

**The field of  $p$  elements** Let  $p$  denote a prime number. Let  $\mathbb{F}_p$  be the collection of residue classes modulo  $p$ ; there are  $p$  such residue classes. Addition is clearly a cyclic commutative group, sometimes referred to as clockwork addition. When all elements except 0 are considered, multiplication forms commutative group on this set. Clearly, the multiplicative identity element is  $1 \pmod{p}$ . Multiplication defined in this way is associative and commutative. If  $n$  and  $m$  are integers and  $n \pmod{p}$  and  $m \pmod{p}$  are both non-zero, then  $nm \pmod{p}$  is also non-zero. Therefore the product of two nonzero elements in  $\mathbb{F}_p$  is always nonzero. Inverses exist because of Fermat's Theorem, which summarized is, if  $a \not\equiv 0 \pmod{p}$  then  $a^{p-1} \equiv 1 \pmod{p}$ . We have  $a \cdot a^{p-2} \equiv 1 \pmod{p}$ , and therefore that the class of  $a^{p-2}$  is a multiplicative inverse of the class of  $a$ . The distributive law holds as a result of the distributivity of modular addition and multiplication.  $\mathbb{F}_p$  forms a field.

**Proposition 1** Suppose  $p$  is a prime. Then  $-1$  is not a square modulo  $p$  if and only if  $p \equiv 3 \pmod{4}$ .

**Proof of Proposition 1**  $\Rightarrow$  Assume that  $p \not\equiv 3 \pmod{4}$ . We are left with three remaining cases. We know there is no prime such that  $p \equiv 0 \pmod{4}$ . There is only one prime such that  $p \equiv 2 \pmod{4}$ , which is 2. Modulo 2,  $1^2 = 1 = -1$ .  $-1$  is a square. In our last case,  $p \equiv 1 \pmod{4}$ . We take the quantity:

$$(1 \cdot 2 \cdot 3 \cdots \frac{p-1}{2})^2 = (1 \cdot 2 \cdot 3 \cdots \frac{p-1}{2})(-1 \cdot -2 \cdot -3 \cdots -\frac{p-1}{2}) \equiv (p-1)! \equiv p-1 \equiv -1 \pmod{p} \quad (1)$$

The first expression clearly shows some number squared. We multiply each distinct term once by  $-1$  to get the second expression. We know there are an even number of negative signs because  $p \equiv 1 \pmod{4}$  and  $\frac{p-1}{2} \equiv 0$  or  $2 \pmod{4}$  which is even. Therefore,  $-1^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ , and we are really just multiplying the first expression by  $1 \pmod{p}$  to get the second expression. Therefore, the first equivalence holds. The additive inverse of 1 is  $p-1$ . Any element  $k \pmod{p}$  has an additive inverse  $p-k \pmod{p}$ . Therefore,  $(-1 \cdot -2 \cdots -\frac{p-1}{2}) = (p-1 \cdot p-2 \cdots \frac{p+1}{2})$ . We use this substitution and express the product as a factorial. Thus, the second equivalence is obtained. To get the third equivalence we pair off and cancel all multiplicative inverses. Because  $p-1$  and 1 are their own multiplicative inverses, they do not cancel off. However, the remainder of terms are between 1 and  $p-1$ . There are an even number of these terms, and they all cancel. Therefore, the third equivalence holds. In this final case  $p \equiv 1 \pmod{4}$ ,  $-1$  is always a square. This completes the proof that  $-1$  is a square when  $p \equiv 1 \pmod{p}$ . This construction was on the 1992 Putnam test.

$\Leftarrow$  If  $p \equiv 3 \pmod{4}$ , then  $-1$  is not a square. We show that if  $-1$  is a square, then  $p \equiv 1 \pmod{4}$  or  $p = 2$ . Let  $-1$  be a square, such that  $b^2 \equiv -1 \pmod{p}$ . Because  $b^4 \equiv 1 \pmod{p}$ ,  $b$  must have order 1, 2, or 4. Suppose  $b$  has order 1. That would imply that  $b \equiv 1 \pmod{p}$  and  $b^2 \equiv 1 \equiv -1 \pmod{p}$  which only happens when  $p = 2$ . Suppose  $b$  has order 2. That would imply that  $b^2 \equiv 1 \pmod{p}$ . but this implies  $1 \equiv -1 \pmod{0}$ . This only happens when  $p = 2$ . In our last case, suppose  $b$  has order 4 and that  $b^4 \equiv 1 \pmod{p}$ . We know that the order of any subgroup of a group divides the order of the group. In this case, the subgroup of order 4 generated by  $b$  divides the order of the multiplicative group of  $\mathbb{F}_p$  which has  $p-1$  elements. Therefore  $4|p-1$ , so  $p-1 \equiv 0 \pmod{4}$ , implying that  $p \equiv 1 \pmod{4}$ .

**The Field of Four Elements** This table describes the operation of multiplication over the field of four elements.

$\mathbb{F}_2[x]/[x^2 + x + 1] \cong \mathbb{F}_2(a)$  where  $a$  is the root of the polynomial  $[x^2 + x + 1]$ . This field can be regarded as the set of equivalence classes in  $\mathbb{F}_2$  modulo the ideal generated by the polynomial  $x^2 + x + 1$ .

$\cdot$	0	1	$x$	$1 + x$
0	0	0	0	0
1	0	1	$x$	$1 + x$
$x$	0	$x$	$1 + x$	1
$1 + x$	0	$1 + x$	1	$x$

This Field is the original field,  $\mathbb{F}_2$ , adjoined with some new element  $a$  which is a root of  $[x^2 + x + 1]$ .

$\cdot$	0	1	$a$	$1 + a$
0	0	0	0	0
1	0	1	$a$	$1 + a$
$a$	0	$a$	$1 + a$	1
$1 + a$	0	$1 + a$	1	$a$

Adjoining some element to a finite field will not always create a new field. For instance, if we adjoin to  $\mathbb{F}_2$  an element  $i$  that is a root of  $x^2 + 1$ , we have not created a field. Note that  $(1 + i)(1 + i) = 0$ , so the set  $\mathbb{F}_2(i) - (0)$  does not form a group under multiplication. Only when the root of an irreducible polynomial is adjoined to a field, is a new field created.

**Definition of  $F(i)$**  Given a field  $F$ ,  $F(i)$  is a commutative two-dimensional ring. Elements are written as  $a + bi$  —  $a, b \in F$ . Addition is the addition of  $F^2$ , which is therefore a commutative group with additive identity  $0 + 0i$ . Multiplication is defined as  $(a + bi)(c + di) = (ac - bd) + (ad + bc)i$ . The multiplicative identity is clearly  $1 + 0i$ . Multiplication is clearly commutative. To see that multiplication is associative, we take the LHS:

$[(a + bi)(c + di)](e + fi) = [(ac - bd) + (ad + bc)i](e + fi) = (ace - bde - adf - bcf) + (acf - bdf + ade + bce)i$  We take the RHS:

$(a + bi)[(c + di)(e + fi)] = (a + bi)[(ce - df) + (de + cf)i] = (ace - bde - adf - bcf) + (acf - bdf + ade + bce)i$  The LHS and RHS are equal, therefore multiplication is associative.

To see that multiplication is distributive, we take the LHS:

$(a + bi)[(c + di) + (e + fi)] = (a + bi)[(c + e) + (d + f)i] = (ac + ae) - (bd + bf) + (ad + af)i + (bc + be)i = (ac + ae - bd - bf) + (ad + af + bc + be)i$  We take the RHS:

$(a + bi)(c + di) + (a + bi)(e + fi) = (ac - bd) + (ad + bc)i + (ae - bf) + (af + be)i = (ac + ae - bd - bf) + (ad + af + bc + be)i$  The LHS and RHS are equal, therefore multiplication is distributive.

**Lemma 1** Suppose  $F$  is a field with elements  $a$  and  $b$  and  $-1$  is not a square in  $F$ . If  $a$  and  $b$  are not both zero, then  $a^2 + b^2$  is not zero.

**Proof of Lemma 1** Suppose on the contrary that  $a^2 + b^2 = 0$ ; that is, that  $a^2 = -b^2$ . Since  $a$  and  $b$  are not both zero, this equation shows that neither  $a$  nor  $b$  is 0. Since  $F$  is a field,  $b$  has a multiplicative inverse. Multiplying the equation by  $(b^{-1})^2$  gives  $(ab^{-1})^2 = -1$ , contradicting the assumption that  $-1$  is not a square in  $F$ . This contradiction shows that  $a^2 + b^2$  is not zero, as we wished to show.

**Proposition 2** Suppose  $p$  is a prime number. The commutative ring  $\mathbb{F}_p(i)$  is also a field if and only if  $-1$  is not a square in  $\mathbb{F}_p$ .

**Proof of Proposition 2**

$\Rightarrow$  If  $\mathbb{F}_p(i)$  is a field then  $-1$  is not a square in  $\mathbb{F}_p$ . Let  $-1$  be a square in  $\mathbb{F}_p$  with  $b^2 = -1$ , and assume that  $\mathbb{F}_p(i)$  is still a field.  $(b + i)(b - i) = b^2 - i^2 + 0 = -1 + 1 = 0$  The product of two elements in the field is zero. This is a contradiction, because if  $\mathbb{F}_p(i)$  is a field, then all elements except zero should form a group under multiplication.

$\Leftarrow$  If  $-1$  is not a square, then  $\mathbb{F}_p(i)$  is a field. Given any nonzero element  $a + bi$ , we can define its multiplicative inverse:

$$\frac{a}{a^2 + b^2} + \frac{-b}{a^2 + b^2}i \tag{2}$$

Due to Lemma 1, we can be sure that  $a^2 + b^2$  is nonzero. When  $a + bi$  and its multiplicative inverse as defined above are multiplied, the result is the multiplicative identity,  $1 + 0i$ .  $\mathbb{F}_p(i)$  is a field.

**Corollary 1** The ring  $\mathbb{F}_p(i)$  is a field, if and only if  $p \equiv 3 \pmod{4}$ .

**Proposition 3** The polynomial  $x^2 + 1$  is reducible if and only if  $-1$  is a square.

$\Rightarrow$  If  $x^2 + 1$  is reducible, then the factors have to be linear:  $x^2 + 1 = (x - a)(x - b)$ . Clearly  $a$  is a root of the polynomial, so  $a^2 + 1 = 0$ , or  $a^2 = -1$ ; so  $-1$  is a square in  $F$ .

$\Leftarrow$  If  $b^2 = -1$ , then  $x^2 + 1 = (x - b)(x + b)$ .

**Suppose  $p$  is a prime.**

	$p \equiv 3 \pmod{4}$	$p \not\equiv 3 \pmod{4}$
<b>Corollary 2: Summary of results</b>	$-1$ is not a square	$-1$ is a square
	$x^2 + 1$ is irreducible	$x^2 + 1$ is reducible
	$\mathbb{F}_p(i)$ is a field	$\mathbb{F}_p(i)$ is not a field

When the root of a polynomial of degree  $n$  is adjoined to a prime field  $\mathbb{F}_p$  the resulting field has  $p^n$  elements.

In order to prove Proposition 4, we must use the following theorem:

**Lemma 2** If  $f$  and  $g$  are nonzero polynomials, there exist two polynomials  $h$  and  $k$  such that  $\gcd(f, g) = fh + gk$ . This lemma is given without proof, but can be found in most standard algebra text books. For calculations in quotient rings of polynomials, I will use the notation as in Artin's text. An element  $f$  of the quotient ring  $F[x]/I$  is given a bar and is expressed  $\bar{f}$ .

**Proposition 4** Suppose  $f$  is a monic polynomial in  $F(x)$ , of degree at least 1. Then  $F[x]/(f)$  is a field if and only if  $f$  is irreducible.

$\Rightarrow$  Suppose on the contrary, that  $f$  not irreducible. Then  $f$  is reducible and there exist two polynomials  $g$  and  $h$ , of lesser degree than  $f$  such that  $f = gh$ . We must have that  $g \notin (f)$  and similarly  $h \notin (f)$ , because both  $g$  and  $h$  are of lesser degree than  $f$ . However, when  $g$  and  $h$  are multiplied,  $\bar{g} \cdot \bar{h} = \bar{f} = 0$ , the result,  $f$  is equal to zero. Therefore,  $F[x]/(f)$  has zero divisors and cannot possibly be a field. Multiplication does not form a group.

$\Leftarrow$  Suppose that  $f$  is irreducible. We need to show that  $F[x]/(f)$  is a field. Due to Gary's presentation on polynomial rings, we know  $F[x]/(f)$  is a commutative ring. Now, all we have left to show is that for any equivalence class of polynomials  $g$ , which does not belong in the ideal  $(f)$ , there exists some multiplicative inverse for this equivalence class. Because  $g \notin (f)$ , we must also have  $f \nmid g$ . Because  $f$  is irreducible, this implies that  $\gcd(f, g) = 1$ . By lemma 1, we know there must exist polynomials  $h$  and  $k$  such that  $fh + gk = 1$ . But then, in  $F[x]/(f)$ , we must have that  $\bar{g} \cdot \bar{k} = \bar{1} - \bar{f}\bar{h} = \bar{1}$ . The first equality holds due to substitution. The second equality holds because in  $F[x]/(f)$ , we know that  $\bar{f} = \bar{0}$ . So for every nonzero polynomial  $g$ , we have show that there exists some multiplicative inverse. This completes the proof that  $F[x]/(f)$  is a field.