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 p** *is*

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

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

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

Examples of characters are

- The **trivial character**
$$\varepsilon : \mathbb{F}_p^\times \longrightarrow \mathbb{C}^\times, \quad \varepsilon(a) = 1 \text{ for all } a \in \mathbb{F}_p^\times.$$
- The **quadratic character**
$$\left(\frac{\cdot}{p}\right) : \mathbb{F}_p^\times \longrightarrow \mathbb{C}^\times, \quad a \longmapsto \left(\frac{a}{p}\right).$$
Here if we change p to q then the Legendre symbol becomes the Jacobi symbol.
- Recall that $\mathbb{F}_p^\times$ 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
$$\chi_o : \mathbb{F}_p^\times \longrightarrow \mathbb{C}^\times, \quad \chi_o(g^n) = \zeta_{p-1}^n, \; n = 0, 1, \ldots, p-2.$$
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. $\chi(1_{\mathbb{F}_p}) = 1_{\mathbb{C}}$.
2. $\chi(a)^{p-1} = 1_{\mathbb{C}}$ *for all $a \in \mathbb{F}_p^\times$, and in fact $\chi(a)^d = 1$ where d is the order of 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.*
4. $\chi(-1) = \pm 1$*, and so $\overline{\chi}(-1) = \chi(-1)$.*

The first three properties follow immediately from the facts that χ is a homomorphism and $\mathbb{F}_p^\times$ is finite. The fourth follows from the second with $d = 2$ or from the third with $a = -1$.

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

Proof. Let g generate $\mathbb{F}_p^\times$. Then any $\chi \in \widehat{\mathbb{F}_p^\times}$ 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 $\widehat{\mathbb{F}_p^\times}$. □

Because $\mathbb{F}_p^\times$ and $\widehat{\mathbb{F}_p^\times}$ 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 endomorphsim $x \mapsto ex$ of G. To study its image and its kernel, let

$$\hat{e} = \gcd(e, q).$$

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 $\hat{e} = \gcd(e, q)$, rather than on the original datum e.

For example, let $q = 6$ and let $e = 10$, so that $\hat{e} = \gcd(10, 6) = 2$. The endomorphism $x \mapsto 10x$ of $\mathbb{Z}/6\mathbb{Z}$ has image $\{0, 2, 4\}$ and kernel $\{0, 3\}$, and these are the image and the kernel of the variant endomorphism $x \mapsto 2x$ of $\mathbb{Z}/6\mathbb{Z}$. This tells us multiplicatively that the endomorphism $x \mapsto x^{10}$ of $(\mathbb{Z}/7\mathbb{Z})^\times$ has image $\{1, 3^2, 3^4\} = \{1, 2, 4\}$ (noting that 3 is generator modulo 7) and kernel $\{1, 3^3\} = \{1, 6\}$, and these are the image and the kernel of the variant endomorphism $x \mapsto x^2$ of $(\mathbb{Z}/7\mathbb{Z})^\times$. However, this does not say that the endomorphisms $x \mapsto x^{10}$ and $x \mapsto x^2$ of $(\mathbb{Z}/7\mathbb{Z})^\times$ are equal.

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,

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

We want to express $\mathrm{N}(x^e = u)$ 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 $\gcd(e, p-1)$. So we freely assume that $e \mid p-1$, i.e., $p = 1 \bmod e$. The result, to be established below, is

$$\boxed{\textit{If } p = 1 \bmod e \textit{ then } \mathrm{N}(x^e = u) = \sum_{\chi^e = \varepsilon} \chi(u) \textit{ for any } u \in \mathbb{F}_p.}$$

We prove the boxed formula. Because the endomorphism $x \mapsto x^e$ has kernel of order e, i.e., the endomorphism is e-to-1, it follows that $\mathrm{N}(x^e = u) \in \{0, e\}$ for all $u \in \mathbb{F}_p^\times$. Consider the order-$e$ subgroup of $\widehat{\mathbb{F}_p^\times}$, consisting of the characters χ such that $\chi^e = \varepsilon$,

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

For example, when $e = 2$ the subgroup is $\{\varepsilon, (\cdot/p)\}$. To prove the boxed formula for $u \in \mathbb{F}_p^\times$ such that if $x_o^e = u$ for some x_o, compute

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

On the other hand, for $u \in \mathbb{F}_p^\times$ such that $x^e \neq u$ for all $x \in \mathbb{F}_p^\times$, note that 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

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

which holds because multiplying by $\chi_o^{(p-1)/e}$ permutes the characters in the order-e subgroup of $\widehat{\mathbb{F}_p^\times}$, specializes to give

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

Finally, to address the case $u = 0$, extend characters modulo p to all of $\mathbb{F}_p$ by defining

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

Then

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

We have proved the boxed formula above in all cases. Reiterating a point already made, the boxed formula contains the information to compute $\mathrm{N}(x^e = u)$ for all positive values of e, not only for divisors e of $p-1$: replace e with $\gcd(e, p-1)$ and the formula for the new e gives the desired solution-count for the original e.

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

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

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 $a_o \in \mathbb{F}_p^\times$; so, because multiplying by a_o permutes $\mathbb{F}_p^\times$,

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

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

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

again the sum vanishes. □

The same methods apply to additive characters $\psi : \mathbb{F}_p \longrightarrow \mathbb{C}^\times$, meaning characters such 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

$$\sum_{\psi \in \widehat{\mathbb{F}_p}} \psi(a) = \begin{cases} p & \text{if } a = 0_{\mathbb{F}_p} \\ 0 & \text{if } a \neq 0_{\mathbb{F}_p}. \end{cases}$$

5. Gauss Sums Again

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

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

Note that χ is a character of the multiplicative group $\mathbb{F}_p^\times$ while $t \mapsto \zeta_p^t$ is a nontrivial character of the additive group $\mathbb{F}_p$. We establish three results, with χ understood to denote a nontrivial character in the second and third,

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

The first result follows from the orthogonality of characters of $\mathbb{F}_p$.

For nontrivial χ we may sum over $t \in \mathbb{F}_p^\times$ because $\chi(0) = 0$. In this case compute, nesting two sums at the first step, replacing t by tu in the inner sum at the second, and exchanging the order of summation at the third,

$$\begin{aligned} \tau(\chi)\tau(\overline{\chi}) &= \sum_{u,t \in \mathbb{F}_p^\times} \chi(tu^{-1})\zeta_p^{t+u} = \sum_{u,t \in \mathbb{F}_p^\times} \chi(tuu^{-1})\zeta_p^{u+tu} \\ &= \sum_{t \in \mathbb{F}_p^\times} \chi(t) \sum_{u \in \mathbb{F}_p} \zeta_p^{(1+t)u} - \sum_{t \in \mathbb{F}_p^\times} \chi(t). \end{aligned}$$

By the orthogonality of characters of $\mathbb{F}_p$, the first term is $\chi(-1)p$, and by the orthogonality of characters of $\mathbb{F}_p^\times$, the second term is 0. Thus we have the second boxed result.

Also for nontrivial χ, noting for the last step that $\overline{\chi}(-1) = \chi(-1)$,

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

This combines with the second boxed result to give the third.

6. More Counting Formulas; Jacobi Sums

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

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

where each a_i is nonzero and each e_i divides $p-1$. We expect the solution-count to be roughly p^{r-1} because 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 $\chi_1, \ldots, \chi_r$ be characters modulo p. The corresponding* **Jacobi sums** *are, with $\vec{u} = (u_1, \ldots, u_r) \in \mathbb{F}_p^r$ in the following two formulas,*

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

and

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

The desired formula is

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

The basic counting formula $\mathrm{N}(x^e = u) = \sum_{\chi^e=\varepsilon} \chi(u)$ for $e \mid p-1$ gives the boxed formula, as follows.

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

Now inspecting the definition of the two types of Jacobi sum shows that the desired counting formula is as claimed.

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

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

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

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

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,

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

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

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

In sum,

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

What's secretly happening here is that the unit circle modulo p really should lie in modulo p *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

$$\mathrm{Q}: x^2-dy^2=1$$

homogenizes to

$$\mathrm{Q}_{\mathrm{hom}}: x^2-dy^2=z^2.$$

The maps

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

and

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

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 $\mathbb{F}_p$. Then

$$|\mathrm{Q}_{\mathrm{hom}}(\mathbb{F}_p)|=|\mathbf{P}^1(\mathbb{F}_p)|=p+1.$$

Furthermore, all points of $\mathbf{P}^1(\mathbb{F}_p)$ map to affine points $[*,*,1]$ of $\mathrm{Q}_{\mathrm{hom}}$ 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

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

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

9. Analysis of the Jacobi Sums

Recall that the Jacobi sums are defined as

$$J_0(\chi_1, \ldots, \chi_r) = \sum_{\vec{u}\,:\,\sum u_i = 0} \chi_1(u_1) \cdots \chi_r(u_r),$$
$$J(\chi_1, \ldots, \chi_r) = \sum_{\vec{u}\,:\,\sum u_i = 1} \chi_1(u_1) \cdots \chi_r(u_r).$$

We will establish the following table.

$\vec{\chi}$	$J(\vec{\chi})$	$\lvert J(\vec{\chi})\rvert$	$J_0(\vec{\chi})$	$\lvert J_0(\vec{\chi})\rvert$
$\vec{\varepsilon}$	p^{r-1}	p^{r-1}	p^{r-1}	p^{r-1}
$(\vec{\varepsilon}_s, \vec{\chi}_{r-s})$	0	0	0	0
$\prod_i \chi_i \neq \varepsilon$	$\dfrac{\tau(\chi_1)\cdots\tau(\chi_r)}{\tau(\chi_1\cdots\chi_r)}$	$p^{(r-1)/2}$	0	0
$\prod_i \chi_i = \varepsilon$	$-\dfrac{\tau(\chi_1)\cdots\tau(\chi_r)}{p}$	$p^{r/2-1}$	$(p-1)\dfrac{\tau(\chi_1)\cdots\tau(\chi_r)}{p}$	$(p-1)p^{r/2-1}$

The table shows that

$$|\mathrm{N}(a_1x_1^{e_1} + a_2x_2^{e_2} + \cdots + a_rx_r^{e_r} = b) - p^{r-1}| \leq \begin{cases} M_0p^{r/2-1} + M_1p^{(r-1)/2} & \text{if } b \neq 0, \\ M_0(p-1)p^{r/2-1} & \text{if } b = 0, \end{cases}$$

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 similarly from the second orthogonality relation. For example,

$$J(\vec{\varepsilon}_s, \vec{\chi}_{r-s}) = \sum_{u_2} \varepsilon(u_2) \cdots \sum_{u_r} \chi_r(u_r)\varepsilon(1 - u_2 - \cdots - u_r) = 0.$$

Next compute that when none of the characters is trivial,

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

The first case of this relation gives the right half of the third row. The second case, in which $\chi_1\cdots\chi_{r-1}\neq\varepsilon$, reduces the right half of the fourth row to the left half of the third row; we will return to this below.

For the left half of the third row, compute for $\prod_i\chi_i\neq\varepsilon$, quoting the $J_0(\vec{\chi})=0$ result that we already have for the right half of the third row,

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

This establishes the left half of the third row.

Now we obtain the right half of the fourth row. Using the formula in the left half of the third row, though with $r-1$ characters rather than r, and noting that $\chi_1\cdots\chi_{r-1}=\overline{\chi}_r$, and recalling for the last equality to follow that $\tau(\overline{\chi}_r)\tau(\chi_r)=\chi_r(-1)p$, compute that

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

Finally, for the left half of the fourth row, so now with $\prod_i\chi_i=\varepsilon$, modify the calculation of the product $\tau(\chi_1)\cdots\tau(\chi_r)$ using the fact that now

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

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 table's value of $J(\vec{\chi})$.

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 $p = 3$ or $p = 2 \bmod 3$ 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, $p = 1 \bmod 3$.

Again referring to the general counting formula, we have

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

This time the relevant characters are ε, χ, and $\overline{\chi}$, where $\chi(g) = \zeta_3$ with g a generator of $\mathbb{F}_p^\times$. Expand the nine terms of the formula and then gather terms,

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

According to the table,

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

We know that $\tau(\chi)\tau(\overline{\chi}) = \chi(-1)p$, and in fact $\chi(-1) = 1$ because -1 is a cube and $\chi^3 = \varepsilon$; specifically, $\chi(-1) = \chi((-1)^3) = \chi^3(-1) = \varepsilon(-1) = 1$. Therefore,

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

Gauss reasoned as follows. We know that

$$J(\chi, \chi) = a + b\omega, \quad a, b \in \mathbb{Z},\ \omega = \zeta_3 = -\tfrac{1}{2} + i\tfrac{\sqrt{3}}{2}.$$

We are seeking

$$2\mathrm{Re}(J(\chi, \chi)) = 2a - b.$$

The process will be twofold:

- study $a + b\omega$ such that $2\mathrm{Re}(J(\chi, \chi)) = 2a - b$,
- then use the results to characterize $2a - b$ in a readily computable form, with no direct reference to a and b.

For the first item, note that $|J(\chi, \chi)|^2 = p$ according to our table, which is to say that $(a + b\omega)(a + b\omega^2) = p$, or

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

Having p and knowing that $|a + b\omega|^2 = p$ does not uniquely determine a and b: the six values $\tilde{a} + \tilde{b}\omega = \pm(a + b\omega), \pm\omega(a + b\omega), \pm\omega^2(a + b\omega)$ all satisfy $|\tilde{a} + \tilde{b}\omega|^2 = p$, and so do the six conjugate values $\tilde{a} + \tilde{b}\omega = \pm(a + b\omega^2), \pm\omega(a + b\omega^2), \pm\omega^2(a + b\omega^2)$. We show that the Jacobi sum value $J(\chi, \chi) = a + b\omega$ satisfies the further conditions $a = 2 \bmod 3$ and $b = 0 \bmod 3$. To see this, 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 in $\mathbb{Z}[\omega]$. On the one hand, because $p = 1 \bmod 3$,

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

and on the other hand,

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

Thus $a = 2 \bmod 3$ and $b = 0 \bmod 3$, as claimed. In our pending studies of the Eisenstein integer ring $\mathbb{Z}[\omega]$, we will see that exactly one conjugate pair of the twelve values $\tilde{a}+\tilde{b}\omega$ such that $p = \tilde{a}^2 - \tilde{a}\tilde{b} + \tilde{b}^2$ satisfy $\tilde{a} = 2 \bmod 3$ and $\tilde{b} = 0 \bmod 3$. Thus we have described $2\mathrm{Re}(J(\chi,\chi)) = 2a - b$ completely by the conditions $p = a^2 - ab + b^2$, $a = 2 \bmod 3$, and $b = 0 \bmod 3$, even though these conditions don't fully determine a and b. More specifically, with $J(\chi,\chi) = a + b\omega$ where $a = 2 \bmod 3$ and $b = 0 \bmod 3$, also $J(\overline{\chi},\overline{\chi}) = a - b - b\omega$ where also $a - b = 2 \bmod 3$ and $-b = 0 \bmod 3$); we don't need to distinguish between these because twice the real part of either is $2a - b$.

The second item in our list is to use the results $p = a^2 - ab + b^2$, $a = 2 \bmod 3$, and $b = 0 \bmod 3$ to characterize $2a - b$ in a readily computable form, with no direct reference to a and b. The equality just quoted is also $p = (a - b/2)^2 + 3(b/2)^2$, or $4p = (2a - b)^2 + 3b^2$, and this combines with the congruences to give

$$4p = A^2 + 27B^2, \qquad A = 1 \bmod 3,$$

in which $A = 2a - b$ is the quantity that we seek, and $B = b/3$. Finding the A specified by the previous display is an easy search because A^2 and $27B^2$ are positive. By contrast, searching for a and b such that $p = a^2 - ab + b^2$ is not so simple because of the minus sign, and searching for a and b such that $p = (a - b/2)^2 + 3(b/2)^2$ involves quarter-integers; further, we want only $2a - b$ in any case. Below in this writeup, we will show that the conditions $4p = A^2 + 27B^2$, $A = 1 \bmod 3$ determine A uniquely. We have proved

Theorem 10.1 (Gauss)**.** *Let $p = 1 \bmod 3$. The number of points on the cubic Fermat curve mod p is*

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

A crucial point of Gauss's theorem, as we soon will see, is that:

> *To solve the problem of counting the Fermat cubic points modulo p in the interesting case $p = 1 \bmod 3$, we need to factor p in the Eisenstein integer ring $\mathbb{Z}[\omega]$.*

Further, the statement of the theorem gives an algorithm to carry out the factorization. As in other examples from this course, such as Fermat's fountainhead theorem about odd primes $p = x^2 + y^2$, we see that algebraic number theory, meaning number theory beyond the basic integer ring $\mathbb{Z}$ and its quotient field $\mathbb{Q}$, arises naturally from problems that are set in $\mathbb{Z}$. Also, we have seen that quadratic reciprocity, despite being set in $\mathbb{Z}$, describes phenomena from algebraic number theory. The distinction between so-called elementary number theory, set entirely in $\mathbb{Z}$ or maybe $\mathbb{Q}$, and algebraic number theory, set in larger rings and/or fields, is arguably artificial.

For example, let $p = 103$, so that $4p = 412$. The only values $27B^2$ less than $4p$ are $27, 108, 243$. Next, $412 - 27 = 385$ and $412 - 108 = 304$ are not squares but

$412 - 243 = 169 = (\pm 13)^2$. Thus $A = 13$. The equation $x^3 + y^3 = 1 \bmod 103$ has $103 - 2 + 13 = 114$ solutions.

We turn to the homogeneous Fermat equation of degree 3, given by $x^3 + y^3 = z^3$. For a prime $p \neq 1 \bmod 3$, this 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 $p = 1 \bmod 3$, the equation has $p - 2 + A$ 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 overall, a revision of Gauss's result is that counting projectively modulo any prime p, and replacing A from above by its additive inverse here,

$$\mathrm{N}(x^3 + y^3 = z^3) = p + 1 - A,$$
$$\text{where } \begin{cases} 4p = A^2 + 27B^2,\ A = 2 \bmod 3 & \text{if } p = 1 \bmod 3, \\ A = 0 & \text{if } p \neq 1 \bmod 3. \end{cases}$$

Here are some values of A in the previous display for primes $p = 1 \bmod 3$.

p	7	13	19	31	37	43	61	67	73	79
A	-1	5	-7	-4	11	8	-1	5	-7	17

The cubic Fermat curve is an *elliptic curve* whose *conductor* is 27. According to the *Modularity Theorem*, each value $A = A_p$ in the previous display must also be the pth Fourier coefficient of a certain *modular cusp form* whose *weight* is 2 and whose *level* matches the conductor. There exists only one weight 2, level 27 cusp form, as follows. For a complex number τ having positive imaginary part, define also $q = e^{2\pi i\tau}$, a complex number of absolute value less than 1. The *Dedekind eta function* is

$$\eta(\tau) = q^{1/24} \prod_{n=1}^{\infty} (1 - q^n),$$

and the unique weight 2, level 27 cusp form is

$$f_{2,27}(\tau) = \eta(3\tau)^2 \eta(9\tau)^2.$$

Its expansion in powers of q begins

$$\begin{aligned} f_{2,27}(\tau) = q - 2q^4 + \boxed{-1}q^7 + \boxed{5}q^{13} + 4q^{16} + \boxed{-7}q^{19} - 5q^{25} + 2q^{28} \\ + \boxed{-4}q^{31} + \boxed{11}q^{37} + \boxed{8}q^{43} - 6q^{49} - 10q^{52} + \boxed{-1}q^{61} - 8q^{64} \\ + \boxed{5}q^{67} + \boxed{-7}q^{73} + 14q^{76} + \boxed{17}q^{79} + \cdots . \end{aligned}$$

We see that each pth Fourier coefficent for $p = 1 \bmod 3$ matches the corresponding A-value in the table above, and further the Fourier coefficients 0 for $p \neq 1 \bmod 3$ match the $A = 0$ values for those primes as well. This phenomenon is the modularity of the cubic Fermat curve.

Finally, we discuss the fact that for any prime $p = 1 \bmod 3$, the condition

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

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

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

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

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

The relation $(a-b)-(-b)/2 = a-b/2$ shows that the quantity $a-b/2$ in the previous display depends only on p, not on a choice between π and $\overline{\pi}$. Multiplying the display by 4 gives a condition of the desired form $4p = A^2 + 27B^2$ with $A = 1 \bmod 3$.

On the other hand, consider a representation $4p = A^2 + 27B^2$ with $A = 1 \bmod 3$. 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 $2a = A + b = 1 \bmod 3$, giving $a = 2 \bmod 3$. This gives a representation of p as in the previous display. Thus $A = 2a - b$ for a suitable $a + b\omega$, and our pending study of $\mathbb{Z}[\omega]$ will show that this quantity is unique to p up to conjugation.