

Exploring Abstract Algebra with Computer Software

PREP Workshop 2004

Section 8: Introduction to Rings

The set of integers mod a fixed n , \mathbf{Z}_n , is a ring with binary operations addition and multiplication mod n . When n is a prime p , \mathbf{Z}_p is a field. That is, \mathbf{Z}_p is a commutative ring with 1 and every nonzero element is a unit.

Fact: The nonzero elements of \mathbf{Z}_p form a cyclic group under multiplication mod p of order $p - 1$.

The function `Z` in GAP creates a generator for this cyclic group. For example:

```
gap> z:= Z(7);
gap> R:=Ring([z]);
GF(7)
gap> Elements(R);
[ 0*z(7), Z(7)^0, Z(7), Z(7)^2, Z(7)^3, Z(7)^4, Z(7)^5 ]
```

The nonzero elements of \mathbf{Z}_7 form a cyclic group of order 6 (under multiplication). The element `Z(7)` of \mathbf{R} denotes a generator of this cyclic group. Note that mod 7, $3^1 = 3, 3^2 = 2, 3^3 = 6, 3^4 = 4, 3^5 = 5$ and $3^6 = 1$, so 3 is a generator of this cyclic group. Also note that mod 7, $5^1 = 5, 5^2 = 4, 5^3 = 6, 5^4 = 2, 5^5 = 3$ and $5^6 = 1$, so 5 is also generator of this cyclic group. Thus `Z(7)` can be taken to mean either the 3 or 5 in \mathbf{Z}_7 . (Mod 7, $2^3 = 1, 4^3 = 1$ and $6^2 = 1$ so `Z(7)` can not be equal to 2, 4 or 6.) Recall cyclic groups of the same order n are isomorphic and are of the form $\{e, a, a^2, a^3, \dots, a^{n-1}\}$, where a denotes a generator (using multiplicative notation). If you would like to have GAP show you which of 3 or 5 in \mathbf{Z}_7 is being used to generate the nonzero elements type:

```
gap> Int(Z(7));
3
```

The `Int` function translate elements of \mathbf{Z}_p into integers. The function `One` is also useful. It gives the multiplicative identity in a ring and can be used to translate integers to elements in R . For example to see how 5 is denoted in $R = \mathbf{Z}_7$ type:

```
gap> 5*One(R);  
Z(7)^5
```

So $3^5 \bmod 7$ must be equal to $5 \bmod 7$:

```
gap> 3^5 mod 7;  
5
```

Section 8, Project 1

8.1 Use GAP to help you find for which of the primes $p = 3, 5, 7, 11, 13$, and 17 the equation $a^2 + b^2 = 0$ has a nontrivial solution in \mathbf{Z}_p . Make a conjecture about the the existence of a nontrivial solution of this equation in \mathbf{Z}_p for p a prime.

We will now investigate the number of idempotents and the number of nilpotent elements in the rings \mathbf{Z}_n . Recall that an *idempotent* in a ring R is an element r such that $r^2 = r$. A *nilpotent* element $r \in R$ is an element such that $r^m = 0$ for some positive integer m .

Fetch the file “nilpotentCount” off the web site. This file contains a function that counts the number of nilpotent elements in a given ring. (Thanks to Alexander Hulpke for providing a revised version of this function.) GAP has a built-in function called `Idempotents` that lists the idempotents in a ring. For an example follow along with the following GAP output. (GAP denotes a mod n in \mathbf{Z}_n by `ZmodnZObj(a,n)`.)

```
gap> M:= Integers mod 6;  
(Integers mod 6)  
gap> Idempotents(M);  
[ ZmodnZObj( 0, 6 ), ZmodnZObj( 1, 6 ), ZmodnZObj( 3, 6 ),  
  ZmodnZObj( 4, 6 ) ]  
gap> Size(Idempotents(M));  
4  
gap> N:= Integers mod 9;  
(Integers mod 9)  
gap> Size(Idempotents(N));  
2
```

The above tells us that \mathbf{Z}_6 has 4 idempotents and \mathbf{Z}_9 has 2 idempotents.

```
gap> Read("nilpotentCount");
gap> nilpotentCount(M);
1
gap> nilpotentCount(N);
3
```

The above tells us that \mathbf{Z}_6 has 1 nilpotent element and \mathbf{Z}_9 has 3 nilpotents.

Section 8, Project 2

8.2 Find the number of idempotents in \mathbf{Z}_n for many values of n . Based on your results answer the following:

- How many idempotents are in \mathbf{Z}_n when n is a prime-power?
- How many idempotents are in \mathbf{Z}_n when n is equal to the product of two distinct primes?
- In general, make a conjecture about the number of idempotents in \mathbf{Z}_n as a function of n .

8.3 Find the number of nilpotents in \mathbf{Z}_n for many values of n . Based on your results answer the following:

- How many nilpotents are in \mathbf{Z}_n when n is a prime-power?
- How many nilpotents are in \mathbf{Z}_n when n is equal to the product of two distinct primes?
- In general, make a conjecture about the number of nilpotents in \mathbf{Z}_n as a function of n .

8.4 Using GAP, find the number of units in \mathbf{Z}_n for many values of n . Make a conjecture about the number of units in \mathbf{Z}_n as a function of n . (The command `Elements(Units(R))` will list all the units in a given ring R .)

The following is the file “nilpotentCount”:

```
nilpotentCount:= function(R)
  local n;
```

```
n:= Size(R);  
return Length(Filtered(Elements(R), i -> IsZero(i^n)));  
end;
```