Finite Fields

P. Danziger

1 Modular Arithmetic

For a positive fixed integer n we define $a \bmod n$ to be the remainder of a when divided by n. Note that $a \bmod n$ always yields a number less than n
C and Java use % to denote mod, i.e. $a \,\%\, b$ means $a \bmod b$

1.1 Addition

Theorem 1 *For a given fixed integer n and any $a, b \in \mathbb{Z}$*

$$(a \bmod n) + (b \bmod n) = (a + b) \bmod n$$

This theorem means that all the usual algebraic rules for addition and subtraction are inherited by modular arithmetic.
This allows us to define arithmetic "modulo n" by $a + b \pmod n = (a + b) \bmod n$.

Example 2
Let $n = 5$. $3 + 1 = 4 \bmod 5$, $3 + 2 = 0 \bmod 5$, $3 + 3 = 1 \bmod 5$, etc.
$3 + 4 + 1 \bmod 5 = (((3 + 4) \bmod 5) + 1) \bmod 5 = 2 + 1 \bmod 5 = 3$,
$3 + 4 + 1 \bmod 5 = (3 + ((4 + 1) \bmod 5) = 3 + 0 \bmod 5 = 3$.
We often write the $\bmod n$ at the end to indicate that the whole calculation is to be done $\bmod n$. By taking $\bmod n$ after each operation we can keep the size of the operands manageable (less than n).
Since there are a finite number of possibilities we may write down the table of addition modulo 5:

+ mod 5	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

Addition mod 5

Notation We use $\mathbb{Z}_n$ to denote the set of integers from 0 to $n - 1$, together with the operation of addition modulo n.

Theorem 3 *Addition modulo n satisfies all of the following:*

Closure For all $a, b \in \mathbb{Z}_n$, $a + b \in \mathbb{Z}_n$.

Associativity For all $a, b, c \in \mathbb{Z}_n$, $(a + b) + c = a + (b + c)$.

Existence of Identity There exist an element of $\mathbb{Z}_n$, denoted 0, such that for every $a \in \mathbb{Z}$, $a + 0 = 0 + a = a$.

Existence of Inverse For every $a \in \mathbb{Z}_n$, there exists $-a \in \mathbb{Z}_n$, called the *additive inverse of a,* such that $a + (-a) = (-a) + a = 0$.

Definition 4 *Given a set S and a binary operation '$+$' defined on S if $+$ satisfies the above axioms $(S, +)$ is called a group. If it also satisfies commutativity below it is called a commutative group or an Abelian group.*

Commutativity For all $a, b \in \mathbb{Z}_n$, $a + b = b + a$

We can find the additive inverse of $a \in \mathbb{F}_n$ by considering what we would have to add to a to get $0 \bmod n$, which is $n \bmod n$. ie $n - a = -a \bmod n$.

Example 5
Take $n = 5$.

a	0	1	2	3	4
$-a$	-0	-1	-2	-3	-4
$-a \bmod 5$	0	4	3	2	1

So, for example, $2 + 3 = 0 \bmod 5$, so $3 = -2 \bmod 5$ and $2 = -3 \bmod 5$.

1.2 Multiplication

We can also define multiplication modulo n in a similar way:

Theorem 6 *For a given fixed integer n and any $a, b \in \mathbb{Z}$*

$$(a \bmod n) \times (b \bmod n) = (a \times b) \bmod n$$

Example 7
Let $n = 5$. $3 \times 1 = 3 \bmod 5$, $3 \times 2 = 1 \bmod 5$, $3 \times 3 = 4 \bmod 5$, etc.
$3 \times 4 \times 2 \bmod 5 = (((3 \times 4) \bmod 5) \times 2) \bmod 5 = 2 \times 2 \bmod 5$.
Once again by taking mod n after each operation we can keep the size of the operands manageable (less than n).
In a similar manner to addition we may write down the table of multiplication modulo 5:

$\times \bmod 5$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Multiplication mod 5

For the moment we will use S_n to denote the integers from 1 to $n-1$, i.e. $S_n = \{1, 2, 3, \ldots, n-1\}$ We would like to say that the operation of $\times$ on S_n is a group. It satisfies closure, associativity and commutativity above. In addition, since we exclude 0 from our set, there is an identity, namely 1. However, there is a problem with inverses. Consider the case where $n = 6$:

x	1	2	3	4	5
$2x \bmod 6$	2	4	0	2	4

There is no $x \in S_6$ such that $2x = 1$. Further $2 \times 3 = 0 \bmod 6$, so there are "zero divisors". Also, division is not well defined: is $4/2 = 2$ or 5 mod 6?
In fact these problems are related. Saying that there are $a, b \in S_n$ such that $ab = 0 \bmod n$ is just saying that a and b are factors of n. If n has no factors (i.e. n is prime) there will be no "zero divisors" and division will be well defined.

Theorem 8 *If p is a prime, then for every $a \in S_p$, there exists $b \in S_p$, called the* multiplicative inverse of a, *such that $ab = ba = 1$. We write a^{-1} for b.*

This means that in the case where n is a prime multiplication is a group on S_n and division is well defined.

1.3 Finite Fields

If a set S has a binary operation $(+)$ defined on it with identity $0 \in S$ and another binary operation on $S \setminus \{0\}$ $(\times)$, $(S, +, \times)$ is called a field if these two operations are both groups and also satisfy the distributive laws below. For all a, b and $c \in S$:

D1 $a \times (b + c) = a \times b + a \times c$.

D2 $(b + c) \times a = b \times a + c \times a$.

The set $\{0, 1, 2, \ldots, p-1\}$, where p is a prime with addition and multiplication modulo p is a field. We denote this field by $\mathbb{F}_p$.

1.3.1 Prime Power Fields

If $q = p^\alpha$ is a power of a prime it is possible to define a multiplication operation that satisfies all of the group axioms. This gives rise to prime power fields.

Example 9
$q = 4 = 2^2$. Addition is defined as usual, multiplication is now given by the table below.

$\times$ in 2^2	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	3	1
3	0	3	1	2

Multiplication in 2^2

We will not consider such fields further in this course. All fields from now on will be either $\mathbb{R}$ or $\mathbb{F}_p$ for some prime p, however most of the ideas herein are the same for any field.

1.4 Binary

A case worthy of special attention is when $p = 2$, $\mathbb{F}_2$ - binary arithmetic.

$+$	0	1
0	0	1
1	1	0

$\times$	0	1
0	0	0
1	0	1

Binary addition is equivalent to the logical operation of XOR and binary multiplication is equivalent to the logical operation of AND.
In particular note that $1 + 1 = 0$, and so $-1 = 1$.

$$0 - 0 = 0 \qquad 1 - 1 = 0 \qquad 1 - 0 = 1 \qquad 0 - 1 = 1.$$

We also have the corresponding operation of *binary division*:

$$\frac{1}{1} = 1 \qquad \frac{0}{1} = 0$$

Exercises 1

1. Find the following. In each case you answer should be an integer between 0 and 4. (Hint there's an easy way to find the value of any integer mod 5)
   (a) $5 + 4 \bmod 5$
   (b) $12384423344 + 2344872309 \bmod 5$
   (c) $12384423344 + 2344872309 + 2 \bmod 5$
   (d) $3 - 4 \bmod 5$
   (e) $-7 \bmod 5$
   (f) $15 - 7 \bmod 5$
   (g) $134857908752 - 954871451098754 \bmod 5$
2. Find the following. In each case you answer should be an integer between 0 and 4.
   (a) $3 \times 2 \bmod 5$
   (b) $5 \times 4 \bmod 5$
   (c) $3 \times (-2) \bmod 5$
   (d) $3 \times (-2) \bmod 5$
   (e) $134857908752 \times 954871451098754 \bmod 5$
3. Find the following. In each case you answer should be an integer between 0 and 4. You will need to use the multiplication table for mod 5 on page 2 to find inverses.
   (a) $a^{-1} \bmod 5$ for each $a \in \{1, 2, 3, 4\}$

(b) $3 \cdot 2^{-1} \bmod 5$.

(c) $1/3 \bmod 5$

(d) $\frac{134857908752}{54871451098754} \bmod 5$

(e) Is $2 \times 4^{-1} = 1 \times 2^{-1} \bmod 5$? i.e. is $\frac{2}{4} = \frac{1}{2} \bmod 5$?

4. Verify that the prime power Field in example 1.3.1 satisfies D1 and D2 on page 3 in the following cases:

(a) $(a, b, c) = (0, 2, 1)$

(b) $(a, b, c) = (3, 2, 1)$

(c) $(a, b, c) = (2, 1, 1)$

2 Multiplicative Inverses

The statement that multiplicative inverses exist is all very well, but they seem to be difficult to find. In this section we investigate some of these difficulties and try to find ways around them.
We can find the multiplicative inverse of $a \in \mathbb{F}_p$ by finding $b \in \mathbb{F}_p$ such that $ab = 1 \bmod p$. This can be done by finding integer solutions to the equation $ax = 1 + py$ or equivalently $ax - py = 1$ over the integers. The value of y is discarded and $b = x \bmod p$. Equations of this form $(ax - py = 1)$ are known as *Diophantine equations.*

2.1 Brute Force

We first try a brute force approach to finding inverses. This can somnetimes be effective, especially for small fields.

Example 10

1. If $p = 5$ we may work from the table above: $2^{-1} = 3$, $3^{-1} = 2$ and $4^{-1} = 4 \bmod 5$.

2. Take $p = 17$.

   To find $2^{-1} \bmod 17$ we must find integer solutions to $2x - 17y = 1$. Let $t \in \mathbb{R}$ then the general solution is $((1 + 17t)/2, t)$ taking $t = 1$, $x = 18/2 = 9$ and so $2^{-1} = 9 \bmod 17$.

   Similarly, to find $3^{-1} \bmod 17$ we must find integer solutions to $3x - 17y = 1$. Let $t \in \mathbb{R}$ then the general solution is $((1 + 17t)/3, t)$ taking $t = 1$, $x = 18/3 = 6$ and so $3^{-1} = 6 \bmod 17$.

   To find 4^{-1} we must find integer solutions to $4x - 17y = 1$. Let $t \in \mathbb{R}$ then the general solution is $((1 + 17t)/4, t)$. Taking $t = 1$ gives $x = 18/4$, which is not integer, $t = 2, 3, 4, 5, 6$ do not yield integer solutions either. Note that we do not have to check values that have a common divisor with 4. $t = 7$ gives $x = 120/4 = 30$, so $4^{-1} = 30 \bmod 17 = 13$.

   We can check this answer by calculating 4×13 and reducing mod 17. Indeed $4 \times 13 = 52$ and $52 \bmod 17 = 1$

Note that for large primes finding multiplicative inverses by this method can be non-trivial, since we may have to check up to p possibilities for t.

2.2 Diophantine equations

We wish to find integer solutions to equations of the form $ax - py = 1$, where p is a prime.
Recall the Euclidean Algorithm for finding $\gcd(a, b)$

int $\gcd(a, b)$ {
If $a = b = 0$, (no gcd) return ERROR.
If $a = b$ return a.
If $a = 0$ return b.
If $b = 0$ return a.
If $a > b$ return $\gcd(b, a \bmod b)$.
Else return $\gcd(a, b \bmod a)$.
}

Now since p is prime we know that $\gcd(a, p) = 1$, we may obtain a solution to $ax - py = 1$ by running the Euclidean algorithm and then reversing back up the steps from 1.

Example 11

1. To find $4^{-1} \bmod 17$ we must find integers x and y such that $4x + 17y = 1$.

   $$\gcd(17, 4) \qquad 17 = 4 \cdot 4 + 1 \qquad \therefore 1 = 17 - 4 \cdot 4$$

   So take $x = -4$ and $y = 1$. Now $-4 = 13 \bmod 17$, so $4^{-1} = 13 \bmod 17$

2. To find $5^{-1} \bmod 17$ we must find integers x and y such that $5x + 17y = 1$.

   $$\begin{array}{lll} \gcd(17, 5) & 17 = 3 \cdot 5 + 2 & \therefore 2 = 17 - 3 \cdot 5 \\ \gcd(5, 2) & 5 = 2 \cdot 2 + 1 & \therefore 1 = 5 - 2 \cdot 2 \end{array}$$

   Now go backwards

   $$\begin{aligned} 1 &= 5 - 2 \cdot \underline{2} \\ &= 5 - 2 \cdot (17 - 3 \cdot 5) \\ &= 7 \cdot 5 - 2 \cdot 17 \end{aligned}$$

   So take $x = 7$, i.e. $5^{-1} = 7 \bmod 17$

3. Find integers x and y such that $37x + 29y = 1$.

   First run the Euclidean algorithm to find $\gcd(37, 29)$, keeping track of the steps. We know that the final answer will be 1.

   $$\begin{array}{lll} \gcd(29, 37) & 37 = 1 \cdot 29 + 8 & \therefore 8 = 37 - 1 \cdot 29 \\ \gcd(29, 8) & 29 = 3 \cdot 8 + 5 & \therefore 5 = 29 - 3 \cdot 8 \\ \gcd(8, 5) & 8 = 1 \cdot 5 + 3 & \therefore 3 = 8 - 1 \cdot 5 \\ \gcd(5, 3) & 5 = 1 \cdot 3 + 2 & \therefore 2 = 5 - 1 \cdot 3 \\ \gcd(3, 2) & 3 = 1 \cdot 2 + 1 & \therefore 1 = 3 - 1 \cdot 2 \end{array}$$

   Now go backwards

   $$\begin{aligned} 1 &= 3 - 1 \cdot \underline{2} \\ &= 3 - 1 \cdot (5 - 1 \cdot 3) \\ &= 2(8 - 1 \cdot 5) - 5 \\ &= 2 \cdot 8 - 3(29 - 3 \cdot 8) \\ &= -3 \cdot 29 + 11(37 - 1 \cdot 29) \\ &= 11 \cdot 37 - 14 \cdot 29 \end{aligned}$$

   $$\begin{aligned} &= 2 \cdot \underline{3} - 5 \\ &= 2 \cdot 8 - 3 \cdot \underline{5} \\ &= -3 \cdot 29 + 11 \cdot \underline{8} \end{aligned}$$

So $37^{-1} \bmod 29 = 11$ and $29^{-1} = -14 = 23 \bmod 37$.

Exercises 2

1. Find the following inverses. Your answer should be an integer between 0 and $n-1$.
   (a) $29^{-1} \bmod 39$
   (b) $17^{-1} \bmod 39$
   (c) $23^{-1} \bmod 59$
   (d) $45^{-1} \bmod 59$
   (e) $5^{-1} \bmod 59$
   (f) $(-1)^{-1} \bmod 59$

3 Geometry over $\mathbb{F}_p$

All the elements of this course rely only on the field structure of $\mathbb{R}$, and so we may effectively do the course replacing $\mathbb{R}$ by $\mathbb{F}_p$.
As in $\mathbb{R}$ we may define algebraic equations, such as $ax = b$ over $\mathbb{F}_p$ and solve them. But since ax is undefined when $a \notin \mathbb{F}_p$ all coefficients and constants must be from 0 to $p-1$. Similarly the solutions must also be in $\mathbb{F}_p$, ie from 0 to $p-1$.
In an analogy with $\mathbb{R}^n$ we may define the space $\mathbb{F}_p^n$:

$$\mathbb{F}_p^n = \{(x_1, \ldots, x_n) \mid x_i \in \mathbb{F}_p\},$$

the set of *vectors of length* n, with components from $\mathbb{F}_p$.

Example 12
$\mathbb{F}_3^2$ has nine points

$$\begin{array}{ccc} (0,2) & (1,2) & (2,2) \\ (0,1) & (1,1) & (2,1) \\ (0,0) & (1,0) & (2,0) \end{array}$$

We can solve equations over $\mathbb{F}_3$. For example $2x = 1 \Rightarrow x = \frac{1}{2} = 2 \bmod 3$
We can also have parametric solutions to linear equations.

Example 13 *Solve* $x + y = 0$ *over* $\mathbb{F}_3$.
Let $t \in \mathbb{F}_3$, set $y = t$, $x = -t = 2t$ ($-1 = 2$ in $\mathbb{F}_3$), so the general solutions is $(2t, t)$. But since $t \in \mathbb{F}_3$ it takes only three possible values $0, 1, 2$. So the set of all solutions is $\{(0,0), (2,1), (1,2)\}$, corresponding to $t = 0, 1, 2$ respectively.
Thus the line $x + y = 0$ in $\mathbb{F}_3$ consists of the three points $(0,0), (2,1)$ and $(1,2)$.

When $p = 2$, ie binary we often don't write the commas or brackets, thus we write $(0,1,1,0,1,0,1,0) \in \mathbb{F}^8$ as 01101010. $\mathbb{F}^8$ is 8-tuples of binary digits, commonly known as a byte.

We define vector addition of binary vectors in $\mathbb{F}_p^n$.

Definition 14 *If* $\mathbf{u} = (u_1, u_2, \ldots, u_n)$ *and* $\mathbf{v} = (v_1, v_2, \ldots v_n)$ *then*

$$\mathbf{u} + \mathbf{v} = (u_1 + v_1, u_2 + v_2, \ldots, u_n + v_n)$$

In the case of binary ($p = 2$) this is often called *bitwise addition* or addition without carry (c.f. bitwise XOR from MTH 110).

Example $p = 2$

$$\begin{array}{rr} & 01101010 \\ + & 11011011 \\ \hline = & 10110001 \end{array}$$

We may also define scalar multiplication $k\mathbf{u}$, for $k \in \mathbb{F}_p$

$$k\mathbf{u} = (ku_1, ku_2, \ldots, ku_n)$$

Note though that in the case of binary k can only be 0 or 1 we either have $k\mathbf{u} = \mathbf{u}$ ($k = 1$) or $k\mathbf{u} = \mathbf{0}$ ($k = 0$).

We may now go on to develop a geometry of $\mathbb{F}^n$ in an analogous way to the geometry over $\mathbb{R}^n$. In such a geometry lines, of are of the form

$$\mathbf{x} = \mathbf{a} + t\mathbf{v}, \quad t \in \mathbb{F}_p.$$

But since $t \in \mathbb{F}_p$, it can only take p values and so lines have exactly p points. Planes (2-parameter solutions) will have exactly p^2 points and so on. So for example, in the binary case ($p = 2$) lines contain only 2 points and planes will contain 4 points.

Exercises 3

1. List all the points in $\mathbb{F}_2^3$, $\mathbb{F}_4^2$.
2. Find all points in the line $x + 3y = 1$ in $\mathbb{F}_5^2$.
3. Find the general solution to the following. In each case indicate how many points are in the solution space.
   (a) $x + 2y = 0$ in $\mathbb{F}_5^2$.
   (b) $x + 2y = 0$ in $\mathbb{F}_7^2$.
   (c) $x + 2y = 0$ in $\mathbb{F}_5^3$.
   (d) $x + 2y + z = 0$ in $\mathbb{F}_5^3$.
4. Find $\mathbf{u} + \mathbf{v}$ for the following values of $\mathbf{u}$ and $\mathbf{v}$, over the given field.
   (a) $\mathbf{u} = (0, 1, 1)$, $\mathbf{v} = (1, 0, 1)$, $\mathbb{F}_2$
   (b) $\mathbf{u} = (0, 1, 1)$, $\mathbf{v} = (1, 0, 1)$, $\mathbb{F}_3$
   (c) $\mathbf{u} = (2, 1, 1, 3)$, $\mathbf{v} = (3, 2, 1, 3)$, $\mathbb{F}_3$
   (d) $\mathbf{u} = (2, 1, 1, 3)$, $\mathbf{v} = (3, 2, 1, 3)$, $\mathbb{F}_5$

5. Find $k\mathbf{u}$ for the following values of k and $\mathbf{u}$.
   (a) $\mathbf{u} = (0, 1, 1)$, $k = 1$, $\mathbb{F}_2$
   (b) $\mathbf{u} = (0, 1, 1)$, $k = 0$, $\mathbb{F}_2$
   (c) $\mathbf{u} = (2, 3, 1, 3)$, $k = 3$, $\mathbb{F}_5$
6. Find $3\mathbf{u} - 4\mathbf{v}$ over $\mathbb{F}_5$, where $\mathbf{u} = (2, 3, 1, 3)$ and $\mathbf{v} = (3, 2, 1, 3)$.
7. What do you notice about $k\mathbf{u}$ over $\mathbb{F}_2$ (binary)?

4 Solving Systems of Equations

We may also form systems of linear equations over $\mathbb{F}_p$, again all coefficients and constants must be from $\mathbb{F}_p$. We may use the methods developed in this course (Gaussian elimination and Gauss-Jordan) to solve them, remembering that all arithmetic is in $\mathbb{F}_p$.
Addition, subtraction, multiplication and division are the only operations necessary to do Gaussian elimination. Thus we may solve systems of equations over any finite field.

Example 15

1. Solve the following system of equations in $\mathbb{F}_3$.

$$\begin{array}{rcrcl} x & + & y & = & 1 \\ x & - & y & = & 0 \end{array}$$

   Note that since we are in $\mathbb{F}_3$ all coefficients and constants must be in $\mathbb{F}_3$, if they are not we may reduce them mod 3. In particular $-1 = 2 \bmod 3$, so the second equation can be rewritten $x + 2y = 0$. Further the solutions x and y are also in $\mathbb{F}_3$. Finally all arithmetic is mod 3.

$$\left(\begin{array}{cc|c} 1 & 1 & 1 \\ 1 & 2 & 0 \end{array}\right)$$
$$\left(\begin{array}{cc|c} 1 & 1 & 1 \\ 0 & 1 & -1 \end{array}\right) \quad R_2 \to R_2 - R_1$$
$$\left(\begin{array}{cc|c} 1 & 1 & 1 \\ 0 & 1 & 2 \end{array}\right) \quad (-1 = 2 \bmod 3)$$

   Now the second equation says $y = 2$, substituting into the first equation ($x + y = 1$) gives $x + 2 = 1$, so $x = 1 - 2 = -1 = 2 \bmod 3$, so the final solution is $(x, y) = (2, 2)$.

2. Solve the following system of equations in $\mathbb{F}_5$.

$$\begin{array}{rcrcl} x & + & 3y & = & 1 \\ 2x & + & 3y & = & 1 \end{array}$$

   Note that since we are in $\mathbb{F}_5$ all coefficients and constants must be in $\mathbb{F}_5$. If they are not we may reduce them mod 5. Further the solutions x and y are also in $\mathbb{F}_5$. Finally all arithmetic

is mod 5.

$$\begin{array}{rll} & \left(\begin{array}{cc|c} 1 & 3 & 1 \\ 2 & 3 & 1 \end{array}\right) & \\ = & \left(\begin{array}{cc|c} 1 & 3 & 1 \\ 0 & 3-1 & 1-2 \end{array}\right) & \begin{array}{l} R_2 \to R_2 - 2R_1 \\ \left(\begin{array}{c} 3 \times 2 = 1 \bmod 5, \\ -1 = 4 \bmod 5 \end{array}\right) \end{array} \\ = & \left(\begin{array}{cc|c} 1 & 3 & 1 \\ 0 & 2 & 4 \end{array}\right) & \\ = & \left(\begin{array}{cc|c} 1 & 3 & 1 \\ 0 & 1 & 2 \end{array}\right) & \begin{array}{l} R_2 \to 3R_2 \\ (3 = \frac{1}{2} \bmod 5) \end{array} \end{array}$$

From the second equation we have that $y = 2$, substituting this in the first gives $x + 3 \times 2 = 1$, so $x = 1 - 1 = 0$. So the solution (mod 5) is $(x, y) = (2, 0)$.

3. Solve the following system of equations in $\mathbb{F}_5$.

$$\begin{array}{rcrcl} x & + & 3y & = & 1 \\ 4x & + & 2y & = & 1 \end{array}$$

Once again all arithmetic is modulo 5.

$$\begin{array}{rll} & \left(\begin{array}{cc|c} 1 & 3 & 1 \\ 4 & 2 & 1 \end{array}\right) & \\ = & \left(\begin{array}{cc|c} 1 & 3 & 1 \\ 0 & 0 & -3 \end{array}\right) & \begin{array}{l} R_2 \to R_2 - 4R_1 \\ (3 \times 4 = 12 = 2 \bmod 5) \end{array} \end{array}$$

So the system has no solution.

4. Solve the following system of equations in $\mathbb{F}_5$.

$$\begin{array}{rcrcl} x & + & 3y & = & 0 \\ 4x & + & 2y & = & 0 \end{array}$$

We reduce as in the previous example and get

$$\left(\begin{array}{cc|c} 1 & 3 & 0 \\ 0 & 0 & 0 \end{array}\right)$$

We now proceed as in the real case, but substituting $\mathbb{F}_5$ for $\mathbb{R}$.

Let $t \in \mathbb{F}_5$, $y = t$, $x = -3t = 2t \bmod 5$. So we have a 1-parameter solution $(x, y) = (2t, t)$. But since $t \in \mathbb{F}_5$ it can take only 5 values, thus this "line" has five points:

$$\{(0,0), (2,1), (4,2), (1,3), (3,4)\}$$

5. Solve the following system over $\mathbb{F}_2$

$$\begin{array}{l} x = 1 \\ x + y = 0 \end{array}$$

The corresponding augmented matrix is

$$\left(\begin{array}{cc|c} 1 & 0 & 1 \\ 1 & 1 & 0 \end{array}\right)$$

$R_2 \to R_2 + R_1$ (remember $-1 = 1$ so this is the same as $R_2 \to R_2 - R_1$)

$$\left(\begin{array}{cc|c} 1 & 0 & 1 \\ 0 & 1 & 1 \end{array}\right)$$

So the solution is $(x, y) = (1, 1)$.

6. Solve the following system over $\mathbb{F}_2$

$$\begin{aligned} x + z &= 1 \\ x + y + z &= 1 \end{aligned}$$

The corresponding augmented matrix is

$$\left(\begin{array}{ccc|c} 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{array}\right)$$

$R_2 \to R_2 + R_1$

$$\left(\begin{array}{ccc|c} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 \end{array}\right)$$

We have a one parameter solution, the parameter will now be in $\mathbb{F}_2$ rather than $\mathbb{R}$.

Let $t \in \mathbb{F}_2$, $z = t$, then $y = 0$, $x = 1 - t$, so the solution is the "line"

$$\mathbf{x} = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} + t \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}$$

But since $t \in \mathbb{F}_2$ it can take only two values, 0 or 1, and thus there are only two points on this line: $\mathbf{x} = (1, 0, 0)$ $(t = 0)$ and $\mathbf{x} = (0, 0, 1)$ $(t = 1)$.

Exercises 4

1. Solve the following systems of equations over the given field.

   (a)

$$\begin{aligned} x + 2y + z &= 1 \\ x + z &= 1 \\ -x - y - z &= -1 \end{aligned} \qquad \text{Over } \mathbb{F}_3$$

   (b)

$$\begin{aligned} x + y &= 2 \\ x + 3y + 3z &= 0 \\ y + 2z &= 1 \end{aligned} \qquad \text{Over } \mathbb{F}_5$$

(c)

$$\begin{array}{ll} x+y+z=0 & \\ y+z=1 & \text{Over } \mathbb{F}_2 \\ x+y=0 & \end{array}$$

2. Solve the following system first over $\mathbb{F}_2$, then over $\mathbb{F}_5$, then over $\mathbb{F}_{11}$ and then over $\mathbb{R}$. (Note you will have to reduce the coefficients first)

$$\begin{aligned} x+3y-z&=0\\ 2x+7y+4z&=3\\ 3x+7y-6z&=6 \end{aligned}$$

Can you think of a quicker way to do this question?

3. Find the values of k so that system has unique solution, no solutions and a one parameter family of solutions over $\mathbb{F}_3$.

$$\begin{aligned} x+y-2z&=2\\ y+z&=1\\ -2y+k^2z&=k+1 \end{aligned}$$

5 Matrices over Finite Fields

We see matrices over a finite field arising naturally. We may define the usual operations of matrix addition and matrix multiplication, but now all arithmetic is in $\mathbb{F}_p$.
In the case of binary ($p=2$) the corresponding matrices are often referred to as *zero one matrices* since all their entries are either 0 or 1. Note that for two zero one matrices A and B, $A+B=0 \Leftrightarrow A=B$.

Example 16
$p=2$

1.

$$\begin{pmatrix} 0 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix} + \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} = \begin{pmatrix} 0+1 & 1+1 & 0+0 \\ 1+1 & 1+0 & 0+1 \\ 0+0 & 1+1 & 1+0 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

2.

$$\begin{aligned} &\begin{pmatrix} 0 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \\ &= \begin{pmatrix} 0\cdot 1+1\cdot 1+0\cdot 0 & 0\cdot 1+1\cdot 0+0\cdot 1 & 0\cdot 0+1\cdot 1+0\cdot 0 \\ 1\cdot 1+1\cdot 1+0\cdot 0 & 1\cdot 1+1\cdot 0+0\cdot 1 & 1\cdot 0+1\cdot 1+0\cdot 0 \\ 0\cdot 1+1\cdot 1+1\cdot 0 & 0\cdot 1+1\cdot 0+1\cdot 1 & 0\cdot 0+1\cdot 1+1\cdot 0 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix} \end{aligned}$$

Just as in $\mathbb{R}$ we may find inverses of matrices. We may use Gauss-Jordan to find the inverse in exactly the same way as with $\mathbb{R}$. Similarly determinants may be found.

Example 17
Find the inverse of the following matrix over $\mathbb{F}_2$

$$A = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \end{pmatrix}$$

We first check that the matrix is invertible by finding the determinant. We find the determinant by expanding along the first row. $|A| = \begin{vmatrix} 1 & 1 \\ 1 & 1 \end{vmatrix} + \begin{vmatrix} 1 & 1 \\ 0 & 1 \end{vmatrix} = 1$. So A is invertible.

$$\longrightarrow \left(\begin{array}{ccc|ccc} 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{array}\right) \longrightarrow \left(\begin{array}{ccc|ccc} 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{array}\right) \quad R_2 \to R_2 + R_1$$

$$\longrightarrow \left(\begin{array}{ccc|ccc} 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 \end{array}\right) \quad R_3 \to R_3 + R_2 \longrightarrow \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 \end{array}\right) \quad R_1 \to R_1 + R_3$$

$$\text{So} \qquad A^{-1} = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix}$$

Exercises 5

1. How many distinct 3×3 matrices over $\mathbb{F}_2$ are there?
2. How many values for $\det(A)$ are there if A is a square matrix over $\mathbb{F}_p$?
3. Find $A + B$ over the given field.

   (a) $A = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix}$, $B = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \end{pmatrix}$ $\mathbb{F}_2$

   (b) $A = \begin{pmatrix} 0 & 2 & 1 & 2 & 3 \\ 1 & 1 & 3 & 3 & 4 \\ 3 & 4 & 1 & 4 & 1 \end{pmatrix}$, $B = \begin{pmatrix} 3 & 3 & 4 & 4 & 2 \\ 2 & 1 & 4 & 2 & 1 \\ 0 & 4 & 1 & 4 & 0 \end{pmatrix}$ $\mathbb{F}_5$
4. Find the given matrix product over the given field.

   (a) Find AB where A and B are the matrices from 3a above over $\mathbb{F}_2$. What can you conclude about these matrices?

   (b) Find AB^T where A and B are the matrices from 3b above over $\mathbb{F}_5$.
5. For each of the following matrices determine if they are invertible and if so find the inverse.

(a) $B = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix}$ $\mathbb{F}_2$

(b) $B = \begin{pmatrix} 1 & 0 & 1 \\ 2 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix}$ $\mathbb{F}_3$