

12 Chapter: Introduction to Rings

The set of integers mod 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 (under multiplication) of order 6. The element `Z(7)` of `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 \mathbf{Z}_p . 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
```

Exercises

12.1 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 non-trivial solution of this equation in \mathbf{Z}_p for p a prime. [Gallian, Chapter 12, Computer Exercise 1] (If this exercise seems repetitive try writing a subroutine in `GAP`.)

The group of units in the ring of 2×2 matrices over \mathbf{Z}_n is denoted in `GAP` by `GL(2, Integers mod`

n). The subgroup of matrices with determinant equal to 1 is denoted by $\text{SL}(2, \text{Integers mod } n)$.

12.2 Find the orders of $\text{GL}(2, \mathbf{Z}_n)$ and $\text{SL}(2, \mathbf{Z}_n)$ for $n = 2, 3, 5, 7, 11$, and 13 . What relationship do you see between the orders of $\text{GL}(2, \mathbf{Z}_n)$ and $\text{SL}(2, \mathbf{Z}_n)$ when n is a prime? Find the orders of $\text{GL}(2, \mathbf{Z}_n)$ and $\text{SL}(2, \mathbf{Z}_n)$ for $n = 16, 27, 25$, and 49 . Make a conjecture about the relationship between the orders of $\text{GL}(2, \mathbf{Z}_n)$ and $\text{SL}(2, \mathbf{Z}_n)$ when n is a power of a prime. [Gallian, Chapter 12, Computer Exercise 4]

12.3 Find the orders of $\text{GL}(2, \mathbf{Z}_n)$ and $\text{SL}(2, \mathbf{Z}_n)$ for $n = 2, 4, 8, 16$, and 32 . How do the orders of the two groups change each time you increase the power of 2 by 1? Find the orders of $\text{GL}(2, \mathbf{Z}_n)$ and $\text{SL}(2, \mathbf{Z}_n)$ for $n = 3, 9, 27$, and 81 . How do the orders of the two groups change each time you increase the power of 3 by 1? Find the orders of $\text{GL}(2, \mathbf{Z}_n)$ and $\text{SL}(2, \mathbf{Z}_n)$ for $n = 5, 25, 125$, and 625 . How do the orders of the two groups change each time you increase the power of 5 by 1? Make a conjecture about the relationship between the orders of $\text{GL}(2, \mathbf{Z}_{p^i})$ and $\text{GL}(2, \mathbf{Z}_{p^{i+1}})$. Make a conjecture about the relationship between the orders of $\text{SL}(2, \mathbf{Z}_{p^i})$ and $\text{SL}(2, \mathbf{Z}_{p^{i+1}})$. [Gallian, Chapter 12, Computer Exercise 4]

12.4 Find the order of $\text{GL}(2, \mathbf{Z}_n)$ for $n = 12, 15, 20, 21$, and 30 . Make a conjecture about the order of $\text{GL}(2, \mathbf{Z}_n)$ in terms of the orders of $\text{GL}(2, \mathbf{Z}_s)$ and $\text{GL}(2, \mathbf{Z}_t)$ where $n = st$ and s and t are relatively prime. [Gallian, Chapter 12, Computer Exercise 4]

12.5 Fetch the subroutine `intror2` from the manual web site and read it into `GAP`. This function takes as input an integer n and returns a list of all the solutions to the equation $x^2 = -1$ in the ring \mathbf{Z}_n . For example `intror2(5)` will list all the solutions in \mathbf{Z}_5 . In the ring \mathbf{Z}_n find the number of solutions to the equation $x^2 = -1$ for n equal to each of the primes between 3 and 29. Make a conjecture about the number of solutions when n is an odd prime. In the ring \mathbf{Z}_n find the number of solutions to the equation $x^2 = -1$ for n the square of each of the primes between 3 and 29. In the ring \mathbf{Z}_n find the number of solutions to the equation $x^2 = -1$ for n the cube of each of the primes between 3 and 29. Make a conjecture about the number of solutions when n is a power of an odd prime. [Gallian, Chapter 12, Computer Exercise 5]

12.6 Using the subroutine mentioned in Exercise 12.5, find the number of solutions to the equation $x^2 = -1$ in \mathbf{Z}_n for $n = 2^k$, $k = 1, 2, 3, 4, 5, 6$. Make a conjecture about the number of solutions when n is a power of two. [Gallian, Chapter 12, Computer Exercise 5]

12.7 Using the subroutine mentioned in Exercise 12.5, find the number of solutions to the equation $x^2 = -1$ for $n = 12, 20, 24, 28$, and 36 . Make a conjecture about the number of solutions when n is a multiple of 4. [Gallian, Chapter 12, Computer Exercise 5]

12.8 Make a conjecture about the number of solutions to the equation $x^2 = -1$ in \mathbf{Z}_n for $n = pq$ and $n = 2pq$ where p and q are odd primes. You should use the subroutine provided in Exercise 12.5 for many values of p and q to help you formulate your conjecture. [Gallian, Chapter 12, Computer Exercise 5]

12.9 Make a conjecture about the number of solutions to the equation $x^2 = -1$ in \mathbf{Z}_n for $n = pqr$

and $n = 2pqr$ where p, q and r are odd primes. You should use the subroutine provided in Exercise 12.5 for many values of p, q and r to help you formulate your conjecture. What relationship do you see between the number of solutions when $n = p, n = q$ and $n = r$ and the case that $n = pqr$? [Gallian, Chapter 12, Computer Exercise 5]

12.10 Based on your answers to Exercises 12.5 - 12.9 formulate a conjecture on the number of solutions to $x^2 = -1$ in \mathbf{Z}_n .

Appendix for Chapter 12

The following is the file "intror2" which is used in this chapter.

```
intror2:= function(n)
local r, x, i;
x:= [];
i:= 1;
Print("The solutions to x^2 = -1 in Z_", n, " are ");
r:= Elements(Integers mod n);
  repeat
    if Int(r[i]^2) = n-1 then
      Add(x,r[i]);
    fi;
    i:= i+1;
  until i=n+1;
return x;
end;
```