

MATH 361: NUMBER THEORY — ELEVENTH LECTURE

The subjects of this lecture are characters, Gauss sums, Jacobi sums, and counting formulas for polynomial equations over finite fields.

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 \mathfrak{p} is

$$\begin{aligned} \widehat{\mathbf{F}_p^\times} &= \{\text{homomorphisms } \mathbf{F}_p^\times \longrightarrow \mathbf{C}^\times\} \\ &= \{\chi : \mathbf{F}_p^\times \longrightarrow \mathbf{C}^\times \mid \chi(ab) = \chi(a)\chi(b) \text{ for all } a, b \in \mathbf{F}_p^\times\}. \end{aligned}$$

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

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

Examples of characters are

- The **trivial character**

$$\varepsilon : \mathbf{F}_p^\times \longrightarrow \mathbf{C}^\times, \quad \varepsilon(a) = 1 \text{ for all } a \in \mathbf{F}_p^\times.$$

- The **quadratic character**

$$\left(\frac{\cdot}{p}\right) : \mathbf{F}_p^\times \longrightarrow \mathbf{C}^\times, \quad a \longmapsto \left(\frac{a}{p}\right).$$

(Here if we change p to q then the Legendre symbol becomes the Jacobi symbol.)

- Recall that \mathbf{F}_p^\times is cyclic of order $p - 1$. Choose a generator g of \mathbf{F}_p^\times , and let $\zeta_{p-1} = e^{2\pi i/(p-1)}$. Define

$$\chi_o : \mathbf{F}_p^\times \longrightarrow \mathbf{C}^\times, \quad \chi_o(g^n) = \zeta_{p-1}^n, \quad n = 0, 1, \dots, p - 2.$$

Note that χ_o is not canonical, but depends on the choice of g .

Proposition 1.2 (Basic Character Properties). For any character χ modulo p , the following properties hold.

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

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

Proposition 1.3. The character group $\widehat{\mathbf{F}_p^\times}$ is cyclic.

Proof. Let g generate \mathbf{F}_p^\times . Then χ is determined by its value on g , and this value must be $\chi(g) = \zeta_{p-1}^k$ for some $k \in \{0, \dots, p - 2\}$. Thus $\chi = \chi_o^k$, showing that χ_o generates $\widehat{\mathbf{F}_p^\times}$. □

Since \mathbf{F}_p^\times and $\widehat{\mathbf{F}_p^\times}$ 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. A BASIC COUNTING FORMULA

Let e be a positive integer, and let $u \in \mathbf{F}_p$. 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,

$$N(x^e = u) = |\{x \in \mathbf{F}_p : x^e = u\}|.$$

We want to express $N(x^e = u)$ in terms of characters.

We may take $1 \leq e \leq p-1$ because of the rule $x^p = x$ in \mathbf{F}_p . Write such e as

$$e = \hat{e}f, \quad \hat{e} = (e, p-1), \quad (f, p-1) = 1.$$

Then the endomorphism $x \mapsto x^f$ of \mathbf{F}_p^\times is an automorphism, because $Af + B(p-1) = 1$ for some integers A and B , so that $(x^f)^A = x$ for all $x \in \mathbf{F}_p^\times$. Also $0^f = 0$, and so the map $x \mapsto x^f$ bijects \mathbf{F}_p . The change of variable $x \mapsto x^f$ shows that for any $u \in \mathbf{F}_p$,

$$N(x^e = u) = N(x^{\hat{e}} = u).$$

That is, to count the solutions of $x^e = u$, we may assume that $e \mid p-1$.

With the problem simplified, now let e be any positive divisor of $p-1$. Note that the equation $x^e = 1$ has e solutions in \mathbf{F}_p^\times , to wit,

$$\{1, g^{(p-1)/e}, g^{2(p-1)/e}, \dots, g^{(e-1)(p-1)/e}\}.$$

It follows that for any $u \in \mathbf{F}_p^\times$, if the equation $x^e = u$ has *any* solutions in \mathbf{F}_p^\times then it has e solutions. That is, $N(x^e = u) \in \{0, e\}$ for all $u \in \mathbf{F}_p^\times$.

The order- e subgroup of $\widehat{\mathbf{F}_p^\times}$, the characters χ such that $\chi^e = \varepsilon$, will play a role in the calculation. (Explicitly, the subgroup is

$$\{\chi^e = \varepsilon\} = \langle \chi_o^{(p-1)/e} \rangle = \{\varepsilon, \chi_o^{(p-1)/e}, \chi_o^{2(p-1)/e}, \dots, \chi_o^{(e-1)(p-1)/e}\}.$$

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

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

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

$$\chi_o^{(p-1)/e}(u) = \chi_o^{(p-1)/e}(g^{Qe+R}) = \zeta_{p-1}^{(Qe+R)(p-1)/e} = \zeta_{p-1}^{R(p-1)/e} \neq 1,$$

and thus the general identity

$$(1) \quad \sum_{\chi^e = \varepsilon} \chi(a) = \chi_o^{(p-1)/e}(a) \sum_{\chi^e = \varepsilon} \chi(a) \quad \text{for all } a \in \mathbf{F}_p^\times$$

(because multiplying by $\chi_o^{(p-1)/e}$ permutes the characters in the order- e subgroup of $\widehat{\mathbf{F}_p^\times}$) shows that in particular $\sum_{\chi^e = \varepsilon} \chi(u) = 0$. And so similarly to before we have

$$N(x^e = u) = 0 = \sum_{\chi^e = \varepsilon} \chi(u).$$

Finally, extend characters modulo p to all of \mathbf{F}_p by defining

$$\varepsilon(0) = 1, \quad \chi(0) = 0 \text{ if } \chi \neq \varepsilon.$$

Then

$$N(x^e = 0) = 1 = \sum_{\chi^e = \varepsilon} \chi(0).$$

And so we have in sum,

$$\text{If } p = 1 \pmod e \text{ then } \sum_{\chi^e = \varepsilon} \chi(u) = N(x^e = u) \text{ for all } u \in \mathbf{F}_p.$$

As explained above, the formula in the box contains the information to compute $N(x^e = u)$ for all all positive values of e .

3. THE ORTHOGONALITY RELATIONS

Proposition 3.1. *The following two relations hold.*

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

and

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

Proof. Both identities are proved essentially as we have already proved identity (1). The first identity is clear if $\chi = \varepsilon$. Otherwise $\chi(a_o) \neq 1$ for some $a_o \in \mathbf{F}_p^\times$, and so (since multiplying by a_o permutes \mathbf{F}_p^\times)

$$\sum_{a \in \mathbf{F}_p^\times} \chi(a) = \sum_{a \in \mathbf{F}_p^\times} \chi(a_o a) = \chi(a_o) \sum_{a \in \mathbf{F}_p^\times} \chi(a),$$

showing that the sum vanishes. The second identity is clear if $a = 1_{\mathbf{F}_p}$. Otherwise $\chi_o(a) \neq 1$ because χ_o sends only $1_{\mathbf{F}_p}$ to $1_{\mathbf{C}}$, and so (since multiplying by χ_o permutes $\widehat{\mathbf{F}_p^\times}$)

$$\sum_{\chi \in \widehat{\mathbf{F}_p^\times}} \chi(a) = \sum_{\chi \in \widehat{\mathbf{F}_p^\times}} (\chi_o \chi)(a) = \chi_o(a) \sum_{\chi \in \widehat{\mathbf{F}_p^\times}} \chi(a),$$

and again the sum vanishes. □

4. GAUSS SUMS AGAIN

Every character χ modulo p has an associated **Gauss sum**,

$$\tau(\chi) = \sum_{t \in \mathbf{F}_p} \chi(t) \zeta_p^t.$$

The finite geometric sum formula shows that

$$\tau(\varepsilon) = 0.$$

For $\chi \neq \varepsilon$ we may sum over $t \in \mathbf{F}_p^\times$ because $\chi(0) = 0$. In this case, compute

$$|\tau(\chi)|^2 = \tau(\chi) \overline{\tau(\chi)} = \sum_{s, t \in \mathbf{F}_p^\times} \chi(s) \overline{\chi}(t) \zeta_p^{s-t} = \sum_{s, t \in \mathbf{F}_p^\times} \chi(st^{-1}) \zeta_p^{s-t}.$$

Let $u = st^{-1}$, so that $t = su^{-1}$, and continue,

$$|\tau(\chi)|^2 = \sum_{s, u \in \mathbf{F}_p^\times} \chi(ss^{-1}u)\zeta_p^{s(1-u^{-1})} = \sum_{u \in \mathbf{F}_p^\times} \chi(u) \sum_{s \in \mathbf{F}_p^\times} \zeta_p^{s(1-u^{-1})}.$$

The inner sum is -1 if $u \neq 1$ and is $p-1$ if $u = 1$. Thus

$$|\tau(\chi)|^2 = p - \sum_{u \in \mathbf{F}_p^\times} \chi(u) = p.$$

Also we have for $\chi \neq \varepsilon$,

$$\overline{\tau(\chi)} = \sum_{t \in \mathbf{F}_p^\times} \overline{\chi(t)}\zeta_p^{-t} = \overline{\chi(-1)} \sum_{t \in \mathbf{F}_p^\times} \overline{\chi(-t)}\zeta_p^{-t} = \chi(-1)\tau(\overline{\chi})$$

(since $\overline{\chi(-1)} = \chi(-1)$). In sum,

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

5. MORE COUNTING FORMULAS; JACOBI SUMS

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

$$\mathbf{N}(a_1x_1^{e_1} + a_2x_2^{e_2} + \cdots + a_rx_r^{e_r} = b)$$

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 condition on r variables from \mathbf{F}_p .

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

Definition 5.1. Let χ_1, \dots, χ_r be characters modulo p . The corresponding **Jacobi sums** are

$$J_0(\chi_1, \dots, \chi_r) = \sum_{\vec{u}: \sum u_i = 0} \chi_1(u_1) \cdots \chi_r(u_r)$$

and

$$J(\chi_1, \dots, \chi_r) = \sum_{\vec{u}: \sum u_i = 1} \chi_1(u_1) \cdots \chi_r(u_r).$$

Recall the basic counting formula for $e \mid p-1$,

$$\mathbf{N}(x^e = u) = \sum_{\chi^e = \varepsilon} \chi(u).$$

Using the basic formula, compute a sprawling expression for the solution-count that we seek,

$$\begin{aligned}
 & \mathbf{N}(a_1x_1^{e_1} + a_2x_2^{e_2} + \cdots + a_rx_r^{e_r} = b) \\
 &= \sum_{\substack{u_1, \dots, u_r \\ u_1 + \dots + u_r = b}} \mathbf{N}(x_1^{e_1} = a_1^{-1}u_1) \cdots \mathbf{N}(x_r^{e_r} = a_r^{-1}u_r) \\
 &= \sum_{\vec{u}: \sum u_i = b} \prod_{i=1}^r \mathbf{N}(x_i^{e_i} = a_i^{-1}u_i) \\
 &= \sum_{\vec{u}: \sum u_i = b} \prod_{i=1}^r \sum_{\chi_i: \chi_i^{e_i} = \varepsilon} \chi_i(a_i^{-1}u_i) \\
 &= \sum_{\vec{u}: \sum u_i = b} \sum_{\substack{(\chi_1, \dots, \chi_r) \\ \text{each } \chi_i^{e_i} = \varepsilon}} \chi_1(a_1^{-1}u_1) \cdots \chi_r(a_r^{-1}u_r) \\
 &= \sum_{\vec{\chi}: \text{each } \chi_i^{e_i} = \varepsilon} \chi_1(a_1^{-1}) \cdots \chi_r(a_r^{-1}) \sum_{\vec{u}: \sum u_i = b} \chi_1(u_1) \cdots \chi_r(u_r)
 \end{aligned}$$

And now inspecting the definition of the two types of Jacobi sum shows that the desired counting formula is

$$\boxed{
 \begin{aligned}
 & \mathbf{N}(a_1x_1^{e_1} + a_2x_2^{e_2} + \cdots + a_rx_r^{e_r} = b) \\
 &= \begin{cases} \sum_{\vec{\chi}: \text{each } \chi_i^{e_i} = \varepsilon} \chi_1(a_1^{-1}) \cdots \chi_r(a_r^{-1}) J_0(\chi_1, \dots, \chi_r) & \text{if } b = 0, \\ \sum_{\vec{\chi}: \text{each } \chi_i^{e_i} = \varepsilon} \chi_1(a_1^{-1}) \cdots \chi_r(a_r^{-1}) (\chi_1 \cdots \chi_r)(b) J(\chi_1, \dots, \chi_r) & \text{if } b \neq 0. \end{cases}
 \end{aligned}
 }$$

6. A QUADRATIC EXAMPLE

Let p be an odd prime. We want to count the points of the unit circle of the mod p world,

$$x^2 + y^2 = 1.$$

The general counting formula gives

$$\mathbf{N}(x^2 + y^2 = 1) = \sum_{\chi_1^2 = \chi_2^2 = \varepsilon} J(\chi_1, \chi_2).$$

The only relevant characters are ε and (\cdot/p) . Thus in fact,

$$\mathbf{N}(x^2 + y^2 = 1) = J(\varepsilon, \varepsilon) + 2J(\varepsilon, \left(\frac{\cdot}{p}\right)) + J\left(\left(\frac{\cdot}{p}\right), \left(\frac{\cdot}{p}\right)\right).$$

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,

$$J\left(\left(\frac{\cdot}{p}\right), \left(\frac{\cdot}{p}\right)\right) = \sum_{u_1 + u_2 = 1} \left(\frac{u_1}{p}\right) \left(\frac{u_2}{p}\right) = \sum_{u_1 \neq 0, 1} \left(\frac{u_1(1-u_1)}{p}\right).$$

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

$$J\left(\left(\frac{\cdot}{p}\right), \left(\frac{\cdot}{p}\right)\right) = \sum_{u_1 \neq 0,1} \left(\frac{u_1^{-1} - 1}{p}\right) = -\left(\frac{-1}{p}\right).$$

In sum,

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

What's secretly happening here is that the unit circle of the mod p world really wants to live 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 $p \pmod{4}$), two of the points are projective or all of them are affine.

7. ANALYSIS OF THE JACOBI SUMS

We will establish the following table.

$\vec{\chi}$	$J(\vec{\chi})$	$ J(\vec{\chi}) $	$J_0(\vec{\chi})$	$ J_0(\vec{\chi}) $
$\vec{\varepsilon}$	p^{r-1}	p^{r-1}	p^{r-1}	p^{r-1}
$(\vec{\varepsilon}_s, \vec{\chi}_{r-s})$	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
$\prod_i \chi_i = \varepsilon$	$-\frac{\tau(\chi_1) \cdots \tau(\chi_r)}{p}$	$p^{r/2-1}$	$(p-1) \frac{\tau(\chi_1) \cdots \tau(\chi_r)}{p}$	$(p-1)p^{r/2-1}$

The table shows that

$$|N(a_1 x_1^{e_1} + a_2 x_2^{e_2} + \cdots + a_r x_r^{e_r} = b) - p^{r-1}| \leq \begin{cases} M_0 p^{r/2-1} + M_1 p^{(r-1)/2} & \text{if } b \neq 0, \\ M_0 (p-1) p^{r/2-1} & \text{if } b = 0, \end{cases}$$

where there are $e_i - 1$ possibilities for each χ_i , and

$$M_0 = |\{\vec{\chi} : \prod_i \chi_i = \varepsilon\}| \quad \text{and} \quad M_1 = |\{\vec{\chi} : \prod_i \chi_i \neq \varepsilon\}|.$$

To derive the various results in the table, begin by noting that its top row is clear because both $J(\vec{\varepsilon})$ and $J_0(\vec{\varepsilon})$ 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 from the second orthogonality relation.

Next compute that when none of the characters is trivial,

$$\begin{aligned}
 J_0(\vec{\chi}) &= \sum_{u_r \in \mathbf{F}_p^\times} \left[\sum_{u_1 + \dots + u_{r-1} = -u_r} \chi_1(u_1) \cdots \chi_{r-1}(u_{r-1}) \right] \chi_r(u_r) \\
 &= \sum_{u_r \in \mathbf{F}_p^\times} \left[\sum_{u_1 + \dots + u_{r-1} = 1} \chi_1(u_1) \cdots \chi_{r-1}(u_{r-1}) \right] (\chi_1 \cdots \chi_{r-1})(-1) (\chi_1 \cdots \chi_r)(u_r) \\
 &= (\chi_1 \cdots \chi_{r-1})(-1) J(\chi_1, \dots, \chi_{r-1}) \sum_{u_r \in \mathbf{F}_p^\times} (\chi_1 \cdots \chi_r)(u_r) \\
 &= \begin{cases} 0 & \text{if } \prod_i \chi_i \neq \varepsilon, \\ (p-1)\chi_r(-1)J(\chi_1, \dots, \chi_{r-1}) & \text{if } \prod_i \chi_i = \varepsilon. \end{cases}
 \end{aligned}$$

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 $\prod_i \chi_i \neq \varepsilon$ (quoting the J_0 calculation just carried out),

$$\begin{aligned}
 \tau(\chi_1) \cdots \tau(\chi_r) &= \sum_{t_1, \dots, t_r \in \mathbf{F}_p} \chi_1(t_1) \cdots \chi_r(t_r) \zeta_p^{t_1 + \dots + t_r} \\
 &= \sum_{u \in \mathbf{F}_p} \sum_{\vec{t}: \sum t_i = u} \chi_1(t_1) \cdots \chi_r(t_r) \zeta_p^u \\
 &= J_0(\vec{\chi}) + J(\vec{\chi}) \sum_{u \in \mathbf{F}_p^\times} (\chi_1 \cdots \chi_r)(u) \zeta_p^u \\
 &= J(\vec{\chi}) \tau(\chi_1 \cdots \chi_r) \quad \text{since the } J_0 \text{ term vanishes.}
 \end{aligned}$$

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,

$$\begin{aligned}
 J_0(\vec{\chi}) &= (p-1)\chi_r(-1)J(\chi_1, \dots, \chi_{r-1}) \\
 &= (p-1)\chi_r(-1) \frac{\tau(\chi_1) \cdots \tau(\chi_{r-1})}{\tau(\chi_1 \cdots \chi_{r-1})} \cdot \frac{\tau(\chi_r)}{\tau(\chi_r)} \\
 &= (p-1)\chi_r(-1) \frac{\tau(\chi_1) \cdots \tau(\chi_r)}{\tau(\vec{\chi}_r) \tau(\chi_r)} \\
 &= (p-1) \frac{\tau(\chi_1) \cdots \tau(\chi_r)}{p}.
 \end{aligned}$$

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 $\prod_i \chi_i = \varepsilon$, using the fact that now

$$\sum_{u \in \mathbf{F}_p^\times} (\chi_1 \cdots \chi_r)(u) \zeta_p^u = \tau(\varepsilon) - 1 = -1,$$

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

$$\begin{aligned}\tau(\chi_1) \cdots \tau(\chi_r) &= J_0(\vec{\chi}) - J(\vec{\chi}) \\ &= (p-1) \frac{\tau(\chi_1) \cdots \tau(\chi_r)}{p} - J(\vec{\chi}).\end{aligned}$$

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

8. A CUBIC EXAMPLE

Let p be prime. We want to count the points of the cubic Fermat curve in the mod p world,

$$x^3 + y^3 = 1.$$

If $p \equiv 2 \pmod{3}$ 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, $p \equiv 1 \pmod{3}$.

Again referring to the general counting formula, we have

$$N(x^3 + y^3 = 1) = \sum_{\chi_1^3 = \chi_2^3 = \varepsilon} J(\chi_1, \chi_2).$$

This time the relevant characters are ε , χ , and $\bar{\chi}$, where $\chi(g) = \zeta_3$. Expand the formula,

$$N(x^3 + y^3 = 1) = J(\varepsilon, \varepsilon) + 2(J(\varepsilon, \chi) + J(\varepsilon, \bar{\chi})) + 2J(\chi, \bar{\chi}) + J(\chi, \chi) + J(\bar{\chi}, \bar{\chi}).$$

According to the table,

$$N(x^3 + y^3 = 1) = p - 2\tau(\chi)\tau(\bar{\chi})/p + 2\operatorname{Re}(J(\chi, \chi)).$$

We know that $\tau(\chi)\tau(\bar{\chi}) = \chi(-1)p$, and in fact $\chi(-1) = 1$ since $\chi^3 = 1$. Therefore,

$$N(x^3 + y^3 = 1) = p - 2 + 2\operatorname{Re}(J(\chi, \chi)).$$

Gauss reasoned as follows. We know that

$$J(\chi, \chi) = a + b\omega, \quad a, b \in \mathbf{Z}, \quad \omega = \zeta_3.$$

By the table, $|J(\chi, \chi)|^2 = p$, i.e.,

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

We are looking for $2\operatorname{Re}(J(\chi, \chi)) = 2a - b$. Knowing p and knowing that $p = |a + b\omega|^2$ does not uniquely a and b . (For example, $\omega(a + b\omega)$ has the same size.) But since $p \equiv 1 \pmod{3}$, it turns out that $4p = A^2 + 27B^2$ with $\pm A$ and $\pm B$ unique (see Ireland and Rosen for the details). So compute,

$$a + b\omega = J(\chi, \chi) = \frac{\tau(\chi)^2}{\tau(\bar{\chi})} = \frac{\tau(\chi)^3}{\tau(\chi)\tau(\bar{\chi})} = \frac{\tau(\chi)^3}{\chi(-1)p} = \frac{\tau(\chi)^3}{p}.$$

Consider the resulting relation $pa + pb\omega = \tau(\chi)^3$ modulo 3. On the one hand,

$$pa + pb\omega \equiv_3 a + b\omega,$$

and on the other hand,

$$\tau(\chi)^3 \equiv_3 \sum_{t \in \mathbf{F}_p^\times} \chi(t)^3 \zeta_p^{3t} = \sum_{t \in \mathbf{F}_p^\times} \zeta_p^{3t} = -1,$$

Thus $a \equiv -1 \pmod{3}$ and $b \equiv 0 \pmod{3}$. And now, since $4p = 4(a^2 - ab + b^2) = (2a - b)^2 + 3b^2$, we have

$$4p = A^2 + 27B^2, \quad A = 2a - b \equiv 1 \pmod{3}, \quad B = b/3 \in \mathbf{Z}.$$

So the desired quantity $2a - b$ is A . We have proved

Theorem 8.1 (Gauss). *Let $p \equiv 1 \pmod{3}$. The number of points on the cubic Fermat curve mod p is*

$$N(x^3 + y^3 = 1) = p - 2 + A \quad \text{where} \quad 4p = A^2 + 27B^2, \quad A \equiv 1 \pmod{3}.$$

The formulas in Gauss's calculation may seem unmotivated, but we will see that they arise naturally in the arithmetic of the ring $D = \mathbf{Z}[\omega]$ where $\omega = \zeta_3 = e^{2\pi i/3} = (-1 + i\sqrt{3})/2$. We will study the ring D soon.

9. A GENERALIZATION OF THE QUADRATIC EXAMPLE BY OTHER MEANS

Let $d \in \mathbf{Z}$ 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

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

and

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

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

Let $p \nmid 2d$ be prime and work over the field \mathbf{F}_p . Then

$$|Q_{\text{hom}}(\mathbf{F}_p)| = |\mathbf{P}^1(\mathbf{F}_p)| = p + 1.$$

Furthermore, all points of $\mathbf{P}^1(\mathbf{F}_p)$ map to affine points $[*, *, 1]$ of Q_{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

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

This is the formula that we obtained by Jacobi sums for $d = -1$.