Cyclotomy and Gauss' Theorem

Xiaomin Li

February, 2019

1. Introduction

Cyclotomy is concerned with the properties of the unity roots of a given order. There was a well-known cyclotomic method to calculate π. In 263 A.D., a Chinese mathematician Liu, Hui used an approach of "cutting" a circle to calculate π: he inscribed regular polygons in a circle and use the area of a polygon to approximate the area of a circle with a certain radius. In his own word, he said that "the finer the circle being cut, the smaller error we get when we estimate; if we continue to cut until the polygon cannot be cut any more, then the area of this polygon yields the area of the circle". This method coincides with the modern infinite series methodology of estimation.

In Chapter 3 of *Multiplicative Number Theory* by Harold Davenport, he proved a main result quoted in Chapter 1: $\prod_R [x - e_q(R)] = \frac{1}{2}[Y(x) - q^{\frac{1}{2}} Z(x)]$ and $\prod_{i=1} [x - e_q(N)] = \frac{1}{2}[Y(x) + q^{\frac{1}{2}} Z(x)]$, where R and N are sets of typical quadratic residues and nonresidues (mod q) between 0 and q for some prime q greater than 2, and $Y(x)$ and $Z(x)$ are polynomials of integer coefficients. Along with the proof, some discussions of the Gauss' Sum and others results are mentioned. Then he talked about 2 generally interesting topics in cyclotomy: the first is *Gauss' Theorem*, which gives the values of q of which it is possible to inscribe a regular q-sided polygon in a given circle using ruler and compasses only; the second topic is the *Kummer's Problem* on the cubic periods. In this presentation, I would only discuss about the first topic.

2. Gauss' Sum and Other Background Discussions

- *Polynomial and Index*

  We first talk about some results the author used in Chapter 1 but only proved in this Chapter. Let q be a primer greater than 2, let ζ be a qth root of unity other than 1. Then we have the set of qth roots of unity $= \{\zeta, \zeta^2, ..., \zeta^q\}$, where $\zeta^q = 1$. Any power of ζ with power greater than q could be reduced into a form where the power is less than q. That is, $\forall a \in \mathbb{N}, \zeta^a = \zeta^r$ where $r \equiv a \mod q$.

  Now for any polynomial in variable ζ with integer coefficients $a_1, a_2, ..., a_n$, we could uniquely express it into the form: $a_1\zeta + a_2\zeta^2 + ... + a_n\zeta^n$ (and the expression is actually unique because the cyclotomic polynomial $x^{q-1} + x^{q-2} + ... + 1$, of which ζ is a zero, is irreducible over the rational field).

  Consider a primitive root g modulus q (by the Primitive Root Theorem, we know q must have a primitive root). We know that if g is a primitive root modulo q, then $\{g, g^2, ..., g^{\phi(q)}\}$ is a set of reduced residues mod q. In particular, as q is prime, $\phi(q) = q - 1$ and the set is a complete residue system without q itself. Therefore, any integer n would be congruent to a power of g if it's not a multiple of q.

In Chapter 1, the author defines $v(n)$ as the index of n relative to a fixed primitive root g (i.e. the exponent v for which $g^v \equiv n$). If n assumes values $1, 2, ..., q-1$, the index also assumes same value in them, as we just mentioned that $\{g, g^2, ..., g^{\phi(q)}\} = \{g, g^2, ..., g^{q-1}\}$ $= \{1, 2, ..., q-1\}$.

- *Gaussian Periods of f Terms*

  As we know $q-1$ is not prime, we can consider a factorization of it. Let $q-1 = e \cdot f$. As when n runs through $1, 2, ..., q-1$, $v(n)$ also run through these values, then we consider the residues of these values modulo e. This would evenly divided them into e subsets, each having f numbers. Consider the corresponding ζ^n for each n, if for each residue class mod e, we sum up these ζ^n, then we obtain what's called the "Gaussian periods of f terms":

$$\eta_j = \sum_{\substack{n \text{ such that} \\ v(n) \equiv j \mod e}} \zeta^n$$

More precisely,

$$\eta_j = \sum_{\substack{n=1 \\ v(n) \equiv j \mod e}}^{q-1} \zeta^n$$

  We do not have to restrict j to be an element in the least residues of e. If we consider, more generally, all numbers j, then η_j is periodic with period e (e.g. $\eta_1 = \eta_{1+e}$ since $v(n) \equiv 1 \mod e$ is equivalent to $v(n) \equiv 1 + e \mod e$).

- *Special case when e = 2*

  Since $q-1$ is even, we can take $e = 2$, then $f = \frac{q-1}{2}$. As the number of subsets is e, we only have 2 subsets here, which are 2 Gaussian periods of $\frac{q-1}{2}$ terms, corresponding to residue 0 and residue 1 (mod e) respectively:

$$\eta_0 = \sum_{\substack{n=1 \\ v(n) \equiv 0 \mod 2}}^{q-1} \zeta^n, \qquad \eta_1 = \sum_{\substack{n=1 \\ v(n) \equiv 1 \mod 2}}^{q-1} \zeta^n$$

  Now we take a closer look at the exponents n's of ζ in each sum:

$$\begin{aligned}
& v(n) \equiv 0 \mod e \\
\Rightarrow\ & v(n) = ke \text{ for some integer k} \\
\Rightarrow\ & g^{ke} \equiv n \mod q \\
\Rightarrow\ & g^{k2} \equiv n \mod q \\
\Rightarrow\ & (g^k)^2 \equiv n \mod q \\
\Rightarrow\ & \text{n is a quadratic residue modulo q} \\
\Rightarrow\ & \left(\frac{n}{q}\right) = 1
\end{aligned}$$

There are exactly $\frac{q-1}{2}$ quadratic residues and exactly $\frac{q-1}{2}$ quadratic nonresidues in $\{1, 2, ..., q-1\}$. As there are $\frac{q-1}{2}$ terms in each subset, so we know the exponents n in η_0 are exactly those quadratic residues mod q, and those in η_1 are the quadratic nonresidues.

- *Gauss' Sum*

In Chapter 2, the author mentioned the "Gauss' Sum", denoted by $G(n)$ and defined by:

$$G(n) = \sum_{m=1}^{q-1} \left(\frac{m}{q}\right) e_q(mn)$$

where $e_q(mn)$ is an abbreviation of $e^{\frac{2\pi imn}{q}}$. We let $G = G(1)$. The author also computed the value of G^2 as the following:

$$G^2 = q\left(\frac{-1}{q}\right) = \begin{cases} q, & \text{if } q \equiv 1 \mod 4. \\ -q, & \text{if } q \equiv 1 \mod 4. \end{cases}$$

In the first case when $q \equiv 1 \mod 4$, $G = q^{\frac{1}{2}}$; in the second case when $q \equiv 3 \mod 4$, $G = (-q)^{\frac{1}{2}}$. Therefore, the author used a combined way to represent the value of G:

$$G = \epsilon q^{\frac{1}{2}},$$

where $\epsilon = 1$ or i when $q \equiv 1$ or $3 \mod 4$, respectively.

Now we go back to look at the two η's. If we fix $\zeta = e^{\frac{2\pi i}{q}}$, as:

$$\forall \text{ quadractice residue n, } \left(\frac{n}{q}\right) = 1$$

$$\Rightarrow \eta_0 = \sum_{\substack{n=1 \\ \text{n is quadratic residue}}}^{q-1} \zeta^n$$

$$\Rightarrow \eta_0 = \sum_{\substack{n=1 \\ \text{n is quadratic residue}}}^{q-1} \left(\frac{n}{q}\right)\zeta^n$$

$$\Rightarrow \eta_0 = \sum_{\substack{n=1 \\ \text{n is quadratic residue}}}^{q-1} \left(\frac{n}{q}\right)e_q(n)$$

Similarly, we can deduce that :

$$\Rightarrow -\eta_1 = \sum_{\substack{n=1 \\ \text{n is quadratic nonresidue}}}^{q-1} \left(\frac{n}{q}\right)e_q(n)$$

Then, we could calculate the values of η_0 and η_1 from the value of Gauss'sum. By the calculation just know, we have:

$$\Rightarrow \eta_0 - \eta_1 = \sum_{m=1}^{q-1} \left(\frac{m}{q}\right) e_q(m) = G(1) = G = \epsilon q^{\frac{1}{2}}.$$

Recall we have $\eta_0 + \eta_1 = \zeta + ... + \zeta^{q-1} = -1$, now combine these two relations, we could deduce that: $\eta_0 = \frac{1}{2}(-1 + \epsilon q^{\frac{1}{2}})$, $\quad \eta_1 = \frac{1}{2}(-1 - \epsilon q^{\frac{1}{2}})$

- *General case*

  In the general case of the values of e, if we continue fixing $\zeta = e^{\frac{2\pi i}{q}}$, the author also provided a formula for η_0:

$$\eta_0 = e^{-1}\sum_{x=1}^{q-1} e_q(x^e)$$

  and η_0 is uniquely determined, while the values of $\eta_1, ..., \eta_{e-1}$ will depend on the choice of primitive root g.

3. Prove Results Quoted in Chapter 1

- *Polynomial $F(\zeta)$*

  Let $F(\zeta)$ be any polynomial in ζ:

$$F(\zeta) = \sum_{r=1}^{q-1} A_r\zeta^r$$

  with integer coefficients and with property:

$$\forall m \text{ s.t. } v(m) \equiv 0 \mod e, \quad F(\zeta^m) = F(\zeta)$$

  Because of the uniqueness of representation of the polynomial, we can prove that whenever $r \equiv sm \mod q-1$, we have $A_r = A_s$. This holds for all m with $v(m) \equiv 0 \mod e$. With more computations, we could group the terms with same coefficients and will obtain:

$$F(\zeta) = A_1\eta_1 + ... + A_e\eta_e,$$

  from which we could see that $F(\zeta)$ is a linear combination of the Gaussian periods. The result does not only hold for integer coefficients A_r, it actually also holds when A_r themselves are polynomials in some indeterminate variable x with integral coefficients.

- *Prove result*

  Now we use the discussion above to evaluate the following polynomial (the polynomial used in Chapter 1) in the special case when $e = 2$:

$$\prod_R (x - \zeta^R).$$

  (note: $\prod_R(x - \zeta^R)$ means R runs through those typical quadratic residues, that is, $\prod_{r\in R}(x - \zeta^r)$)

  If we expand this product and write it into the standard form, then we will have the coefficients of powers of ζ as some polynomials in variable x with integer coefficients. Consider any integer m such that $v(m) \equiv 0 \mod e$, that is, $v(m) \equiv 0 \mod 2$. Then as $v(m)$ is even, we have $g^v \equiv m \mod q$, and therefore m is a quadratic residue mod q. If we multiply each quadratic residue in set R by m, then all the products are distinct quadratic residues. As we have $\zeta^q = 1$, we could reduce the new polynomial of ζ into the standard form, then those powers would be the same quadratic residues R in different order. So we have obtained back the same set R. That implies:

$$F(\zeta^m) = \prod_R (x - \zeta^{Rm}) = \prod_R (x - \zeta^R) = F(\zeta).$$

Hence, we know our $F(\zeta)$ satisfies the property we discussed before. Now we could apply our results above to get:

$$F(\zeta) = A_0(x)\eta_0 + A_1(x)\eta_1.$$

Recall that we had calculated:

$$\eta_0 = \frac{1}{2}(-1 + \epsilon q^{\frac{1}{2}}), \quad \eta_1 = \frac{1}{2}(-1 - \epsilon q^{\frac{1}{2}}).$$

So we would obtain:

$$\begin{aligned} F(\zeta) &= A_0(x)\frac{1}{2}(-1 + \epsilon q^{\frac{1}{2}}) + A_1(x)\frac{1}{2}(-1 - \epsilon q^{\frac{1}{2}}) \\ &= \frac{1}{2}[Y(x) - \epsilon q^{\frac{1}{2}} Z(x)] \end{aligned}$$

for some polynomials $Y(x)$ and $Z(x)$ with integer coefficients.

Similarly, one can deduce that:

$$\prod_N (x - \zeta^N) = \frac{1}{2}[Y(x) + \epsilon q^{\frac{1}{2}} Z(x)].$$

This completes the proof of the main result in this Chapter.

4. Gauss' Theorem

- *Gauss' Theorem*

  Gauss' Theorem asserts that if q is a prime of the form $2^k + 1$ (e.g. 3, 5, 17, 257, or 65537), each qth root of unity can be expressed in terms of rational numbers by using a succession of square root signs.

  With further observations, one can deduce: for prime q of the form $2^k + 1$ (Fermat Primes), a q-sided regular polygon can be constructed by a Euclidean construction, using only ruler and compasses, through the approach to inscribe the regular polygon in a circle.

- *Sketch of Proof*

  As $q - 1 = 2^k$, all the possible factors e are powers of 2:

$$\begin{aligned} &e_1 = 2,\ f_1 = \frac{q-1}{2} \\ &e_2 = 2^2\ f_2 = \frac{q-1}{2^2} \\ &... \\ &e_2 = 2^k,\ f_2 = \frac{q-1}{2^k} = 1 \end{aligned}$$

For each e_r, we have e_r Gaussian periods of f_r terms. Let us denote them by:

$$\eta_1^{(r)}, ..., \eta_e^{(r)} \qquad (e = e_r),$$

where r runs through 1 to k.

Actually, our discussion of the special case when $e = 2$, is evaluating $\eta_1^{(1)}$ and $\eta_2^{(1)}$, which are $\frac{-1\pm\sqrt{q'}}{2}$, where $q' = q$ when $q \equiv 1 \mod 4$ and $q' = -q$ when $q \equiv 3 \mod 4$. For the latter, as $q = 2^k + 1$, when $q > 3$, we know this case cannot happen since we must have $q \equiv 1 \mod 4$.

Now consider the case when $r = 2$, so $e_r = 2^r = 4$ and we have 4 periods $\eta_1^{(2)}, \eta_2^{(2)}, \eta_3^{(2)}, \eta_4^{(2)}$. Recall the definition is:

$$\eta_j^{(2)} = \sum_{v(n)\equiv j \mod 4} \zeta^n.$$

Look at the polynomial in ζ:

$$(x - \eta_1^{(2)})(x - \eta_3^{(2)}).$$

As discussed before, if we have number m such that $v(m) \equiv 0 \mod 2$, which means index v of m is even, then m is a quadratic residue. By earlier results, we know replacing ζ by ζ^m will not alter the polynomial. Before, we have such polynomial $F(\zeta) = \prod_R (x - \zeta^R)$ would equal to $A_0(x)\eta_0 + A_1(x)\eta_1$ for some polynomials $A_0(x)$ and $A_1(x)$ with integer coefficients. Now it's just the special case when we only have the product of 2 such terms, so we know:

$$F(\zeta) = (x - \eta_1^{(2)})(x - \eta_3^{(2)}) = A_0(x)\eta_0 + A_1(x)\eta_1$$

for some polynomials $A_0(x)$ and $A_1(x)$ with integer coefficients.

View the LHS and RHS as the polynomials of x, then as they are equal, we could match the coefficients and conclude that each coefficient (of variable x) on the LHS is expressible by rational numberss and $\sqrt{q'}$. Therefore, $\eta_1^{(2)}$ and $\eta_3^{(2)}$ are expressible by nested radicals (double square root signs). For $\eta_2^{(2)}$ and $\eta_4^{(2)}$, it's similar. Do this inductively, we would finally reach the case when $e = 2^k$ and $f = 1$, where we have 2^k periods of just 1 term. By the definition of η, where each η is a sum of powers of ζ and there are f of them in all the e sets. Now each sum is just one term, so those periods turn out to be just: $\zeta, \zeta^2, ..., \zeta^{q-1}$. Each of them is expressible by combining rational numbers and k-layered nested radicals. This proves the assertion of Gauss that each qth root of unity can be expressed in terms of rational numbers by using a succession of square root signs, when q is a Fermat Prime.

- *Heptadecagon*

  One main reason that I chose this Chapter to present is that I have got interested in the Euclidean construction problem of heptadecagon, and I had studied this topic for a while back in high school. The value of $cos\frac{2\pi}{17}$ actually looks quite complicated and extremely attractive for a high school student. I present the value here:

$$cos\frac{2\pi}{17} = \frac{-1+\sqrt{17}+\sqrt{34-2\sqrt{17}}+2\sqrt{17+3\sqrt{17}-\sqrt{34-2\sqrt{17}}-2\sqrt{34+2\sqrt{17}}}}{16}.$$

One story I have heard is that Gauss requested to engrave a heptadecagon to his tombstone, but it was not granted for some reason. Some people also say if you draw the heptadecagon on the tombstone, it would be extremely undistinguishable from a circle. I have not verified this story but it is indeed a remarkable achievement that Gauss relate the Fermat primes to the constructable polygons by only ruler and compasses. Here is a link to a video of drawing heptadecagon and it is the same one which caught me interest when I was in high school: https://www.youtube.com/watch?v=uYqXeZJl74w.

References

- Davenport, H. T. (1980). Multiplicative number theory. Estados Unidos: Springer.

- Liu Hui and his mathematic career. (2014, April 12). Retrieved February 20, 2019, from https://liuhuimathmatician.wordpress.com/tag/cyclotomic-method/

- P. (2015, October 02). Retrieved February 21, 2019, from https://www.youtube.com/watch?v=uYqXeZJl74w