CMM Power Round 2025: Jacobi

The main topic of this power round is Jacobi sums. These are useful mathematical objects with nature depending more on the defining character itself than the defining prime. For this reason, they often provide nontrivial information about the prime and are a natural setting for reciprocity laws, like quadratic and cubic reciprocity. The simplest case of a Jacobi sum is already naturally encoded by the aptly-named Jacobi symbol, which is explored early on in this power round, already having significant applications to quadratic forms. The connection between Jacobi sums and a more well-known relative, Gauss sums, is then explored, with applications of the latter. Then more sophisticated Jacobi sums are explored later on, proving to be a useful tool for counting problems and even certain divisibility statements.

You can use previous problem statements to prove a problem statement.

1 Jacobi Symbols

1.1 Introduction to Jacobi and Legendre Symbols

The Jacobi symbol is a generalization of the Legendre symbol to when the modulus is not necessarily a prime but any odd positive integer.

To understand Jacobi symbols, we first review the Legendre symbol and its properties.

For this entire power round, we will let p be an odd prime.

Definition 1.1. A *quadratic residue* modulo an integer n is a residue relatively prime to n that is congruent to the square of another residue $\pmod{n}$. A *quadratic nonresidue* $\pmod{n}$ is a residue relatively prime to n that is not congruent to the square of another residue.

Example 1.1. 2 is a quadratic residue $\pmod 7$ since $4^2 \equiv 2 \pmod 7$. We say that there are 3 quadratic residues $\pmod 7$: $\{1,2,4\}$. $1+7=8$ is also a quadratic residue $\pmod 7$, but when we count the quadratic residues, we only count the ones that are in $\{1,2,\dots,6\}$. 5 is not a quadratic residue $\pmod 9$ since no square is congruent to $5 \pmod 9$. The set of quadratic residues $\pmod 9$ is $\{1,4,7\}$.

Definition 1.2. Given an odd prime p and an integer a, the Legendre symbol $\left(\frac{a}{p}\right)$ is defined as:

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue modulo } p, \\ -1 & \text{if } a \text{ is a quadratic nonresidue modulo } p, \\ 0 & \text{if } p \mid a. \end{cases}$$

A powerful way to determine whether a is a quadratic residue modulo p is through Euler's criterion:

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

Theorem 1.3. For every prime p, there exists a *primitive root* modulo that prime, which is a residue r such that the powers of r achieve all nonzero residues $\pmod{p}$. In other words, the smallest integer $n>0$ such that $r^n \equiv 1 \pmod{p}$ is $p-1$.

If this primitive root is g, then all the nonzero residues $\pmod p$ can be expressed as $g, g^2, \ldots, g^{p-1}$.

Problem 1.1 (2 Points)**.** Prove that if $a \not\equiv 0 \pmod p$, then:

(a) (1 point) a is a quadratic residue $\pmod p$ if and only if $a^{\frac{p-1}{2}} \equiv 1 \pmod p$.

(b) (1 point) a is a quadratic nonresidue $\pmod p$ if and only if $a^{\frac{p-1}{2}} \equiv -1 \pmod p$.

Definition 1.4. Let $q = q_1 q_2 \cdots q_n$ be a product of odd primes (not necessarily distinct), and let a be an integer coprime to q. The Jacobi symbol $\left(\frac{a}{q}\right)$ is defined as:

$$\left(\frac{a}{q}\right) = \left(\frac{a}{q_1}\right) \cdot \left(\frac{a}{q_2}\right) \cdot \ldots \cdot \left(\frac{a}{q_n}\right),$$

where each $\left(\frac{a}{q_i}\right)$ is a Legendre symbol.

Remark. The Jacobi symbol coincides with the Legendre symbol when q is an odd prime.

Remark. Unlike the Legendre symbol, $\left(\frac{a}{q}\right) = 1$ does not necessarily mean a is a quadratic residue modulo q.

Problem 1.2 (2 Points)**.** Let a be an integer and n a positive integer. Let n factor into primes as $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$. Prove that a is a quadratic residue modulo n if and only if a is a quadratic residue modulo $p_i^{e_i}$ for all i.

Problem 1.3 (4 Points)**.** Let n be an odd positive integer and $p \nmid a, b$. Prove that:

(a) (1 point) There are $\frac{p-1}{2}$ (nonzero) quadratic residues modulo p.

(b) (2 points)

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right).$$

(c) (1 point)

$$\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right) \cdot \left(\frac{b}{n}\right).$$

Problem 1.4 (5 Points)**.** We can extend this idea to compute the number of quadratic residues modulo an odd composite number.

(a) (3 points) Prove that if p is an odd prime and a is a residue $\pmod{p^k}$ that's congruent to a quadratic residue $\pmod p$, then it is a quadratic residue $\pmod{p^k}$.

(b) (2 points) $\phi(n)$ is the Euler Totient Function, which is the number of relatively prime residues $\pmod n$ and is equal to

$$\phi(n) = n \prod_{p|n} \frac{p-1}{p}.$$

Prove that the number of quadratic residues $\pmod n$, for an odd positive integer n, is $\frac{\phi(n)}{2^m}$, if m is the number of distinct primes that divide n.

Problem 1.5 (2 Points)**.** Let p be an odd positive prime. Prove that the Jacobi symbol for -1 satisfies:

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 4, \\ -1 & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

Problem 1.6 (4 Points)**.** Prove that the Jacobi symbol for 2 satisfies:

$$\left(\frac{2}{n}\right) = \begin{cases} 1 & \text{if } n \equiv 1,7 \pmod 8, \\ -1 & \text{if } n \equiv 3,5 \pmod 8. \end{cases}$$

2 Dirichlet Characters, Gauss Sums, and Jacobi Sums

The Jacobi symbol is actually a special case of a larger family of functions, the Dirichlet characters. In this section, we'll focus on equations in $\pmod p$, for a prime p. The objective will be to compute the number of solutions to Diophantine equations in $\pmod p$, or a bound on it if the exact number is difficult to calculate. We will use tools such as Dirichlet characters, Gauss sums, and Jacobi sums.

2.1 Dirichlet Characters

Definition 2.1. A Dirichlet character χ of modulus m for an integer m is a function from residues $\pmod m$ to the set of complex numbers $\mathbb{C}$ satisfying:

- $\chi(a) = 0$ if and only if $\gcd(a,m) \neq 1$
- χ is periodic $\pmod m$, so $\chi(a) = \chi(a+m)$
- $\chi(ab) = \chi(a)\chi(b)$ for all residues $a, b \pmod m$

This is the general definition, but we'll only be using Dirichlet characters of prime moduli in this power round.

Remark. $\chi(1)\chi(1) = \chi(1)$, so $\chi(1) = 1$ or 0, but it must be 1 because $\gcd(1,m) = 1$. Also, $\chi(-1)\chi(-1) = \chi(1) = 1$, so $\chi(-1) = \pm 1$.

Since χ takes complex number values, we can compute its magnitude $|\chi|$, and the magnitude function is also in fact multiplicative since $|\chi(ab)| = |\chi(a)\chi(b)| = |\chi(a)||\chi(b)|$.

Remark. For a complex number ζ, $\overline{\zeta}$ is the complex conjugate of ζ, or the reflection of ζ over the real axis, and if $\zeta \neq 0$ then ζ^{-1} is the unique complex number such that $\zeta\zeta^{-1} = \zeta^{-1}\zeta = 1$.

Problem 2.1 (3 Points)**.** χ is a Dirichlet character of modulus p, and a is an integer such that $p \nmid a$.

(a) (1 point) Prove that the nonzero complex values achieved by a Dirichlet character χ of modulus p are all roots of unity (i.e. if $p \nmid a$ then some integer power of $\chi(a)$ equals 1).

(b) (1 point) Prove that $\chi(a^{-1}) = \chi(a)^{-1} = \overline{\chi}(a)$.

(c) (1 point) Prove that $\sum_{t=0}^{p-1} \chi(t)$ is equal to either 0 or $p-1$.

Since all the nonzero values achieved by a Dirichlet character are roots of unity, we can assign an order to it.

Definition 2.2. The *order* of a Dirichlet character χ of modulus p is the smallest integer n such that if $\gcd(a,m) = 1$ then $(\chi(a))^n = 1$.

Remark. Dirichlet characters of order 2 are called quadratic, order 3 cubic, and order 4 quartic.

Problem 2.2 (3 Points)**.** Let p be a prime, and g a primitive root $\pmod p$. Prove that:

(a) (1 point) If χ is a Dirichlet character of modulus p, then $\chi(a)$ is a $p-1$th root of unity for all a such that $p \nmid a$.

(b) (1 point) Dirichlet characters χ of modulus p are uniquely determined by the value of $\chi(g)$.

(c) (1 point) There are exactly $p-1$ distinct Dirichlet characters of modulus p.

Definition 2.3. We have two different types of identity Dirichlet characters: the character 1_1 of modulus 1 which takes the value 1 on all positive integers, and the characters 1_m of modulus $m > 1$ which take the value 0 on the residue $0 \pmod m$, and 1 on everything else.

Remark. The Jacobi symbol is a quadratic Dirichlet character: Since $\left(\frac{a}{q}\right)$ is the product of 1's and -1's, its square is 1, so the square of the Jacobi symbol is the identity character. Problem 1.3(c) shows that $\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$, so $\chi(ab) = \chi(a)\chi(b)$ holds. And the Jacobi symbol is equal to 0 if and only if a is 0 mod some prime dividing q, which is equivalent to $\gcd(a,q) \neq 1$.

Definition 2.4. Here, we say that $\chi^n = \mathbf{1}$ if χ is a Dirichlet character of modulus dividing p (so either p or 1), and $\chi \neq 1_p$, but $\chi^n = 1_1$ or 1_p.

Problem 2.3 (2 Points)**.** Prove that for all residues $a \pmod p$, the number of solutions (residues x) to $x^n \equiv a \pmod p$, which we will denote by $\#(x^n \equiv a)$, is equal to

$$\sum_{\chi^n=\mathbf{1}} \chi(a).$$

Problem 2.4 (4 Points)**.** Let p be an odd prime.

(a) (1 point) Prove that the only Dirichlet character of modulus p and order 2 is the Legendre symbol (the character that returns 1 on quadratic residues and -1 on quadratic nonresidues).

(b) (1 point) Prove that for a positive integer r, there exists a Dirichlet character of modulus p and order r if and only if $p \equiv 1 \pmod r$

(c) (2 points) Prove that if $p \equiv 1 \pmod n$, then there are exactly n Dirichlet characters of modulus p and order dividing n, and we can choose one of them to be χ_1 such that all the others can be expressed as powers of χ_1.

2.2 Gauss Sums

Definition 2.5. Given a Dirichlet character χ of modulus some prime p, for every integer a which is not a multiple of p, the Gauss Sum $g_a(\chi)$ is defined by

$$g_a(\chi) = \sum_{t=0}^{p-1} \chi(t) \left(e^{a\cdot 2\pi i/p}\right)^t.$$

If $\zeta_p = e^{2\pi i/p}$, then $g_a(\chi) = \sum_{t=0}^{p-1} \chi(t)\zeta_p^{at}$. This is the more common form that we will see often.

Problem 2.5 (3 Points)**.** χ is a Dirichlet character of modulus p. Prove that $g_a(\chi) = \chi(a^{-1})g_1(\chi)$.

2.3 Jacobi Sums

Jacobi sums work hand in hand with Gauss sums.

Definition 2.6. Given two Dirichlet characters χ_1 and χ_2 of modulus dividing p, the Jacobi sum $J(\chi_1, \chi_2)$ is defined by

$$J(\chi_1,\chi_2) = \sum_{t=0}^{p-1} \chi_1(t)\chi_2(1-t) = \chi_1(0)\chi_2(1) + \chi_1(1)\chi_2(0) + \cdots + \chi_1(p-1)\chi_2(2).$$

Problem 2.6 (4 points)**.** $\chi \neq 1_p$ is a Dirichlet character of modulus p. Prove the following useful Jacobi sums:

(a) (1 point) $J(1_1, 1_1) = p$

(b) (1 point) $J(1_1, \chi) = 0$

(c) (2 points) $J(\chi, \chi^{-1}) = -\chi(-1)$

Remark. If χ is the Legendre symbol, then $\chi = \chi^{-1}$.

Problem 2.7 (1 point)**.** Prove that if χ_1, χ_2 are Dirichlet characters of prime modulus p, then $\overline{J(\chi_1,\chi_2)} = J(\overline{\chi_1}, \overline{\chi_2})$, where the bar denotes complex conjugate.

Suppose $p \equiv 1 \pmod{n}$. Denote by $\#(x^n + y^n \equiv 1)$ the number of ordered pairs (x, y) of residues $\in \{0, 1, \ldots, p-1\}$ satisfying $x^n + y^n \equiv 1 \pmod{p}$. We can calculate it using Problem 2.3:

$$\#(x^n + y^n \equiv 1) = \sum_{a+b\equiv 1} \#(x^n \equiv a)\#(y^n \equiv b) = \sum_{a+b\equiv 1} \left(\sum_{\chi_1^n = \mathbf{1}} \chi_1(a)\right)\left(\sum_{\chi_2^n=\mathbf{1}} \chi_2(b)\right)$$

$$= \sum_{\chi_1^n=\chi_2^n=\mathbf{1}} \left(\sum_{a+b\equiv 1} \chi_1(a)\chi_2(b)\right) = \sum_{\chi_1^n=\chi_2^n=\mathbf{1}} J(\chi_1,\chi_2).$$

Thus, we get the following theorem:

Theorem 2.7.

$$\#(x^n + y^n \equiv 1) = \sum_{\chi_1^n=\chi_2^n=\mathbf{1}} J(\chi_1,\chi_2).$$

Problem 2.8 (4 Points)**.** Prove that if $p \equiv 1 \pmod{4}$ and χ is a character of modulus p and order 4, then:

(a) (2 points) $\#(x^4 + y^4 \equiv 1) = p + J(\chi,\chi) + \overline{J(\chi,\chi)} + 2J(\chi,\chi^2) + 2\overline{J(\chi,\chi^2)} - 3$ if -1 is congruent to a 4th power $\pmod{p}$.

(b) (2 points) $\#(x^4 + y^4 \equiv 1) = p + J(\chi,\chi) + \overline{J(\chi,\chi)} + 2J(\chi,\chi^2) + 2\overline{J(\chi,\chi^2)} + 1$ if -1 is not congruent to a 4th power $\pmod{p}$.

Theorem 2.8. χ_1 and χ_2 are Dirichlet characters of some prime modulus p, that are $\neq 1_p$.

- If $\chi_1\chi_2 \neq 1_p$, then $g_a(\chi_1)g_a(\chi_2) = J(\chi_1,\chi_2)g_a(\chi_1\chi_2)$.
- $g_a(\chi)g_a(\chi^{-1}) = \chi(-1)p$.

Problem 2.9 (4 Points)**.** Prove Theorem 2.8. *Hint: Expand the products.*

Problem 2.10 (3 Points)**.** Prove that $\overline{g_a(\chi)} = \chi(-1)g_a(\overline{\chi})$, if χ is a Dirichlet character of prime modulus.

Since $\chi^{-1} = \overline{\chi}$, and $\chi^2(-1) = 1$, $g_a(\chi)\overline{g_a(\chi)} = |g_a(\chi)|^2 = p$.

Theorem 2.9. If χ is a Dirichlet character of modulus p which is $\neq 1_p$, then $|g_a(\chi)| = p^{1/2}$.

Theorem 2.10. If χ_1,χ_2 are both Dirichlet characters of modulus p, and $\chi_1,\chi_2,\chi_1\chi_2 \neq 1_p$, then $|J(\chi_1,\chi_2)| = p^{1/2}$.

Problem 2.11 (2 Points)**.** Prove Theorem 2.10.

This gives us a bound on $J(\chi_1,\chi_2)$ for some χ_1,χ_2, which will be helpful when counting the number of solutions to a Diophantine equation.

Theorem 2.11. The norm function satisfies the Triangle Inequality. Given complex numbers $\{x_1,x_2,\dots x_n\}$,

$$\sum_{t=1}^{n}|x_t| \geq \left|\sum_{t=1}^{n}x_t\right|.$$

Thus, we can get from Problem 2.8 that

$$p-3-6\sqrt{p} \leq \#(x^4+y^4 \equiv 1) \leq p+1+6\sqrt{p},$$

meaning the existence of many solutions (x,y) to $x^4+y^4 \equiv 1$ for large p.

2.4 Generalizations to residues other than 1

We can calculate $\#(x^m+y^n \equiv r)$, the number of ordered pairs (x,y) of residues $\pmod p$ such that $x^m+y^n \equiv r \pmod p$ for $p \nmid r$, in a similar way:

$$\#(x^m+y^n \equiv r) = \sum_{a+b\equiv r}\#(x^m \equiv a)\#(y^n \equiv b) = \sum_{\chi_1^m=\chi_2^n=\mathbf{1}}\left(\sum_{a+b\equiv r}\chi_1(a)\chi_2(b)\right)$$
$$= \sum_{\chi_1^m=\chi_2^n=\mathbf{1}}\chi_1(r)\chi_2(r)\sum_{a+b\equiv 1}\chi_1(a)\chi_2(b) = \sum_{\chi_1^m=\chi_2^n=\mathbf{1}}\chi_1\chi_2(r)J(\chi_1,\chi_2).$$

The case where $r \equiv 0 \pmod p$ is slightly different, as it becomes

$$\#(x^m+y^m \equiv 0) = \sum_{\chi_1^m=\chi_2^n=\mathbf{1}}\sum_{a=0}^{p-1}\chi_1(a)\chi_2(-a) = \sum_{\chi_1^m=\chi_2^n=\mathbf{1}}\chi_2(-1)\sum_{a=0}^{p-1}\chi_1\chi_2(a),$$

and the $\sum_{a=0}^{p-1} \chi_1\chi_2(a)$ term disappears whenever $\chi_1\chi_2 \neq 1_p$.

Problem 2.12 (2 Points)**.** Let χ_1, χ_2 be Dirichlet characters of modulus p and orders 2 and 3. Prove that $\#(x^3 + y^2 \equiv 1) = p + J(\chi_1, \chi_2) + \overline{J(\chi_1, \chi_2)}$.

Problem 2.13 (4 Points)**.** Prove that if $p > 5$ is a prime, then

$$\#(x^2 + 2y^2 \equiv 5 \pmod p) = \begin{cases} p-1 & \text{if } p \equiv 1,3 \pmod 8, \\ p+1 & \text{if } p \equiv 5,7 \pmod 8. \end{cases}$$

Problem 2.14 (7 Points)**.** Let χ be a Dirichlet character of order 4, modulo a prime that's $1 \pmod 4$. Prove that:

- If $p \equiv 1 \pmod 8$, then $J(\chi, \chi)$ is a complex number $a + bi$ with a and b integers and $a \equiv 3 \pmod 4$ and $b \equiv 0 \pmod 4$.
- If $p \equiv 5 \pmod 8$, then $J(\chi, \chi)$ is a complex number $a + bi$ with a and b integers and $a \equiv 3 \pmod 4$ and $b \equiv 2 \pmod 4$.

Problem 2.15 (4 Points)**.** 2029 is prime. Let χ be a Dirichlet character of modulus 2029 and order 4. Let $J(\chi, \chi) = a + bi$. Determine, with proof, $(a, |b|)$.

We can also generalize to more than two terms.

2.5 Generalizations to more than 2 terms

Definition 2.12. For Dirichlet characters $\chi_1, \chi_2, \ldots, \chi_n$ of modulus p, we can generalize the Jacobi sum to include more terms:

$$J(\chi_1, \ldots, \chi_n) = \sum_{t_1 + \cdots + t_n \equiv 1} \chi_1(t_1)\chi_2(t_2)\ldots\chi_n(t_n)$$

and

$$J_0(\chi_1, \ldots, \chi_n) = \sum_{t_1 + \cdots + t_n \equiv 0} \chi_1(t_1)\chi_2(t_2)\ldots\chi_n(t_n).$$

Note that

$$J_0(\chi_1, \ldots, \chi_n) = \sum_{t_n} \left(\sum_{t_1 + \cdots + t_{n-1} \equiv -t_n} \chi_1(t_1)\chi_2(t_2)\ldots\chi_{n-1}(t_{n-1}) \right) \chi_n(t_n).$$

Furthermore,

$$\#(x_1^{e_1} + x_2^{e_2} + \cdots + x_n^{e_n} \equiv r) = \sum_{t_1 + \cdots + t_n \equiv r} \left(\sum_{\chi_1^{e_1} = \mathbf{1}} \chi_1(t_1) \right) \cdots \left(\sum_{\chi_n^{e_n} = \mathbf{1}} \chi_n(t_n) \right)$$

$$\sum_{\chi_1^{e_1} = \cdots = \chi_n^{e_n} = \mathbf{1}} \left(\sum_{t_1 + \cdots + t_n \equiv r} \chi_1(t_1)\ldots\chi_n(t_n) \right) = \begin{cases} \sum_{\chi_1^{e_1} = \cdots = \chi_n^{e_n} = \mathbf{1}} \chi_1\ldots\chi_n(r) J(\chi_1, \ldots, \chi_n) & \text{if } r \not\equiv 0 \pmod p, \\ \sum_{\chi_1^{e_1} = \cdots = \chi_n^{e_n} = \mathbf{1}} J_0(\chi_1, \ldots, \chi_n) & \text{if } r \equiv 0 \pmod p. \end{cases}$$

Problem 2.16 (17 Points)**.** $\chi_1, \chi_2, \dots, \chi_n$ are Dirichlet characters that are either 1_1 or have modulus p but are not 1_p. Prove that:

(a) (2 points) If $\chi_1 = \chi_2 = \cdots = \chi_n = 1_1$, then $J(\chi_1, \chi_2, \dots, \chi_n) = J_0(\chi_1, \chi_2, \dots, \chi_n) = p^{n-1}$.

(b) (3 points) If some but not all of the χ's are equal to 1_1, then $J(\chi_1, \chi_2, \dots, \chi_n) = J_0(\chi_1, \chi_2, \dots, \chi_n) = 0$.

(c) (4 points) If $\chi_1, \chi_2, \dots, \chi_n \neq 1_1$, and $\chi_1\chi_2\dots\chi_n \neq 1_p$, then $J_0(\chi_1, \chi_2, \dots, \chi_n) = 0$ and

$$g_a(\chi_1)g_a(\chi_2)\dots g_a(\chi_n) = J(\chi_1, \chi_2, \dots, \chi_n)g_a(\chi_1\chi_2\cdots\chi_n).$$

(d) (4 points) If $\chi_1, \chi_2, \dots, \chi_n \neq 1_1$ and $\chi_1\chi_2\dots\chi_n = 1_p$, then $J(\chi_1, \dots, \chi_n) = -\chi_n(-1)J(\chi_1, \dots, \chi_{n-1})$.

(e) (4 points) If $\chi_1, \chi_2, \dots, \chi_n \neq 1_1$, and $\chi_1\chi_2\dots\chi_n = 1_p$, then

$$J_0(\chi_1, \chi_2, \dots, \chi_n) = \chi_n(-1)(p-1)J(\chi_1, \dots, \chi_{n-1})$$

and

$$g_a(\chi_1)g_a(\chi_2)\dots g_a(\chi_n) = \chi_n(-1)pJ(\chi_1, \chi_2, \dots, \chi_{n-1}).$$

Because of Theorem 2.9 and Problem 2.16, we obtain the following facts:

Theorem 2.13. If $\chi_1, \chi_2, \dots, \chi_n \neq 1_p$ are Dirichlet characters of modulus p, then:

If $\chi_1\chi_2\dots\chi_n \neq 1_p$:

- $|J(\chi_1, \dots, \chi_n)| = p^{\frac{n-1}{2}}$
- $J_0(\chi_1, \dots, \chi_n) = 0$

If $\chi_1\chi_2\dots\chi_n = 1_p$:

- $|J(\chi_1, \dots, \chi_n)| = p^{\frac{n}{2}-1}$
- $|J_0(\chi_1, \dots, \chi_n)| = (p-1)p^{\frac{n}{2}-1}$

Problem 2.17 (5 Points)**.** Let $p \equiv 1 \pmod 4$ be a prime. $\#(x^4+y^4+z^4 \equiv r)$ denotes the number of ordered triples (x, y, z) of residues $\pmod p$ such that $x^4+y^4+z^4 \equiv r \pmod p$. Prove that:

- If $r \not\equiv 0 \pmod p$, then $|\#(x^4+y^4+z^4 \equiv r) - p^2| \leq 21p + 6\sqrt{p}$.
- If $r \equiv 0 \pmod p$, then $|\#(x^4+y^4+z^4 \equiv r) - p^2| \leq 6(p-1)\sqrt{p}$.

3 Harder Applications

3.1 Quadratic characters and Gauss Sums

We now consider the particular case of the quadratic character modulo p, i.e., the order 2 character ψ given by $\psi(a) = \left(\frac{a}{p}\right)$. For this section, we let ψ denote the quadratic character and assume that p is an odd prime.

Problem 3.1 (2 Points)**.** For $p \nmid a$, show that $g_a(\psi)^2 = \left(\frac{-1}{p}\right) \cdot p$.

The Gauss sum $g_a(\psi)$ has immediate applications to questions of counting solutions to Diophantine equations modulo p. Consider the following examples:

Problem 3.2 (2 Points)**.** Let $G_k = \sum_{n=0}^{p-1} \zeta_p^{n^k}$. Show that $g_1(\psi) = G_2$.

Problem 3.3 (6 Points)**.** For p an odd prime and $a_1, \ldots, a_n$ integers relative prime to p, compute the number of solutions to $a_1x_1^2 + \cdots + a_nx_n^2 \equiv 1 \pmod{p}$ in terms of the quadratic residue $\left(\frac{a_1 \cdots a_n}{p}\right)$.

Keeping the notation from Problem 3.2, we can also compute G_4, in the spirit of Problem 2.14.

Problem 3.4 (5 Points)**.** Let $p \equiv 1 \pmod{4}$ be a prime and let a and b be integers such that $a^2 + b^2 = p$ and $a \equiv -(2/p) \pmod{4}$. Show that

$$(G_4 - G_2)^2 = 2\left(\frac{2}{p}\right)(p + aG_2)$$

Note that Problem 3.1 implies that $G_2 = \varepsilon \cdot \sqrt{p}$, where $\varepsilon = \pm 1$ if $p \equiv 1 \pmod{4}$ and $\varepsilon = \pm i$ if $p \equiv 3 \pmod{4}$. In fact, the sign of G_2 is determined by a famous result due to Gauss:

Theorem 3.1. $G_2 = \begin{cases} \sqrt{p} & \text{if } p \equiv 1 \pmod{4} \\ i\sqrt{p} & \text{if } p \equiv 3 \pmod{4} \end{cases}$

Problem 3.5 (5 Points)**.** Show that for $p \equiv 3 \pmod{4}$,

$$\sum_{n=1}^{\infty} \frac{1}{2n-1}\left(\frac{2n-1}{p}\right) = \frac{\pi}{4\sqrt{p}}\left(\sum_{k=1}^{(p-1)/2}\left(\frac{k}{p}\right) - \sum_{k=(p+1)/2}^{p-1}\left(\frac{k}{p}\right)\right)$$

We can now make the following observation. For any $s > 1$, the following summation factorizes as

$$\sum_{n=1}^{\infty} \frac{1}{(2n-1)^s}\left(\frac{2n-1}{p}\right) = \prod_{q>2} \frac{1}{1 - q^{-s}\left(\frac{q}{p}\right)}$$

Taking a limit as $s \to 1$, we deduce that

$$\sum_{n=1}^{\infty} \frac{1}{2n-1}\left(\frac{2n-1}{p}\right) > 0 \implies \sum_{k=1}^{(p-1)/2}\left(\frac{k}{p}\right) > 0$$

That is to say, there are more quadratic residues between 1 and $\frac{p-1}{2}$ than nonquadratic residues.

3.2 Quintic Sums

Define $K(\chi) = \chi(4)J(\chi,\chi)$. In this section, we will explore how we can compute $K(\chi)$ in the case where χ is a character of order 10. The answer shall be expressed in terms of integers that make up a quadratic form expression for the prime p. This technique applies to other cases where χ is of small order, such as 3 or powers of 2.

Problem 3.6 (5 Points)**.** Show that any nontrivial character χ satisfies $K(\chi) = J(\chi,\psi)$.

Problem 3.7 (3 Points)**.** Show that if χ is of order $2k$ for some positive integer k, then

$$K(\chi) = \left(\frac{-1}{p}\right) K(\chi^{k-1})$$

Now suppose that $p \equiv 1 \pmod{10}$ and that χ is a character of order 10.

Problem 3.8 (8 Points)**.** Show that $\frac{1}{2}\text{Re } K(\chi)$ is an algebraic integer when $p \equiv 3 \mod 4$ and $\frac{1}{2}(\text{Re } K(\chi)+1)$ is an algebraic integer when $p \equiv 1 \mod 4$. Here, Re denotes the real part of a complex numbers. (Hint: Show that $K(\chi)+K(\chi^6)$ is twice an algebraic integer, and relate it with χ.)

Problem 3.9 (12 Points)**.** In the setting of the previous problem, show that

(a) (6 points) There exist integers a,b,c,d such that

$$K(\chi) = a + b\sqrt{5} + ci\sqrt{5+2\sqrt{5}} + di\sqrt{5-2\sqrt{5}}$$

(b) (6 points) Show that for any $p \equiv 1 \pmod{10}$, there exists integers a,b,c,d such that

- $a^2 + 5b^2 + 5c^2 + 5d^2 = p$
- $ab + cd = d^2 - c^2$
- $a \equiv (-1)^{(p+1)/2} \pmod{5}$.

4 An Application to Binomial Coefficients

We will now demonstrate a relationship between binomial coefficients and Jacobi sums. Throughout this section, we will set $p = 3k+1$ a prime (so that $p \equiv 1 \mod 3$).

Problem 4.1 (10 Points)**.** Let S be the number of residues $a \not\equiv -1, 0 \mod p$ such that $a, a+1$ are both cubic residues $\mod p$. Show that $\binom{2k}{k} \equiv -8 - 9S \mod p$.

Obtaining relatively weak information on S will already give rather nontrivial results. For example, if one can show that $S > 0$ for some p, then since $0 \le S \le p-2$ (since S is counting a subset of residue classes $\mod p$ excluding $-1, 0$), we know that $\binom{2k}{k} \not\equiv -8 \mod p$, and so $p | \binom{2k}{k} + 8$ precisely when $S = 0$. This turns out to occur only when $p = 7$ or 13.

To begin our analysis of S, the crucial insight is that we can analyze S in terms of Jacobi sums. In particular, we have the following result:

Problem 4.2 (2 Points)**.** Let T be the number of solutions (x,y) of residues $\pmod p$ to $x^3+y^3 \equiv 1 \mod p$. Then $T = 9S+6$.

From this we immediately conclude that $\binom{2k}{k} \equiv -T-2 \mod p$, but now T is something directly amenable to Jacobi sums. In particular, let χ be a cubic character $\mod p$. Then we have the following formula for T:

Problem 4.3 (2 Points)**.** Show that $T = p-2+J(\chi,\chi)+\overline{J(\chi,\chi)}$.

Plugging this into our congruence, we already get the remarkable result that $\binom{2k}{k} \equiv -J(\chi,\chi)-\overline{J(\chi,\chi)} \mod p$, which can be rewritten as $\binom{2k}{k} \equiv -2\mathrm{Re}(J(\chi,\chi)) \mod p$. Furthermore, we can now solve our initial problem:

Problem 4.4 (3 Points)**.** Show that $p | \binom{2k}{k}+8$ if and only if $p = 7, 13$.

We will be able to evaluate $J(\chi,\chi)$ explicitly. Recall that a primitive third root of unity ω is a complex number such that $\omega^3 = 1$ but $\omega \neq 1$ (hence either $e^{\frac{2\pi i}{3}}$ or $e^{\frac{4\pi i}{3}}$). Firstly, we have the following characterization for $J(\chi,\chi)$:

Problem 4.5 (10 Points)**.** Let ω be a primitive third root of unity. Then we have that $J(\chi,\chi) = a+b\omega$, where $a \equiv 2 \mod 3$ and $b \equiv 0 \mod 3$ are integers. (Hint: It might help to relate the Jacobi sum to a Gauss sum.)

This will already be enough to determine the precise value of $J(\chi,\chi)$. In particular, we have the following result:

Problem 4.6 (6 Points)**.** Show the following:

- (1 point) We have $a^2-ab+b^2 = p$.
- (5 points) Show that (a,b) and $(a-b,-b)$ are the only pairs (m,n) of integers such that $m \equiv 2 \mod 3, n \equiv 0 \mod 3$, and $m^2-mn+n^2 = p$.

This problem then immediately implies that $J(\chi,\chi) = a+b\omega$ or $a-b-b\omega$ (and given one value, the other is taken by $J(\overline{\chi},\overline{\chi}) = \overline{J(\chi,\chi)}$, completely determining the value of $J(\chi,\chi)$). Note that picking a different primitive third root of unity, namely ω^2, also swaps which of the two corresponds to that $J(\chi,\chi)$ value.

Another consequence of Problem 4.5 is a criterion for when 2 is a cubic residue modulo p:

Problem 4.7 (5 Points)**.** Show that 2 is a perfect cube modulo p if and only if p is expressible as x^2+27y^2 for integers x and y. (Hint: Prove $K(\chi)$ is of the form $m+ni\sqrt{3}$ for integers m and n; compare with Problem 4.5.)

Returning to our congruence problem, now we can obtain an explicit solution. In particular, our final result is the following:

Problem 4.8 (2 Points)**.** Show that $\binom{2k}{k} \equiv -2a+b \mod p$.

A key point to notice here is that in Problem 4.5, we could have chosen ω^2 instead of ω, in which case we would get $a+b(-1-\omega^2) = a-b-b\omega^2$, corresponding to the other solution to $m^2-mn+n^2 = p$. However, the congruence of Problem 4.7 should be independent of the choice of the root of unity (and thus the choice of a,b), and this is exactly what happens: we have $-2a+b = -2(a-b)-b$. Thus the congruence is actually capturing a linear symmetry among a,b.

As an example, we have that $7 = 2^2-2\cdot 3+3^2$, and so in this case $a = 2, b = 3$, which implies that $\binom{4}{2} \equiv 2(-2)+3 \equiv -1 \mod 7$. However, we may have also taken $a = 2-3 = -1, b = -3$, which yields the same result. Similarly, for $p = 13$, we have that $a = -4, b = -3$, giving $\binom{8}{4} \equiv (-2)(-4)+(-3) \equiv 5 \mod 13$. However, once again we could take $a = -1, b = 3$, and still get $-2a+b = 5$, giving the congruence.

With this finer description, we can now see which residues are relatively sparse. For example, we have that:

Problem 4.9 (3 Points)**.** Let $r \not\equiv 2 \mod 3$ be a fixed integer. Show that there are only finitely many p such that $\binom{2k}{k} \equiv r \mod p$.

This is a generalization of the case of $r = -8$, which we already carefully handled in Problem 4.4, and this elucidates a more general phenomenon.