Math Level 2.5 Handouts

Dylan Yu

June 17, 2020

§0 Contents

§1 Number Theory Basics

§1.1 Prime Factorization

Theorem 1.1 (Fundamental Theorem of Arithmetic). All positive integers n can be expressed as

$$n = 2^{e_1} \cdot 3^{e_2} \cdot 5^{e_3} \cdot \ldots,$$

where $e_1, e_2, e_3, \ldots$ are all nonnegative integers.

§1.2 GCD and LCM

You likely know the definitions for GCD and LCM:

Definition 1.1 (GCD and LCM). For two numbers

$$m = 2^{m_1} \cdot 3^{m_2} \cdot 5^{m_3} \cdot \ldots,$$

$$n = 2^{n_1} \cdot 3^{n_2} \cdot 5^{n_3} \cdot \ldots,$$

we have

$$\gcd(m, n) = 2^{\min(m_1, n_1)} \cdot 3^{\min(m_2, n_2)} \cdot 5^{\min(m_3, n_3)} \cdot \ldots,$$

$$\operatorname{lcm}(m, n) = 2^{\max(m_1, n_1)} \cdot 3^{\max(m_2, n_2)} \cdot 5^{\max(m_3, n_3)} \cdot \ldots.$$

Theorem 1.2. For any two positive integers m, n,

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

There are a few methods to find the gcd and lcm, namely the **Cake Method** and simply applying the process above. I will explain them very briefly in class, but I expect you to know how to calculate it.

Example 1.1. Find the value of $\gcd(3, 6)$ and $\operatorname{lcm}(3, 6)$.

Solution. By simply calculating, we get 3 and 6, respectively. □

Note that the value of $\gcd(0, n)$ is n for all positive integer n.

§1.3 Euclidean Algorithm

Theorem 1.3 ("Dumb" Euclidean Algorithm). For all positive integers $m > n$,

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

Example 1.2. Find the value of $\gcd(104, 78)$.

Solution. Applying the algorithm above, we get

$$\gcd(104, 78) = \gcd(26, 78) = \gcd(26, 52) = \gcd(26, 26) = 26.$$

□

So how can we speed this up?

Theorem 1.4 (Efficient Euclidean Algorithm). For all positive integers $m > n$,

$$\gcd(m, n) = \gcd(m \pmod n, n) = \gcd(n, m \pmod n).$$

The theorem above can be rephrased:

Theorem 1.5. Let a, b be integers, with $b \neq 0$, and let q, r be the unique integers such that $a = qb + r$. Then

$$\gcd(a, b) = \gcd(b, r).$$

§1.4 Coprime Integers

Definition 1.2 (Coprime). Let a, b be integers. We say that a and b are **coprime**, or **relatively prime**, if a and b share no common factors. That is to say, a and b are coprime if $\gcd(a, b) = 1$.

Coprimality can be useful with thinking about common divisors. In particular, we have the following useful theorem:

Theorem 1.6 (Coprime). Let a, b be nonzero integers, and let $d = \gcd(a, b)$. Then

- $\frac{a}{d}$ and $\frac{b}{d}$ are coprime.
- Write $a = dk$ for some integer k. Then for some integer y, if $a \mid (dy)$, then $k \mid y$.

§1.5 Modular Arithmetic

§1.5.1 Introduction and Notation

Example 1.3. Suppose it is 1 : 00 now. What time will it be exactly 1000 hours from now?

Solution. We know that the times will repeat themselves every 12 hours. In other words, the time will be 1 : 00 whenever the number of hours from now is a multiple of 12.

What is the multiple of 12 that is closest to 1000? After some experimentation, we see that the closest multiple is 996, so 996 hours from now it will be 1 : 00 as well. Thus, exactly 1000 hours from now the time will be $\boxed{5:00.}$

We can group the integers into groups called **residue classes modulo** n that have a common remainder when divided by n, and we say two integers a and b are **congruent** or **equivalent** modulo n if they lie in the same residue class. The notation for this is $a \equiv b \pmod{n}$.

For example, because $4, 16, 1000$, and 4252 all share the same remainder when divided by 12, the following equation is valid:

$$4 \equiv 16 \equiv 1000 \equiv 4252 \pmod{12}.$$

□

§1.5.2 Basic Formulas

Many of the rules of arithmetic apply to modular arithmetic as well.

If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then all of the following hold.

- $a + c \equiv b + d \pmod{n}$
- $ac \equiv bd \pmod{n}$
- $a^k \equiv b^k \pmod{n}$, where k is a positive integer

This is most easily seen with a few examples.

Example 1.4. What are the remainders when $3333 + 4444$ and $3333 \cdot 4444$ are divided by 5?

Solution. We have $3333 \equiv 3 \pmod{5}$ and $4444 \equiv 4 \pmod{5}$, so $3333 + 4444 \equiv 3 + 4 \equiv 7 \equiv \boxed{2} \pmod{5}$. Similarly, $3333 \cdot 4444 \equiv 3 \cdot 4 \equiv 12 \equiv \boxed{2} \pmod{5}$. In general, we can take any integer and replace it with an integer within the same residue class. We can do this multiple times within a problem. □

Example 1.5. What is the remainder when 7^{2015} is divided by 48?

Solution. At first, it seems that even modular arithmetic can't prevent this problem from becoming messy. However, upon further inspection, we can see that $7^2 = 49$, which leaves a remainder of 1 when divided by 48! Hence, we can write

$$7^{2015} \equiv 7 \cdot (7^2)^{1007} \equiv 7 \cdot 1^{1007} \equiv \boxed{7} \pmod{48}.$$

□

Example 1.6. What are the last two digits of the integer 17^{198}?

Solution. Note that $17^2 \equiv 289 \equiv -11 \pmod{100}$. Thus, the problem is simplified to computing $(-11)^{99} \equiv -11^{99} \pmod{100}$. Now note that by the Binomial Theorem

$$11^{99} = (10+1)^{99} = 10^{99} + \cdots + \binom{99}{2}10^2 + \binom{99}{1}10^1 + 1.$$

When this expansion is reduced modulo 100, all but the last two terms will go away since they are all divisible by 100, so $11^{99} \equiv \binom{99}{1} \cdot 10 + 1 \equiv 91 \pmod{100}$. As a result, $17^{198} \equiv -91 \equiv \boxed{09} \pmod{100}$. □

§1.5.3 Divisibility with Modular Arithmetic

From our work above, it seems that the only uses for modular arithmetic all relate to finding remainders for really large numbers. This is not true! Modular arithmetic is a key tool which is useful for all different aspects of Number Theory, including solving equations in integers. Here are a few problems which showcase modular arithmetic and its uses in other types of problems.

Example 1.7. Prove that any integer is divisible by 2^n if and only if the integer formed by its last n digits is also divisible by 2^n.

Solution. Let Y be the integer formed by the last n digits and let X be the integer formed by the digits to the left of these n digits. For example, in the 124564 case above, $X = 1245$ and $Y = 64$. Note that the integer can thus be written as $10^n X + Y$. Now note that $10^n \equiv (2^n)(5^n) \equiv 0 \pmod{2^n}$, so $10^n X + Y \equiv Y \pmod{2^n}$. This immediately implies the conclusion. □

Example 1.8. Let $N = \overline{a_0 a_1 a_2 \ldots a_n}$ be an integer. (The bar above the previous expression suggests the variables are digits and that we are not multiplying them together.) Prove that N is divisible by 9 if and only if

$$a_0 + a_1 + a_2 + \cdots + a_n$$

is also divisible by 9.

Solution. Note that N can be written more mathematically as

$$N = a_0 \cdot 10^n + a_1 \cdot 10^{n-1} + a_2 \cdot 10^{n-2} + \cdots + a_{n-1} \cdot 10 + a_n.$$

We attempt to simplify this modulo 9. The key here is to note that $10 \equiv 1 \pmod{9}$. This further implies that $10^2 \equiv 1 \pmod{9}$, $10^3 \equiv 1 \pmod{9}$, and so on. Making all the necessary substitutions gives

$$N \equiv a_0 + a_1 + a_2 + \cdots + a_n \pmod{9}.$$

Thus N and the sum of the digits of N give the same remainder upon division by 9, implying the conclusion. □

Example 1.9 (AMC 8 2014/21). The 7-digit numbers $\underline{74A52B1}$ and $\underline{326AB4C}$ are each multiples of 3. Which of the following could be the value of C?

(A) 1 **(B)** 2 **(C)** 3 **(D)** 5 **(E)** 8

Solution. The sum of a number's digits $\bmod 3$ is congruent to the number $\pmod 3$. $74A52B1 \bmod 3$ must be congruent to 0, since it is divisible by 3. Therefore, $7+4+A+5+2+B+1 \bmod 3$ is also congruent to 0. $7+4+5+2+1 \equiv 1 \pmod 3$, so $A+B \equiv 2 \pmod 3$. As we know, $326AB4C \equiv 0 \pmod 3$, so $3+2+6+A+B+4+C = 15+A+B+C \equiv 0 \pmod 3$, and therefore $A+B+C \equiv 0 \pmod 3$. We can substitute 2 for $A+B$, so $2+C \equiv 0 \pmod 3$, and therefore $C \equiv 1 \pmod 3$. This means that C can be 1, 4, or 7, but the only one of those that is an answer choice is $\boxed{\textbf{(A)}\ 1}$. □

§1.5.4 Solving Systems of Congruences

Most of you have probably seen a problem like below:

Example 1.10. Mr. Yu wants to divide the class into groups. When he tries to divide into groups of 3, 1 student is left over. When he tries to divide into groups of 4, 1 student is left over. And when he tries to divide into groups of 5, 1 student is left over. What is the least number of students he could have, assuming he has more than 1 student?

Solution. We simply write these equations in terms of mods. If the number of students he has is n, then

$$n \equiv 1 \pmod 3,$$

$$n \equiv 1 \pmod 4,$$

$$n \equiv 1 \pmod 5.$$

To the first two equations, we realize that one works. One also works for the third equation, but because we have to find the next greatest equation, we add $3 \cdot 4 \cdot 5$ to get $n = 61$. □

In general, we have

Theorem 1.7 (Special Case of Modular Arithmetic). If $n \equiv c \pmod{m_1} \equiv c \pmod{m_2} \equiv \ldots \equiv c \pmod{m_k}$ (all of these variables are integers), then

$$n \equiv c \pmod{m_1 m_2 m_3 \ldots m_k} \equiv \pmod{\operatorname{lcm}(m_1, m_2, m_3, \ldots, m_k)}.$$

Theorem 1.8. If

$$n \equiv c \pmod{\operatorname{lcm}(m_1, m_2, m_3, \ldots, m_k)},$$

and

$$\operatorname{lcm}(m_1, m_2, m_3, \ldots, m_k) \mid d$$

for some random integer d, then

$$n \equiv c \pmod{d}.$$

§1.5.5 Euler's Totient Function

Later on, you will learn just how useful this is (assuming you continue to learn higher math, if you don't it probably won't be very useful). We can show the motivation for this function in the following example:

Example 1.11. How many positive integers less than 12 are relatively prime to 12?

Solution. We know that $1, 5, 7$, and 11 are relatively prime to 12, so the answer is 4. □

What if we replaced 12 with 100? Or what if we used 10000? That would take a **very** long time. So instead we use **Euler's totient function**:

Definition 1.3. The totient function $\phi(n)$ is defined as the number of positive integers less than n that are relatively prime to n.

Theorem 1.9 (Euler's Totient Function). If $n = p_1^{e_1} p_2^{e_2} \cdots p_m^{e_m}$, then $\phi(n)$

$$\phi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_m}\right).$$

This following theorem is a bit random, but it is still **very important**. Please memorize it.

Theorem 1.10 (Chicken McNugget Theorem). For any two relatively prime positive integers m, n, the greatest integer that cannot be written in the form $am + bn$ for nonnegative integers a, b is $mn - m - n$.

Theorem 1.11. The number of $c = p_1^{e_1} p_2^{e_2} \ldots p_k^{e_k}$ inside $n!$ is

$$\min\left(\frac{\lfloor \frac{n}{p_i} \rfloor + \lfloor \frac{n}{p_i^2} \rfloor + \lfloor \frac{n}{p_i^3} \rfloor + \ldots}{e_i}\right),$$

and the minimum is found from testing all possible $i = 1, 2, \ldots, k$.

For example, to find the number of zeroes inside $n!$, the answer is

$$\lfloor \frac{n}{5} \rfloor + \lfloor \frac{n}{5^2} \rfloor + \lfloor \frac{n}{5^3} \rfloor + \ldots$$

§1.6 Problems

Problem 1.1. Are 37 and 111 coprime?

Problem 1.2. Find the value of $\gcd(0, 4, 10)$.

Problem 1.3. Find the value of $\text{lcm}(4, 6, 10)$.

Problem 1.4. What is the value of

$$\gcd(33, 121) \cdot \text{lcm}(33, 121)?$$

Problem 1.5. Find the largest n such that $n \mid 8, 10, 12$.

Problem 1.6. Find all solutions to the equation $2x + 3y = 46$.

Problem 1.7. Find the remainder when 5^{15} is divided by 128.

Problem 1.8. Find the remainder when 12^9 is divided by 1000.

Problem 1.9. Find the remainder when $1 + 2 + \cdots + 2020$ is divided by 1000.

Problem 1.10. Find the value of $\phi(12)$ and $\phi(1001)$.

Problem 1.11. Find the last two digits of 312^{84}.

Problem 1.12. Find the form of the solutions to the equation

$$x \equiv 2 \pmod 3,$$

$$x \equiv 3 \pmod 4.$$

Problem 1.13. What is the smallest number that cannot be formed from 7s and 11s?

Problem 1.14. What is the largest power of 2 that divides 1000!?

Problem 1.15 (Purple Comet HS 2013). There is a pile of eggs. Joan counted the eggs, but her count was off by 1 in the 1's place. Tom counted in the eggs, but his count was off by 1 in the 10's place. Raoul counted the eggs, but his count was off by 1 in the 100's place. Sasha, Jose, Peter, and Morris all counted the eggs and got the correct count. When these seven people added their counts together, the sum was 3162. How many eggs were in the pile?