EXPLORING p-ADIC NUMBERS AND DIRICHLET CHARACTERS

JAIME SORENSON

University of Rochester
Professor John Harper
MTH 391W
Spring 2009

1. An Introduction to p-Adic Numbers

Kurt Hensel is responsible for first developing p-adic numbers. His work followed that of his supervisor in the development of arithmetic in algebraic number fields. In 1897, the Weierstrass method of power-series development for algebraic functions led him to the invention of the p-adic numbers. Hensel was interested in the exact power of a prime which divides the discriminant of an algebraic number field. The p-adic numbers can be regarded as a completion of the rational numbers in a different way from the usual completion which leads to the real numbers. The potential of p-adic numbers remained untapped until 1921 when Hasse formulated the local-global principle, now reffered to as the Hasse principle. This showed that an equation in the quadratic form has a rational solution if and only if it has a solution in the p-adic numbers for every prime p and a solution in the reals. [9][1]

1.1. p-**Adic Numbers.**

1.1.1. *Metrics and Norms.* There are some basic ideas that must be understood before dealing with p-adic numbers. The first concept is a metric space.

Definition 1. *A metric space is a set X together with a metric d usually denoted as (X,d).*

Now you may ask, what is a metric? It is a function that dictates the distance between two points in a set.

Definition 2. *A metric on a non-empty set X is a function d(x,y) with x,y* $\in X$.

(1) $d(x, y) = 0$ *if an only if* $x = y$.
(2) $d(x, y) = d(y, x)$.
(3) $d(x, z) \leq d(x, y) + d(y, z)$.

The function d sends the pair of elements (x, y) to the non-negative real numbers. The first property is called the Identity of Indiscernibles. If two points are in the exact same position, then it is obvious that they have no distance separating them. If the distance between two points in 0, then the points must actually be the same, or at least in the exact same location.

The second property is the symmetric property. This simply says that the distance from x to y is the same as the distance from y to x.

The third property is the Triangle Inequality. Pretend that we are at one corner, x, of a square and we want to get to the opposite corner, z. If we were trying to go from point x to point z, we would travel in a straight line through the middle of the square. However, if we needed to stop at point y on the way to point z, then we might need to travel further. If y was on our shortest path, then we would not need to walk any more so $d(x, z) = d(x, y) + d(y, z)$. If y was off our path, then $d(x, z) < d(x, y) + d(y, z)$.

The next term to define is a field.

Definition 3. *A field,* $\mathbf{F}$ *is a set together with two operations, additive* $(+)$ *and multiplicative* $(\cdot)$*, such that* $\mathbf{F}$ *is a commutative group under* $+$, $\mathbf{F} - \{0\}$ *is a commutative group under* $\cdot$*, and the distributive law holds.*

Two examples of fields that should be familiar are the real numbers, $\mathbb{R}$, and the rational numbers, $\mathbb{Q}$.

Definition 4. *A norm on a field* $\mathbf{F}$ *satisfies*

(1) $\|a\| = 0$ *if and only if* $a = 0$
(2) $\|ab\| = \|a\| \, \|b\|$
(3) $\|a + b\| \leq \|a\| + \|b\|$

Note: If $\mathbf{F}$ *has a norm* $\|\cdot\|$, *we can define a metric of* $\mathbf{F}$ *by:* $d(x, y) := \|x - y\|$

1.1.2. *Norms on* $\mathbb{Q}$. One norm that we are quite familiar with is the absolute value, $|\cdot|$. When we set $\mathbf{F}$ to be $\mathbb{Q}$, we can define a metric to be $d := |x - y|$. Is this the only norm on $\mathbb{Q}$? The answer is no. There are infinitely many norms of $\mathbb{Q}$, one for each prime p. These are our p-adic norms.

Let p be a prime number. For $n \in \mathbb{Z}, n = mp^v$ where $gcd(m, p) = 1$.

Definition 5. *The p-adic ordinal of n is v. The ordinal is denoted* $ord_p(n) = v$ *where* $v \in \mathbb{Z}_{\geq 0}$.

Example 1. *Consider the number* 45. 45 *factors into* $3^2 \cdot 5$. *Letting* $p = 3$, $ord_3(45) = 2$ *since* 2 *is the exponent on* 3. *By changing p to be* 7, $ord_7(45) = 0$ *since* $45 = 7^0 \cdot 45$. □

We can also find the p-adic ordinal of any rational number by the following:

$$ord_p\left(\frac{a}{b}\right) := ord_p(a) - ord_p(b).$$

To write it so that is mirrors the first introduced form,

$$\frac{a}{b} = \frac{c}{d}p^v \text{ with } gcd(c, p) = 1 = gcd(d, p) \text{ hence } ord_p\left(\frac{a}{b}\right) = v.$$

Example 2. *We now have two ways to find* $ord_3\left(\frac{10}{21}\right)$ *where* $p = 3$. *The first way mentioned goes like this:*

$$\frac{10}{21} = \left(\frac{10}{7}\right)\left(\frac{1}{3}\right) = \left(\frac{10}{7}\right)3^{-1} \implies ord_3\left(\frac{10}{21}\right) = -1$$

The second method is as follows:

$$ord_3\left(\frac{10}{21}\right) = ord_3\left(10\right) - ord_3\left(21\right).$$

$ord_3\,(10) = 0$ because $10 = 3^0 \cdot 10$ and $ord_3(21) = 1$ since $21 = 3^1 \cdot 7$. Thus we get

$$ord_3(10) - ord_3(21) = 0 - 1 = -1.$$

Both methods give us the same answer, -1. □

As I have said, there is one norm for every prime that we can use to build a metric on $\mathbb{Q}$.

Definition 6. *The p-adic norm, $|\cdot|_p$ on $\mathbb{Q}$ is defined by*

$$|x|_p := \begin{cases} 0 & \text{if } x = 0 \\ \frac{1}{p^{ord_3(x)}} & \text{if } x \neq 0 \end{cases}$$

The normal absolute value that we are familiar with is geometric. It measures the distance a point is from the origin. The p-adic absolute value is arithmetic in nature. It measures how "divisible" a number is by p. It is the basis for the algebra of p-adic numbers. When considering $|x - y|_p$, it measures how many digits past the "decimal point" in the base p expansions of x and y are the same, but counting from the rightmost digit[4]. (See 1.1.3)

Definition 7. *A norm is called non-Archimedean if*

$$\|x + y\| \leq max\{\|x\|, \|y\|\} \leq \|x\| + \|y\|$$

or if $\|x\| \neq 0 \neq \|y\|$,

$$\|x + y\| \leq max\{\|x\|, \|y\|\} < \|x\| + \|y\|$$

The p-adic norm satisfies the relations

(1) $|x|_p \geq 0 \quad \forall x$
(2) $|x|_p = 0$ if and only if $x = 0$
(3) $|xy|_p = |x|_p |y|_p \quad \forall x$ and y
(4) $|x + y|_p \leq |x|_p + |y|_p \quad \forall x$ and y
(5) $|x + y|_p \leq max(|x|_p, |y|_p) \quad \forall x$ and y

Relation 4 is the triangle inequality which falls out trivially from relation 5, also known as the strong triangle inequality. [8] The above relations show that $|\cdot|_p$ is non Archimedean. However, $|\cdot|$ is not non-Archimedean, making it Archimedean.

Example 3.

- $|21|_3$

$$21 = 3 \cdot 7. \qquad \frac{1}{3^{ord_3(21)}} = \frac{1}{3^1} = \frac{1}{3}.$$

- $|45|_3$

$$45 = 3^2 \cdot 5. \qquad \frac{1}{3^{ord_3(45)}} = \frac{1}{3^2} = \frac{1}{9}.$$

- $|p|_p$

$$p = p^1. \qquad \frac{1}{p^{ord_p(p)}} = \frac{1}{p^1} = \frac{1}{p}.$$

□

When the prime p divides the number x in $|x|_p$ many times, the resulting value will be small. Similarly, if the denominator of x is highly divisible by p, then the answer will be large. A nice example of this is $|27|_3 = \frac{1}{3^3}$ and $\left|\frac{1}{27}\right|_3 = 3^3$.

1.1.3. *The Field of p-Adics.* Using $|\cdot|$ on $\mathbb{Q}$, we create $\mathbb{R}$. Using $|\cdot|_p$ on $\mathbb{Q}$, we create $\mathbb{Q}_p$. $\mathbb{Q}_p$ is the completion of $\mathbb{Q}$ by using the p-adic norm. This is the field that the we will be working with in the following sections. But first, we will build up an abstract definition of $\mathbb{R}$ and then expand that definition to make $\mathbb{Q}_p$.

Definition 8. *A sequence is Cauchy if*

$$\forall \epsilon > 0, \exists N > 0 \text{ so that } \forall n, m \geq N, |a_n - a_m| < \epsilon.$$

The beauty of a Cauchy sequence is that it does not mention the limit of the sequence itself, but it encapsulates the convergence of the sequence.

If we define a set **S** to be the set of all Cauchy sequences of $\mathbb{Q}$, then $\mathbb{R}$ is the set of all equivalence classes of **S**. This abstract definition of $\mathbb{R}$ can be made to describe $\mathbb{Q}_p$ by changing the norm used. To build $\mathbb{R}$, we used $|\cdot|$, so to make $\mathbb{Q}_p$, we will simply use $|\cdot|_p$ for a fixed $p \neq \infty$

Lemma 1. *If $x \in \mathbb{Q}$ and $|x_p| \leq 1$, then for any i, $\exists \alpha \in \mathbb{Z}$ such that $0 \leq \alpha \leq p^i$ such that $|\alpha - x|_p \leq \frac{1}{p^i}$.*

Proof. Let $x = \frac{a}{b}$ where gcd(a, b)=1. Since $|x|_p \leq 1$, it follows that $p \nmid b$ so $(p, b) = 1$ and hence b and p^i are relatively prime. So we can find integers m and n such that $mb + np^i = 1$. Let $\alpha = a_m$.

$$|\alpha - x|_p = \left|am - \left(\frac{a}{b}\right)\right|_p = \left|\frac{a}{b}\right|_p |mb - 1|_p$$

$$\leq |mb - 1|_p = |np^i|_p = |n|_p |p^i|_p.$$

$|p^i|_p = \frac{1}{p^{ord_p(p^i)}}$. So also $|n|_p = \frac{1}{p^{ord_p(n)}}$. No matter what i is, $|n|_p|p^i|_p \leq \frac{1}{p^i}$. We can add a multiple of p^i to α to obtain and integer between 0 and p^i for which $|\alpha - x|_p \leq p^{-i}$ still holds.[6] □

We will use this lemma in the proof of the following theorem. After proving the next theorem, we will not need to think about "equivalence classes of Cauchy sequences" again.

Theorem 1. *Every equivalence class a in $\mathbb{Q}_p$ for which $|a|_p \leq 1$ has exactly one representative Cauchy sequence of the form $\{a_i\}$ for which:*

(1) $0 \leq a_i < p^i$ *for* $i = 1, 2, 3, \ldots$
(2) $a_i \equiv a_{i+1} \pmod{p}^i$ *for* $i = 1, 2, 3, \ldots$

Proof. We first prove uniqueness. If $\{a'_i\}$ is a different sequence satisfying (1) and (2), and if $a_{i_0} \neq a'_{i_0}$, then $a_{i_0} \neq a'_{i_0} \pmod{p^{i_0}}$. This is because both are between 0 and p^{i_0}. But then, for all $i \geq i_0$, we have $a_i \equiv a_{i_0} \not\equiv a'_{i_0} \equiv a_i \pmod{p}^{i_0}$. Thus

$$|a_i - a'_i|_p > \frac{1}{p^{i_0}}$$

for all $i \geq i_0$, and $\{a_i\} \nsim \{a'_i\}$.

So suppose we have a Cauchy sequence $\{b_i\}$. We want to find an equivalent sequence $\{a_i\}$ satisfying (1) and (2). To do this, we use Lemma 1. For every $j = 1, 2, 3, \ldots$, let $N(j)$ be a natural number such that $|b_i - b'_i|_p \leq p^{-j}$ whenever $i, i' \geq N(j)$. Notice that $|b_i|_p \leq 1$ if $i \geq N(1)$, because for all $i' \geq N(1)$,

$$|b_i|_p \leq max(|b'_i|_p, |b_i - b'_i|_p)$$
$$\leq max(|b'_i|_p, 1/p)$$

and $|b'_i|_p \to |a|_p \leq 1$ as $i' \to \infty$.

We now use the lemma to find a sequence of integers a_j, where $0 \leq a_j < p_j$, such that

$$|a_j - b_{N(j)}|_p \leq \frac{1}{p^j}.$$

$a_{j+1} \equiv a_j \pmod{p}^j$. $\quad |a_{j+1} - a_i|_p = |a_{j+1} - b_{N(j+1)} + b_{N(j+1)} - b_{N(j)} - (a_i - b_{N(j)})|_p$

$$\leq max(|a_{j+1} - b_{N(j+1)}|_p, |b_{N(j+1)} - b_{N(j)}|_p)$$

$$\leq max\left(\frac{1}{p^{j+1}}, \frac{1}{p^j}, \frac{1}{p^j}\right) = \frac{1}{p^j}.$$

Take $j \geq N(j)$ and $i \geq N(j)$.

$$\begin{aligned} |a_i - b_i|_p &= |a_i - a_j + a_j - b_{N(j)} - (b_i - b_{N(j)})|_p \\ &\leq max(|a_i - a_j|_p, |a_j - b_{N(j)}|_p, |b_i - b_{N(j)}|_p) \\ &\leq max\left(\frac{1}{p^j}, \frac{1}{p^j}, \frac{1}{p^j}\right) = \frac{1}{p^j}. \end{aligned}$$

This is the same limit point as before. $|a_i - b_i|_p \to 0$ as $i \to \infty$ and thus the proof is finished.[6] □

To summarize what we have just done, consider $a \in \mathbb{Q}_p$ where $|a|_p \leq 1$. By the theorem, $a = b_0 + b_1 p + b_2 p^2 + \ldots$ where $b_i \in \mathbb{Z}$ satisfy $0 \leq b_i \leq p - 1$.

$$\begin{gathered} a_1 = b_0 \\ a_2 = b_0 + b_1 p \\ a_3 = b_0 + b_1 p + b_2 p^2 \\ \vdots \end{gathered}$$

and so on. Note how $a_3 \equiv a_2 \pmod{p^2}$ which essentially kills off terms $p^2, p^3, \ldots$. When $|a|_p > 1$, $\exists N$ such that $|p^N a|_p = \frac{1}{p^N}|a|_p$. As N increases, $\frac{1}{p^N}|a|_p \leq 1$. So,

$$p^N a = b_0 + b_1 p + b_2 p^2 + \ldots$$

$$a = \frac{b_0}{p^N} + \frac{b_1}{p_{N+1}} + \frac{b_2}{p^{N+2}} + \ldots + b_N + b_{N+1} p + \ldots$$

This is the p-adic expansion of a and will be a convenient way to write out numbers in $\mathbb{Q}_p$. Now, what might the p-adic integers look like? They are numbers in $\mathbb{Q}_p$ whose p-adic expansion involves no negative powers of p. $\mathbb{Z}_p = \{a \in \mathbb{Q}_p \mid |a|_p \leq 1\}$. If we take $a, b \in \mathbb{Q}_p$, if $\frac{(a-b)}{p^n} \in \mathbb{Z}_p$ then we can say that $a \equiv b \pmod{p^n}$. This is equivalent to saying that if the first nonzero digit in the p-adic expansion of $a-b$ does not occur prior to the p^n-place.

1.1.4. *Arithmetic in* $\mathbb{Q}_p$. Now we have set up a new way of writing p-adic numbers. Since $\mathbb{Q}_p$ is a field, let's now figure out how to add, subtract, multiply, and divide. Let's put our new theoretical knowledge to a 'practical' use. These operations in $\mathbb{Q}_p$ are extremely similar to the corresponding operations in our normal decimal numbers, the same operations we learned in grade school. The only difference is that we work from left to right in $\mathbb{Q}_p$ rather than right to left. This includes borrowing and carrying.

Example 4. *Addition in* $\mathbb{Q}_7$
Step 1: Since $5+4=9=7^1+2\equiv 2 \pmod 7$,

$$\begin{array}{rl} & 5\times 7^{-1}+0\times 7^{0}+4\times 7^{1}+\dots \\ + & \underline{4\times 7^{-1}+6\times 7^{0}+5\times 7^{1}+\dots} \\ & 2\times 7^{-1} \end{array}$$

Step 2: Now we carry the 7^1 *to the next power of* 7, *namely* 7^0 *in this example. In this step, we now have* $0+6+1=7\equiv 0 \pmod 7$.

$$\begin{array}{rl} & 5\times 7^{-1}+0\times 7^{0}+4\times 7^{1}+\dots \\ + & \underline{4\times 7^{-1}+6\times 7^{0}+5\times 7^{1}+\dots} \\ & 2\times 7^{-1}+0\times 7^{0} \end{array}$$

Step 3: We continue to add an carry as far as needed, ending up with

$$\begin{array}{rl} & 5\times 7^{-1}+0\times 7^{0}+4\times 7^{1}+\dots \\ + & \underline{4\times 7^{-1}+6\times 7^{0}+5\times 7^{1}+\dots} \\ & 2\times 7^{-1}+0\times 7^{0}+3\times 7^{1}+\dots \end{array}$$

□

Subtraction works the same way. Here is an example using the same numbers as in the previous example.

Example 5. *Subtraction in* $\mathbb{Q}_7$
Since we cannot subtract 4 *from* 2*, we try to borrow from the* 7^0 *place. Unfortunately this is* 0*, so we try the next place over,* 7^1

$$\begin{array}{r} 2\times 7^{-1}+0\times 7^0+3\times 7^1+\dots \\ -\ \underline{4\times 7^{-1}+6\times 7^0+5\times 7^1+\dots} \end{array} \quad\Longrightarrow\quad \begin{array}{r} 9\times 7^{-1}+6\times 7^0+2\times 7^1+\dots \\ -\ \underline{4\times 7^{-1}+6\times 7^0+5\times 7^1+\dots} \end{array}$$

Now we can continue to subtract and borrow like we just did to finish the problem.

$$\begin{array}{r} 2\times 7^{-1}+0\times 7^0+3\times 7^1+\dots \\ \underline{4\times 7^{-1}+6\times 7^0+5\times 7^1+\dots} \\ 5\times 7^{-1}+0\times 7^0+4\times 7^1+\dots \end{array}$$

□

We will not go through multiplication and division in such detail. Here are two completed examples that would be beneficial to work through if there are any uncertainties about the process.

Example 6. *Multiplication in* $\mathbb{Q}_7$

$$\begin{array}{r} 3+6\times 7+2\times 7^2+\dots \\ \times\ \underline{4+5\times 7+1\times 7^2+\dots} \\ 5+4\times 7+4\times 7^2+\dots \\ 1\times 7+4\times 7^2+\dots \\ \underline{\qquad\qquad\qquad 3\times 7^2+\dots} \\ 5+5\times 7+4\times 7^2+\dots \end{array}$$

□

Example 7. *Division in* $\mathbb{Q}_7$

$$\begin{array}{r|r}
 & 5+1\times 7+6\times 7^2+\ldots \\ \cline{2-2}
3+5\times 7+1\times 7^2+\ldots & 1+2\times 7+4\times 7^2+\ldots \\
 & \underline{1+6\times 7+1\times 7^2+\ldots} \\
 & 3\times 7+2\times 7^2+\ldots \\
 & \underline{3\times 7+5\times 7^2+\ldots} \\
 & 4\times 7^2+\ldots \\
 & \underline{4\times 7^2+\ldots}
\end{array}$$

□

The most important things to remember when doing arithmetic in $\mathbb{Q}_p$ is to remember to work left to right and to remember what the value of p is.

1.1.5. *Hensel's Lemma.*

Theorem 2. (Hensel's Lemma). *Let* $F(x) = c_0 + c_1x + \ldots + c_nx^n$ *be a polynomial whose coefficients are* p*-adic integers. Let* $F'(x) = c_1 + 2c_2x + 3c_3x^2 + \ldots + nc_nx^{n-1}$ *be the derivative of* $F(x)$*. Let* a_0 *be a* p*-adic integer such that* $F(a_0) \neq 0 \pmod{p})$*. Then there exists a unique* p*-adic integer* a *such that*

$$F(a) = 0 \ \ \textit{and} \ \ a \equiv a_0 \pmod{p}.$$

This version of the lemma was apparently first give in Serge Lang's Ph.D. thesis in 1952 (*Annals of Mathematics*, Vol. 55, p. 380). Hensel's lemma is often called the p-adic Newton's lemma. It is important result in valuation theory which gives information on finding roots of polynomials [7]. The following proof is taken from Neal Koblitz's book [6] because it is one of the more elegant proofs I have found.

Proof. By induction on n, we will prove that there are unique sequences of rational integers $a_1, a_2, \ldots$ such that for all $n \geq 1$:

(1) $F(a_n) \equiv 0 \pmod{p^{n+1}}$.
(2) $a_n \equiv a_{n-1} \pmod{p^n}$.
(3) $0 \leq a_n < p^{n+1}$.

If $n = 1$, first let $\tilde{a}_0$ be the unique integer in $\{0, 1, \ldots, p-1\}$ which is congruent to a_0 mod p. Any a_1 satisfying (2) and (3) must be of the form $\tilde{a}_0 + b_1 p$, where $0 \leq b_1 \leq p - 1$. Now, looking at $F(\tilde{a}_0 = b_1 p)$, we expand the polynomial. Since we only need congruence to 0 mod p^2, we can ignore any terms divisible by p^2:

$$\begin{aligned} F(a_1) = F(\tilde{a}_0 + b_1 p) &= \sum c_i (\tilde{a}_0 + b_1 p)^i \\ &= \sum (c_i \tilde{a}_0^i + i c_i \tilde{a}_0^{i-1} b_1 p + \text{terms divisible by } p^2) \\ &\equiv \sum c_i \tilde{a}_0^i + \left(\sum i c_i \tilde{a}_0^{i-1} \right) b_1 p \pmod{p^2} \\ &= F(\tilde{a}_0) + F'(\tilde{a}_0) b_1 p. \end{aligned}$$

Since $F(a_0) \equiv 0 \pmod{p}$ by assumption, we can write $F(\tilde{a}_0) \equiv \alpha p \pmod{p^2}$ for some $\alpha \in \{0, 1, \ldots, p-1\}$. In order to get $F(a_1) \equiv 0 \pmod{p^2}$ we must get $\alpha p + F'(\tilde{a}_0) b_1 p \equiv 0 \pmod{p^2}$, or equivalently, $\alpha + F'(\tilde{a}_0) b_1 \equiv 0 \pmod{p}$. But, since $F'(a_0) \not\equiv 0 \pmod{p}$ by assumption, this equation can always be solved for the unknown b_1. Using Lemma 1 from 1.1.3, we chose $b_1 \in \{0, 1, \ldots, p-1\}$ so that $b_1 \equiv -\alpha / F'(\tilde{a}_0) \pmod{p}$. Clearly this b_1 is uniquely determined by this condition.

Now, to proceed with the induction, suppose we already have $a_1, a_2, \ldots, a_{n-1}$. We want to find a_N By (2) and (3), we need $a_n = a_{n-1} + b_n p^n$ with $b_n \in \{0, 1, \ldots, p-1\}$. We expand $F(a_{n-1} + b_n p^n)$ as we did before when n was 1, only this time we ignore terms divisible by p^{n+1}. This gives us:

$$F(a_n) = F(a_{n-1} + b_n p^n) \equiv F(a_{n-1}) b_n p^n \pmod{p^{n+1}}.$$

Since $F(a_{n-1}) \equiv 0 \pmod{p^n}$ by the induction assumption, we can write $F(a_{n-1}) \equiv \alpha' p^n \pmod{p^{n+1}}$, and our goal of $F(a_n) \equiv 0 \pmod{p^{n_1}}$ becomes

$$\begin{aligned} \alpha' p^n + F'(a_{n-1}) b_n p^n \equiv 0 \pmod{p^{n+1}} \\ \alpha' + F'(a_{n-1}) b_n \equiv 0 \pmod{p} \end{aligned}$$

Now, since $a_{n-1} \equiv a_0 \pmod{p}$, it easily follows that $F'(a_{n-1}) \equiv F'(a_0) \not\equiv 0 \pmod{p}$, and we can find the required b_n the exact same way as in the case of b_1. The theorem follows immediately from what was just proved, just let $a = \tilde{a}_0 + b_1p + b_2p^2 + \ldots$. Since for all n we have $F(a) \equiv F(a_n) \equiv 0 \pmod{p^{n+1}}$, it follows that the p-adic number $F(a)$ must be 0. Conversely, any $a = \tilde{a}_0 + b_1p + b_2p^2 + \ldots$. gives a sequence of a_n as in (1), (2), and (3). The uniqueness of that sequence implies the uniqueness of the a.

□

2. A Glimpse at Dirichlet Functions

Dirichlet functions were created by none other than Johann Peter Gustave Lejeune Dirichlet. Born February 13, 1805 in the French Empire, he attended the Jesuit gymnasium in Cologne where he learned from Georg Ohm. His first paper was a partial proof of Fermat's last theorem for the case $n = 5$. In 1831, Dirichlet introduced Dirichlet characters and their L-series in order to prove a theory of his about arithmetic progressions. Dirichlet only studied these functions for real s, especially as it tends to 1. Bernhard Riemann extended these functions to complex s in 1859 [2]. Dirichlet characters are used to define Dirichlet L-functions, which are meromorphic functions with a variety of interesting analytic properties. If χ is a Dirichlet character, one defines its Dirichlet L-series by

$$L(\chi, s) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$$

where s is a complex number with real part > 1 [3].

2.1. Definition and properties.

Definition 9. *A Dirichlet character is any function, $\chi : \mathbb{Z} \to \mathbb{C}$, which satisfies the following three properties:*

(1) *$\exists k \in \mathbb{Z}^+$ such that $\chi(n) = \chi(n + k)$, $\forall n \in \mathbb{Z}$. This is called the* modulus *of χ.*

(2) *$gcd(n,k) > 1 \implies \chi(n) = 0$; $gcd(n,k) = 1 \implies \chi(n) \neq 0$.*

(3) $\chi(m,n) = \chi(m)\chi(n),\ \forall m,n \in \mathbb{Z}$

Note: property (1) *of a Dirichlet character is equivalent to saying $a \equiv b$* mod $k \implies \chi(a) = \chi(b)$.

Corollary 1. *$\chi(0) = 0,\ \forall k > 1$, and $\chi(0) = 1$ if $k = 1$.*

Proof. By property (1), $\chi(0) = \chi(k)$ since $0 \equiv k \mod k$. Since $gcd(k,k) = k$, then property (2) implies that $\chi(k) = 0$ when $k > 1$ and $\chi(0) = 1$ when $k = 1$. □

Corollary 2. *$\chi(1) = 1$, for any Dirichlet character.*

Proof. Property (3) of the Dirichlet definition implies that $\chi(1) = \chi(1)\chi(1)$, and since $gcd(1,k) = 1,\ \forall k$, then $\chi(1) \neq 0$ by property (2). Hence $\frac{\chi(1)}{\chi(1)} = \chi(1) = 1$. □

Corollary 3. *$gcd(a,k) = 1 \implies \chi(a)$ is a $\varphi(k)^{th}$ root of unity.*

Proof. $a^{\varphi(k)} \equiv 1 \mod k$, where $\varphi(k)$ is the Euler φ-function, that is $\varphi(k)$ is the number of integers $j \leq k$ such that $gcd(j,k) = 1$. This implies that $\chi(a^{\varphi(k)}) = 1$ by property (1) and Corollary 2. Since χ is multiplicative, we get $\chi(a^{\varphi(k)}) = \chi(a)^{\varphi(k)} = 1$. Hence $\chi(a)$ is a solution to the polynomial $z^{\varphi(k)} = 1$, which means $\chi(a)$ is a $\varphi(k)^{\text{th}}$ root of unity; the n^{th} roots of unity are the complex numbers of the form $e^{2\pi i\ell/n}$ where $0 \leq \ell < n$. □

Definition 10. *The unique Dirichlet character of modulus* 1 *is called the* trivial character.

Definition 11. *A Dirichlet character, $\chi(n)$, is called* principal *if it is equal to 1 for all n relatively prime to its modulus and equal to 0 otherwise.*

Definition 12. *A Dirichlet character is called* real *if it only assumes real values. Therefore, Corollary 3 implies that a real character can only attain the values 0, 1, or -1. Any character that is not real is called* complex.

2.2. **Character Tables and Constructions.**

Fix a modulus k. Then $\chi(a)=\chi(b) \iff a \equiv b \pmod{k}$, where χ is any k-modulus Dirichlet character function. We know that the values that χ can take on are the $\varphi(k)$ roots of unity. The important thing to remember though is how the group of units modulo k are generated. The set of all units, modulo k, form an abelian group.

Definition 13. *A unit modulo k is an integer in $\mathbb{Z}_k$ such that it has a multiplicative inverse. That is, a is a unit if there exists b in $\mathbb{Z}_k$ such that $ab = ba = 1 \pmod{k}$.*
Note: This is not the same as the roots of unity.

The Dirichlet character designations $\chi_1, \chi_2, \ldots$ are arbitrary. Usually, χ_1 is reserved for the trivial character. In the character charts, the rows can be rearranged because of these arbitrary designations.

Example 8. *Character table modulus 5: a cyclic group*

Because $\varphi(5)=4$ there are 4 unique Dirichlet characters making the rows of the table. Since this is modulo 5, there are 5 possible values for n which make the columns of the table. 2 will generate the group of units modulo 5 so first we tackle that n value first. This is because $2^1 \equiv 2 \pmod{5}, 2^2 \equiv 4 \pmod{5}, 2^3 \equiv 3 \pmod{5}, 2^4 \equiv 1 \pmod{5}$ is the set of all units in $\mathbb{Z}_5$.

Since $\varphi(5)=4$, each Dirichlet character takes on values in the set of 4^{th} roots of unity. And since 2 will generate all the units of $\mathbb{Z}_5$, then for any fixed value of $\chi(2)$, we will define one unique character function. (Note: since the sets of units are the integers modulo k that have inverses, then $gcd(n,k)=1$ if n is a unit. Hence, if an integer m modulo k is not *a unit, then $gcd(m,k) \neq 1 \implies \chi(m)=0$).*

χ	0	1	2	3	4
$\chi_1(n)$	0	1	1	1	1
$\chi_2(n)$	0	1	i	$-i$	-1
$\chi_3(n)$	0	1	-1	-1	1
$\chi_4(n)$	0	1	$-i$	i	-1

Since the 4^{th} roots of unity are $1, -1, i, -i$, let's start the first character function, $\chi_1(n)$, by setting $\chi(2) = 1$. Thus

$$\chi(2)\chi(2) = \chi(2 \cdot 2) = \chi(4) = 1 \cdot 1 = 1.$$

$$\chi(2)\chi(4) = \chi(2 \cdot 4) = \chi(8) = \chi(3) = 1 \cdot 1 = 1.$$

$$\chi(2)\chi(3) = \chi(2 \cdot 3) = \chi(6) = \chi(1) = 1 \cdot 1 = 1.$$

This leaves $\chi(0) = 0$. Now let the second character function start with $\chi(2) = -1$. This implies that

$$\chi(2)\chi(2) = \chi(2 \cdot 2) = \chi(4) = -1 \cdot -1 = 1.$$

$$\chi(2)\chi(4) = \chi(2 \cdot 4) = \chi(8) = \chi(3) = -1 \cdot 1 = -1.$$

$$\chi(2)\chi(3) = \chi(2 \cdot 3) = \chi(6) = \chi(1) = -1 \cdot -1 = 1.$$

Setting the third character to be $\chi(2) = i$,

$$\chi(2)\chi(2) = \chi(2 \cdot 2) = \chi(4) = i \cdot i = -1.$$

$$\chi(2)\chi(4) = \chi(2 \cdot 4) = \chi(8) = \chi(3) = i \cdot -1 = -i.$$

$$\chi(2)\chi(3) = \chi(2 \cdot 3) = \chi(6) = \chi(1) = i \cdot -i = 1.$$

The unit remaining will be assigned to the last character, $\chi(2) = -i$.

$$\chi(2)\chi(2) = \chi(2 \cdot 2) = \chi(4) = -i \cdot -i = -1.$$

$$\chi(2)\chi(4) = \chi(2 \cdot 4) = \chi(8) = \chi(3) = -i \cdot -1 = i.$$

$$\chi(2)\chi(3) = \chi(2 \cdot 3) = \chi(6) = \chi(1) = -i \cdot i = 1.$$

These values all correspond to the values in the above table. □

Modulus 5 is a straight forward example. However, there are other types of groups out there. Consider modulus 8. This is more complicated since $\mathbb{Z}_8$ has a unit group structure of $C_2 \times C_2$ and has two generators for the set of units; they are 3 and 7. We know how to deal with one generator, but what about two?

Example 9. *The set of units modulo* 8 *is* $\{1, 3, 5, 7\}$ *which can be generated by powers of* 3 *and* 7*. Thus* $\chi(0) = \chi(2) = \chi(4) = \chi(6) = 0$ *for all character functions below. These numbers also share a factor with* 8 *so their gcd with* 8 *is not* 1*. Since* $\varphi(8) = 4$*, there will be exaclty* 4 *unique Dirichlet characters of modulus* 8*. Since* 7 *generates one of the copies of* C_2 *and* 3 *generates the other copy, then we can arbistrarily assign* 2^{nd} *roots of unity to each of* $\chi(3)$ *and* $\chi(7)$*.*

Since there are two choices for each of $\chi(3)$ *and* $\chi(7)$*, then there are four possible choices:*

- $\chi(3) = 1$ $\quad\quad\chi(7) = 1$
- $\chi(3) = 1$ $\quad\quad\chi(7) = -1$
- $\chi(3) = -1$ $\quad\quad\chi(7) = 1$
- $\chi(3) = -1$ $\quad\quad\chi(7) = -1$

The same method of multiplication as in example 8 will yield the following table of values.

$\chi \setminus n$	0	1	2	3	4	5	6	7
$\chi_1(n)$	0	1	0	1	0	1	0	1
$\chi_2(n)$	0	1	0	1	0	-1	0	-1
$\chi_3(n)$	0	1	0	-1	0	1	0	-1
$\chi_4(n)$	0	1	0	-1	0	-1	0	1

□

3. Concluding Remarks

This paper is a partial compilation of my notes from an independent study I did under Professor C. Doug Haessig in the Fall of 2008 and Spring of 2009 at the University of Rochester. It closely follows the two books that we studied from, Neal Koblitz [6] and Kenkichi Iwasawa [5].

I would like to thank Professor Haessig for all the time he has spent teaching me some really amazing math and for all of the times my fellow students and I sidetracked him from his office hours.

References

[1] http://www-history.mcs.st-andrews.ac.uk/Mathematicians/Hensel.html

[2] http://www-history.mcs.st-andrews.ac.uk/Biographies/Dirichlet.html

[3] http://en.wikipedia.org/wiki/Dirichlet_character

[4] http://everything2.com/title/p-adic%2520norm

[5] Iwasawa, Kenkichi, *Lectures on p-Adic L-functions.* Princeton University Press, 1972

[6] Koblitz, Neal, *Graduate Texts in Mathematics: p-adic Numbers, p-adic Analysis, and Zeta-Functions.* Springer, New York, 2nd Edition, 1991

[7] Weisstein, Eric W. "Hensel's Lemma." From MathWorld–A Wolfram Web Resource. http://mathworld.wolfram.com/HenselsLemma.html

[8] Weisstein, Eric W. "p-adic Norm." From MathWorld–A Wolfram Web Resource. http://mathworld.wolfram.com/p-adicNorm.html

[9] Weisstein, Eric W. "p-adic Number." From MathWorld–A Wolfram Web Resource. http://mathworld.wolfram.com/p-adicNumber.html