More modular arithmetic

<u>Recall</u>: Fix $n \in \mathbb{N}$. for $a, b \in \mathbb{Z}$

$$a \equiv b \mod n \iff n \mid b-a$$

$[a] = \{ b \in \mathbb{Z} \mid a \equiv b \mod n \}$ = congreunce class of a modulo n.

$$\mathbb{Z}_n = \{ [a] \mid a \in \mathbb{Z} \} = \{ [0], [1], \dots, [n-1] \}$$

Defie $[a]+[b] = [a+b]$ and $[a][b] = [ab]$
this is independent of choice of representatives since
$a \equiv a' \mod n$ and $b \equiv b' \mod n \Rightarrow a+b \equiv a'+b' \mod n$
$ab \equiv a'b' \mod n$.

$+$ and $\cdot$ are commutative and associative. Distributive law holds.
$[0]$ is additive identity $[1]$ is multiplicative identity
additive inverses exist.

A <u>Group</u> is a set with an operation which satisfies the associative law, has an identity element, and for which every element has an inverse.

$(\mathbb{Z}_n, +)$ is a group: $([a]+[b])+[c] = [a]+([b]+[c])$
$[0]+[a] = [a]$
$[a]+[-a] = [0]$

$(\mathbb{Z}_n, \cdot)$ is not a group: $([a][b])[c] = [a]([b][c])$ ok
$[1][a] = [a]$ ok
But there may not be an inverse $[a]^{-1}$ such that
$[a]^{-1}[a] = [1]$ Eg if $[a]=[0]$. $[0][a] = [0] \neq [1]$

We pose this as a problem: Which $[a] \in \mathbb{Z}_n$ have a multiplicative inverse $[a]^{-1} \in \mathbb{Z}_n$

Eg. $n=5$, $a=2$, then if $b=3$ we have
$[a][b] = [2][3] = [6] = [1]$ in $\mathbb{Z}_5$
so $[2]^{-1} = [3]$ in $\mathbb{Z}_5$.

<u>Proposition 1.9.9</u> Fix $n \geq 2$. $[a] \in \mathbb{Z}_n$ has multiplicative inverse iff $\gcd(a,n) = 1$.
(a and n are relatively prime).

<u>Proof</u> Suppose $[a]$ has mult. inverse $[b]$, so
$[a][b] = [1]$ in $\mathbb{Z}_n$.
then $ab \equiv 1 \mod n$, $n \mid 1-ab$,
for some $t \in \mathbb{Z}$, $tn = 1-ab$
so $1 = tn + ab$. If $x \mid a$ and $x \mid n$, then $x \mid tn+ab = 1$ so $x = \pm 1$. Thus the greatest common divisor is 1.

Conversely, suppose $\gcd(a,n) = 1$. We can find $t, b \in \mathbb{Z}$ so that $tn + ab = \gcd(a,n) = 1$ then
$1 - ab = tn$ so $ab \equiv 1 \mod n$ so $[a][b] = [1]$. ∎

<u>Notation</u>: let $\mathbb{Z}_n^{\times} = \{[a] \in \mathbb{Z}_n \mid \gcd(a,n) = 1\} = \{[a] \mid [a] \text{ has mult. inv.}\}$

Denote by $[a]^{-1}$ a multiplicative inverse of $[a]$.

<u>Ex</u> $\mathbb{Z}_5^{\times} = \{[1], [2], [3], [4]\}$ $\mathbb{Z}_8^{\times} = \{[1], [3], [5], [7]\}$

<u>Proposition</u> $(\mathbb{Z}_n^\times, \cdot)$ is a group.

<u>Proof</u> Need to check $\mathbb{Z}_n^\times$ is <u>closed</u> under $\cdot$, that is, the product of two elements of $\mathbb{Z}_n^\times$ is an element of $\mathbb{Z}_n^\times$. (So far, we only know it is an element of $\mathbb{Z}_n$).

So suppose $[a], [b] \in \mathbb{Z}_n^\times$ then have $[a]^{-1}$ and $[b]^{-1}$ in $\mathbb{Z}_n$. then $([a][b])([a]^{-1}[b]^{-1}) = [a][a]^{-1}[b][b]^{-1} = [1][1] = [1]$. So $[a]^{-1}[b]^{-1}$ is an inverse for $[a][b]$, and we conclude $[a][b] \in \mathbb{Z}_n^\times$.

Associative ✓ Identity $[1] \in \mathbb{Z}_n^\times$ ✓ Inverses - by construction ✓

<u>Zero divisors</u> These are the elements $[a] \in \mathbb{Z}_n$, $[a] \neq 0$, there is a $[b] \in \mathbb{Z}_n$, $[b] \neq 0$, with $[a][b] = [0]$

e.g. in $\mathbb{Z}_6$ $[2][3] = [6] = [0]$.

<u>Fact</u>: in $\mathbb{Z}_n$, every element is either $[0]$, invertible, or a zero divisor.

<u>Chinese remainder theorem</u>:

"Suppose we wish to count a certain set of things. When we count by threes, we have two left over and when we count by fives we have three left over. How many things are there?"

This amounts to solving the system of congruences:

$$\begin{cases} x \equiv 2 \mod 3 \\ x \equiv 3 \mod 5 \end{cases}$$

<u>Proposition 1.7.9</u> (CRT) Take $a, b \in \mathbb{N}$ with $\gcd(a,b)=1$. For any $\alpha, \beta \in \mathbb{Z}$, the system of congruences

$$\begin{Bmatrix} x \equiv \alpha \mod a \\ x \equiv \beta \mod b \end{Bmatrix}$$

has a solution $x \in \mathbb{Z}$. Any two solutions are congruent modulo ab.

<u>Proof</u>: Since $\gcd(a,b)=1$, there exist $s, t \in \mathbb{Z}$ with $sa + tb = 1$.

Let $x_1 = 1 - sa = tb$ and $x_2 = 1 - tb = sa$

then $\begin{Bmatrix} x_1 \equiv 1 \mod a \\ x_1 \equiv 0 \mod b \end{Bmatrix}$ and $\begin{Bmatrix} x_2 \equiv 0 \mod a \\ x_2 \equiv 1 \mod b \end{Bmatrix}$

Let $x = \alpha x_1 + \beta x_2$: $x \equiv \alpha(1) + \beta(0) = \alpha \mod a$

$x \equiv \alpha(0) + \beta(1) = \beta \mod b.$

Uniqueness modulo ab: Suppose x and x' are two solutions then $x \equiv x' \mod a$, $x \equiv x' \mod b$ so $a \mid x - x'$ and $b \mid x - x'$

Because a and b are relatively prime, we find $ab \mid x - x'$ so $x \equiv x' \mod ab$. $\blacksquare$

<u>Reformulation</u>: Define a function $f: \mathbb{Z}_{ab} \to \mathbb{Z}_a \times \mathbb{Z}_b$

$$f([x]_{ab}) = ([x]_a, [x]_b)$$

The Chinese remainder theorem is equivalent to the statement that f is a bijection when $\gcd(a,b)=1$.

Now on to abstract groups!

<u>Definition</u>: A <u>group</u> consists of a set G and a binary operation
$$* : G \times G \to G \qquad (g,h) \mapsto g*h$$
satisfying

(1) for all $a,b,c \in G$, $a*(b*c) = (a*b)*c$

(2) There is an element $e \in G$ such that for all $a \in G$,
$$e*a = a = a*e$$

(3) For each $a \in G$ there is a $b \in G$ such that
$$a*b = e = b*a$$

We often omit the symbol $*$ and use juxaposition to denote the group operation: gh. The element b whose existence is gaurunteed by axiom (3) is denoted a^{-1}.

<u>Uniqueness of the identity</u>: There is only one element e such that $ea = a = ae$ for all $a \in G$

<u>Proof</u>: suppose e and e' are identities. so $ea = a = ae$ for all a
$e'a = a = ae'$ for all a

Consider ee'. $ee' = e'$ since e is identity
$ee' = e$ since e' is identity.

So $e = e'$ $\blacksquare$

<u>Uniqueness of inverses</u> For each $a \in G$ there is only one $b \in G$ such that $ab = e = ba$.

<u>Proof</u> suppose b and b' are both inverses. so
$$ab = e = ba \qquad ab' = e = b'a.$$

Consider
$$bab' = (ba)b' = eb' = b'$$
$$bab' = b(ab') = be = b$$
so $b = b'$ $\blacksquare$.

<u>Inverse of the inverse = same</u> For any $g \in G$, $(g^{-1})^{-1} = g$

<u>Proof</u> $gg^{-1} = e = g^{-1}g$, so g is an inverse of g^{-1}.

by uniqueness of the inverse of g^{-1}, $g = (g^{-1})^{-1}$.

<u>Inverse of a product</u>: For any $g, h \in G$, $(gh)^{-1} = h^{-1}g^{-1}$

NOTE ORDER.

<u>Proof</u>: $(gh)(h^{-1}g^{-1}) = g(h(h^{-1}g^{-1})) = g((hh^{-1})g^{-1})$

$= g(eg^{-1}) = gg^{-1} = e$ so $h^{-1}g^{-1}$ is an inverse of gh

use uniqueness of inverses.

<u>General associative law</u>: consider a product of k factors.

$a_1 a_2 \cdots a_k$.

We can put parentheses in in many different ways.

$((a_1a_2)a_3)a_4$ vs $(a_1a_2)(a_3a_4)$ vs $a_1(a_2(a_3a_4))$

vs $a_1((a_2a_3)a_4)$ vs $(a_1(a_2a_3))a_4$.

The <u>general associative law</u> is the statement that all ways of grouping give the same result.

<u>Fact</u>: The basic associative law $(ab)c = a(bc)$ implies the general associative law.

Intuitively: any two "parenthesizations" can be connected by repeated application of the basic associative law.

See Goodman Proposition 2.1.19.