PELL CONICS AND QUADRATIC RECIPROCITY

S. HAMBLETON AND V. SCHARASCHKIN

ABSTRACT. We give a proof of quadratic reciprocity, based on the arithmetic of conics. The proof works in all cases, and the calculations are remarkably simple.

1. Introduction. A large number of proofs of quadratic reciprocity are known [3]. In this paper we give a proof using the arithmetic of conics. This approach has the advantage that all the calculations are almost trivial, and we avoid Gauss's lemma.

If \( f \) is a polynomial let \( V(f) \) be the list of roots of \( f \) (in a splitting field), with multiplicity. If \( f \in \mathbb{Z}[x] \), let \( \tilde{f} \in \mathbb{F}_p[x] \) denote the reduction of \( f \) modulo \( p \).

In Proposition 2.3 we show that for all odd primes \( p \) and \( q \) there exist monic polynomials \( F_p, F_q \in \mathbb{Z}[x] \) of degrees \( (p - 1)/2 \) and \( (q - 1)/2 \) such that

\[
\left( \frac{q}{p} \right) = \prod_{a \in V(F_p)} F_q(a).
\]

The main part of quadratic reciprocity follows immediately from the next proposition. We shall derive the supplementary law for the prime 2 similarly.

Proposition 1.1. Let \( g \) and \( h \) be monic polynomials. Then

\[
\prod_{a \in V(g)} h(a) = (-1)^{\deg g \cdot \deg h} \prod_{b \in V(h)} g(b).
\]

Proof. This is a property of resultants. See [1, Chapter 3]. We give a proof for completeness. Clearly \( h(x) = \prod_{b \in V(h)} (x - b) = \)
affine Pell conics, analogous to addition on elliptic curves. Let \( h(a) = (-1)^{deg h} \prod_{b \in V(h)} (b - a) \). So

\[
\prod_{a \in V(g)} h(a) = \prod_{a \in V(g)} (-1)^{deg h} \prod_{b \in V(h)} (b - a)
\]

and

\[
= (-1)^{deg g} \prod_{b \in V(h)} g(b).
\]

2. Quadratic reciprocity. Lemmermeyer defined a group law on affine Pell conics, analogous to addition on elliptic curves. See [4]. In this framework, the polynomials \( F_m \), we use are derived from the conic analogues of the \( m \)-division polynomials for elliptic curves.

Let \( d \neq 0 \) be a square-free integer and let \( \Delta = d \) if \( d \equiv 1 \pmod{4} \) and \( \Delta = 4d \) if \( d \equiv 2 \) and 3 \( \pmod{4} \). Let \( \mathcal{C} \) be the affine conic defined by

\[
\mathcal{C} : x^2 - \Delta y^2 = 4.
\]

(For our purposes nothing is lost by only considering \( \Delta > 0 \), or even fixing \( \Delta = 8 \).)

If \((u,v)\) and \((x,y)\) are points on \( \mathcal{C} \), we define \((u,v) \oplus (x,y) = ((ux + \Delta vy)/2, (uv + vx)/2)\). The following properties all follow easily from this definition.

**Proposition 2.1.** (1) The set of points on \( \mathcal{C} \) with integer coordinates, \( \mathcal{C}(\mathbb{Z}) \), is an Abelian group with identity \( O = (2,0) \), and point \( T = (-2,0) \) of order 2. No other points have \( y = 0 \) or \( x = 2 \). The inverse of \((x,y)\) is \((x,-y)\).

(2) There are no points of finite order \((x,y)\) with \( x > 2 \).

(3) If \( p \) is a prime not dividing \( 2\Delta \) and \( q = p^l \) we may consider \( \mathcal{C} \) defined over the field \( \mathbb{F}_q \), which we denote \( \mathcal{C} \). The group \( \mathcal{C}(\mathbb{F}_q) \) has order \( q \pm 1 \).

**Proof.** (1) follows immediately from the definition.

(2) If \( m(x,y) = O \) with \( x > 2 \), then \( m(x,-y) = O \) also, so without loss of generality we may assume \( y > 0 \). Suppose \( P = (u,v), Q = (x,y) \) are points on the conic with \( u, x > 2 \) and \( v, y > 0 \). Clearly \( y(P \oplus Q) > 0 \). If \( x = u \) then \( v = y \) so \( x(P \oplus Q) = x^2 - 2 > 2 \). Otherwise \( 4(x - u)^2 > 0 \) implies \( (ux - 4)^2 > (u^2 - 4)(x^2 - 4) = (\Delta y)^2 \) so again \( x(P \oplus Q) > 2 \).

(3) This follows on considering the birational map from \( \mathcal{C} \) to the affine hyperbola \( \mathcal{H} : uv = \Delta \) given by

\[
P = (x,y) \mapsto \left(\frac{x - 2, x + 2}{y}, \frac{y}{y}ight)
\]

for \( P \neq \mathcal{O}, T \),

with inverse map \( \mathcal{H} \to \mathcal{C} \) given by

\[
Q = (u,v) \mapsto \left(\frac{2(u + v)}{v}, \frac{u}{v}ight)
\]

for \( u \neq v \).

Define monic polynomials \( f_m, g_m \in \mathbb{Z}[x] \) of degrees \( m, m-1 \) (if \( m > 1 \)) respectively by \( f_0 = 2, f_1 = x, g_0 = 0, g_1 = 1 \) and for \( m \geq 1 \) define

\[
f_{m+1} = x f_m - f_{m-1}, \quad g_{m+1} = x g_m - g_{m-1}.
\]

The polynomials \( f_m \) and \( g_m \) are conic analogues of the division polynomials \( \psi_m, \phi_m, \omega_m \) for elliptic curves [6, Example 3.7, page 105], with the advantage that \( f_m \) and \( g_m \) are independent of \( \Delta \).

**Proposition 2.2.** Let \( P = (x,y) \) be a point on \( \mathcal{C} \). Then \( m P = (f_m(x), y g_m(x)) \) for \( m \geq 0 \). Furthermore, \( f_m(2) = 2, f_m'(2) = m^2 \) and \( f_m''(2) = (1/6)m^2(m^2 - 1) \).

**Proof.** These results are all straightforward induction arguments. We check that for all \( m \geq 1 \)

\[
(x^2 - 4)g_m = xf_m - 2f_{m-1}, \quad 2g_{m+1} = f_m + xg_m.
\]

Let \( m P = (x_m, y_m) \). The addition formula gives \( x_{m+1} = (xf_m + (x^2 - 4)g_m)/2 = xf_m - f_{m-1} \) and the required result follows by induction, and similarly for \( y_{m+1} \). Also \( mO = 0 \) so \( f_m(2) = 2 \). The derivative properties follow similarly.

In particular, the group of \( m \)-torsion points \( \mathcal{C}[m] \) is finite, and indeed \( m(x,y) = O \) if and only if \( f_m(x) = 2 \).
Since $mp$ lies on $C$ we have $(f_m - 2)(f_m + 2) = (x^2 - 4)g_m^2$, with the factors on the left hand side relatively prime. Also $(x - 2) | (f_m - 2)$, while if $m$ is odd then $m \neq 0$, so $(x + 2) \nmid (f_m - 2)$. Thus $(f_m(x) - 2)/(x - 2)$ must be a square. That is,

\[ f_m(x) - 2 = (x - 2)^2 \quad (\text{m odd}) \]

for some monic polynomial $F_m \in \mathbb{Z}[x]$ of degree $(m - 1)/2$. Also define $F_2(x) = x$.

**Proposition 2.3.** Let $p$ and $q$ be prime numbers with $p \neq 2$. Then

\[ \left( \frac{q}{p} \right) = \prod_{a \in V(F_p)} F_q(a) \]

(where in the product the $a$ occur according to their multiplicity).

**Proof.** We may assume $p \neq q$. Let $L_{q,p} = \prod_{a \in V(F_p)} F_q(a)$. Choose $\Delta$ not divisible by $p$, and consider the associated conic $C$.

Let $\mathcal{P}$ be a splitting field of $F_p$ over $F_p$. By Proposition 2.1 no element of $\mathcal{C}(\mathcal{P})$ has order $p$. Thus the only root of $F_p$ in $\mathcal{P}$ is $x = 2$, so

\[ F_p(x) = (x - 2)^{(p-1)/2}. \]

Hence

\[ L_{q,p} = \prod_{a \in V(F_p)} F_q(a) \equiv F_q(2)^{(p-1)/2} \equiv \left( \frac{F_q(2)}{p} \right) \quad (\text{mod } p). \]

If $q = 2$ then $F_q(2) = q$. Otherwise, by Proposition 2.2 the Taylor series expansion of $f_m$ about $x = 2$ is $f_m(x) = 2 + m(x - 2) + (1/12)m^2(m^2 - 1)(x - 2)^2 + \cdots$. By equation (1) the Taylor series expansion of $F_m$ about $x = 2$ for odd $m$ is

\[ \pm F_m(x) = m + \frac{m(m^2 - 1)}{24}(x - 2) + (\text{higher order terms}), \]

and so $F_m(2) = \pm m$. If $F_m(2) = -m$, then $F_m$ has a real root greater than 2, contradicting Proposition 2.1 (2), so the sign in equation (3) is $+$ and in all cases

\[ \left( \frac{F_q(2)}{p} \right) = q. \]

Thus $L_{q,p} \equiv (q/p) \quad (\text{mod } p)$.

To finish the proof we show that $L_{q,p} = \pm 1$. Multiplication by $q$ is an automorphism of the group of $p$-torsion points $\mathcal{C}[p]$, and hence $f_q$ permutes $V(F_p)$. Thus

\[ \prod_{x \in V(F_p)} (x - 2) = \prod_{x \in V(F_p)} (f_q(x) - 2) = \prod_{x \in V(F_p)} (x - 2)F_q(x)^2. \]

Canceling the factors $(x - 2)$ (which are nonzero by equation (4)) shows that $L_{q,p} = \pm 1$. \(\square\)

This establishes quadratic reciprocity for odd primes. If $q = 2$, then applying Proposition 1.1 to equation (2) gives

\[ \left( \frac{2}{p} \right) = L_{2,p} = (-1)^{p-1/2} F_p(0). \]

Thus $F_p(0) = \pm 1$. To determine the sign of $F_p(0)$ it suffices to find $F_p(0) \pmod{4}$. Evaluating equation (3) at $x = 0$ gives

\[ F_p(0) = \begin{cases} +1 & \text{if } p = 1, 3 \pmod{8} \\ -1 & \text{if } p = 5, 7 \pmod{8} \end{cases}. \]

The quadratic character of 2 follows.

3. **Remarks.** Let $T_n(x) = \cos(n \arccos x)$, so that $T_n$ is the $n$th Chebyshev polynomial. See [5]. The $T_n$ satisfy almost the same recurrence relation as the $f_n$ and one checks easily that $f_n(x) = 2T_n(x/2)$. Thus

\[ f_n(x) = \prod_{j=0}^{n-1} \left( x - 2 \cos \left( \frac{(2j+1)\pi}{2n} \right) \right). \]
Our proof can therefore be viewed as Eisenstein's trigonometric proof in disguise. Compare [2, Chapter 5.3].

ENDNOTES

1. We consider the 0 polynomial to be degree \(-1\).

REFERENCES


DEPT. MATHEMATICS, UNIVERSITY OF QUEENSLAND, ST LUCIA, QUEENSLAND, AUSTRALIA
Email address: sah@maths.uq.edu.au

DEPT. MATHEMATICS, UNIVERSITY OF QUEENSLAND, ST LUCIA, QUEENSLAND, AUSTRALIA
Email address: victors@maths.uq.edu.au

ABSTRACT. The tensor product of two proper Hausdorff locally \(m\)-convex \(H^*\)-algebras with continuous involution, endowed with the projective tensor product topology, along with its completion, are algebras of the same type with the factors. Under appropriate conditions, a canonical orthogonal basis is provided in the completion of the tensor product algebra. Based on this, the minimal closed 2-sided ideals are determined, yielding, in turn, the second Wedderburn structure theorem.

0. Introduction. The theory of \(H^*\)-(Banach) algebras with the corresponding Wedderburn structure theorems have been developed by Ambrose in [1]. The notion of an \(H^*\)-algebra is the abstract version of characteristic properties of the algebra \(L^2(G)\) of a compact group (with the convolution as ring multiplication). It is known (ibid) that an \(H^*\)-algebra lies between the group algebra of a compact group and that of a (non-compact) locally compact group.

In [9–11, 14, 15] we considered extensions of the results in [1] to locally \(m\)-convex topological algebras. Our point of view is justified by theoretical reasons with an increasing interest in topological \(*\)-algebras (function algebras, topological \(K\)-theory, [7, 19, 20]), especially, in \(*\)-algebras endowed with locally convex topologies generated by \(C^*\)-seminorms, applicable, for instance, even to relativistic quantum theory. See, e.g., [2, 3, 16, 18]. In this context, we also note that a particular locally \(m\)-convex \(H^*\)-algebra admits a locally \(m\)-convex \(C^*\)-topology (cf. [13, page 198, Proposition 2.5], [4, page 265, Proposition 2.3]; see also [5, 6]). Our study reveals some hidden characteristic