Characters (definition)

Let p be a prime. A character on $\mathbb{F}_p$ is a group homomorphism $\mathbb{F}_p^\times \to \mathbb{C}^\times$.

Example

The map $a \mapsto 1 \ \forall\, a \in \mathbb{F}_p^\times$ is called the trivial character, henceforth denoted by ϵ.

Example

If g is a generator of $\mathbb{F}_p^\times$ and ζ is any $(p-1)^{\text{th}}$ root of unity in $\mathbb{C}$, the map $\mathbb{F}_p^\times \to \mathbb{C}^\times$, $g^k \mapsto \zeta^k$ is a character. In fact, it is easy to show that every character on $\mathbb{F}_p$ is of this form.

Characters (properties)

For any character χ on $\mathbb{F}_p$, $a \in \mathbb{F}_p^\times$

1. $\chi(1) = 1$
2. $\chi(a)^{p-1} = 1$
3. $\chi(a^{-1}) = \chi(a)^{-1} = \overline{\chi(a)}$

Under multiplication of functions, the characters on $\mathbb{F}_p$ form a cyclic group of order $p-1$. The generators are the maps $g^k \mapsto \zeta^k$, where g, ζ are generators of $\mathbb{F}_p^\times, \mu_{p-1}$, respectively.

Characters (extending domain)

For the rest of this discussion, we will extend the domain of a character on $\mathbb{F}_p$ to include 0 using the following rule:

1. $\chi(0) = 0$ for $\chi \neq \epsilon$
2. $\epsilon(0) = 1$

Note that this does not compromise the multiplicativity of characters.

For any non-trivial character χ on $\mathbb{F}_p$,

$$\sum_{a \in \mathbb{F}_p} \chi(a) = 0$$

A particular character: the Legendre symbol

Let p be an odd prime. For any integer a, we define the Legendre symbol

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & a \equiv \square \not\equiv 0 \quad (p) \\ -1 & a \not\equiv \square \quad (p) \\ 0 & a \equiv 0 \quad (p) \end{cases}$$

It is straightforward to show that

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \quad (p)$$

from which we get,

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \qquad \left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$$

A particular character: the Legendre symbol (II)

Note that the function $\mathbb{Z} \to \mathbb{C}$ defined by the Legendre symbol with denominator p does not distinguish between integers in the same congruence class modulo p. Thus, it defines a function $\mathbb{F}_p \to \mathbb{C}$. Since the Legendre symbol is multiplicative, this function is a character; in fact, it is the unique character on $\mathbb{F}_p$ of order 2. We call it the quadratic character on $\mathbb{F}_p$ and denote it by λ_p.

A particular character: the Legendre symbol (III)

Lemma 1

Let p be an odd prime, $a \in \mathbb{F}_p$, K a field extension of $\mathbb{F}_p$, and suppose $a = \alpha^2$ for some $\alpha \in K$. Then

$$\alpha^{p-1} = \lambda_p(a)$$

Pf: In K, we have

$$\alpha^{p-1} = \left(\alpha^2\right)^{\frac{p-1}{2}} = a^{\frac{p-1}{2}} = \lambda_p(a)$$

$\square$

Gauss sums (definition)

Let p be a prime, χ a character on $\mathbb{F}_p$, and $a \in \mathbb{F}_p$. We define

$$g_a(\chi) = \sum_{t \in \mathbb{F}_p} \chi(t) \zeta^{at}$$

where $\zeta_p = e^{2\pi i/p}$, and define $g(\chi) = g_1(\chi)$. Sums of this form are called <u>Gauss sums</u>.

Example

$$g(\epsilon) = \sum_{t \in \mathbb{F}_p} 1 \cdot \zeta_p^t = 0$$

Gauss sums (one result)

Claim

For any character χ on $\mathbb{F}_p$, $a \in \mathbb{F}_p^\times$,

$$g_a(\chi) = \chi(a^{-1})g(\chi)$$

Proof: We have

$$\begin{aligned} g_a(\chi) &= \sum_{t \in \mathbb{F}_p} \chi(t)\zeta_p^{at} = \sum_{u \in \mathbb{F}_\mathbb{P}} \chi(a^{-1}u)\zeta_p^u \\ &= \chi(a^{-1}) \sum_{u \in \mathbb{F}_p} \chi(u)\zeta_p^u = \chi(a^{-1})g(\chi) \end{aligned}$$

$\square$

Gauss sums (another result)

Claim

For any non-trivial character χ on $\mathbb{F}_p$,

$$|g(\chi)|^2 = p$$

Pf: We have

$$\begin{aligned} g(\chi)\overline{g(\chi)} &= \sum_{t,u\in\mathbb{F}_p} \chi(tu^{-1})\zeta_p^{t-u} = \sum_{v\in\mathbb{F}_p} \zeta_p^v \sum_{u\in\mathbb{F}_p^\times} \chi(1+vu^{-1}) \\ &= \sum_{u\in\mathbb{F}_p} 1 + \sum_{v\in\mathbb{F}_p^\times} \zeta_p^v \sum_{w\in\mathbb{F}_p-\{1\}} \chi(w) = p-1-\sum_{v\in\mathbb{F}_p^\times} \zeta_p^v \\ &= p-1-(-1) = p \end{aligned}$$

$\square$

Gauss sums (yet another result)

Claim

For any character χ on $\mathbb{F}_p$,

$$\overline{g(\chi)} = \chi(-1)g(\overline{\chi})$$

Proof: We have

$$\begin{aligned}\overline{g(\chi)} = \sum_{t\in\mathbb{F}_p} \overline{\chi(t)}\zeta_p^{-t} &= \sum_{u\in\mathbb{F}_p} \overline{\chi(-u)}\zeta_p^{u} \\ &= \overline{\chi(-1)} \sum_{u\in\mathbb{F}_p} \overline{\chi(u)}\zeta_p^{u} = \overline{\chi(-1)}g(\overline{\chi})\end{aligned}$$

Now note that $\chi(-1)^2 = \chi((-1)^2) = \chi(1) = 1$, so $\chi(-1) = \pm 1$. In particular, $\overline{\chi(-1)} = \chi(-1)$. $\square$

Gauss sums (final result)

Lemma 2

For any odd prime q,

$$g(\lambda_q)^2 = (-1)^{\frac{q-1}{2}} q$$

Pf: From previous results, $g(\lambda_q)\overline{g(\lambda_q)} = q$ and $\overline{g(\lambda_q)} = \lambda_q(-1)g(\overline{\lambda_q})$. We obtain the above statement by noting that $\lambda_q(-1) = (-1)^{(q-1)/2}$ and $\overline{\lambda_q} = \lambda_q$ since λ_q takes values in $\{\pm 1\}$. $\square$

By Lemma 1, this implies

Corollary

For any odd primes p, q,

$$g(\lambda_q)^{p-1} \equiv (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \lambda_p(q) \mod p$$

Law of quadratic reciprocity

Theorem

For any pair p, q of distinct odd primes,

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

Let $\zeta \neq 1$ be a q^{th} root of unity in $\mathbb{C}$, and let $\mathfrak{p}$ be a prime ideal in $\mathbb{Z}[\zeta]$ containing p (and, hence, excluding q). Define $K = \mathbb{Z}[\zeta]/\mathfrak{p}$. K is a finite field of characteristic p, so it is an extension of $\mathbb{F}_p$. We will show that

$$\lambda_q(p) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\lambda_p(q)$$

in K and hence in $\mathbb{Z}[\zeta]$, proving the theorem.

Proof of quadratic reciprocity

Pf: Since $\mathrm{char}(K) = p$, in K we have

$$g(\lambda_q)^p = \left(\sum_{t\in\mathbb{F}_q} \lambda_q(t)\zeta_q^t\right)^p = \sum_{t\in\mathbb{F}_q} \lambda_q(t)\zeta_q^{tp}$$
$$= \sum_{u\in\mathbb{F}_q} \lambda_q(p^{-1}u)\zeta_q^u = \lambda_q(p)g(\lambda_q)$$

Since $g(\lambda_q)^2 = \pm q \neq 0$ in K, we can divide both sides by $g(\lambda_q)$ to obtain

$$\lambda_q(p) = g(\lambda_q)^{p-1} = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\lambda_p(q)$$

by the corollary to Lemma 2. Since this quantity is ± 1, equality must hold in $\mathbb{Z}[\zeta]$ as well. $\square$

Jacobi sums (definition)

For any prime p and characters χ, ψ on $\mathbb{F}_p$, we define

$$J(\chi, \psi) = \sum_{\substack{a,b \in \mathbb{F}_p \\ a+b=1}} \chi(a)\psi(b)$$

Such sums are called Jacobi sums.

Examples

1. $J(\epsilon, \epsilon) = \sum_{a+b=1} 1 = \sum_{a \in \mathbb{F}_p} 1 = p$
2. For $\chi \neq \epsilon$, $J(\chi, \epsilon) = \sum_{a+b=1} \chi(a) = \sum_{a \in \mathbb{F}_p} \chi(a) = 0$

Relation between Jacobi sums and Gauss sums

Claim

For any characters χ, ψ on $\mathbb{F}_p$ on $\mathbb{F}_p$ with $\chi\psi \neq \epsilon$,

$$J(\chi, \psi) = \frac{g(\chi)g(\psi)}{g(\chi\psi)}$$

Pf: Note that $g(\chi\psi) \neq 0$ since $\chi\psi \neq \epsilon$. We have

$$\begin{aligned} g(\chi)g(\psi) &= \sum_{t,u\in\mathbb{F}_p} \chi(t)\psi(u)\zeta_p^{t+u} = \sum_{v\in\mathbb{F}_p} \zeta_p^v \sum_{t+u=v} \chi(t)\psi(u) \\ &= \psi(-1)\sum_{t\in\mathbb{F}_p}(\chi\psi)(t) + \sum_{v\in\mathbb{F}_p^\times} \zeta_p^v \sum_{r+s=1} \chi(vr)\psi(vs) \\ &= \sum_{v\in\mathbb{F}_p^\times}(\chi\psi)(v)\zeta_p^v \sum_{r+s=1}\chi(r)\psi(s) = g(\chi\psi)J(\chi,\psi) \end{aligned}$$

Relation between Jacobi sums and Gauss sums (II)

Lemma 3

Suppose $3 \big| p-1$, and let χ be a non-trivial cubic character on $\mathbb{F}_p$ (i.e., a character of order 3). Then

$$g(\chi)^3 = pJ(\chi,\chi)$$

Pf: Note that $\chi^2 = \overline{\chi}$ is the other non-trivial cubic character on $\mathbb{F}_p$. From a previous result, we have $g(\overline{\chi}) = \chi(-1)\overline{g(\chi)} = \overline{g(\chi)}$, where the last equality holds because χ is cubic. Thus, by the previous claim, we have

$$J(\chi,\chi) = \frac{g(\chi)^2}{g(\chi^2)} = \frac{g(\chi)^2}{g(\overline{\chi})} = \frac{g(\chi)^2}{\overline{g(\chi)}} == \frac{g(\chi)^3}{|g(\chi)|^2} = \frac{g(\chi)^3}{p}$$

$\square$

Eisenstein integers

Let $\omega = e^{2\pi i/3}$. We call $D = \mathbb{Z}[\omega]$ the ring of <u>Eisenstein integers</u>. Each element of D can be written uniquely as a sum $a + b\omega$, $a, b \in \mathbb{Z}$. D is a Euclidean domain under the norm

$$N(a + b\omega) = (a + b\omega)\overline{(a + b\omega)} = a^2 - ab + b^2$$

and hence it is a PID. The units in D are the elements of norm 1, and these are $1, \omega, \omega^2, -1, -\omega, -\omega^2$, i.e., the sixth roots of unity. Note that a prime in $\mathbb{Z}$ need not be prime in D. Indeed,

$$3 = -\omega^2(1 - \omega)^2$$
$$7 = (3 + \omega)(2 - \omega)$$

Primes in D

Let $\pi \in D$. If $N\pi$ is a prime in $\mathbb{Z}$, one easily shows that π is prime in D.

If π is prime in D, then $D/\pi D$ is a field with $N\pi$ elements, and either

1. $N\pi = p$ for some prime p in $\mathbb{Z}$, $p \equiv 1 \mod 3$
2. $N\pi = q^2$ for some prime q in $\mathbb{Z}$, $q \equiv 2 \mod 3$; in this case, π is an associate of q
3. $N\pi = 3$; in this case, π is an associate of $1 - \omega$

So for $\pi \not\sim 1 - \omega$ prime in D, $3 \big| N\pi - 1$. In addition, for each such π, $\exists\,!$ associate $\pi' \in D$ s.t. $\pi' \equiv 2 \ (3)$. This happens iff $\pi' = a + b\omega$ for some $a, b \in \mathbb{Z}$ satisfying

$$a \equiv 2 \quad (3)$$
$$b \equiv 0 \quad (3)$$

A prime $\pi' \in D$ satisfying $\pi' \equiv 2 \ (3)$ is called primary.

Lemma 4

Let p be a prime in $\mathbb{Z}$ satisfying $p \equiv 1\,(3)$, χ a non-trivial cubic character on $\mathbb{F}_p$. The Jacobi sum $J(\chi,\chi)$ is primary in D.

Pf: One verifies that indeed $J(\chi,\chi) \in D$. We have shown that $N(J(\chi,\chi)) = |J(\chi,\chi)|^2 = p$, so $J(\chi,\chi)$ is prime in D. In the ring of algebraic integers, by Lemma 3,

$$\begin{aligned} J(\chi,\chi) \equiv pJ(\chi,\chi) = g(\chi)^3 &= \left(\sum_{t\in\mathbb{F}_p} \chi(t)\zeta_p^t\right)^3 \\ &\equiv \sum_{t\in\mathbb{F}_p} \chi(t)^3\zeta_p^{3t} = \sum_{t\in\mathbb{F}_p^\times} \zeta_p^{3t} = -1 \end{aligned}$$

where the congruences are modulo (3). Similarly,

$$\overline{J(\chi,\chi)} = J(\overline{\chi},\overline{\chi}) \equiv -1 \;\; (3)$$

Setting $J(\chi,\chi) = a + b\omega$, we obtain from the above that

$$0 \equiv b(\omega - \overline{\omega}) \;=\; b\sqrt{-3}$$

which implies that $-3b^2 \equiv 0\,(9)$. Since every rational algebraic integer is an integer, this holds in $\mathbb{Z}$ as well, so $b \equiv 0\,(3)$, and consequently $a \equiv -1 \equiv 2\,(3)$. $\square$

Cubic residue symbol

Let π be a prime in D with $N\pi \neq 3$. One can show that for any $\alpha \in D$ s.t. $\pi \nmid \alpha$, $\exists\,!\, m \in \{0,1,2\}$ s.t. $\alpha^{(N\pi-1)/3} \equiv \omega^m \ (\pi)$. Thus, for any $\alpha \in D$, we may define the cubic residue character

$$\left(\frac{\alpha}{\pi}\right)_3 = \begin{cases} 0 & \alpha \equiv 0 \ (\pi) \\ \omega^m & \alpha^{(N\pi-1)/3} \equiv \omega^m \ (\pi) \end{cases}$$

For any $\alpha, \beta \in D$, we have

1. $(\alpha/\pi)_3 \equiv \alpha^{(N\pi-1)/3} \ \ (\pi)$
2. $\overline{(\alpha/\pi)_3} = (\alpha/\pi)_3^2 = (\alpha^2/\pi)_3$
3. $\overline{(\alpha/\pi)_3} = (\overline{\alpha}/\overline{\pi})_3$
4. if $\pi \nmid \alpha$, $(\alpha/\pi)_3 = 1$ iff $\alpha \equiv x^3 \ (\pi)$ for some $x \in D$
5. $(\alpha\beta/\pi)_3 \ = \ (\alpha/\pi)_3(\beta/\pi)_3$

Special case of cubic reciprocity

Note that properties (2) and (3) imply that for $n, q \in \mathbb{Z}$, q a prime in D,

$$\left(\frac{n}{q}\right)_3^2 = \left(\frac{n}{q}\right)_3$$

If $q \nmid n$, this implies $(n/q)_3 = 1$. Thus, if $p, q \in \mathbb{Z}$ are distinct primes in D,

$$\left(\frac{p}{q}\right)_3 = 1 = \left(\frac{q}{p}\right)_3$$

This is a special case of the cubic reciprocity law, which we will soon prove.

Cubic residue character

Note that the cubic residue symbol with denominator π does not distinguish between Eisenstein integers in the same congruence class modulo π, and thus defines a map $D/\pi D \to \mathbb{C}$. We call it the cubic residue character on $D/\pi D$ and denote it by χ_π. It is multiplicative by property (3) above.

If $N\pi = p \equiv 1 \ (3)$, then $D/\pi D$ is a field with p elements. $\mathbb{F}_p \cong D/\pi D$ through the map that sends n to the coset of n in $D/\pi D$. Thus, we may view the cubic residue character as a map $\mathbb{F}_p \to \mathbb{C}$. Since the former is multiplicative, this map is in fact a non-trivial cubic character on $\mathbb{F}_p$ in the sense defined previously.

Jacobi sum of a CRC

Lemma 5

Let π be primary in D with $N\pi = p \equiv 1$ (3). Then $J(\chi_\pi, \chi_\pi) = \pi$ and hence $g(\chi_\pi)^3 = p\pi$.

Pf: Since $N(J(\chi_\pi, \chi_\pi)) = p$ and $J(\chi_\pi, \chi_\pi)$ is primary by Lemma 4, it suffices to show that $\pi \big| J(\chi_\pi, \chi_\pi)$. We have

$$\begin{aligned} J(\chi_\pi, \chi_\pi) &= \sum_{a \in \mathbb{F}_p} \chi_\pi(a)\chi_\pi(1-a) \equiv \sum_{a \in \mathbb{F}_p} a^{(p-1)/3}(1-a)^{(p-1)/3} \\ &= \sum_{a \in \mathbb{F}_p} \sum_{j=0}^{2(p-1)/3} c_j a^j = \sum_{j=0}^{2(p-1)/3} c_j \sum_{a \in \mathbb{F}_p} a^j \end{aligned}$$

where the congruence is mod π. But since $j < p - 1$, $\sum_{a \in \mathbb{F}_p} a^j \equiv 0$ mod p, and hence mod π. $\square$

Law of cubic reciprocity I

Theorem

Let π_1, π_2 be primary in D, $N\pi_1 \neq N\pi_2$. Then

$$\left(\frac{\pi_1}{\pi_2}\right)_3 = \left(\frac{\pi_2}{\pi_1}\right)_3$$

Pf: We have already shown this to be true if $\pi_1, \pi_2 \in \mathbb{Z}$. We will prove it for the case $\pi_1 \in \mathbb{Z}$, $\pi_2 \notin \mathbb{Z}$. So $\pi_1 = q$ for some prime q in $\mathbb{Z}$, $q \equiv 2\ (3)$ and $N\pi_2 = p$ for some prime p in $\mathbb{Z}$, $p \equiv 1\ (3)$. Set $\pi_2 = \pi$. By Lemma 5, we have

$$\begin{aligned} g(\chi_\pi)^{q^2-1} &= (p\pi)^{\frac{q^2-1}{3}} \equiv \chi_q(p\pi) \quad (q) \\ &= \chi_q(p)\chi_q(\pi) = \chi_q(\pi) \end{aligned}$$

Law of cubic reciprocity II

and so, since $q^2 \equiv 1 \pmod 3$ and $\chi_\pi(t)$ is a cube root of unity for $t \in \mathbb{F}_p^\times$,

$$\begin{aligned}
\chi_q(\pi)g(\chi_\pi) &\equiv g(\chi_\pi)^{q^2} = \left(\sum_{t\in\mathbb{F}_p} \chi_\pi(t)\zeta_p^t\right)^{q^2} \equiv \sum_{t\in\mathbb{F}_p} \chi_\pi(t)^{q^2}\zeta_p^{q^2 t} \\
&= \sum_{t\in\mathbb{F}_p} \chi_\pi(t)\zeta_p^{q^2 t} = g_{q^2}(\chi_\pi) = \chi_\pi(q^{-2})g(\chi_\pi) \\
&= \chi_\pi(q)g(\chi_\pi)
\end{aligned}$$

where the congruences are mod q. Since $g(\chi_\pi)\overline{g(\chi_\pi)} = p \not\equiv 0 \pmod q$, we can divide both sides by $g(\chi)$ to obtain $\chi_q(\pi) \equiv \chi_\pi(q) \pmod q$. $\square$

Cubic reciprocity for non-primary primes

Note that the law of cubic reciprocity allows us to draw conclusions about non-primary primes as well. Suppose π_1', π_2' are primes in D, $N\pi_1', N\pi_2' \neq 3$, $N\pi_1' \neq N\pi_2'$. Then $\pi_j' = u_j \pi_j$ for some π_1, π_2 primary in D, u_1, u_2 units in D. Thus,

$$\begin{aligned}
\left(\frac{\pi_1'}{\pi_2'}\right)_3 &= \left(\frac{u_1\pi_1}{u_2\pi_2}\right)_3 = \left(\frac{u_1\pi_1}{\pi_2}\right)_3 \\
&= \left(\frac{u_1}{\pi_2}\right)_3 \left(\frac{\pi_1}{\pi_2}\right)_3 \equiv u_1^{(N\pi_2-1)/3} \left(\frac{\pi_1}{\pi_2}\right)_3 \quad (\pi_2) \\
&= u_1^{(N\pi_2-1)/3} \left(\frac{\pi_2}{\pi_1}\right)_3
\end{aligned}$$

by cubic reciprocity.

When does $x^3 - 2$ split?

We would like to know modulo which primes the polynomial $x^3 - 2$ splits (in the strong sense described in Weinstein's paper). It clearly does not split mod 2. Modulo 3, we have

$$x^3 - 2 = x^3 + 1 = (x + 1)^3$$

so $x^3 - 2$ does not split in this case.

For primes $p \equiv 1 \ (3)$, it is enough to show that $x^3 - 2$ has a root in $\mathbb{F}_p$ to show that it splits mod p; if a is one root, the others are $g^{(p-1)/3}a, g^{2(p-1)/3}a$, where g is a generator for $\mathbb{F}_p^\times$, and these are all distinct.

When does $x^3 - 2$ split? (Theorem) I

Claim

For $p \equiv 1 \ (3)$, $x^3 - 2$ splits mod p iff there are integers c, d s.t. $p = c^2 + 27d^2$.

Pf: Let $\pi = a + b\omega$ be primary in D s.t. $N\pi = p$. Note

$$\left(\frac{2}{\pi}\right)_3 = \left(\frac{\pi}{2}\right)_3 \overset{(2)}{\equiv} \pi^{(4-1)/3} = \pi \qquad (*)$$

Suppose $x^3 - 2$ splits mod p. Then it splits mod π. Thus, by $(*)$,

$$\pi \overset{(2)}{\equiv} \left(\frac{2}{\pi}\right)_3 = 1$$

When does $x^3 - 2$ split? (Theorem) II

In particular, b is even. b is also divisible by 3 since π is primary. We have $p = N\pi = a^2 - ab + b^2$ and so

$$4p = (2a - b)^2 + 3b^2 = 4c^2 + 4 \cdot 27d^2$$

where $c = a - b/2$ and $d = b/6$.
Now suppose $p = c^2 + 27d^2$. Then

$$(2a - b)^2 + 27(b/3)^2 = 4p = (2c)^2 + 27(2d)^2$$

Thus, $b/3 = \pm 2d$; in particular, b is even. Since π is prime, a must be odd, and so $\pi = a + b\omega \equiv 1 \ (2)$. Thus, by $(*)$, $x^3 - 2$ splits in $D/\pi D$, and hence in $\mathbb{F}_p$. $\square$