Lecture 10: The monoid $\mathbb{Z}_n$ and the group U_n

In the last lecture, I developed the group theory I shall need. In this lecture, I shall introduce the groups that we shall study. These are the most important groups in elementary number theory. We shall define them as groups of units of some monoids so it is with the monoids we shall start.

The monoid $\mathbb{Z}_n$

The monoid of integers $\mathbb{Z}$ — which we always regard as being equipped with the binary operation of multiplication — can be regarded as being laid out in a straight line infinite in both directions. We shall now show how it can be rolled up into circles of different sizes. The idea goes back to Gauss (who else?).

Let $n \geq 1$. We fix this number and call it our *modulus*. We define a relation on $\mathbb{Z}$ in terms of n as follows:

$$a \equiv b \pmod{n}$$

iff a and b have the same remainder when each number is divided by n; equivalently,

$$n \mid a - b.$$

We say that *a is equivalent to b modulo n*. When n is known I shall just write $a \equiv b$.

Proposition 0.1. *With the above definition we have the following:*

(1) $\equiv$ *is an equivalence relation.*
(2) *If $a \equiv a'$ and $b \equiv b'$ then $ab \equiv a'b'$.*

Proof. (1) This will be set as an exercise.

(2) Suppose that $a \equiv b$ and $a' \equiv b'$. Then by definition $a = a' + nr$ and $b = b' + ns$ for some integers r and s. It follows that $ab = a'b' + nsa' + nrb' + n^2rs$ and so $ab - a'b'$ is divisible by n. □

This the congruence relation partitions the set set of integers into a finite number of blocks. I shall denote the set of congruence classes of $\equiv$ by $\mathbb{Z}_n$. I shall denote the congruence class containing a by $[a]$.

Proposition 0.2. *On the set $\mathbb{Z}_n$ define the operation*

$$[a][b] = [ab].$$

Then this is well-defined and with respect to it $\mathbb{Z}_n$ becomes a commutative monoid

Proof. I'll just prove that the multiplication is well-defined and leave the remainder of the proof for the exercises. We need to prove that if

$[a] = [a']$ and $[b] = [b']$ then $[ab] = [a'b']$. But $[a][b] = [ab] = [a'b']$ be the above and so the multiplication is well-defined. □

It is this monoid that will play the key role in cryptography.

Notation One problem is the the equivalence class $[a]$ contains infinitely many elements. This means that each congruence class has infinitely many names — the same is true for the elements of $\mathbb{Q}$. Usually, the elements of $\mathbb{Z}_n$ will be named thus

$$\mathbb{Z}_n = \{[0], [1], [2], [3], \ldots, [n-1]\}.$$

We often omit the square brackets and write 2 when we mean [2]. This is not a problem as long as we remember that we are working with an equivalence relation.

As an example, here is the Cayley table for the multiplicative monoid $\mathbb{Z}_{10}$. I have written a instead of $[a]$ and I therefore need only deal with the numbers in the range $0 \leq a < 10$. In this example, I have highlighted the invertible elements and so the group of units of $\mathbb{Z}_{10}$.

	0	**1**	2	**3**	4	5	6	**7**	8	**9**
0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9
2	0	2	4	6	8	0	2	4	6	8
3	0	3	6	9	2	5	8	1	4	7
4	0	4	8	2	6	0	4	8	2	6
5	0	5	0	5	0	5	0	5	0	5
6	0	6	2	8	4	0	6	2	8	4
7	0	7	4	1	8	5	2	9	6	3
8	0	8	6	4	2	0	8	6	4	2
9	0	9	8	7	6	5	4	3	2	1

Here $U(\mathbf{Z}_{10}) = \{1, 3, 7, 9\}$. We now examine this topic in the general case.

The group $\mathbb{U}_n$

We have a monoid so we may ask what its group of units is. It is this group that is our main interest.

Proposition 0.3. *In the monoid $\mathbb{Z}_n$ an element $[a]$ is invertible if and only if $\gcd(a, n) = 1$. If it is invertible, we may calculate its inverse using Bézout's Lemma.*

Proof. Suppose first that $[a]$ is invertible. Then there exists an element $[b]$ such that $[a][b] = [1]$. By definition $[ab] = [1]$. It follows that

when ab is divided by n the remainder is 1. We may therefore write $ab = qn + 1$. Thus $1 = ab - qn$. Any common divisor of a and n must divide 1. It follows that $\gcd(a, n) = 1$.

To prove the converse, suppose that $\gcd(a, n) = 1$. Then by Bézout's theorem there exist integers x and y such that $ax + ny = 1$. It follows that mod n we have that $ax \equiv 1$ and so $[a][x] = [1]$ and we have shown that $[a]$ is invertible. □

We denote by U_n the group of units of the monoid $\mathbb{Z}_n$. To determine if $0 \leq a < n$ is invertible we use Euclid's algorithm: $[a]$ is invertible if and only if $\gcd(a, n) = 1$; that is, if and only if a and n is coprime. If it is invertible then we shall want to find its inverse. To do that we use Blankinship's algorithm to find integers x and y such that

$$1 = ax + ny.$$

Thus the inverse of $[a]$ is $[x]$. Usually, we want $0 \leq x < n$ as well. That is easy to accomplish by adding or subtracting suitable multiples of n. Here is a concrete example.

Show that 3 is invertible in $\mathbb{Z}_{220}$ and find its inverse. First we check that $\gcd(3, 220) = 1$. This turns out to be the case and so now we apply Blankinship and we get that

$$1 = 220 \times 1 + (-73) \times 3.$$

Thus $[-73][3] = [1]$. However, we would like an answer in the usual range. Here it is enough to consider $220 - 73 = 147$. Thus $[3]^{-1} = [147]$ in $\mathbb{Z}_{220}$. You should of course always check your answers.

We see by the above result that the order of $\mathbb{U}_n$ is equal to the number of natural numbers less than or equal to n which are coprime to n. We denote this number by $\phi(n)$, called the *Euler ϕ-function.*

$\mathbb{Z}_n$ is actually a ring

In fact, $\mathbb{Z}_n$ is not just a monoid. This would be an opportune moment to refresh your memory on some standard definitions in algebra.

Algebraic structures usually come in two types: those with one binary operation and those with two. Semigroups, monoids, groups and abelian groups each have one binary operation. Classically, structures with two binary operations have the following form: there is an abelian group $(R, +)$ and there is a monoid $(R, \times)$ which also has a zero. The two operations are linked by the left and right distributivity laws:

$$a \times (b + c) = a \times b + a \times c \quad (b + c) \times a = b \times a + c \times a.$$

Such a structure is called a *ring.* If the monoid is also commutative it is called a *commutative ring.* A commutative ring in which every

element of the monoid apart from the zero is invertible is called a *field*. Thus $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are all fields, and $\mathbb{Z}$ is a ring as is $M_n(\mathbb{R})$.

It is not hard to show that $\mathbb{Z}_n$ is in fact a ring: the other operation is addition where $[a] + [b] = [a + b]$. That this is well-defined is easy to prove and $\mathbb{Z}_n$ with respect to addition is an abelian group.

It is important to remember that in this course the only operation we consider on $\mathbb{Z}_n$ is multiplication.