# MODULAR ARITHMETIC, MATH 215 FALL 2018 (WHYTE)

We are used to dividing the integers in to even and odd numbers:

$$Even = \{\ldots, -2, 0, 2, 4, \ldots\}$$

and

$$Odd = \{\ldots, -3, -1, 1, 3, 5, \ldots\}$$

and we know the rules for arithmetic :

$$Even + Even = Even$$
$$Even + Odd = Odd$$
$$Odd + Odd = Even$$

and

$$Even \times Even = Even$$
$$Even \times Odd = Even$$
$$Odd \times Odd = Odd$$

We can phrase this a bit more carefully using our discussions of congruences and the division algorithm. The evens are the integers congruent to 0 mod 2 and the odds are the numbers congruent to 1 mod 2. The rules that let us determine which type we get when adding or multiplying say :

**Proposition 0.1.** *Let $a$ and $b$ be integers, then:*

(1) *If $a \equiv 0$ mod 2 and $b \equiv 0$ mod 2 then $a + b \equiv 0$ mod 2 and $ab \equiv 0$ mod 2*
(2) *If $a \equiv 0$ mod 2 and $b \equiv 1$ mod 2 then $a + b \equiv 1$ mod 2 and $ab \equiv 0$ mod 2*
(3) *If $a \equiv 1$ mod 2 and $b \equiv 1$ mod 2 then $a + b \equiv 0$ mod 2 and $ab \equiv 1$ mod 2*

We can generalize this to equivalence modulo numbers other than 2. To begin with, when looking at equivalence modulo $n$, there are $n$ different classes, not just 2:

**Proposition 0.2.** *Let $n$ be a natural number. For any integer $a$ there is exactly one $r$ with $0 \leq r < n$ so that $a \equiv r \mod n$.*

And then we can see that if you know what class $a$ and $b$ are in then we know what classes $a + b$ and $ab$ are in:

**Proposition 0.3.** *Let $n$ be a natural number. For any integers $a \equiv a' \mod n$ and $b \equiv b' \mod n$ then:*

(1) $a + b \equiv a' + b' \mod n$
(2) $ab \equiv a'b' \mod n$

**Question 0.4.** *Why do we need to work with congruence classes - can't we just work with the two types of numbers : those divisible by $n$ and those not divisible by $n$? What goes wrong?*

This "arithmetic modulo $n$" is an example of what mathematician call a **ring** - a set of objects that can be added and multiplied and where most of the usual axioms of arithmetic hold:

**Proposition 0.5.** *For any $n \in \mathbb{N}$ the following hold:*

(1) *For any $a$ and $b$ we have $a + b \equiv b + a \mod n$ and $ab \equiv ba \mod n$*
(2) *For any $a$, $b$, and $c$ we have $(a + b) + c \equiv a + (b + c) \mod n$ and $(ab)c \equiv a(bc) \mod n$*
(3) *For any $a$, $b$, and $c$ we have $(a + b)c \equiv ac + bc \mod n$*
(4) *For any $a$ we have $a + 0 \equiv a \mod n$ and $a \times 1 \equiv a \mod n$*
(5) *For any $a$ there is a $b$ with $a + b \equiv 0 \mod n$*

All of these follow almost immediately from the corresponding axioms from $\mathbb{Z}$. But be careful, not everything is quite as simple as it looks. For example if we are working mod 5, so that set of remainders are $\{0, 1, 2, 3, 4\}$. In statement (5) above for $a = 2$ the corresponding $b$ is 3 ( we can't take $b = -2$ as that's not on our list, but $-2 \equiv 3 \mod 5$ and 3 is on the list)

To get some practice with modular arithmetic, here are some calculations

**Problem 0.6.** *Which of the following are true modulo* $12$*?*

(1) *Does* $5x \equiv 6$ *mod* $12$ *have a solution? How many?*
(2) *Does* $4x \equiv 6$ *mod* $12$ *have a solution? How many?*
(3) *Does* $x^2 + 1 \equiv 0$ *mod* $12$ *have a solution? How many?*
(4) *If* $xy \equiv 0$ *mod* $12$ *does it follow that* $x \equiv 0$ *mod* $12$ *or* $y \equiv 0$ *mod* $12$

The last part of this problem is the key to many questions of this sort, and it turns out to be closely related to Euclid's lemma.

**Proposition 0.7.** *Show that if* $p$ *is a prime number then* $xy \equiv 0$ *mod* $p$ *implies that* $x \equiv 0$ *mod* $p$ *or* $y \equiv 0$ *mod* $p$

on the other hand

**Proposition 0.8.** *Show that if* $n$ *is composite then there are* $x$ *and* $y$ *with* $x \not\equiv 0$ *mod* $n$ *and* $y \not\equiv 0$ *mod* $n$ *but where* $xy \equiv 0$ *mod* $n$

This says that arithmetic modulo primes is better behaved, for example:

**Proposition 0.9.** *Show that if* $p$ *is a prime number then every equation of the form* $ax \equiv b$ *mod* $p$ *with* $a \not\equiv 0$ *mod* $p$ *has at most one solution.*

and

**Proposition 0.10.** *Show that if* $p$ *is a prime number then if* $x^2 \equiv y^2$ *mod* $p$ *then* $x \equiv y$ *mod* $p$ *or* $x \equiv -y$ *mod* $p$

In some ways the arithmetic modulo a prime is even better behaved than for the integers. One of the things that makes the arithmetic of the integers complicated is that you can't always divide, but modulo a prime you can. To see this, start by proving there are reciprocals:

**Proposition 0.11.** *Show that if* $p$ *is a prime number then for every* $a \not\equiv 0$ *mod* $p$ *there is a* $b$ *with* $ab \equiv 1$ *mod* $p$ *(hint: Use the same fact that we use in the proof of Euclid's lemma - that there are* $n$ *and* $m$ *with* $an + pm = 1$*)*

and from there:

**Proposition 0.12.** *Show that if* $p$ *is a prime number then every equation of the form* $ax \equiv b$ *mod* $p$ *with* $a \not\equiv 0$ *mod* $p$ *has exactly one solution.*

For arithmetic modulo $n$ which is composite, this only sometimes works:

**Proposition 0.13.** *Show that if* $n$ *is a natural number then given an* $a$ *there is a* $b$ *with* $ab \equiv 1$ *mod* $n$ *if and only if* $gcd(a, n) = 1$ *(hint: Again, copy the proof of Euclid's lemma)*