

Basic notions:

1. the integers \mathbb{Z} and the natural numbers (non-negatives) \mathbb{N} ,
2. divisibility: d divides n if n is a multiple of d - the functional use here is, $d|a$ iff $a = dt$ for some $t \in \mathbb{Z}$.
3. the division algorithm: for $a, n \in \mathbb{Z}$, $n > 1$, there exist unique $q, r \in \mathbb{Z}$ such that $a = nq + r$ and $0 \leq r < n$. The uniqueness is an important aspect that appears in many elementary proofs.
4. common divisors and greatest common divisors. Recall that the gcd is NOT defined as the numerically largest common divisor; rather $d = \gcd(a, b)$ if (i) $d|a$ and $d|b$, and (ii) if $d_1|a$ and $d_2|b$ then $d_1|d$.

Linear equations in two variables in \mathbb{Z} .

For $a, b \in \mathbb{Z}$, not both 0, and $c \in \mathbb{Z}$, the equation

$$ax + by = c$$

has a solution in $x, y \in \mathbb{Z}$, if and only if $\gcd(a, b) = d|c$.

This is the fundamental observation that we need when we start to investigate linear equations in congruences, modulo n and in \mathbb{Z}_n , in the variables x and y ; *i.e.*,

$$ax \equiv b \pmod{n},$$

$$[a]_n[x]_n = [b]_n.$$

The linear congruence

$[a]_n[x]_n = [b]_n$ has a solution $[x]_n \in \mathbb{Z}_n$

$\Leftrightarrow ax \equiv b \pmod{n}$ has a solution $x \in \mathbb{Z}$ (and, hence infinitely many solutions $x + nt$, for all $t \in \mathbb{Z}$)

\Leftrightarrow

$ax + nt = b$ has a solution in $x, t \in \mathbb{Z}$

Our theorem says this only happens if $\gcd(a, n)|b$. So to solve any one of these problems we solve by using the Euclidean algorithm and working backwards to find x .

So we have three different ways of considering remainders:

1. The division algorithm. A static result, telling us what the remainder is.
2. Congruence. A dynamic approach to studying remainders: If a and b have remainders p and q , when divided by n , then the remainder of ab [$a \pm b$] when divided by n is the same as that obtained when pq [$p \pm q$] is divided by n .
3. The system \mathbb{Z}_n . This reduces our study to the set of congruence classes, a finite set. The algebraic system $(\mathbb{Z}_n, +, \cdot)$ is a set with operations addition and multiplication. We will continue to investigate the similarities between \mathbb{Z}_n and other systems, such as \mathbb{Z} and the set of polynomials over \mathbb{Z} , $\mathbb{Z}[x]$.

A very important thing to consider is the following: Our end result is to develop an understanding of the *FINITE* structures \mathbb{Z}_n and their behavior under addition and subtraction.

First of all there are the basic properties of \mathbb{Z}_n in different guises:

Addition is commutative		
$a + b = b + a$	$a + b \equiv b + a \pmod{n}$	$[a]_n + [b]_n = [b]_n + [a]_n$
Multiplication is commutative		
You	Do	It
Addition is associative		
$a + (b + c) = (a + b) + c$	$a + (b + c) \equiv (a + b) + c \pmod{n}$	$[a]_n + ([b]_n + [c]_n) = ([a]_n + [b]_n) + [c]_n$
Multiplication is associative		
You	Do	It
The Distributive laws		
You	Do	It
Additive identity		
$a + 0 = a$	$a + 0 \equiv a \pmod{n}$	$[a]_n + [0]_n = [a]_n$
Additive inverses- for $\forall a \in \mathbb{Z}$, $\exists(-a) \in \mathbb{Z}$		
$a + (-a) = 0$	$a + (-a) \equiv 0 \pmod{n}$	$[a]_n + [(-a)]_n = [0]_n$
Multiplicative identity		
$a \cdot 1 = a$	$a \cdot 1 \equiv a \pmod{n}$	$[a]_n \cdot [1]_n = [a]_n$

We know do an example showing that our ideas are connected.

EXAMPLE: Solve $[6]_{15}[x]_{15} = [9]_{15}$.

This is equivalent to the congruence $6x \equiv 9 \pmod{15}$.

This has a solution if and only if $\gcd(6, 15) | 9$, which it does.

To solve $6x \equiv 9 \pmod{15}$, we change to the equivalent equation $6x + 15y = 9$ in \mathbb{Z} . Note this is a special case (see Thm 1.3.5).

1. We first divide $6x + 15y = 9$ by 3 obtaining $2x + 5y = 3$ [$2x \equiv 3 \pmod{5}$].
2. Now solve $2x + 5y = 1 = \gcd(2, 5)$ by Euclidean algorithm and *working backwards*, to obtain the solution $x = -2, y = 1$.
3. So $2(-2) + 5(1) = 1$, and multiplying by 3 we get $2(-6) + 5(3) = 3$, so $x = -6$ is a solution to $2x \equiv 3 \pmod{5}$. Or since $-6 \equiv 4 \pmod{5}$, 4 is a solution.
4. Our solutions to $6x \equiv 9 \pmod{15}$ and $x \equiv 4, 9, 14 \pmod{15}$, and the solutions to $[6]_{15}[x]_{15} = [9]_{15}$ are $[4]_{15}, [9]_{15}, [14]_{15}$

So What's the deal about \mathbb{Z}_n^\times ?

Recall that $\mathbb{Z}_n^\times = \{[a]_n : (a, n) = 1\}$.

Comments:

1. This is a well defined criterion for inclusion in \mathbb{Z}_n^\times . What do we mean by that? Well, one of your exercises was to prove that if $a \equiv b \pmod{n}$, then $\gcd(a, n) = \gcd(b, n)$. So, if a is relatively prime to n , then any number in $[a]_n$ is also relatively prime to n - *doesn't matter* which representative we test.
2. We also know that if $(a, n) = 1$ and $(b, n) = 1$, then $(ab, n) = 1$ (Why?), so if $[a]_n, [b]_n \in \mathbb{Z}_n^\times$, then $[ab]_n \in \mathbb{Z}_n^\times$. OR, \mathbb{Z}_n^\times is *closed* under multiplication.
3. If $[a]_n \in \mathbb{Z}_n^\times$, then $[-a]_n \in \mathbb{Z}_n^\times$.
4. If $[a]_n \in \mathbb{Z}_n^\times$, then there is $[r]_n \in \mathbb{Z}_n^\times$ such that $[a]_n[r]_n = [1]_n$. Then $[r]_n[a]_n = [1]_n$, and in this case we say that $[r]_n$ is the *inverse* of $[a]_n$. The following facts should be accessible:
 - (a) The inverse is unique, that is, if $[a]_n[r]_n = [a]_n[s]_n = [1]_n$, then $[r]_n = [s]_n$, thus the notation $[a]_n^{-1} = [r]_n$ is well defined and useful. This is proved by our "sandwich" method for proving unicity - similar to the proof that identities and additive inverses are unique.
 - (b) If $[a]_n$ is *invertible* (that is, $[a]_n \in \mathbb{Z}_n^\times$), then $[r]_n = [a]_n^{-1} \in \mathbb{Z}_n^\times$. So \mathbb{Z}_n^\times is *closed under the taking of inverses*. This is straightforward: if $[a]_n[r]_n = [1]_n$, then $[r]_n$ has inverse $[a]_n$ and is thus invertible, in \mathbb{Z}_n^\times .
5. However,
 \mathbb{Z}_n^\times is *not closed under addition*, after all, $[0]_n = [a]_n + [-a]_n$ is never in \mathbb{Z}_n^\times .

So, \mathbb{Z}_n^\times is closed under \times , but not $+$; thus we don't consider addition when we discuss \mathbb{Z}_n^\times . These are the key points about \mathbb{Z}_n^\times :

1. Multiplication in \mathbb{Z}_n^\times is commutative - this is inherited from \mathbb{Z} which has commutative multiplication.
2. Multiplication in \mathbb{Z}_n^\times is associative.
3. There is an identity, $[1]_n$, it is its own inverse. That is, $[1]_n[a]_n = [a]_n$ for all $[a]_n \in \mathbb{Z}_n$, including $[1]_n[1]_n = [1]_n$.
4. Every element of \mathbb{Z}_n^\times has an inverse.

This is our first example of what is called a *finite group*.

The next example of a group is the set of bijections (one-to-one and onto functions) from a set S to S is the collection of functions $Sym(S)$. If S is finite, with n elements we generally operate as if $S = \{1, 2, \dots, n\}$, and denote the set of functions S_n . Our focus now is on S finite. Notice that S_n has many similarities with \mathbb{Z}_n^\times : These are the key points about \mathbb{Z}_n^\times :

1. Multiplication in S_n is *NOT* commutative - this is typical for families of functions.
2. Multiplication in S_n is associative. This is because composition of functions is associative.
3. There is an identity, (1) , it is also its own inverse.
4. Every element of S_n has an inverse (function). Note, any bijection has an inverse function.

So \mathbb{Z}_n^\times and S_n have the following in common: (i) they have an associative multiplication, (ii) there is a unique identity, (iii) every element has a unique inverse. The most apparent difference is that multiplication in \mathbb{Z}_n^\times is associative and that in S_n is not. \mathbb{Z}_n^\times is a *commutative (or abelian)* group, and S_n is not commutative (non-abelian). A *group* is a set G with an operation $*$ that is associative, has an identity and every element has an inverse. We will study these in detail, but you need only know the properties above, not the vocabulary. So what do you need to know HOW to do?

Procedures:

1. Properly apply the division algorithm - careful when dividing negative numbers!
2. Apply the Euclidean algorithm and express the gcd as a linear combo of the two integers involved.
3. Use of the above to solve linear congruences and equations in \mathbb{Z}_n as discussed in the example.
4. Solving linear congruence continued: application of Thm 1.3.5, and the Chinese remainder theorem (thm 1.3.6 and example 1.3.4).
5. Computation of the number of elements of \mathbb{Z}_n^\times and identifying them (sec 1.4)
6. Proving something is invertible or a zero divisor.
7. Computing powers, modulo n , efficiently.
8. Proving a function is well-defined, one-to-one or onto.
9. Finding equivalence classes for common equivalence relations.
10. Working with permutations: two line and cycle notation - how to convert between the two. How do you multiply? What's the order of an element? When is a permutation even/odd?

You need to know the definitions and theorems we discussed in class. Don't forget the definitions about partitions, and functions. Short proofs that might be on the test include:

1. If we apply the division algorithm to a by dividing by d , then we get $a = nq + r$, prove $\gcd(a, n) = \gcd(r, n)$.
2. $a \equiv b \pmod{n}$ if and only if $n|(b - a)$.
3. Prop 1.2.3, 1.2.5, 1.3.3, 1.3.4, 1.4.5.
4. Composition of 1-1 (onto) functions is a 1-1 (onto) functions.
5. Equivalence classes form a partition, and a partition induces an equivalence relation - be able to "explain" this.
6. Be able to explain the ideas presented in Defn 2.26 and Thm 2.2.7.
7. Questions on S_n and $Sym(S)$ will be limited to definitions and calculations in S_n (using both notations).