Divisibility Tricks

by Arnav Kumar

In contests, there are many instances where we may seek fast ways to decide if a number divides another. This will explore tricks that help determine divisibility, and in the process of doing so, will introduce modular arithmetic. This introduction is not formal in any sense, and assumes certain knowledge.

Definition 1 *Let $m, n \in \mathbb{Z}$. We say that m **divides** n if there exists some $k \in \mathbb{Z}$ such that $k\,m = n$. This is notated as $m \mid n$. We can also say that n is an (integer) **multiple** of m.*

Note 1. This definition means that for all $a \in \mathbb{Z}$, we have $a \mid 0$ since $0 \times a = 0$. Additionally, $0 \mid a$ if and only if $a = 0$.

Given an arbitrary integer, n, we can express all of the multiples of n as a set, namely $\{k\,n : k \in \mathbb{Z}\}$. What about the rest of the integers? We seem to have created some sort of set of numbers, each a "distance" n from its neighbour, all of which are divisible by n.

What if we consider those numbers which aren't divisible by n, but always yeild the same "remainder" when divided by n? Perhaps this question is a weird one if you start to think about negative numbers, so let's rephrase what we want to say. Instead, consider the set of numbers, which are divisible by n upon subtracting a fixed integer a from it. This refers to the set $\{k\,n + a : k \in \mathbb{Z}\}$.

Definition 2 *Given a positive integer n, and an integer a, we say $[a]_n := \{k\,n + a : k \in \mathbb{Z}\}$ is a **congruence class**, **residue class**, or **equivalence class**. It is often implicit what the value of n is, and we can instead write $\bar{a}$ to refer to $[a]_n$. For any two $b, c \in \bar{a}$, we say that b and c are congruent **modulo n** which can be denoted as $b \equiv c \pmod{n}$. When it is obvious what the modulus is, we can omit the $\pmod{n}$.*

Remark 1. As an aside, the notation $\mathbb{Z}_n$ is used to refer to $\{[x]_n : x \in \mathbb{Z}\}$, the set of congruence classes modulo n. This may seem confusing as it is a set of sets, but is something you don't have to worry about.

Now we can take some time to familiarize ourselves with what this means. For the integers, our definition of congruence classes gives us exactly what we want, all of the numbers which have a certain remainer when divided by n. These numbers are spaced every n numbers away from each other as well. An easy way to interpret a congruence relation is then to say that when dividing both sides by n, they yield the same remainder. This seems like a logical next step to help us determine divisibility tricks since $n \mid m$ if and only if $m \equiv 0 \pmod{n}$.

Playing around with the definitions given produces the following results:

Theorem 1 **(Properties of Modular Arithmetic)** *If $n, m \in \mathbb{Z}_{>0}$, and $a, b, c, d \in \mathbb{Z}$, then we see that:*

- *If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then $a + c \equiv b + d \pmod{n}$*
- *If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then $a\,c \equiv b\,d \pmod{n}$*
- *If $a \equiv b \pmod{n}$, then $a^m \equiv b^m \pmod{n}$*

So how does this relate back to divisibility and what is useful about this? Modular arithmetic is a very powerful idea in mathematics that helps you prove or disprove certain number theory propositions since it helps you say something about the behaviour of an entire set of numbers. It is often a technique to break problems into cases based on the congruence class of a variable, such as breaking a problem based on even or odd (which is just modulo 2). Now let's dive into some divisibility tricks.

Theorem 2 **(Divisibility Tricks)** *Let $n \in \mathbb{N}$ be arbitrary where $0 \notin \mathbb{N}$.*

Let $d_k \colon \mathbb{N} \to \mathbb{N}$ be a function that returns the last k digits of the input.

Let $s \colon \mathbb{N} \to \mathbb{N}$ be a function which returns the sum of the digits of the input.

Let $s' \colon \mathbb{N} \to \mathbb{N}$ be the sum of digits of its input with alternating sign, where the units digit is positive.

Let $s'' \colon \mathbb{N} \to \mathbb{N}$ be the sum of the two digit pairs of its input where the ones and tens digits are paired together.

- $2 \mid n$ *if and only if* $2 \mid d_1(n)$.
- $3 \mid n$ *if and only if* $3 \mid s(n)$.
- $4 \mid n$ *if and only if* $4 \mid d_2(n)$.
- $5 \mid n$ *if and only if* $5 \mid d_1(n)$.
- $6 \mid n$ *if and only if* $2 \mid n$ *and* $3 \mid n$.
- *Let* $a, b \in \mathbb{Z}_{\geqslant 0}$ *with* $0 \leqslant b < 10$ *such that* $n = 10a + b$. *Now,* $7 \mid n$ *if* $7 \mid a - 2b$. *The converse is not true.*
- $8 \mid n$ *if and only if* $8 \mid d_3(n)$.
- $9 \mid n$ *if and only if* $9 \mid s(n)$.
- $10 \mid n$ *if and only if the last digit of* n *is* 0.
- $11 \mid n$ *if and only if* $11 \mid s'(n)$ *if and only if* $11 \mid s''(n)$.

Remark 2. There is nothing special about what we did for these numbers. The only important facts to consider are that we get nice results when considering numbers which divide a power of 10, or who have a multiple which is very close to a power of 10. Additionally, when the divisor is composite (like 6), it may be useful to seperate it into a product of coprime numbers.

Exercise 1. (1999 IMC A1) Find the remiander when 122333444455555666666777777788888888999999999 is divided by 9.

Exercise 2. Find a divisibility trick for 37.

Exercise 3. (1999 IMC A3) How many of the numbers $1^2, 2^2, \ldots, 1999^2$ have odd numbers in their tens digit?

Exercise 4. (2000 IMC A1) Find the units digit of 17^{2000}.

Exercise 5. (1993 MMO A1) Denote by $S(x)$ the sum of the digits of a positive integer x. Solve:

a) $x + S(x) + S(S(x)) = 1993$

b) $x + S(x) + S(S(x)) + S(S(S(x))) = 1993$

IMC refers to the Junior High School Division International Mathematics Competition and MMO refers to the Moscow Mathematics Olympiad.