Factoring Polynomials over Finite Fields

Ting Gong, Nick VanderLaan, and Nikhil Shankar

March 17, 2018

Abstract

Let $f(x) = x^n + c_{n-1}x^{n-1} + \dots c_1x + c_0$ be a monic polynomial function with $c_i \in \mathbb{Z}/p\mathbb{Z}$. Such a function can sometimes be factored as follows: $f(x) = f_1(x) \cdot f_2(x) \cdot \ldots \cdot f_k(x)$ where the orders of the f_i give a partition of n. We will explore such a factorization is possible.

1 Introduction

By the Fundamental Theorem of Algebra, every non-constant, complex polynomial has a root in $\mathbb{C}$, and therefore can be written as the product of linear and constant terms. Over $\mathbb{R}$, not every polynomial has a root, the prototypical example being $x^2 + 1$. However, we can write any real polynomial as the product of linear and quadratic factors, so every polynomial of degree ≥ 3 is reducible. Over $\mathbb{Q}$ this is no longer the case, as $x^4 + 1$ admits neither linear nor quadratic factors. This paper concerns itself with understanding factoring over finite fields, namely the classification of irreducible, degree 2, monic polynomials.

1.1 Notation and Definitions

1. We denote $\mathbb{F}_p$ as the finite field $\mathbb{Z}/p\mathbb{Z}$ where p is a prime number.
2. $\mathbb{F}_p[x]$ is the polynomial ring over field $\mathbb{F}_p$.
3. One quadratic polynomial in $\mathbb{F}_p[x]$ can be written as $f(x) = x^2 + c_1x + c_0$ where $c_0, c_1 \in \mathbb{F}_p$.

Definition 1. A polynomial $q \in \mathbb{F}_p[x]$ is said to be **reducible** if we can write $q = fg$ where $f, g \in \mathbb{F}_p[x]$ non-constant polynomials. If no such factorization exists, q is said to be **irreducible**.

We claim that when this factorization exists, it is unique. [1]

1.2 Polynomials and Polynomial Functions

It is important we define and agree on the definition of a polynomial. For the purposes of this paper, a (univariate) polynomial $r \in \mathbb{F}_p[x]$ is given by

$$\sum_{k=0}^{n} a_k x^k$$

where n is the degree of r, $a_k \in \mathbb{F}_p \ \forall k$ and x is a formal symbol. Given two polynomials like r and s below:

$$r = \sum_{k=0}^{n} a_k x^k, \qquad s = \sum_{k=0}^{m} b_k x^k$$

We say that $r = s \iff n = m$ and $a_k = b_k \ \forall 0 \leq k \leq n$.

This contrasts with the notion of a polynomial function

$$\begin{aligned} f : \mathbb{F}_p &\to \mathbb{F}_p \\ x &\mapsto \sum_{k=0}^{n} a_k x^k. \end{aligned}$$

To thoroughly convince the reader that these two notions are not equivalent, consider the polynomials $u = x^p - x$ and $v = 0$. Regarded as polynomials, $u \neq v$ as the degree of u is p, whereas the degree of v is 0. However as polynomial functions, $u(y) = y^p - y = 0 \ \forall y \in \mathbb{F}_p$ because $y^p \equiv y \pmod{p} \forall y \in \mathbb{F}_p$. For now, we only consider polynomials. Again all polynomials will be considered monic unless clearly stated otherwise.

1.3 Time estimates

It is reasonable to believe that different factoring processes will have different speeds. We would like a way to record and compare the efficiency of different algorithms. To do this, we adopt a "Big-O" notation common in number theory and computer science.

Definition. given ordered sets A and B, and functions $f, g : A \to B$, we say that $f \in \mathcal{O}(g)$ if $\forall m \in B \ \exists \ x'$ such that $|f(x)| \leq M|g(x)| \ \forall x > x'$.

Loosely, f is smaller than g for large x, and we can ignore leading constants as well as smaller order terms. For example, if $e, f, g, h : \mathbb{R} \to \mathbb{R}, e(x) = x + 37, f(x) = x^2 + x + 1, g(x) = x^2, h(x) = x^3$, we have the following:

function	$\in \mathcal{O}(e)$?	$\in \mathcal{O}(f)$?	$\in \mathcal{O}(g)$?	$\in \mathcal{O}(h)$?
e	True	True	True	True
f	False	True	True	True
g	False	True	True	True
h	False	False	False	False

2 Factoring Quadratic Polynomials mod p

Lemma. *If $r \in \mathbb{F}_p$ is a root of a quadratic polynomial $f(x)$, i.e, $f(r) = 0$, then f can be written as $f = (x - r) \cdot g$ where g is a (quotient) polynomial.*

Proof. Suppose

$$f(r) = 0 = r^2 + c_1 r + c_0$$

Then we can see $c_0 = -r^2 - c_1 r$ which implies:

$$\begin{aligned} x^2 + c_1 x + c_0 &= x^2 + c_1 x - r^2 - c_1 r \\ &= (x + r)(x - r) + c_1(x - r) = (x - r)(x + r + c_1) = 0 \end{aligned}$$

Note we have also shown that $g = (x + r + c_1)$. □

Theorem. *A quadratic polynomial $f(x)$ over $\mathbb{F}_p$ is reducible if and only if it has a root in $\mathbb{F}_p$.*

Proof. Using the above lemma it is clear that if the quadratic is reducible, r is a root. Further if r is a root , then the quadratic is reducible. □

Lemma. *Let $f(x) = x^2 + c_1 x + c_0$ be a polynomial in $\mathbb{F}_p[x]$. If $1 + c_1 + c_0 = p$, then $f(x)$ is reducible.*

Proof. By the above theorem it suffices to show that when $1 + c_1 + c_0 = p - 1$, $f(x)$ has a root in $\mathbb{F}_p$.
Set $f(x) = x^2 + c_1 x + c_0 = 0$, and substitute c_1 by $c_1 = p - 1 - c_0$. Then

$$\begin{aligned} x^2 + (p - 1 - c_0)x + c_0 = 0 \\ \Rightarrow x^2 + (1 + c_0)x + c_0 = 0 \\ \Rightarrow x = -1 \equiv p - 1 \pmod p \end{aligned}$$

Since for arbitrary c_0, c_1 such that $1 + c_1 + c_0 = p$, we find a root for $f(x)$, i.e, $x = p-1$, we can conclude that $f(x)$ is reducible whenever $1+c_1+c_0 = p-1$. □

3 Counting Irreducible Polynomials

3.1 Ratio of Quadratic Reducible to Irreducible Polynomials

Note that given $\mathbb{F}_p$, there are at maximum p^2 quadratic functions with coefficients in $\mathbb{F}_p$. Below are some interesting results regarding the ratio of reducible polynomials to irreducible polynomials computed using *Sage*, a free, open-source computer algebra system. [2]

p	2	3	5	7	11 ...	37
Reducible : Irreducible	1/3	1/2	2/3	3/4	5/6...	18/19

Table 1: If we ignore the fact that some polynomials may be duplicates, we seem to be approaching a ratio of 1:1 between reducible and irreducible polynomials as p grows large.

3.2 Counting Formulas

We have determined formulas for counting the number of quadratic and cubic irreducible polynomials over a given $\mathbb{F}_p$.

Lemma 1. *The number of irreducible, monic, quadratic polynomials in $\mathbb{F}_p[x]$ is given by:*

$$p^2 - \frac{p(p+1)}{2} = \frac{1}{2}(p^2 - p)$$

Proof. We begin by noting there are p^2 monic, quadratic polynomials in $\mathbb{F}_p$. To see this, we note that a monic polynomial is of the form

$$x^2 + \sum_{n=0}^{1} a_n x^n$$

and so we only get to pick two a_n's per polynomial, and $a_n \in \mathbb{F}_p$, so there are at most p^2 choices for a_n. We now count the linear polynomials in $\mathbb{F}_p[x]$. They are of the form $x+\alpha$ where again, $\alpha \in \mathbb{F}_p$, so there are at most p linear polynomials. Every reducible quadratic polynomial splits as the product of two linear factors. Thus the number of reducible quadratics is equal to the number of combinations of 2 linear factors. So we assign to each linear polynomial a label in the set of symbols (not numbers) $\{1, \dots, p\}$, and count pairs (which don't consider order as multiplication is commutative over a field) of two as follows:

$$\begin{array}{ccccccc}
11 & 12 & 13 & \dots & & 1(p-1) & 1p \\
22 & 23 & 24 & \dots & 2(p-1) & 2p & \\
33 & 34 & 35 & & 3p & & \\
\vdots & & & & & & \\
pp & & & & & &
\end{array}$$

which is equivalent to

$$\sum_{n=1}^{p} p = \frac{p(p+1)}{2}.$$

And since a polynomial is either reducible or irreducible (but not both), we have that the number of irreducibles is

$$p^2 - \frac{p(p+1)}{2}$$

as desired. □

Lemma 2. *The number of irreducible, monic, cubic polynomials in $\mathbb{F}_p[x]$ is given by:*

$$p^3 - \left[p^2 + \binom{p}{3} + p\left(p^2 - \frac{p(p+1)}{2}\right)\right] = \frac{1}{3}(p^3 - p)$$

Proof. As in Lemma 1, we begin by noting the number of monic, cubic polynomials in $\mathbb{F}_p[x] = p^3$. Let $a \in \mathbb{F}_p[x]$. Then there are three cases:

1. a is irreducible.

2. a splits as the product of three linear factors.

3. a splits as the product of a linear factor and an irreducible quadratic.

The number of irreducible monic, cubic polynomials will thus be p^3 minus the number of reducibles. We begin by counting the number of polynomials which can be written as the product of a linear factor and an irreducible quadratic. We recall that in Lemma 1, the number of irreducible quadratics in $\mathbb{F}_p[x]$ is

$$p^2 - \frac{p(p+1)}{2}$$

and the number of linear monic polynomials is simply p. Thus we count the number of ways to choose one linear factor and one irreducible quadratic, of which there are

$$p\left(p^2 - \frac{p(p+1)}{2}\right)$$

many.

Finally we count the number of polynomials that can be written as the product of three linear factors. Again labeling each linear polynomial with a label in the set of symbols (not numbers) $\{1, \ldots, p\}$, there are $\binom{p}{3}$ ways of picking three distinct linear factors. There are p many ways to pick something of the form a^3, where $a \in \{1, \ldots p\}$, and there are $p(p-1)$ many ways to pick something of the form a^2b with $a \neq b$, so in total there are

$$p + p(p-1) + p\left(p^2 - \frac{p(p+1)}{2}\right) = p^2 + \binom{p}{3} + p\left(p^2 - \frac{p(p+1)}{2}\right)$$

many reducibles, and therefore

$$p^3 - \left[p^2 + \binom{p}{3} + p\left(p^2 - \frac{p(p+1)}{2}\right)\right]$$

many irreducible, monic, cubic polynomials in $\mathbb{F}_p[x]$. □

Further computation in Sage [2] seems to suggest that for biquadratic polynomials, the number of irreducibles is

$$\frac{1}{4}(p^4 - p^2)$$

Which looks like a pattern. Indeed we conjecture the number of irreducible, degree 5 polynomials in $\mathbb{F}_p[x]$ is

$$\frac{1}{5}(p^5 - p)$$

but we also conjecture the number of irreducible, degree 6 polynomials over $\mathbb{F} - p[x]$ is

$$\frac{1}{6}(p^6 - p^3 - p^2 + p)$$

not following any of the earlier patterns.

3.2.1 Counting Polynomial Functions

Note that since there is a distinction between polynomials and polynomial functions, these counting formulas may double count some polynomial functions, even if they give the exact number of irreducible monic polynomials. Based on computational evidence we currently conjecture that the counting formulas do not double count any functions.

4 Approaches to Factoring

Ideally we would have a constant time algorithm ($\mathcal{O}(1)$) algorithm for determining whether a polynomial of degree n splits over $\mathbb{F} - p$. What follows are a few non-constant time algorithms

Approach 1:

Lemma 3. *For a quadratic polynomial $f = x^2 + bx + c$, If $\exists x \in \mathbb{F}_p$ such that $x^2 = b^2 - 4c$ then f is reducible.*

Proof. We can embed f in $\mathbb{R}[x]$, call it $f_\mathbb{R}$, and check for roots there via the quadratic formula! We are given that

$$r = \frac{-b \pm \sqrt{b^2 - 4c}}{2}$$

is a root of $f_\mathbb{R}$. Indeed by our hypothesis we have

$$r = \frac{-b \pm x}{2}$$

and since $b, x \in \mathbb{F}_p, -b \pm x \in \mathbb{F}_p$, and $\mathbb{F}_p$ a field, thus closed under non-zero division, so we conclude $r \in \mathbb{F}_p$, and since $f_\mathbb{R}(r) = 0, f(r) = 0$. □

The glaring limitation of this approach is that it only works for quadratic polynomials. Potentially we could employ similar methodology with the cubic and biquadratic formulæ, but beyond degree 4, there is no formula for finding roots. Even in the biquadratic case, we encounter the issue of polynomials that are reducible, but do not have roots. An example of this is $p = (x^2 + x + 1)^2 \in \mathbb{F}_2[x]$.

The other shortcoming of this approach is that while it looks like an $\mathcal{O}(1)$ algorithm for determining reducibility, it is contingent on us being able to determine if $b^2 + 4c \equiv x^2 \pmod{p}$ for some $x \in \mathbb{F}_p$. At present, the best method we know of doing this is iterating through the non-zero elements of $\mathbb{F}_p$ to see if any of them squares to $b^2 - 4c$. So in reality, the above method runs in time $\mathcal{O}(p)$. We can optimize slightly by making table T of squares in $\mathbb{F}_p$ initially and then looking up whether $b^2 - 4c \in T$, reducing our runtime to an average $\mathcal{O}(\log p)$. Still this only works for quadratic (and possibly cubic polynomials).

A Related Result:

Lemma. *If $q \in \mathbb{F}_p$ has a square root in $\mathbb{F}_p$ then $\exists d \in \mathbb{F}_p$ such that $q + dp \in \mathbb{Z}$ has a square root in $\mathbb{Z}$.*

Remark. It may be easier to find square roots in $\mathbb{Z}$ than in $\mathbb{F}_p$ which could make the contrapositive of this statement useful.

Proof. Suppose we fix such a $q \in \mathbb{F}_p$, then choose a $k \in \mathbb{F}_p$ such that $k^2 = q \bmod p$. Note that in this case, a way to think about mod p is that $\exists d$ such that $k^2 = q + dp$, and since $p^2 > k^2 \in \mathbb{Z}$ it follows that $d \in \mathbb{F}_p$. □

Approach 2: Perhaps the most obvious approach, given a polynomial f of degree n, we do the following: for each $x \in \mathbb{F}_p$ if $f(x) = 0$ then f splits, else we try the next element of $\mathbb{F}_p$. This approach works only for polynomials of degree ≤ 3, as we encounter the issue of polynomials of degree 4 that are reducible, but do not have roots. An example of this is $p = (x^2 + x + 1)^2 \in \mathbb{F}_2[x]$. The runtime of this process is $\mathcal{O}(p \cdot n)$ as for each element in $\mathbb{F}_p$, we need evaluate it in n many terms of f.

Approach 3: The method of counting irreducibles gives us another way of determining whether a given polynomial q factors. We construct a look-up table of reducibles of degree equal to that of q, call it R. If $q \in R$, q is reducible, else q must be irreducible. Lookup in this table will be $\mathcal{O}(n \log p)$. We can compute this table one for a large degree, and then make use of it until we need to test a polynomial of higher degree. Table construction proceeds as follows:

1. Make a table I to hold irreducibles
2. $\forall p, q$ linear, store pq in R.
3. add all quadratic polynomials not in R to I.
4. for each pair of elements in R, add their product to R
5. for each element in $i \in I$, multiply it with each element in $r \in R$ and add each ir to R
6. for each pair of elements in I, add their product to R

7. Repeat steps 4-6 $n - 2$ times where n is the degree of the polynomial you want to lookup.

The time-complexity of constructing this table is certainly significant, but it will work for polynomials of any degree.

References

[1] Michael Artin, *Algebra*, Pearson India Education Services 2nd edition, 2015.

[2] Sage Foundation SageMath https://www.sagemath.org, 2018