MODULAR PELL CONICS

F. LEMMERMEYER

Abstract. In this article we introduce Pell forms, explain their modularity, and relate it to known results such as the Herglotz trick or Bernoulli distributions.

April 2, 2011

Introduction

One of the greatest mathematical achievements in the early 20th century was class field theory: starting out as an attempt to generalize the quadratic reciprocity law, it ended up as a theory of abelian extensions of number fields. Yet, the reciprocity law kept its central role, but was formulated in a way that made it difficult to recognize it as a reciprocity law: instead of relating power residue symbols, Artin's reciprocity law is an isomorphism between two abelian groups.

The corresponding theory for nonabelian extensions, Langlands' program, is still largely conjectural, at least for global fields, although considerable progress has been made in the last few years. Those who see Langlands' ideas for the first time will probably be surprised to find that analytic objects such as cusp forms are supposed to be the correct generalization of Dirichlet and Hecke characters, and cannot see why e.g. the modularity theorem for elliptic curves is some kind of reciprocity law. A good explanation of these facts for readers who know class field theory can be found in Neukirch's survey [28]. Ash and Gross [2] have written a beautiful book in which they explain these mysteries to the non-initiated; these notes are my attempt at telling the same story, following ideas put forth by Darmon and Levesque [8, 9].

1. The Modularity of Pell Conics

For a quadratic discriminant Δ consider the associated Pell conic

$$\mathcal{C} : Q_0(X,Y) = 1, \tag{1}$$

where

$$Q_0(X,Y) = \begin{cases} X^2 - mY^2 & \text{if } \Delta = 4m, \\ X^2 - XY + \frac{1-m}{4}Y^2 & \text{if } \Delta = 4m+1 \end{cases}$$

is the principal binary quadratic form with discriminant Δ. For each prime $p \nmid \Delta$, let $N_p = p - a_p$ denote the number of $\mathbb{F}_p$-rational points on $\mathcal{C}$, i.e., the number of solutions of the congruence $Q_0(X,Y) \equiv 1 \bmod p$. It is a classical and elementary result that $a_p = (\frac{\Delta}{p})$, where $(\frac{\Delta}{p})$ is the Kronecker symbol. We encode the information on the number of $\mathbb{F}_p$-rational points in a formal power series

$$f_{\mathcal{C}}(q) = \sum a_n q^n, \tag{2}$$

where $a_n = \prod a_p$ for $n = \prod p$, and call this power series a *Pell form.* It is easily checked that (2) converges absolutely for $|q| < 1$.

As an example, consider the Pell conic $\mathcal{C} : X^2 + Y^2 = 1$ with discriminant $\Delta = -4$; a simple calculation shows

p	2	3	5	7	11	13
N_p	2	4	4	8	12	12

Thus the Pell form attached to the unit circle is

$$f_{\mathcal{C}}(q) = q - q^3 + q^5 - q^7 + q^9 - q^{11} + q^{13} \pm \ldots .$$

Fermat and Euler observed that the sign of q^n in this series only depends on the residue class of n modulo 4. In fact, by parametrizing the conic $\mathcal{C} : x^2 + y^2 = 1$ it is easily seen that, for odd primes p, the number of $\mathbb{F}_p$-rational points on $\mathcal{C}$ is $p - 1$ if $(\frac{-1}{p}) = +1$, and $p + 1$ otherwise. Since the element $(0, 1)$ has order 4 in the group $\mathcal{C}(\mathbb{F}_p)$, it follows that $(\frac{-1}{p}) = +1$ if and only if $p \equiv 1 \bmod 4$.

More generally, Euler came up with the following conjecture:

Euler's Modularity Conjecture. *For every Pell conic (1) there is a modulus N such that the values a_p only depend on the residue class of p modulo N.*

If we suspect that, for the conic $\mathcal{C} : X^2 + Y^2 = 1$, the modulus $N = 4$ works, then we can numerically check the modularity conjecture for arbitrarily many primes. In general, testing the conjecture only became possible through the following refinement of the modularity conjecture, which is also due to Euler:

Euler's Modularity Conjecture (Precise Version). *For every Pell conic (1), the values a_p only depend on the residue class of p modulo $4m$.*

In fact, the smallest value of N that works, which is called the *conductor* of $\mathcal{C}$, is given by $N = |\Delta|$.

2. Consequences of Modularity

The main consequence of the modularity of Pell conics is Euler's version of the quadratic reciprocity law (which can easily be shown to be equivalent to Legendre's version):

Quadratic Reciprocity Law. *If the Pell conic (1) is modular with conductor N, then $(\frac{\Delta}{p}) = (\frac{\Delta}{q})$ for positive prime numbers $p \equiv q \bmod N$.*

This is just a reformulation of the modularity property. A more precise version of the modularity property is *Dirichlet's Lemma.* For stating it, recall that a Dirichlet character defined mod m is a homomorphism $\chi : (\mathbb{Z}/m\mathbb{Z})^\times \longrightarrow \mathbb{C}^1$, where $\mathbb{C}^1$ denotes the complex unit circle, i.e., the group of complex numbers with absolute value 1. A quadratic Dirichlet character is a Dirichlet character with values ± 1. A Dirichlet character defined modulo m is defined modulo a divisor m_1 of m if it factors through $(\mathbb{Z}/m_1\mathbb{Z})^\times$; if a Dirichlet character χ is defined modulo m_1 and m_2, it is also defined modulo $\gcd(m_1, m_2)$, and the smallest defining modulus is called the conductor of χ. A Dirichlet character $\chi : (\mathbb{Z}/m\mathbb{Z})^\times \longrightarrow \mathbb{C}^1$ is called primitive if m is equal to the conductor of χ, i.e., if χ cannot be defined modulo some modulus smaller than m. In his proof of the theorem on primes in arithmetic progressions, Dirichlet used what is now known as

Dirichlet's Lemma. *The modularity conjecture provides us with a bijection between Pell conics $Q_0(X,Y) = 1$ for squarefree integers m and primitive Dirichlet characters. The conductor of the Pell conic equals the conductor of the attached Dirichlet character.*

Like the modularity conjecture , Dirichlet's Lemma is a variant of quadratic reciprocity: if $q \equiv 1 \bmod 4$ is prime, the Kronecker symbol $(\frac{q}{\cdot})$ equals some quadratic Dirichlet character with conductor q; by Euler's criterion, the only such character is $(\frac{\cdot}{q})$, and we deduce that $(\frac{q}{p}) = (\frac{p}{q})$ for all primes $p \ne q$. If $q \equiv 3 \bmod 4$, then $(\frac{-q}{\cdot})$ equals some quadratic Dirichlet character with conductor q, and as above we find $(\frac{-q}{p}) = (\frac{p}{q})$.

The modularity of Pell conics also has strong implications for the analytic behaviour of Pell forms. For describing the properties of Pell forms we will use the *Fekete polynomials*

$$F_N(q) = -\sum_{n=1}^{N-1} \chi(n) q^n. \tag{3}$$

Traditionally, Fekete polynomials are defined without this minus sign, which we have introduced in order to have the monic polynomial $q^N - 1$ in the denominator rather than $1 - q^N$.

Theorem 1. *If the Pell conic (1) is modular with conductor N, then the associated Pell form can be extended meromorphically to the whole complex plane, where it represents a rational function of q and satisfies a functional equation relating $f(q)$ and $f(\frac{1}{q})$. In fact,*

$$f_{\mathcal{C}}(q) = \frac{F_N(q)}{q^N - 1}, \tag{4}$$

where the $F_N(X)$ are Fekete polynomials.

The Pell form satisfies the functional equation

$$f_{\mathcal{C}}\Big(\frac{1}{q}\Big) = -\chi(-1) f_{\mathcal{C}}(q), \tag{5}$$

where χ is the Dirichlet character mod N attached to $\mathcal{C}$.

Proof. Since χ is periodic with period N, we have

$$f_{\mathcal{C}}(q) = \Big(\sum_{n=1}^{N-1} \chi(n) q^n\Big)(1 + q^N + q^{2N} + \ldots) = \frac{F_\chi(q)}{q^N - 1}$$

inside the domain of convergence as claimed.

The functional equation follows from the symmetry

$$\chi(N-a) = \chi(-1) \cdot \chi(a). \tag{6}$$

In fact, let $F \in \mathbb{Z}[X]$ be a poynomial of degree g. Then the "reflected polynomial" $F^*(X) = X^g F(\frac{1}{X})$ is also a polynomial with integral coefficients, and if we write

$$F(X) = a_0 + a_1 X + \ldots + a_g X^g,$$

then we have

$$F^*(X) = a_g + a_{g-1} X + \ldots + a_1 X^{g-1} + a_0 X^g.$$

Clearly

$$F_N^*(X) = \chi(-1)F_N(X) \tag{7}$$

is just a reformulation of the symmetry of the Dirichlet character expressed by (6). Now we find

$$f_{\mathcal{C}}\Big(\frac{1}{q}\Big) = \frac{F_N(\frac{1}{q})}{q^{-d}-1} = \frac{q^N F_N(\frac{1}{q})}{q^N(q^{-N}-1)} = \frac{F_N^*(q)}{1-q^N} = -\chi(-1)f_{\mathcal{C}}(q).$$

This proves our claims. □

The functional equation allows us to predict the vanishing of $f_{\mathcal{C}}(1)$ for certain Pell conics:

Corollary 2. *If $\chi(-1)=1$, then $f_{\mathcal{C}}(1)=0$.*

Dirichlet characters χ with $\chi(-1)=-1$ are called odd, those with $\chi(-1)=+1$ even. Thus $f_{\mathcal{C}}(q)$ vanishes at $q=1$ if χ is even. Below we will see that the value $f_{\mathcal{C}}(1)$ is equal to $L(0,\chi)$, where $L(s,\chi)$ is the Dirichlet L-series attached to χ. The order of vanishing of $L(s,\chi)$ at $s=0$ is, by the analogue of the conjecture of Birch and Swinnerton-Dyer, equal to the $\mathbb{Z}$-rank of the solutions of the Pell equation $\mathcal{C}: Q_0(X,Y)=1$ in integers. Thus Cor. 2 and the analogue of the Birch–Swinnerton-Dyer conjecture predict the solvability of the Pell equation for positive nonsquares m.

3. Poles of Pell Forms and Gauss Sums

Let us now investigate the poles of the Pell forms (3). This is most easily accomplished by decomposing the right hand side of (3) into partial fractions. From

$$\frac{F_N(x)}{x^N-1} = \sum_{j=0}^{N-1} \frac{A_j}{x-\zeta^j},$$

where ζ is a primitive N-th root of unity, we get

$$F_N(x) = \sum_{j=0}^{N-1} \frac{A_j}{x-\zeta^j}(x^N-1).$$

Putting $x=\zeta^r$ we find

$$\begin{aligned} F_N(\zeta^r) &= A_r(\zeta^r-1)(\zeta^r-\zeta)\cdots(\zeta^r-\zeta^{r-1})(\zeta^r-\zeta^{r+1})\cdots(\zeta^r-\zeta^{N-1}) \\ &= A_r\zeta^{r(N-1)}(1-\zeta)(1-\zeta^2)\cdots(1-\zeta^{N-1}) = A_r\zeta^{-r}N. \end{aligned}$$

The values

$$F_N(\zeta^r) = -\sum_{n=1}^{N-1}\chi(n)\zeta^{rn}$$

are called *Gauss sums* (as for Fekete polynomials, we have used a sign convention for Gauss sums that most authors do not follow) and are usually denoted by $G_r(\chi)$. The following result is classical:

Proposition 3. *For a Dirichlet character χ and any integer r, we have*

$$G_r(\chi) = \overline{\chi(r)}\ G(\chi),$$

where $G(\chi)=G_1(\chi)$. Moreover, we have

$$G(\chi)\overline{G(\chi)} = N.$$

Observe that we do not assume that r is coprime to the conductor N; in this case, the proof of Prop. 3 is purely formal. If a and N have a common divisor, the proof requires more work (see e.g. Knapp [17, Lemma 7.18]).

Using this result we find

Theorem 4. *The decomposition of $f_{\mathcal{C}}(q)$ into partial fractions is given by*

$$f_{\mathcal{C}}(q) = \frac{G(\chi)}{N} \cdot \sum_{r=0}^{N-1} \frac{\overline{\chi(r)}\zeta^r}{q - \zeta^r}.$$

We now can locate the poles of Pell forms:

Corollary 5. *The Pell form $f_{\mathcal{C}}(q)$ has poles of order 1 exactly at the primitive N-th roots of unity, and is holomorphic everywhere else.*

In fact, the terms with denominator $q - \zeta^r$ and $\gcd(r, d) \neq 1$ vanish because $\chi(r) = 0$ for such r.

Prop. 3 shows that $F_N(q)$ and $1 - q^d$ have the roots ζ^m in common, where m runs through the integers $0 \le m < N$ not coprime to N. These are exactly the roots of the polynomial $\prod_{j|N, j\neq N} \Phi_j(q)$. Thus

$$F_N(q) = h_N(q) \cdot \prod_{j|N, j\neq N} \Phi_j(q) \tag{8}$$

for some polynomial $h_N \in \mathbb{Z}[q]$. For showing that the polynomials h_N and F_N are coprime we observe that $F_N(\zeta^a) = \chi(a)G(\chi) \neq 0$ whenever $\gcd(a, N) = 1$.

Proposition 6. *Let χ be a Dirichlet character with conductor d. Then*

$$f_{\mathcal{C}}(q) = \frac{h_N(q)}{\Phi_N(q)}, \tag{9}$$

where Φ_N is the N-th cyclotomic polynomial, and h_N is a polynomial in $q\mathbb{Z}[q]$ with degree $\phi(N) - 1$ and coprime to Φ_N.

The factors $h_N(q)$ of the Fekete polynomials are highly mysterious, even for prime values of N. The following table gives these polynomials for small conductors:

χ	N	$\chi(-1)$	$f_N(q)$	$f_N(1)$
$(\frac{-3}{\cdot})$	3	-1	$\frac{q}{1+q+q^2}$	$\frac{1}{3}$
$(\frac{-1}{\cdot})$	4	-1	$\frac{q}{1+q^2}$	$\frac{1}{2}$
$(\frac{5}{\cdot})$	5	$+1$	$\frac{q-q^3}{1+q+q^2+q^3+q^4}$	0
$(\frac{-7}{\cdot})$	7	-1	$\frac{q+2q^2+q^3+2q^4+q^5}{1+q+q^2+q^3+q^4+q^5+q^6}$	1
$(\frac{2}{\cdot})$	8	$+1$	$\frac{q-q^3}{1+q^4}$	0
$(\frac{-2}{\cdot})$	8	-1	$\frac{q+q^3}{1+q^4}$	1
$(\frac{3}{\cdot})$	12	$+1$	$\frac{q-q^3}{1-q^2+q^4}$	0
$(\frac{-15}{\cdot})$	15	-1	$\frac{q-q^3+2q^4-q^5+q^7}{1-q+q^3-q^4+q^5-q^7+q^8}$	2

Numerical experiments indicate that the polynomials $h_N(q)$ have lots of properties, some of which can be proved easily:

Proposition 7. *Let p be a prime $p \equiv 1 \bmod 4$, χ the quadratic Dirichlet character mod p, and set*

$$F_p(x) = x(x-1)^2(x+1)G_p(x).$$

Then G_p is a monic polynomial with integral coefficients and degree $p-5$. Moreover, G_p is recursive, i.e., $G_p^*(X) = X^{p-5}G_p(\frac{1}{X}) = G_p(X)$.

The divisibility of $F_p(x)$ by the factors $x(x-1)^2(x+1)$ follows from the distribution of quadratic residues modulo p. Other properties seem to lie deeper: numerical experiments suggest that $h_p(x+1)$ is divisible by $x^{(p-5)/2}$ in $\mathbb{F}_p[x]$, and it can be verified that $G_p(x)$ is irreducible for all primes $p < 400$.

4. Hecke Operators

We can interpret $f(q)$ as a function of the complex variable z by setting $q = e^{2\pi i z}$. The series $f_{\mathcal{C}}(q) = \sum a_n q^n$ converges for all $|q| < 1$, which in turn is equivalent to $z \in \mathbb{H}$, where $\mathbb{H}$ denotes the upper half plane. On the other hand we have shown that $f_{\mathcal{C}}(q)$ can be extended to a meromorphic function on the whole complex plane.

As a function of z, the Pell form $f_{\mathcal{C}}$ has the property $f_{\mathcal{C}}(z+1) = f_{\mathcal{C}}(z)$. The functional equation becomes $f_{\mathcal{C}}(-z) = -\chi(-1)f_{\mathcal{C}}(z)$. The poles in the strip $0 < \mathrm{Re} z < 1$ lie at $z = \frac{r}{N}$ for $1 \le r < N$ with $\gcd(r, N) = 1$.

In the following, we will consider Pell forms f as functions of z. For a Pell form with conductor N and a prime $p \nmid N$, define the Hecke operator T_p via

$$f|_{T_p}(z) = \frac{1}{p}\sum_{a=1}^{p-1} f\Big(\frac{z+a}{p}\Big).$$

It is easy to check that the Hecke operators are multiplicative ($T_mT_n = T_{mn}$) and commute. Hecke operators allow us to extract the Dirichlet character χ from the corresponding Pell form:

Theorem 8. *Let $f(q) = \sum \chi(n)q^n$ be the Pell form attached to the quadratic Dirichlet character χ of conductor N. Set $q = e^{2\pi i z}$, so $f(z) = \sum \chi(n)e^{2\pi i n z}$. For any prime $p \nmid N$, we have $f|_{T_p}(z) = \chi(p)f(z)$. Thus f is an eigenfunction for the Hecke operators T_p with eigenvalues $\chi(p)$.*

Proof. Set $r = \exp(2\pi i z/p)$; then $r^p = q$ and $\exp(2\pi i(z+a)/p) = \zeta^a r$ for $\zeta = \exp(2\pi i/p)$. Now we have

$$\begin{aligned} pf|_{T_p} &= f\Big(\frac{z}{p}\Big) + f\Big(\frac{z+1}{p}\Big) + \ldots + f\Big(\frac{z+p-1}{p}\Big) \\ &= \sum_{n=1}^{\infty} \chi(n)r^n + \sum_{n=1}^{\infty} \chi(n)(\zeta r)^n + \ldots \\ &= \sum_{a=1}^{p-1}\sum_{n=1}^{\infty} \zeta^{an}\chi(n)r^n = \chi(p)\cdot p \cdot f(z). \end{aligned}$$

The claim follows. □

Quite a few nice and important functions are eigenfunctions of the Hecke operators T_p.

The Cotangent. We start with the classical

Proposition 9. *The cotangent function $f(x) = \pi \cot(\pi x)$ is an eigenfunction of T_n with eigenvalue 1 for every integer $n \ge 1$.*

This follows from the identity

$$\pi \cot \pi x = \frac{1}{x} + \sum_{k=1}^{\infty} \Big(\frac{1}{k+x} - \frac{1}{k-x} \Big), \tag{10}$$

which is valid for all $x \in \mathbb{C} \setminus \mathbb{Z}$.

Bernoulli Polynomials. The Bernoulli polynomials $B_n(x)$ are defined by

$$\frac{te^{tx}}{e^t - 1} = \sum_{n=0}^{\infty} B_n(x) t^n.$$

We find $B_1(x) = x - \frac{1}{2}$, $B_2(x) = \frac{1}{2!}(x^2 - x + \frac{1}{6})$, ... Bernoulli polynomials are also eigenfunctions of our Hecke operators:

Proposition 10. *The Bernoulli polynomial $B_n(x)$ of degree n is an eigenfunction of the Hecke operator T_k for the eigenvalue k^{-n}.*

Proof. We have

$$\begin{aligned} k \sum_{n=0}^{\infty} \Big(\frac{t}{k}\Big)^n B_n(x) = \frac{te^{tx/k}}{e^{t/k} - 1} &= \sum_{m=0}^{k-1} \frac{te^{t(x+m)/k}}{e^t - 1} \\ &= \sum_{n=0}^{\infty} t^n \bigg(B_n\Big(\frac{x}{k}\Big) + \ldots + B_n\Big(\frac{x+k-1}{k}\Big)\bigg). \end{aligned}$$

Comparing the coefficients of t^n in the power series expansions we find

$$B_n(x)|_{T_k} = \frac{1}{k}\bigg(B_n\Big(\frac{x}{k}\Big) + \ldots + B_n\Big(\frac{x+k-1}{k}\Big)\bigg) = k^{-n} B_n(x)$$

as claimed. □

Hurwitz Zeta Functions. The Hurwitz zeta function $\zeta(s, x)$ is defined for all $s \in \mathbb{C}$ with real part > 1 by

$$\zeta(s, x) = \sum_{n=0}^{\infty} \frac{1}{(x+n)^s}.$$

Observe that $\zeta(s, 1) = \zeta(s)$ is the Riemann zeta function. Just as the cotangent function and the Bernoulli polynomials, the Hurwitz zeta function is an eigenfunction of the Hecke operators:

Proposition 11. *The Hurwitz zeta function $\zeta(s, x)$ is an eigenfunction of T_k for the eigenvalue k^{s-1}.*

Proof. We find

$$\begin{aligned} k\zeta(s, x)|_{t_k} &= \sum_{m=0}^{\infty} \sum_{l=0}^{k-1} \Big(\frac{x}{k} + m + \frac{l}{k} \Big)^{-s} = k^s \sum_{m=0}^{\infty} \sum_{l=0}^{k-1} (x + km + l)^{-s} \\ &= k^s \sum_{n=0}^{\infty} (x+n)^{-s}, \end{aligned}$$

which proves the claim. □

Comparing the last two results shows that both the Bernoulli polynomials $B_n(x)$ and the Hurwitz zeta function $\zeta(1-n,x)$ are eigenfunctions of T_k for the same eigenvalue k^{-n}. In fact, there is a close relation between the values $\zeta(1-n,x)$ and $B_n(x)$ (see [34, Thm. 4.2]):

Theorem 12. *We have*

$$\zeta(1-n,x) = -\frac{1}{n}B_n(x)$$

for $0 < x \le 1$.

The special case $\zeta(0) = \zeta(0,1) = -\frac{1}{2}$ was already known to Euler.

5. Quadratic Reciprocity

Let f be a function defined on the reals with the following properties:

$$\begin{cases} f(z) \ne 0 \text{ for } z = \frac{m}{2n+1},\ 1 \le m \le 2n; \\ f(-z) = -f(z) \text{ for } z \in \mathbb{R}; \\ f(z+1) = f(z) \text{ for } z \in \mathbb{R}. \end{cases} \tag{11}$$

Two functions with these properties are $f(z) = \sin z$ and $f(z) = e^{2\pi iz} - e^{-2\pi iz}$.

Lemma 13 (Gauss's Lemma)**.** *Let p be an odd prime number and A a half system modulo p. For any function f such as above we have*

$$\Big(\frac{m}{p}\Big) = \prod_{a\in A} \frac{f(\frac{am}{p})}{f(\frac{a}{p})}.$$

In order to be able to say precisely which properties f must have for the proof to work, let us go through it in detail.

Proof. Let $A = \{a_1,\ldots,a_n\}$ be a half system modulo $p = 2n+1$; thus each coprime residue class is represented either by some a_j or by $-a_j$. Thus

$$ma_j \equiv (-1)^{m_j} a_{j'} \bmod p \tag{12}$$

for $m_j \in \{0,1\}$; the map $j \to j'$ is a permutation of the index set $\{1,2,\ldots,n\}$. Multiplying these congruences gives $m^{(p-1)/2}\prod a_j \equiv (-1)^\mu \prod a_{j'} \bmod p$, where $\mu = m_1 + \ldots + m_n$ is the number of "sign changes". By Euler's criterion we find $(\frac{m}{p}) = (-1)^\mu$.

The congruence (12) is equivalent to $ma_j = (-1)^{m_j} a_{j'} + kp$; dividing through by p shows that $\frac{ma_j}{p} = (-1)^{m_j}\frac{a_{j'}}{p} + k$. Now we apply f to this equation and use $f(z+1) = f(z)$, as well as $f(-z) = -f(z)$; this gives $f(\frac{ma_j}{p}) = (-1)^{m_j} f(\frac{a_{j'}}{p})$. Taking the product of this equation over a half system now proves our claim since $f(\frac{a}{p}) \ne 0$ for $0 < a < p$. □

Eigenfunctions of "multiplicative Hecke operators" defined by

$$f|_{M_n}(z) = \prod_{k \bmod n} f\Big(\frac{z+k}{n}\Big)$$

are well suited to applications to Gauss's Lemma. We remark that the M_n are indeed the multiplicative analogs of Hecke operators: if f is an eigenfunction of M_n

with eigenvalue 1, then its logarithmic derivative $\phi = f'/f$ is an eigenfunction of T_n with eigenvalue 1.

In particular, we have

$$\frac{f(nz)}{f(z)} = \prod_{k=1}^{n-1} f\Big(z + \frac{k}{n}\Big).$$

Now assume that f satisfies (11) and, in addition, is an eigenfunction with eigenvalues 1 for all M_n with odd integers n. Let p and q be distinct odd primes with half systems A and B, respectively. Then

$$\Big(\frac{q}{p}\Big) = \prod_{a\in A} \frac{f(\frac{aq}{p})}{f(\frac{a}{p})} = \prod_{a\in A}\prod_{b\in\pm B} f\Big(\frac{a}{p}+\frac{b}{q}\Big) = \prod_{a\in A}\prod_{b\in B} f\Big(\frac{a}{p}+\frac{b}{q}\Big) f\Big(\frac{a}{p}-\frac{b}{q}\Big), \tag{13}$$

hence, by symmetry,

$$\Big(\frac{p}{q}\Big) = \prod_{a\in A}\prod_{b\in B} f\Big(\frac{b}{q}+\frac{a}{p}\Big) f\Big(\frac{b}{q}-\frac{a}{p}\Big).$$

Comparing these expressions shows that

$$\Big(\frac{p}{q}\Big)\Big(\frac{q}{p}\Big) = \prod_{a\in A}\prod_{b\in B}(-1) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}},$$

which is the quadratic reciprocity law in Legendre's form.

Each function f with the desired properties will now give us a proof of the quadratic reciprocity law. Since the cotangent is the logarithmic derivative of the sine function, we may hope that the sine provides us with another example, and it does:

Lemma 14. *The function $f(z) = 2i\sin(\pi z) = e^{2\pi iz} - e^{-2\pi iz}$ is an eigenfunction with eigenvalue 1 for all M_n, where n is an odd integer.*

6. L-Series

Pell forms are just one out of many ways of encoding the information from a Kronecker character in some analytic function; other examples include theta functions, Lambert series, or L-series. In this section we will exhibit a few connections between Pell forms and L-series. To this end, we define the Mellin transform $M(f)$ of a suitable function $f : (0,\infty) \longrightarrow \mathbb{C}$ by

$$M(f)(s) = \int_0^\infty f(t)t^s\frac{dt}{t}.$$

The Mellin transform of $f(t) = e^{-t}$ is the Gamma function.

We will now compute the Mellin transform of Pell forms $f_{\mathcal{C}}(q)$ regarded as a function of z via $q = e^{2\pi iz}$. Since $f_{\mathcal{C}}(it) = \sum\limits_{n=1}^{\infty}\chi(n)e^{-2\pi nt}$ we find that the Mellin transform of $f(it)$ is given by

$$\begin{aligned} M(f)(s) &= \int_0^\infty f(it)t^s\frac{dt}{t} = \int_0^\infty \sum_{n=1}^\infty \chi(n)e^{-2\pi nt}t^s\frac{dt}{t} \\ &= \sum_{n=1}^\infty \chi(n)\int_0^\infty e^{-u}(2\pi n)^{-s}u^s\frac{du}{u} = (2\pi)^{-s}\Gamma(s)L(s,\chi), \end{aligned}$$

where we have used the substitution $u = 2\pi nt$.

The connection between Pell forms and Dirichlet L-series goes far beyond the fact that the L-series are essentially the Mellin transforms of Pell forms. In fact, summing the well known identity

$$n^{-s}\Gamma(s) = \int_0^\infty e^{-nt} t^s \frac{dt}{t}$$

for $n = 1, 2, 3 \ldots$ we find

$$\Gamma(s)\zeta(s) = \int_0^\infty \frac{e^{-t}}{1-e^{-t}} t^s \frac{dt}{t}.$$

Similarly we get

$$\Gamma(s)L(s,\chi) = \int_0^\infty \frac{F_N(e^{-t})}{e^{-mt}-1} t^s \frac{dt}{t},$$

where the F_N are Fekete polynomials.

Even more striking is the following observation. We have already seen that $f_{\mathcal{C}}(1) = 0$ if χ is even; the values $f_{\mathcal{C}}(1)$ for odd characters are essentially class numbers. In fact, let χ be an odd Dirichlet character with conductor N attached to a Pell conic $\mathcal{C}$. Then the Pell form $f_{\mathcal{C}}$ attains a nonzero value at $q = 1$ via Equ. (9). By working shamelessly with divergent series such as (2) for $q = 1$, we find $f_{\mathcal{C}}(1) = \sum \chi(n) = L(0,\chi)$, where $L(s,\chi) = \sum \chi(n)n^{-s}$. In order to make sense of this "equality" we have to explain how to evaluate both sides of this equation.

We can evaluate $f_{\mathcal{C}}(1)$ using (9); equivalently we can use (4) and L'Hospital's rule:

$$\begin{aligned} f_{\mathcal{C}}(1) &= \lim_{q\to 1} \frac{F_N(q)}{q^N-1} = \frac{1}{N}F'_N(1) \\ &= -\frac{1}{N}(1 + 2\chi(2) + 3\chi(3) + \ldots + (N-1)\chi(N-1)) \end{aligned}$$

For example, for the conic with conductor 7 we find

$$f_{\mathcal{C}}(1) = -\frac{1}{7}(1+2-3+4-5-6) = 1.$$

Evaluating Dirichlet's L-series $L(s,\chi)$ at $s = 0$ is more difficult; the standard procedure is extending the L-series to the complex plane and using the functional equation. In this picture, the value $L(0,\chi)$ is related to the residue of $L(1,\chi)$, the classical ingredient in Dirichlet's proof of the class number formula and the theorem on primes in arithmetic progressions.

The next theorem due to Dirichlet shows that the equation $f_{\mathcal{C}}(1) = L(0,\chi)$ is indeed correct:

Theorem 15. *Let χ be an odd primitive Dirichlet character with conductor N; then $-N$ is the discriminant of a complex quadratic number field K. Let $f_{\mathcal{C}}(q)$ be the Pell form attached to the Pell conic with conductor $-N$. Then*

$$f_{\mathcal{C}}(1) = \frac{2h}{w},$$

where w denotes the number of roots of unity in K (hence $w = 2$ unless $N = 3$ or $N = 4$), and where $h = h_K$ denotes the class number of K.

The proof now essentially consists in referring to Dirichlet's class number formula and the functional equation of his L-series.

7. The Big Picture

The main object from our point of view is the Pell conic $\mathcal{C} : Q_0(X,Y) = 1$ with discriminant N. The number N_p of points in $\mathcal{C}(\mathbb{F}_p)$ is counted by a Kronecker character: $N_p = p - (\frac{N}{p})$. This Kronecker character describes the decomposition law in the quadratic number field $K = \mathbb{Q}(\sqrt{N}\,)$ with discriminant N. The units in the maximal order $\mathcal{O}_K$ of K correspond bijectively to the integral points on the conic, and in fact the group of units with positive norm is isomorphic to the group $\mathcal{C}(\mathbb{Z})$ of integral points on $\mathcal{C}$.

The modular objects attached to Kronecker characters via Dirichlets' Lemma are Dirichlet characters. These describe the decomposition law in the cyclotomic number fields $L = \mathbb{Q}(\zeta_N)$, which are the modular objects attached to quadratic number fields via the theorem of Kronecker-Weber. Finally, the units in the ring of integers $\mathbb{Z}[\zeta_N]$ in L are integral points on certain affine varieties A_N defined via restriction of scalars: the fact that an element $\eta = x_0 + x_1\zeta + x_2\zeta^2 + \ldots \in \mathbb{Z}[\zeta_N]$ has norm 1 means that a certain polynomial $\Phi(x_0, x_1, \ldots)$ in $\phi(N)$ variables has the value 1; the equation $\Phi(x_0, x_1, \ldots) = 1$ defines an affine variety A_N whose integral points form a group $A_N(\mathbb{Z})$ isomorphic to the unit group in $\mathbb{Z}[\zeta_N]$ (in general number fields: to the group of units with positive norm), and there is a polynomial map $A_N(\mathbb{Z}) \longrightarrow \mathcal{C}(\mathbb{Z})$ whose image has finite index (for trivial reasons in the case of negative discriminants, and by Dirichlet's class number formula if the discriminants are positive).

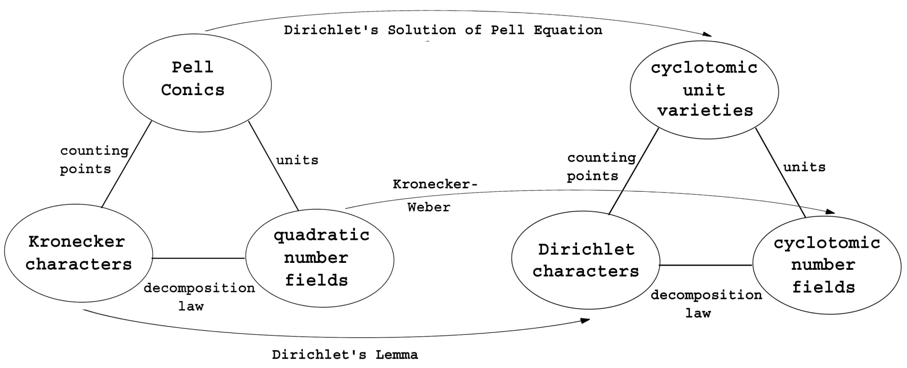

Figure 1. Modular Pell Conics

The technical tool that captures all of these pieces of the picture is Dirichlet's L-series. The L-series attached to the Pell conic is constructed as follows: let N_r denote the number of points on the Pell conic over the finite field with p^r elements; then we can compute the local Euler factors $Z_p(T)$ via

$$\log Z_p(T) = \sum_{r \ge 1} N_r \frac{T^r}{r}$$

and find

$$Z_p(T) = \frac{1 - \chi(p)T}{1 - pT}$$

for the Kronecker character χ attached to $\mathcal{C}$. The product

$$L(s,\mathcal{C}) = \prod_p \frac{1}{1-\chi(p)p^{-s}}$$

then turns out to be the classical L-series

$$L(s,\chi) = \sum_{n\ge 1} \chi(n)n^{-s}$$

for the character χ. The fact that this L-series has an Euler factorization is equivalent to the decomposition law.

If χ is even, i.e., if the quadratic number field is real, then the L-series contains enough information to give us an integral point on the Pell conic: in this case, Dirichlet's class number formula says

$$L(1,\mathcal{C}) = \frac{h}{\sqrt{N}} \cdot \log \varepsilon,$$

where N is the conductor of $\mathcal{C}$, h the class number of the quadratic number field, and ε its fundamental unit. For getting a solution of the Pell equation one has to take the square of the fundamental unit if it has norm -1.

The global L-series on the modular side can be constructed in exactly the same way by counting points of the cyclotomic unit variety A_N in finite fields (see [24]). In this case, $L(s, A_N) = \zeta_K(s)/\zeta(s)$, and the fact that this L-series has an Euler factorization is equivalent to the decomposition law in cyclotomic varieties. From the values of the individual L-series $L(1,\chi)$ for even Dirichlet characters χ we can retrieve the logarithms of $|1-\zeta_n^a|$, which in turn can be used to construct cyclotomic units.

Weil Conjectures for Number Fields. The Hasse-Weil zeta functions $Z_p(T)$ attached to the unit varieties A_K introduced above possess properties that are similar to those satisfied by the zeta functions of smooth projective varieties.

(1) The zeta function $Z_p(T)$ is a rational function of T. More exactly, $Z_p(T)$ can be written in the form

$$Z_p(T) = \begin{cases} \frac{P_0(T)P_2(T)\cdots P_{n-1}(T)}{P_1(T)P_3(T)\cdots P_n(T)} & \text{if } n \text{ is odd,} \\ \frac{P_1(T)P_3(T)\cdots P_{n-1}(T)}{P_0(T)P_2(T)\cdots P_n(T)} & \text{if } n \text{ is even.} \end{cases}$$

(2) The inverse roots of P_j have absolute value p^j for $0 \le j \le n$.

(3) The zeta function $Z_p(T)$ admits a functional equation of the form

$$Z_p\Big(\varepsilon_p \frac{1}{p^n T}\Big) = \eta_p Z_p(T)^{(-1)^n},$$

where $\varepsilon_p = Z_p(\infty)$ and $\eta_n = 1$ except when $n = 2$.

(4) The global zeta function $Z_K(s)$ is constructed from the factor $P_{n-2}(T)$ of $Z_p(T)$ as follows: set $L_p(s) = P_{n-2}(p^{2-n-s})$ and $Z(s) = \prod_p L_p(s)$. Then $Z(s) = \zeta_K(s)/\zeta(s)$ up to Euler factors for the ramified primes, where ζ_K is the Dedekind zeta function of K.

These conjectures are far less deep than the original Weil conjectures for smooth projective varieties; for cyclic extensions of prime degree, explicit formulas for the $P_j(T)$ can be found in [24] along with proofs of the above conjectures for general number fields.

8. Euler vs. Legendre

Legendre's version of the quadratic reciprocity law, the formula

$$\Big(\frac{p}{q}\Big) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\Big(\frac{q}{p}\Big),$$

is the goal of many an elementary introduction to number theory. Most instructors are well aware of the defects of this formulation:

(1) There is, at first sight, no reason to expect a connection between the quadratic residuacity of p mod q and that of q mod p. Worse yet, it is not clear at all to most students why they should care about such a connection. In the eyes of many students, the reciprocity law remains a surprising and mysterious accident.

(2) With each generalization of the quadratic reciprocity law (cubic and quartic reciprocity, quadratic reciprocity in number fields, the general p-th power reciprocity law, Artin's reciprocity law) one moves farther and farther away from the original formulation.

The situation is completely different for Euler's version of the reciprocity law:

(1) Its formulation, $(\frac{a}{p}) = (\frac{a}{q})$ for positive primes $p \equiv q \bmod a$, is hardly more complicated than Legendre's version.

(2) Euler's version does not suggest any mysterious connection between p being a square in $\mathbb{F}_q^\times$ and q being a square in $\mathbb{F}_p^\times$; rather it emphasizes the fundamental fact that the Legendre symbol is periodic as a function of its denominator. More precisely: the symbol $(\frac{m}{p})$ only depends on the class of p in the class group attached to the class field $\mathbb{Q}(\sqrt{m}\,)$, hence on the residue class of p modulo $4m\infty$. This means, as Kronecker and Edwards [10] have observed, that Euler's version of the quadratic reciprocity law is the special case of Artin's reciprocity law for quadratic extensions.

(3) Euler's version generalizes immediately to number fields: we have $(\frac{\alpha}{\pi}) = (\frac{\alpha}{\rho})$ for all primes $\pi \equiv \rho \bmod 4\alpha\infty$. In fact, the modulus $4\alpha\infty$ can be replaced by the product of the infinite ramified primes and the relative discriminant of $K(\sqrt{\alpha}\,)/K$. The generalization to higher reciprocity laws is now immediate.

(4) Many applications of the quadratic reciprocity law become cleaner when Legendre's version is replaced by Euler's.

(5) When interpreted as a modularity conjecture, Euler's version of the reciprocity law makes it clear why we *want* the reciprocity law to hold: it allows us to prove that the Pell form is a rational function of q, or to evaluate L-series for Kronecker characters at $s = 1$.

(6) Once you have written down the Pell form and asked for its poles, quadratic Gauss sums more or less introduce themselves and have not to be pulled out of a hat.

Using Pell conics and their modularity as central objects has a couple of additional advantages: immediately after introducing Pell forms one stumbles upon myterious formulas such as $f_{\mathcal{C}}(1) = L(0,\chi)$ that point far beyond an introductory course to elementary number theory. And most theorems and conjectures in the theory of elliptic curves and modular forms can be motivated by simply replacing Pell conics by elliptic curves.

9. Additional Remarks.

Let us finally make a couple of comments concerning related material in the literature. The group structure of rational points on Pell conics and its historical ramifications were presented in [20, 21, 22]; see also [32, 36]. The idea of attaching L-series to conics can already be found in Darmon's inspirational article [8]. The analogue of the conjecture of Birch and Swinnerton-Dyer for conics was developed in [23]. A different way of generalizing Pell conics by studying "Pell surfaces" was suggested by Hambleton; see [14].

The expression "Dirichlet's Lemma" is taken from [6]. The fact that every Kronecker symbol $(\frac{a}{\cdot})$ defines a Dirichlet character defined modulo $4a$ still holds over general number fields: every quadratic residue symbol $(\frac{\alpha}{\cdot})$ for some nonzero α in a number field defines a Dirichlet character defined modulo 4α by the quadratic reciprocity law in number fields. In general, however, Dirichlet's Lemma fails to hold because not every primitive quadratic Dirichlet character can be represented in the form $(\frac{\alpha}{\cdot})$. Details will be published elsewhere.

The partial fraction decomposition in Thm. 4 is taken from [3]. The fact that Hecke operators commute is stated explicitly in [12, Lemma 1]. Herglotz found a clever way of deriving the identity (10) from the fact that $\cot x$ is an eigenfunction of T_2 with eigenvalue 1; his method is nowadays called the Herglotz trick; for a recent exposition, see [11]. I do not know whether Thm. 12 can also be proved using the Herglotz trick.

Fekete polynomials were introduced in [13]; see also [29]. The main question concerning Fekete polynomials that was studied in the literature is the location of its real roots in the interval $(0, 1)$; this question is related to the existence of Siegel zeros. For the most recent work in this direction, see [7].

The distribution relation for Bernoulli polynomials seems to be due to Raabe [30] and can be found, together with the corresponding relation for the Hurwitz zeta function, in [27]; see also [4, 5]. Artin studied similar functional equations in his book [1] on the Gamma function. Eigenfunctions of the operators T_k are often called replicative in the literature; see [31, 16, 33, 35]. The concept of distributions in this sense was developed by Kubert and Lang; see e.g. [18, 26, 34]. For more connections between Bernoulli polynomials, Hurwitz zeta functions and the cotangent function see [25].

The idea of using the sine function for proving the quadratic reciprocity law is due to Eisenstein (see Ireland & Rosen [15], in particular for the proof of Lemma 14). Kronecker observed that the sign of the right hand side in (13) suffices for determining $(\frac{q}{p})$, and since $\operatorname{sgn}(\sin \pi x) = \operatorname{sgn}(x)$ for $-1 < x < 1$, we obtain

$$\Big(\frac{q}{p}\Big) = \prod_{a \in A} \prod_{b \in B} \operatorname{sgn}\Big(\frac{a}{p} - \frac{b}{q}\Big),$$

which is the basis of one of Kronecker's proofs of the quadratic reciprocity law (see [19] for references).

References

[1] E. Artin, *The Gamma Function*, New York 1964 14

[2] A. Ash, R. Gross, *Fearless symmetry*, Princeton Univ. Press 2006 1

[3] R. Ayoub, *On L-Functions*, Monatsh. Math. **71** (1967), 193–202 14

[4] L. Carlitz, *The multiplication formulas for the Bernoulli and Euler polynomials*, Math. Mag. **27** (1952), 59–64 14

[5] L. Carlitz, *A note on the multiplication formulas for the Bernoulli and Euler polynomials*, Proc. Amer. Math. Soc. **4** (1953), 184–188 14

[6] H. Cohn, *A second course in number theory*, John Wiley and Sons 1962; 2nd ed. *Advanced number theory*, Dover 1980 14

[7] B. Conrey, A. Granville, B. Poonen, K. Soundararajan, *Zeros of Fekete polynomials*, Ann. Inst. Fourier **50** (2000), 865–889 14

[8] H. Darmon, *Wiles' Theorem and the arithmetic of elliptic curves*, in *Modular forms and Fermat's Last Theorem*, (Cornell, Silverman, Stevens (eds.)), Springer-Verlag 1997, 549–569 1, 14

[9] H. Darmon, C. Levesque, *Sommes infinies, équations diophantiennes et le dernier théorème de Fermat*, Comptes-Rendus Coll. Sci. Math. Québec, October 1995; and Gaz. Sci. Math. Québec **18** (1996); 1

[10] H.M. Edwards, *Euler and quadratic reciprocity*, Math. Mag. **56** (1983), 285–291 13

[11] J. Elstrodt *Partialbruchentwicklung des Kotangens, Herglotz-Trick und die Weierstraßsche stetige, nirgends differenzierbare Funktion*, Math. Semesterber. **45** (1998), 207–220 14

[12] J. Elstrodt, *Mittelwertoperatoren und Charakterisierung des Kotangens durch Funktionalgleichungen*, Math. Semesterber. **52** (2005), 197–219 14

[13] M. Fekete, G. Polya, *Über ein Problem von Laguerre*, Rend. Palermo **34** (1912), 89–120 14

[14] S. Hambleton, F. Lemmermeyer, *Arithmetic of Pell Surfaces*, Acta Arith. (2011) 14

[15] K. Ireland, M. Rosen, *A classical introduction to modern number theory*, Springer-Verlag 1990 14

[16] R. Jäger, *Charakterisierung des Cotangens mit Replikativität*, manusc. math. **56** (1986), 167–175 14

[17] A.W. Knapp, *Elliptic Curves*, Princeton Univ. Press 1992 5

[18] D. Kubert, *The universal ordinary distribution*, Bull. Soc. Math. France **107** (1979), 179–202 14

[19] F. Lemmermeyer, *Reciprocity Laws. From Euler to Eisenstein*, Springer-Verlag 2000 14

[20] F. Lemmermeyer, *Higher descent on Pell conics. I. From Legendre to Selmer*, arXiv: math/0311309v1 14

[21] F. Lemmermeyer, *Higher descent on Pell conics. II Two centuries of missed opportunities*, arXiv: math/0311296v1 14

[22] F. Lemmermeyer, *Higher descent on Pell conics. III The first* 2*-descent*, arXiv: math/0311310v1 14

[23] F. Lemmermeyer, *Conics – a poor man's elliptic curves*, arXiv:math/0311306v1 14

[24] F. Lemmermeyer, *The Weil conjectures for number fields*, in preparation 12

[25] H.L. Li, M. Hashimoto, S. Kanemitsu, *The structural elucidation of Eisenstein's formula*, Sci. China Math. (2010), 1–10 14

[26] J. Milnor, *On polylogarithms, Hurwitz zeta functions, and the Kubert identities*, Ens. Math. **29** (1983), 281–322 14

[27] L. Mordell, *Integral formulae of arithmetical character*, J. London Math. Soc. **33** (1958), 371–375 14

[28] J. Neukirch, *Ansichten über die Langlands-Vermutung*, Regensburger Trichter 18 (1983), 54 pp 1

[29] G. Polya, *Verschiedene Bemerkungen zur Zahlentheorie*, Jahresber. DMV **28** , 31–40 14

[30] J.L. Raabe, *Die Jacob-Bernoullische Function*, Zurich 1848 14

[31] P. Schroth, *On* $(1, b_p)$*-replicative functions with isolated discontinuities*, Aequ. Math. **20** (1980), 73–79 14

[32] S. Shirali, *Groups associated with conics*, Math. Gaz. **93** (2009), 27–41 14

[33] H. Walum, *Multiplication formulae for periodic functions*, Pac. J. Math. **149** (1991), 383–396 14

[34] L. Washington, *Introduction to cyclotomic fields*, Springer-Verlag 1982 8, 14

[35] M.F. Yoder, *Continuous replicative functions*, Aequat. Math. **13** (1975), 251–261 14

[36] N J Wildberger, *AlgTop2: Homeomorphism and the group structure on a circle*, online lecture, `http://www.youtube.com/watch?v=-ypicun4AbM` 14