THE 2011 T-SHIRT: CUBIC RECIPROCITY

JEREMY BOOHER

Cubic reciprocity provides an answer to the question of which elements are cubes, just as quadratic reciprocity regards the squares modulo p. However, the natural setting for cubic reciprocity is not $\mathbb{Z}$, but rather $\mathbb{Z}[\zeta_3] = \mathbb{Z}[\frac{-1+\sqrt{-3}}{2}]$. This ring is known as the Eisenstein integers. This summer, you might have shown that this ring has unique prime factorization.

Let π be a prime in $\mathbb{Z}[\zeta_3]$ that does not divide 3. Consider $\mathbb{Z}[\zeta_3]_\pi$. The analogue of Euler's Theorem says that for any α relatively prime to π, $\alpha^{N\pi-1} \equiv 1 \mod \pi$. Hence $\alpha^{(N\pi-1)/3}$ is a cube root of unity modulo π. Since the cube roots of unity are distinct, factoring $x^{N\pi-1}-1$ shows there is a unique $m = 0, 1, 2$ such that $\alpha^{(N\pi-1)/3} \equiv \zeta_3^m \mod \pi$.

Definition 1. Let ζ_3^m be the unique root of unity such that $\alpha^{(N\pi-1)/3} \equiv \zeta_3^m \mod \pi$. Define the cubic residue character to be

$$\left(\frac{\alpha}{\pi}\right)_3 := \zeta_3^m.$$

If $\pi|3$, define $\left(\frac{\alpha}{\pi}\right) := 0$.

The cubic residue character shares many algebraic properties with the quadratic character. They are established in the same way. For example, it is straightforward to verify that $\left(\frac{\alpha}{\pi}\right)_3$ depends only on $\alpha \mod \pi$ and that the character is multiplicative. (See Problem Set 19, Problem 8.)

An added complication caused by moving from $\mathbb{Z}$ to $\mathbb{Z}[\zeta_3]$ is the additional units. The notion of a primary prime distinguishes between the various associates of π.

Definition 2. If π is a prime in $\mathbb{Z}[\zeta_3]$, then π is primary if $\pi \equiv 2 \mod 3$.

Lemma 3. *Let $N\pi = p \equiv 1 \mod 3$. Then exactly one of the associates of π is primary. If π is primary, so is $\overline{\pi}$.*

This will be proven in the next section. This provides enough notation to state the law.

Theorem 4 (Cubic Reciprocity)**.** *Let π_1 and π_2 be primary primes, $N\pi_1 \neq N\pi_2 \neq 3$. Then*

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

Remark 5. There are also supplemental laws for units and the prime dividing 3.

The proof of cubic reciprocity, first published by Eisenstein in 1844, uses Gauss and Jacobi sums. These are examples of a general class of sums called character sums. We first will explain the arithmetic of $\mathbb{Z}[\zeta_3]$, then introduce character sums before moving on to the proof of cubic reciprocity.

1. Preliminaries about $\mathbb{Z}[\zeta_3]$

We now prove Lemma 3, the result about primary primes.

Proof. Write $\pi = a + b\zeta_3$. The associates of π are π, $\zeta_3\pi$, $\zeta_3^2\pi$, $-\pi$, $-\zeta_3\pi$, and $-\zeta_3^2\pi$. In terms of a and b, these are

$$a + b\zeta_3, \quad -b + (a-b)\zeta_3, \quad (b-a) - a\zeta_3, \quad -a - b\zeta_3, \quad b + (b-a)\zeta_3, \quad (a-b) + a\zeta_3$$

Date: August 20, 2011.

Since $p = a^2 - ab + b^2 \equiv 1 \mod 3$, one of a and b is not a multiple of 3. If a is a multiple of 3, then either the third or sixth is primary depending on whether $b \equiv 1 \mod 3$. If a is not a multiple of 3, replacing π by $-\pi$ we may assume $a \equiv 2 \mod 3$. But $a^2 - ab + b^2 \equiv 1 \mod 3$ implies that $b(b-2) \equiv 0 \mod 3$. If $3|b$, then π is primary. If $b \equiv 2 \mod 3$, $b + (b-a)\zeta_3$ is primary.

For uniqueness, assume $a + b\zeta_3$ is primary. A direct inspection shows none of the other associates satisfies the correct congruence conditions.

If $\pi = a + b\zeta_3$ is primary, $\overline{\pi} = a + b(-1-\zeta_3) = a - b - b\zeta_3$ is obviously primary. □

Let π be a complex prime of norm p. This means that $p \equiv 1 \mod 3$. The residue field $\mathbb{Z}[\zeta_3]_\pi$ a finite field with $N(\pi) = p$ elements. But this is the same as $\mathbb{Z}_p$: simply map $1 \in \mathbb{Z}[\zeta_3]_\pi$ to $1 \in \mathbb{Z}_p$ and send multiples of 1 to the same multiple of 1. The cubic residue character modulo p is thus defined on $\mathbb{Z}_p$.

There is an interaction between the complex conjugation and the cubic residue character. In particular

$$\overline{\left(\frac{\alpha}{\pi}\right)_3} = \left(\frac{\alpha^2}{\pi}\right)_3 \quad \text{and} \quad \overline{\left(\frac{\alpha}{\pi}\right)_3} = \left(\frac{\overline{\alpha}}{\overline{\pi}}\right)_3.$$

To prove the first, note that $\left(\frac{\alpha}{\pi}\right)_3$ is a cube root of unity, so conjugation is the same as taking the multiplicative inverse which is the same as squaring. For the second, conjugating the expression

$$\pi | \alpha^{(N(\pi)-1)/3} - \left(\frac{\alpha}{\pi}\right)_3 \quad \text{gives} \quad \overline{\pi} | \overline{\alpha}^{(N(\pi)-1)/3} - \overline{\left(\frac{\alpha}{\pi}\right)_3}.$$

Since $N(\pi) = N(\overline{\pi})$, this implies $\overline{\left(\frac{\alpha}{\pi}\right)_3} = \left(\frac{\overline{\alpha}}{\overline{\pi}}\right)_3$.

In particular, if $n \in \mathbb{Z}$ and q is a rational prime that is prime in $\mathbb{Z}[\zeta_3]$, $\left(\frac{n}{q}\right)_3 = \overline{\left(\frac{n}{q}\right)_3} = 1$. The primes in $\mathbb{Z}$ that remain prime in $\mathbb{Z}[\zeta_3]$ are those for which $\left(\frac{-3}{q}\right) = -1$, which is equivalent to $q \equiv 2 \mod 3$. But in this case $3 \not| (q-1)$, the order of $(\mathbb{Z}/q\mathbb{Z})^\times$, so every element is a cube as the cubic character indicates.

2. Characters, Gauss and Jacobi Sums

Definition 6. In this setting, a character is a map $\chi : U_p \to \mathbb{C}^\times$ such that for $a, b \in U_p$, $\chi(a)\chi(b) = \chi(ab)$. Sometimes we extend this to a map $\chi : \mathbb{Z} \to \mathbb{C}^\times$ by setting $\chi(n) = \chi(n \mod p)$ if $n \neq 0 \mod p$, and $\chi(n) = 0$ if $p|n$.

For example, the Legendre symbol $a \to \left(\frac{a}{p}\right)$ is a character for U_p. A boring character is the trivial character which sends all non-zero elements to 1. If $p \equiv 1 \mod 3$, there is a cubic residue character as well.

The fundamental result about characters we will need is called the orthogonality of characters.

Proposition 7. *Let χ be a characters of $\mathbb{Z}_p$. Then*

$$\sum_{x \in U_p} \chi(x) = 0$$

unless χ is the trivial in character, in which case the sum is $p-1$.

Proof. Multiplication by $a \in U_p$ is a permutation of U_p, so

$$\sum_{x \in U_p} \chi(x) = \sum_{x \in U_p} \chi(ax) = \chi(a) \sum_{x \in U_p} \chi(x).$$

Since χ is non-trivial, there is an a with $\chi(a) \neq 1$, which forces the sum to be 0. If χ is trivial, the sum of $p-1$ ones is $p-1$. □

Corollary 8. *If χ and χ' are characters and $\chi \neq \chi'$, then*

$$\sum_{x \in U_p} \chi(x)\overline{\chi'(x)} = 0$$

Proof. The function $f(x) = \chi(x)\overline{\chi'(x)}$ is a character. □

Along the same lines, we have a result about roots of unity.

Proposition 9. *Let p be a prime and ζ_p a primitive pth root of unity (like $e^{2\pi i/p}$). Then for $a \in \mathbb{Z}$ $\sum_{k=0}^{p-1} \zeta_p^{ak} = 0$ if $a \neq 0 \mod p$, while if $a \equiv 0 \mod p$ the sum is p.*

Proof. The pth roots of unity are solutions to $x^p - 1 = 0$. The sum of the roots of this polynomial is 0 as the coefficient of x^{p-1} is zero. Raising the pth roots of unity to the a power permutes them unless a is a multiple of p, in which case they all map to 1. □

With these preliminaries about characters, we can now analyze Gauss and Jacobi sums.

Definition 10. Let p be a prime and χ a character $U_p \to \mathbb{C}^\times$. Let $\zeta_p = e^{2\pi i/p}$. The Gauss sum $g(\chi)$ is defined to be

$$g(\chi) := \sum_{x \in U_p} \chi(x)\zeta_p^x.$$

What is a root of unity raised to an integer modulo p? If we pick two integers n, m that are equivalent modulo p, we know $\zeta_p^n = \zeta_p^m$ as $\zeta_p^p = 1$. Thus define $\zeta_p^x = \zeta_p^n$ when n is any integer that reduces to $x \in U_p$. Note that we can equally well sum over $x \in \mathbb{Z}_p$, since we defined $\chi(x) = 0$ if $p|x$.

Definition 11. Let p be a prime and χ_1 and χ_2 characters $U_p \to \mathbb{C}^\times$. The Jacobi sum $J(\chi_1, \chi_2)$ is defined to be

$$J(\chi_1, \chi_2) := \sum_{x \in \mathbb{Z}_p} \chi_1(x)\chi_2(1-x)$$

Proposition 12. *Let χ and χ' be non-trivial characters modulo p. Then $|g(\chi)|^2 = p$ and if $\chi \neq (\chi')^{-1}$ then $J(\chi, \chi') = \frac{g(\chi)g(\chi')}{g(\chi\chi')}$.*

Proof. For the first assertion about the Gauss sum, we will use a "twisted" Gauss sum

$$g_a(\chi) = \sum_{x \in \mathbb{Z}_p} \chi(x)\zeta_p^{ax}.$$

Note that $g_0(\chi) = 0$ by the orthogonality relations. We will calculate

$$S = \sum_{a \in U_p} g_a(\chi)\overline{g_a(\chi)} = \sum_{a \in \mathbb{Z}_p} g_a(\chi)\overline{g_a(\chi)}$$

in two different ways. On one hand, as multiplying by $a \neq 0$ is a permutation of U_p so

$$g_a(\chi) = \chi(a)^{-1} \sum_{x \in \mathbb{Z}_p} \chi(a)\chi(x)\zeta_p^{ax} = \chi(a)^{-1} g(\chi).$$

Thus we can evaluate S as

$$S = \sum_{a \in U_p} g_a(\chi)\overline{g_a(\chi)} = \sum_{a \in U_p} \chi(a)^{-1} g(\chi)\overline{\chi^{-1}(a)g(\chi)} = |g(\chi)|^2 \sum_{a \in U_p} \chi(a)^{-1}\overline{\chi^{-1}(a)} = (p-1)|g(\chi)|^2.$$

On the other hand,

$$\begin{aligned} S &= \sum_{a \in \mathbb{Z}_p} \sum_{x,y \in \mathbb{Z}_p} \chi(x)\overline{\chi(y)}\zeta_p^{a(x-y)} \\ &= \sum_{x,y \in \mathbb{Z}_p} \chi(x)\overline{\chi(y)} \sum_{a \in \mathbb{Z}_p} \zeta_p^{a(x-y)}. \end{aligned}$$

When $x - y \neq 0$, the inner sum is a sum over all pth roots of unity, so equals 0. Otherwise it is the sum of p ones. Thus as $\chi(x)\overline{\chi(x)} = 1$ if $x \neq 0 \mod p$, we have

$$S = \sum_{x \in \mathbb{Z}_p} \chi(x)\overline{\chi(x)}(p-1) = p(p-1).$$

Equating the two expressions for S gives $|g(\chi)|^2 = p$.

For the second, note that

$$\begin{aligned} g(\chi)g(\chi') &= \left(\sum_x \chi(x)\zeta_p^x\right)\left(\sum_y \chi'(y)\zeta_p^y\right) \\ &= \sum_{x,y} \chi(x)\chi'(y)\zeta_p^{x+y} \\ &= \sum_t \sum_{x+y=t} \chi(x)\chi'(y)\zeta_p^t. \end{aligned}$$

Evaluating the sum over $x + y = t$ first, if $t = 0$ orthogonality of characters implies

$$\sum_{x \in \mathbb{Z}_p} \chi(x)\chi'(-x) = \chi'(-1) \sum_{x \in \mathbb{Z}_p} \chi(x)\chi'(x) = 0$$

since the product character $\chi\chi'$ is non-trivial. If $t \neq 0$, then $tx + ty = t$, so

$$\sum_{x+y=t} \chi(x)\chi'(y) = \sum_{x+y=1} \chi(tx)\chi(ty) = \chi(t)\chi'(t)J(\chi,\chi').$$

Substituting, we see that

$$g(\chi)g(\chi') = \sum_{t \neq 0} \chi(t)\chi'(t)J(\chi,\chi')\zeta_p^t = J(\chi,\chi')g(\chi\chi'). \qquad \square$$

3. The Proof of Cubic Reciprocity

We now specialize to the case we care about, that of the cubic residue character. Denote it by $\chi_\pi := \left(\frac{\cdot}{\pi}\right)_3$. The key fact about the Gauss and Jacobi sums is the following.

Theorem 13. *Let χ_π be the cubic residue character. Then $|g(\chi_\pi)|^2 = p$. Additionally, $g(\chi_\pi)^3 = pJ(\chi_\pi,\chi_\pi)$ and $J(\chi_\pi,\chi_\pi)$ is a primary prime in $\mathbb{Z}[\zeta_3]$.*

Proof. The first is just Proposition 12. For the second, note that χ_π^2 is not the trivial character, so by the same Proposition we also know that

$$g(\chi_\pi)^3 = g(\chi_\pi)g(\chi_\pi^2)J(\chi_\pi,\chi_\pi) = g(\chi_\pi)g(\overline{\chi_\pi})J(\chi_\pi,\chi_\pi) = pJ(\chi_\pi,\chi_\pi).$$

Finally, to show that $J(\chi_\pi,\chi_\pi)$ is primary, recall that $p \equiv 1 \mod 3$. Then we know

$$g(\chi_\pi)^3 = \left(\sum_{x \in \mathbb{Z}_p} \chi_\pi(x)\zeta_p^x\right)^3 \equiv \sum_{x \in \mathbb{Z}_p} \chi_\pi(x)^3\zeta_p^{3x} \mod 3.$$

However, as χ_π is a cubic character, $\chi_\pi(x)^3 = 1$ unless $\pi|x$. Therefore the sum simplifies and we conclude

$$pJ(\chi_\pi, \chi_\pi) = g(\chi)^3 \equiv \sum_{x\neq 0} \zeta_p^{3x} \equiv -1 \mod 3.$$

Since $p \equiv 1 \mod 3$, we conclude $J(\chi,\chi) \equiv -1 + 0\cdot\zeta_3 \mod 3$. This is exactly what is means to be primary. □

The first step in the proof is to find the factorization of $g(\chi_\pi)^3$.

Proposition 14. *If π is primary, $J(\chi_\pi, \chi_\pi) = \pi$ and consequently $g(\chi_\pi)^3 = \pi^2\overline{\pi}$.*

Proof. Let $J(\chi_\pi, \chi_\pi) = \pi'$. π' must be a primary prime dividing p, so it is either π or $\overline{\pi}$ as both are primary but none of the associates are primary. We need to rule out the later.

Directly from the definition and Euler's criterion

$$J(\chi_\pi, \chi_\pi) = \sum_x \chi_\pi(x)\chi_\pi(1-x) \equiv \sum_x x^{(p-1)/3}(1-x)^{(p-1)/3} \mod \pi.$$

However, we know that

$$\sum_{x\in\mathbb{Z}_p} x^j \equiv 0 \mod p$$

if $0 < j < p-1$ (see problem 30 on problem set 13, question 1). Summing each of the coefficients of the polynomial $x^{(p-1)/3}(1-x)^{(p-1)/3}$ separately, the sum over $\mathbb{Z}_p$ is 0. Since π divides p, $J(\chi_\pi,\chi_\pi) \equiv 0 \mod \pi$. Thus $\pi'|\pi$, so $\pi = \pi'$. The assertion about $g(\chi_\pi)^3$ then follows from Proposition 13. □

Since $g(\chi_{\pi_2})$ is a cube root of $p\pi$, $g(\chi_{\pi_2})^{N\pi_1-1}$ is $\chi_{\pi_1}(p\pi)$ modulo π_1. Raising things to the $N\pi_1$ power is very easy to do in characteristic $N\pi_1$, so an alternate expression can be obtained: cubic reciprocity falls out. This will be done in three cases.

First, if both π_1 and π_2 are primary rational primes, then $\left(\frac{\pi_1}{\pi_2}\right)_3 = \left(\frac{\pi_2}{\pi_1}\right)_3 = 1$ because the primes are invariant under conjugation (recall Section 1).

Secondly, consider the case when $\pi_1 = q$ is a primary rational prime and π_2 has norm p. From Proposition 13, raising $g(\chi_{\pi_2})^3$ to the $(q^2-1)/3$ power and using Euler's criteria we obtain

$$g(\chi_{\pi_2})^{q^2-1} \equiv \chi_q(p\pi_2) \mod q.$$

But since p and q are rational, $\chi_q(p) = 1$. Multiplying by $g(\chi_{\pi_2})$ gives

$$g(\chi_{\pi_2})^{q^2} \equiv \chi_q(\pi_2)g(\chi_{\pi_2}) \mod q. \tag{1}$$

On the other hand,

$$g(\chi_{\pi_2})^{q^2} \equiv \sum_{t\in\mathbb{Z}_p} \chi_{\pi_2}(t)^{q^2}\zeta_p^{q^2t} \mod q.$$

But χ_{π_2} is a cubic character and q is a prime, so $q^2 \equiv 1 \mod 3$ and hence

$$g(\chi_{\pi_2})^{q^2} \equiv \chi_{\pi_2}(q^{-2})\sum_t \chi_{\pi_2}(tq^2)\zeta_p^{tq^2} = \chi_{\pi_2}(q)g(\chi_{\pi_2}) \mod q. \tag{2}$$

Combining our two expressions for $g(\chi_{\pi_2})^{q^2}$ we obtain that

$$\chi_{\pi_2}(q)g(\chi_{\pi_2}) \equiv \chi_q(\pi_2)g(\chi_{\pi_2}) \mod q$$

and after canceling $g(\chi_\pi)$ that $\chi_q(\pi_2) = \chi_{\pi_2}(q)$ as desired.

The third case is when both π_1 and π_2 are complex primes with norms p_1 and p_2, primes congruent to 1 modulo 3. The same argument as above works, except we can no longer eliminate the analogue of the $\chi_q(p)$ term. Starting with $g(\chi_{\overline{\pi_1}})^3 = p\overline{\pi_1}$ and raising to the $(p_2-1)/3$ power, we obtain that

$$\chi_{\overline{\pi_1}}(p_2^2) = \chi_{\pi_2}(p_1\overline{\pi_1}).$$

Starting from $g(\chi_{\pi_2})^3 = p_2\pi_2$, we obtain

$$\chi_{\pi_2}(p_1^2) = \chi_{\pi_1}(p_2\pi_2).$$

Now note that $\chi_{\overline{\pi_1}}(p_2^2) = \chi_{\pi_1}(p_2)$ upon conjugating. But then combining these we have

$$\begin{aligned}\chi_{\pi_1}(\pi_2)\chi_{\pi_2}(p_1\overline{\pi_1}) &= \chi_{\pi_1}(\pi_2)\chi_{\overline{\pi_1}}(p_2^2)\\ &= \chi_{\pi_1}(\pi_2)\chi_{\pi_1}(p_2)\\ &= \chi_{\pi_2}(p_1^2)\\ &= \chi_{\pi_2}(\pi_1)\chi_{\pi_2}(p_1\overline{\pi_1}).\end{aligned}$$

Canceling the $\chi_{\pi_2}(p_1\overline{\pi_1})$ finishes the proof. □

The two key ingredients in this proof, are the factorization $g(\chi_\pi)^3 = \pi^2\overline{\pi}$ and the double calculation of $g(\chi_{\pi_2})^{N\pi_1-1}$ as a value of the cubic character and by directly expanding the Gauss sum modulo p. These can also be used to give an alternate proof of quadratic reciprocity.

Finally, there is the stronger question of when an integer is a cube of an *integer* modulo p. This is significantly more complicated, and leads to the study of rational reciprocity laws.

A good reference for this in subject matter is Ireland and Rosen's book. [1]

4. Exercises

(1) Prove that $\mathbb{Z}[\zeta_3]_\pi$ has $N(\pi)$ elements, and that for any α, $\alpha^{N(\pi)} \equiv \alpha \mod \pi$.
(2) Show that if p is a rational prime and $\left(\frac{-3}{p}\right) = -1$, then p is prime in $\mathbb{Z}[\zeta_3]$.
(3) Prove that $\mathbb{Z}[\zeta_3]$ has unique prime factorization.
(4) Let $p \equiv 1 \mod 4$. Let g be a generator for U_p. It has order a multiple of 4, so we can let $\chi_4(g^k) = i^k$. Use the fact that $|J\chi_4, \chi_4)|^2 = p$ for this character to show that p is a sum of two squares. Note that this provides an explicit method of finding them.
(5) Formulate and proof supplemental laws for the prime $1 - \zeta_3$ and the units of $\mathbb{Z}[\zeta_3]$. These are analogous to the special rules for the Legendre symbol of -1 and 2.
(6) Show that
$$\sum_{x \in \mathbb{Z}[\zeta_3]_\pi} x^j \equiv 0 \mod p$$
if $0 < j < N(\pi)$. Can you do this without first proving the existence of a generator?
(7) Generalize the proof of cubic reciprocity to give a proof of quadratic reciprocity. You should work over $\mathbb{Z}$, and look at the Gauss sum involving the quadratic residue character. How about fourth powers in $\mathbb{Z}[i]$?
(8) Find and prove a law for rational cubic reciprocity. You might try writing primes of the form $3n + 1$ as $\frac{1}{4}\left(L^2 + 27M^2\right)$.

References

1. Kenneth Ireland and Michael Rosen, *A classical introduction to modern number theory*, Springer, 1990.