LECTURE NOTES IN CRYPTOGRAPHY

Thomas Johansson 2005/2006

Chapter 1

Abstract algebra and Number theory

Before we start the treatment of cryptography we need to review some basic facts from number theory and abstract algebra.

1.1 Number theory

The set of integers $\{\ldots, -2, -1, 0, 1, 2, \ldots\}$ is denoted by $\mathbb{Z}$.

Definition 1.1. *Let $a, b \in \mathbb{Z}$. We say that a* divides *b (written $a|b$) if there exists an integer c such that $b = ac$.*

The following facts are easily checked.

(i) $a|a$.

(ii) If $a|b$ and $b|c$ then $a|c$.

(iii) If $a|b$ and $a|c$ then $a|(bx + cy)$ for any $x, y \in \mathbb{Z}$.

(iv) If $a|b$ and $b|a$ then $a = \pm b$.

Let a and b be integers with $b \geq 1$. Then an ordinary long division of a by b yields two integers q and r such that

$$a = qb + r, \text{ where } 0 \leq r < b. \tag{1.1}$$

The integers q and r are called the *quotient* and the *remainder*, respectively, and they are unique.

Definition 1.2. *The remainder (r) of a divided by b is denoted $a \bmod b$. The quotient (q) of a divided by b is denoted $a \operatorname{div} b$.*

Example 1.1. *Let $a = 47$ and $b = 7$. Then $a \bmod b = 5$ and $a \operatorname{div} b = 6$.*

We call an integer c a *common divisor* of integers a and b if $c|a$ and $c|b$.

Definition 1.3. *A non-negative integer d is called the* greatest common divisor *of integers a and b if*

(i) d is a common divisor of a and b.

(ii) for every other common divisor c it hold that $c|d$.

The greatest common divisor of integers a and b is denoted $\gcd(a, b)$.

Clearly, $\gcd(a, b)$ is the largest positive integer dividing both a and b (except $\gcd(0, 0) = 0$).

Example 1.2. *The common divisors of* 28 *and* 42 *are* $\{\pm 2, \pm 7, \pm 14\}$ *and* $\gcd(28, 42) = 14$.

In a similar fashion as above we define the least common multiple.

Definition 1.4. *A non-negative integer d is called the* least common multiple *of integers a and b if*

(i) $a|d$ and $b|d$.

(ii) for every integer c such that $a|c$ and $b|c$ we have $d|c$.

The least common multiple of integers a and b is denoted $\mathrm{lcm}(a, b)$.

Clearly, $\mathrm{lcm}(a, b)$ is the smallest positive integer divisible by both a and b. The following relationship is often useful. If a and b are positive integers, then

$$\mathrm{lcm}(a, b) \cdot gcd(a, b) = a \cdot b. \tag{1.2}$$

Two integers a, b are called *relatively prime* if $\gcd(a, b) = 1$. Also, an integer $p \geq 2$ is called *prime* if its only positive divisors are 1 and p. Otherwise p is called a *composite*. Prime numbers play a fundamental role in cryptography. Let us review some known facts about them. Let $\pi(x)$ denote the number of primes $\leq x$. Some known facts about primes.

(i) There are infinitely many primes.

(ii) $\lim_{x\to\infty} \frac{\pi(x)}{x/\ln x} = 1$.

(iii) For $x \geq 17$, $x/\ln x < \pi(x) < 1.25506x/\ln x$.

The following theorem is a well known result.

Theorem 1.1 (Unique factorization theorem)**.** *Every integer $n \geq 2$ can be written as a product of prime powers,*

$$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k},$$

where $p_1, p_2, \ldots, p_k$ are distinct primes and $e_1, e_2, \ldots e_k$ are positive integers. Furthermore, the factorization is unique up to rearrangement of factors.

The proof of this theorem is not as easy as it may seem. We refer to any textbook in number theory. The unique factorization theorem can be used to express the greatest common divisor and the least common multiple in a simple way.

If $a = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ and $b = p_1^{f_1} p_2^{f_2} \cdots p_k^{f_k}$, where e_i, f_i, $i = 1, 2, \ldots k$ are now nonnegative integers, then

$$\gcd(a, b) = p_1^{\min(e_1, f_1)} p_2^{\min(e_2, f_2)} \cdots p_k^{\min(e_k, f_k)} \tag{1.3}$$

and

$$\operatorname{lcm}(a, b) = p_1^{\max(e_1, f_1)} p_2^{\max(e_2, f_2)} \cdots p_k^{\max(e_k, f_k)}. \tag{1.4}$$

Definition 1.5. *For $n \geq 1$, let $\phi(n)$ denote the number of integers in the interval $[1, n]$ which are relatively prime to n. This function is called the* Euler phi function.

Let us prove the following facts concerning the Euler phi function.

Theorem 1.2. *(i) If p is a prime, then $\phi(p) = p - 1$.*

(ii) If $gcd(a, b) = 1$ then $\phi(ab) = \phi(a)\phi(b)$.

(iii) If $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ then

$$\phi(n) = (p_1^{e_1} - p_1^{e_1 - 1})(p_2^{e_2} - p_2^{e_2 - 1}) \cdots (p_k^{e_k} - p_k^{e_k - 1}).$$

Proof. The proof is left as an exercise. □

Let us consider the problem of computing the greatest common divisor between two integers. We could use the expression derived in (1.3), but this requires us to first find the prime factors of the two integers. This is not always an easy task, as we will see later. Fortunately, there is an easier and better way of calculating the greatest common divisor. It relies on the following simple fact.

Lemma 1.3. *If a and b are positive integers with $a > b$, then* $\gcd(a, b) = \gcd(b, a \bmod b)$.

Proof. The proof is left as an exercise. □

Of course, we can now use the above lemma repeatedly until the problem is small enough to be trivially solved. This leads to the famous *Euclidean algorithm* for computing $\gcd(a, b)$.

Algorithm 1.1 (Euclidean algorithm)**.**

INPUT: *Two non-negative integers a, b where $a \geq b$.*

OUTPUT: $\gcd(a, b)$

FLOW:
1. *Set $r_0 \leftarrow a$, $r_1 \leftarrow b$, $i \leftarrow 1$.*
2. *While $r_i \neq 0$ do:*
   2.1 Set $r_{i+1} \leftarrow r_{i-1} \bmod r_i$, $i \leftarrow i + 1$.
3. *Return(r_{i-1}).*

In essence, the algorithm sets $r_0 = a$, $r_1 = b$ and then computes the following set of long divisions,

$$\begin{aligned} r_0 &= q_1 r_1 + r_2 \\ r_1 &= q_2 r_2 + r_3 \\ &\vdots \quad \vdots \quad \vdots \\ r_{i-2} &= q_{i-1} r_{i-1} + r_i \\ r_{i-1} &= q_i r_i. \end{aligned}$$

Since $\gcd(a,b) = \gcd(r_0, r_1) = \gcd(r_1, r_2) = \ldots = gcd(r_{i-1}, r_i) = r_i$, the algorithm terminates with the correct answer. Let us illustrate the Euclidean algorithm with an example.

Example 1.3. *Compute* $\gcd(1495, 1365)$.

We have

$$\begin{aligned} 1495 &= 1 \cdot 1365 + 130 \\ 1365 &= 10 \cdot 130 + 65 \\ 130 &= 2 \cdot 65 + 0, \end{aligned}$$

and $\gcd(1495, 1365) = 65$.

The following fact is important.

Theorem 1.4. *Let a and b be two non-negative integers. Then there exist integers x, y such that* $\gcd(a,b)$ *can be written as*

$$\gcd(a,b) = ax + by.$$

Proof. Following the set of long divisions above we have

$$\begin{aligned} \gcd(a,b) &= r_i \\ &= r_{i-2} - q_{i-1} r_{i-1} \\ &= r_{i-2} - q_{i-1}(r_{i-3} - q_{i-2} r_{i-2}) \\ &\vdots \quad \vdots \\ &= r_0 x + r_1 y \\ &= ax + by, \end{aligned}$$

for some integers $x, y \in \mathbb{Z}$.

□

In the proof of the theorem, we see how we can calculate the integers x and y. There is also an extended version of Euclidean algorithm which returns not only $gcd(a,b)$ but also the integers x, y. So when we need to calculate x, y we can either use Eulidean algorithm and then go "backwards" again, as in the proof, or we can use an extended version of the Eulidean algorithm.

Algorithm 1.2 (Extended Euclidean algorithm)**.**

INPUT: *Two non-negative integers a, b where $a \geq b$.*

OUTPUT: *$d = \gcd(a, b)$ and two integers x, y such that $d = ax + by$.*

FLOW:

1. *If $b = 0$ then return(a,$x \leftarrow 1$,$y \leftarrow 0$).*
2. *Set $x_2 \leftarrow 1, x_1 \leftarrow 0, y_2 \leftarrow 0, y_1 \leftarrow 1$.*
3. *While $b > 0$ do:*
   - *3.1 $q \leftarrow a \operatorname{div} b, r \leftarrow a - qb, x \leftarrow x_2 - qx_1, y \leftarrow y_2 - qy_1$,*
   - *3.2 $a \leftarrow b$, $b \leftarrow r$, $x_2 \leftarrow x_1, x_1 \leftarrow x, y_2 \leftarrow y_1, y_1 \leftarrow y$.*
4. *Set $d \leftarrow a$, $x \leftarrow x_2$, $y \leftarrow y_2$ and Return(d, x, y).*

Example 1.4. *Compute* $\gcd(1495, 1365)$ *and find two integers x, y such that* $\gcd(1495, 1365) = 1495x + 1365y$.

q	r	x	y	a	b	x_2	x_1	y_2	y_1
				1495	*1365*	*1*	*0*	*0*	*1*
1	130	*1*	*-1*	*1365*	*130*	*0*	*1*	*1*	*-1*
10	65	*-10*	*11*	*130*	*65*	*1*	*-10*	*-1*	*11*
2	*0*	*21*	*-23*	*65*		*-10*	*21*	*11*	*-23*

So $\gcd(1495, 1365) = 65 = 1495 \cdot (-10) + 1365 \cdot 11$.

If we instead of using the extended version of the Euclidean algorithm would use the standard version and then go backwards, we would get

$$\begin{aligned} 1495 &= 1 \cdot 1365 + 130 \\ 1365 &= 10 \cdot 130 + 65 \\ 130 &= 2 \cdot 65 + 0 \end{aligned}$$

and backwards

$$\begin{aligned} 65 &= 1365 - 10 \cdot 130 \\ &= 1365 - 10 \cdot (1495 - 1 \cdot 1365) \\ &= 11 \cdot 1365 - 10 \cdot 1495. \end{aligned}$$

1.2 The integers modulo n

Let n be a positive integer. If a and b are integers, then a is said to be *congruent to b modulo n*, which is written $a \equiv b \pmod{n}$, if n divides $(a - b)$. We call n the *modulus* of the congruence. We can check the following properties.

Theorem 1.5. *For $a, a_1, b, b_1, c \in \mathbb{Z}$ we have*

(i) $a \equiv b \pmod{n}$ *if and only if* a *and* b *leaves the same remainder when divided by* n.

(ii) $a \equiv a \pmod{n}$.

(iii) *If* $a \equiv b \pmod{n}$ *then* $b \equiv a \pmod{n}$.

iv) *If* $a \equiv b \pmod{n}$ *and* $b \equiv c \pmod{n}$, *then* $a \equiv c \pmod{n}$.

v) *If* $a \equiv a_1 \pmod{n}$ *and* $b \equiv b_1 \pmod{n}$, *then* $a + b \equiv a_1 + b_1 \pmod{n}$ *and* $ab \equiv a_1 b_1 \pmod{n}$.

The properties ii), iii), and iv) are called *reflexivity, symmetry* and *transitivity*, respectively.

Proof. The proof can be found in any textbook on number theory. □

From the above we can see that the integers in the set $\{\ldots, -n, 0, n, 2n, \ldots\}$ are all congruent to each other modulo n. Similarly, the integers in the set $\{\ldots, -n+1, 1, n+1, 2n+1, \ldots\}$ are all congruent to each other modulo n. So the relation of congruence modulo n partitions $\mathbb{Z}$ into n sets, called *equivalence classes* (each integer belongs to exactly one equivalence class). Since all elements in an equivalence class have the same remainder r, we use r as an *representative* for the equivalence class.

Definition 1.6. *The integers modulo* n, *denoted* $\mathbb{Z}_n$, *is the set of (equivalence classes of) integers* $\{0, 1, \ldots, n-1\}$. *Addition, subtraction, and multiplication are performed modulo* n.

Example 1.5. *Calculate* $7 + 11$, $7 - 11$ *and* $7 \cdot 11$ *in* $\mathbb{Z}_{12}$.

$$\begin{aligned} 7 + 11 &= 6 \\ 7 - 11 &= 7 + (-11) = 7 + 1 = 8 \\ 7 \cdot 11 &= 77 \bmod 12 = 5. \end{aligned}$$

As we have seen, addition, subtraction, and multiplication are trivially performed in $\mathbb{Z}_n$. However, the concept of division is a bit trickier.

Definition 1.7. *Let* $a \in \mathbb{Z}_n$. *The* multiplicative inverse *of* a *is an integer* $x \in \mathbb{Z}_n$ *such that* $ax = 1$. *If such an integer* x *exists, then* a *is said to be* invertible *and* x *is called the inverse of* a, *denoted* a^{-1}.

Definition 1.8. *Division of* a *by an element* b *in* $\mathbb{Z}_n$ *(written* a/b*) is defined as* ab^{-1}, *and only defined if* b *is invertible.*

Lemma 1.6. *Let* $a \in \mathbb{Z}_n$. *Then* a *is invertible if and only if* $\gcd(a, n) = 1$.

Proof. Assume that $\gcd(a, n) = 1$. We know that $1 = \gcd(a, n) = xa + yn$ for some $x, y \in \mathbb{Z}$. Then $x \bmod n$ is an inverse to a.

Now assume $\gcd(a, n) > 1$. If a has an inverse x then $a \cdot x = 1 \bmod n$, which means $1 = a \cdot x + n \cdot y$ for some $x, y \in \mathbb{Z}$, directly contradicting the assumption. □

Example 1.6. *Calculate* $7/11$ *in* $\mathbb{Z}_{12}$.

By definition $7/11 = 7 \cdot 11^{-1}$. *We use Euclidean algorithm to find integers such that* $\gcd(11, 12) = 1 = 12 - 1 \cdot 11$. *This gives* $11^{-1} = 11$ *and* $7/11 = 7 \cdot 11^{-1} = 7 \cdot 11 = 5$.

A very important basic result is the Chinese remainder theorem, or CRT for short.

Theorem 1.7 (Chinese Remainder Theorem)**.** *Let the integers* $n_1, n_2, \ldots, n_k$ *be pairwise relatively prime. Then the system of congruences*

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \\ &\vdots \\ x &\equiv a_k \pmod{n_k} \end{aligned}$$

has a unique solution modulo $n = n_1 n_2 \cdots n_k$.

Proof. □

Algorithm 1.3 (Gauss's algorithm)**.** *The solution* x *to the system of congruences promised by the CRT can be calculated as*

$$x = \sum_{i=1}^{k} a_i N_i M_i \bmod n,$$

where $N_i = n/n_i$ *and* $M_i = N_i^{-1} \bmod n_i$.

The CRT allows us to change the way we represent elements. Suppose we are considering the integers modulo n, where $n = n_1 n_2$ and $\gcd(n_1, n_2) = 1$. An element $a \in \mathbb{Z}_n$ has a unique representation from the pair $(a \bmod n_1, a \bmod n_2)$. Let us denote this map by $\gamma : \mathbb{Z}_n \to \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}$. The following properties are easily verified.

(i) $\gamma(a) = \gamma(b)$ if and only if $a = b$.

ii) For all $(a_1, a_2) \in \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}$ there exists an a such that $\gamma(a) = (a_1, a_2)$.

(ii) $\gamma(a + b) = \gamma(a) + \gamma(b)$.

(iii) $\gamma(ab) = \gamma(a)\gamma(b)$.

These properties make γ an *isomorphism*. This roughly means that we can use any of the two representations when we do calculus.

Example 1.7. *We would like to calculate* 9^{10} *in* $\mathbb{Z}_{10}$ *in two ways, direct calculation and through the CRT.*

Direct calculation gives

$$9^{10} = (81 \bmod 10)^5 = 1^5 = 1.$$

Using the CRT, we first set $n = n_1 n_2$, *where* $n_1 = 2$, $n_2 = 5$. *This gives* $N_1 = 5$, $N_2 = 2$, $M_1 = 5^{-1} \bmod 2 = 1$ *and* $M_2 = 2^{-1} \bmod 5 = 3$. *Then we calculate the CRT representation*

$$\begin{aligned} a_1 &= 9^{10} \bmod 2 = 1 \\ a_2 &= 9^{10} \bmod 5 = 4^{10} \bmod 5 = 1 \end{aligned}$$

Finally, we can reconstruct the integer in $\mathbb{Z}_{10}$ *corresponding to* $(a_1, a_2) = (1, 1)$ *through Gauss's algorithm,*

$$x = \sum_{i=1}^{2} a_i N_i M_i \bmod 10 = 1 \cdot 5 \cdot 1 + 1 \cdot 2 \cdot 3 = 1.$$

Let us continue and define the *multiplicative group* of $\mathbb{Z}_n$, denoted $\mathbb{Z}_n^*$, as the set of all invertible elements, i.e.,

$$\mathbb{Z}_n^* = \{a \in \mathbb{Z}_n | \gcd(a, n) = 1\}.$$

The *order* of $\mathbb{Z}_n^*$ refers to the number of elements in $\mathbb{Z}_n^*$ and is also denoted $|\mathbb{Z}_n^*|$. It follows from the definition of the Euler phi function that $|\mathbb{Z}_n^*| = \phi(n)$.

Since the product of two invertible elements is again an invertible element, we say that $|\mathbb{Z}_n^*|$ is closed under multiplication.

Theorem 1.8 (Euler's theorem). *If* $a \in \mathbb{Z}_n^*$ *then*

$$a^{\phi(n)} \equiv 1 \pmod{n}.$$

Proof. Let $\mathbb{Z}_n^* = \{a_1, a_2, \ldots, a_{\phi}(n)\}$. Looking at the set of elements $A = \{aa_1, aa_2, \ldots, aa_{\phi}(n)\}$, it is easy to see that $A = \mathbb{Z}_n^*$. So we have two ways of writing the product of all elements, i.e.,

$$\prod_{i=1}^{\phi(n)} aa_i = \prod_{i=1}^{\phi(n)} a_i,$$

leading to

$$\prod_{i=1}^{\phi(n)} a = a^{\phi(n)} = 1.$$

□

A special case of Euler's theorem is celebrated as Fermat's little theorem.

Corollary 1.9 (Fermat's little theorem). *Let* p *be a prime. If* $\gcd(a, p) = 1$ *then*

$$a^{p-1} \equiv 1 \pmod{p}.$$

From Euler's theorem we see that when working in $\mathbb{Z}_n$ all exponents can be reduced modulo $\phi(n)$.

Let $a \in \mathbb{Z}_n^*$. The *order* of the element a, denoted $\mathrm{ord}(a)$ is defined as the least positive integer t such that $a^t = 1$.

Lemma 1.10. *Let $a \in \mathbb{Z}_n^*$. If $a^s = 1$ for some s, then* $\text{ord}(a)|s$. *In particular,* $\text{ord}(a)|\phi(n)$.

Proof. Let $t = \text{ord}(a)$. By long division $s = qt + r$, where $r < t$. Then $a^s = a^{qt+r} = a^{qt}a^r$ and since $a^t = 1$ we have $a^s = a^r$ and $a^r = 1$. But $r < t$ so we must have $r = 0$ and so $\text{ord}(a)|s$. □

Definition 1.9. *Let $a \in \mathbb{Z}_n^*$. If* $\text{ord}(a) = \phi(n)$, *then a is said to be a* generator *(or a primitive element) of $\mathbb{Z}_n^*$. Furthermore, if $\mathbb{Z}_n^*$ has a generator then $\mathbb{Z}_n^*$ is said to be* cyclic.

It is clear that if $a \in \mathbb{Z}_n^*$ is a generator, then every element in $\mathbb{Z}_n^*$ can be expressed as a^i for some integer i. So we can write

$$\mathbb{Z}_n^* = \{a^i | 0 \leq i \leq \phi(n) - 1\}.$$

Finally, we shortly introduce the concept of quadratic residues. An element $a \in \mathbb{Z}_n^*$ is said to be a *quadratic residue* modulo n (or a square) if there exists an $x \in \mathbb{Z}_n^*$ such that $x^2 = a$. Otherwise, a is called a *quadratic non-residue* modulo n. If $x^2 = a$ then x is called the *square root* of a modulo n.

Example 1.8. *Determine the quadratic residues in $\mathbb{Z}_{11}^*$, knowing that it is cyclic.*

Knowing that $\mathbb{Z}_{11}^*$ is cyclic, it can be expressed as

$$\mathbb{Z}_{11}^* = \{a^i | 0 \leq i \leq 10\},$$

where $\text{ord}(a) = \phi(11) = 10$. *As 10 factors as $10 = 2 \cdot 5$ the possible orders for any element are $1, 2, 5$, or 10. We try to find a generator a.*

We start by testing $a = 2$. As $2^2 = 4$, $2^5 = 10$, we know that 2 must be a generator of $\mathbb{Z}_{11}^*$ without having to test further.

An element $b = a^i$ is a quadratic residue if there is an $x = 2^j$ such that $x^2 = b$, or $2^{2j} = 2^i$ for some j. This makes it clear that the quadratic residues are the elements of the form a^i where i is even. This gives the set $\{2^0 = 1, 2^2 = 4, 2^4 = 5, 2^6 = 9, 2^8 = 3\}$.

1.3 Basic abstract algebra

In the previous sections we have presented various aspects concerning the integers and calculus modulo n. However, this covered just a few examples of algebraic structures. In this section we briefly review some basic concepts from abstract algebra, which provides a more general treatment of algebraic structures.

1.3.1 Groups

A *binary operation* $*$ on a set S is a mapping from $S \times S$ to S. Our general purpose is to introduce various environments where we can perform different operations, which are similar to what we are used to do with the ordinary numbers, like the real numbers. A binary operation on the real numbers could for example be addition.

In our world of cryptography, as in many other areas, we must be able to represent our elements in an exact way when implemented. As an infinite set does not support this, we are in general only interested in *finite* sets.

Definition 1.10. *A* group $(G, *)$ *is a set* G *and a binary operation* $*$ *on* G *which satisfies the following.*

(i) $a * (b * c) = (a * b) * c$ *for all* $a, b, c \in G$ *(*associativity*).*

(ii) There is a special element $1 \in G$ *such that* $a * 1 = 1 * a = a$ *for all* $a \in G$.

(iii) For each $a \in G$ *there is an element* $a^{-1} \in G$ *such that* $a * a^{-1} = a^{-1} * a = 1$.

We call 1 *the* identity element *and we call* a^{-1} *the inverse of* a. *Furthermore, if*

(iv) $a * b = b * a$ *for all* $a, b \in G$,

then G *is called* abelian *(or* commutative*).*

Definition 1.11. *A group is* finite *if the number of elements in* G *(*$|G|$*) is finite. The number of elements is called the* order *of the group.*

If we recall the treatment of number theory, we see that the set of integers $\mathbb{Z}$ with the addition operation, denoted $(\mathbb{Z}, +)$, is a group. Finite groups are $(\mathbb{Z}_n, +)$, and $(\mathbb{Z}_n^*, \cdot)$, where $\cdot$ denotes multiplication modulo n. Note that $(\mathbb{Z}_n, \cdot)$ is not a group. Neither is $(\mathbb{Z}, \cdot)$.

A non-empty subset H of a group G is called a *subgroup* of G, if it is itself a group with respect to the operation of G. Similar to what we defined before, we say that a group G is *cyclic* if there is an element $a \in G$ such that each $b \in G$ can be written as a^i for some integer i. The element a is called a *generator* of G.

The *order* of an element $a \in G$ is the least positive integer such that $a^t = 1$, if such an integer exists. If it does not, then the order of a is defined to be ∞.

Lemma 1.11. *Let* $a \in G$ *be an element of finite order* t. *Then the set of all powers of* a *forms a cyclic subgroup of* G, *denoted by* $< a >$. *Furthermore, the order of* $< a >$ *is* t.

We can note some further properties. Suppose $a^n = 1$ for some $n > 0$. Perform a long division and write $n = k \cdot \mathrm{ord}(a) + r$, where $0 \leq r \leq \mathrm{ord}(a)$. Then $1 = a^n = a^{=k \cdot \mathrm{ord}(a) + r} = a^r$ and $r = 0$. So we must have $\mathrm{ord}(a) | n$.

Another interesting property. If G is a finite group, all elements must have finite order. Choose k as the product of the orders of all different elements in G. Then $a^k = 1$ for all $a \in G$. The conclusion is that there exists a positive integer k such that $a^k = 1$ all the time (for any $a \in G$).

Let H be a subgroup in G and pick an element $a \in G$. A set of elements of the form

$$aH = \{ah | h \in H\}$$

is called a *left coset* of H. If G is commutative we simply call it a coset. The set consisting of of all such left cosets is written G/H. We note that H itself is a left coset. Furthermore, every left coset contains the same number of elements (the order of H) and every element is contained in exactly one left coset.

So the elements of G are partitioned into $|G|/|H|$ different cosets, each containing $|H|$ elements. This leads to the following famous result.

Theorem 1.12 (Lagrange's theorem)**.** *If* G *is a finite group and* H *is a subgroup of* G, *then* $|H|$ *divides* $|G|$. *In particular, if* $a \in G$ *then the order of* a *divides* $|G|$.

We end the section by another observation. If $|G|$ is a prime number, then the order of an element a is either 1 or $|G|$. In particular, if $|G|$ is a prime number then G must be cyclic.

1.3.2 Rings

A group was defined through a set G together with one binary operation. A ring is defined through a set R together with two binary operations.

Definition 1.12. *A ring (with unity) $(R, +, \cdot)$ consists of a set R with two binary operations, denoted $+$ and $\cdot$, on R, satisfying the following conditions:*

(i) $(R, +)$ *is an abelian group with an identity element denoted* 0.

(ii) $a \cdot (b \cdot c) = (a \cdot b) \cdot c$, *for all* $a, b, c \in R$ (associative).

(iii) There is a multiplicative identity denoted 1, *with* $1 \neq 0$, *such that* $1 \cdot a = a \cdot 1 = a$, *for all* $a \in R$.

(iv) $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ *and* $(b + c) \cdot a = (b \cdot a) + (c \cdot a)$, *for all* $a, b, c \in R$.

A commutative ring *is a ring where additionally*

(v) $a \cdot b = b \cdot a$, *for all* $a, b \in R$.

One example of a commutative ring is $(\mathbb{Z}, +, \cdot)$, where $+$ and $\cdot$ are the usual operations of addition and multiplication. Another example is $\mathbb{Z}_n$ with addition and multiplication modulo n.

Note that the additive inverse of an element $a \in R$ is denoted $-a$. So the subtraction expression $a - b$ should be interpreted as $a + (-b)$. The multiplication $a \cdot b$ is equivalently written ab; similarily, $a^2 = aa = a \cdot a$.

Definition 1.13. *An element $a \in R$ is called an* invertible element *(or a unit) if there is an element $b \in R$ such that $a \cdot b = b \cdot a = 1$.*

The set of units in a ring R forms a group under multiplication. For example, the group of units of the ring $\mathbb{Z}_n$ is $\mathbb{Z}_n^*$.

The multiplicative inverse of an element $a \in R$ is denoted by a^{-1}, assuming that it exists. The division expression a/b should then be interpreted as $a \cdot b^{-1}$.

Definition 1.14. *A commutative ring where all nonzero elements have (multiplicative) inverses is called a* field.

Definition 1.15. *The* characteristic *of a field is the least integer $m > 0$ such that*

$$\overbrace{1 + 1 + \cdots + 1}^{m} = 0.$$

If no such integer m exists, the characteristic is defined to be 0.

Examples of fields are the rational numbers $\mathbb{Q}$, the real numbers $\mathbb{R}$ and the complex numbers $\mathbb{C}$. Note that the set of integers under the usual operations of addition and multiplication is not a field, since the only elements with multiplicative inverses are 1 and -1.

Theorem 1.13. *$\mathbb{Z}_n$ is a field if and only if n is a prime number. If n is a prime, the characteristic of $\mathbb{Z}_n$ is n.*

Finally, a subset F of a field E is called a *subfield* of E if F is itself a field with respect to the operations of E. Then we say that E is an *extension field* of F.

1.3.3 Polynomial rings

Definition 1.16. *A* polynomial *in the indeterminate x over the ring R is an expression of the form*

$$f(x) = a_n x^n + \cdots + a_2 x^2 + a_1 x + a_0,$$

where each $a_i \in R$, $a_n \neq 0$, and $n \geq 0$. We say that $f(x)$ has degree *n, denoted* $\deg f(x) = n$. *We also allow $f(x)$ to be the polynomial with all coefficients zero, in which case the degree is defined to be $-\infty$. A polynomial $f(x)$ is said to be* monic *if the leading coefficient is equal to 1, i.e., $a_n = 1$.*

Definition 1.17. *Let R be a commutative ring. Then the* polynomial ring*, denoted by $R[x]$ is the ring formed by the set of all polynomials in the indeteminate x having coefficients from R. The operations are addition and multiplication of polynomials, with the coefficient aritmethic performed in R.*

Example 1.9. *Compute $(x^2 + 2x + 9)(x^3 + 11x^2 + x + 7)$ in $\mathbb{Z}_{12}[x]$.*

$$\begin{aligned}(x^2 + 2x + 9)(x^3 + 11x^2 + x + 7) &= x^5 + 11x^4 + x^3 + 7x^2 + 2x^4 + 10x^3 + 2x^2 + 2x + \\ &\quad +9x^3 + 3x^2 + 9x + 3 \\ &= x^5 + x^4 + 8x^3 + 11x + 3.\end{aligned}$$

We now consider the polynomial ring $F[x]$, where F denotes an arbitrary field. As we will see, the polynomial ring $F[x]$ has many properties in common with integers.

Definition 1.18. *A polynomial $f(x) \in F[x]$ of degree $d \geq 1$ is called* irreducible *if it cannot be written as a product of two polynomials in $F[x]$, both of degree less than d.*

Irreducible polynomials are the polynomial ring counterpart of prime numbers. Similar as for integers, we have a division algorithm for polynomials.

Lemma 1.14. *If $g(x), h(x) \in F[x]$, with $h(x) \neq 0$, then there are polynomials $q(x), r(x) \in F[x]$ such that*

$$g(x) = q(x)h(x) + r(x),$$

where $\deg r(x) < \deg h(x)$. *Furthermore, $q(x)$ and $r(x)$ are unique and are referred to as the* quotient *and the* remainder*, respectively. The remainder $r(x)$ is also denoted by* $g(x) \bmod h(x)$.

Example 1.10. *Compute $(x^3 + 11x^2 + x + 7) \bmod (x^2 + 2x + 9)$ in $\mathbb{Z}_{13}[x]$.*

Long division of polynomials. By

$$\begin{aligned}(x^3 + 11x^2 + x + 7) - (x^2 + 2x + 9) \cdot x &= 11x^2 - 2x^2 + x - 9x + 7 = 9x^2 + 5x + 7 \\ (9x^2 + 5x + 7) - (x^2 + 2x + 9) \cdot 9 &= 5x - 5x + 7 - 3 = 4\end{aligned}$$

we have $(x^3 + 11x^2 + x + 7) = (x^2 + 2x + 9) \cdot (x + 9) + 4$, so

$$(x^3 + 11x^2 + x + 7) \bmod (x^2 + 2x + 9) = 4.$$

If $g(x), h(x) \in F[x]$, then $h(x)$ is said to *divide* $g(x)$, written as $h(x)|g(x)$, if $g(x) \bmod h(x) = 0$.

Let $f(x)$ be some fixed polynomial in $F[x]$. Similar as for the integers, we can define congruences of polynomials in $F[x]$ based on division by $f(x)$.

Definition 1.19. *Let $g(x), h(x) \in F[x]$. then $g(x)$ is said to be congruent to $h(x)$ modulo $f(x)$ if $f(x)|(g(x) - h(x))$. We denote this by $g(x) \equiv h(x) \pmod{f(x)}$.*

We can verify a lot of properties regarding congruences between polynomials.

Theorem 1.15. *For $g(x), h(x), g_1(x), h_1(x), s(x) \in F[x]$ we have*

(i) $g(x) \equiv h(x) \pmod{f(x)}$ *if and only if* $g(x)$ *and* $h(x)$ *leaves the same remainder when divided by* $f(x)$.

(ii) $g(x) \equiv g(x) \pmod{f(x)}$.

(iii) If $g(x) \equiv h(x) \pmod{f(x)}$ *then* $h(x) \equiv g(x) \pmod{f(x)}$.

iv) If $g(x) \equiv h(x) \pmod{f(x)}$ *and* $h(x) \equiv s(x) \pmod{f(x)}$, *then* $g(x) \equiv s(x) \pmod{f(x)}$.

v) If $g(x) \equiv g_1(x) \pmod{f(x)}$ *and* $h(x) \equiv h_1(x) \pmod{f(x)}$, *then* $g(x)+h(x) \equiv g_1(x)+h_1(x) \pmod{f(x)}$ *and* $g(x)h(x) \equiv g_1(x)h_1(x) \pmod{f(x)}$.

The properties ii), iii), and iv) are again called *reflexivity, symmetry* and *transitivity*, respectivly. The proof of the theorem is again not given here.

From the above properties we see that the polynomials in $F[x]$ can be divided into sets, called *equivalence classes*, where each equivalence class contains all polynomials that leaves a certain remainder when divided by $f(x)$. Furthermore, since the remainder $r(x)$ itself is a polynomial in the equivalence class, we use it as a *representative* of the equivalence class. Note that $\deg r(x) < \deg f(x)$.

Definition 1.20. *By $F[x]/(f(x))$ we denote the set of (equivalence classes of) polynomials in $F[x]$ of degree less than $\deg f(x)$. The addition and multiplication operations are performed modulo $f(x)$.*

Theorem 1.16. *$F[x]/(f(x))$ is a commutative ring.*

Theorem 1.17. *If $f(x) \in F[x]$ is irreducible, then $F[x]/(f(x))$ is a field.*

1.4 Finite fields

A *finite field* is a field which contains a finite number of elements. The number of elements is also called the *order* of the field.

We now give a few results which are out of the scope of this text to prove.

Theorem 1.18. *(i) If F is a finite field, then the order of F is p^m for some prime p and integer $m \geq 1$.*

(ii) For every prime power order p^m, there is a unique (up to isomorphism) finite field of order p^m. This field is denoted by $\mathbb{F}_{p^m}$, or $GF(p^m)$.

Two fields are isomorphic if they are structually the same, but elements have different representation. We know already that for p prime $\mathbb{Z}_p$ is a field of order p. So we associate the finite field $\mathbb{F}_p$ with $\mathbb{Z}_p$ and its representation.

Theorem 1.19. *(i) If $\mathbb{F}_q$ is a finite field of order $q = p^m$, p prime, then the characteristic of $\mathbb{F}_q$ is p. Furthermore, $\mathbb{F}_q$ contains a copy of $\mathbb{Z}_p$ as a subfield.*

(ii) Let $\mathbb{F}_q$ be a finite field of order $q = p^m$. Then every subfield of $\mathbb{F}_q$ has order p^n for some positive integer n where $n|m$. Conversely, if $n|m$ then there are exactly one subfield of $\mathbb{F}_q$ of order p^n.

(iii) An element $a \in \mathbb{F}_q$ is in the subfield $\mathbb{F}_{p^n}$ if and only if $a^{p^n-1} = 1$.

The non-zero elements of $\mathbb{F}_q$ all have inverses and thus they form a group under multiplication. This group is called the *multiplicative group* of $\mathbb{F}_q$ and denoted by $\mathbb{F}_q^*$. It can be shown that $\mathbb{F}_q^*$ is a cyclic group (of order $q-1$). Especially, this means that $a^{q-1} = 1$ for all $a \in \mathbb{F}_q$.

Definition 1.21. *A generator of the cyclic group $\mathbb{F}_q^*$ is called a* primitive element.

We know already that the finite fields of prime order p can be realized by a simple modulo p arithmetic. The question that remains is how to realize the finite fields of prime power order p^m, where $m > 1$. In order to do this we need to extend the theory of greatest common divisors and the Euclidean algorithm to the polynomial ring $F[x]$.

Definition 1.22. *Let $g(x), h(x) \in \mathbb{Z}_p[x]$, where not both are zero. Then the* greatest common divisor *of $g(x)$ and $h(x)$, denoted* $\gcd(g(x), h(x))$*, is the monic polynomial of greatest degree in $\mathbb{Z}_p[x]$ which divides both $g(x)$ and $h(x)$. By definition* $\gcd(0, 0) = 0$.

Similar to the fundamental theorem of arithmetics, we have

Theorem 1.20. *Every non-zero polynomial $f(x) \in \mathbb{Z}_p[x]$ has a factorization*

$$f(x) = af_1(x)^{e_1} f_2(x)^{e_2} \cdots f_k(x)^{e_k},$$

where each f_i is a distinct monic irreducible polynomial in $\mathbb{Z}_p[x]$, the e_i are positive integers, and $a \in \mathbb{Z}_p$. The factorization is unique up to rearrangement of factors.

Now we give the polynomial version of the Euclidean algorithm.

Algorithm 1.4 (Euclidean algorithm for polynomials)**.**

INPUT: *Two non-negative polynomials $a(x), b(x) \in F_q[x]$.*

OUTPUT: $\gcd(a(x), b(x))$

FLOW: *1. Set $r_0(x) \leftarrow a(x)$, $r_1(x) \leftarrow b(x)$, $i \leftarrow 1$.*

2. *While* $r_i(x) \neq 0$ *do:*
   2.1 *Set* $r_{i+1}(x) \leftarrow r_{i-1}(x) \bmod r_i(x)$, $i \leftarrow i+1$.
3. *Return*$(r_{i-1}(x))$.

Here is an example.

Example 1.11. *Compute* $\gcd(x^3+x^2+2x+2, x^2+x+1)$ *in* $\mathbb{Z}_3$.

$$\begin{aligned} x^3+x^2+2x+2 &= x\cdot(x^2+x+1)+x+2 \\ (x^2+x+1) &= (x+2)\cdot(x+2)+0 \end{aligned}$$

So $\gcd(x^3+x^2+2x+2, x^2+x+1) = x+2$.

Theorem 1.21. *Let* $a(x)$ *and* $b(x)$ *be two non-negative polynomials in* $F_q[x]$. *Then there exist polynomials* $s(x), t(x)$ *such that* $\gcd(a(x), b(x))$ *can be written as*

$$\gcd(a(x), b(x)) = a(x)s(x) + b(x)t(x).$$

Example 1.12. *Continuing from Example 1.11, we can directly write*

$$\gcd(x^3+x^2+2x+2, x^2+x+1) = (x+2) = (x^3+x^2+2x+2) - x\cdot(x^2+x+1),$$

so $s(x) = 1$ *and* $t(x) = -x = 2x$.

As for the integer case, there is also an extended version of the Euclidean algorithm that in addition to $\gcd(a(x), b(x))$ also returns the polynomials $s(x), t(x)$ above.

1.4.1 Finite field arithmetics

The most common representation for the elements of a finite field $\mathbb{F}_q$, where $q = p^m$, p prime, is a *polynomial basis representation.*

Theorem 1.22. *Let* $f(x) \in \mathbb{Z}_p[x]$ *be an irreducible polynomial of degree* m. *Then* $\mathbb{Z}_p[x]/(f(x))$ *is a finite field of order* p^m. *The elements are all polynomials of degree less than* m. *Addition and multiplication of elements is performed modulo* $f(x)$.

The following fact assures that all finite fields can be represented in this manner.

Lemma 1.23. *For each* $m \geq 1$, *there exists a monic irreducible polynomial of degree* m *over* $\mathbb{Z}_p$.

Example 1.13. *Let us examine the field* $\mathbb{F}_{2^3}$. *To construct it we need an irreducible polynomial of degree* 3 *over* $\mathbb{F}_2$. *The polynomial* $\pi(x) = x^3+x+1$ *is indeed an irreducible polynomial since* $\pi(0) = \pi(1) = 1$.

The elements are the polynomials of degree less than 3, *i.e., the set*

$$\mathbb{F}_{2^3} = \{0, 1, x, x+1, x^2, x^2+1, x^2+x, x^2+x+1\}.$$

Addition of the elements x^2+1 *and* $x+1$ *gives*

$$(x^2+1)+(x+1)=x^2+x,$$

and multiplication of the elements x^2+1 *and* $x+1$ *gives*

$$(x^2+1)(x+1)=x^3+x^2+x+1\equiv x^2 \pmod{\pi}(x),$$

so $(x^2+1)(x+1)=x^2$.

Our elements in $\mathbb{F}_q$ are represented by polynomials in the indeterminate x. As we might want consider polynomials over $\mathbb{F}_q$, we now change the representation of the elements.

The argument goes as follows. The polynomial $f(x)$ is irreducible over $\mathbb{Z}_p$. However, there exists some element α in some extension field $\mathbb{F}_q$ for which $f(\alpha)=0$. Instead of representing our elements as polynomials in the indeterminate x we represent them using α and the fact that $f(\alpha)=0$. From a practical point of view, this simply means that our indeterminate x in the elements is replaced by α.

Example 1.14. *Considering the previous example,* $\pi(x)=x^3+x+1$. *We introduce* α *through* $\pi(\alpha)=0$. *This gives us the rule*

$$\alpha^3=\alpha+1.$$

The elements are

$$\mathbb{F}_{2^3}=\{0,1,\alpha,\alpha+1,\alpha^2,\alpha^2+1,\alpha^2+\alpha,\alpha^2+\alpha+1\},$$

and, for example

$$(\alpha^2+1)(\alpha+1)=\alpha^3+\alpha^2+\alpha+1=\alpha^2,$$

using the reduction rule $\alpha^3=\alpha+1$.

Let us look at the arithmetics in a finite field with element representation as above. Addition of two elements is done by usual addition of two polynomials in $\mathbb{F}_q$. Multiplying two elements $g(\alpha)$ and $h(\alpha)$ is done by usual multiplication of the two polynomials and then a reduction of the result through $f(\alpha)=0$. Finally, multiplicative inverses can be computed by going backwards in the Euclidean algorithm for $\mathbb{F}_q[x]$.

We might also want to consider an alternative representation through powers of α.

Definition 1.23. *An irreducible polynomial* $f(x)\in\mathbb{Z}_p[x]$ *is called* primitive *if the element* α *corresponding to* $f(\alpha)=0$ *is a generator of* $\mathbb{F}_q^*$.

As α is a generator of $\mathbb{F}_q^*$, every non-zero element of $\mathbb{F}_q$ can be written as a power of α, i.e., α^i for some $i, 0\leq i\leq q-1$. This gives us an alternative element representation, namely as powers of α. This will give a very simple multiplication operation, but instead the addition is more complicated and involves a polynomial modulo reduction.

If we want to do extensive calculations in small finite fields, the best approach is to tabulate both representations side by side, and use the one most suitable for the operation.

(Binary representation)	Polynomial basis	Power of α
0000	0	0
0001	1	1
0010	α	α
0100	α^2	α^2
1000	α^3	α^3
0011	$\alpha+1$	α^4
0110	$\alpha^2+\alpha$	α^5
1100	$\alpha^3+\alpha^2$	α^6
1011	$\alpha^3+\alpha+1$	α^7
0101	α^2+1	α^8
1010	$\alpha^3+\alpha$	α^9
0111	$\alpha^2+\alpha+1$	α^{10}
1110	$\alpha^3+\alpha^2+\alpha$	α^{11}
1111	$\alpha^3+\alpha^2+\alpha+1$	α^{12}
1101	$\alpha^3+\alpha^2+1$	α^{13}
1001	α^3+1	α^{14}

Table 1.1: Table representation of the field with 16 elements using $\pi(x) = x^4 + x + 1$, $\pi(\alpha) = 0$.

Example 1.15. *Let us represent $\mathbb{F}_{2^4}$ using the primitive polynomial $\pi(x) = x^4 + x + 1$ and $\pi(x) = 0$. Using the rule $\alpha^4 = \alpha + 1$ we can either represent our elements in a polynomial basis or as powers of α. We get the table in Table 1.1 for the elements in $\mathbb{F}_{2^4}$ (each row corresponds to one element).*

Note that $\alpha^{15} = 1$. Having this table representation of the field, it is very easy to perform operations by switching to the most apropriate representation.

For example, calculating

$$(\alpha^3+\alpha+1)(\alpha^3+\alpha) = [\textit{ switch repr.}] = \alpha^7\alpha^9 = \alpha^{16} = \alpha$$

and

$$(\alpha^3+\alpha+1)^{-1} = (\alpha^7)^{-1} = \alpha^{-7} = \alpha^{-7+15} = \alpha^8.$$

Finally $\alpha/(\alpha+1)$ is calculated as

$$\alpha/(\alpha+1) = \alpha/\alpha^4 = \alpha^{-3} = \alpha^{12}.$$

1.5 Exercises

Exercise 1.1.

(a) Calculate $\gcd(222, 1870)$.

(b) Find integers x and y such that $\gcd(222, 1870) = 222x + 1870y$.

Exercise 1.2.

(a) Find the value of $\phi(36)$.

(b) Write up all the units in $\mathbb{Z}_{36}$.

(c) Calculate 5^{-1} *in* $\mathbb{Z}_{36}$.

Exercise 1.3.

(a) Write $143 = 11 \cdot 13$. *Let* $x = 2$ *and calculate* x^{-1} *in* $\mathbb{Z}_{143}$.

(b) Now we do the same again but we use CRT. Calculate $x^{-1} \pmod{11}$ *and* $x^{-1} \pmod{13}$.

(c) Use the result in (b) to recover the value of x^{-1} *in* $\mathbb{Z}_{143}$.

Exercise 1.4. *Find all integer solutions to the following system of congruences.*

$$\begin{aligned} x &\equiv 3 \pmod{7} \\ x &\equiv 1 \pmod{13} \\ x &\equiv 13 \pmod{17} \end{aligned}$$

Exercise 1.5. *Find all integer solutions to the following system of congruences.*

$$\begin{aligned} x &\equiv 3 \pmod{3} \\ x &\equiv 1 \pmod{7} \\ x &\equiv 13 \pmod{14} \end{aligned}$$

Exercise 1.6.

(a) Calculate $2/5$ *in* $\mathbb{Z}_8^*$.

(b) Find $\operatorname{ord}(5)$ *in* $\mathbb{Z}_8^*$.

(c) Is $\mathbb{Z}_8^*$ *a cyclic group?*

Exercise 1.7. *Find the square root of* 10 *in* $\mathbb{Z}_{13}$.

Exercise 1.8. *Let* S *be the set of binary triples, i.e,* $S = \{(s_0, s_1, s_2), s_i \in \mathbb{Z}_2\}$. *Let the operation be bitwise addition.*

(a) Show that S *is a group.*

(b) What is the order of the group?

(c) What is the order of the element $(1, 1, 1)$*?*

(d) Is there a generator in the group?

Exercise 1.9. *Find a generator for the additive group $\mathbb{Z}_{13}$ (under the addition operation).*

Exercise 1.10. *Find all subgroups in the multiplicative group $\mathbb{Z}_{19}^*$ (under the multiplication operation).*

Exercise 1.11. *Prove that $\mathbb{Z}_4$ is not a field.*

Exercise 1.12. *Let F be the finite field $\mathbb{F}_8$ constructed using the irreducible polynomial $f(x) = x^3 + x + 1$ over $\mathbb{F}_2$.*

Let F' be the finite field $\mathbb{F}_8$ constructed using the irreducible polynomial $f(x) = x^3 + x^2 + 1$ over $\mathbb{F}_2$.

Find an isomorphism γ between F and F', i.e, tabulate $\gamma(a)$ for all $a \in F$.

Exercise 1.13. *Let $\mathbb{F}_{2^4}$ be constructed using the irreducible polynomial $f(x) = x^4 + x + 1$ over $\mathbb{F}_2$, $f(\alpha) = 0$.*

(a) Calculate $(\alpha^3 + 1) \cdot (\alpha^2 + \alpha)$.

(b) Calculate $(\alpha^3 + 1)^{-1}$.

(c) Calculate $(\alpha^3 + 1)^{357}$.

(d) Solve the linear equation $(\alpha^3 + 1)x = \alpha$.

(e) Solve the equation $((\alpha^3 + 1)x + \alpha)^{2^8} = 1$.

Exercise 1.14. *For each of the polynomials, find out if they are reducible, irreducible and/or primitive,*

(a) $x^4 + x + 1$ over $\mathbb{Z}_2$,

(b) $x^4 + x^3 + x^2 + x + 1$ over $\mathbb{Z}_2$

(c) $x^4 + x^2 + 1$ over $\mathbb{Z}_2$,

(d) $x^4 + x + 1$ over $\mathbb{Z}_3$.