Cryptology Fall 2017

Chloe Martindale
TU/e

September 19, 2017

These notes are based on notes by Tanja Lange and Ruben Niederhagen.

Recall from previous courses the definition of a group:

Definition 1. A set together with an operation $(G, *)$ is a *group* if the following axioms are satisfied:

(G1) for all $a, b \in G$, $a * b \in G$.

(G2) for all $a, b, c \in G$, $(a * b) * c = a * (b * c)$.

(G3) there exists $e \in G$ such that for all $a \in G$, $a * e = e * a = a$.

(G4) for all $a \in G$, there exists $b \in G$ such that $a * b = b * a = e$.

If furthermore for all $a, binG$ we have that $a * b = b * a$ then we say that G is *abelian*.

Examples.

- $(\mathbb{Z}, +)$ is an abelian group, with $e = 0$. In this case, inversion is given by $-$.
- $(\mathbb{Z}/p\mathbb{Z}, +)$ is an abelian group, again with $e = 0$.
- $(\mathbb{Z}, \cdot)$ is *not* an abelian group! (G4) is not satisfied.
- $(\mathbb{Z}/p\mathbb{Z}, \cdot)$ is not an abelian group - (G4) is not satisfied for 0.
- Defining $(\mathbb{Z}/p\mathbb{Z})^* := \mathbb{Z}/p\mathbb{Z} - \{0\}$ gives an abelian group $((\mathbb{Z}/p\mathbb{Z})^*, \cdot)$.

Definition 2. A set K is a *field* with respect to $+$ and $\cdot$ if the following axioms are satisfied:

(F1) $(K, +)$ is an abelian group.

(F2) $(K^*, \cdot)$ is an abelian group, where $K^* = K - \{0\}$.

(F3) for every $a, b \in K$, $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$.

Remark 1. A field has no zero divisors. (That is, there do not exist $a, b \in K - \{0\}$ such that $a \cdot b = 0$.)

Proof. Exercise. ∎

Examples.

- $\mathbb{Q}$, $\mathbb{C}$, $\mathbb{R}$, and $\mathbb{Z}/p\mathbb{Z}$ are all fields.
- $\mathbb{Q}(i) := \{a + bi | a, b \in \mathbb{Q}\}$ is a field.
- $\mathbb{Z}$ is not a field - fails on (F2).
- $\mathbb{Z}[i] := \{a + bi | a, b \in \mathbb{Z}\}$ is not a field - also fails on (F2).

Definition 3. If K and L are fields and $K \subseteq L$, then K is a *subfield* of L, and L is an *extension field* of K.

Some facts about subfields:

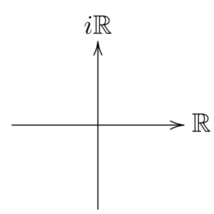
- We can add and multiply elements of K with elements of L.
- L is a vector space over K.

Examples.

- $\mathbb{Q} \subseteq \mathbb{Q}(i)$, so $\mathbb{Q}$ is a subfield of $\mathbb{Q}(i)$.
- $\mathbb{Q} \subseteq \mathbb{R}$, so $\mathbb{Q}$ is a subfield of $\mathbb{R}$.
- $\mathbb{Q}(i) \not\subseteq \mathbb{R}$, so $\mathbb{Q}(i)$ is not a subfield of $\mathbb{R}$.

Definition 4. Let K be a field and let L be an extension field of K. The *extension degree* $[L : K]$ is defined as $\dim_K(L)$, the dimension of L as a K-vector space.

Example. Let $K = \mathbb{R}$ and $L = \mathbb{C}$. Note that $\mathbb{C} = \mathbb{R}(i) = \{a + bi | a, b \in \mathbb{R}\}$, so that $\mathbb{C}$ is a 2-dimensional $\mathbb{R}$-vector space. You can visualise this by thinking of the complex plane:



So $[\mathbb{C} : \mathbb{R}] = \dim_{\mathbb{R}}(\mathbb{C}) = 2$.

Warning! The extension degree is not always finite!

Definition 5. Let K be a field. The *characteristic* of K, denoted $\mathrm{char}(K)$, is the smallest positive integer m such that $m \cdot 1 = 0$. If no such integer exists, we define $\mathrm{char}(K) = 0$.

Examples.

- $\mathrm{char}(\mathbb{Q}) = 0$.
- $\mathrm{char}(\mathbb{Z}/p\mathbb{Z}) = p$.

Lemma 1. The characteristic of a field is 0 or a prime.

Proof. Suppose that $\text{char}(K) = a \cdot b = n$, where $a, b \in \mathbb{Z}$ and $1 < a, b < n$. Then

$$\begin{aligned} 0 &= (a \cdot b) \cdot 1 \\ &= ((a \cdot 1) \cdot b) \cdot 1 && \text{by (G3)} \\ &= (a \cdot 1) \cdot (b \cdot 1) && \text{by (G2)} \\ &= a \cdot b. && \text{by (G3)} \end{aligned}$$

Then Remark 1 implies that a or b is 0, which contradicts the minimality of n. $\square$

Lemma 2. A finite field K has characteristic p for some prime p.

Proof. (F1) and (G1) imply that for all $i \in \mathbb{Z}_{>0}$, we have that $i = i \cdot 1 = 1 + \cdots 1 \in K$. Then as K is finite, there must exist $i, j \in \mathbb{Z}_{>0}$ with $i > j$ such that $i \cdot 1 = j \cdot 1$, which implies by (F3) that $(i - j) \cdot 1 = 0$. Therefore, the characteristic of K is a non-zero divisor of $(i - j)$, hence is prime by Lemma 1. $\square$

We are starting to get a handle on what a finite field can look like. Let's now assume that we find a finite field L somewhere in nature. What do we already know about it? We know:

Facts 1.

1. $0 \in L$, by (F1) and (G3).
2. $1 \in L$, by (F2) and (G3).
3. $0 \neq 1$, by definition of L^* and (F2).
4. $1, 1 + 1, 1 + 1 + 1, ... \in L$ by (F1) and (G1).
5. there exists a prime p such that $p \cdot 1 = 0$ by Lemma 2.

We also know a subfield of L: for all $a \in \mathbb{Z}$ such that $0 \leq a < p$ and for all $k, k' \in \mathbb{Z}$, we know that inside L,

$$n = a + kp = a + k'p = n',$$

which looks like $n \equiv n' \mod p$. Mathematicians say in this instance that there is a subfield of L that is 'isomorphic' to $\mathbb{Z}/p\mathbb{Z}$.

Definition 6. Let L be a field.The smallest subfield contained in L is called the *prime field* of L.

Lemma 3. Let L be a finite field of characteristic p. The prime field of L is isomorphic to $\mathbb{Z}/p\mathbb{Z}$.

Proof. There is a subfield of L that is isomorphic to $\mathbb{Z}/p\mathbb{Z}$, and all finite fields have prime characteristic by Lemma 2. $\square$

From now on, we will identify the prime of L as above with $\mathbb{Z}/p\mathbb{Z}$. That is, we will write 'prime field = $\mathbb{Z}/p\mathbb{Z}$'. So now we can add a fact to our list from Facts 1:

6. The prime field of L is $\mathbb{Z}/p\mathbb{Z}$.

Now we try to write down some elements of L that are not in $\mathbb{Z}/p\mathbb{Z}$. Recall from Definition 3 that L is an extension field of $\mathbb{Z}/p\mathbb{Z}$ and hence is a $\mathbb{Z}/p\mathbb{Z}$-vector space. Define

$$n := \dim_{\mathbb{Z}/p\mathbb{Z}}(L) = [L : \mathbb{Z}/p\mathbb{Z}].$$

This means that there exists a $\mathbb{Z}/p\mathbb{Z}$-basis $\{\alpha_1, \dots, \alpha_n\}$ of L. (Recall: a $\mathbb{Z}/p\mathbb{Z}$-basis of L is a set $\{\alpha_1, \dots, \alpha_n\}$ of elements of L such that for all $y \in L$, there exist unique $y_1, \dots, y_n \in \mathbb{Z}/p\mathbb{Z}$ such that $x = \sum_{i=1}^n y_i\alpha_i$.) Now we have a representation of all the elements of L, let's add this to our list Facts 1:

7. Let $\{\alpha_1, \dots, \alpha_n\}$ be a $\mathbb{Z}/p\mathbb{Z}$-basis of L. Then

$$L = \{\sum_{i=1}^n y_i\alpha_i | y_1, \dots, y_n \in \mathbb{Z}/p\mathbb{Z}\}.$$

In particular, we can see from (7) that there are p^n choices for the coefficients $y_1, \dots, y_n$ of the elements of L, so L has p^n elements, giving us another fact for our list Facts 1:

8. L has p^n elements, where $n = [L : \mathbb{Z}/p\mathbb{Z}]$.

The above can be summarised in the following lemma:

Lemma 4. Let L be a finite field. There exists a prime p and an integer $n \in \mathbb{Z}_{>0}$ such that $|L| = p^n$ and $\text{char}(L) = p$.

Definition 7. A finite field of size p^n is written as

$$\mathbb{F}_{p^n}$$

or

$$GF(p^n).$$

In particular, there do not exist finite fields which have size not a power of a prime! So no finite fields of size 6,10,14,15,...

Remember from (F1) and (F2) that we should be able to add and multiply in our field L. Let's take the representation of elements given in (7). Adding is easy:

$$x + y = \sum_{i=1}^n x_i\alpha_i + \sum_{i=1}^n y_i\alpha_i = \sum_{i=1}^n (x_i + y_i)\alpha_i.$$

However to multiply, we need to know how to represent $\alpha_i\alpha_j$ in the right form. Let's investigate the 'multiplicative structure'. Recall from (F2) that $L^* = L - \{0\}$ is a multiplicative group. Recall also from group theory that if G is a finite (multiplicative) group, and $m = |G|$, then for all $g \in G$, $g^m = 1$. Now L^* is a finite multiplicative group, and

$$|L^*| = |L - \{0\}| = |L| - 1 = p^n - 1.$$

Hence, for all $y \in L^*$, $y^{p^n-1} = 1$.

Remark 2. If there exists some $y \in L^*$ such that for all $t \in \mathbb{Z}$ with $0 < t < p^n - 1$, $y^t \neq 1$, then

$$L^* = \{y, y^2, \ldots, y^{p^n-1}\}.$$

Proof. Suppose for a contradiction that for some $i, j \in \mathbb{Z}$ with $0 < i < j \leq p^n - 1$ that $y^i = y^j$. Then $y^{i-j} = 1$, so $i - j = p^n - 1$, which is a contradiction. □

If we are lucky and we can find a $y \in L^*$ as in the above remark, then we say that L^* is *cyclic*, or *generated by one element* (where that element is y). In this case, we write

$$L^* = \langle y \rangle.$$

Definition 8. Let $y \in L^*$. The minimal $t \in \mathbb{Z}_{>0}$ such that $y^t = 1$ is called the *order* of y, written as $t = \mathrm{ord}(y)$.

Let's look for an element in L^* of order $p^n - 1$, since if one exists then we can deduce so much about the structure! Observe that we can create elements of high order from elements of lower order:

Suppose that $x, y \in L^*$, that $\mathrm{ord}(x) = k$, and that $\mathrm{ord}(y) = \ell$. Then by definition of order, we have that $x^k = y^\ell = 1$, so that in particular

$$(xy)^{k\ell} = (x^k)^\ell (y^\ell)^k = 1.$$

So

$$\mathrm{ord}(xy) | k\ell.$$

Lemma 5. Let x and y be above. Then

$$\mathrm{ord}(xy) = \mathrm{lcm}(k, \ell).$$

Proof. Exercise. □

Lemma 6. The smallest integer $e > 0$ such that for all $y \in L^*$ we have $x^e = 1$ is $p^n - 1$.

Proof. Assume that there exists an exponent $e \leq p^n - 1$ such that for every $y \in L^*$ we have $x^e = 1$. Then $x^e - 1$ has a root at every $a \in L^*$. In particular, we get that

$$\prod_{a \in L^*} (x - a) | x^e - 1.$$

But the degree of the polynomial $\prod_{a \in L^*}(x - a)$ is $p^n - 1$, so the degree of $x^e - 1$ is at least $p^n - 1$. Hence $e \geq p^n - 1$. □

Lemma 7. There exists $g \in L^*$ such that $\mathrm{ord}(x) = p^n - 1$.

Proof. Exercise. Hint: factorise $p^n - 1$ into primes as $p^n - 1 = q_1^{m_1} \cdots q_r^{m_r}$, use Lemma 5 and Lemma 6, and use that for every $y \in L^*$, we have that $\mathrm{ord}(y) | p^n - 1$. □

Corollary 1. *Let L be a finite field. The multiplicative group $L^* = L - \{0\}$ is cyclic.*

Definition 9. Let L be a finite field. A generator g of L^* (so that $L^* = \{g, g^2, \dots, g^{p^n-1}\}$) is called a *primitive element*.

This gives us a new way of representing elements of L! So let's add that to our list Facts 1:

8. There exists a $g \in L^*$ such that
$$L = \{0, g, g^2, \dots, g^{p^n-1}\}.$$

Remember that we want to add and multiply elements for (F1) and (F2), but in the vector space representation it was hard to multiply. In this representation, multiplying is easy:

$$g^i \cdot g^j = g^{i+j} \quad g^i \cdot 0 = 0 \quad 0 \cdot 0 = 0.$$

(Here you should take the exponent mod p^n).

What about adding? Let's try to add 2 non-zero elements: suppose that $0 < i \leq j < p^n$. Then
$$g^i + g^j = g^i(1 + g^{j-i}).$$
As $1 + g^{j-i} \in L$, we know that either $g^{j-i} = -1$ or there exists some $k \in \mathbb{Z}$ such that $g^k = 1 + g^{j-i}$. Now as $(-1)^2 = 1 = g^{p^n-1}$, we have that $g^{(p^n-1)/2} = -1$. So if $g^{j-i} = -1$ then $j - i = (p^n - 1)/2$. Hence in this case we can add. So suppose that $j \neq i + (p^n - 1/2$. Then there exists some $k \in \mathbb{Z}$ such that $g^k = 1 + g^{j-i}$. There exists an algorithm to compute k, Zech's algorithm, and this is implemented in most computer algebra systems. But it is inefficient! What else can we do?

This is all a lot of work. We should check that finite fields other than $\mathbb{Z}/p\mathbb{Z}$ even exist to make sure that our efforts are not in vain. The smallest example we can try that is not of the form $\mathbb{Z}/p\mathbb{Z}$ is a finite field of 4 elements, or $\mathbb{F}_4$. If we check our list Facts 1 we see that $\mathbb{F}_4$ should be a 2 dimensional vector space over $\mathbb{Z}/2\mathbb{Z}$, and hence there exists a $\mathbb{Z}/2\mathbb{Z}$-basis $\{1, \alpha\}$ of $\mathbb{F}_4$. That is, to construct a field $\mathbb{F}_4$ we must formally choose an α such that

$$\begin{aligned} \mathbb{F}_4 &= \mathbb{Z}/2\mathbb{Z} + \alpha\mathbb{Z}/2\mathbb{Z} \\ &= \{0, 1, \alpha, 1 + \alpha\}. \end{aligned}$$

Let's check if we can add and multiply so that (F1) and (F2) are satisfied. Using the vector space structure, we can draw the group addition table for $\mathbb{F}_4$:

$+$	0	1	α	$1+\alpha$
0	0	1	α	$1+\alpha$
1	1	0	$1+\alpha$	α
α	α	$1+\alpha$	0	1
$1+\alpha$	$1+\alpha$	α	1	0

The multiplication table for $\mathbb{F}_4^*$ (below) is a bit more work: we first fill in the black entries, and then we show that $\alpha^2 = \alpha + 1$ using that in a group multiplication table each element occurs exactly once. (If $\alpha^2 = 1$ then $\alpha(\alpha+1) = 1 + \alpha$ giving $1 + \alpha$ twice in the last column, a contradiction.)

$\cdot$	1	α	$1+\alpha$
1	1	α	$1+\alpha$
α	α	$1+\alpha$	1
$1+\alpha$	$1+\alpha$	1	α

These tables show that it is possible to define addition and multiplicative, and checking the other axioms is left as an exercise. So there exists a field with 4 elements! Let's look at the next simplest case: a field with $8 = 2^3$ elements, or $\mathbb{F}_8$. Checking our list Facts 1, we see that $\mathbb{F}_8$ (if it exists) is a 3-dimensional vector space over $\mathbb{Z}/2\mathbb{Z}$, so let's choose a basis $\{1, \alpha, \beta\}$. Then

$$\mathbb{F}_8 = \{0, 1, \alpha, \beta, 1 + \alpha, 1 + \beta, \alpha + \beta, 1 + \alpha + \beta\}.$$

Addition will work exactly as before using the vector space representation - but it's less clear that we will be able to multiply. So let's try to create a multiplication table. Again, we can easily fill in the black entries of of the multiplication table for $\mathbb{F}_8^*$ (below) but we get stuck when we get to α^2. As before, we can't take $\alpha^2 = 1$ or α, and if we choose $\alpha^2 = \alpha + 1$ then we'll get the same field as before, so not $\mathbb{F}_8$. As we have some freedom in choosing the basis, there is more than one choice for α^2, so we try

$$\alpha^2 = \beta. \tag{1}$$

With this we can fill in the red entries, but again we get stuck at $\alpha\beta$. As elements cannot appear more than once in any given row or column, we know from the black and red entries that $\alpha\beta \neq \alpha, \beta, \alpha + \beta$. Also, if $\alpha\beta = 1$ then the second entry in the final column is $\alpha(1 + \alpha + \beta) = 1 + \alpha + \beta$, which occurs already as a black entry in the final column, given a contradiction. Similarly, if $\alpha\beta \neq 1 + \alpha + \beta$, then $\alpha(1 + \beta) = 1 + \beta$ which leads to a double entry in the 5th column. So we are left with $\alpha\beta = 1 + \alpha$ or $1 + \beta$, and we try

$$\alpha\beta = 1 + \alpha. \tag{2}$$

With this we can fill in the blue entries, and in fact arguining by contradiction as above, you can show that β^2 is uniquely defined as $\alpha + \beta$, giving the green entries.

$\cdot$	1	α	β	$1+\alpha$	$1+\beta$	$\alpha+\beta$	$1+\alpha+\beta$
1	1	α	β	$1+\alpha$	$1+\beta$	$\alpha+\beta$	$1+\alpha+\beta$
α	α	β	$1+\alpha$	$\alpha+\beta$	1	$1+\alpha+\beta$	$1+\beta$
β	β	$1+\alpha$	$\alpha+\beta$	$1+\alpha+\beta$	α	$1+\beta$	1
$1+\alpha$	$1+\alpha$	$\alpha+\beta$	$1+\alpha+\beta$	$1+\beta$	β	1	α
$1+\beta$	$1+\beta$	1	α	β	$1+\alpha+\beta$	$1+\alpha$	$\alpha+\beta$
$\alpha+\beta$	$\alpha+\beta$	$1+\alpha+\beta$	$1+\beta$	1	$1+\alpha$	α	β
$1+\alpha+\beta$	$1+\alpha+\beta$	$1+\beta$	1	α	$\alpha+\beta$	β	$1+\alpha$

Everything from this point on was not covered in the lecture on 19/09/2017, but is included here to help with the exercises.

It seems as if we will be able construct many finite fields by hand, but this is a lot of work! How can we write down what we are doing when we fix equations like (1) and (2) in a more general way?

Definition 10. If K is a field, then the *polynomial ring* $K[x]$ is defined to be

$$K[x] = \left\{ \sum_{i=1}^{n} a_i x^i | n \in \mathbb{Z}_{\geq 1},\, a_i \in K \right\}.$$

For $f(x) = \sum_{i=1}^{n} a_i x^i \in K[x]$ with $a_n \neq 0$, we say that a_n is the *leading coefficient* of $f(x)$, that $a_n x^n$ is the *leading term* of $f(x)$, and we define the *degree* of $f(x)$ to be n, written $\deg(f)$. If a_n, then we say that $f(x)$ is *monic*.

Definition 11. We say that a polynomial $f(x) \in K[x]$ is *irreducible* if $\deg(f) \geq 1$ and it cannot be written as the product of polynomials of lower degree over the same field. Otherwise we say that $f(x)$ is *reducible*.

Examples.

- $x^2 - 1 = (x-1)(x+1)$ is reducible in $\mathbb{Q}[x]$.
- $x^2 + 1$ is irreducible in $\mathbb{R}[x]$, but not in $\mathbb{C}[x]$.
- $x^4 + 2x^2 + 1 = (x^2+1)^2$ is reducible in $\mathbb{R}[x]$.
- $f(x) = x^3 + 6x^2 + 4$ is irreducible in $\mathbb{Z}/7\mathbb{Z}$, as there are no $a \in \mathbb{Z}/7\mathbb{Z}$ such that $f(a) = 0$, and a degree 3 polynomial is irreducible if and only if it has no roots. (Do you see why?)

How does this help us generalise multiplication in finite fields? Recall that with $\mathbb{F}_8^*$ our definition of multiplication was dependant on (1) and (2), which were $\alpha^2 = \beta$ and $\alpha\beta = 1 + \alpha$, which together give

$$\alpha^3 + \alpha + 1 = 0.$$

(Remember that our coefficients are all mod 2 so sign doesn't matter.) That is, if the basis element α is a root of the polynomial

$$f(x) = x^3 + x + 1 \in \mathbb{F}_2[x],$$

then $\{1, \alpha, \alpha^2\}$ is a $\mathbb{Z}/2\mathbb{Z}$-basis of $\mathbb{F}_8$. You should think of calculating in $\mathbb{F}_8$ as calculating 'mod $\alpha^3 + \alpha + 1$', in the following way:

$$\mathbb{F}_8 = (\mathbb{Z}/2\mathbb{Z})[x]/(f(x)(\mathbb{Z}/2\mathbb{Z})[x]) = \{\sum_{i=0}^{n-1} a_i x^i \bmod f(x) | a_i \in \mathbb{Z}/2\mathbb{Z}\},$$

and we define addition and multiplication in $\mathbb{F}_8$ as addition and multiplication in $(\mathbb{Z}/2\mathbb{Z})[x]$ followed by reduction mod $f(x)$.

As $f(x)$ is a degree 3 polynomial we can easily check if it's irreducible: if $f(x)$ is reducible then at least one factor must be linear, and hence either $f(0)$ or $f(1) = 0$. But $f(0) = f(1) = 1 \bmod 2$ so $f(x)$ is irreducible. In fact, we would have run into trouble in our multiplication table is $f(x)$ had been reducible (it would be similar to trying to compute modulo a non-prime in $\mathbb{Z}$).

With the above it is now a natural next step to see how to define addition and multiplication in $\mathbb{F}_{p^n}$: let $f(x) \in (\mathbb{Z}/p\mathbb{Z})[x]$ be a monic irreducible polynomial of degree n. Then we write $\mathbb{F}_{p^n}$ as

$$\mathbb{F}_{p^n} = (\mathbb{Z}/p\mathbb{Z})[x]/(f(x)(\mathbb{Z}/p\mathbb{Z})[x]) = \{\sum_{i=0}^{n-1} a_i x^i \bmod f(x) | a_i \in \mathbb{Z}/p\mathbb{Z}\},$$

and we define addition and multiplication in $\mathbb{F}_{p^n}$ as addition and multiplication in $(\mathbb{Z}/p\mathbb{Z})[x]$ followed by reduction mod $f(x)$.

Example. Let's see an example of how to compute in $\mathbb{F}_8$ using this general construction. Define $f(x) = x^3 + x^2 + 1 \in (\mathbb{Z}/2\mathbb{Z})[x]$. As $\deg(f) = 3$ and $f(0) = f(1) = 1$ in $\mathbb{Z}/2\mathbb{Z}$ it is irreducible in $(\mathbb{Z}/2\mathbb{Z})[x]$, and it is clearly monic, hence

$$\mathbb{F}_{2^3} = (\mathbb{Z}/2\mathbb{Z})[x]/(f(x)(\mathbb{Z}/2\mathbb{Z})[x]).$$

Now $\overline{x^2+1} \in (\mathbb{Z}/2\mathbb{Z})[x]/(f(x)(\mathbb{Z}/2\mathbb{Z})[x])$, where $\bar{\cdot}$ denotes reduction mod $f(x)$, so what is $\overline{(x^2+1)}^{-1}$?

For any element g of $(\mathbb{Z}/2\mathbb{Z})[x]/(f(x)(\mathbb{Z}/2\mathbb{Z})[x])$, there exist $a, b, c \in \mathbb{Z}/2\mathbb{Z}$ such that $g = \overline{ax^2 + bx + c}$, and if $g = \overline{(x^2+1)}^{-1}$, then

$$\begin{aligned}
&(x^2+1)(ax^2+bx+c) \equiv 1 \bmod f(x)\\
\Rightarrow &(b+c)x^2 + (a+b)x + a + b + c \equiv 1 \bmod f(x)\\
\Rightarrow &a + b + c \equiv 1 \bmod 2, \text{ and } a \equiv b \equiv c \bmod 2\\
\Rightarrow &\overline{(x^2+1)}^{-1} = \overline{x^2 + x + 1}.
\end{aligned}$$

The only ingredient that we are missing from our nice representation of finite fields is how to check if a polynomial is irreducible. In all the examples we saw so far the polynomial had small enough degree that if it was reducible then it had a root, but for polynomials of degree ≥ 4 this will no longer work! For this we have the *Robin test:*

Robin Test. *Let $\mathbb{F}_q$ be a finite field with $q = p^r$ elements for p a prime and $r \in \mathbb{Z}_{>0}$, and let $f(x) \in \mathbb{F}_q[x]$ be a degree n polynomial. Then $f(x)$ is irreducible if and only if*

(i) $f(x)|(x^{q^n} - x)$ in $\mathbb{F}_q[x]$ and

(ii) for all $d|n$ such that $d \neq n$, $\gcd(f(x), x^{q^d} - x) = 1$.

Notes on the Robin test:

1. It is enough to check for prime divisors d of n.
2. Reductions mod $f(x)$ are particularly efficient if $f(x)$ is a binomial (i.e. $f(x) = x^n - a$ for some a).

Example. We saw above that $x^3 + x^2 + 1 \in \mathbb{F}_2[x]$ is irreducible, so let's check that it satisfies (i) and (ii) of the Robin test.

- $x^{2^3} + x = x(x^7+1) = x(x^3+x^2+1)(x^4+x^3+x^2+1)$, so $(x^3+x^2+1)|(x^{2^3}-x)$ in $\mathbb{F}_2[x]$.
- $\{d|3|d \neq 3\} = \{1\}$, so it suffices to prove that $\gcd((x^2-x),(x^3+x^2+1)) = 1$. But $x^2 - x = x(x-1)$ neither x nor $x-1$ divide x^3+x^2+1 as neither 0 or 1 are roots of x^3+x^2+1. Hence $\gcd((x^2-x),(x^3+x^2+1)) = 1$.

Now by the Robin test, $x^3 + x^2 + 1$ is irreducible in $\mathbb{F}_2[x]$.

Example. Let's look at a slightly bigger example: $f(x) = x^5+x^4+x^3+x^2+1 \in \mathbb{F}_2[x]$. Here $n = 5$ and $q = 2$. Now

$$\begin{aligned} x^{2^5} - x = x(x^5+x^4+x^3+x^2+1)(&x^{26}+x^{25}+x^{22}+x^{19}+x^{18}+x^{17}+x^{16} \\ &+x^{15}+x^{13}+x^{12}+x^{11}+x^7+x^5 \\ &+x^3+x^2+1), \end{aligned}$$

so $f(x)|(x^{2^5}-x)$ and hence (i) of the Robin test in satisfied. As $n = 5$ is prime, for (ii) it suffices to show that $\gcd(f(x), x^2-x) = 1$. As $x^2 - x = x(x-1)$ and neither 0 nor 1 are roots of $f(x)$ this holds. Hence $f(x)$ is irreducible in $\mathbb{F}_2[x]$.