MAT 240 : Notes on Finite Fields

Recall that an integer $p \geq 2$ is prime if p and 1 are the only positive integers which divide p. In these notes, we explain how to use integers and addition and multiplication "modulo p" to see that there is a field containing p elements for each prime p.

Let $\mathbb{Z} = \{ 0, \pm 1, \pm 2, \pm 3, \dots \}$ be the set of integers. Let p be a prime. We begin by defining a function $r_p : \mathbb{Z} \to \{ 0, 1, 2, \dots, p-2, p-1 \}$. If n is an integer, then there exist unique integers q and $r_p(n)$ satisfying:

$$n = qp + r_p(n), \quad r_p(n) \in \{ 0, 1, 2, \dots, p-2, p-1 \}.$$

The value $r_p(n)$ is the remainder that we get after dividing n by p, where the remainder is always taken in the set $\{ 0, 1, 2, \dots, p-2, p-1 \}$. Of course, if $n \in \{ 0, 1, \dots, p-1 \}$, then $r_p(n) = n$.

Examples:

(1) If $p = 7$, then $r_p(-20) = 1$. To see this, add multiples of 7 to 20 until you get an integer between 1 and $p - 1 = 6$: $-20 + 7 = -14$, $-20 + 2 \cdot 7 = -6$, $-20 + 3 \cdot 7 = 1$. So $-20 = -3 \cdot 7 + 1$, and $r_7(-20) = 1$.

(2) If $p = 5$ and $n = 67$, then the largest multiple of 5 that is no greater than 67 is $65 = 13 \cdot 5$. Therefore $67 = 13 \cdot 5 + 2$ and $r_5(67) = 2$.

If p is prime, as a set, the finite field $\mathbb{F}_p$ is equal to the set $\{ 0, 1, 2, \dots, p-2, p-1 \}$ (which certainly contains p elements). Note that the set $\mathbb{F}_p$ is clearly not closed under the usual addition of integers or under the usual multiplication of integers.

If a, $b \in \mathbb{Z}$, the sum of a and b modulo p, which we will write $a + b (\bmod p)$, is defined by:

$$a + b (\bmod p) = r_p(a + b).$$

And the product of a and b modulo p, which we will write $ab (\bmod p)$, is defined by:

$$a \cdot b (\bmod p) = ab (\bmod p) = r_p(ab).$$

We actually only need $a + b (\bmod p)$ and $ab (\bmod p)$ for a and b belonging to $\mathbb{F}_p$, but the definitions make sense for arbitrary pairs of integers. The following lemma will be useful for proving the theorem below.

Lemma. *Let p be a prime. Then $r_p(n + mp) = r_p(n)$ for all integers n and m.*

PROOF. Write $n = qp + r_p(n)$ for some integer q. Then $n + mp = qp + r_p(n) + mp = (q + m)p + r_p(n)$. Now $r_p(n) \in \mathbb{F}_p$, so we must have $r_p(n + mp) = r_p(n)$.

Theorem. *The set $\mathbb{F}_p$, with addition mod p and multiplication mod p, is a field.*

Before discussing the proof of the theorem, we look at some examples of addition and multiplication mod p.

Examples:

$$2 + 3 (\bmod 7) = r_7(2 + 3) = r_7(5) = 5, \ 2 + 6 (\bmod 7) = r_7(8) = 1, \ 2 \cdot 6 (\bmod 7) = r_7(12) = 5,$$
$$79 \cdot 86 (\bmod 101) = r_{101}(79 \cdot 86) = r_{101}(6794) = r_{101}(67 \cdot 101 + 27) = 27$$

PROOF OF THEOREM: To verify axiom (i) (referring to numbering in the notes on fields), we need to show that $r_p(a+b) = r_p(b+a)$ holds for all a and b in $\mathbb{F}_p$. This follows from the fact that $a+b = b+a$ for all integers a and b.

For axiom (ii), note that, for a, b and $c \in \mathbb{F}_p$,

$$((a+b)(\bmod p)+c)(\bmod p) = r_p(r_p(a+b)+c) \quad \text{and} \quad (a+(b+c)(\bmod p)))(\bmod p) = r_p(a+r_p(b+c)).$$

So we need to show that $r_p(r_b(a+b)+c) = r_p(a+r_p(b+c))$. Note that $a+b = qp+r_p(a+b)$, and $b+c = \ell p + r_p(b+c)$, where q and ℓ are integers. Substituting, we obtain

$$\begin{aligned} r_p(r_p(a+b)+c) &= r_p(a+b-qp+c) = r_p(a+b+c-qp) \\ r_p(a+r_p(b+c)) &= r_p(a+b+c-\ell p) \end{aligned}$$

Now apply part (1) of the above lemma to conclude that $r_p(a+b+c-\ell p) = r_p(a+b+c-qp) = r_p(a+b+c)$.

If $a \in \mathbb{F}_p$, then $a + 0(\bmod p) = r_p(a+0) = r_p(a) = a$. Therefore 0 is the additive identity in $\mathbb{F}_p$.

For axiom (iv), it is easy to see that $-0 = 0$, since $0 + 0(\bmod p) = r_p(0+0) = 0$. Now suppose that $a \in \mathbb{F}_p$ and $a \neq 0$. Then the integer $-a$ does not belong to $\mathbb{F}_p$. But the integer $p-a$ does belong to $\mathbb{F}_p$, and

$$a + (p-a)(\bmod p) = r_p(a+(p-a)) = r_p(p) = 0,$$

so the additive inverse of a in $\mathbb{F}_p$ is the integer $p-a$.

For axiom (v), note that $ab(\bmod p) = r_p(ab) = r_p(ba) = ba(\bmod p)$.

For axiom (vi), note that

$$((ab)(\bmod p)c)(\bmod p) = r_p(r_p(ab)c) \quad \text{and} \quad (a(bc)(\bmod p)))(\bmod p) = r_p(ar_p(bc)).$$

Expressing $ab = mp + r_p(ab)$ and $bc = kp + r_p(bc)$ for integers m and k, substituting, and applying the lemma above, we see that

$$\begin{aligned} r_p(r_p(ab)c) &= r_p((ab-mp)c) = r_p(abc-cmp) = r_p(abc) \\ r_p(a\, r_p(bc)) &= r_p(a(bc-kp)) = r_p(abc-akp) = r_p(abc), \end{aligned}$$

and this is what we need for axiom (vi) to hold.

The proof of axiom (vii) is similar to the proofs of axioms (ii) and (vi) and is left as an exercise.

Because $a \cdot 1(\bmod p) = r_p(a \cdot 1) = r_p(a) = a$, we see that 1 is a multiplicative indentity in $\mathbb{F}_p$.

The most difficult axiom to prove is axiom (ix).

In particular, examples, we can just test to find multiplicative inverses when p is small. For example, if p is 7, and we want to find the multiplicative inverse of 3 in $\mathbb{F}_7$, we simply compute $3 \cdot a(\bmod 7)$ for $a \in \mathbb{F}_7$ until we find an a for which $r_7(3a) = 1$: $r_7(3 \cdot 1) = 3 \neq 1$,

$r_7(3 \cdot 2) = 6 \neq 1$, $r_7(3 \cdot 3) = 2 \neq 1$, $r_7(3 \cdot 4) = 5 \neq 1$, $r_7(3 \cdot 5) = 1$. Hence 5 is the multiplicative inverse of 3 in $\mathbb{F}_7$.

But there are arbitrarily large primes, so testing is not useful in the general setting. We need to prove that if $a \in \{1, 2, \ldots, p-1\}$, there exists $b \in \{1, 2, \ldots, p-1\}$ such that $ab (\bmod p) = r_p(ab) = 1$. Equivalently, we must prove that the set

$$S = \{ a = r_p(a), r_p(2a), r_p(3a), r_p(4a), \ldots, r_p((p-1)a) \}$$

contains 1. First, we show that the set S does not contain 0. Since $1 \leq a \leq p-1$, p does not divide a. Similarly if $1 \leq j \leq p-1$, p does not divide j. Because p is prime, if $r_p(ja) = 0$, the fact that p divides the product ja implies that p divides one of the factors j and a. But this is impossible. Hence $r_p(ja) \neq 0$. Next, we show that no two of the elements of S are equal. Suppose that $r_p(ja) = r_p(ka)$ and $1 \leq k \leq j \leq p-1$. Then $ja = qp + r_p(ja) = qp + r_p(ka)$ for some integer q, and $ka = mp + r_p(ka)$ for some integer m. Subtracting, we obtain

$$(j-k)a = ja - ka = qp + r_p(ka) - mp + r_p(ka) = qp - mp = (q-m)p.$$

Therefore p divides the product $(j-k)a$. Since p is prime and p does not divide a, we must have that p divides $j-k$. But $1 \leq k \leq j \leq p-1$ implies that $0 \leq j-k \leq p-2$. The only integer between 0 and $p-2$ that is divisible by p is 0. Therefore we have shown that if $r_p(ja) = r_p(ka)$, with $1 \leq k \leq j \leq p-1$, we must have $j = k$.

We have proved that the set S contains exactly $p-1$ distinct integers, each of which belongs to $\{1, 2, \ldots, p-1\}$. This means that

$$S = \{ r_p(a), r_p(2a), r_p(3a), \ldots, r_p((p-1)a) \} = \{ 1, 2, \ldots, p-1 \}.$$

Of course, the elements are not necessarily listed in the same order above. We now can conclude that $r_p(ja) = 1$ for some integer j such that $1 \leq j \leq p-1$. The integer j is the multiplicative inverse of a in $\mathbb{F}_p$. This concludes the proof of the theorem.

Remark: If we examine the proof of axioms (ii) and (vi) above, we can show that if $a_1, a_2, \ldots, a_n \in \mathbb{F}_p$, then the sum modulo p of $a_1, a_2, \ldots, a_n$ is equal to $r_p(a_1 + a_2 + \cdots + a_n)$ and the product modulo p of these same elements is equal to $r_p(a_1 \cdot a_2 \cdots a_n)$.

A polynomial with coefficients in $\mathbb{F}_p$ is an expression of the form

$$f(t) = a_n t^n + a_{n-1} t^{n-1} + \cdots + a_2 t^2 + a_1 t + a_0, \qquad a_n,\ a_{n-1}, \ldots, a_2,\ a_1,\ a_0 \in \mathbb{F}_p,\ \ n \in \mathbb{Z},\ n \geq 0.$$

An element $c \in \mathbb{F}_p$ is a *zero* of $f(t)$ if

$$f(c) (\bmod p) = a_n c^n (\bmod p) + a_{n-1} c^{n-1} (\bmod p) + \cdots a_2 c^2 (\bmod p) + a_1 c (\bmod p) + a_0 (\bmod p) = 0.$$

When computing powers of elements in $\mathbb{F}_p$, it is useful to note that the nth power $c^n (\bmod p)$ of c is the product mod p of c with itself n times. Therefore, according to the remark above, $c^n (\bmod p) = r_p(c^n)$. And we also have

$$f(c) (\bmod p) = (a_n c^n + a_{n-1} c^{n-1} + \cdots + a_1 c + a_0) (\bmod p) = r_p(a_n c^n + \cdots + a_1 c + a_0).$$

Examples:

(1) $p = 7$, $f(t) = t^2 + 1$ has no zeros in $\mathbb{F}_7$, because

$$\begin{aligned} f(0)(\operatorname{mod} 7) &= (0 \cdot 0 + 1)(\operatorname{mod} 7) = r_7(0+1) = r_7(1) = 1 \\ f(1)(\operatorname{mod} 7) &= (1 \cdot 1 + 1)(\operatorname{mod} 7) = r_7(1) = 2 \\ f(2)(\operatorname{mod} 7) &= (2 \cdot 2 + 1)(\operatorname{mod} 7) = r_7(5) = 5 \\ f(3)(\operatorname{mod} 7) &= (3 \cdot 3 + 1)(\operatorname{mod} 7) = r_7(10) = 3 \\ f(4)(\operatorname{mod} 7) &= (4 \cdot 4 + 1)(\operatorname{mod} 7) = r_7(17) = 3 \\ f(5)(\operatorname{mod} 7) &= (5 \cdot 5 + 1)(\operatorname{mod} 7) = r_7(26) = 5 \\ f(6)(\operatorname{mod} 7) &= (6 \cdot 6 + 1)(\operatorname{mod} 7) = r_7(37) = 2 \end{aligned}$$

It follows that the additive inverse $-1(\operatorname{mod} 7) = 6$ of 1 in $\mathbb{F}_7$ is not a square in $\mathbb{F}_7$.

(2) $p = 5$, $f(t) = t^2 + 1$. Note that $f(2) = (2 \cdot 2 + 1)(\operatorname{mod} 5) = r_5(5) = 0$ and $f(3) = (3 \cdot 3 + 1)(\operatorname{mod} 5) = r_5(5) = 0$. So the additive inverse $-1(\operatorname{mod} 5) = 4$ of 1 in $\mathbb{F}_5$ has two square roots, 2 and 3. We can factor the polynomial as $t^2 + 1 = (t+2)(t+3)$ (addition and multiplication are modulo 5 here!).

(3) Which elements in $\mathbb{F}_7$ are cubes in $\mathbb{F}_7$? That is, for which $a \in \mathbb{F}_7$ does the polynomial $t^3 + (7 - a)$ have zeros in $\mathbb{F}_7$? *Answer*: 0, 1, and 6 are cubes in $\mathbb{F}_7$, and 2, 3, and 5 are non-cubes in $\mathbb{F}_7$. The details are left as an exercise.

(3) How do the polynomials $t^3 + 6$ and $t^3 + 1$ factor over $\mathbb{F}_7$? *Answer*: $t^3 + 1 = (t+1)(t+2)(t+4)$ and $t^3 + 6 = (t+6)(t+3)(t+5)$. The details are left as an exercise.

Now let m be an integer such that $m \geq 2$. We can define a function r_m from the integers to the set $\{0, 1, 2, \ldots, m-1\}$ as we did when m was prime. Given an integer n, there are unique integers q and $r_m(n)$ such that $n = qm + r_m(n)$, and $0 \leq r_m(n) \leq m - 1$. The function r_m can be used to define addition modulo m and multiplication modulo m, making the set $\{0, 1, 2, \ldots, m-1\}$ into a set with a new addition and multiplication. If m is not prime (that is, if there is a prime p with $p < m$ and p dividing m), then axioms (i)–(vii) will hold. But axiom (ix) does not hold when m is composite. The integer p belongs to the set $\{0, \ldots, m-1\}$, and p is nonzero. If there existed a multiplicative inverse modulo m for p, then there would be an integer n with $1 \leq n \leq m - 1$ and $p \cdot n(\operatorname{mod} m) = r_m(pn) = 1$. That would mean that $pn = mk + 1$ for some integer k. But p divides both pn and mk. Therefore p divides $1 = pn - mk$. This is impossible. Therefore p does not have a multiplicative inverse modulo m. (For example, 2 and 3 do not have multiplicative inverses modulo 6).

The finite field $\mathbb{F}_p$ contains p elements. There are other finite fields. It can be shown that if F is a finite field (that is, a field that contains finitely many elements) then there exists a prime p and a positive integer n such that F contains p^n elements.