Introduction to Number Theory

Colin Curtis; August Deer, Matthew Mallory, Glenn Sun and Richard Yim

9 August 2020

1 Definitions

On a clock, the hours are 1 through 12. In mathematics, we usually like to think about clocks as having hours from 0 to 11 instead, since those are the possible remainders when dividing by 12. To mathematically capture the idea that 5 o'clock is the same as 17 o'clock and 29 o'clock, let us formally define the following:

Definition 1.1. For integers a, b, n, we write $a \equiv b \pmod{n}$ (read "a is congruent to b mod n") if a and b have the same remainder when divided by n. Equivalently, $a \equiv b \pmod{n}$ if $a - b$ is divisible by n.

For example, numbers mod 12 represent the hours on a clock.
Statements such as $2 \equiv 14 \pmod{12}$ and $-12 \equiv 120 \pmod{12}$ are true. Here are some quick questions to test your understanding of the definition:

Question 1.2. Think about what it means to look at the integers mod 2.
What does it mean if $x \equiv 0 \pmod{2}$, or $x \equiv 1 \pmod{2}$?

Question 1.3. Using the definition of congruent numbers and the modulus, find **all** possible values for x.

1. $18 \equiv x \bmod 7$

2. $x \equiv 4 \bmod 5$

3. $9 \equiv 3 \bmod x$

2 Addition and Multiplication

When we do arithmetic (such as addition and multiplication) with numbers mod n, it is called modular arithmetic. Doing modular arithmetic is very similar to doing normal arithmetic, and one example is the following. It means that you can add equal things to both sides of an equation.

Proposition 2.1. *If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then $a + c \equiv b + d \pmod{n}$.*

Proof. By definition, $a \equiv b \pmod{n}$ means $a - b$ is divisible by n. That means we can write $a - b = kn$ for some integer k. Similarly, $c - d = jn$ for some integer j. Then $(a - b) + (c - d) = kn + jn = (k + j)n$, so $(a - b) + (c - d)$ is divisible by n. But this means $(a + c) - (b + d)$ is divisible by n, so by definition $a + c \equiv b + d \pmod{n}$. □

Remember that when we prove things, we have to use the definition and write in justified logical steps. It's not enough to just try some cases and say that we notice a pattern, because how do you know that the pattern continues forever?

Try the following for yourself.

Question 2.2. For each of the following statements, is it always true or are there cases where it is false? If always true, give proof. If sometimes false, give counterexample.

1. If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then $ac \equiv bd \pmod{n}$.
2. If $a \equiv b \pmod{n}$, then $a^k \equiv b^k \pmod{n}$ for all $k \geq 1$.
3. If $a + c \equiv b + c \pmod{n}$, then $a \equiv b \pmod{n}$.
4. If $ac \equiv bc \pmod{n}$, then $a \equiv b \pmod{n}$.

Now, try using these modular arithmetic rules to solve the following questions:

Question 2.3. What is the remainder when 16^{10} is divided by 15?

Question 2.4. What are the last two digits of the number $98^4 - 15^{10}$?