

Cyclotomic extension

Let p be an odd prime number. And let a be any integer. We say a is a quadratic residue mod p iff $x^2 \equiv a \pmod{p}$ is solvable. Otherwise we say a is a quadratic non-residue. Let $p \nmid a$ (so $\gcd(a, p) = 1$) if a is a quadratic residue we define $(a/p) = 1$ if it is a quadratic non-residue we define $(a/p) = -1$. And if $p|a$ we define $(a/p) = 0$. This is referred to the Legendre symbol.

We would like to have a test which tells us when a is a quadratic residue. It is safe to assume that $p \nmid a$ because if $p|a$ then certainly $0^2 \equiv a \pmod{p}$ and therefore it is a quadratic residue, and from now on we will assume that $p \nmid a$. Say that a is a quadratic residue then $x^2 \equiv a \pmod{p}$ and then $a^{(p-1)/2} \equiv (x^2)^{(p-1)/2} = x^{p-1} \equiv 1 \pmod{p}$. This tells us that if a is quadratic residue then $a^{(p-1)/2} \equiv 1 \pmod{p}$. It is reasonable to ask whether the converse is true. It turns out that it is! The fact that we need is that \mathbb{F}_p (the integers modulo p) is a finite field and therefore \mathbb{F}_p^\times is a cyclic group. Let r be a generator of this group. Therefore $a \equiv r^k \pmod{p}$ for some k . If $a^{(p-1)/2} \equiv 1 \pmod{p}$ it means $r^{k(p-1)/2} \equiv 1 \pmod{p}$. Since the order of r is $p-1$ (remember it is a generator) it follows that $(p-1) | (k \cdot \frac{p-1}{2})$ and therefore $2|k$ i.e. k must be even. Since k is even it means $k/2$ is an integer and so $(r^{k/2})^2 \equiv a \pmod{p}$ which means $(a/p) = 1$. In conclusion, we have that a is a quadratic residue if and only if $a^{(p-1)/2} \equiv 1 \pmod{p}$.

There are some simple and useful properties of the Legendre symbol :

- $(ab/p) = (a/p)(b/p)$
- $(a/p) = (b/p)$ if $a \equiv b \pmod{p}$
- $(a/p) \equiv a^{(p-1)/2} \pmod{p}$
- $(-1/p) = (-1)^{(p-1)/2}$

The first two properties should be obvious, the third one is easy too. If $(a/p) = 1$ then by above $a^{(p-1)/2} \equiv 1 \pmod{p}$; otherwise if $(a/p) = -1$ then $a^{(p-1)/2} \not\equiv 1 \pmod{p}$ and it follows from Fermat's theorem that $a^{p-1} \equiv 1 \pmod{p} \implies a^{p-1} - 1 \equiv 0 \pmod{p}$ factor $(a^{(p-1)/2} - 1)(a^{(p-1)/2} + 1) \equiv 0 \pmod{p}$. Since we are assuming the first factor is non-zero it means $a^{(p-1)/2} \equiv -1 \equiv (a/p) \pmod{p}$ which completes the proof. The fourth property is based on the third. Since if p is odd prime we have either $p \equiv 1 \pmod{4}$ or $p \equiv 3 \pmod{4}$. If $p \equiv 1 \pmod{4}$ then $(p-1)/2$ is even so $(-1)^{(p-1)/2} = 1$ in other case we get $(-1)^{(p-1)/2} = -1$.

Theorem 1 : $\sum_{x=0}^{p-1} (x/p) = 0$.

Proof : A number x (relatively prime to p) is a quadratic residue if and only if $x^{(p-1)/2} \equiv 1 \pmod{p}$. It should be a known fact that $x^d \equiv 1 \pmod{p}$ has exactly d solutions (in each

congruence class) if $d|(p-1)$. (If this fact is not familiar note that this congruence is asking the # of elements of order d in the group \mathbb{F}_p^\times , since this group is cyclic by the theory of cyclic groups there are exactly d such elements). And it immediately follows that there are exactly $\frac{p-1}{2}$ quadratic residues (relatively prime to p) since 0 is quadratic residue the remaining ones are non-residues i.e. there are $\frac{p-1}{2}$ non-residues. And finally because we have as many pluses from $(a/p) = 1$ as minuses from $(a/p) = -1$ it means the entire sum is zero.

Let $\zeta = e^{2\pi i/p}$ a primitive p -th root of unity. It should be a known fact that $1 + \zeta + \dots + \zeta^{p-1} = 0$. We can verify this geometrically by looking at the equally spaced point on the unit circle in the complex plane, or we can use geometric series. We can in fact do better, let a be an integer. Then $1 + \zeta^a + \zeta^{2a} + \dots + \zeta^{(p-1)a}$ is equal to 0 if $p \nmid a$, and if $p|a$ then this sum is p . To verify this again use geometric series. Just be careful! Geometric summation formula for $1 + x + x^2 + \dots + x^{p-1}$ **does not** work when $x = 1$ - this is why we get two separate cases. Using this fact as a corollary we see that $1 + \zeta^{a-b} + \dots + \zeta^{(a-b)(p-1)} = p\delta_{ab}$. (Here $\delta_{ab} = 1$ if $a \equiv b \pmod{p}$ otherwise $\delta_{ab} = 0$).

We will now define the quadratic Gauss sum. Let a be an integer. Define $g_a = \sum_{j=0}^{p-1} (j/p)\zeta^{aj}$.

Theorem 2 : We have that $g_a = (a/p)g_1$.

Proof : If $p|a$ then $g_a = 0$ by above observations thus the proof is complete. If $p \nmid a$ then,

$$(a/p)g_a = \sum_{j=0}^{p-1} (aj/p)\zeta^{aj} = \sum_{k=0}^{p-1} (k/p)\zeta^k = g_1$$

This summation in the middle holds because aj goes through all the remainders mod p as j varies. Thus, $(a/p)^2 g_a = (a/p)g_1 \implies g_a = (a/p)g_1$ and proof is complete.

The following theorem is the main result that we are after.

Theorem 3 : We have that $g_1^2 = (-1)^{(p-1)/2}p$.

Proof : We will evaluate the sum $\sum_{c=0}^{p-1} g_c g_{-c}$ in two different ways and compare results. The first way is to realize if $p \nmid c$ then $g_c g_{-c} = (c/p)(-c/p)g_1^2 = (-1/p)g_1^2$, thus,

$$\sum_{c=0}^{p-1} g_c g_{-c} = (-1/p)(p-1)g_1^2$$

The second way is by definition of Gauss sums,

$$g_c g_{-c} = \sum_{a=0}^{p-1} \sum_{b=0}^{p-1} (a/p)(b/p)\zeta^{c(a-b)}$$

Using the fact on summing roots of unity it means,

$$\sum_{c=0}^{p-1} g_c g_{-c} = \sum_{a=0}^{p-1} \sum_{b=0}^{p-1} (a/p)(b/p)\delta_{ab}p = (p-1)p$$

Thus, $(-1/p)(p-1)g_1^2 = (p-1)p \implies g_1^2 = (-1/p)p \implies g_1^2 = (-1)^{(p-1)/2}p$.

As a result we get one of the nicest looking identities. If $p \equiv 1 \pmod{p}$ then $g_1 = \pm\sqrt{p}$ if $p \equiv 3 \pmod{p}$ then $g_1 = i \pm \sqrt{p}$. In fact the identity gets even nicer, it was proven by Gauss again that the Gauss sum always takes the positive value. But we will not need this fact.

For example, let $p = 5$. Then $g_1 = (1/5)\zeta + (2/5)\zeta^2 + (3/5)\zeta^3 + (4/5)\zeta^4 = \sqrt{5}$. (I know I said we will not use the fact that the sum takes always the positive value but this is strictly for the purpose of illustration). It is trivial check that $(1/5) = (4/5) = 1$ and $(2/5) = (3/5) = -1$. Thus, $\zeta - \zeta^2 - \zeta^3 + \zeta^4 = \sqrt{5}$. Since $\zeta = \cos \frac{2\pi}{5} + i \sin \frac{2\pi}{5}$ we see by equating real parts that $\cos \frac{2\pi}{5} - \cos \frac{4\pi}{5} - \cos \frac{6\pi}{5} + \cos \frac{8\pi}{5} = \sqrt{5}$. Reduce angles by $\cos(\pi + x) = -\cos x$ to get $\cos \frac{\pi}{5} + \cos \frac{2\pi}{5} - \cos \frac{3\pi}{5} - \cos \frac{4\pi}{5} = \sqrt{5}$. What a wonderful looking identity!

The fundamental point of this identity is that \sqrt{p} is expressible in terms of ζ . Well almost, depending whether it is congruent to 1 or 3 mod 4. But that will not stop us.

Theorem 4 : If p is odd prime then $\sqrt{p} \in \mathbb{Q}_{2p}$.

Proof : Let $\zeta = e^{2\pi i/p}$. If $p \equiv 1 \pmod{4}$ then $\pm\sqrt{p} = \sum_{j=0}^{p-1} (j/p)\zeta^j \in \mathbb{Q}_p$. But $p|2p$ which means $\mathbb{Q}_p \subseteq \mathbb{Q}_{2p}$ thus $\sqrt{p} \in \mathbb{Q}_{2p}$. If $p \equiv 3 \pmod{p}$ then $\pm i\sqrt{p} = \sum_{j=0}^{p-1} (j/p)\zeta^j \in \mathbb{Q}_p \subseteq \mathbb{Q}_{2p}$. But $i \in \mathbb{Q}_{2p}$ since $2p$ is even and so $i(\pm i\sqrt{p}) = \pm\sqrt{p} \in \mathbb{Q}_{2p}$. This completes the proof.

What happens if p is even? Then $p = 2$ and then $\sqrt{2} \in \mathbb{Q}_8$. Thus it is still contained in a cyclotomic extension. We can summarize by saying if p is any prime then $\sqrt{p} \in \mathbb{Q}_{4p}$.

Theorem 5 : If $n \in \mathbb{Z}^+$ then $\sqrt{n} \in \mathbb{Q}_{4n}$.

Proof : It is safe to assume n is not a square. Furthermore, we can factor out all the squares, thus it is safe to assume n is square free and it factors as $n = p_1 p_2 \dots p_k$. Thus $\sqrt{n} = \sqrt{p_1} \cdot \dots \cdot \sqrt{p_k}$. But $\sqrt{p_i} \in \mathbb{Q}_{4p_i} \subset \mathbb{Q}_{4n}$. This means $\sqrt{n} \in \mathbb{Q}_{4n}$.

What happens if $n < 0$? Then $\sqrt{n} = i\sqrt{-n}$ and this is contained in $\mathbb{Q}_{4(-n)}$. We can summarize by saying if $n \neq 0$ then $\sqrt{n} \in \mathbb{Q}_{4|n|}$.

Theorem 6 : If $d \in \mathbb{Q}$ then $\mathbb{Q}(\sqrt{d})$ is contained in a cyclotomic field.

Proof : It suffices to show \sqrt{d} is contained in a cyclotomic field. Write $d = n/m$ where $\gcd(n, m) = 1$ assuming $d \neq 0$. Then $\sqrt{n} \in \mathbb{Q}_{4|n|}$ and $\sqrt{m} \in \mathbb{Q}_{4|m|}$. It $\sqrt{n}, \sqrt{m} \in \mathbb{Q}_{4|nm|}$. Thus, $\sqrt{d} = \sqrt{n}/\sqrt{m} \in \mathbb{Q}_{4|nm|}$.

This proves problem #15.