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 AMC's and beyond, and therefore it must be reserved as our first topic.

Divisibility. We say that an integer m is **divisible by** another integer n and equivalently n **divides** m (neither are necessarily positive, though we will mostly work with positive integers in this unit), notated as $n|m$, if there exists another integer k with $m = kn$.

Remark: If we instead define divisibility by saying that $\frac{m}{n} = k$ is an integer, our picture falls apart when 0 is introduced. Indeed, we can get that 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 $a \leq b$; if $a \mid b$, $b \mid a$ and both a, b are positive then $a = b$.
2. If $a \mid b$ and $b \mid c$ then $a \mid c$.
3. If $a \mid b$ then $a \mid bc$ for all integers c.
4. If $a \mid b$ and $a \mid c$, then $a \mid db + ec$ for any integers d, e.

WARNING: There are several common false results in divisibility that might be cited or used mistakenly. The most common ones will be listed below.

1. If $a \mid c$ and $b \mid c$, it is NOT NECESSARILY true that $ab \mid c$; take $a = 4, b = 8, c = 16$ for a counterexample. However, this claim is always true if a, b are relatively prime. (can you see why?)
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 concept of GCD and LCM also appear frequently; they will be covered more thoroughly in the unit NQV-Prime.

LCM/GCD. 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.

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.

Two integers a, b are **relatively prime** if and only if their GCD 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 throrugh 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?)
- 3/9: If the sum of digits of n is a multiple of 3/9, then n is a multiple of 3/9. (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 apply 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 simply combining their divisibility rules. For example, the divisibility rule of 60 is simply 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]. You will find you will be able to do almost everything $\pmod n$ that you would be able to do normally. Make sure you understand the rigorous reasons why these things are true, but you should simultaneously feel free to do whatever you want given a few restrictions.

Note that the modulus does have to be positive and greater than 1, unlike the previous section.

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

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

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 obviously false.)

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

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

It can be helpful to think of b as the remainder of a when divided by n.

2.1 Modular Operations

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

Adding. 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 $n \mid (x + y) - (a + b)$.

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

Multiplying. 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 clearly divisible by n.

Exponentiating. For integer a, b and positive integers n, k, if $a \equiv b \pmod{n}$, then $a^k \equiv b^k \pmod{n}$.

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

As an exercise for the operations we've 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.

Dividing. 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** $\gcd(c, n) = 1$!

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

Strengthened 3/9 divisibility. Let the sum of digits of a positive integer n be equal to m. Then, $n \equiv m \pmod 9$.

Proof. $10^0 \cdot d_0 + 10^1 \cdot d_1 + 10^2 \cdot d^2 + \ldots \equiv 1^0 \cdot d_0 + 1^1 \cdot d_1 + 1^2 \cdot d_2 \ldots \pmod 9$

Strengthened powers of 2/5 divisibility. 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. $10^0 \cdot d_0 + 10^1 \cdot d_1 \ldots + 10^{\max(a,b)} d_{\max(a,b)} + \ldots = 2^0 5^0 \cdot d_0 + 2^1 5^1 \cdot d_1 \ldots + 2^{\max(a,b)} 5^{\max(a,b)} \cdot d_{\max(a,b)} + \ldots \equiv 10^0 \cdot d_0 + 10^1 \cdot d_1 \ldots + 10^{\max(a,b)-1} \cdot d_{\max(a,b)-1} + 0 \cdot d_{\max(a,b)} + 0 \ldots \pmod{2^a 5^b}$

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,D. It seems somewhat tedious to count the number of occurrences of each digit, which motivates the observation that $1 + 2 + 3 \ldots + 4 + 3 + 4 + 4 \equiv 1 + 2 + 3 \ldots + 43 + 44 = \frac{44 \cdot 45}{2} \equiv 0 \pmod 9$, which eliminates choices D,E. Our final answer is (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 $\gcd(a, n) = 1$.

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 $1 \leq a, b, c, d \leq 4$ 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.

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 did 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 $6A \equiv 3 \pmod 7$, which means

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

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

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

3 Problems

Minimum is [54 ♟]. 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