The algebra of $\mathbb{Z}_n$

Geoff Smith, University of Bath

29th October 2018

Addition and Multiplication

Addition in $\mathbb{Z}_n$ is commutative, associative, it has a unique two sided identity $[0]$, and each $[x]$ has a unique additive inverse $[-x]$. These facts are consequences of analogous laws for $\mathbb{Z}$, as we now demonstrate.

(i) Commutativity of addition: suppose that $[x], [y] \in \mathbb{Z}_n$. Then $[x] + [y] = [x + y]$ by definition of addition in $\mathbb{Z}_n$. Now $x + y = y + x$ because addition of integers is commutative. Then unwrap using the definition of addition in $\mathbb{Z}_n$ again:

$$[x] + [y] = [x + y] = [y + x] = [y] + [x].$$

Therefore addition in $\mathbb{Z}_n$ is commutative.

(ii) Associativity of addition: suppose that $[x], [y], [z] \in \mathbb{Z}_n$.

$$([x] + [y]) + [z] = [x + y] + [z] = [(x + y) + z]$$

by definition of addition in $\mathbb{Z}_n$. Now use the associative law in $\mathbb{Z}$ and unwrap.

$$([x] + [y]) + [z] = [(x + y) + z] = [x + (y + z)] = [x] + ([y] + [z]).$$

Therefore addition in $\mathbb{Z}_n$ is associative.

(iii) Notice that $[0]$ is an additive identity in $\mathbb{Z}_n$ because for all $[x] \in \mathbb{Z}_n$ we have

$$[x] + [0] = [x] = [0] + [x].$$

If $[u]$ is a rival additive identity, then for each $[x] \in \mathbb{Z}_n$ we have

$$[x] + [u] = [x] = [u] + [x]. \tag{1}$$

Apply the second equation of equations (1) when $x = 0$ to deduce that $[0] = [u] + [0]$. However, $[u] + [0] = [u + 0] = [u]$. Therefore $[u] = [0]$ (i.e. $n \mid u$). Therefore $\mathbb{Z}_n$ has a unique additive identity.

(iv) Existence and uniqueness of additive inverses. Suppose that $[x] \in \mathbb{Z}_n$. Clearly $[x] + [-x] = [-x] + [x] = [0]$ so $[-x]$ is an additive inverse for $[x]$. Suppose that $[y]$ is a rival additive inverse for $[x]$. Then

$$[x] + [y] = [0] = [y] + [x]. \tag{2}$$

Now $[x] + [y] = [0]$ from the first equation of equations 2. Add $[-x]$ to both sides: $[-x]+([x]+[y]) = [-x]+[0]$. Use the associtive law on the left so $([-x]+[x])+[y] = [-x]$. Therefore $[0]+[y] = [-x]$ and so $[y] = [-x]$. Therefore $[-x]$ is the unique additive inverse of $[x]$.

Next we tackle the multiplicative structure of $\mathbb{Z}_n$ with the same enthusiasm.

(v) Commutativity of multiplication: suppose that $[x], [y] \in \mathbb{Z}_n$. Then $[x][y] = [xy]$ by definition of addition in $\mathbb{Z}_n$ and $xy = yx$ because multiplication of integers is commutative. Then unwrap using the definition of multiplication in $\mathbb{Z}_n$ again:

$$[x][y] = [xy] = [yx] = [y][x].$$

Therefore multiplication in $\mathbb{Z}_n$ is commutative.

(vi) Associativity of multiplication: suppose that $[x], [y], [z] \in \mathbb{Z}_n$.

$$([x][y])[z] = [xy][z] = [(xy)z]$$

by definition of multiplication in $\mathbb{Z}_n$. Now use the associative law in $\mathbb{Z}$ and unwrap.

$$([x][y])[z] = [(xy)z] = [x(yz)] = [x]([y][z]).$$

Therefore multiplication in $\mathbb{Z}_n$ is associative.

(vii) Notice that $[1]$ is a multiplicative identity in $\mathbb{Z}_n$ because for all $[x] \in \mathbb{Z}_n$ we have

$$[x][1] = [x] = [1][x].$$

If $[u]$ is a rival multiplicative identity, then for each $[x] \in \mathbb{Z}_n$ we have

$$[x][u] = [x] = [u][x]. \tag{3}$$

Apply the second equation of equations (3) when $x = 1$ to deduce that $[1] = [u][1]$. However, $[u][1] = [u1] = [u]$. Therefore $[u] = [1]$ (i.e. $n \mid u - 1$). Therefore $\mathbb{Z}_n$ has a unique multiplicative identity element $[1]$.

(viii) Existence and uniqueness of multiplicative inverses. Suppose that $[x] \in \mathbb{Z}_n$. Clearly if $\gcd(x, n) \neq 1$, then it follows from theory in lecture that $[x]$ has no inverse in $\mathbb{Z}_n$. However, suppose that $\gcd(x, n) = 1$, so $[x]$ has a multiplicative inverse $[y]$. Suppose that $[z]$ is also a multiplicative inverse for $[x]$. Then $[x][y] = [1] = [y][x]$ and $[x][z] = [1] = [z][x]$. Therefore $[x][y] = [x][z]$. Multiply on the left be $[y]$,s

$$[y]([x][y]) = [y]([x][z])].$$

Deploy the associative law so that

$$([y][x])[y] = ([y][x])[z]$$

so $[1][y] = [1][z]$ and so $[y] = [z]$. Therefore $[x]$ has a unique multiplicative inverse.

How do addition and multiplication interact?

Multiplication distributes over addition. Suppose that $[x], [y], [z] \in \mathbb{Z}$. Then

$$[x]([y] + [z]) = [x]([y + z]$$

) by definition of addition in $\mathbb{Z}_n$. Therefore

$$[x]([y] + [z]) = [x(y + z)] = [xy + xz]$$

because multiplication distributes over addition in $\mathbb{Z}$. Therefore

$$[x]([y] + [z]) = [x][y] + [x][z]$$

and multiplication distributes over addition in $\mathbb{Z}_n$. By deploying the commutative law of multiplication, it follows that

$$([y] + [z])[x] = [y][x] + [z][x].$$

Observation

As we all know $\frac{1}{2} + \frac{1}{3} + \frac{1}{6} = 1$. Equivalently $3 + 2 + 1 = 6$ (multiplying through by 6). Now choose an integer n coprime to 6, and therefore coprime to 2 and 3. Then working in $\mathbb{Z}_n$ (i.e. modulo n) we have $[3] + [2] + [1] = [6]$. Now $[6]$ has a (unique) multiplicative inverse $[6]^{-1}$, as do $[2]$ and $[3]$. Also note that $[2]^{-1}[3]^{-1}$ is a multipliative inverse for $[6] = [2][3]$ and so $[2]^{-1}[3]^{-1} = [6]^{-1}$ by uniqueness of multiplicative inverses. Now multiply through by $[6]^{-1}$ to discover that $[2]^{-1} + [3]^{-1} + [6]^{-1} = [1]$ which is an echo of $\frac{1}{2} + \frac{1}{3} + \frac{1}{6} = 1$ in $\mathbb{Q}$. By similar reasoning, any correct equation relating rational numbers will be true in $\mathbb{Z}_n$ provided that n is coprime to the denominators of all fractions mentioned in the equation.

Thus it makes perfect sense to talk about the equivalence class of a rational number, providing that the denominator is coprime with the modulus. For example, consider $22/7$ mod 100. this is $[22][7]^{-1}$. Now $7^4 = 2401 \equiv 1 \bmod 100$, so $[7]^3 = [7]^{-1}$ and so $[7]^{-1} = [343] = [43]$ in $\mathbb{Z}_{100}$. Therefore

$$[22/7] = [22][43] = [946] = [46] \in \mathbb{Z}_{100}.$$