QUADRATIC RECIPROCITY IN ODD CHARACTERISTIC

KEITH CONRAD

1. Introduction

Let π be irreducible in $\mathbf{F}[T]$, where $\mathbf{F}$ is a finite field with odd characteristic. For instance, $\mathbf{F}$ could be $\mathbf{F}_p = \mathbf{Z}/(p)$ for a prime $p \neq 2$. The basic question we ask is: how can we decide if, for $f \in \mathbf{F}[T]$ with $f \not\equiv 0 \bmod \pi$, the congruence

$$f \equiv x^2 \bmod \pi$$

is solvable? In alternate notation, we write: when is $f \equiv \square \bmod \pi$?

Example 1.1. In $\mathbf{F}_5[T]$, is $T^2 + 3T + 3 \equiv \square \bmod T^3 + T + 1$?

The answer to questions like this can be found with the quadratic reciprocity law in $\mathbf{F}[T]$. It has a strong resemblance to the quadratic reciprocity law in $\mathbf{Z}$. We restrict to $\mathbf{F}$ with odd characteristic because when $\mathbf{F}$ has characteristic 2 *every* element of $\mathbf{F}[T]/(\pi)$ is a square, so our basic question is silly in characteritic 2. (There is a good analogue of quadratic reciprocity in characteristic 2, but we don't discuss it here.)

In Section 2, we define the Legendre symbol in $\mathbf{F}[T]$, establish some of its properties, and state the quadratic reciprocity law. The proof of the law is in Section 3. Some applications are given in Section 4 and a little history behind the reciprocity law is in Section 5.

Throughout our discussion, $\mathbf{F}$ will denote a finite field with *odd* characteristic and size q. For a nonzero polynomial $f \in \mathbf{F}[T]$, we set

$$\mathrm{N}f = \#\mathbf{F}[T]/(f) = q^{\deg f},$$

which is the analogue of the absolute value on $\mathbf{Z}$ ($\#\mathbf{Z}/(n) = |n|$ for $n \neq 0$). When we make analogies between $\mathbf{F}[T]/(\pi)$ and $\mathbf{Z}/(p)$, it will be understood that p is an odd prime.

2. The Legendre symbol

Let π be irreducible in $\mathbf{F}[T]$. The number of nonzero elements in the field $\mathbf{F}[T]/(\pi)$ is $\mathrm{N}\pi - 1 = q^{\deg \pi} - 1$, and squaring is 2-to-1 on these elements, so the number of nonzero squares in $\mathbf{F}[T]/(\pi)$ is $(\mathrm{N}\pi - 1)/2$. This is analogous to $(p-1)/2$ being the number of nonzero squares in $\mathbf{Z}/(p)$.

Any $f \not\equiv 0 \bmod \pi$ satisfies $f^{\mathrm{N}\pi - 1} \equiv 1 \bmod \pi$. Therefore $f^{(\mathrm{N}\pi-1)/2}$ satisfies $x^2 \equiv 1 \bmod \pi$, so $f^{(\mathrm{N}\pi-1)/2} \equiv \pm 1 \bmod \pi$.

Theorem 2.1. *For $f \not\equiv 0 \bmod \pi$, $f^{(\mathrm{N}\pi-1)/2} \equiv 1 \bmod \pi$ if and only if $f \bmod \pi$ is a square.*

Proof. This is just like the fact that, for $a \not\equiv 0 \bmod p$, $a^{(p-1)/2} \equiv 1 \bmod p$ if and only if $a \equiv \square \bmod p$. We will give details here, but omit proofs of later results which resemble proofs from the integer case.

If $f \equiv g^2 \bmod \pi$, then $f^{(\mathrm{N}\pi-1)/2} \equiv g^{\mathrm{N}\pi - 1} \equiv 1 \bmod \pi$. So any nonzero square in the field $\mathbf{F}[T]/(\pi)$ is a root of $X^{(\mathrm{N}\pi-1)/2} - 1$. This polynomial has at most $(\mathrm{N}\pi - 1)/2$ roots in a

field, and there are $(\mathrm{N}\pi - 1)/2$ nonzero squares in $\mathbf{F}[T]/(\pi)$, so the roots of the polynomial are exactly the nonzero squares. □

Definition 2.2. For irreducible π in $\mathbf{F}[T]$ and any $f \not\equiv 0 \bmod \pi$, set

$$\left(\frac{f}{\pi}\right) = \begin{cases} 1, & \text{if } f \equiv \square \bmod \pi, \\ -1, & \text{if } f \not\equiv \square \bmod \pi. \end{cases}$$

When $f \equiv 0 \bmod \pi$, set $(\frac{f}{\pi}) = 0$. We call $(\frac{f}{\pi})$ a *Legendre symbol*.

Theorem 2.3. *The Legendre symbol satisfies the following properties:*

(1) *if* $f_1 \equiv f_2 \bmod \pi$, *then* $\left(\dfrac{f_1}{\pi}\right) = \left(\dfrac{f_2}{\pi}\right)$,

(2) $f^{(\mathrm{N}\pi-1)/2} \equiv \left(\dfrac{f}{\pi}\right) \bmod \pi$ *for all* f *in* $\mathbf{F}[T]$,

(3) $\left(\dfrac{fg}{\pi}\right) = \left(\dfrac{f}{\pi}\right)\left(\dfrac{g}{\pi}\right)$,

(4) $\left(\dfrac{f^2}{\pi}\right) = 1$ *if* $f \not\equiv 0 \bmod \pi$.

Proof. The proofs are identical to the classical case in $\mathbf{Z}$, and are left to the reader. The proof of the second property, which is analogous to Euler's congruence, uses Theorem 2.1. □

Example 2.4. In $\mathbf{F}_3[T]$, the polynomial $\pi(T) = T^3 - T + 1$ is irreducible. We compute $(\frac{T}{\pi})$ using Euler's congruence:

$$\begin{aligned} \left(\frac{T}{\pi}\right) &\equiv T^{(27-1)/2} \bmod \pi \\ &\equiv T^{13} \bmod \pi \\ &\equiv -1 \bmod \pi, \end{aligned}$$

so $(\frac{T}{\pi}) = -1$.

In the Legendre symbol $(\frac{f}{\pi})$, the modulus π may without loss of generality be taken to be *monic*. When $f \neq 0$, factor it into a constant times a product of monic irreducibles (not necessarily distinct):

$$f = c\pi_1\pi_2 \cdots \pi_r.$$

Then

$$\left(\frac{f}{\pi}\right) = \left(\frac{c}{\pi}\right)\left(\frac{\pi_1}{\pi}\right)\left(\frac{\pi_2}{\pi}\right)\cdots\left(\frac{\pi_r}{\pi}\right).$$

Thus, the general calculation of $(\frac{f}{\pi})$ is reduced to the case of $(\frac{c}{\pi})$ for $c \in \mathbf{F}^\times$ and $(\frac{\pi_1}{\pi_2})$ for distinct monic irreducibles π_1 and π_2.

Theorem 2.5. *For distinct monic irreducible* π_1 *and* π_2 *in* $\mathbf{F}[T]$,

$$\left(\frac{\pi_2}{\pi_1}\right) = (-1)^{\frac{\mathrm{N}\pi_1-1}{2}\cdot\frac{\mathrm{N}\pi_2-1}{2}}\left(\frac{\pi_1}{\pi_2}\right). \tag{2.1}$$

For $c \in \mathbf{F}^\times$ *and irreducible* π *in* $\mathbf{F}[T]$,

$$\left(\frac{c}{\pi}\right) = c^{(\mathrm{N}\pi-1)/2}. \tag{2.2}$$

Equation (2.1) is the main law of quadratic reciprocity and (2.2) is the supplementary law. The supplementary law closely resembles the formula $(\frac{-1}{p}) = (-1)^{(p-1)/2}$. In $\mathbf{F}[T]$ there is no parallel to the supplementary law for $(\frac{2}{p})$. Theorem 2.5 is proved in Section 3.

Example 2.6. Let's see an example in $\mathbf{F}_3[T]$. The polynomials T^2+1 and T^3-T+1 are both irreducible, with respective norms 9 and 27. Then

$$\begin{aligned}\left(\frac{T^2+1}{T^3-T+1}\right) &= (-1)^{\frac{9-1}{2}\cdot\frac{27-1}{2}}\left(\frac{T^3-T+1}{T^2+1}\right)\\ &= \left(\frac{T+1}{T^2+1}\right)\\ &= (-1)^{\frac{3-1}{2}\cdot\frac{9-1}{2}}\left(\frac{T^2+1}{T+1}\right)\\ &= \left(\frac{2}{T+1}\right)\\ &= 2^{(3-1)/2}\\ &= 2\\ &= -1.\end{aligned}$$

The calculations are carried out in characteristic 3, which is why $2 = -1$.

For computational purposes, it is worthwhile to simplify the exponents appearing in (2.1) and (2.2). The exponent of -1 only matters modulo 2, and

$$\begin{aligned}\frac{\mathrm{N}\pi-1}{2} &= \frac{q^{\deg\pi}-1}{2}\\ &= \left(\frac{q-1}{2}\right)(1+q+\cdots+q^{\deg\pi-1})\\ &\equiv \left(\frac{q-1}{2}\right)\deg\pi \bmod 2\end{aligned}$$

since $q \equiv 1 \bmod 2$.

Therefore the exponent of -1 in the main law can be rewritten as

$$\left(\frac{q-1}{2}\right)\deg\pi_1\cdot\left(\frac{q-1}{2}\right)\deg\pi_2 \equiv \left(\frac{q-1}{2}\right)(\deg\pi_1)(\deg\pi_2) \bmod 2$$

since $a^2 \equiv a \bmod 2$ for any integer a. For $c \in \mathbf{F}^\times$, we can rewrite the right side of (2.2) as $c^{(\mathrm{N}\pi-1)/2} = c^{\frac{q-1}{2}\cdot(1+q+\cdots+q^{\deg\pi-1})}$. Since $c^{(q-1)/2} = \pm 1$, the term $1+q+\cdots+q^{\deg\pi-1}$ only matters modulo 2, so we can replace each power of q with 1. Thus, quadratic reciprocity is equivalent to the formulas

$$\left(\frac{\pi_2}{\pi_1}\right) = (-1)^{(\deg\pi_1)(\deg\pi_2)(q-1)/2}\left(\frac{\pi_1}{\pi_2}\right), \quad \left(\frac{c}{\pi}\right) = c^{(\deg\pi)(q-1)/2}. \tag{2.3}$$

When $\mathbf{F} = \mathbf{F}_p$ for a prime $p \neq 2$, then inside $\mathbf{F}$ we have $c^{(q-1)/2} = c^{(p-1)/2} = (\frac{c}{p})$, using the usual Legendre symbol. Thus, the supplementary law in $\mathbf{F}_p[T]$ takes on the form

$$\left(\frac{c}{\pi}\right) = \left(\frac{c}{p}\right)^{\deg\pi}. \tag{2.4}$$

The expression of the main law in (2.3), rather than in (2.1), is the form in which we will prove it. We wrote the main law originally as in (2.1) rather than as in (2.3) to make clearer the resemblance to the classical case of the integers: the main law in (2.3) merely looks similar to the integer case, while (2.1) looks exactly like the integer case.

From (2.3), we draw an immediate corollary.

Corollary 2.7. *Let q be the size of $\mathbf{F}$. Using the notation of Theorem 2.5, $(\frac{\pi_2}{\pi_1}) = (\frac{\pi_1}{\pi_2})$ if $q \equiv 1 \bmod 4$ or if π_1 or π_2 has even degree. If $\deg \pi$ is even then $(\frac{c}{\pi}) = 1$.*

For example, the main law in $\mathbf{F}_5[T]$ is $(\frac{\pi_2}{\pi_1}) = (\frac{\pi_1}{\pi_2})$, with no extra power of -1 floating around.

3. Proof of the reciprocity law

We start with a proof of the supplementary law for $(\frac{c}{\pi})$. By Euler's congruence,

$$\left(\frac{c}{\pi}\right) \equiv c^{(\mathrm{N}\pi-1)/2} \bmod \pi. \tag{3.1}$$

Both sides are in $\mathbf{F}$, so their congruence modulo π must be equality in $\mathbf{F}$ and the supplementary law drops out.

To prove the main law (2.1), we will use the following four background facts about finite fields, where $q = \#\mathbf{F}$.

(1) If $f(T) \in \mathbf{F}[T]$, then $f(T)^q = f(T^q)$.

(2) For any $f(T) \in \mathbf{F}[T]$, there is a field $F \supset \mathbf{F}$ such that $f(T)$ has a full set of roots in F:
$$f(T) = c(T - r_1)(T - r_2)\cdots(T - r_d).$$
For example, let $f(T) = T^2 + 1$ in $\mathbf{F}_3[T]$. Let $F = \mathbf{F}_3[y]/(y^2 + 1)$. In $F[T]$, $f(T) = (T + y)(T - y)$.

(3) When π is irreducible of degree m in $\mathbf{F}[T]$, with root r in some field $F \supset \mathbf{F}$, then all the roots are $r, r^q, \cdots, r^{q^{m-1}}$. Therefore in $F[T]$,
$$\pi(T) = c(T - r)(T - r^q)\cdots(T - r^{q^{m-1}}).$$
For example, let $f(T) = T^2 + 1$ in $\mathbf{F}_3[T]$. Let $F = \mathbf{F}_3[y]/(y^2 + 1)$. In $F[T]$, $f(T) = (T - y)(T - y^3)$ since $y^3 = -y$.

(4) When $f(T) \equiv g(T) \bmod \pi(T)$ and r is a root of $\pi(T)$ in some field $F \supset \mathbf{F}$, then $f(r) = g(r)$.
For example, in $\mathbf{F}_3[T]$, $T^4 + T^3 + 1 \equiv T^3 + T^2 \bmod T^2 + 1$. When $r^2 + 1 = 0$, $r^4 + r^3 + 1 = 2 - r$ and $r^3 + r^2 = 2 - r$.

Now we are ready to prove the main law of quadratic reciprocity.

Let π_1 and π_2 be distinct monic irreducibles in $\mathbf{F}[T]$, with respective degrees m and n. There is a field $F \supset \mathbf{F}$ containing a full set of roots for both π_1 and π_2. Let $\alpha \in F$ be a root of π_1 and β be a root of π_2. Then

$$\pi_1(T) = (T - \alpha)(T - \alpha^q)\cdots(T - \alpha^{q^{m-1}}) \tag{3.2}$$

and

$$\pi_2(T) = (T - \beta)(T - \beta^q)\cdots(T - \beta^{q^{n-1}}). \tag{3.3}$$

From the congruence $(\frac{\pi_1}{\pi_2}) = \pi_1(T)^{(\mathrm{N}\pi_2-1)/2} \bmod \pi_2(T)$, set $T = \beta$ to get

$$\left(\frac{\pi_1}{\pi_2}\right) = \pi_1(\beta)^{(\mathrm{N}\pi_2-1)/2} \tag{3.4}$$

in F. (The left side is a constant ± 1, so it does not change when we substitute β for T.) Similarly,

$$\left(\frac{\pi_2}{\pi_1}\right) = \pi_2(\alpha)^{(\mathrm{N}\pi_1-1)/2} \tag{3.5}$$

in F. Now we use the factorizations of $\pi_1(T)$ and $\pi_2(T)$ over F. From (3.2) and (3.4),

$$\begin{aligned}
\left(\frac{\pi_1}{\pi_2}\right) &= \pi_1(\beta)^{(q^n-1)/2} \\
&= \pi_1(\beta)^{(1+q+\cdots+q^{n-1})(q-1)/2} \\
&= (\pi_1(\beta)\pi_1(\beta)^q \cdots \pi_1(\beta)^{q^{n-1}})^{(q-1)/2} \\
&= (\pi_1(\beta)\pi_1(\beta^q) \cdots \pi_1(\beta^{q^{n-1}}))^{(q-1)/2} \\
&= ((\beta-\alpha)(\beta-\alpha^q)\cdots(\beta-\alpha^{q^{m-1}}) \\
&\qquad (\beta^q-\alpha)(\beta^q-\alpha^q)\cdots(\beta^q-\alpha^{q^{m-1}}) \\
&\qquad\qquad \vdots \\
&\qquad (\beta^{q^{n-1}}-\alpha)(\beta^{q^{n-1}}-\alpha^q)\cdots(\beta^{q^{n-1}}-\alpha^{q^{m-1}}))^{(q-1)/2}
\end{aligned}$$

and from (3.3) and (3.5),

$$\begin{aligned}
\left(\frac{\pi_2}{\pi_1}\right) &= ((\alpha-\beta)(\alpha-\beta^q)\cdots(\alpha-\beta^{q^{n-1}}) \\
&\qquad (\alpha^q-\beta)(\alpha^q-\beta^q)\cdots(\alpha^q-\beta^{q^{n-1}}) \\
&\qquad\qquad \vdots \\
&\qquad (\alpha^{q^{m-1}}-\beta)(\alpha^{q^{m-1}}-\beta^q)\cdots(\alpha^{q^{m-1}}-\beta^{q^{n-1}}))^{(q-1)/2}.
\end{aligned}$$

The terms in these formulas for $(\frac{\pi_1}{\pi_2})$ and $(\frac{\pi_2}{\pi_1})$ agree up to systematic minus signs. There are a total of mn minus signs to get the two formulas to match, so

$$\left(\frac{\pi_2}{\pi_1}\right) = (-1)^{mn(q-1)/2}\left(\frac{\pi_1}{\pi_2}\right). \tag{3.6}$$

The exponent of -1 in (3.6) matches the exponent in (2.3), which concludes the proof of quadratic reciprocity.

All the usual consequences of quadratic reciprocity in $\mathbf{Z}$ carry over to $\mathbf{F}[T]$. We give some concrete calculations in $\mathbf{F}_p[T]$ as illustrations, using (2.3) and (2.4).

Example 3.1. We return to Example 1.1: is $T^2+3T+3 \equiv \square \bmod T^3+T+1$ in $\mathbf{F}_5[T]$? In $\mathbf{F}_5[T]$, $(\frac{\pi_1}{\pi_2}) = (\frac{\pi_2}{\pi_1})$. Both T^2+3T+3 and T^3+T+1 are monic ireducibles, so

$$\begin{aligned}\left(\frac{T^2+3T+3}{T^3+T+1}\right) &= \left(\frac{T^3+T+1}{T^2+3T+3}\right)\\ &= \left(\frac{2T}{T^2+3T+3}\right)\\ &= \left(\frac{2}{T^2+3T+3}\right)\left(\frac{T}{T^2+3T+3}\right)\\ &= \left(\frac{2}{5}\right)^2\left(\frac{T^2+3T+3}{T}\right)\\ &= \left(\frac{3}{T}\right)\\ &= \left(\frac{3}{5}\right)\\ &= -1,\end{aligned}$$

so $T^2+3T+3 \not\equiv \square \bmod T^3+T+1$.

Example 3.2. Is $2T^2+1 \equiv \square \bmod T^3+T+1$ in $\mathbf{F}_5[T]$? The modulus T^3+T+1 is irreducible. By quadratic reciprocity,

$$\begin{aligned}\left(\frac{2T^2+1}{T^3+T+1}\right) &= \left(\frac{2(T^2+3)}{T^3+T+1}\right)\\ &= \left(\frac{2}{T^3+T+1}\right)\left(\frac{T^2+3}{T^3+T+1}\right)\\ &= \left(\frac{2}{5}\right)^3\left(\frac{T^3+T+1}{T^2+3}\right)\\ &= -\left(\frac{3T+1}{T^2+3}\right)\\ &= -\left(\frac{3}{T^2+3}\right)\left(\frac{T+2}{T^2+3}\right)\\ &= -\left(\frac{3}{5}\right)^2\left(\frac{T^2+3}{T+2}\right)\\ &= -\left(\frac{2}{T+2}\right)\\ &= -\left(\frac{2}{5}\right)\\ &= 1,\end{aligned}$$

so $2T^2+1 \bmod T^3+T+1$ is a perfect square. By brute force, a square root is $3T^2+3T+2$.

A Jacobi symbol on $\mathbf{F}[T]$ can be defined in the usual way. For f and g in $\mathbf{F}[T]$, with $\deg g > 0$, factor $g = c\pi_1\pi_2\cdots\pi_s$ with $c \in \mathbf{F}^\times$ and monic irreducible π_i (not necessarily

distinct). Set

$$\left(\frac{f}{g}\right) = \left(\frac{f}{\pi_1}\right)\left(\frac{f}{\pi_2}\right)\cdots\left(\frac{f}{\pi_s}\right).$$

Here is the main law and the supplementary law of Jacobi reciprocity:

$$\left(\frac{f}{g}\right) = (-1)^{\frac{\mathrm{N}f-1}{2}\cdot\frac{\mathrm{N}g-1}{2}}\left(\frac{g}{f}\right) \tag{3.7}$$

for monic relatively prime nonconstant f and g, and

$$\left(\frac{c}{g}\right) = c^{(\mathrm{N}g-1)/2} \tag{3.8}$$

for $c \in \mathbf{F}^\times$ and nonconstant g. The proofs are left to the reader.

Versions of (3.7) and (3.8) which are better for computations are

$$\left(\frac{f}{g}\right) = (-1)^{(\deg f)(\deg g)(q-1)/2}\left(\frac{g}{f}\right), \quad \left(\frac{c}{g}\right) = c^{(\deg g)(q-1)/2}. \tag{3.9}$$

In particular, when $q \equiv 1 \bmod 4$, (3.7) simplifies to $(\frac{f}{g}) = (\frac{g}{f})$. When $\mathbf{F} = \mathbf{F}_p$, so nonzero constants can be viewed as integers modulo p, the supplementary law (3.8) can be rewritten as

$$\left(\frac{c}{g}\right) = \left(\frac{c}{p}\right)^{\deg g}. \tag{3.10}$$

4. Applications

We give applications of the Jacobi reciprocity law in $\mathbf{F}[T]$, both computational and theoretical, which correspond to some basic applications of Jacobi reciprocity in $\mathbf{Z}$.

Example 4.1. In $\mathbf{F}_3[T]$, is the quadratic congruence $x^2 + Tx + T + 1 \equiv 0 \bmod T^3 + T^2 - 1$ solvable?

The modulus $T^3 + T^2 - 1$ is irreducible. Denote it by π. Solvability of the congruence for x is equivalent to the discriminant being a square. The discriminant is $T^2 - 4(T+1) = T^2 - T - 1$. We compute

$$\begin{aligned}\left(\frac{T^2-T-1}{T^3+T^2-1}\right) &= \left(\frac{T^3+T^2-1}{T^2-T-1}\right)\\ &= \left(\frac{1}{T^2-T-1}\right)\\ &= 1,\end{aligned}$$

so the congruence has solutions. An explicit search finds them: $T^2 + 2T + 2$ and $2T^2 + 1$.

For fixed nonzero $a \in \mathbf{Z}$, the condition $(\frac{a}{p}) = 1$ can be converted by the quadratic reciprocity law into congruence conditions on odd primes p which don't divide a. Reciprocity in $\mathbf{F}[T]$ leads to similar results for polynomials.

Example 4.2. In $\mathbf{F}_3[T]$, we will describe the condition $(\frac{T^3-T}{\pi}) = 1$ in terms of congruences on monic irreducible π not dividing $T^3 - T$ and a parity constraint on $\deg \pi$. In fact, since we are going to use Jacobi reciprocity, there is nothing special about a prime denominator. For any monic nonconstant g in $\mathbf{F}_3[T]$ which is relatively prime to $T^3 - T$, we analyze the condition $(\frac{T^3-T}{g}) = 1$.

By (3.9) and (3.10) in $\mathbf{F}_3[T]$,

$$\begin{aligned}\left(\frac{T^3-T}{g}\right) &= (-1)^{\deg g}\left(\frac{g}{T^3-T}\right)\\ &= (-1)^{\deg g}\left(\frac{g}{T}\right)\left(\frac{g}{T-1}\right)\left(\frac{g}{T+1}\right)\\ &= (-1)^{\deg g}\left(\frac{g(0)}{3}\right)\left(\frac{g(1)}{3}\right)\left(\frac{g(2)}{3}\right)\\ &= (-1)^{\deg g}\left(\frac{g(0)g(1)g(2)}{3}\right).\end{aligned}$$

Letting g run through the 8 units of $\mathbf{F}_3[T]/(T^3-T)$, we get the value 1 under the following conditions:

$$\deg g \text{ is even and } g \equiv 1,\ T^2+1,\ T^2+T+2,\ T^2+2T+2 \bmod T^3-T \tag{4.1}$$

and

$$\deg g \text{ is odd and } g \equiv 2,\ 2T^2+2,\ 2T^2+2T+1,\ 2T^2+T+1 \bmod T^3-T. \tag{4.2}$$

Thus, for monic g in $\mathbf{F}_3[T]$ which is relatively prime to T^3-T, we have $(\frac{T^3-T}{g}) = 1$ if and only if g satisfies either (4.1) or (4.2).

When a is a fixed squarefree integer, the Jacobi symbol $(\frac{a}{n})$ as a function of $n > 1$ has period $4|a|$ if $a \equiv 1 \bmod 4$ and period $|a|$ if $a \equiv 2, 3 \bmod 4$. Here is a polynomial analogue.

Theorem 4.3. *When f is a fixed squarefree nonconstant polynomial in $\mathbf{F}[T]$ or a nonsquare constant in $\mathbf{F}^\times$, the Jacobi symbol $(\frac{f}{g})$ as a function of nonconstant monic g relatively prime to f satisfies*

$$g_1 \equiv g_2 \bmod f,\ \deg g_1 \equiv \deg g_2 \bmod 2 \Longrightarrow \left(\frac{f}{g_1}\right) = \left(\frac{f}{g_2}\right), \tag{4.3}$$

and we can't replace the modulus f by a smaller degree polynomial.

Proof. When $f = c$ is a constant nonsquare in $\mathbf{F}$, $(\frac{f}{g}) = c^{(\deg g)(q-1)/2} = (-1)^{\deg g}$ by the supplementary law, so the result is clear. Now take f to be a squarefree nonconstant polynomial. Then (4.3) follows from the main law of Jacobi reciprocity.

To show f is the smallest modulus of periodicity, we show for any monic irreducible factor of f, say π, that f/π is not a modulus of periodicity. (The minimal modulus of periodicity divides f.) If f/π were a modulus of periodicity, then whenever g is monic with even degree and $g \equiv 1 \bmod f/\pi$, we would have $(\frac{f}{g}) = 1$. (Use $g_1 = g$ and $g_2 = 1 + f^2$ in (4.3).) We are going to find g such that $(\frac{f}{g}) = -1$ while g is monic of even degree and $g \equiv 1 \bmod f/\pi$.

Let $h \bmod \pi$ be a nonsquare in $\mathbf{F}[T]/(\pi)$. Let g be a monic polynomial satisfying the conditions

$$g \equiv h \bmod \pi, \quad g \equiv 1 \bmod f/\pi, \quad \deg g \equiv 0 \bmod 2.$$

(We solve the first two congruences using the Chinese remainder theorem and then make the solution monic with even degree by adding a suitable multiple of f to the solution.) Then

$$\left(\frac{f}{g}\right) = \left(\frac{g}{f}\right) = \left(\frac{g}{\pi}\right)\left(\frac{g}{f/\pi}\right) = \left(\frac{h}{\pi}\right)\left(\frac{1}{f/\pi}\right) = -1.$$

□

When a is not a square in $\mathbf{Z}$, there are infinitely many primes p such that $(\frac{a}{p}) = -1$. We will prove this by Jacobi reciprocity and then adapt that proof to $\mathbf{F}[T]$.

Theorem 4.4. *Let a be an integer which is not a perfect square. Then there are infinitely many primes p such that $(\frac{a}{p}) = -1$.*

Proof. Let $a = bc^2$, where b is a squarefree. Then $b \neq 1$. We have $(\frac{a}{p}) = (\frac{b}{p})$ for all p not dividing a, so it suffices to prove the theorem with b in place of a. That is, we can assume a is squarefree and $a \neq 1$. To show $(\frac{a}{p}) = -1$ for infinitely many p, we consider four cases: $a = -1$, $a = 2$, $a = -2$, and a has an odd prime factor.

First we treat the cases $a = -1$, $a = 2$ and $a = -2$. For odd prime p,

$$\left(\frac{-1}{p}\right) = 1 \iff p \equiv 1 \bmod 4,$$
$$\left(\frac{2}{p}\right) = 1 \iff p \equiv 1, 7 \bmod 8,$$
$$\left(\frac{-2}{p}\right) = 1 \iff p \equiv 1, 3 \bmod 8,$$

so to show the equations $(\frac{-1}{p}) = -1$, $(\frac{2}{p}) = -1$, and $(\frac{-2}{p}) = -1$ each hold for infinitely many p, it suffices to show there are infinitely many primes $p \equiv 3 \bmod 4$ (so $(\frac{-1}{p}) = -1$) and there are infinitely many primes $p \equiv 5 \bmod 8$ (so $(\frac{2}{p}) = -1$ and $(\frac{-2}{p}) = -1$).

$p \equiv 3 \bmod 4$: One such prime is 3. If $p_1, \ldots, p_r$ are primes $\equiv 3 \bmod 4$, let

$$N = 4p_1p_2 \cdots p_r - 1 > 1.$$

Then N is not divisible by 2 or by any of $p_1, \ldots, p_r$. Since $N \equiv -1 \equiv 3 \bmod 4$, the prime divisors of N are not all 1 mod 4 (otherwise $N \equiv 1 \bmod 4$). Therefore N has a prime divisor p which is $\equiv 3 \bmod 4$. This prime is different from $p_1, \ldots, p_r$, so there are infinitely many primes $\equiv 3 \bmod 4$.

$p \equiv 5 \bmod 8$: One such prime is 5. If $p_1, \ldots, p_r$ are primes $\equiv 5 \bmod 8$, let

$$N = (2p_1p_2 \cdots p_r)^2 + 1 > 1.$$

Then N is not divisible by 2 or by any of $p_1, \ldots, p_r$. Let p be any prime factor of N. From $N \equiv 0 \bmod p$ we get $-1 \equiv (2p_1p_2 \cdots p_r)^2 \bmod p$, so $-1 \equiv \square \bmod p$. Therefore, since $p \neq 2$, we have $p \equiv 1 \bmod 4$, which is the same as $p \equiv 1$ or $5 \bmod 8$. If every prime factor of N is 1 mod 8, then $N \equiv 1 \bmod 8$, but in fact $N \equiv 5 \bmod 8$ since $p_i^2 \equiv 1 \bmod 8$ for all i. Therefore some prime factor of N is not 1 mod 8, so that prime is 5 mod 8. This prime is different from $p_1, \ldots, p_r$, so there are infinitely many primes $\equiv 5 \bmod 8$.

Now we want to show $(\frac{a}{p}) = -1$ for infinitely many p when a is squarefree with an odd prime factor. Assume we have primes $p_1, \ldots, p_r$ such that $(\frac{a}{p_i}) = -1$ for $i = 1, \ldots, r$. We want to find a new prime with this property.

Write $a = (-1)^{e_0}2^{e_1}a'$, where a' is a positive odd number. For any odd $m > 0$,

$$\left(\frac{a}{m}\right) = \left(\frac{-1}{m}\right)^{e_0}\left(\frac{2}{m}\right)^{e_1}\left(\frac{a'}{m}\right) = \left(\frac{-1}{m}\right)^{e_0}\left(\frac{2}{m}\right)^{e_1}(-1)^{(m-1)/2\cdot(a'-1)/2}\left(\frac{m}{a'}\right).$$

If also $m \equiv 1 \bmod 8$, then $(\frac{a}{m}) = (\frac{m}{a'})$.

Pick an odd prime factor ℓ of a' and write $a' = \ell a''$, so ℓ and a'' are relatively prime. Then $(\frac{m}{a'}) = (\frac{m}{\ell})(\frac{m}{a''})$. The constraint $(\frac{m}{\ell}) = -1$ is a set of mod ℓ congruence conditions on m. By the Chinese remainder theorem, we can find an $m \in \mathbf{Z}$ satisfying

$$m \equiv 1 \bmod 8p_1 \cdots p_r, \quad \left(\frac{m}{\ell}\right) = -1, \quad m \equiv 1 \bmod a''.$$

(When $r = 0$, interpret the empty product $p_1 \cdots p_r$ as 1.) Adding a high multiple of $8p_1 \cdots p_r \ell a'' = 8p_1 \cdots p_r a'$ to m doesn't change the congruence conditions on it but can make m positive. So there is an m which fits all the congruence condition and is positive. For such an m,

$$\left(\frac{a}{m}\right) = \left(\frac{m}{a'}\right) = \left(\frac{m}{\ell}\right)\left(\frac{m}{a''}\right) = \left(\frac{m}{\ell}\right)\left(\frac{1}{a''}\right) = -1.$$

Therefore $(\frac{a}{p}) = -1$ for some prime factor p of m. Since m is divisible by p but $m \equiv 1 \bmod p_i$ by construction, p is not one of $p_1, \ldots, p_r$. Thus p is a new prime such that $(\frac{a}{p}) = -1$, so we are done. □

Theorem 4.5. *If $f \in \mathbf{F}[T]$ is not a square, then $(\frac{f}{\pi}) = -1$ for infinitely many monic irreducible π.*

Proof. Suppose first that $f = c$ is constant. Then c is a nonsquare in $\mathbf{F}^\times$, so $c^{(q-1)/2} = -1$. Thus $(\frac{c}{\pi}) = (-1)^{\deg \pi}$. There are infinitely many monic irreducibles with odd degree (there is at least one of each degree, for instance), so we're done.

Now suppose f is nonconstant. Write $f = cf_1$ where $c \in \mathbf{F}^\times$ and f_1 is monic. For any g which is monic, relatively prime to f, and of even degree,

$$\left(\frac{f}{g}\right) = \left(\frac{c}{g}\right)\left(\frac{f_1}{g}\right) = \left(\frac{g}{f_1}\right). \tag{4.4}$$

Let π be a monic irreducible factor of f_1 and write $f_1 = \pi\widetilde{f}$, so π and $\widetilde{f}$ are relatively prime. Let $h \bmod \pi$ be a nonsquare, so $(\frac{h}{\pi}) = -1$.

Assume by induction that we have monic irreducibles $\pi_1, \ldots, \pi_r$ such that $(\frac{f}{\pi_i}) = -1$. As in the proof of Theorem 4.3, we can pick a polynomial g which is monic, of even degree, and additionally satisfies

$$g \equiv h \bmod \pi, \quad g \equiv 1 \bmod \pi_1 \cdots \pi_r \widetilde{f}.$$

Then $(\frac{g}{f_1}) = (\frac{g}{\pi})(\frac{g}{\widetilde{f}}) = (\frac{h}{\pi})(\frac{1}{\widetilde{f}}) = -1$, so $(\frac{f}{g}) = -1$ by (4.4). Since $(\frac{f}{g})$ is multiplicative in g, there is a monic irreducible π_{r+1} dividing g such that $(\frac{f}{\pi_{r+1}}) = -1$. Since g is divisible by π_{r+1} and is relatively prime to $\pi_1 \cdots \pi_r$, π_{r+1} is not equal to any of $\pi_1, \ldots, \pi_r$. So by induction we have shown there are infinitely many monic irreducible π_i such that $(\frac{f}{\pi_i}) = -1$. □

5. History

The first statement of the quadratic reciprocity law in $\mathbf{F}[T]$ (with $\mathbf{F}$ of odd characteristic) was given by Dedekind [2] in 1857. Dedekind omitted a proof since he felt one of Gauss' proofs carried over essentially unchanged. A proof was published in 1902 by Kühne [4] using a polynomial analogue of Gauss' lemma for the Legendre symbol. In 1924, E. Artin [1] proved the law using the theory of quadratic fields over $\mathbf{F}(T)$. In 1928, F. K. Schmidt [8] proved the law using resultants (which is essentially the proof we gave here). A proof using theta functions was given by Merrill and Walling [6] in 1996.

For further information on number theory in $\mathbf{F}[T]$, see [7] and [9]. A detailed treatment of reciprocity laws is in [5].

References

[1] E. Artin, Quadratische Körper im Gebiet der höheren Kongruenzen I, *Math. Zeit.* **19** (1924), 153–206.

[2] R. Dedekind, Abriss einer Theorie der höheren Kongruenzen in Bezug auf einer reellen Primzahl-Modulus, *J. Reine Angew. Math.* **54** (1857), 1–26,

[3] K. Ireland and M. Rosen, A Classical Introduction to Modern Number Theory, 2nd ed., Springer-Verlag, New York, 1990.

[4] H. Kühne, Eine Wechselbeziehung zwischen Funktionen mehrerer Unbestimmter, die zu Reziprozitätsgesetzen führt, *J. Reine Angew. Math.* **124** (1902), 121–133.

[5] F. Lemmermeyer, "Reciprocity Laws," Springer-Verlag, Berlin, 2000.

[6] K. D. Merrill and L. H. Walling, On quadratic Reciprocity over Function Fields, *Pacific J. Math.* **173** (1996), 147–150.

[7] P. Roquette, The Riemann hypothesis in characteristic p, its origin and development. I. The formation of the zeta-functions of Artin and of F. K. Schmidt. *Mitt. Math. Ges. Hamburg* **21** (2002), 79–157.

[8] F. K. Schmidt, Zur Zahlentheorie in Körpern von der Charakteristik p, *Sitz. Phys-Med Soc. zu Erlangen* **58-59** (1928), 159–172.

[9] M. Rosen, "Number theory in function fields," Springer–Verlag, New York, 2002.