions to some of the examples, and **bissue** for helping proofread the handout.

Contents

1 Introduction

1.1 First off, what is Number Theory?

This handout is the corresponding handout to the first lecture of ALP's Number Theory lecture series. Now, we begin with the question: "What exactly is Number Theory?"

Well, Number Theory is the study of integers and integer-valued functions. It's one of the most beautiful subjects in mathematics.

We first explore Prime Factorization and Divisibility, which provides the basis for GCD & LCM. We also go into Modular Arithmetic, the theory, and the sometimes magical applications on most Number Theory problems. Finally, we go over Base Numbers and Diophantine Equations; while not as popular as the three previously mentioned, it is still worthwhile to learn.

1.2 Some Basic Terms and Notation

We all know the following terms. However, it's good for refreshing our memory on them as we will build on these definitions for the concepts we see in this handout.

- A natural number is ***prime*** if it cannot be expressed as a product of two smaller natural numbers. In other words, its only factors are 1 and the number itself.
- A natural number is ***composite*** if it can be expressed as a product of two smaller natural numbers. In other words, it has multiple factors other than 1 and itself.
- ***Multiples*** of a number are that number multiplied by an integer, implying a multiple of a number is ***divisible*** by that number.
- Note that a divisor of a number can also be called a ***factor*** of that number.
- Two integers are ***coprime*** if the only positive integer that is a divisor of both of them is 1. (This is most commonly referred to as being "relatively prime.")

We finish this section off by introducing some notation.

Notation

- We write $m \mid n$ if m divides n and $m \nmid n$ if m does not divide n.
- We can express $m \mid n$ as $n = am$ for some integer a.

> *Remark 1.1.* When we say "m divides n," we're essentially stating the fact that n is divisible by m.

2 Prime Factorization

Prime Factorization

The ***prime factorization*** of a number n is the representation of n as a product of not necessarily distinct primes, written as

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

where p_i is the ith prime and e_i is the power of p_i in n.

The existence of a prime factorization for every integer implies that you can break down a natural number into its prime number counterparts. We can consider prime numbers to be the building blocks of all integers. This is because we can take primes, this simple unit, and either make it stand on its own or multiply them together to generate any given integer. Now, before moving on, let's briefly examine how we can determine if any given natural number is prime.

2.1 To be prime, or not to be prime, that is the question.

Well, we know that if a natural number p is prime, then it is only divisible by 1 and itself. Therefore, we can check all integers from 2 to $p-1$ to see if they divide p. If not, then we know that p is prime. However, this is very sub-optimal.

Sure, this method works for smaller integers, but the larger a number gets, the more exhaustive you have to be, and soon enough, you'll be midway through when you drop down your head on your desk and start napping. Thus, we need to find a more optimal strategy.

First off, as previously mentioned, primes are the building blocks to all integers. If this is the case, then all of the number's divisors can be broken down as simply prime counterparts. After all, this is the concept of prime factorization.

So, we have our first simplification: instead of checking all integers, we can check only all of the primes from 2 to $p-1$ to see if they divide p. However, this can still be tedious, even if it is progress.

So, we explore something more technical. We know that if $k \mid p$, then $\frac{p}{k} \mid p$. We know that because p cannot be a perfect square, then we know for sure that one of either k or $\frac{p}{k}$ is less than $\sqrt{p}$. Noting that, if $\frac{p}{k}$ is an integer equal to 1, then we know for sure that p is composite.

So, we have our second and final simplification: instead of checking all of the primes from 2 to $p-1$, we check only all of the primes from 2 to $\lceil \sqrt{p} \rceil$.

We can't do much from here, but rest assured this is probably satisfactory for our purposes.

Example 2.1
Prove that 23 is prime.

Proof. Immediately, we calculate $\lceil \sqrt{23} \rceil$ to get 5. Wow, this is nice: there are only 3 primes from 2 to 5 (namely, $2, 3$, and 5). We proceed to check each prime to see if they divide 23.

Obviously, it cannot be divisible by 2 as the units digit of 23 is 3, which is not even. It also can't be divisible by 5, as the units digit (3) is neither 0 nor 5. So, the only prime left to check is 3. Performing, simple division, we can see 3 does not divide 23, as it leaves a remainder of 2. Therefore, we've exhausted all cases, and our proof is complete. □

This was a trivial example. However, now you understand how to determine whether a natural number is prime or composite. Also, notice that this system we use to do this is much more optimal than checking all integers greater than or equal to 2 but less than or equal to $p - 1$. Given this, we can move on to the next section.

> *Remark 2.2.* For your convenience, here is a list of prime numbers up to 100:
>
> $$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97.$$
>
> Note: it is a common mistake to think 91 is prime, but keep in mind that $91 = 7 \cdot 13$!

2.2 Fundamental Theorem of Arithmetic

We know that all natural numbers can be represented as a product of primes (in other words, a prime factorization). However, the Fundamental Theorem of Arithmetic builds off of that idea.

Theorem 2.3 (Fundamental Theorem of Arithmetic)
The ***Fundamental Theorem of Arithmetic*** states that every integer has a unique prime factorization up to (except for) the order of the factors.

This allows us to gain more information about the divisors. You'll see the importance of this later on.

2.3 Problem Solving

Example 2.4 (1998 AHSME)
If 1998 is written as a product of two positive integers whose difference is as small as possible, then what is the difference?

Solution. The two positive integers must be as close to $\sqrt{1998}$ as possible to minimize the difference as much as possible. We note that $\sqrt{1998} \approx 44$ to 45. Prime factorizing 1998:

$$1998 = 2 \cdot 3^3 \cdot 37.$$

As you see, 37 is really close to 44, and no number between 38 and 44 is a factor of 1998. So, we have $2 \cdot 3^3 = 54$ as the other positive integer. Their difference is $54 - 37 = \boxed{17}$. □

Example 2.5 (2000 AIME I)
Find the least positive integer n such that no matter how 10^n is expressed as the product of any two positive integers, at least one of these two integers contains the digit 0.

Solution. Suppose a positive integer that is a factor of 10^n has both a 2 and a 5 in its prime factorization. Then, it will end in a 0. So, all that's left to consider is when the factors do not have both a 2 and a 5. (In other words, it's separated.)

We test from $n = 1$ till at least one of 2^n, and 5^n has a digit of 0. Doing so, we find that when $n = 8$, then $2^8 = 256$ and $5^8 = 390625$. As you can see, the latter has a digit of 0. Therefore, our answer is $\boxed{8}$. □

Example 2.6 (1983 AIME)
What is the largest 2-digit prime factor of the integer $n = \binom{200}{100}$?

Solution. By the definition of combinations:

$$\binom{200}{100} = \frac{200!}{100!100!} = \frac{200 \cdot 199 \cdots 101}{100 \cdot 99 \cdots 1}.$$

If we try the largest two-digit primes such as 97, we'll see that the top and bottom both have a factor of 97, so they cancel out. So, our goal is to find a two-digit prime that appears twice in the numerator and only once in the denominator. If we call this prime n, we know that

$$3n \leq 200, 2n \geq 100.$$

This way, we will have one copy of the two-digit prime in the denominator and two of n in the numerator. We can simplify the inequalities to

$$20 \leq n \leq \frac{200}{3}.$$

After some quick checking, we can see that the largest prime that fits inside these conditions is $\boxed{61}$. □

Example 2.7 (2001 AMC 12)
Four positive integers a, b, c, and d have a product of $8!$ and satisfy:

$$\begin{aligned} ab + a + b &= 524 \\ bc + b + c &= 146 \\ cd + c + d &= 104 \end{aligned}$$

What is $a - d$?

Solution. We factor like so:

$$\begin{aligned} (a+1)(b+1) &= 525, \\ (b+1)(c+1) &= 147, \\ (c+1)(d+1) &= 105. \end{aligned}$$

> *Remark 2.8.* You can check that this factorization works right now. We will expand on this idea (known as SFFT, Simon's Favorite Factoring Trick) in a future handout.

We prime-factorize each of the numbers on the right-hand side:

$$\begin{aligned}525 &= 3 \cdot 5^2 \cdot 7,\\ 147 &= 3 \cdot 7^2,\\ 105 &= 3 \cdot 5 \cdot 7.\end{aligned}$$

As you can see, 7^2 divides $(b+1)(c+1) = 147$. However, 7^2 does not divide neither $(a+1)(b+1) = 525$ nor $(b+1)(c+1) = 105$. So, both the quantities $b+1$ and $c+1$ have a maximum of 1 factor of 7 each. So, either $(b+1, c+1) = (7, 21)$ or $(21, 7)$, because one of the two must also have a factor of 3.

Now, this leaves us with two possibilities. Either:

$$(a+1, b+1, c+1, d+1) = (75, 7, 21, 5) \Rightarrow (a, b, c, d) = (74, 6, 20, 4)$$

Or:

$$(a+1, b+1, c+1, d+1) = (25, 21, 7, 15) \Rightarrow (a, b, c, d) = (24, 20, 6, 14).$$

Well, note the restriction that $abcd = 8!$. (In case you don't know, $8! = 8 \cdot 7 \cdots 2 \cdot 1$.) Well, without having to multiply out $abcd$ for each possibility, we can simply note that none of a, b, c or d has a factor of 7 in the scenario where $(a, b, c, d) = (74, 6, 20, 4)$. So, it's virtually impossible for $abcd$ to multiply to $8!$ in this case, and therefore only the case $(a, b, c, d) = (24, 20, 6, 14)$ works.

So, our answer is $24 - 14 = \boxed{10}$. □

> *Remark 2.9.* If there is ever a time when you're in doubt regarding really anything about a problem, go ahead and re-read it. You might catch something you forgot or didn't read that may appear useful.

3 Number and Sum of Divisors

3.1 Propositions

In this section, we cover the propositions of the Number and Sum of Divisors.

Proposition 3.1 (Number of Divisors)
If a number n has the prime factorization

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

then the number of divisors n has is

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

Proof. Any divisor of
$$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$$
is of the form $p_1^{a_1} p_2^{a_2} \cdots p_k^{e_k}$ for some

$$a_1 \in \{0, 1, \ldots, e_1 - 1, e_1\}, a_2 \in \{0, 1, \ldots, e_2 - 1, e_2\},$$

and so on and so forth till $a_k \in \{0, 1, \ldots, e_k - 1, e_k\}$. (Why?) Hence, there are $e_1 + 1$ choices for a_1, $e_2 + 1$ choices for a_2, and so on and so forth, for a total of

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

divisors. □

Proposition 3.2 (Sum of Divisors)
If a number n has the prime factorization

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

then the sum of the divisors of n is

$$\sigma(n) = (1 + p_1 + \cdots + p_1^{e_1})(1 + p_2 + \cdots + p_2^{k_2}) \cdots (1 + p_k + \cdots + p_k^{e_k}).$$

Exercise 3.3. Prove Proposition 3.2.

3.2 Problem Solving

Example 3.4 (2005 AMC 10A)
How many positive cubes divide $3! \cdot 5! \cdot 7!$?

Solution. We can simplify the term, $N = 3! \cdot 5! \cdot 7!$, by writing out its prime factorization. We get
$$N = 2^8 \cdot 3^4 \cdot 5^2 \cdot 7.$$
We know 5 and 7 cannot be part of the cubes that divide N; there are less than 3 of both of them. We know that the exponent of a cube is always a multiple of 3. So, we can think of the remaining N as
$$2^6 \cdot 3^3.$$
Now, we can think of them in increments of 3 because we need the exponents to be a multiple of three. So we let $A = 2^3$ and $B = 3^3$. Therefore, our N becomes

$$A^2 \cdot B.$$

Now, we count the number of factors this has while is $(2 + 1)(1 + 1) = 6$. □

Example 3.5 (1990 AIME)
Let n be the smallest positive integer that is a multiple of 75 and has exactly 75 positive integral divisors, including 1 and itself. Find $\frac{n}{75}$.

Solution. We start by noting the prime factorization of 75 is $3 \cdot 5^2$. So, for n to be a multiple of 75, it must have 3 and 5 as two of its prime factors. Also, since we want n to be as small as possible, we may as well introduce its third prime factor: 2.

So now, we know that n is in the form $2^a 3^b 5^c$. If we want n to have 75 integral factors, including 1 and itself, then we know that $(a+1)(b+1)(c+1) = 75$ must be true. Since 5 is the greatest prime factor of all of them, then we want it's exponent, c, in the prime factorization of n to be minimized.

Since the smallest prime factor of 75 is 3, and in it's representation 3 is not raised to any power, we let $c + 1 = 3 \implies c = 2$. Now, we have two factors of 5 left. To deal with this, we evenly distribute both of them to the quantities $a+1$ and $b+1$. Therefore, $a = b = 4$. So, $n = 2^4 \cdot 3^4 \cdot 5^2$. Dividing this by $75 = 3 \cdot 5^2$, our answer is $\boxed{432}$. □

Remark 3.6. Always note that multiples of a number build off of that number's prime factorization.

Example 3.7 (2017 AMC 12B)
The number $21! = 51,090,942,171,709,440,000$ has over $60,000$ positive integer divisors. One of them is chosen at random. What is the probability that it is odd?

Solution. Writing this number in it's prime factorization would be much prettier, so that is what we do. This can be done through some quick counting.

$$2^{18} \cdot 3^9 \cdot 5^4 \cdot 7^3 \cdot 11 \cdot 13 \cdot 17 \cdot 19.$$

The probability that a factor is odd can be calculated by the number of odd divisors divided by the total number of divisors. The total number of odd divisors can be thought of as a factor of

$$M = 3^9 \cdot 5^4 \cdot 7^3 \cdot 11 \cdot 13 \cdot 17 \cdot 19,$$

because we want the number to be a factor of 21! and it cannot have 2 as a factor. We can count the number of factors to M to get

$$(9+1)(4+1)(3+1)(1+1)(1+1)(1+1)(1+1).$$

We can then count the number of factors of 21! to get

$$(18+1)(9+1)(4+1)(3+1)(1+1)(1+1)(1+1)(1+1).$$

So we end with the probability

$$\frac{(9+1)(4+1)(3+1)(1+1)(1+1)(1+1)(1+1)}{(18+1)(9+1)(4+1)(3+1)(1+1)(1+1)(1+1)(1+1)},$$

and canceling terms, we get that the answer is $\frac{1}{(1+18)} = \boxed{\frac{1}{19}}$. □

Remark 3.8. There exists a much quicker solution to this problem if you look carefully enough. Try to find it on your own!

4 Problems

Minimum is [11 ♟]. Problems denoted with ♜ are required. (They still count towards the point total.)

> "Some numbers, even large ones, have no factors - except themselves, of course, and 1. These are called prime numbers, because everything they are starts with themselves. They are original, gnarled, unpredictable, the freaks of the number world."
>
> *Richard Friedberg*

[3 ♟] Problem 1 (2007 PUMaC). If you multiply all positive integer factors of 24, you get 24^x. Find x.

[4 ♟] Problem 2 (2011 PUMaC). The only prime factors of an integer n are 2 and 3. If the sum of the divisors of n (including itself) is 1815, find n.

[5 ♟] Problem 3 (2013 PUMaC). How many factors of $(20^{12})^2$ less than 20^{12} are not factors of 20^{12} ?

[5 ♟] Problem 4 (2020 AIME I). Let S be the set of positive integers N with the property that the last four digits of N are 2020, and when the last four digits are removed, the result is a divisor of N. For example, $42,020$ is in S because 4 is a divisor of $42,020$. Find the sum of all the digits of all the numbers in S. For example, the number $42,020$ contributes $4+2+0+2+0=8$ to this total.

[6 ♟] Problem 5 (2013 AMC 10B). A positive integer n is nice if there is a positive integer m with exactly four positive divisors (including 1 and m) 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?

[6 ♟] Problem 6 (2019 AIME I). Let $\tau(n)$ denote the number of positive integer divisors of n. Find the sum of the six least positive integers n that are solutions to $\tau(n)+\tau(n+1)=7$.