Introduction to Divisibility and Modular Arithmetic

Dennis Chen, Kelin Zhu

NPU

1 Divisibility

The concept of divisibility is a cornerstone of number theory across the AMCs and beyond; therefore, it must be reserved as our first topic.

Divisibility. An integer b is **divisible by** an integer a if there exists an integer c with $b = ca$. Alternatively, we say a divides b, denoted by $a \mid b$.

Remark: If instead we define divisibility by saying that $\frac{b}{a}$ is an integer, our picture falls apart when 0 is introduced. For instance, 0 is divisible by 0, but $\frac{0}{0}$ is indeterminate.

We can derive some useful results immediately:

Divisibility Results.

1. If $a \mid b$ and both a, b are positive, then $a \leq b$
2. If $a \mid b$, $b \mid a$, and both a, b are positive, then $a = b$.
3. If $a \mid b$ and $b \mid c$, then $a \mid c$.
4. If $a \mid b$, then $a \mid bc$ for all integers c.
5. If $a \mid b$ and $a \mid c$, then $a \mid b + c$ and $a \mid b - c$.

On the other hand, there are many *false* results in divisibility that might be cited or used mistakenly. Common ones are listed below.

1. If $a \mid c$ and $b \mid c$, it is *not necessarily* true that $ab \mid c$; take $a = 4, b = 8, c = 16$ as a counterexample. (However, this claim is always true if a, b are relatively prime, defined shortly.)
2. If $a \mid bc$, it is *not necessarily* true that $a \mid b$ or $a \mid c$; again, $a = 16, b = 4, c = 8$ is a counterexample.
3. Conversely, if a divides neither b nor c, it is *not necessarily* true that a does not divide bc.

The concepts of GCD and LCM also appear frequently; they are covered more thoroughly in the unit NQV-Prime.

Least Common Multiple. The **least common multiple** (often abbreviated as **LCM**) of two integers a, b is the smallest positive integer that is a multiple of both a and b.

Greatest Common Divisor. The **greatest common divisor** (often abbreviated as **GCD**) of two integers a, b is the greatest positive integer that divides both a and b. In particular, the GCD of 0 and n for any integer n is equal to n, and the GCD of 0 and 0 is undefined.

Relatively Prime. Two integers a, b are **relatively prime** if and only if $\gcd(a, b)$ is equal to 1. In particular, 1 and -1 are relatively prime to all integers.

These concepts can be extended to three or more integers, but at this stage, we only really work with two.

To top off the section, here are a few relatively well-known divisibility rules. For a challenge, try proving all of them on your own after reading through the next section!

Divisibility Rules.

- 2: If the last digit of n is even, then n is even.
- 4: If the last 2 digits of n is a multiple of 4, then n is a multiple of 4.
- 8: If the last 3 digits of n is a multiple of 8, then n is a multiple of 8. (Can you see a pattern?)
- 3 or 9: If the sum of digits of n is a multiple of $3/9$, then n is a multiple of 3 or 9. (This does *not* generalize to 27 or greater powers of 3.)
- 5: If the last digit of n is a multiple of 5, then n is a multiple of 5.
- 25: If the last 2 digits of n is a multiple of 25, then n is a multiple of 25.
- 125: If the last 3 digits of n is a multiple of 125, then n is a multiple of 125. (The pattern for powers of 2 also applies here.)
- 11: Let a be the sum of the 1st, 3rd, 5th... digits from the right of n, and let b be the sum of the 2nd, 4th, 6th... digits from the right of n. If $a - b$ is a multiple of 11, then n is a multiple of 11.

For pairwise relatively prime integers, we can construct the divisibility rule of their product by combining their divisibility rules. For example, the divisibility rule of 60 is being divisible by $3, 4, 5$, since any two of $3, 4, 5$ have GCD 1.

All of the above are bidirectional; that is, all multiples of x will satisfy the divisibility rules of x, and all numbers that satisfy the divisibility rules of x will be multiples of x.

2 Modular Arithmetic

The following section describes operations in modular arithmetic, intuitively motivated by operations over the integers, rationals, and even real and complex numbers[1].

Note that the modulus does have to be positive and greater than 1, unlike the previous section. For the rest of the exposition below, assume that the given variables are integers or positive integers when reasonable.

Modular Congruence. We say $a \equiv b \pmod{n}$ if and only if $n \mid a - b$.

The intuitive way to think about this is that a and b have the same remainder when divided by n. (Remember that negative numbers also have a remainder when divided.)

As a corollary, we can derive the following: if $a \equiv b \pmod{n}$, then $a \equiv b \pmod{d}$ for any divisor d of n. (The converse is false.)

[1] Yes, you can find $i \pmod{p}$.

Modular Residue. We say the *residue* of an integer $a \pmod{n}$ is the integer b that satisfies

- $0 \le b < n$
- $a \equiv b \pmod{n}$.

It can be helpful to think of b as the remainder of a when divided by n, but care should be taken when applying this intuition with negative numbers.

You may find that almost all arithmetic mod n is extremely similar to normal arithmetic. Make sure you understand why the following results are true, but you should simultaneously feel free to do whatever you want given a few restrictions.

2.1 Modular Operations

You can add, subtract, multiply, and exponentiate modulos. You can also divide, but care must be taken.

Addition. If $a \equiv x \pmod{n}$ and $b \equiv y \pmod{n}$, $a + b \equiv x + y \pmod{n}$.

Proof. Since $n \mid x - a$ and $n \mid y - b$, clearly $n \mid (x + y) - (a + b)$.

Subtraction is identical, so we do not discuss it further.

Multiplication. If $a \equiv x \pmod{n}$ and $b \equiv y \pmod{n}$, $ab \equiv xy \pmod{n}$.

Proof. Say $a = a_p n + q$ and $x = x_p n + q$ where q is the residue of a and x, and $b = b_p n + r$ and $y = y_p n + r$ where r is the residue of b and y. Then

$$\begin{aligned} xy - ab &= (x_p n + q)(y_p n + r) - (a_p n + q)(b_p n + r) \\ &= n^2(x_p y_p - a_p b_p) + n(x_p r + y_p q - a_p r - b_p q) + qr - qr \\ &= n^2(x_p y_p - a_p b_p) + n(x_p r + y_p q - a_p r - b_p q), \end{aligned}$$

which is divisible by n.

Exponentiation. If $a \equiv b \pmod{n}$, then $a^k \equiv b^k \pmod{n}$ for any positive integer k.

Proof. Note that $n \mid a - b \mid a^k - b^k$.

As an exercise for the operations we have defined so far, pick your favorite ordered triple of positive integers (a, b, n), and compute the remainder of $a + b$, $a - b$, ab, and a^b[2] when divided by n.

Division. Let a, b, c be positive integers such that $c \mid a$ and $c \mid b$. If $a \equiv b \pmod{n}$ **and** $\gcd(c, n) = 1$, then $\frac{a}{c} \equiv \frac{b}{c} \pmod{n}$.

Be careful to remember that we **must have** $\gcd(c, n) = 1$! (To strengthen your understanding of modular artihmetic, try to explain why this condition is necessary.)

[2]For large enough b, you'll want to know Fermat's Little Theorem!

Strengthened Divisibility of 3 or 9. Let m be the sum of digits of a positive integer n. Then, $n \equiv m \pmod 9$.

Proof. Let $n = \overline{d_k d_{k-1} \cdots d_2 d_1 d_0}$. We have

$$\begin{aligned} n &\equiv 10^k \cdot d_k + 10^{k-1} \cdot d_{k-1} + \cdots + 10^2 \cdot d_2 + 10^1 \cdot d_1 + 10^0 \cdot d_0 \\ &\equiv 1^k \cdot d_k + 1^{k-1} \cdot d_{k-1} + \cdots + 1^2 \cdot d_2 + 1^1 \cdot d_1 + 1^0 \cdot d_0 \\ &\equiv d_k + d_{k-1} + \cdots + d_2 + d_1 + d_0 \\ &\equiv m \pmod 9. \end{aligned}$$

Strengthened Divisibility of Powers of 2 or 5. For nonnegative integers n, a, b, the remainder when n is divided by $2^a 5^b$ is equal to the remainder when the last $\max(a, b)$ digits of n is divided by $2^a 5^b$.

Proof. We have $10^0 \cdot d_0 + 10^1 \cdot d_1 \ldots + 10^{\max(a,b)} d_{\max(a,b)} + \ldots = 2^0 5^0 \cdot d_0 + 2^1 5^1 \cdot d_1 \ldots + 2^{\max(a,b)} 5^{\max(a,b)} \cdot d_{\max(a,b)} + \ldots \equiv 10^0 \cdot d_0 + 10^1 \cdot d_1 \ldots + 10^{\max(a,b)-1} \cdot d_{\max(a,b)-1} + 0 \cdot d_{\max(a,b)} + 0 \ldots \pmod{2^a 5^b}$

The above rules allows us to kill an AMC last five in mere seconds:

Example (AMC 10B 2017/23). The positive integer $N = 1234 \cdots 44$ is the concatenation of the numbers $1, 2, 3, \ldots, 44$. Find the remainder when N is divided by 45.
(A) 1 **(B)** 4 **(C)** 9 **(D)** 18 **(E)** 44

Solution. N is equivalent to 4 mod 5 from its last digit, which immediately rules out choices A and D. It seems somewhat tedious to count the number of occurrences of each digit, which motivates the observation that $1 + 0 + 1 + 1 + \ldots + 4 + 3 + 4 + 4 \equiv 10 + 11 + \ldots + 43 + 44 = \frac{44 \cdot 45}{2} \equiv 0 \pmod 9$, which eliminates choices D and E. Our final answer is $\textbf{(C) 9}$.

2.2 Modular Inverses

In normal arithmetic, we define $a \cdot a^{-1} = 1$. We can do something similar in modular arithmetic.

Modular Inverse. We define a^{-1} to be the number mod n such that $a \cdot a^{-1} \equiv 1 \pmod n$. We say that a^{-1} is the inverse of $a \pmod n$.
The modular inverse is defined if and only if $\gcd(a, n) = 1$. (Why?)

We can treat inverses as fractions; for instance, $\frac{1}{2} + \frac{1}{3} + \frac{1}{6} \equiv 1 \pmod p$ for $p \neq 2, 3$. The proof is non-trivial and inverses should be treated with care, so we will prove that all of these operations are valid.

You should rewrite all of these operations into fractions to understand what they're really saying. The proofs follow directly from the associative, distributive, and commutative properties.

Adding Inverses. For integers a, b relatively prime to n, $a^{-1} + b^{-1} \equiv (a + b)(ab)^{-1} \pmod n$.

Proof. Note that $(a + b)(ab)^{-1} \equiv aa^{-1}b^{-1} + ba^{-1}b^{-1} \equiv b^{-1} + a^{-1} \pmod n$.

Multiplying Inverses. For integers a, b relatively prime to n, $a^{-1}b^{-1} \equiv (ab)^{-1} \pmod{n}$.

Proof. Note that $(ab)^{-1}ab \equiv 1 \pmod{n}$ and $a^{-1}b^{-1}(ab) \equiv aa^{-1}bb^{-1} \equiv 1 \pmod{n}$.

Here is an example that uses the fact that modular inverses exist.

Example. How many ordered quadruplets of integers (a, b, c, d) with $1 \le a, b, c, d \le 4$ exist such that $5 \mid ab - cd$?

Solution. Note that this implies $ab \equiv cd \pmod{5}$, or $\frac{ab}{c} \equiv d \pmod{5}$. Notice that a choice of (a, b, c) will uniquely determine d, so the answer is just the number of ways to choose (a, b, c), or $4^3 = 64$ ways.

Make sure you understand **why** d is uniquely determined!

General negative exponents. We can also define any negative exponents mod n; m^{-a} is the inverse of m^a, or $m^{-1} \cdot m^a$; both definitions give us the same residue.

Here is one last example, that uses purely standard modular arithmetic techniques; it epitomizes the ideas of this section. This is also an exercise in reading the problem carefully, and many students tried overzealous approaches, for example bashing through all the cases. Unfourtunately, the answer was E, so this took a lot of time.[3]

Example (AMC 10B 2017/25). Last year Isabella took 7 math tests and received 7 different scores, each an integer between 91 and 100, inclusive. After each test she noticed that the average of her test scores was an integer. Her score on the seventh test was 95. What was her score on the sixth test?
(A) 92 **(B)** 94 **(C)** 96 **(D)** 98 **(E)** 100

Solution. Let A be the average of the first 6 tests. We know $6A + 95$ is a multiple of 7, as it is the sum of the first seven tests, or

$$6A + 95 \equiv 0 \pmod{7}.$$

This means we have $6A \equiv 3 \pmod{7}$, so

$$A \equiv \frac{1}{2} \equiv \frac{8}{2} = 4 \pmod{7}.$$

However, A must be one of $91, 92, \ldots, 100$. Thus, $A = 95$. If the sixth score is S and the average of the first 5 tests is B, since $570 = S + 5B$, S is multiple of 5 and must be **(E) 100**.

3 Wilson's Theorem

Factorials rarely appear in number theory (at least for the AMCs and the AIME). But Wilson's Theorem is still one of the standard tools you need to have at your disposal.

Wilson's Theorem. For prime p,

$$(p-1)! \equiv -1 \pmod{p}.$$

[3] I (Ethan) seem to recall simply getting it wrong. Oops.

Proof. Notice that the numbers $2, 3, 4 \dots p-2$ all have modular inverses. In addition, modular inverses come in pairs. Since p is odd (the case where $p = 2$ is very easy to deal with), then the modular inverses all multiply to 1. This leaves us with $(p-1)! \equiv 1 \cdot (p-1) \equiv -1 \pmod{p}$, as desired.

We do not include $1, p-1$ in the pairing because for prime p, 1 and $p-1$ are the only numbers whose modular inverses are themselves.

Here is how Wilson's theorem simplifies a problem you might have solved in the Season 3 application:

Example (NARML/4, MAST S3 Diagnostics/N1). Compute the smallest positive integer n such that $9(n+3)$ divides $4n! + n + 5$.

Solution. Brute force works here, but there is an easier route.

First, we can check that none of $1 \le n \le 5$ work, and therefore $4n! + n + 5 \equiv n + 5 \pmod{9}$ as $n!$ is necessarily a multiple of $3 \cdot 6 = 9 \cdot 2$. From here, we can see that n must be equivalent to 4 mod 9.

Next, suppose that $n+3$ is composite; as $n \ge 6$, we have $2n > n+3$ and therefore $n!$ will be a multiple of $n+3$; we would need $n+5$ to be a multiple of $n+3$ which is impossible. Therefore, $n+3$ must be a prime.

The smallest possible n that satisfies the above conditions is **40**. Indeed, by Wilson's theorem, $40! \equiv \frac{-1}{41 \cdot 42} \equiv \frac{-1}{2} \pmod{43}$ and $4 \cdot \frac{-1}{2} + 40 + 5 = 40 + 5 - 2 = 43$.

Remark: Even though Wilson's is only used towards the end to verify our solution, it invisibly motivates the entire solution. The idea of checking if $n+3$ is prime should naturally arise after seeing factorials in the problem.

4 Problems

Minimum is [34 ♟]. Problems denoted with ♞ are required. (They still count towards the point total.)

> "Take what fortune grants you, use it while you've got it!"
>
> Death Note Musical

[1 ♟] **Problem 1** Find the inverse of 2 $\pmod{p}$ for odd prime p in terms of p.

[1 ♟] **Problem 2** Find the remainder of 98! when divided by 101.

[2 ♟] **Problem 3** What is the residue of $\frac{1}{1\cdot 2} \cdot \frac{1}{2\cdot 3} \cdot \dots \cdot \frac{1}{11\cdot 12} \pmod{13}$?

[2 ♟] **Problem 4 (AMC 10B 2021/3, buffed)** An after-school program contains a nonzero amount of juniors and seniors, with no other grades present. Among the 28 students in the program, 25% of the juniors and 10% of the seniors are on the debate team. how many juniors are in the program?

[3 ♟] **Problem 5 (1001 Problems in Number Theory)** For which positive integers n is it true that $1+2+\cdots+n \mid 1\cdot 2\cdot \dots \cdot n$?

[3 ♟] **Problem 6 (AMC 10A 2017/13)** Define a sequence recursively by $F_0 = 0$, $F_1 = 1$, and F_n = the remainder when $F_{n-1} + F_{n-2}$ is divided by 3, for all $n \geq 2$. Thus the sequence starts $0, 1, 1, 2, 0, 2 \dots$. What is $F_{2017} + F_{2018} + F_{2019} + F_{2020} + F_{2021} + F_{2022} + F_{2023} + F_{2024}$?

[4 ♞] **Problem 7 (AMC 10B 2019/14)** The base-ten representation for 19! is $121, 6T5, 100, 40M, 832, H00$, where T, M, and H denote digits that are not given. What is $T + M + H$?

[4 ♟] **Problem 8 (AIME I 2020/4, modified)** Let S be the set of positive integers N with the property that the last three digits of N are 343, and when the last three digits are removed, the result is a divisor of N. For example, 7343 is in S because 7 is a divisor of 7343. Find the sum of all the digits of all the numbers in S. For example, the number 7343 contributes $7 + 3 + 4 + 3 = 17$ to this total.

[6 ♟] **Problem 9 (AIME II 2017/8)** Find the number of positive integers n less than 2017 such that

$$1 + n + \frac{n^2}{2!} + \frac{n^3}{3!} + \frac{n^4}{4!} + \frac{n^5}{5!} + \frac{n^6}{6!}$$

is an integer.

[6 ♟] **Problem 10 (AOIME 2020/10)** Find the sum of all positive integers n such that when $1^3+2^3+3^3+\cdots+n^3$ is divided by $n + 5$, the remainder is 17.

[9 ♞] **Problem 11 (AIME 1989/9)** One of Euler's conjectures was disproved in the 1960s by three American mathematicians when they showed there was a positive integer such that $133^5 + 110^5 + 84^5 + 27^5 = n^5$. Find the value of n.

[9 ♟] **Problem 12 (USAMO 1979/1)** Determine all non-negative integral solutions $(n_1, n_2, \dots, n_k)$, if any, apart from permutations, of the Diophantine equation

$$n_1^4 + n_2^4 + \cdots + n_{14}^4 = 1599.$$

[13 ♟] **Problem 13 (IMO 2005/4)** Determine all positive integers relatively prime to all the terms of the infinite sequence

$$a_n = 2^n + 3^n + 6^n - 1,\ n \geq 1.$$