1. Definitions, Basic Properties

Let $p$ be an odd prime. (However, essentially everything to follow here works verbatim upon replacing $p$ by $q = p^e$.)

**Definition 1.1.** The character group (or dual group) modulo $p$ is

$$\hat{\mathbb{F}}_p^\times = \{ \text{homomorphisms} : \mathbb{F}_p^\times \rightarrow \mathbb{C}^\times \}$$

$$= \{ \chi : \mathbb{F}_p^\times \rightarrow \mathbb{C}^\times \mid \chi(ab) = \chi(a)\chi(b) \text{ for all } a, b \in \mathbb{F}_p^\times \}. $$

The group law on the character group is that for all $\chi, \lambda \in \hat{\mathbb{F}}_p^\times$, the product $\chi \lambda$ is given by

$$(\chi \lambda)(a) = \chi(a)\lambda(a) \text{ for all } a \in \mathbb{F}_p^\times. $$

Examples of characters are

- The trivial character $\varepsilon : \mathbb{F}_p^\times \rightarrow \mathbb{C}^\times$, $\varepsilon(a) = 1$ for all $a \in \mathbb{F}_p^\times$.

- The quadratic character $\left( \frac{\cdot}{p} \right) : \mathbb{F}_p^\times \rightarrow \mathbb{C}^\times$, $a \mapsto \left( \frac{a}{p} \right)$. (Here if we change $p$ to $q$ then the Legendre symbol becomes the Jacobi symbol.)

- Recall that $\mathbb{F}_p^\times$ is cyclic of order $p - 1$. Choose a generator $g$ of $\mathbb{F}_p^\times$, and let $\zeta_{p-1} = e^{2\pi i/(p-1)}$. Define $\chi_0 : \mathbb{F}_p^\times \rightarrow \mathbb{C}^\times$, $\chi_0(g^n) = \zeta_{p-1}^n$, $n = 0, 1, \ldots, p - 2$.

Note that $\chi_0$ is not canonical, but depends on the choice of $g$.

**Proposition 1.2** (Basic Character Properties). For any character $\chi$ modulo $p$, the following properties hold.

1. $\chi(1_{\mathbb{F}_p}) = 1_{\mathbb{C}}$.
2. $\chi(a)^{p-1} = 1_{\mathbb{C}}$ for all $a \in \mathbb{F}_p^\times$.
3. $\chi(a^{-1}) = \chi(a)^{-1} = \overline{\chi(a)}$ for all $a \in \mathbb{F}_p^\times$, and $\overline{\chi}$ is again a character.

The properties follow immediately from the facts that $\chi$ is a homomorphism and $\mathbb{F}_p^\times$ is finite.

**Proposition 1.3.** The character group $\hat{\mathbb{F}}_p^\times$ is cyclic.
Proof. Let \( g \) generate \( \hat{\mathbb{F}_p^\times} \). Then any \( \chi \in \hat{\mathbb{F}_p^\times} \) is determined by its value on \( g \), and this value must be \( \chi(g) = \zeta_p^k \) for some \( k \in \{0, \ldots, p-2\} \). Thus \( \chi = \chi_o^{\hat{e}} \), showing that \( \chi_o \) generates \( \hat{\mathbb{F}_p^\times} \). \( \square \)

Since \( \mathbb{F}_p^\times \) and \( \hat{\mathbb{F}_p^\times} \) are both cyclic of order \( p-1 \), they are isomorphic. But they are noncanonically isomorphic, meaning that there is no one preferred way to choose the isomorphism between them.

2. An Image and a Kernel

Consider a finite cyclic group, written additively, \( G = \mathbb{Z}/q\mathbb{Z} \). Let \( e \) be a positive integer, and consider the endomorphism \( x \mapsto e x \) of \( G \). To study its image and its kernel, let

\[
\hat{e} = \text{gcd}(e, q).
\]

Thinking in terms of ideals quickly shows that the endomorphism has as its image

\[
\langle e + q\mathbb{Z} \rangle = \{ me + nq + q\mathbb{Z} \} = \langle \hat{e} + q\mathbb{Z} \rangle,
\]

the unique order-\( q/\hat{e} \) subgroup of \( G \). Consequently its kernel is the unique order-\( \hat{e} \) subgroup,

\[
\langle q/\hat{e} + q\mathbb{Z} \rangle,
\]

and the endomorphism is \( \hat{e} \)-to-1 to its image. Note that the image, the kernel, and the multiplicity depend only on \( \hat{e} = \text{gcd}(e, q) \), rather than on the original datum \( e \).

3. A Basic Counting Formula

Let \( e \) be a positive integer, and let \( u \in \mathbb{F}_p \). This section will use characters to count the solutions \( x \) modulo \( p \) of the equation \( x^e = u \). Let the symbol \( N \) denote solution-count,

\[
N(x^e = u) = |\{ x \in \mathbb{F}_p : x^e = u \}|.
\]

We want to express \( N(x^e = u) \) in terms of characters. The previous section has shown that the kernel and the image of the endomorphism \( x \mapsto x^e \) of \( \mathbb{F}_p^\times \) depend only on \( \text{gcd}(e, p-1) \). So we freely assume that \( e \mid p-1 \). Since the endomorphism \( x \mapsto x^e \) has kernel of order \( e \), it follows that \( N(x^e = u) \in \{0, e\} \) for all \( u \in \mathbb{F}_p^\times \).

Consider the order-\( e \) subgroup of \( \hat{\mathbb{F}_p^\times} \), consisting of the characters \( \chi \) such that \( \chi^e = \hat{\varepsilon} \),

\[
\{ \hat{\varepsilon}, \chi_0^{(p-1)/e}, \chi_0^{2(p-1)/e}, \ldots, \chi_0^{(e-1)(p-1)/e} \}.
\]

(For example, if \( e = 2 \) then the subgroup is \( \{ \hat{\varepsilon}, (\cdot/p) \} \).) If \( x^e = u \) for some \( x \) then

\[
\sum_{\chi^e = \hat{\varepsilon}} \chi(u) = \sum_{\chi^e = \hat{\varepsilon}} \chi(x^e) = \sum_{\chi^e = \hat{\varepsilon}} \chi(x)^e = \sum_{\chi^e = \hat{\varepsilon}} 1 = e = N(x^e = u).
\]

On the other hand, if \( x^e \neq u \) for all \( x \in \mathbb{F}_p^\times \) then \( u \) takes the form \( u = g^{Qe+R} \) where \( 0 < R < e \). Therefore,

\[
\chi_0^{(p-1)/e}(u) = \chi_0^{(p-1)/e}(g^{Qe+R}) = \zeta_p^{(Qe+R)(p-1)/e} = \zeta_p^{R(p-1)/e} \neq 1,
\]

and thus the general identity

\[
(1) \quad \sum_{\chi^e = \hat{\varepsilon}} \chi(a) = \chi_0^{(p-1)/e}(a) \sum_{\chi^e = \hat{\varepsilon}} \chi(a) \quad \text{for any } a \in \mathbb{F}_p^\times
\]
(because multiplying by \( \chi_o^{(p-1)/e} \) permutes the characters in the order-\( e \) subgroup of \( \hat{\mathbb{F}_p}^\times \)) shows that in particular
\[
\sum_{\chi^e=u} \chi(u) = 0 = N(x^e = u).
\]
Finally, extend characters modulo \( p \) to all of \( \mathbb{F}_p \) by defining
\[
\varepsilon(0) = 1, \quad \chi(0) = 0 \text{ if } \chi \neq \varepsilon.
\]
Then
\[
\sum_{\chi^e=u} \chi(0) = 1 = N(x^e = 0).
\]
And so we have in all cases,
\[
\text{If } p = 1 \mod e \text{ then } \sum_{\chi^e=u} \chi(u) = N(x^e = u) \text{ for any } u \in \mathbb{F}_p.
\]
As explained above, the formula in the box contains the information to compute \( N(x^e = u) \) for all positive values of \( e \), not only for divisors \( e \) of \( p - 1 \).

4. The Orthogonality Relations

**Proposition 4.1.** The following two relations hold.

\[
\sum_{a \in \mathbb{F}_p^\times} \chi(a) = \begin{cases} p - 1 & \text{if } \chi = \varepsilon, \\ 0 & \text{if } \chi \neq \varepsilon \end{cases}
\]

and

\[
\sum_{\chi \in \hat{\mathbb{F}_p}^\times} \chi(a) = \begin{cases} p - 1 & \text{if } a = 1_{\mathbb{F}_p}, \\ 0 & \text{if } a \neq 1_{\mathbb{F}_p}. \end{cases}
\]

**Proof.** Both identities are proved essentially as we proved identity (1) in the previous section. The first identity is clear if \( \chi = \varepsilon \). Otherwise \( \chi(a_o) \neq 1 \) for some \( a_o \in \mathbb{F}_p^\times \), and so (since multiplying by \( a_o \) permutes \( \hat{\mathbb{F}_p}^\times \))
\[
\sum_{a \in \mathbb{F}_p^\times} \chi(a) = \sum_{a \in \mathbb{F}_p^\times} \chi(a_o a) = \chi(a_o) \sum_{a \in \mathbb{F}_p^\times} \chi(a),
\]
showing that the sum vanishes. The second identity is clear if \( a = 1_{\mathbb{F}_p} \). Otherwise \( \chi_o(a) \neq 1 \) because \( \chi_o \) sends only \( 1_{\mathbb{F}_p} \) to \( 1_\mathbb{C} \), and so (since multiplying by \( \chi_o \) permutes \( \hat{\mathbb{F}_p}^\times \))
\[
\sum_{\chi \in \hat{\mathbb{F}_p}^\times} \chi(a) = \sum_{\chi \in \hat{\mathbb{F}_p}^\times} (\chi_o \chi)(a) = \chi_o(a) \sum_{\chi \in \hat{\mathbb{F}_p}^\times} \chi(a),
\]
and again the sum vanishes.

The same methods apply to additive characters \( \psi : \mathbb{F}_p \to \mathbb{C}^\times \), meaning that \( \psi(a+b) = \psi(a) \psi(b) \) for all \( a, b \in \mathbb{F}_p \). For example, the character \( \psi(a) = e^{2\pi i a/p} = \zeta_p^a \) for \( a \in \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} \) is additive. Thus we have
\[
\sum_{a \in \mathbb{F}_p} \psi(a) = \begin{cases} p & \text{if } \psi = \varepsilon, \\ 0 & \text{if } \psi \neq \varepsilon \end{cases}
\]
and

\[ \sum_{\psi \in \hat{F}_p} \psi(a) = \begin{cases} p & \text{if } a = 0_F, \\ 0 & \text{if } a \neq 0_F. \end{cases} \]

5. **Gauss Sums Again**

Every character \( \chi \) modulo \( p \) has an associated **Gauss sum**,  
\[ \tau(\chi) = \sum_{t \in F_p^\times} \chi(t) \zeta_p^t. \]

Note that \( \chi \) is a character of the multiplicative group \( F_p^\times \) while \( t \mapsto \zeta_p^t \) is a nontrivial character of the additive group \( F_p \). By orthogonality of additive characters,  
\[ \tau(\varepsilon) = 0. \]

For \( \chi \neq \varepsilon \) we may sum over \( t \in F_p^\times \) because \( \chi(0) = 0 \). In this case compute, exchanging the order of summation and replacing \( t \) by \( tu \) in the inner sum at the second step, exchanging the order of summation again at the third, and using orthogonality for the fourth,

\[ \tau(\chi) \tau(\overline{\chi}) = \sum_{t,u \in F_p^\times} \chi(tu^{-1}) \zeta_p^{tu} = \sum_{u,t \in F_p^\times} \chi(u^{-1}tu) \zeta_p^{u+tu} \]
\[ = \sum_{t \in F_p^\times} \chi(t) \sum_{u \in F_p} \zeta_p^{(1+t)u} - \sum_{t \in F_p^\times} \chi(t). \]

By orthogonality of characters of \( F_p \), the first term is \( \chi(-1)p \), and by orthogonality of characters of \( F_p^\times \), the second term is 0. Thus overall,

\[ \tau(\chi) \tau(\overline{\chi}) = \chi(-1)p. \]

Also, still for \( \chi \neq \varepsilon \), noting for the last step that \( \overline{\chi}(-1) = \chi(-1) \),

\[ \tau(\overline{\chi}) = \sum_{t \in F_p^\times} \overline{\chi}(t) \zeta_p^t = \chi(-1) \sum_{t \in F_p^\times} \chi(-t) \zeta_p^{-t} = \chi(-1) \tau(\chi). \]

This gives the third of our results,

\[ \tau(\varepsilon) = 0, \quad \tau(\chi) \tau(\overline{\chi}) = \chi(-1)p, \quad |\tau(\chi)| = \sqrt{p}. \]

6. **More Counting Formulas; Jacobi Sums**

Still working over \( \mathbb{F}_p \), we now want the solution-count

\[ N(a_1 x_1^{e_1} + a_2 x_2^{e_2} + \cdots + a_r x_r^{e_r} = b) \]

where each \( a_i \) is nonzero and each \( e_i \) divides \( p - 1 \).

We expect the solution-count to be roughly \( p^{r-1} \) since the condition imposes one constraint on \( r \) variables from \( \mathbb{F}_p \).

The following two quantities will arise in the course of calculating the solution-count.

**Definition 6.1.** Let \( \chi_1, \cdots, \chi_r \) be characters modulo \( p \). The corresponding **Jacobi sums** are

\[ J_0(\chi_1, \cdots, \chi_r) = \sum_{\vec{a} : \sum_{i=0}^r a_i = 0} \chi_1(u_1) \cdots \chi_r(u_r) \]
and
\[ J(\chi_1, \cdots, \chi_r) = \sum_{\mathbf{u} : \sum u_i = 1} \chi_1(u_1) \cdots \chi_r(u_r). \]

Recall the basic counting formula for \( e | p - 1, \)
\[ N(x^e = u) = \sum_{\chi^e = \epsilon} \chi(u). \]

Using the basic formula, compute a sprawling expression for the solution-count that
we seek,
\[
N(a_1 x_1^{e_1} + a_2 x_2^{e_2} + \cdots + a_r x_r^{e_r} = b)
= \sum_{\mathbf{u}_i : \sum u_i = b} \prod_{i=1}^r N(x_i^{e_i} = a_i^{-1} u_i)
= \sum_{\mathbf{u}_i : \sum u_i = b} \prod_{i=1}^r \sum_{\chi_i(a_i^{-1} u_i) \chi_i^r = \epsilon} \chi_i(a_i^{-1} u_i)
= \sum_{\mathbf{u}_i : \sum u_i = b} \chi_1(a_1^{-1} u_1) \cdots \chi_r(a_r^{-1} u_r) \sum_{\mathbf{u}_i : \sum u_i = b} \chi_1(u_1) \cdots \chi_r(u_r)
\]

And now inspecting the definition of the two types of Jacobi sum shows that the
desired counting formula is
\[
N(a_1 x_1^{e_1} + a_2 x_2^{e_2} + \cdots + a_r x_r^{e_r} = b)
= \sum_{\mathbf{\chi}_i : \text{each } \chi_i^r = \epsilon} \chi_1(a_1^{-1}) \cdots \chi_r(a_r^{-1}) \cdot \begin{cases} J_0(\chi_1, \cdots, \chi_r) & \text{if } b = 0, \\ (\chi_1 \cdots \chi_r)(b) J(\chi_1, \cdots, \chi_r) & \text{if } b \neq 0. \end{cases}
\]

7. A Quadratic Example

Let \( p \) be an odd prime. We count the points of the unit circle modulo \( p, \)
\[ x^2 + y^2 = 1. \]

The general counting formula gives
\[ N(x^2 + y^2 = 1) = \sum_{\chi_1^2 = \chi_2^2 = \epsilon} J(\chi_1, \chi_2). \]

The only relevant characters are \( \epsilon \) and \((\cdot/p)\). Thus in fact,
\[ N(x^2 + y^2 = 1) = J(\epsilon, \epsilon) + 2J(\epsilon, \left(\frac{\cdot}{p}\right)) + J\left(\left(\frac{\cdot}{p}\right), \left(\frac{\cdot}{p}\right)\right). \]
But \( J(\varepsilon, \varepsilon) = p \) (and we expect this to be the dominant term in the answer), while \( J(\varepsilon, (\cdot)/p) = 0 \) by the second orthogonality relation, and finally,

\[
J\left( \left( \begin{array}{c} \varepsilon \\ p \end{array} \right), \left( \begin{array}{c} \varepsilon \\ p \end{array} \right) \right) = \sum_{u_1+u_2=1} \left( \frac{u_1}{p} \right) \left( \frac{u_2}{p} \right) = \sum_{u_1 \neq 0,1} \left( \frac{u_1(1-u_1)}{p} \right).
\]

Since we are working with the quadratic character, we may replace the first \( u_1 \) in the numerator by \( u_1^{-1} \) to get

\[
J\left( \left( \begin{array}{c} \cdot \\ p \end{array} \right), \left( \begin{array}{c} \cdot \\ p \end{array} \right) \right) = \sum_{u_1 \neq 0,1} \left( \frac{u_1^{-1}-1}{p} \right) = -\left( \frac{-1}{p} \right).
\]

In sum,

\[
N(x^2 + y^2 = 1) = p - \left( \frac{-1}{p} \right) = \begin{cases} p - 1 & \text{if } p = 1 \text{ mod } 4, \\ p + 1 & \text{if } p = 3 \text{ mod } 4. \end{cases}
\]

What’s secretly happening here is that the unit circle modulo \( p \) world really should lie in projective space, where it has \( p+1 \) points for all \( p \). Depending on the quadratic character of \(-1\) modulo \( p \) (i.e., depending on \( p \) mod 4), two of the points are projective or all of them are affine. We explain this next.

8. A Generalization of the Quadratic Example by Other Means

Let \( d \in \mathbb{Z} \) be squarefree. So in particular, \( d \neq 0 \). The quadratic curve

\[
Q : x^2 - dy^2 = 1
\]

homogenizes to

\[
Q_{\text{hom}} : x^2 - dy^2 = z^2.
\]

The maps

\[
\mathbb{P}^1 \longrightarrow Q_{\text{hom}}, \quad [s, t] \longmapsto [s^2 + dt^2, 2st, s^2 - dt^2]
\]

and

\[
Q_{\text{hom}} \longrightarrow \mathbb{P}^1, \quad \begin{cases} [x, y, z] \longmapsto [x + z, y] & \text{if } [x, y, z] \neq [1, 0, -1], \\ [1, 0, -1] \longmapsto [0, 1] \end{cases}
\]

are readily checked to be inverses provided that \( 2 \neq 0 \) and \( d \neq 0 \).

Let \( p \mid 2d \) be prime and work over the field \( \mathbb{F}_p \). Then

\[
|Q_{\text{hom}}(\mathbb{F}_p)| = |\mathbb{P}^1(\mathbb{F}_p)| = p + 1.
\]

Furthermore, all points of \( \mathbb{P}^1(\mathbb{F}_p) \) map to affine points \([s, s, 1]\) of \( Q_{\text{hom}} \) except for the points \([s, 1] : s^2 = d\). There are no exceptional points if \( (d/p) = -1 \) and there are two exceptional points if \( (d/p) = 1 \). Thus the number of affine points is

\[
|Q(\mathbb{F}_p)| = \begin{cases} p - 1 & \text{if } (d/p) = 1, \\ p + 1 & \text{if } (d/p) = -1 \\ = p - (d/p). \end{cases}
\]

This is the formula that we obtained by Jacobi sums for \( d = -1 \).
9. Analysis of the Jacobi Sums

We will establish the following table.

| \( \bar{\chi} \) | \( J(\bar{\chi}) \) | \( |J(\bar{\chi})| \) | \( J_0(\bar{\chi}) \) | \( |J_0(\bar{\chi})| \) |
|---------------|----------------|-----------------|----------------|----------------|
| \( \varepsilon \) | \( p^{r-1} \) | \( p^{r-1} \) | \( p^{r-1} \) | \( p^{r-1} \) |
| \( (\bar{\varepsilon}, \bar{\chi}_{r-s}) \) | \( 0 \) | \( 0 \) | \( 0 \) | \( 0 \) |
| \( \prod_i \chi_i \neq \varepsilon \) | \( \frac{\tau(\chi_1) \cdots \tau(\chi_r)}{\tau(\chi_1 \cdots \chi_r)} \) \( p^{(r-1)/2} \) | \( 0 \) | \( 0 \) | \( 0 \) |
| \( \prod_i \chi_i = \varepsilon \) | \( \frac{-\tau(\chi_1) \cdots \tau(\chi_r)}{p} \) \( p^{r-2} \) | \( (p-1) \frac{\tau(\chi_1) \cdots \tau(\chi_r)}{p} \) | \( (p-1)p^{r/2-1} \) | \( (p-1)p^{r/2-1} \) |

The table shows that

\[
|N(a_1x_1^{e_1} + a_2x_2^{e_2} + \cdots + a_rx_r^{e_r} = b)| - p^{r-1} \leq \begin{cases} M_0 p^{r/2-1} + M_1 p^{(r-1)/2} & \text{if } b \neq 0, \\ M_0 (p-1)p^{r/2-1} & \text{if } b = 0, \end{cases}
\]

where there are \( e_i - 1 \) possibilities for each \( \chi_i \), and

\[
M_0 = |\{ \bar{\chi} : \prod_i \chi_i = \varepsilon \}| \quad \text{and} \quad M_1 = |\{ \bar{\chi} : \prod_i \chi_i \neq \varepsilon \}|.
\]

To derive the various results in the table, begin by noting that its top row is clear because both \( J(\varepsilon) \) and \( J_0(\varepsilon) \) sum the value 1 over \( r \)-tuples \( u \) such that \( \sum_i u_i = 1 \) or \( \sum_i u_i = 0 \). In both cases, the first \( r-1 \) constants \( u_i \) are free and then \( u_r \) is determined. The second row of the table follows similarly from the second orthogonality relation. For example,

\[
\sum_{u_2} \varepsilon(u_2) \cdots \sum_{u_r} \chi_r(u_r) \varepsilon(1 - u_2 - \cdots - u_r) = 0.
\]

Next compute that when none of the characters is trivial,

\[
J_0(\bar{\chi}) = \sum_{u_r \in \mathbb{F}_p^\times} \left[ \sum_{u_1 + \cdots + u_{r-1} = -u_r} \chi_1(u_1) \cdots \chi_{r-1}(u_{r-1}) \right] \chi_r(u_r)
\]

\[
= \sum_{u_r \in \mathbb{F}_p^\times} \left[ \sum_{u_1 + \cdots + u_{r-1} = 1} \chi_1(u_1) \cdots \chi_{r-1}(u_{r-1}) \right] (\chi_1 \cdots \chi_{r-1})(-1)(\chi_1 \cdots \chi_r)(u_r)
\]

\[
= (\chi_1 \cdots \chi_{r-1})(-1)J(\chi_1, \cdots, \chi_{r-1}) \sum_{u_r \in \mathbb{F}_p^\times} (\chi_1 \cdots \chi_r)(u_r)
\]

\[
= \begin{cases} 0 & \text{if } \prod_i \chi_i \neq \varepsilon, \\ (p-1)\chi_r(-1)J(\chi_1, \cdots, \chi_{r-1}) & \text{if } \prod_i \chi_i = \varepsilon. \end{cases}
\]

This gives the right half of the third row, and since \( \chi_1 \cdots \chi_{r-1} \neq \varepsilon \) it reduces the right half of the fourth row to the left half of the third row. We will return to the right half of the fourth row below.
For the left half of the third row, compute that when \( \prod \chi_i \neq \varepsilon \) (quoting the \( J_0 \) calculation just carried out),

\[
\tau(\chi_1) \cdots \tau(\chi_r) = \sum_{t_1, \ldots, t_r \in \mathbb{F}_p} \chi_1(t_1) \cdots \chi_r(t_r) \zeta_p^{t_1 + \cdots + t_r} \\
= \sum_{u \in \mathbb{F}_p} \sum_{t \in u} \chi_1(t_1) \cdots \chi_r(t_r) \zeta_p^u \\
= J_0(\bar{\chi}) + J(\bar{\chi}) \sum_{u \in \mathbb{F}_p^n} (\chi_1 \cdots \chi_r)(u) \zeta_p^u \\
= J(\bar{\chi}) \tau(\chi_1 \cdots \chi_r) \text{ since the } J_0 \text{ term vanishes.}
\]

This establishes the left half of the third row. Also, returning to the right half of the fourth row, we have \( \chi_1 \cdots \chi_{r-1} \neq \varepsilon \), and so we may now quote the left half of the third row as we continue the calculation of \( J_0 \) in the nonzero case,

\[
J_0(\bar{\chi}) = (p - 1)\chi_r(-1)J(\chi_1, \cdots, \chi_{r-1}) \\
= (p - 1)\chi_r(-1) \frac{\tau(\chi_1) \cdots \tau(\chi_{r-1})}{\tau(\chi_1 \cdots \chi_{r-1})} \cdot \frac{\tau(\chi_r)}{\tau(\chi_r)} \\
= (p - 1)\chi_r(-1) \frac{\tau(\chi_1) \cdots \tau(\chi_{r-1})}{\tau(\chi_r)} \\
= (p - 1) \frac{\tau(\chi_1) \cdots \tau(\chi_r)}{p}.
\]

Finally, for the left half of the fourth row, modify the calculation of the product \( \tau(\chi_1) \cdots \tau(\chi_r) \) to take into account the relation \( \prod \chi_i = \varepsilon \), using the fact that now

\[
\sum_{u \in \mathbb{F}_p^n} (\chi_1 \cdots \chi_r)(u) \zeta_p^u = \tau(\varepsilon) - 1 = -1,
\]

and using the relevant \( J_0 \)-value now that we know it,

\[
\tau(\chi_1) \cdots \tau(\chi_r) = J_0(\bar{\chi}) - J(\bar{\chi}) \\
= (p - 1) \frac{\tau(\chi_1) \cdots \tau(\chi_r)}{p} - J(\bar{\chi}).
\]

From here basic algebra gives the desired value of \( J(\bar{\chi}) \).

10. A Cubic Example

Let \( p \) be prime. We want to count the points of the cubic Fermat curve modulo \( p \),

\[
x^3 + y^3 = 1.
\]

If \( p = 2 \mod 3 \) then cubing is an automorphism modulo \( p \), and the counting problem reduces to \( x + y = 1 \), which trivially has \( p \) solutions. So from now on we assume that we are in the interesting case, \( p = 1 \mod 3 \).

Again referring to the general counting formula, we have

\[
N(x^3 + y^3 = 1) = \sum_{\chi_1^3 = \chi_2 = \varepsilon} J(\chi_1, \chi_2).
\]
This time the relevant characters are $\varepsilon$, $\chi$, and $\overline{\chi}$, where $\chi(g) = \zeta_3$. Expand the formula,
\[ N(x^3 + y^3 = 1) = J(\varepsilon, \varepsilon) + 2(J(\varepsilon, \chi) + J(\varepsilon, \overline{\chi})) + 2J(\chi, \chi) + J(\chi, \overline{\chi}) + J(\overline{\chi}, \overline{\chi}). \]
According to the table,
\[ N(x^3 + y^3 = 1) = p - 2\tau(\chi)\tau(\overline{\chi})/p + 2\text{Re}(J(\chi, \chi)). \]
We know that $\tau(\chi)\tau(\overline{\chi}) = \chi(-1)p$, and in fact $\chi(-1) = 1$ since $\chi^3 = 1$. Therefore,
\[ N(x^3 + y^3 = 1) = p - 2 + 2\text{Re}(J(\chi, \chi)). \]

Gauss reasoned as follows. We know that
\[ J(\chi, \chi) = a + b\omega, \quad a, b \in \mathbb{Z}, \quad \omega = \zeta_3. \]
We are looking for $2\text{Re}(J(\chi, \chi)) = 2a - b$. By the table, $|J(\chi, \chi)|^2 = p$, i.e.,
\[ a^2 - ab + b^2 = p. \]
Knowing $p$ and knowing that $|a + b\omega|^2 = p$ does not uniquely determine $a$ and $b$. Indeed, the six values $\alpha + \beta\omega$ in values $\pm(a + b\omega), \pm\omega(a + b\omega), \pm\omega^2(a + b\omega)$ satisfy $|\alpha + \beta\omega|^2 = p$. But as we will see soon in our studies of the Eisenstein integer ring $\mathbb{Z}[\omega]$, exactly one of these six values $\alpha + \beta\omega$ is such that $\alpha = 2 \equiv 1 \pmod{3}$ and $\beta = 0 \pmod{3}$. These congruences give
\[ 4p = (2\alpha - \beta)^2 + 3\beta^2 = A^2 + 27B^2, \quad A = 2\alpha - \beta = 1 \pmod{3}, \quad B = b/3. \]

Note that finding the integers $A$ and $B$ is an easy search because both terms of $A^2 + 27B^2$ are positive. (By contrast, searching for $\alpha$ and $\beta$ such that $p = \alpha^2 - \alpha\beta + \beta^2$ is not so simple because of the minus sign, and searching for $\alpha$ and $\beta$ such that $p = (\alpha - \beta/2)^2 + 3\beta^2/4$ involves quarter-integers.) Below we will show that the conditions $4p = A^2 + 27B^2$, $A = 1 \pmod{3}$ determine $A$ uniquely. Returning to the Jacobi sum $J(\chi, \chi)$, we want to show that among the six Eisenstein integers $a + b\omega$ with $p = a^2 - ab + b^2$, the Jacobi sum is in fact the distinguished one such that $a = 2 \pmod{3}$ and $b = 0 \pmod{3}$. Compute,
\[ a + b\omega = J(\chi, \chi) = \frac{\tau(\chi)^2}{\tau(\overline{\chi})} = \frac{\tau(\chi)^3}{\tau(\chi)\tau(\overline{\chi})} = \frac{\tau(\chi)^3}{\chi(-1)p} = \frac{\tau(\chi)^3}{p}. \]

Consider the resulting equality $pa + pb\omega = \tau(\chi)^3$, working modulo 3. On the one hand,
\[ pa + pb\omega \equiv_3 a + b\omega, \]
and on the other hand,
\[ \tau(\chi)^3 \equiv_3 \sum_{t \in \mathbb{F}_p^*} \chi(t)^3 \xi_p^t = \sum_{t \in \mathbb{F}_p^*} \xi_p^t = -1, \]
Thus $a = 2 \pmod{3}$ and $b = 0 \pmod{3}$, as claimed. This shows that the desired value $2\text{Re}(J(\chi, \chi)) = 2a - b$ is $A$. We have proved

**Theorem 10.1** (Gauss). Let $p = 1 \pmod{3}$. The number of points on the cubic Fermat curve $x^3 + y^3 = 1$ is
\[ N(x^3 + y^3 = 1) = p - 2 + A \quad \text{where} \quad 4p = A^2 + 27B^2, \quad A = 1 \pmod{3}. \]
For example, let $p = 103$, so that $4p = 412$. The only values $27B^2$ less than $4p$ are 27, 108, 243. Next, $412 - 27 = 405$ and $412 - 108 = 304$ are not squares but $412 - 243 = 169 = (\pm 13)^2$. Thus $A = 13$. The equation $x^3 + y^3 = 1 \mod 103$ has $103 - 2 + 13 = 114$ solutions.

The homogeneous Fermat equation of degree 3 is $x^3 + y^3 = z^3$. For a prime $p \neq 1 \mod 3$ the equation has $p + 1$ projective solutions: the $p$ affine solutions $[x : y : 1]$ arising from the circumstance that the cubing map is an automorphism modulo $p$, and one non-affine solution $[-1 : 1 : 0]$ arising from the circumstance that $-1$ is the unique cube root of $-1$ modulo $p$. Certainly $[1 : 0 : 0]$ is not a solution.

On the other hand, for a prime $p = 1 \mod 3$, the equation has $p - 2 + 13$ affine solutions according to Gauss, and also it has three non-affine solutions $[x : 1 : 0]$ because now $-1$ has three cube roots modulo $p$. Again $[1 : 0 : 0]$ is not a solution.

So a revision of Gauss’s result is that counting projectively modulo any prime $p$ (and replacing $A$ from above by its additive inverse here),

$$N(x^3 + y^3 = z^3) = p + 1 - A,$$

$$\begin{cases} 4p = A^2 + 27B^2, & A = 2 \mod 3 \quad \text{if } p = 1 \mod 3, \\ A = 0 & \text{if } p \neq 1 \mod 3. \end{cases}$$

The cubic Fermat curve is an elliptic curve whose conductor is $27$. According to the Modularity Theorem, the value $A = A_p$ in the previous display must also be the $p$th Fourier coefficient of a certain modular form, a cusp form whose level matches the conductor. There exists only one suitable cusp form of level 27, whose Fourier coefficients can be found in tables online, and one can check that indeed each $p$th Fourier coefficient matches the value $A_p$ in the previous display.

Finally, we discuss the fact that for $p = 1 \mod 3$, the condition

$$4p = A^2 + 27B^2, \quad A = 1 \mod 3$$

holds for a unique $A$. Soon we will see that there exists an Eisenstein integer $\pi = a + b\omega$ with $a = 2 \mod 3$ and $b = 0 \mod 3$ such that

$$p = a^2 - ab + b^2,$$

and furthermore the only other such Eisenstein integer is $\pi' = (a - b) - b\omega$. Rearranging the previous display,

$$p = (a - b/2)^2 + 3(b/2)^2, \quad a = 2 \mod 3, \quad b = 0 \mod 3.$$ 

Note that $(a - b) - (b^2)/2 = a - b^2/2$, showing that the quantity $a - b^2/2$ in the previous display depends only on $p$, not on a choice between $\pi$ and $\pi'$. Multiplying the display by 4 gives a condition of the desired form $4p = A^2 + 27B^2$ with $A = 1 \mod 3$.

On the other hand, consider a representation $4p = A^2 + 27B^2$ with $A = 1 \mod 3$. Set $b = 3B$ to get $4p = A^2 + 3B^2$. Note that $b$ has the same parity as $A$. Now set $a = (A + b)/2$, so that $2a = A + b = 1 \mod 3$, giving $a = 2 \mod 3$. This gives a representation of $p$ as in the previous display. Thus $A = 2a - b$ for a suitable $a + b\omega$, and we have seen that this quantity is unique to $p$. 
