2. Modular Arithmetic and Algebra.

Notation: The expression “$k|n$” means “$k$ divides $n$.”

Now fix a natural number $k > 1$.

**Definition 2.1.** Integers $a$ and $b$ are congruent modulo $k$ if $k|(a - b)$.

**Examples:**

- Odd numbers are congruent to other odd numbers modulo 2.
- Evens are congruent to evens (but not odds) modulo 2.
- Every natural number (or integer) $a$ is congruent to its remainder:  
  \[ a \equiv r \mod k \]
  where $r$ is, by definition, a whole number between 0 and $k - 1$.

Notation:

- We usually shorten “modulo” to “mod.”
- We write “$a \equiv b \mod k$” to mean “$a$ is congruent to $b \mod k$.”

**Congruence mod $k$** is an equivalence relation. That is:

(i) It is reflexive: $a \equiv a \mod k$.

(ii) It is symmetric: if $a \equiv b$, then $b \equiv a \mod k$.

(iii) It is transitive: if $a \equiv b$ and $b \equiv c$, then $a \equiv c \mod k$.

(The first two are easy, the third uses $(a - b) + (b - c) = (a - c)$).

There are $k$ equivalence classes of integers mod $k$. Namely:

- $[0] = \text{All the integers congruent to } 0 \mod k$
- $[1] = \text{All the integers congruent to } 1 \mod k$
- $...$
- $[d-1] = \text{All the integers congruent to } d - 1 \mod k$.

For example, the two equivalence classes of integers mod 2 are:

$[0] = \text{The even integers}$

$[1] = \text{The odd integers}$

**Mod $k$ arithmetic** is ordinary arithmetic applied to the $k$ equivalence classes of integers mod $k$. It can be computed by adding or multiplying “remainders” (between 0 and $k - 1$) and then taking the remainder.
Example: $2 + 3 = 5$ for natural numbers, but mod $k$ this looks like:

$$2 + 3 \equiv 0 + 1 \equiv 1 \mod 2$$
$$2 + 3 \equiv 2 + 0 \equiv 2 \mod 3$$
$$2 + 3 \equiv 5 \equiv 1 \mod 4$$
$$2 + 3 \equiv 5 \equiv 0 \mod 5$$
$$2 + 3 \equiv 5 \mod 6 \text{ or more.}$$

Example: $2 \cdot 3 = 6$, but mod $k$ this looks like:

$$2 \cdot 3 \equiv 0 \cdot 1 \equiv 0 \mod 2$$
$$2 \cdot 3 \equiv 2 \cdot 0 \equiv 0 \mod 3$$
$$2 \cdot 3 \equiv 6 \equiv 2 \mod 4$$
$$2 \cdot 3 \equiv 6 \equiv 1 \mod 5$$
$$2 \cdot 3 \equiv 6 \equiv 0 \mod 6$$
$$2 \cdot 3 \equiv 6 \mod 7 \text{ or more.}$$

Math Interlude: To be sure that the arithmetic is “well-defined:”

$$[a] + [b] := [a + b], \quad [a] \cdot [b] := [ab]$$

one needs to check that substitutions do not change the results mod $k$. That is, one needs to check that if $a \equiv a'$ and $b \equiv b'$ mod $k$, then:

$$a + b \equiv a' + b' \text{ and } ab \equiv a'b' \mod k$$

This is true because:

$$(a + b) - (a' + b') = (a - a') + (b - b') \text{ and } ab - a'b' = (a - a')b + a'(b - b')$$

The first few addition and multiplication tables:

Mod 2

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>

Mod 3

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
<th>2</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
<th>2</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>2</td>
<td>1</td>
</tr>
</tbody>
</table>
More mod k arithmetic: The additive inverse of an integer n is \(-n\).
This is of course also true mod k, but if we want to express the additive inverse in terms of remainders, we get:

\[ k - r \text{ is the additive inverse of } r \text{ because } r + (k - r) \equiv 0 \mod k \]

This means we can **subtract** by adding:

\[ r - s \equiv r + (k - s) \mod k \]

Much more interestingly, there can also be reciprocals (multiplicative inverses) mod k. Whenever s and t are integers that satisfy:

\[ st - 1 = nk \text{ for some } n, \text{ then } st \equiv 1 \mod k \]

and we’ll sloppily write \( t \equiv 1/s \mod k \). Then we can **divide** by s:

\[ r/s \equiv r \cdot t \mod k \]

**Examples:** 0 never has a reciprocal, and 1 is always its own reciprocal.

- (Mod 3) \( 1/2 \equiv 2 \) because \( 2 \cdot 2 - 1 = 3 \).
- (Mod 4) 2 has no reciprocal, \( 1/3 \equiv 3 \) because \( 3 \cdot 3 - 1 = 2 \cdot 4 \).
- (Mod 5) \( 1/2 \equiv 3, 1/3 \equiv 2, 1/4 \equiv 4 \).

**Mod k algebra** looks just like ordinary algebra except:

(i) The arithmetic is mod k arithmetic.

(ii) The equality is mod k congruence.

(iii) The variables stand for equivalence classes \([0],[1],\ldots,[k-1]\).
Observation: Unlike ordinary algebra of integers (or rational numbers), you can solve algebraic equations $\mod k$ by trying everything.

Example: Solve $x^2 \equiv -1 \mod k$ for small values of $k$:

- (Mod 2) $-1 \equiv 1$, and $1^2 \equiv 1$. One solution.
- (Mod 3) $-1 \equiv 2$ and $1^2 \equiv 1, 2^2 \equiv 1$. No solutions.
- (Mod 4) $-1 \equiv 1, 2^2 \equiv 0, 3^2 \equiv 1$. No solutions.
- (Mod 5) $-1 \equiv 4$ and $1^2 \equiv 1, 2^2 \equiv 4, 3^2 \equiv 4, 4^2 \equiv 1$. Two solutions!

Linear Equations: These are equations of the form $ax \equiv b \mod k$

Case 1. If $a$ has a reciprocal mod $k$, then $x \equiv b/a$ is the only solution.

Case 2. If $a$ has no reciprocal mod $k$, there may be no solutions or one solution or more than one solution! For example:

- $2x \equiv 3 \mod 4$ has no solutions, but $2x \equiv 2 \mod 4$ has two solutions ($x = 1$ and $x = 3$).

We generally like Case 1 (where things are certain) more than Case 2!

Roots of Polynomials: Suppose we are given a “mod $k$” polynomial:

$$p(x) = x^d + c_1 x^{d-1} + \cdots + c_d$$

and a root $r$ of the polynomial (mod $k$) (so that $p(r) \equiv 0 \mod k$). Then as in ordinary algebra, $x - r$ “goes into” $p(x) \mod k$. That is:

$$p(x) \equiv q(x)(x - r) \mod k$$

for some polynomial $q(x)$ and if we keep finding roots $r = r_1, \ldots, r_d$ we can keep factoring:

$$p(x) \equiv (x - r_1)(x - r_2) \cdots (x - r_d) \mod k$$

In ordinary algebra, there are no other roots of $p(x)$. That may not be the case here. Suppose $s$ is different from $r_1, r_2, \ldots, r_d$. Then:

$$p(s) \equiv (s - r_1)(s - r_2) \cdots (s - r_d) \mod k$$

Each $s - r_i \neq 0 \mod k$, but we can only conclude $p(s) \neq 0 \mod k$ if we know that products of non-zero numbers are non-zero mod $k$.

This is not true if $k$ is composite! If $k = ab$, then $ab \equiv 0 \mod k$.

This is true if $k$ is prime. When $k$ is prime, we will also see (in §4) that as is the case with the rational numbers and real numbers, every number (mod $k$) except for 0 will have a mod $k$ reciprocal.
Nasty and Nice Examples:

(a) Consider the polynomial $x^2 - 1 \mod 8$. This factors:

$$p(x) = (x - 1)(x + 1) \equiv (x - 1)(x - 7) \mod 8$$

BUT there are two other roots, namely $x \equiv 3$ and $x \equiv 5$ because:

$$2 \cdot 4 \equiv 0 \text{ and } 4 \cdot 6 \equiv 0 \mod 8$$

This is something we don’t usually want our polynomials to do!

(b) Consider next the polynomial $x^4 - 1$ modulo the first few primes, where the algebra of taking roots behaves better.

(Mod 2) this has one root and it factors:

$$x^4 - 1 \equiv (x - 1)^4 \mod 2$$

(Mod 3) this has two roots: 1 and 2 $\equiv -1$, and it factors:

$$x^4 - 1 \equiv (x^2 + 1)(x - 1)(x + 1) \equiv (x^2 + 1)(x - 1)(x - 2) \mod 3$$

with a polynomial left over $(x^2 + 1)$ that has no roots.

(Mod 5) this has four roots: $1, 2, 3, 4$, and it factors:

$$x^4 - 1 \equiv (x - 1)(x - 2)(x - 3)(x - 4) \mod 5$$

Completing the Square Mod $p$: Suppose we are given:

$$ax^2 + bx + c \equiv 0 \text{ with } a \not\equiv 0 \mod k$$

where $k = p$ is an odd prime (i.e. a prime other than 2). Then

(i) Subtract $c$ from both sides:

$$ax^2 + bx \equiv -c \mod k$$

(ii) Multiply both sides by $4a$ (which has a reciprocal):

$$4a^2x^2 + 4abx \equiv -4ac \mod k$$

(iii) Add $b^2$ to both sides:

$$4a^2x^2 + 4abx + b^2 \equiv b^2 - 4ac \mod k$$

(iv) Factor the left side as a perfect square:

$$(2ax + b)^2 \equiv b^2 - 4ac \mod k$$

Conclusion: As with ordinary quadratics there are three cases:

Case 1: $b^2 - 4ac \equiv 0 \mod k$. Then there is one root.

Case 2: $b^2 - 4ac \equiv d^2 \mod k$ for some $d$. Then there are two roots:

$$x \equiv (-b + d)/2a \text{ and } x \equiv (-b - d)/2a \mod k$$

Case 3: $b^2 - 4ac$ is not a square mod $k$. Then there are no roots.
Question 2.1. What numbers mod $p$ have square roots when $p$ is prime?

Notice: Every square except 0 (mod $p$) has two square roots (mod $p$), so it follows that half the numbers from 1 to $p - 1$ (mod $p$) are squares and the other half are not.

Examples:

(Mod 3) 1 is a square and 2 is not.

(Mod 5) 1 and 4 are squares. 2 and 3 are not.

(Mod 7) 1, 4 and 2 are squares. 3, 5 and 6 are not.

(Mod 11) 1, 4, 9, 5 and 3 are squares. 2, 6, 7, 8 and 10 are not.

(Mod 13) 1, 4, 9, 3, 12 and 10 are squares.

Example: How many mod $p$ roots does $x^2 + x + 1$ have?

$$b^2 - 4ac = 1 - 4 \equiv p - 3 \mod p$$

(Mod 3) $x^2 + x + 1$ has one root since $b^2 - 4ac \equiv 0$.

(Mod 5) $x^2 + x + 1$ has no roots, since 2 is not a square.

(Mod 7) $x^2 + x + 1$ has two roots, since 4 is a square.

(Mod 11) $x^2 + x + 1$ has no roots since 8 is not a square.

(Mod 13) $x^2 + x + 1$ has two roots, since 10 is a square.

Finally, something that has no analogue in “ordinary” algebra;

Definition 2.2: $a$ is primitive mod $p$ if the powers:

$$a, a^2, a^3, a^4, \ldots, a^{p-1} \mod p$$

are all different, hence fill up all the numbers mod $p$ except for 0.

Note: We’ll see later that primitives always exist.

Examples: When is 2 primitive mod $p$? (Obviously 1 never is!)

(Mod 3) $2^1 = 2, 2^2 \equiv 1$ so 2 is primitive.

(Mod 5) $2^1 \equiv 2, 2^2 \equiv 4, 2^3 \equiv 3, 2^4 \equiv 1$ so 2 is primitive.

(Mod 7) $2^1 \equiv 2, 2^2 \equiv 4, 2^3 \equiv 1, 2^4 \equiv 2$. Stop. 2 isn’t primitive!

(Mod 11) 2, 4, 8, 5, 10, 9, 7, 3, 6, 1 are the powers, so 2 is primitive!.

Open Problem 4. Is 2 primitive mod $p$ for infinitely many primes? Is any number primitive mod $p$ for infinitely many primes?

Fun Fact: Once you find a primitive, then you know exactly which numbers have square roots! They are the even powers of the primitive. For example, 2 is primitive mod 11 and its even powers are: 4, 5, 9, 3, 1.