# Experiments on the splitting of cyclotomic polynomials

Ferran Espuña Bertomeu

December 13, 2023

## 1 $\phi_{11}$ in $\mathbb{F}_p$

In this part I will explain the experiments I have done on the splitting of cyclotomic polynomials in fields of prime order. On the first experiment, I have computed how the polynomial $\phi_{11}(X) = X^{10} + X^9 + \cdots + X + 1$ splits over $\mathbb{F}_p$, for $p$ a prime number. I have done this for all primes $p$ less than $200,000$ (excluding 11). The goal of this experiment is to see if there is a pattern on how many irreducible factors $\phi_{11}$ has over $\mathbb{F}_p$. Excluding the prime $p = 11$, the polynomial $\phi_{11}$ is separable over $\mathbb{F}_p$ for all primes $p$, so the extension $\mathbb{F}_p(\zeta_{11}) \mid \mathbb{F}_p$ is Galois, where $\zeta_{11}$ is a primitive 11-th root of unity. Therefore, the polynomial $\phi_{11}$ splits into irreducible factors of the same degree. The only options are:

1. $\phi_{11}$ is irreducible over $\mathbb{F}_p$.
2. $\phi_{11}$ splits into two irreducible factors of degree 5 over $\mathbb{F}_p$.
3. $\phi_{11}$ splits into five irreducible factors of degree 2 over $\mathbb{F}_p$.
4. $\phi_{11}$ splits into ten irreducible factors of degree 1 over $\mathbb{F}_p$.

Note that the last case corresponds to the case where $\mathbb{F}_p(\zeta_{11}) = \mathbb{F}_p$, that is, $\mathbb{F}_p$ contains all the 11-th roots of unity. I distinguish between the cases using the Berlekamp algorithm: Every time I find a nontrivial factorization of $\phi_{11}$, I run the algorithm again on the smallest of the two factors, until I get a polynomial whose number of irreducible factors I can deduce (an irreducible one, or one of degree not dividing 10, in which case I deduce $\phi_{11}$ splits into degree 1 factors).
Initially, I wanted to just know how often each case happens, so I tallied the number of times each case happened in the following table:

| Number of irreducible factors mod p | 1 | 2 | 5 | 10 |
|---|---|---|---|---|
| Number of primes p | 7213 | 7178 | 1798 | 1794 |

There are a total of 17983 primes less than $200,000$ (excluding 11). This means that, for a random prime $p$ less than a million, the probability of each case happening is approximately:

| Number of irreducible factors mod p | 1 | 2 | 5 | 10 |
|---|---|---|---|---|
| fraction of primes p | 0.401 | 0.399 | 0.100 | 0.100 |

These fractions are very close to fractions with denominator 10, which is suspicious as $10 = 11 - 1$. This prompted me to take a look at the remainders of each prime $p$ modulo 11. Sure enough, the remainders perfectly charaterized the splitting behaviour of $\phi_{11}$ modulo each prime, for all primes less than a million. In particular:

- The first case happens if and only if $p \equiv 2, 6, 7, 8 \pmod{11}$.
- The second case happens if and only if $p \equiv 3, 4, 5, 9 \pmod{11}$.
- The third case happens if and only if $p \equiv 10 \pmod{11}$.
- The fourth case happens if and only if $p \equiv 1 \pmod{11}$.

As it turns out, the *degree* of each irreducible factor is exactly the order of $p$ modulo 11. This is not a coincidence. We can prove this the fact that the degree of each irreducible factor is the order of one of its roots (a primitive 11-th root of unity) under the Frobenius automorphism $\varphi : x \mapsto x^p$ (as we are in a finite extension of $\mathbb{F}_p$). But $1 = \varphi^k(\zeta_{11}) = \zeta_{11}^{p^k} \iff p^k \equiv 1 \pmod{11}$, so the order of $\zeta_{11}$ under $\varphi$ is exactly the order of $p$ modulo 11. Of course, this generalizes to any $q$-th cyclotomic polynomial for any prime $q$. As for the reason why the fractions coincide with the fraction of remainders modulo 11, this is explained by Dirichlet's theorem on arithmetic progressions.
Through my experiments, I have also made the following remarkable observation: the number of irreducible factors is equal to the dimension of the kernel of the relevant matrix, at least to the extent of my experiments. I have tried to prove this, but I have not been able to do so. An open question is whether this is true in general, and for arbitrary cyclotomic polynomials (or even Galois extensions?). or if it is just a coincidence.

## 2 $[T^2 + T + 1]$ in $\mathbb{F}_2[T]/(\pi)$

In this case, we have seen in class that the relevant Galois group is isomorphic to $(\mathbb{F}_2[T]/(T^2+T+1))^\times$, which is a cyclic group of order 3. The only options are therefore that the polynomial $T^2 + T + 1$ splits completely into linear factors, or it is irreducible. $\pi$ of $\mathbb{F}_2[T]$ either splits completely into linear factors (whenever $\pi \equiv 1 \pmod{T^2 + T + 1}$), or it is irreducible (whenever $\pi \equiv 1$ or $T \pmod{T^2 + T + 1}$). We can generate primes of $\mathbb{F}_2[T]$ by running the Berlekamp algorithm on polynomials of degree up to 16 and seeing which are irreducible. Then we can compile statistics on each case:

| $\pi \pmod{M}$ | 1 | $T$ | $T+1$ |
|---|---|---|---|
| Number of polynomials | 2929 | 2935 | 2935 |

We see that the number of polynomials in each case is very close to $\frac{1}{3}$ of the total number of polynomials. I hypotesize that this is actually the case when we make our maximum degree go to infinity. In that case, the polynomial splits into linear factors if and only if $\pi \equiv 1 \pmod{T^2 + T + 1}$, that is, one third of the time. Meanwhile, $\pi$ is irreducible if and only if $\pi \equiv 1$ or $T \pmod{T^2 + T + 1}$, that is, two thirds of the time.