ORMC AMC Group: Week 3
Number Theory

October 9, 2022

1 Greatest Common Divisor (gcd)

The **greatest common divisor** of two numbers $\gcd(a, b)$ is the largest positive integer that divides both numbers. GCD's can be helpful when factoring numbers or working in modular arithmetic. But in general, how do you find the GCD of two numbers?

1.1 Division Algorithm

In general, division takes a dividend a, a divisor b, and produces a quotient q and remainder r. This is often expressed in an equation as: $a = qb + r$. Specifically, we want $0 \leq r < b$.

1.2 The Euclidean Algorithm

One of the most useful ways to find the gcd of two numbers is the **Euclidean Algorithm**. Given $a, b \in \mathbb{Z}$, we do the following:

1. Use division algorithm on (a, b) and produce quotient q_1 and remainder $0 \leq r_1 < b$. $(a = q_1 b + r_1)$
2. Apply the division algorithm to b, r_1 to produce quotient q_2 and remainder r_2. $(b = q_2 r_1 + r_2)$
3. Continue dividing r_{n-1} by r_n to produce r_{n+1}. When $r_{n+1} = 0$, we will have $r_n = \gcd(a, b)$.

Note that we would get the same result if, instead of subtracting the entire quantity $q_1 b$ from a, we subtracted a single b at a time. While this would be less efficient, it can occasionally be helpful to see the intermediate steps, especially if a and/or b are expressions with variables, as opposed to just numbers.

1.3 Euclidean Algorithm Exercises

1. Find a pair of integers (a, b) such that $2022a + 1003b = 1$.

2. (**IMO 1959 #1, modified**) For what integer values of n is $\dfrac{21n + 4}{14n + 3}$ irreducible?

3. (**2020 AMC 10A #24**) Let n be the least positive integer greater than 1000 for which

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

What is the sum of the digits of n?

2 Primes and Factoring Integers

A prime is a positive integer whose only integer divisors are 1 and itself.

2.1 The Fundamental Theorem of Arithmetic

The Fundamental Theorem of Arithmetic states that for any integer, there exists a unique factorization of that integer into prime numbers. That is, for each integer, there is exactly one way to write it as $p_1^{e_1} \dots p_k^{e_k}$.where all the p_i are prime, and all the e_i are nonnegative integers.

2.2 GCD and LCM

Prime factorizations give us another way of thinking about greatest common divisors, as well as least common multiples. The **least common multiple(LCM)** of a and b is the smallest number that is divisible by both a and b. From the uniqueness of prime factorizations, we have:

$$a = p_1^{m_1} \cdots p_k^{m_k}, \quad b = p_1^{n_1} \cdots p_k^{n_k}$$

$$\implies \gcd(a,b) = p_1^{\min(m_1,n_1)} \cdots p_k^{\min(m_k,n_k)}, \quad \operatorname{lcm}(a,b) = p_1^{\max(m_1,n_1)} \cdots p_k^{\max(m_k,n_k)}.$$

Notice that these formulas highlight the power of the fundamental theorem of arithmetic. What the theorem really tells us is that in general, ***we can focus on individual primes as opposed to the number as a whole, <u>and</u> we can work with different primes independently***– even when they are being multiplied together as part of the same larger (composite) number. This will be one of your most dependable techniques: especially when faced with large number(s), it is helpful to shift your focus to the prime factorization(s).

2.3 Prime Factorization Exercises

1. Show that if $m, n \in \mathbb{Z}$ and $ma + nb > 0$, then $ma + nb \geq \gcd(a,b)$.

2. How many even factors does 15! have? How many square factors?

3. (**2018 AMC 10B #23**) How many ordered pairs (a,b) of positive integers satisfy the equation

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

4. If $\gcd(a,c) = 1$ and $\gcd(b,c) = 1$, then what is $\gcd(ab,c)$? What about when $\gcd(a,c) = d > 1$?

5. (**2018 AMC 10A #22**) 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?

(A) 5 (B) 7 (C) 11 (D) 13 (E) 17

3 Modular Arithmetic

Recall from last week that modular arithmetic involves *only integers*, and centers around a modulus m. We say two integers a, b are "congruent modulo m" (written $a \equiv b \pmod{m}$ if m divides their difference. This can be written in a few different ways:

- $m \mid a - b$
- $a - b = km$ for some integer k
- $a = km + b$ for some integer k (note the similarity to the division algorithm)

Recall from last week that we can add, subtract, or multiply both sides of a congruence by the same thing. That is, if $a \equiv b, c \equiv d \pmod{m}$, then $a \pm c \equiv b \pm d, ac \equiv bd \pmod{m}$.

3.1 Modular Inverses

In general, *we cannot do division in the normal way.* Consider the following motivating examples, which have solutions but would appear to require "division", or fractions (remember, only integers!):

$$2x \equiv 7 \pmod{13}, \quad 4x \equiv 1 \pmod{5}$$

In place of "division", we can get rid of a constant multiple a by multiplying by an additional constant b such that $ba \equiv 1 \pmod{m}$. This value b is called the **modular inverse** of $a \mod m$ and is often written a^{-1}. As discussed last week, an inverse of $a \mod m$ exists if and only if $\gcd(a, m) = 1$. This is easiest to see when we write $a^{-1}a \equiv 1 \pmod{m}$ as $a^{-1}a \equiv km + 1 \pmod{m}$, for some integer k.

3.2 Modular Arithmetic Exercises

1. Let $\overline{a_n \cdots a_1 a_0}$ represent the number with digits $a_n, a_{n-1}, \ldots, a_1, a_0$.
   Find k such that if $\overline{a_n \cdots a_1 a_0} \equiv 0 \pmod{17}$, then $\overline{a_n \cdots a_1} - ka_0 \equiv 0 \pmod{17}$.

2. (**AMC 12B 2010 #16**) Positive integers a, b, and c are randomly selected with replacement from the set $\{1, 2, 3, \ldots, 2010\}$. What is the probability that $abc + ab + a$ is divisible by 3?

3. (**AMC 12A 2010 #23**) The number obtained from the last two nonzero digits of 90! is equal to n. What is n?

4. Let $Rem_m(S)$ denote the set of remainders $0 \leq r < m$ produced when each element of S is divided by m. For example,

   $$Rem_3(\{5, 9, 14, 28, 14, 12\}) = \{2, 0, 2, 1, 2, 0\} = \{0, 1, 2\}.$$

   What is $Rem_n(\{0, a, 2a, 3a \ldots, (n-1)a\})$, when $\gcd(a, n) = 1$?

4 Number Theory Techniques

Consider exponents $\mod m$. There are only m different values $\mod m$, so at some point, the exponents must "wrap around". For example, $2^4 \equiv 1 \pmod 5$, so $2 \equiv 2^5 \equiv 2^9 \equiv 2^1 3 \cdots \pmod 5$. To use this fact to our advantage, we want to know when the exponents repeat.

4.1 Fermat's Little Theorem

Fermat's Little Theorem gives us a way to do this if our modulus is a prime p. In particular, the theorem states:

$$a^p \equiv a \pmod p$$

Note then that if a is invertible, meaning $\gcd(a, p) = 1$ or $p \nmid a$, then $a^{p-1} \equiv 1 \pmod p$. So, when we are working modulo a prime p, ***exponents repeat for every*** $p-1$. Note that this repetition suggests modular computation for the exponent: *we can simplify the exponent* $\pmod{p-1}$.

4.2 Euler's Totient Theorem

Fermat's Little Theorem only works for primes, but we really want something that works for all integers. Recall that for an integer m with prime factorization $p_1^{e_1} \cdots p_k^{e_k}$, Euler's Totient Function $\phi(m)$ is defined to be:

$$\phi(m) = m\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_k}\right) = \left((p_1 - 1)p_1^{e_1 - 1}\right) \cdots \left((p_k - 1)p_k^{e_k - 1}\right)$$

Then, for a modulus m and an integer a with $\gcd(a, m) = 1$, Euler's Totient Theorem states:

$$a^{\phi(m)} = 1.$$

Proof. By exercises 2.3.4 and 3.2.4,

$$S = \{k \mod m \mid 0 \le k < m, \gcd(k, m) = 1\} = \{ak \mod m \mid 0 \le k < m, \gcd(k, m) = 1\} = aS$$

. And since $|S| = \phi(m)$ by definition of ϕ, and k^{-1} exists when $\gcd(k, m) = 1$:

$$\prod_{k \in S} k \equiv \prod_{k \in aS} k \equiv \prod_{k \in S} ak \equiv a^{\phi(m)} \prod_{k \in S} k \pmod m \implies a^{\phi(m)} \equiv 1 \pmod m.$$

□

4.3 Modular Exponentiation Exercises

1. Find the remainder when $1 + 7 + 7^2 + \cdots + 7^{2022}$ is divided by 1000.

2. Determine the remainder when $2004^{2003^{2002}}$ is divided by 1000.

3. (**AMC 12A 2008 #15**) Let $k = 2008^2 + 2^{2008}$. What is the units digit of $k^2 + 2^k$?

4. (**AMC 12A 2021 #10**) The base-nine representation of the number N is $27{,}006{,}000{,}052_9$. What is the remainder when N is divided by 5?

4.4 The Chinese Remainder Theorem

Just like with regular equations, we can have systems of modular congruences. The Chinese Remainder Theorem can help us determine when a system has a solution, and can help us find the solution in some cases. For a system of congruences:

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_n \pmod{m_n}, \end{aligned}$$

where all the m_i are pairwise relatively prime, there exists exactly one integer $0 \leq x < m_1 m_2 \cdots m_n$ which satisfies all the congruences.

We will work through the following example in class, to demonstrate some common techniques of applying the chinese remainder theorem:

$$\begin{aligned} x &\equiv 1 \mod 2 \\ x &\equiv 2 \mod 3 \\ x &\equiv 3 \mod 5 \\ x &\equiv 4 \mod 7 \end{aligned}$$

One important application of this is congruence with a very large modulus. Instead of working with a large modulus, it is easier to break it down into its prime factorization, and instead work with a system of congruences modulo the powers of primes. Then, we can use the chinese remainder theorem to find the solution.

4.5 Chinese Remainder Theorem Exercises

1. 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?

2. (**AMC 12B 2017 #19**) Let $N = 123456789101112\ldots4344$ be the 79-digit number that is formed by writing the integers from 1 to 44 in order, one after the other. What is the remainder when N is divided by 45?

3. (**AIME 2021 #13**) Find the least positive integer n for which $2^n + 5^n - n$ is a multiple of 1000.