Math 542 HW7

Hongtao Zhang

1 Factorization of Cyclotomic Polynomials

Let l be a prime and let $\Phi_l(x) = \frac{x^l-1}{x-1} = x^{l-1} + x^{l-2} ... + x + 1 \in \mathbb{Z}[x]$ be the l^{th} cyclotomic polynomial, which is irreducible in $\mathbb{Z}[x]$. This exercise determines the factorization of $\Phi_{l(x)}$ modulo p for any prime p. Let ζ denote any fixed primitive l^{th} root of unity.

1.1

Show that $p = l \Rightarrow \Phi_l(x) = (x-1)^{l-1} \in \mathbb{F}_{l[x]}$

Solution 1.1.1

$$(x-1)^{l-1} = \sum_{i=0}^{l-1} \binom{l-1}{i} x^i (-1)^{l-1-i}$$

Consider each binomial coefficient $\binom{l-1}{i}$ modulo l. Since l is prime, $(l-1)! \equiv -1 \bmod n$.

$$\binom{l-1}{i} = \frac{(l-1)!}{(l-1-i)!i!}$$

$$\Leftrightarrow \binom{l-1}{i}(l-1-i)!i! \equiv (l-1)! \equiv -1 \bmod l \quad \text{(Wilson Theorem)}$$

$$\Leftrightarrow \binom{l-1}{i} \equiv -\frac{1}{(l-1-i)!i!} \bmod l$$

1.2

Suppose $p \neq l$ and let f denote the order of $p \bmod l$, i.e. f is the smallest power of p with $p^f \equiv 1 \bmod l$. Use the fact that $\mathbb{F}_{p^n}^\times$ is a cyclic group to show that $n = f$ is the smallest power p^n of p with $\zeta \in \mathbb{F}_{p^n}$. Conclude that the minimal polynomial of ζ over $\mathbb{F}_p$ has degree f.

Solution 1.2.1

Since $\mathbb{F}_{p^n}^\times$ is a cyclic group, and ζ is a l-th primitive root of unity, for ζ to be in $\mathbb{F}_p^n$, we must have some element that has order l. Therefore $n = f$ is the smallest power of p^n of p with $\zeta \in \mathbb{F}_p^n$ by construction.

Solution 1.2.2

Because we have the minimum extension of ζ to be in $\mathbb{F}_p^n$, which is a degree n extension, the minimal polynomial of ζ over $\mathbb{F}_p$ has degree $n = f$.

1.3

Show that $\mathbb{F}_p(\zeta) = \mathbb{F}_p(\zeta^a)$ for any integer a not divisible by l. [Hint:]

Solution 1.3.1

One direction, it suffices to check that ζ^a can be generated by ζ, which is obvious.

The other direction suffices to check that ζ can be generated by ζ^a, which follows from the hint that $\zeta = (\zeta^a)^b$ where b is the multiplicative inverse of $a \bmod l$.

Conclude using (Section 1.2) that, in $\mathbb{F}_p[x]$, $\Phi_l(x)$ is the product of $\frac{l-1}{f}$ distinct irreducible polynomials of degree f.

Solution 1.3.2

Since all primitive roots of unity have f-degree minimal polynomial, and all other roots of unity are generated by primitive roots of unity, we have that $\Phi_{l(x)}$ is the product of $\frac{l-1}{f}$ distinct irreducible polynomials of degree f.

1.4

In particular, prove that, viewed in $\mathbb{F}_p[x]$, $\Phi_7(x) = x^6 + x^5 + \dots + x + 1$ is $(x-1)^6$ for $p = 7$, a product of distint linear factor for $p \equiv 1 \bmod 7$, a product of 3 irreducible quadratics for $p \equiv 6 \bmod 7$, a product of 2 irreducible cubics for $p \equiv 2, 4 \bmod 7$, and is irreducible for $p \equiv 3, 5 \bmod 7$.

Solution 1.4.1

By previous part, we have $\mathbb{F}_p(\zeta) = \mathbb{F}_p(\zeta^a)$ for any integer a not divisible by l.

Therefore we naturlly have the conjugacy classes of ζ^k by the modulo subgroup of l.

For $p = 7$, Φ_l is $(x-1)^6$ because 1 is the only element having degree 7.

For $p \equiv 1 \bmod 7$, Φ_l is a product of distinct linear factors based on last part since $f = 1$.

For $p \equiv 6 \bmod 7$, Φ_l is a product of 3 irreducible quadratics based on last part since $f = 2$.

For $p \equiv 2, 4 \bmod 7$, Φ_l is a product of 2 irreducible cubics based on last part since $f = 3$.

For $p \equiv 3, 5 \bmod 7$, Φ_l is irreducible based on last part since $f = 6$.

2

2.1

Let φ denote the Frobenius map $x \mapsto x^p$ on the finite field $\mathbb{F}_p^n$ as in the previous exercise. Determine the rational canonical form over $\mathbb{F}_p$ for φ considered as an $\mathbb{F}_p$-linear transformation of the n-dimensional $\mathbb{F}_p$-vector space $\mathbb{F}_p^n$.

Solution 2.1.1

To derive the rational canonical form over $\mathbb{F}_p$ it suffices to find the minimal polynomial of φ.

Lemma 2.1.1

The minimal polynomial of φ is $x^{p^n} - 1$.

Proof: Suppose we have lower degree polynomial P such that $P(\varphi) = 0$. We can write this polynomial as $\sum a\sigma_p^k$, and we know that it is 0. Then

$$\left(\sum a\sigma_p^k\right)(x) = \sum a\sigma_p^k(x) = \sum ax^{p^k} = 0$$

Thus all x is a root of P, which is a contradiction because the degree of this polynomial is less than p^n. □

Thus the rational canonical form is

$$\begin{pmatrix} 0 & 0 & \dots & 0 & 1 \\ 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 & 0 \end{pmatrix}$$

2.2

Let φ denote the Frobenius map $x \mapsto x^p$ on the finite field $\mathbb{F}_p^n$ as in the previous exercise. Determine the Jordan canonical form (over a field containing all the eigenvalues) for φ considered as an $\mathbb{F}_p$-linear transformation of the n-dimensional $\mathbb{F}_p$-vector space $\mathbb{F}_p^n$.

Solution 2.2.1

Follow a similar construction, it suffices to consider the chraacteristic polynomial of φ.

However, since the degree of the characteristic polynomial is p^n, we have the minimal polynomial is the characteristic polynomial.

$x^{p^n} - 1$ is separable when p does not divides n.

Thus the Jordan canonical form is

$$\begin{pmatrix} \zeta_1 & 0 & \dots & 0 \\ 0 & \zeta_2 & \dots & 0 \\ 0 & 0 & \dots & \zeta_n \end{pmatrix}$$

where ζ_i are the p^n-th primitive root of unity.

When p divides n, we have the minimal polynomial $x^{q^{p^k}} - 1^{p^k} = (x^q - 1)^{p^k}$, and let $\lambda_1, \dots, \lambda_q$ be the roots of $x^q - 1$, we have the Jordan canonical form is

$$\begin{pmatrix} \lambda_1 & 1 & \dots & 0 & 0 \\ 0 & \lambda_1 & \dots & 0 & 0 \\ 0 & 0 & \dots & \lambda_q & 1 \\ 0 & 0 & \dots & 0 & \lambda_q \end{pmatrix}$$

where each jordan block are size p^k.

3 Wedderburn's Theorem on Finite Division Rings

The exercise outline a proof of Wedderburn's Theorem that a finite division ring D is a field.

3.1

Let Z denote the center of D. Prove that Z is a field containing $\mathbb{F}_p$ for some prime p. If $Z = \mathbb{F}_q$ prove that D has order q^n for some integer n.

Solution 3.1.1

Because we know that the center of D is finite and commutative, and thus is a finite field. Further, we know that any finite field containing some $\mathbb{F}_p$ for some prime p.

We also know that D is a finite dimensional vector space over Z, since the regular ring addition and multiplication can be used, and thus D has order q^n for some integer n.

3.2

The nonzero elements $D^\times$ of D form a multiplicative group. For any $x \in D^\times$ shows that the elements of D which commute with x form a division ring which contains Z. Show that this division ring is of order q^m for some integer m and that $m < n$ if x is not an element of Z.

Solution 3.2.1

Since Z is the center, so all elements of $D^\times$ commute with x will contain Z.

It suffices to verify that this is a ring, which follows from that we cannot goes from commute with x to something not commute with x by addition and multiplication.

Since this division ring is also a vector space over Z, we have its order equal to some m, and $m < n$ because if $m = n$ then this division ring has to be the whole ring and thus x has to be in Z.

3.3

Show that the class equation for the group $D^\times$ is

$$q^n - 1 = (q - 1) + \sum_{i=1}^{r} \frac{q^n - 1}{|C_D^\times(x_i)|}$$

where x_i are representatives of the distinct conjugacy classes in $D^\times$ not contained in the center of $D^\times$. Conclude that for each i, $|C_D^\times(x_i)| = q^{m_i} - 1$ for some $m_i < n$.

Solution 3.3.1

We have the class equation for the group $D^\times$ is

$$|Z(D)^\times| + \sum_{i=1}^{r} \frac{|D^\times|}{|C_D^\times(x_i)|} = q^n - 1 = (q - 1) + \sum_{i=1}^{r} \frac{q^n - 1}{|C_D^\times(x_i)|}$$

Thus

$$\sum \frac{q^n - 1}{|C_D^\times(x_i)|} = q^{n-1}$$

From previous part we know that $|C_D^\times(x_i)| = q^{m_i} - 1$ for some $m_i < n$.

3.4

Prove that since $\frac{q^n-1}{q_i^m=1} = |D^\times : C_D^\times(x_i)|$ is an integer then m_i divides n. Conclude that $\Phi_n(x)$ divides $\frac{x^n-1}{x^{m_i}-1}$ and hence that the integer $\Phi_n(q)$ divides $\frac{q^n-1}{q^{m_i}-1}$ for $i = 1, 2, ..., r$.

Solution 3.4.1

Since $\frac{q^n-1}{q^{m_i}-1} = |D^\times : C_D^\times(x_i)|$ is an integer

Let $n = km_i + r$

$$(q^n - 1) - (q^r - 1) = q^n - q^r = q^{km} - 1 = (q^m - 1)l$$

for some l.

Thus it is equivqlent to prove thqt $q^n - 1 \mid q^r - 1$ by euclideqn qlgorithm.

However since $n > r$ by construction, we hqve $q^n - 1 \mid q^r - 1 \Leftrightarrow q^r - 1 = 0 \Leftrightarrow r = 0$ which implies the claim.

Note that $\Phi_{n(q)} = \frac{x^n-1}{x-1}$, thus it suffices to check $x^{m_i} - 1 \mid x - 1$, which is always true.

3.5

Prove that $\Phi_n(q) = \prod_{\zeta \text{ primitive}}(q - \zeta)$ divides $q - 1$. Prove that $|q - \zeta| > q - 1$ (complex absolute value) for any root of unity $\zeta \neq 1$. [note that 1 is the closest point on the unit circle in $\mathbb{C}$ to the point q on the real line]

Conclude that $n = 1 \Leftrightarrow D = Z$.

Solution 3.5.1

We have $\Phi_n(x) = \prod_{d \mid n} \Phi_d = \prod_{\zeta \text{ primitive}}(x - \zeta)$. We have $\Phi_n(q)$ divides $\frac{q^n-1}{q^{m_i}-1}$. Since we can have all kind of $m_i < n$, their LCM will be $q^{n-1} - 1$, and thus $\Phi_n(q) \mid q - 1$.

Since q is prime, so $p > 1$ and $p \in \mathbb{R}$. Therefore, since ζ lies on the unit circle, and 1 is the closest points to p lying on the unit circle, $|q - \zeta| > q - 1$.

Therefore, since $\Phi_n(q) = \prod_{\zeta \text{ primitive}}(x - \zeta)$, $|\Phi_n(q)| = \prod_{\zeta \text{ primitive}}|x - \zeta|$, and thus $n = 1$, since it divides $q - 1$.

4 Dirichlet's Theorem

4.1

Given any monic polynomial $P(x) \in \mathbb{Z}[x]$ of degree at least one show that there are infinitely many distinct prime divisors of the integers

$$P(1), P(2), P(3), \dots, P(n), \dots.$$

[Suppose $p_1, p_2, \dots, p_k$ are the only primes dividing the values $P(n)$, $n = 1, 2, \dots$. Let N be an integer with $P(N) = a \neq 0$. Show that $Q(x) = a^{-1}P(N + a\, p_1 p_2 \dots p_k\, x)$ is an element of $\mathbb{Z}[x]$ and that $Q(n) \equiv 1 \pmod{p_1 p_2 \dots p_k}$ for $n = 1, 2, \dots$. Conclude that there is some integer M such that $Q(M)$ has a prime factor different from $p_1, p_2, \dots, p_k$ and hence that $P(N + ap_1p_2 \cdots p_kM)$ has a prime factor different from $p_1, p_2, \dots, p_k$.]

Suppose $p_1, p_2, ..., p_k$ are the only primes the dividing values $P(n)$.

Consider a integer N such that $P(N) = a \neq 0$. Consider the polynomial $Q(x) = a^{-1} P(N + a p_1 p_2 ... p_k x)$.

Lemma 4.1.1

$$Q(x) \in \mathbb{Z}[x]$$

Proof: Since P is a polynomial, we can write $P = b_1 x^n + b_2 x^{n-1} + ... b_{n+1}$. Then consider $P(N + a p_1 p_2 ... p_k x)$, by binomial theorem we have each terms being writeen as some product of N and $a p_1 p_2 ... p_k x$. Any term involving the second part is certainly divisible by a, and the grouping of term that only contains N is equal to $P(N)$, and by assumpition, is divisible by a since $P(N) = a$. Therefore $Q(x) \in \mathbb{Z}[x]$. □

Lemma 4.1.2

$$Q(n) = 1$$

Proof: We can show the following by a similar construction as above:

$$Q(n) = \frac{P(N + n a p_1 p_2 ... p_k)}{a} \equiv \frac{P(N)}{a} \equiv 1 \pmod{p_1 p_2 ... p_k}$$

□

Corollary 4.1.2.1

There are some $M \in \mathbb{Z}$ such that $Q(M)$ is coprime with $p_1 p_2 ... p_k$.

Proof: It suffices to check that $Q(n)$ is not 1 for some integer n.

Assume $Q(n) = 1 \forall n$, we have Q is a degree 0 polynomial, which is a contradiction because $Q = a^{-1} P(N + a p_1 ... p_k x)$, but P has degree greater than 1. □

Corollary 4.1.2.2

$P(N + a p_1 p_2 ... p_k M)$ is divisible by some prime p not in $p_1 p_2 ... p_k$.

Proof: This is trivial given that $Q(M)$ is coprime with $p_1 p_2 ... p_k$ and $P(N + a p_1 p_2 ... p_k M) = a Q(M)$. □

4.2

Let p be an odd prime not dividing m and let $\Phi_m(x)$ be the m^{th} cyclotomic polynomial. Suppose $a \in \mathbb{Z}$ satisfies $\Phi_m(a) \equiv 0 \pmod{p}$. Prove that a is relatively prime to p and that the order of a in $(\mathbb{Z}/p\mathbb{Z})^\times$ is precisely m. [Since

$$x^m - 1 = \prod_{d|m} \Phi_d(x) = \Phi_m(x) \prod_{\substack{d|m \\ d<m}} \Phi_d(x)$$

we see first that $a^m - 1 \equiv 0 \pmod{p}$ i.e., $a^m \equiv 1 \pmod{p}$. If the order of a mod p were less than m, then $a^d \equiv 1 \pmod{p}$ for some d dividing m, so then $\Phi_d(a) \equiv 0 \pmod{p}$ for some $d < m$. But then $x^m - 1$ would have a as a multiple root mod p, a contradiction.]

Since $a \in \mathbb{Z}$ satisfied $\Phi_{m(a)} \equiv 0 \bmod p$. We have a is a root of Φ_m in $\mathbb{F}_p$. Thus the order of $a \bmod p$ were less than m and $\exists d : a^d \equiv 1 \bmod p$ for some $d \mid m$.

Further we know that $x^m - 1 = \prod_{d \mid m} \Phi_d(x) = \Phi_m(x) \prod_{\substack{d \mid m \\ d<m}} \Phi_d(x)$.

Since $a^d \equiv 1 \bmod p$ and $d \mid m$, we have $\Phi_d(a) \equiv 0 \bmod p$.

However this suggests that we have $x^m - 1$ is not separable because two of its factor contains a as a root, which is a contradiction when p does not divides m.

Then since p does not divides m, we have a is relatively prime to p because its order is m.

4.3

Let $a \in \mathbb{Z}$. Show that if p is an odd prime dividing $\Phi_m(a)$ then either p divides m or $p \equiv 1 \bmod m$.

Solution 4.3.1

If p divides $\Phi_m(a)$, then a is a solution of Φ_m under $\mathbb{F}_p$. From previous exercise we have shown that a is relatively prime to p and the order of a in $(\mathbb{Z}/p)^\times$ is precisely m if p does not divides m.

Since we know that the order of an arbitary element of a group divides the order of the group, we have $m \mid p - 1$.

4.4

Prove there are infinitely many primes p with $p \equiv 1 \bmod m$.

Solution 4.4.1

It suffices to find infinitely many pairs of p, a such that p divides $\Phi_m(a)$ by previous part.

By Section 4.1 we know that for any monic polynomial P, there are infinitely many prime factors of the sequence $P(1), P(2), \dots$. Thus for any m, there are infinitely many primes p with such that it divides $\Phi_m(a)$ for a sequences of a. Thus we know that we have infinitely many pair of p and a satisfying the condition we have for previous parts.