Finite Rings and Fields

Computer Algebra for Cryptography (B-KUL-H0E74A)

1 Rings

Rings are sets of elements with two operations $+$ and $\cdot$, which are compatible, i.e. such that the distributive law holds. The formal definition is given in Appendix A.

Typical examples of well-known rings are the integers $\mathbb{Z}$ and the integers modulo N, denoted as $\mathbb{Z}/N\mathbb{Z}$ or $\mathbb{Z}_N$. The most important distinction between a ring and a field, is that the operation $\cdot$ does not have to be commutative (an example of this are 2×2-matrices), and that not every non-zero element has to have an inverse.

In Magma, the above rings can be constructed as

```
Z := Integers();  // rings of integers
ZN := Integers(N);  // integers modulo N
a := Random(ZN) // gives a random element in ZN
b := ZN ! 11;  // forces the integer 11 into ZN
```

Exercise 1.

- Construct the ring of integers $\mathbb{Z}$ and also the ring of integers modulo 105.
- Generate a couple of random elements in $\mathbb{Z}_N$ and ask for their inverse. What do you see?
- Use the built-in `XGCD` function to compute the inverse via the greatest common divisor.
- Compute the inverse of an element using Lagrange's theorem from the lectures. What is $\varphi(N)$ in this case? What is the expression for the inverse as a power of the element? Verify that these methods all give the same answer.

2 Prime fields

When all non-zero elements are invertible, and the operation $\cdot$ is commutative, the ring is called a field. Examples are $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, which are all infinite. Note that $\mathbb{Z}$ is not a field since the only invertible elements are ± 1. We are mostly interested in **finite** fields. The *characteristic* of a field is the smallest integer n such that

$$\underbrace{1 + 1 + \ldots + 1}_{n \text{ times}}$$

equals zero if such n exists; if such n does not exist, we say that the field has characteristic zero. One can prove that the only possibilities for field charateristics are zero (such as $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$) and primes. The easiest fields with prime characteristic are $\mathbb{Z}_p$, for any prime p, which are typically denoted $\mathbb{F}_p$ or $GF(p)$. Computing in this field is simply the well-known modular arithmetic. The fastest way to construct a finite field in Magma is to use the command `GF(q::RngIntElt) -> FldFin`.

Exercise 2.

- Construct a finite field with 31 elements, and write a `for` loop that verifies Fermat's little theorem, i.e. that for all elements in $\mathbb{F}_p$ one has $a^p \equiv a \bmod p$.

As explained in the lectures, there exist finite fields of the form $\mathbb{F}_{p^n}$ for every prime p and extension degree n. For this we will require polynomials over $\mathbb{F}_p$ that are irreducible. You can construct a polynomial ring over any coefficient ring using the command `PolynomialRing(R::Rng) -> RngUPol`.

Exercise 3.

- Construct a polynomial ring over your finite field of 31 elements with variable name `x`. If the name of your ring is `R`, then you can always access `x` simply as `R.1`.
- Write a function `GenRandomIrreduciblePol(K::FldFin, n::RngIntElt) -> pol:RngUPolElt` which takes in a finite field K, constructs a polynomialring over the field and generates random monic polynomials of degree n until one is irreducible. You can use the Magma function `IsIrreducible(f::RngUPolElt) -> BoolElt`.

3 Extension fields

As explained in the lectures, we can construct finite fields of the form $\mathbb{F}_{p^n}$ for every prime p and extension degree n.

Important remark: Although the finite field $\mathbb{F}_p$ corresponds to computing with integers modulo p, the field $\mathbb{F}_{p^n}$ does **not** correspond to computing modulo

p^n. Indeed, it is easy to see that the element $p \bmod p^n$ does not have an inverse modulo p^n, which shows that not all non-zero elements have an inverse.

To construct an extension field $\mathbb{F}_{p^n}$ one can proceed in exactly the same way as the complex numbers $\mathbb{C}$ are constructed from the reals $\mathbb{R}$, i.e. by adjoining a root of an irreducible polynomial:

$$\mathbb{C}\langle i \rangle \cong \frac{\mathbb{R}[x]}{(x^2+1)} \, .$$

Here the quantity i is defined as a formal root of the irreducible polynomial $x^2 + 1 \in \mathbb{R}[x]$, i.e. $i^2 + 1 = 0$. In particular, we recover the well known identity $i^2 = -1$, which allows to reduce all powers of i higher than 1. Hence, $\mathbb{C}$ is seen as a two-dimensional vectorspace over $\mathbb{R}$, and we can write $\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}\}$.

Similarly we can construct the field $\mathbb{F}_{p^n}$ by adjoining a formal root of an irreducible polynomial of degree n over $\mathbb{F}_p$. If you have an irreducible polynomial f of degree n over $\mathbb{F}_p$, you can create the extension field as:

```
Fpn<w> := ext<Fp | f>;
```

The above notation means that `w` is the name of a formal root of f, just like in the case of the complexes above. In particular, if you would evaluate the polynomial f in `w` you would obtain 0. The elements in $\mathbb{F}_{p^n}$ can therefore be represented as polynomials in `w` of degree strictly less than n and with coefficients in $\mathbb{F}_p$.

Exercise 4.

- Use the built-in Magma function `RandomIrreduciblePolynomial(K::FldFin, n::RngIntElt) -> RngUPolElt` to generate a polynomial f of degree 3 over $\mathbb{F}_{31}$ which is irreducible.
- Construct the finite field $\mathbb{F}_{31^3}$ as above, and verify that indeed `w` is a root of f. You can use the built-in function `Evaluate` to do so.
- Generate a random element in $\mathbb{F}_{31^3}$ by calling the `Random` function, and print the element. You will see that the element is indeed represented as a polynomial in `w` of degree less than n.
- Compute the inverse of the element using `^-1` and also using the XGCD algorithm. Note that to be able to run XGCD, your element should be first represented as a polynomial over $\mathbb{F}_p$.
- If you run `RandomIrreduciblePolynomial` again you will see that there are many irreducible polynomials of degree 3 over $\mathbb{F}_{31}$. In general, there will be roughly p^n/n monic irreducible polynomials of degree n (when p is large compared to n).

The above exercise showed that in general there are many irreducible polynomials of degree n over $\mathbb{F}_p$. For each of these choices, you will get a finite field with p^n elements. Let f and g be two irreducible polynomials of degree n over $\mathbb{F}_p$, then using Magma you can construct the two finite fields:

```
Fpn1<w1> := ext<Fp | f>;
Fpn2<w2> := ext<Fp | g>;
```

Here `w1` is a formal root of f and `w2` is a formal root of g.

An amazing proprety of finite fields is that if you create an extension field using an irreducible polynomial f as above, then **all** irreducible polynomials of degree n will split **completely** over $\mathbb{F}_{p^n}$. This shows that up to isomorphism there is only one finite field with p^n elements. Using the above notation, one of these isomorphisms is given by mapping `w1` to `w2`, but mapping `w1` to any root of g is also a valid isomorphism.

Exercise 5.

- Use the built-in Magma function `RandomIrreduciblePolynomial(K::FldFin, n::RngIntElt) -> RngUPolElt` to generate two polynomials f and g of degree 3 over $\mathbb{F}_{31}$ which are irreducible.
- Construct the finite field $\mathbb{F}_{31^3}$ using f, and ask for the roots of f and g in $\mathbb{F}_{31^3}$. For this you can use the built-in function `Roots(f::RngUPolElt[FldRat], R::FldPad) -> SeqEnum` which takes in a polynomial f and a field R and returns the roots of f in the field R. Note that both f as well as g split completely over $\mathbb{F}_{31^3}$, and that `w1` is indeed one of the roots of f.
- Construct the finite field $\mathbb{F}_{31^3}$ using g, and ask again for the roots of f and g. Now `w2` will be a root of g. Since `w2` is a root of g, and you already know the roots of g in terms of `w1`, you see that any isomorphism must map this root `w2` to one of the three roots in terms of `w1`.

A Definitions

A ring $(R, +, \cdot)$ consists of a non-empty set R with two operations $+$ and $\cdot$ such that

- for all $a, b \in R$ we have $a + b \in R$ and $a \cdot b \in R$;
- for all $a, b, c \in R$ we have $a + (b + c) = (a + b) + c$ and $a \cdot (b \cdot c) = (a \cdot b) \cdot c$;
- there exists a $0 \in R$ such that for all $a \in R$ we have $a + 0 = a = 0 + a$;
- there exists a $1 \in R$ such that for all $a \in R$ we have $1 \cdot a = a = a \cdot 1$;
- for all $a \in R$ there exists a $-a \in R$ such that $a + (-a) = 0 = (-a) + a$;
- for all $a, b \in R$ we have $a + b = b + a$;

- for all $a, b, c \in R$ we have $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(a + b) \cdot c = a \cdot c + a \cdot c$.

A field $(F, +, \cdot)$ is a ring with two additional properties:

1. for all $a, b \in F$ we have $a \cdot b = b \cdot a$;
2. for all $a \in F$ (with $a \neq 0$) there exists an element a^{-1} such that $a \cdot a^{-1} = 1$.