ACTA ARITHMETICA
146.1 (2011)

Arithmetic of Pell surfaces

by

S. Hambleton (Brisbane) and F. Lemmermeyer (Jagstzell)

1. Introduction. A classical technique for constructing quadratic number fields with class number divisible by n is studying integral solutions of the equation

$$X^2 - \Delta Y^2 = 4Z^n, \quad \gcd(X,Z) = 1,\ \Delta \text{ a fundamental discriminant.} \tag{1.1}$$

For each integral point (X,Y,Z) we can form the ideal

$$\mathfrak{a} = \left(\frac{X + Y\sqrt{\Delta}}{2}, Z\right)$$

in the ring of integers of $\mathbb{Q}(\sqrt{\Delta})$; the ideal $\mathfrak{a}$ has norm $|Z|$ and satisfies $\mathfrak{a}^n = \left(\frac{X+Y\sqrt{\Delta}}{2}\right)$, hence generates an ideal class of order dividing n.

It seems that P. Joubert [6] was the first to observe that a class of prime order n in the group of binary quadratic forms with negative discriminant Δ implies the solvability of the equation (1.1); Joubert used techniques from the theory of complex multiplication to exploit this observation. Nagell [11] later used (1.1) to prove the existence of infinitely many complex quadratic number fields with class number divisible by n. By extending Nagell's approach, Yamamoto [13] was able to prove the existence of infinitely many *real* quadratic number fields with class number divisible by n.

The same approach was further extended by various authors; we mention in particular Craig [4].

In this article, we interpret (1.1) as an affine surface and show that a certain subset $\mathcal{S}_n(\mathbb{Z})$ of the integral points on (1.1) can be given a group structure in such a way that

(a) the integral points on the hyperplane $Z = 1$, which lie on the Pell conic $X^2 - \Delta Y^2 = 4$, form a subgroup with respect to the classical group structure on Pell conics (see [7, 8, 9]);

2010 *Mathematics Subject Classification*: Primary 14J25, 11G10; Secondary 11R11, 11R29.
Key words and phrases: surface arithmetic, Pell conics, class group, quadratic number field, norm form.

DOI: 10.4064/aa146-1-1 © Instytut Matematyczny PAN, 2011

(b) there is a surjective group homomorphism $\mathcal{S}_n(\mathbb{Z}) \to \mathrm{Cl}^+(K)[n]$ to the n-torsion of the narrow class group of $K = \mathbb{Q}(\sqrt{\Delta})$.

These results explain the success of Yamamoto's approach, and at the same time raise a few new problems that we do not yet fully understand. The rational points on the surface lying on the hyperplane $Y = 1$ form (the affine part of) a hyperelliptic curve $E : X^2 = 4Z^n + \Delta$; in the case $n = 3$, this is an elliptic curve. Although the integral points on E do not form a group in general, it was observed by Buell [2, 3] and Soleng [12] that the integral points on E (and, more generally, certain rational points satisfying some technical conditions) give ideal classes of order dividing 3 in such a way that the map from E to the 3-class group respects the group law on the elliptic curve, i.e., that collinear points get mapped to classes whose product is trivial. Bölling [1] has extended Buell's results [2, 3] to the hyperelliptic curves lying on the surface (1.1).

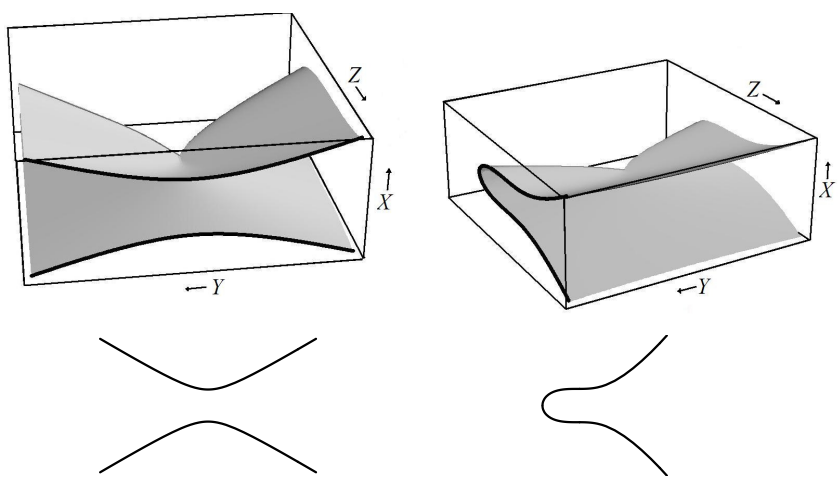

Fig. 1. Top: Different views of $\mathcal{S}_3$ for some $\Delta > 0$ showing cross-sections $Z = 1$, a Pell conic on the left, and $Y = 1$, an elliptic curve on the right. Bottom: The corresponding curves in the XY and XZ planes respectively.

Although we will see below that the group law ([1]) is best understood by using ideals in quadratic number fields, the explicit addition formulas are tied closely to the composition of binary quadratic forms. For this reason, we replace the equation (1.1) of the surface by $Q_0(X, Y) = Z^n$, where Q_0 is the principal form with discriminant Δ defined below. For a brief introduction to the composition of binary quadratic forms via Bhargava's cubes see

([1]) The group law on Pell surfaces was discovered by the first author, as was the homomorphism to the class group.

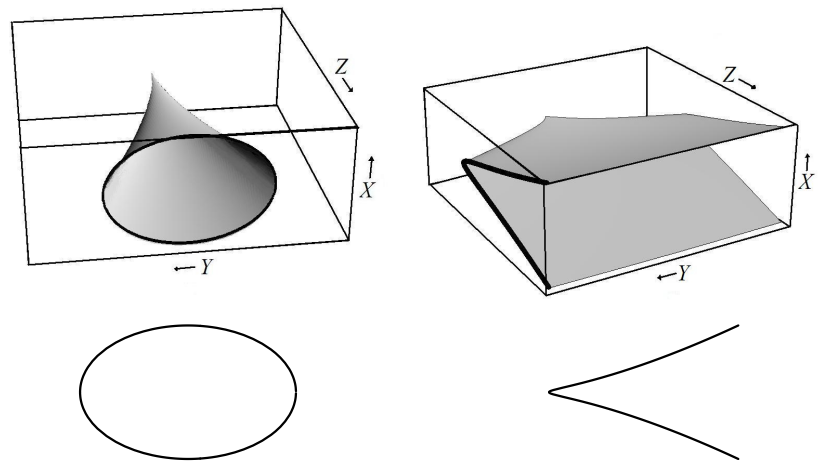

Fig. 2. Different views of $\mathcal{S}_3$ for some $\Delta < 0$ showing cross sections as in Figure 1

Lemmermeyer [10]; more details along more classical lines can be found in Flath [5].

2. Primitive points on Pell surfaces. Let Δ be a *fundamental discriminant* (the discriminant of a quadratic number field). The principal form with discriminant Δ is defined by

$$Q_0(x,y) = \begin{cases} x^2 - my^2 & \text{if } \Delta = 4m, \\ x^2 + xy - my^2 & \text{if } \Delta = 4m+1. \end{cases}$$

By $Q = (a,b,c)$ we denote the binary quadratic form $ax^2 + bxy + cy^2$. Such a form Q *represents* an integer d if $Q(x,y) = d$ for some integers x, y; it is said to represent d *primitively* if, in addition, $\gcd(x,y) = 1$.

An integral point (A,B,C) on the Pell surface

$$\mathcal{S}_n : Q_0(B,C) = A^n \tag{2.1}$$

is called *primitive* if $\gcd(B,C) = 1$. The set of primitive points on $\mathcal{S}_n$ will be denoted by $\mathcal{S}_n(\mathbb{Z})$.

Now consider (1.1) and map a point (A,B,C) on the Pell surface (2.1) to a point (X,Y,Z) on (1.1) by setting

$$(X,Y,Z) = \begin{cases} (2B,C,A) & \text{if } \Delta = 4m, \\ (2B+C,C,A) & \text{if } \Delta = 4m+1. \end{cases}$$

This clearly gives a bijection between the integral points on these surfaces. In addition, Yamamoto's condition $\gcd(X,Z) = 1$ is easily seen to be equivalent to the primitivity of (A,B,C), that is, to $\gcd(B,C) = 1$.

3. The group law. Let $\mathcal{O}$ denote the ring of integers of the quadratic number field $\mathbb{Q}(\sqrt{\Delta})$. There is a natural map $\pi_0 : \mathcal{S}_n(\mathbb{Z}) \to \mathcal{O}$ defined by $\pi_0(A,B,C) = B + C\omega$, where

$$\omega = \frac{\sigma + \sqrt{\Delta}}{2},$$

and $\sigma \in \{0,1\}$ is defined by $\Delta = 4m + \sigma$. The elements in the image of π_0 have the property that their norms are nth powers: $N(\pi_0(A,B,C)) = Q_0(B,C) = A^n$.

Consider the set $\mathcal{O}^*$ of nonzero elements in $\mathcal{O}$ and its subset $\mathbb{N}$ of nonzero natural numbers. The set $\mathcal{O}^*/\mathbb{N}^n$, using $\mathbb{N}^n$ to refer to positive integers which are nth powers, is a group with respect to multiplication: the neutral element is $1\mathbb{N}^n$, the inverse of $\alpha\mathbb{N}^n$ is $\alpha^{-1}|N(\alpha)|^n\mathbb{N}^n$ (the element $|N\alpha|/\alpha$ is, up to sign, simply the conjugate α' of α, and so belongs to $\mathcal{O}^*$). The norm map induces a group homomorphism $N : \mathcal{O}^*/\mathbb{N}^n \to \mathbb{Z}^*/\mathbb{Z}^{*n}$, where $\mathbb{Z}^* = \mathbb{Z} \setminus \{0\}$ and $\mathbb{N}$ denote the monoids of nonzero and of positive integers, respectively.

Observe that if $\alpha, \beta \in \mathcal{O}^*$ are primitive (this means that $p \nmid \alpha$ for all primes $p \in \mathbb{N}$) and $\alpha\mathbb{N}^n \cdot \beta\mathbb{N}^n = \gamma\mathbb{N}^n$, then in general γ cannot be chosen to be primitive. An example is provided by $\alpha = 3 + \sqrt{3}$ and $\beta = \sqrt{3}$, where $\gamma = 3+3\sqrt{3}$; here $\gamma\mathbb{N}^n$ is not generated by a primitive element for any $n \ge 2$. On the other hand we shall prove below

PROPOSITION 3.1. *The cosets of primitive elements in the kernel of the norm map $N : \mathcal{O}^*/\mathbb{N}^n \to \mathbb{Z}^*/\mathbb{Z}^{*n}$ form a subgroup Π_n of $\mathcal{O}^*/\mathbb{N}^n$.*

This fact allows us to prove that there is a bijective map $\pi : \mathcal{S}_n(\mathbb{Z}) \to \Pi_n$ given by $\pi(A,B,C) = (B + C\omega)\mathbb{N}^n$; using this bijection we can make $\mathcal{S}_n(\mathbb{Z})$ into an abelian group. The situation is summed up by the following diagram:

$$\begin{array}{ccccccc} \mathcal{S}_n(\mathbb{Z}) & \xrightarrow[\simeq]{\pi} & \Pi_n & & & & \\ & & \downarrow & & & & \\ 1 & \longrightarrow & \ker N & \longrightarrow & \mathcal{O}^*/\mathbb{N}^n & \xrightarrow{N} & \mathbb{Z}^*/\mathbb{Z}^{*n} \end{array}$$

THEOREM 3.2. *The map $\pi : \mathcal{S}_n(\mathbb{Z}) \to \Pi_n$ is bijective; thus $\mathcal{S}_n(\mathbb{Z})$ becomes an abelian group by transport of structure.*

Proof. Injectivity. Assume that there are elements $(A,B,C), (A',B',C') \in \mathcal{S}_n(\mathbb{Z})$ with $\pi(A,B,C) = \pi(A',B',C')$. Then there exist $a, b \in \mathbb{N}$ with $(B + C\omega)a^n = (B' + C'\omega)b^n$, and the primitivity of $B + C\omega$ and $B' + C'\omega$ implies that a^n and b^n must be units. Since $a, b \in \mathbb{N}$, this implies $a^n = b^n = 1$.

Surjectivity. Assume that $\alpha = B + C\omega$ is primitive with $\alpha\mathbb{N}^n \in \Pi_n$. Then $N\alpha = A^n$ for some number $A \in \mathbb{Z}^*$ implies $Q_0(B,C) = A^n$, hence $(A,B,C) \in \mathcal{S}_n(\mathbb{Z})$ with $\pi(A,B,C) = \alpha$. ∎

Observe that the neutral element of $\mathcal{S}_n(\mathbb{Z})$ is the point $(A,B,C) = (1,1,0)$, and that the inverse of (A,B,C) is given by

$$-(A,B,C) = \begin{cases} (A, B+\sigma C, -C) & \text{if } A > 0, \\ (A, -B-\sigma C, C) & \text{if } A < 0. \end{cases}$$

Observe also that the integral points on the Pell conic $Q_0(T,U) = 1$, which correspond to the points $(1,T,U)$ on the Pell surface, inherit their classical group structure since $(T_1+U_1\omega)(T_2+U_2\omega) = T_3+U_3\omega$, where $(T_3,U_3) = (T_1T_2+mU_1U_2, T_1U_2+T_2U_1)$ if $\Delta = 4m$ and $(T_3,U_3) = (T_1T_2+mU_1U_2, T_1U_2+T_2U_1+U_1U_2)$ if $\Delta = 4m+1$. In fact, since the elements $\alpha_j = T_j+U_j\omega$ have norm 1, the element $\alpha_3 = \alpha_1\alpha_2$ is always primitive.

For proving Proposition 3.1 we use the following characterization of primitive elements:

LEMMA 3.3. *Let $\alpha \in \mathcal{O}^*$ be a nonzero element of the order $\mathcal{O}$.*

(a) *α is primitive if and only if $(\alpha)+(\alpha') = \mathfrak{d}$ for some ideal $\mathfrak{d}$ dividing the product of all ramified primes.*
(b) *If $N\alpha = a^n$ for some $n \geq 2$, then α is primitive if and only if $(\alpha)+(\alpha') = (1)$.*

Proof. Assume first that α is primitive, let $\mathfrak{p}$ be an unramified prime ideal, and set $(\alpha)+(\alpha') = \mathfrak{d}$. If we had $\mathfrak{p} \,|\, \mathfrak{d}$, then $\mathfrak{p} \,|\, (\alpha)$ and $\mathfrak{p}' \,|\, (\alpha)$. Since $\mathfrak{p}$ is unramified, the prime p below $\mathfrak{p}$ either splits (and then $(p) = \mathfrak{p}\mathfrak{p}'$), or $\mathfrak{p} = (p)$ is inert. In both cases we deduce that $p \,|\, (\alpha)$, which contradicts our assumption that α be primitive.

Conversely, assume that $\mathfrak{d}$ divides the product of all ramified primes. If $p \mid \alpha$ for some prime $p \in \mathbb{N}$, then $p \mid \alpha'$, hence $p \mid \mathfrak{d}$. This shows that $(\alpha)+(\alpha')$ is divisible either by an unramified prime ideal or by the square of a ramified prime ideal, proving (a).

To prove (b), assume first that $(\alpha)+(\alpha') = (1)$; then (α) is primitive by what we have already proved.

Finally, if $N\alpha = a^n$ and α is primitive, then $\mathfrak{d}$ is a product of ramified prime ideals. But if $\mathfrak{p} \,\|\, \alpha$ for some ramified prime ideal $\mathfrak{p}$ above p, then $p \,\|\, \alpha\alpha' = a^n$, and this is impossible for $n \geq 2$. ∎

LEMMA 3.4. *Let α be a primitive element. If $\alpha\mathbb{N}^n \in \ker N$, then $(\alpha) = \mathfrak{a}^n$ is an nth ideal power. The converse holds if α is totally positive.*

Proof. The claim is trivial for $n = 1$; assume therefore that $n \geq 2$.

If α is primitive and $N\alpha = a^n$, Lemma 3.3 implies that α and α' are coprime. Now $(\alpha)(\alpha') = a^n$ implies that $(\alpha) = \mathfrak{a}^n$ is an nth ideal power.

Now assume that $(\alpha) = \mathfrak{a}^n$. Then $N\alpha = \pm A^n$ for some positive integer A, and since α is totally positive, we have $N\alpha > 0$. ∎

Proof of Proposition 3.1. Assume that α and β are primitive elements representing cosets in the kernel of the norm map. Write $\alpha\beta = \gamma a^n$ with $\gamma \in \mathcal{O}^*$ and with $a \ge 1$ maximal. We have to show that γ is primitive.

Assume not; then $p \,|\, \gamma$ for some rational prime p. Since $p \nmid \alpha$ and $p \nmid \beta$ (by the primitivity of these elements), the prime p cannot be inert, and there is a prime ideal $\mathfrak{p}$ above p with $\mathfrak{p} \,|\, (\alpha)$ and $\mathfrak{p}' \,|\, (\beta)$. Since α and β are nth ideal powers, we must have $\mathfrak{p}^{kn} \,\|\, (\alpha)$ and $\mathfrak{p}'^{kn} \,\|\, (\beta)$, and this implies $p^{kn} = (\mathfrak{p}\mathfrak{p}')^{kn} \,\|\, \gamma a^n$. By the maximality of a we must have $p^{kn} \,\|\, a^n$, and this implies $p \nmid \gamma$.

Thus Π_n is closed under multiplication; since the inverse of $\alpha\mathbb{N}^n$ is $\pm\alpha'\mathbb{N}^n$ (with the sign chosen in such a way that $\alpha \cdot (\pm\alpha') > 0$), the set Π_n forms a subgroup of $\ker N$. ∎

Remark. The points with $A = 1$ on $\mathcal{S}_n$ form a subgroup of $\mathcal{S}_n(\mathbb{Z})$; such points $(1, B, C)$ correspond to units $B + C\omega \in \mathcal{O}$, and the group law is induced by the usual multiplication of units. This shows that the group law on the Pell conic $Q_0(B, C) = 1$ coincides with the standard group law on these curves.

4. The homomorphism $\mathcal{S}_n(\mathbb{Z}) \to \mathrm{Cl}^+(K)[n]$. We have already remarked that the set $\mathcal{S}_n(\mathbb{Z})$ was used to extract information on the n-torsion of the class group $\mathrm{Cl}(K)$ of the quadratic number field $K = \mathbb{Q}(\sqrt{\Delta})$. Given a point $(A, B, C) \in \mathcal{S}_n(\mathbb{Z})$, we know that $\alpha = B + C\omega$ is an nth ideal power: $(\alpha) = \mathfrak{a}^n$. Sending α to the narrow ideal class of $\mathfrak{a}$ we get a map $c : \mathcal{S}_n(\mathbb{Z}) \to \mathrm{Cl}^+(K)[n]$ from $\mathcal{S}_n(\mathbb{Z})$ to the group of ideal classes (in the strict sense) in K whose order divides n:

Proposition 4.1. *The map*

$$c : \mathcal{S}_n(\mathbb{Z}) \to \mathrm{Cl}^+(K)[n]$$

is a surjective group homomorphism.

Proof. Proving that c is a group homomorphism is easy: let $P_j = (A_j, B_j, C_j) \in \mathcal{S}_n(\mathbb{Z})$ with $P_1 \oplus P_2 = P_3$, and put $\alpha_j = B_j + C_j\omega$. Then $(\alpha_j) = \mathfrak{a}_j^n$, and $\alpha_1\mathbb{N}^n \cdot \alpha_2\mathbb{N}^n = \alpha_3\mathbb{N}^n$ for some α_3 that differs from $\alpha_1\alpha_2$ by the nth power of some positive integer a. This implies that $\mathfrak{a}_1^n\mathfrak{a}_2^n = \mathfrak{a}_3^n \cdot a^n$, hence $c(P_1)c(P_2) = c(P_1 \oplus P_2)$ as claimed.

To prove that c is onto, consider the narrow ideal class $[\mathfrak{a}] \in \mathrm{Cl}^+(K)[n]$ for some ideal $\mathfrak{a}$ coprime to the discriminant. Then $\mathfrak{a}^n = (\alpha)$ for some $\alpha = B + C\omega$. We claim that we can choose $\mathfrak{a}$ in such a way that α is primitive. In fact, let p be a prime dividing B and C. If p is inert, then $\mathfrak{a} = p\mathfrak{b}$, and replacing $\mathfrak{a}$ by $\mathfrak{b}$ does not change the ideal class. If $(p) = \mathfrak{p}\mathfrak{p}'$ is split, then we must have $\mathfrak{p} \,|\, \mathfrak{a}$ and $\mathfrak{p}' \,|\, \mathfrak{a}$, so again $\mathfrak{a} = p\mathfrak{b}$. Since $\mathfrak{a}$ is coprime to the discriminant, ramified prime ideals do not divide $\mathfrak{a}$. Since (α) is principal

in the strict sense, we have $A^n = N\alpha > 0$; writing $\alpha = B + C\omega$ we find $(A, B, C) \in \mathcal{S}_n(\mathbb{Z})$ as claimed. ∎

Observe that $\mathcal{S}_n^+(\mathbb{Z})$, the subset of all $(A, B, C) \in \mathcal{S}_n(\mathbb{Z})$ with $A > 0$, forms a subgroup of $\mathcal{S}_n(\mathbb{Z})$, and that the proof above shows that the natural map $\mathcal{S}_n^+(\mathbb{Z}) \to \mathrm{Cl}^+(K)[n]$ is surjective.

It is in general difficult to tell whether a point $(A, B, C) \in \mathcal{S}_n(\mathbb{Z})$ gives rise to an element of exact order n or not, or more generally, whether two points generate independent elements. In the following, we shall briefly recall the criterion used by Yamamoto.

To this end, we introduce a natural homomorphisms between the groups $\mathcal{S}_n(\mathbb{Z})$:

PROPOSITION 4.2. *Assume that $m \mid n$; then there is a group homomorphism*

$$\iota_{m\to n} : \mathcal{S}_m(\mathbb{Z}) \to \mathcal{S}_n(\mathbb{Z}).$$

In order to avoid a problematic case, we let $\mathcal{S}_1(\mathbb{Z})$ denote the set of all primitive points (A, B, C) such that $\gcd(A, \Delta) = 1$; equivalently, $B + C\omega$ is primitive and not divisible by any ramified prime ideal.

Proof. Assume that $(A, B, C) \in \mathcal{S}_m(\mathbb{Z})$. With $\alpha = B + C\omega$ we have $(\alpha) = \mathfrak{a}^m$; setting $n = km$, we find $(\alpha^k) = \mathfrak{a}^n$, hence $N(\alpha^k) = (A^m)^k = A^n$. Observe that α^k is primitive if α is, except possibly when $m = 1$ and α is divisible by a ramified prime.

Setting $\alpha^k = B' + C'\omega$, we have $(A, B', C') \in \mathcal{S}_n(\mathbb{Z})$. Since the map $\iota_{m\to n}$ sending (A, B, C) to (A, B', C') is compatible with the group structure (in fact: if $(B_1 + C_1\omega)a_1^m \cdot (B_2 + C_2\omega)a_2^m = (B_3 + C_3\omega)a_3^m$, then raising this equation to the kth power shows that $(B_1' + C_1'\omega)a_1^n \cdot (B_2' + C_2'\omega)a_2^n = (B_3' + C_3'\omega)a_3^n$), the claim follows. ∎

As an example, consider the surface $B^2 + BC + 6C^2 = A^3$; using the point $(6, 1, -1)$ on $\mathcal{S}_1(\mathbb{Z})$ we find $(1 - \omega)^3 = -11 + 5\omega$, which gives us the point $(6, -11, 5) \in \mathcal{S}_3(\mathbb{Z})$.

It is desirable to have criteria for deciding whether a point $P \in \mathcal{S}_n(\mathbb{Z})$ is actually a newpoint, i.e., does not come from $\mathcal{S}_m(\mathbb{Z})$ for some proper divisor m of n.

PROPOSITION 4.3. *Assume that $\Delta < -4$. If $P = (A, B, C) \in \mathcal{S}_n(\mathbb{Z})$ and $n = mp$ for some odd prime p, then $P = \iota_{m\to n}(Q)$ for some $Q \in \mathcal{S}_m(\mathbb{Z})$ implies that $2B + \sigma C$ is a pth power modulo q for every prime $q \mid A$.*

Proof. Let $\alpha = B + C\omega$ and $(\alpha) = \mathfrak{a}^n$. If $P = \iota_{m\to n}(Q)$ for some $Q \in \mathcal{S}_m(\mathbb{Z})$, then $\mathfrak{a}^m = (\beta)$ for $\beta = b + c\omega$ and $Q = (A, b, c)$. Thus $\alpha = \pm\beta^p = (\pm\beta)^p$ is a pth power. Let q be a prime dividing A; then $(q) = \mathfrak{q}\mathfrak{q}'$ splits in k, and we have $\beta \in \mathfrak{q}'$ and $\beta' \in \mathfrak{q}$.

If $\Delta = 4m$, then $b \equiv c\sqrt{m} \bmod \mathfrak{q}$, hence $\beta = b + c\sqrt{m} \equiv 2b \bmod \mathfrak{q}$, $\alpha = B + C\sqrt{m} \equiv 2B \bmod \mathfrak{q}$, and so $2B \equiv \alpha = \beta^p \equiv (2b)^p \bmod \mathfrak{q}$. This implies $2B \equiv (2b)^p \bmod q$ as claimed.

Now assume that $\Delta = 4m+1$. Then $b+c\omega' \in \mathfrak{q}$ shows that $b + c \equiv c\omega \bmod \mathfrak{q}$ (since $\omega\omega' = 1$), hence $2B + C \equiv B + C\omega = (b + c\omega)^p \equiv (2b + c)^p \bmod q$. ∎

This criterion is not very strong; it does not detect that the points $(2, 1, 1)$ or $(3, 1, 2)$ on $\mathcal{S}_3 : B^2 + BC + 6C^2 = A^3$ are newpoints. On the other hand, $(13, 37, 6)$ must be a newpoint since $80 = 2 \cdot 37 + 6$ is not a cube modulo 13.

5. Explicit formulas. Let us now make the group law on $\mathcal{S}_n(\mathbb{Z})$ explicit by deriving addition formulas

$$(A_1, B_1, C_1) \oplus (A_2, B_2, C_2) = (A_3, B_3, C_3). \tag{5.1}$$

From the definition of the group law it is clear that such addition formulas must involve computations of greatest common divisors. The following lemma contains the technical part of the proof:

LEMMA 5.1. *For points $(A_j, B_j, C_j) \in \mathcal{S}_n(\mathbb{Z})$, $j \le 3$, we set $\alpha_j = B_j + C_j\omega$. Let $\mathfrak{d} = (\alpha_1, \alpha_2')$; then $\mathfrak{d} = \mathfrak{e}^n$ is an nth ideal power, and with $e = N\mathfrak{e}$, we have*

$$\gcd(B_1B_2 + mC_1C_2, B_1C_2 + B_2C_1 + \sigma C_1C_2) = e^n. \tag{5.2}$$

Conversely, the gcd on the left hand side of (5.2) *is an nth power, and if* (5.2) *holds, then $(\alpha_1, \alpha_2') = \mathfrak{e}^n$ for an ideal $\mathfrak{e}$ with norm e.*

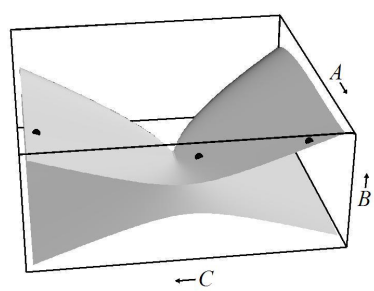

Fig. 3. From left to right, $(3, 92, 13) \oplus (3, 17, -2) \oplus (9, 93, -11) = (1, 1, 0)$ on $B^2 + BC - 57C^2 = A^3$.

Proof. Since $(\alpha_j) = \mathfrak{a}_j^n$, the ideal $\mathfrak{d}$ must be an nth power. From $\mathfrak{e} \mid \mathfrak{a}_1$ and $\mathfrak{e} \mid \mathfrak{a}_2'$ we deduce that $(e^n) = (\mathfrak{e}\mathfrak{e}')^n \mid (\alpha_1\alpha_2)$, and now

$$\begin{aligned} \alpha_1\alpha_2 &= (B_1 + C_1\omega)(B_2 + C_2\omega) \\ &= B_1B_2 + C_1C_2m + (B_1C_2 + B_2C_1 + \sigma C_1C_2)\omega \end{aligned} \tag{5.3}$$

implies $e^n \mid \gcd(B_1B_2 + C_1C_2m, B_1C_2 + B_2C_1 + \sigma C_1C_2)$.

If, conversely, p is a prime dividing $d = \gcd(B_1B_2 + C_1C_2m, B_1C_2 + B_2C_1 + \sigma C_1C_2)$, then the primitivity of P_j implies that $(p) = \mathfrak{p}\mathfrak{p}'$ must be split in $K = \mathbb{Q}(\sqrt{\Delta})$. If, say, $\mathfrak{p} \mid \alpha_1$, then the primitivity of α_1 shows that we must have $\mathfrak{p}' \mid \alpha_2$ and therefore $\mathfrak{p}' \mid \alpha_1'$. Thus if p^m is the exact power of p dividing d, then $\mathfrak{p}^m$ is the exact power of $\mathfrak{p}$ dividing α_1, and the fact that (α_1) is an nth ideal power shows that m must be a multiple of n. This implies that

- $d = e^n$ must be an nth power,
- $(e) = \mathfrak{e}\mathfrak{e}'$ is the norm of an ideal $\mathfrak{e}$, and
- $\mathfrak{e}^n \mid (\alpha_1, \alpha_2')$.

This completes the proof. ∎

Now we can present the explicit formulas for adding points on $\mathcal{S}_n(\mathbb{Z})$:

PROPOSITION 5.2. *For $(A_1, B_1, C_1), (A_2, B_2, C_2) \in \mathcal{S}_n(\mathbb{Z})$ we have the addition formula* (5.1)*, where*

$$A_3 = \frac{A_1A_2}{e^2}, \qquad B_3 = \frac{B_1B_2 + mC_1C_2}{e^n}, \qquad C_3 = \frac{B_1C_2 + B_2C_1 + \sigma C_1C_2}{e^n},$$

with e as in (5.2)*.*

Proof. The group law is defined via $\alpha_1\mathbb{N}^n \cdot \alpha_2\mathbb{N}^n = \alpha_3\mathbb{N}^n$, where α_3 is required to be primitive. Equation (5.3) and Lemma 5.1 show that $\alpha_3 = \alpha_1\alpha_2/e^n$. Taking norms yields $A_3^n = A_1^nA_2^n/e^{2n}$, and this proves the claim. ∎

6. From points to forms. Since there is a bijection between ideal classes and equivalence classes of binary quadratic forms, we can also describe the group law in terms of forms. It turns out that the geometric aspect of the description of the group law on $\mathcal{S}_n(\mathbb{Z})$ in terms of forms adds a lot to our understanding of the arithmetic of Pell surfaces and Pell conics. For this reason, we will now construct a map sending primitive points on $\mathcal{S}_n(\mathbb{Z})$ to primitive quadratic forms with discriminant Δ.

Given $(A, B, C) \in \mathcal{S}_n(\mathbb{Z})$, consider the form

$$\widetilde{Q}_P = (A, 2B + \sigma C, A^{n-1}).$$

In order to get positive definite forms if $\Delta < 0$ we now agree to replace $\mathcal{S}_n(\mathbb{Z})$ by $\mathcal{S}_n(\mathbb{Z})^+$ in this case. It is easily checked that $\operatorname{disc} \widetilde{Q}_P = \Delta C^2$; moreover, Dirichlet composition immediately shows that $\widetilde{Q}_P^n$ is the principal form (with discriminant ΔC^2). To construct a form with discriminant Δ, we have to "underive" $\widetilde{Q}_P$. This process replaces a form (a, b, c) with discriminant ΔC^2 by an equivalent form $(a', b'C, c'C^2)$, and then maps it to $Q_P = (a', b', c')$, which is a primitive form with discriminant Δ. Mapping $P \in \mathcal{S}_n(\mathbb{Z})$ to the equivalence class of the form Q_P turns out to be a homomorphism $\mathcal{S}_n(\mathbb{Z}) \to \mathrm{Cl}^+(\Delta)[n]$.

Underiving $\widetilde{Q}_P$ is accomplished by changing the middle coefficient modulo $2A$ in such a way that it becomes a multiple of C. To motivate the following lemma, consider the equation $2B + 2Ak = 2\beta C$; dividing through by 2 and reducing mod A yields $\beta C \equiv B \bmod A$, and this congruence has a unique solution. In this way we find

LEMMA 6.1. *Given a point $P = (A, B, C) \in \mathcal{S}_n(\mathbb{Z})$ with $B^2 - 4AC = \Delta C^2$, let β be an integer satisfying the congruence $\beta \equiv B/C \bmod A$; then $\beta^2 \equiv \Delta \bmod A$. Define a quadratic form $Q_P = (A, 2\beta + \sigma, \gamma)$ with $\gamma = Q_0(\beta, 1)/A$. Then Q_P is a primitive form with discriminant Δ, and Q_P is positive definite if $\Delta < 0$.*

Proof. The claim concerning β follows easily from $\beta^2 \equiv B^2/C^2 \equiv (B^2 - 4AC)/C^2 = \Delta \bmod A$.

Assume now that $\Delta = 4m$, and set $A = (A, 2B, A^{n-1})$. From $\beta \equiv B/C \bmod A$ we see that there is an integer k with $\beta C = B + Ak$. Setting $S = \left(\begin{smallmatrix} 1 & k \\ 0 & 1 \end{smallmatrix}\right)$ we find $Q' = Q|_S = (A, 2B', C')$ with $2B' = 2B + 2Ak = 2\beta C$; the integer C' is determined by $(2B')^2 - 4AC' = \Delta C^2$, which gives $C' = \frac{\beta^2 - m}{A} C^2$. Set $\gamma = (\beta^2 - m)/A$; then the form $Q_1 = (A, 2\beta, \gamma)$ is primitive, has discriminant Δ, and the fact that $A > 0$ implies that Q_1 is positive definite if $\Delta < 0$.

The proof in the case $\Delta = 4m + 1$ is analogous; here we find $\gamma = (\beta^2 + \beta - m)/A$. ∎

Sending $P \mapsto Q_P$ defines a map $b : \mathcal{S}_n(\mathbb{Z}) \to \mathrm{Cl}^+(\Delta)$ between two abelian groups; we already know that the corresponding map to the ideal class group is a homomorphism, and of course the same holds for form classes. We will check the details below; now let us determine the kernel of b. To this end, recall how we constructed b: to a point $(A, B, C) \in \mathcal{S}_n(\mathbb{Z})$ we have attached a quadratic form $\widetilde{Q}_P = (A, 2B + \sigma C, A^{n-1})$ with discriminant ΔC^2; this form $\widetilde{Q}_P$ is equivalent to a form $Q'_P = (A, (2\beta + \sigma)C, \gamma C^2)$, and underiving Q'_P gave us $Q_P = (A, 2\beta + \sigma, \gamma)$.

Now a point $P = (A, B, C) \in \mathcal{S}_n(\mathbb{Z})$ is in the kernel if and only if $Q_P \sim Q_0$, which happens if and only if Q_P represents 1. Multiplying $Q_P(x, y) = 1$ through by C^2 this shows that $Q'_P(Cx, y) = C^2$ (conversely, this equation implies $Q_P(x, y) = 1$). But Q'_P represents C^2 properly if and only if the equivalent form $\widetilde{Q}_P$ does. Thus we have shown

PROPOSITION 6.2. *The kernel of the map $b : \mathcal{S}_n(\mathbb{Z}) \to \mathrm{Cl}^+(\Delta)$ consists of all points $(A, B, C) \in \mathcal{S}_n(\mathbb{Z})$ with the following property: there exist coprime integers T, U such that $AT^2 + (2B + \sigma C)TU + A^{n-1}U^2 = C^2$.*

To decide whether the point $(2, 1, 1)$ on $\mathcal{S}_3 : B^2 + BC + 6C^2 = A^3$ is in the kernel of b we have to look at $2T^2 + 3TU + 4U^2 = 1$. This equation has

solutions if and only if the form $(2,3,4)$ with discriminant -23 represents 1, hence is equivalent to the principal form Q_0. This is not the case, since $(2,3,4) \sim (2,-1,6)$. We may also multiply the original equation through by 8 and complete squares; this gives $(4T+3U)^2+23U^2 = 8$. This equation is clearly unsolvable in integers, but has rational solutions, such as $(T,U) = (0,1/2)$, for example; this implies that we do not have a chance to show the unsolvability of the equation using congruences or p-adic methods.

The map $b : \mathcal{S}_n(\mathbb{Z}) \to \mathrm{Cl}^+(\Delta)$ is a homomorphism. Consider a point $P = (A,B,C)$ on $\mathcal{S}_n(\mathbb{Z})$. We know that $\alpha = B + C\omega = \mathfrak{a}^n$ for some ideal $\mathfrak{a}$ in the maximal order of K. To find the form attached to $\mathfrak{a}$ we have to find an oriented $\mathbb{Z}$-basis $\{A, b+\omega\}$ of $\mathfrak{a}$. Let c be an integer such that $cC \equiv 1 \bmod A$; then $(A, B+C\omega) = (A, cB+cC\omega) = (A, \beta+\omega)$, where β denotes an integer in the residue class $cB \equiv B/C \bmod A$. It is easy to see that $\{A, \beta+\omega\}$ has the desired properties; the form attached to $\mathfrak{a}$ then is

$$Q_{\mathfrak{a}}(x,y) = \frac{N(Ax+(\beta+\omega)y)}{A} = (A, 2\beta+\sigma, \gamma),$$

where $\gamma = N(\beta+\omega)/A = Q_0(\beta,1)/A$. In particular, $Q_{\mathfrak{a}} = Q_P$.

The map sending $\mathfrak{a}$ to $Q_{\mathfrak{a}}$ is known to induce an isomorphism between the ideal class group of $\mathbb{Q}(\sqrt{\Delta}\,)$ and the strict class group of forms with discriminant Δ.

References

[1] R. Bölling, *Über einen Homomorphismus der rationalen Punkte elliptischer Kurven*, Math. Nachr. 96 (1980), 207–244.

[2] D. Buell, *Class groups of quadratic fields*, Math. Comp. 30 (1976), 610–623.

[3] —, *Elliptic curves and class groups of quadratic fields*, J. London Math. Soc. (2) 15 (1977), 19–25.

[4] M. Craig, *A type of class group for imaginary quadratic fields*, Acta Arith. 22 (1973), 449–459.

[5] D. Flath, *Introduction to Number Theory*, Wiley, New York, 1989.

[6] P. Joubert, *Sur la théorie des fonctions elliptiques et son application à la théorie des nombres*, C. R. Acad. Sci. Paris 50 (1860), 774–779.

[7] F. Lemmermeyer, *Kreise und Quadrate modulo p*, Math. Semesterber. 47 (2000), 51–73.

[8] —, *Conics—a poor man's elliptic curves*, arXiv:math/0311306v1, 2003.

[9] —, *Higher descent on Pell conics III. The first 2-descent*, arXiv:math/0311310v1, 2003.

[10] —, *Binary quadratic forms and counterexamples to Hasse's local-global principle*, preprint, 2009.

[11] T. Nagell, *Über die Klassenzahl imaginär-quadratischer Zahlkörper*, Abh. Math. Sem. Hamburg 1 (1922), 140–150.

[12] R. Soleng, *Homomorphisms from the group of rational points on elliptic curves to class groups of quadratic number fields*, J. Number Theory 46 (1994), 214–229.

[13] Y. Yamamoto, *On unramified Galois extensions of quadratic number fields*, Osaka J. Math. 7 (1970), 57–76.

S. Hambleton
Department of Mathematics
The University of Queensland
St. Lucia, Brisbane, Qld., Australia 4072
E-mail: sah@maths.uq.edu.au

F. Lemmermeyer
Mörikeweg 1
73489 Jagstzell, Germany
E-mail: hb3@ix.urz.uni-heidelberg.de

Received on 29.6.2009
and in revised form on 10.7.2010 (6071)