Number Theory 101

Graham Middle School Math Olympiad Team

NUMBER THEORY DEFINITIONS

Counting Numbers = $\{1,\ 2,\ 3,\ ...\}$ are the numbers we use for counting.
(Yes, this is the definition.)
The brackets here mean "the set including."
Mathematicians use $\mathbb{N}$ as the symbol for this set.

Whole Numbers = $\{0,\ 1,\ 2,\ 3,\ ...\}$, so this is the set of counting numbers plus the element zero.
Mathematicians use $\mathbb{N}_0$ or $\mathbb{Z}_+$ as the symbol for this set.

Integers = $\{..., -3, -2, -1, 0, +1, +2, +3, ...\}$, so this set includes negative numbers as well.
Mathematicians use $\mathbb{Z}$ as the symbol for this set.

The study of math, which involves the properties of integers, is called **Number Theory**.

A **prime number** (also a **prime**) is a counting number with exactly two different factors, namely the number itself and the number 1.
First 10 prime numbers:

$$2,\ 3,\ 5,\ 7,\ 11,\ 13,\ 17,\ 19,\ 23,\ 29,\ ....$$

Note that 2 is the only even prime.

A **composite number** is a counting number that has *at least three* different factors.

The **number** 1 is *neither prime nor composite* since it has exactly one factor.

As a result, all counting numbers are split into 3 groups:

- prime numbers,
- composite numbers, and
- the group with only number 1.

PRIME FACTORIZATION

All counting numbers may be presented as a product of prime numbers. The existence and uniqueness of this presentation are proven by the **fundamental theorem of arithmetic**.
The process of presenting a number as a product of prime numbers is called **prime factorization**.

Factor 5720?

We already know the divisibility rules for prime numbers 2, 3, 5, and 11. Let's apply them.
First we see that 5720 is divisible by 2. Let's do that: $5720 \div 2 = 2860$.
2860 is also divisible by 2: $2860 \div 2 = 1430$.
Continue: $1430 \div 2 = 715$.
715 is no longer divisible by 2. Let's try whether it is divisible by 3. No luck, since $7 + 1 + 5 = 13$, which isn't divisible by 3.
It ends in 5, so it is divisible by 5: $715 \div 5 = 143$. Then check whether it is divisible by 7, the remainder is 3.
Then check it is divisible by 11: $143 \div 11 = 13$, which is already a prime number. So

$$5720 = 2 \times 2 \times 2 \times 5 \times 11 \times 13 = 2^3 \times 5 \times 11 \times 13.$$

Tips and tricks: It is easy to find the prime factors when factors are 2, 3, 5, or 11. But what if you've already extracted them, but are still not sure whether a *remainder number* is prime or composite?

1. Check the *last digit* if it is even or 5. Check a *sum* and an *alternating sum* of numbers, probably it is still divisible by 3 or 11.
2. Then try to divide it by the successive primes: 7, 13, 17, 19, 23, 29, etc. If the last prime you've been attempting to divide by being squared is bigger than your number, your number is a prime. That means you don't need to try primes bigger than 7 for numbers less than 100 since $11 \times 11 > 100$ already.
3. Organize your calculations into something like this:

5720	2
2860	2
1430	2
715	5
143	11
13	13

$$\begin{array}{r} 13 \\ 11\overline{)143} \\ 5\overline{)715} \\ 2\overline{)1430} \\ 2\overline{)2860} \\ 2\overline{)5720} \end{array}$$

GREATEST COMMON DIVISOR

Coach Barak wants to set up Teamattack teams, But he doesn't know how many students will attend class: 24 or 30. What is the **greatest** number of teams he should arrange, so each team has equal numbers of participants?

If he knows for sure there will be 24 students, he may arrange 1, 2, 3, 4, 6, 8, 12, and 24 student teams.
If it would be 30 students, 1, 2, 3, 5, 6, 10, 15 and 30 student teams are possible.
The greatest number present in both lists is 6, so coach Barak should arrange 6 teams.

The number we just found is called

The **Greatest Common Divisor (GCD)** of two counting numbers is the largest counting number that *divides each* of the two given numbers.

The GCD of two number is often denoted as $\gcd(a,\ b)$ or simply (in some context) $(a,\ b)$.

You've already met the Greatest Common Divisor when study reducing of common fractions.

In the name "greatest common divisor", the adjective "greatest" may be replaced by "highest", and the word "divisor" may be replaced by "factor", so that other names include **greatest common factor (GCF)**, etc. Historically, other names for the same concept have included the *greatest common measure*.

FINDING GREATEST COMMON DIVISOR

To find the **GCD** of two numbers, it is often helpful to perform a **prime factorization** of the numbers.

The GCD is the **product of all of shared prime factors** of numbers.

What is the GCD of 144 and 900?

$$144 = 2^4 \cdot 3^2, \qquad 900 = 2^2 \cdot 3^2 \cdot 5^2.$$

From their prime factorizations, we see that 144 and 900 share two factors of 2 and two factors of 3, so $\gcd(144,\ 900) = 2^2 \cdot 3^2 = 36$.

If the GCD of two numbers is 1, we say the numbers are relatively prime or **coprime**.

For example, neither 35 nor 12 is a prime number, but they are coprime.

A prime factorization of huge numbers is a super hard problem. In fact, modern computer security is based that no one can factor huge numbers in a reasonable time.

But sometimes, the prime factorization itself is a problem. In this case, the **Euclidean algorithm** will help. It is based on the fact that

$$\text{if } a > b, \text{ then } \gcd(a,\ b) = \gcd(a - k \cdot b, b).$$

What is the GCD of 833 and 221?

The prime factorization isn't trivial, so we start with division with a reminder:

$$\mathbf{833 = 221 \times 3 + 170}.$$

So we get, that $\gcd(833, 221) = \gcd(221, 170)$. Then we will do next step and continue until we get a reminder 0, that means the previous value is the GCD

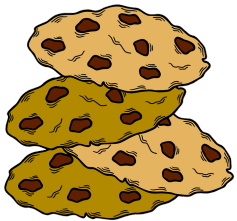
$$\mathbf{221 = 170 \times 1 + 51},$$
$$\mathbf{170 = 51 \times 3 + 17},$$
$$\mathbf{51 = 17 \times 3 + 0}.$$

That reminder 0 says that 51 is multiple of 17, so $\gcd(51,\ 17) = 17$, and that means $\gcd(833,\ 221) = 17$.

LEAST COMMON MULTIPLE

Alice has invited friends to a party and wants to buy cookies for everyone. She knows there will be 24 or 30 guests, so she wants that everybody to get an equal amount of cookies. What is the **minimum** amount of cookies should she buy?

To split cookies equally between 24 friends, she can buy 24, 48, 72, 96, 120, 144, and so on.
To split cookies equally between 30 friends, she can buy 30, 60, 90, 120, 150, and so on.
Therefore, we may see, the minimum amount of cookies she should buy is 120.



The **Least Common Multiple (LCM)** of two counting numbers is the smallest counting number that each of the given numbers divides evenly.

The LCM of two numbers is often denoted as $\mathrm{lcm}(a,\ b)$ or simply (in some context) $[a,\ b]$.
To find the LCM of two numbers, it is also helpful to perform a **prime factorization** of the numbers. The LCM of two numbers is the product of all primes in *their maximal power* in the factorization of each number.

What is the LCM of 144 and 900?

$$144 = 2^4 3^2, \qquad 900 = 2^2 3^2 5^2.$$

Their prime factorizations show that maximal power of 2 is 4, maximal power of 3 is 2, and maximal power of 5 is also 2. So

$$\mathrm{lcm}(144,\ 900) = 2^4 3^2 5^2 = 3600.$$

Curious mind probably noted, that

$$144 \times 900 = 36 \times 3600 = 129600.$$

Indeed, $a \times b = \gcd(a,\ b) \times \mathrm{lcm}(a,\ b)$, a proof follows from the prime factorization.

THE CHICKEN MCNUGGETS THEOREM

When they were first introduced, McDonald's Chicken McNuggets came in boxes of 9 or 20. What was the largest number of McNuggets that was not expressible as the sum of integer multiples of 9 and 20?

Let's look at a simpler version of this problem:

What is the largest integer that cannot be expressed as the sum of integer multiples of 3 and 5?

To find the solution, we need to find the largest integer by counting upwards before we first find 3 *integers in a row* that can be expressed as the sum of multiples of 3 and 5. After that, we can simply add factors of 3 to get the series to repeat to infinity.

$$6 = 2 \times 3,$$
$$7 \text{ cannot be expressed},$$
$$8 = 3 + 5,$$
$$9 = 3 \times 3,$$
$$10 = 2 \times 5.$$

So 7 is the answer.

For 9 and 20, a lot of counting (or a little computer coding) will tell you the answer is 151, but we can use the following theorem.

Theorem:

For *coprime* integers m and n, let $L\{m,\ n\}$ be the largest integer that cannot be expressed as the sum of integer multiples m and n. Then

$$L\{m,\ n\} = mn - m - n.$$

Since 9 and 20 are coprime ($\gcd(9,\ 20) = 1$),

$$L\{9,\ 20\} = 9 \times 20 - 9 - 20 = 151,$$
$$L\{3,\ 5\} = 3 \times 5 - 3 - 5 = 7.$$

DIVISIBILITY RULES FOR 3 AND 9

Is 5479 divisible by 9?

Let's write a number 5479 as a sum

$$5472 = 5 \cdot 1000 + 4 \cdot 100 + 7 \cdot 10 + 2.$$

And then write 1000 as a sum $999 + 1$, $100 = 99 + 1$ and $10 = 9 + 1$. So

$$5472 = 5 \cdot (999+1) + 4 \cdot (99+1) + 7 \cdot (9+1) + 9 =$$
$$= 5 \cdot 999 + 5 + 4 \cdot 99 + 4 + 7 \cdot 9 + 7 + 2.$$

And finally we can realize that 999, 99, and 9 are divisible by 9. That means that divisibility of 5479 by 9 depends on divisibility of sum $5 + 4 + 7 + 2$.

A number is divisible by 9, if the **sum of its digits** is divisible by 9.

And since 9, 99, 999, 9999 and so on is also divisible by 3, we get

A number is divisible by 3, if the **sum of its digits** is divisible by 3.

$\overline{abcd}$ is a mathematical notation that a number is written with digits a, b, c, and d. So

$$\overline{abcd} = a \cdot 10^3 + b \cdot 10^2 + c \cdot 10 + d.$$

This allows us to write the rules as

$$\overline{abcd} \equiv a + b + c + d \pmod{9 \text{ or } 3}.$$

The divisibility rule by 9 allows us quickly check if our arithmetic operations are correct.

$$\begin{array}{r} 384 \\ \times \quad 56 \\ \hline 2304 \\ 1820 \\ \hline 20504 \end{array}$$

Lets see remainders of factors and product

$$384 \equiv 6 \pmod 9, \quad 56 \equiv 2 \pmod 9,$$
$$20504 \equiv 2 \pmod 9.$$

But $6 \times 2 \not\equiv 2 \pmod 9$, so there is an error.

DIVISIBILITY RULES FOR 11

The divisibility rules for 9 and 3 works because 10, 100, $1{,}000$, and so on are all divisible by 9 with remainder 1. But what about 11?

$$1\underbrace{00\ldots0}_{\text{even zeros}}-1=\underbrace{99\ldots9}_{\text{even nines}}$$

is divisible by 11 because it is sum of

$$99\ 99\ \ldots 99=99\cdot 10^{n}+\ldots+99$$

which all are divisible by 11.
From other hand

$$1\underbrace{00\ldots0}_{\text{odd zeros}}+1=\underbrace{99\ldots9}_{\text{even nines}}\ 0+11$$

is also divisible by 11.

Is 3432 divisible by 11?

$$3432=3\cdot 1000+4\cdot 100+3\cdot 10+2=$$
$$=3\cdot(1001-1)+4\cdot(99+1)+3\cdot(11-1)+2\equiv$$

when we get rid of all multiples of 11

$$\equiv -3+4-3+2=0\ (\text{mod}\ 11).$$

As we see, our final computation is the digits of the number with alternate signs.

A number is divisible by 11 if the **difference** between the **sum of the odd-place digits** and the **sum of the even-place digits** is 0 or a multiple of 11.

The combinations of the divisibility rules may also create additional divisibility rules.
For example to check if number is divisible by 6 we may check if it divisible by 2 and 3. This will works when the divisor may be split in product of **coprime**[1] factors.
But the rule will not work for example for $27=9\times 3$, since testing for 9 we already testing for 3.

[1] *coprime numbers are numbers without common divisors.*

SUMMARY OF THE DIVISIBILITY RULES

An integer number n is divisible by

2. if the *last digit of n is divisible by* 2, e.g. is equal to 0, 2, 4, 6, or 8;
3. if the *sum of digits of n is divisible by* 3;
4. if the *last two digits of n is divisible by* 4.
5. if the *last digit of n is divisible by* 5, e.g. is equal to 0 or 5;
6. if n is divisible by both 2 and 3;
7. if *subtracting twice the last digit of n from the remaining digits* gives a multiple of 7;
8. if the *last three digits of n is divisible by* 8;
9. if the *sum of digits of n is divisible by* 9;
10. if n is divisible by both 2 and 5;
11. if the *difference of the alternating sum of digits of n* is a multiple of 11;
12. if n is divisible by both 3 and 4.

You might notice the strange divisibility rule for 7. The proof of this rule is not straightforward as for all other. Let's write $n = a \cdot 10 + b$, where b is the last digit and a is the number build with remaining digits. Then suppose n is divisible by 7

$$\begin{aligned} a \cdot 10 + b &\equiv 0 \pmod 7, && \text{multiply all by } 2 \\ a \cdot 20 + b \cdot 2 &\equiv 0 \pmod 7, && \text{subtract } 21a \\ a \cdot (-1) + b \cdot 2 &\equiv 0 \pmod 7, && \text{multiply by } -1 \\ a - b \cdot 2 &\equiv 0 \pmod 7. \end{aligned}$$

Doing the same operations in reverse order, we can get the divisibility rule for 7. This is possible because 2 and -1 are *coprime* with 7.
The rule may be repeated several times to get a number small enough for the direct check.

Similar divisibility rules may be obtained for other primes

13. if *adding 4 times the last digit of n to the remaining digits* gives a multiple of 13;
17. if *subtracting 5 times the last digit of n from the remaining digits* gives a multiple of 17.

But these rules aren't simpler than divide by the number.

EXERCISES

1. What is the remainder when 301×349 is divided by 9?
2. Find the GCD and LCM of 42 and 98.
3. The GCD of two numbers A and B is 7. What are possible values of GCD of $15 \cdot A$ and $35 \cdot B$?
4. The numbers 6545 can be written as the product of a pair of positive two-digit integers. What are these two integers?
5. What is the smallest prime factor of $11^7 + 7^5$?
6. The four digit number $A55B$ is divisible by 36. What is the sum of A and B?
7. What is the sum of the digits of $\dfrac{10^{25} + 8}{9}$?
8. Find the GCD of $2n + 13$ and $n + 7$ by Euclid's algorithm.

CHALLENGE PROBLEMS

1. The positive integers A, B, $A - B$, and $A + B$ are all prime numbers. What is the sum of these four primes?
2. Show that every prime greater than 3 must be of the form $6n + 1$ or $6n - 1$ for a positive integer n.
3. If p, q and r are prime numbers such that their product is 19 times their sum, find $p^2 + q^2 + r^2$.
4. 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: 5, 7, 11, 13, or 17?