Modular Arithmetic

Graham Middle School Math Olympiad Team

MODULAR ARITHMETIC

Modular arithmetic is a system of arithmetic for integers, which considers the remainder. In modular arithmetic, numbers ”wrap around” upon reaching a given fixed quantity (this given quantity is known as the *modulus*) to leave a remainder.

An intuitive usage of modular arithmetic is with a 12-hour clock. If it is 10:00 now, then in 5 hours the clock will show 3:00 instead of 15:00. 3 is the remainder of 15 with a modulus of 12.

A number $x \bmod N$ is the equivalent of asking for the remainder of x when divided by N. Two integers a and b are said to be congruent (or in the same equivalence class) modulo N if they have the same remainder upon division by N. In such a case, we say that

$$a \equiv b \pmod{N}.$$

ADDITION THEOREM FOR MODULAR ARITHMETIC

If $a + b = c$, then

$$a \pmod N + b \pmod N \equiv c \pmod N.$$

In other words, to find the remainder of the sum of two (or more) integers, we can instead sum the remainders of the individual integers. You might never have considered if this is true, but it has to be because $a/N + b/N = (a + b)/N$.

In elementary school you learned that all even numbers are divisible by 2. So you only need to know the last digit of a number to know if it is divisible by 2. We can prove that's true. Let a, b, c, d, e be the digits of a 5-digit number.

$$\overline{abcde} = a\times10^4+b\times10^3+c\times10^2+d\times10^1+e\times10^0.$$

With the exception of the units digit term, each term in this sum must have a value of zero $\pmod 2$ because all multiples of 10 are divisible by 2. By the addition theorem of modular arithmetic

$$\overline{abcde} \pmod 2 \equiv \overline{abcd0} \pmod 2 + e \pmod 2 \equiv e \pmod 2$$

note also that

$$\overline{abcde} \pmod 5 \equiv \overline{abcd0} \pmod 5 + e \pmod 5 \equiv e \pmod 5$$

since all powers of 10 are divisible by 5.

What about divisibility by 4? Ten is not divisible by 4, but every power of 10 greater than 100 is, so all multiples of 100 have a value of $0 \pmod 4$. Hence, the value of any number greater than $100 \pmod 4$ is equal to the value $\pmod 4$ of its last 2 digits. This gives us the divisibility rule for 4: a number is divisible by 4 if the number formed by its last two digits is divisible by 4. In fact, the remainder of any number divided by 4 is the remainder of the number formed by its last two digits. Going to the next power of 2,