ACTA ARITHMETICA
159.1 (2013)

On congruent primes and class numbers of imaginary quadratic fields

by

Nils Bruin (Burnaby) and Brett Hemenway (Ann Arbor, MI)

1. Introduction. The results in this article are inspired by two related questions:

(1) What exponents can occur for class groups of number fields?
(2) What exponents can occur for Tate–Shafarevich groups of abelian varieties?

In particular, we consider the 2-power part of class groups of imaginary quadratic fields and the 2-power part of the Tate–Shafarevich groups of quadratic twists of the elliptic curve $E_1\colon y^2 = x^3 - x$; these are the curves that play a role in the classical *congruent number problem.*

In either case, it is known that the *size* of the 2-power parts of the groups can be made arbitrarily large by making the 2-torsion subgroups arbitrarily large. For class groups, these results come from Gauss's genus theory (see [Lem00, 2.2]) and for Tate–Shafarevich groups from an analogous construction (see [Kra83]).

We limit ourselves to imaginary quadratic fields $\mathbb{Q}(\sqrt{-p})$, and quadratic twists $E_p\colon y^2 = x^3 - p^2x$, where in either case p is a prime. It is known that there are infinitely many primes p such that the group of classes of fractional ideals modulo principal ideals, $\mathrm{Cl}(\mathbb{Q}(\sqrt{-p}))$, contains elements of order 2, 4, or 8. Existing results establish a similar fact for the Tate–Shafarevich group $Ш(E_p)$ of E_p, namely that there are infinitely many primes p such that $Ш(E_p)[2] \simeq (\mathbb{Z}/2)^2$, and, if one assumes that elliptic curves of rank 2 are extremely rare, that one has $\mathbb{Z}/4 \hookrightarrow Ш(E_p)$ for infinitely many p. The proofs in either case consist in observing that the answer to either question is governed by the splitting of p in some fixed number field. The Chebotarev

2010 *Mathematics Subject Classification*: Primary 11G05; Secondary 11R29.
Key words and phrases: congruent numbers, Tate–Shafarevich groups, class numbers, descent.

DOI: 10.4064/aa159-1-4

Density Theorem then guarantees the existence of infinitely many p with the desired property.

Our results provide a characterization of the primes for which the relevant groups are one step bigger. Unfortunately, the results do not seem to correspond to a splitting condition in some fixed extension anymore, so an infinite number of primes satisfying the criterion is not guaranteed. We introduce some notation to formulate our results precisely.

It follows from genus theory that for $p \equiv 3 \pmod 4$, the class number of $\mathbb{Q}(\sqrt{-p})$ is odd. For $p \equiv 1 \pmod 4$, we write $h(-4p) = \#\operatorname{Cl}(\mathbb{Z}[\sqrt{-p}])$, which is equal to the class number of $\mathbb{Q}(\sqrt{-p})$. In this case genus theory also guarantees that $\operatorname{Cl}(\mathbb{Z}[\sqrt{-p}])/2\operatorname{Cl}(\mathbb{Z}[\sqrt{-p}]) \simeq \mathbb{Z}/2$, so the 2-power part of $\operatorname{Cl}(\mathbb{Z}[\sqrt{-p}])$ is cyclic.

Question A. Given $e \geq 0$, how can we characterize the primes p such that $2^e \mid h(-4p)$?

Note that 2 is ramified in $\mathbb{Q}(\sqrt{-p})$ if $p \equiv 1 \pmod 4$, so there is an ideal $\mathfrak{t} \subset \mathbb{Z}[\sqrt{-p}]$ such that $\mathfrak{t}^2 = 2\mathbb{Z}[\sqrt{-p}]$. Since $\mathbb{Z}[\sqrt{-p}]$ does not contain an element of norm 2, we find that $[\mathfrak{t}] \in \operatorname{Cl}(\mathbb{Z}(\sqrt{-p}))$ is of order 2. Answers to Question A can therefore take the form of descriptions of the sets

$$\begin{aligned} V(e) &= \{p \text{ prime} : p \equiv 1 \pmod 4 \text{ and } 2^e \mid h(-4p)\}, \\ &= \{p \text{ prime} : p \equiv 1 \pmod 4 \text{ and } [\mathfrak{t}] \in 2^{e-1}\operatorname{Cl}(\mathbb{Q}(\sqrt{-p}))\}. \end{aligned}$$

Classical results together with Barrucand–Cohn (see [BC69]) establish (see Section 4 for notation)

$$V(1) = \{p \text{ prime} : p \equiv 1 \pmod 4\}, \tag{1.1a}$$

$$V(2) = \{p \text{ prime} : p \equiv 1 \pmod 8\}, \tag{1.1b}$$

$$V(3) = \left\{p \text{ prime} : p \equiv 1 \pmod 8 \text{ and } \left(\frac{1+i}{p}\right) = 1\right\}. \tag{1.1c}$$

The set $V(3)$ consists exactly of the primes that completely split in $K_1 = \mathbb{Q}(\sqrt{1+i}) = \mathbb{Q}(\alpha)$, where $\alpha^4 - 2\alpha^2 + 2 = 0$. Let $\delta_p \in K_1$ be an algebraic integer satisfying

$$\operatorname{Norm}_{K_1/\mathbb{Q}(i)}(\delta_p) = p$$

and let $\mathfrak{p}_p$ be a prime of K_1 above p such that $\delta_p \notin \mathfrak{p}_p$. We will check that the quadratic symbol $\left(\frac{\alpha\delta_p}{\mathfrak{p}_p}\right)$ does not depend on the actual choices of δ_p and $\mathfrak{p}_p$. We prove

Theorem A.

$$V(4) = \left\{p \textit{ prime} : p \equiv 1 \pmod 8 \textit{ and } \left(\frac{1+i}{p}\right) = \left(\frac{\alpha\delta_p}{\mathfrak{p}_p}\right) = 1\right\}. \tag{1.1d}$$

In [Ste93, Theorem 2], which provides references for (1.1a), (1.1b), (1.1c), there is a different criterion for membership of $V(4)$, in terms of the 2-adic logarithm of the fundamental unit of $\mathbb{Q}(\sqrt{p})$.

For $Ш(E_p)$ we proceed in a way similar to Question A. For an abelian group G we write $G[2^\infty]$ for its 2-primary subgroup.

Question B. Given $e \geq 0$, how can we characterize the primes p such that $Ш(E_p)[2^\infty]$ contains an element of order 2^e?

In classical terminology, a positive integer n is called *congruent* if $E_n(\mathbb{Q})$ has positive rank. In order to avoid confusion with other uses of the word, we italicize it whenever used with this meaning.

It is already known (see Section 6) that if $n = p$ is a prime with $p \not\equiv 1 \pmod 8$ then $Ш(E_p)[2^\infty]$ is trivial. Therefore, we concentrate on the case $p \equiv 1 \pmod 8$. Then either p is *congruent* or $Ш(E_p)[2] \simeq (\mathbb{Z}/2)^2$. In fact, we can write down three principal homogeneous spaces of E_p, given by

$$\begin{aligned} &C_{p,1}\colon y^2 = p(x^4 - 6x^2 + 1) = p(x^2 + 2x - 1)(x^2 - 2x - 1),\\ &C_{p,2}\colon y^2 = p(x^4 + 4) = p(x^2 + 2x + 2)(x^2 - 2x + 2),\\ &C_{p,3}\colon y^2 = p(x^4 + 1), \end{aligned} \tag{1.2}$$

which have points everywhere locally. They represent possibly trivial classes $\xi_1, \xi_2, \xi_3 \in Ш(E_p)[2]$ which generate the group and satisfy $\xi_1 + \xi_2 = \xi_3$. To test the triviality of ξ_i, we are led to considering

$$W(e) = \{p \text{ prime} : p \equiv 1 \pmod 8 \text{ and } \xi_i \in 2^{e-1}Ш(E_p)\}.$$

The *Cassels–Tate pairing* [Cas62] implies that if there exists an $e \geq 1$ such that $\xi_i \notin 2^eШ(E_p)$ (i.e., ξ_i is not totally 2-divisible) then $Ш(E_p)[2] \simeq (\mathbb{Z}/2)^2$. In that case no $C_{p,i}$ has a rational point and p is not *congruent.* It also implies that the definition of $W(e)$ does not depend on which ξ_i is chosen.

For Question A, we know that $[\mathfrak{t}]$ is non-trivial, so divisibility of this class directly yields results on $h(-4p)$. We do not have a corresponding guarantee for Question B. For instance, if all ξ_i are trivial, as happens for $p = 41$, then $p \in W(e)$ for all e but $Ш(E_p)[2^\infty] = 0$. On the other hand, if we establish that $p \in W(e)$ and $p \notin W(e+1)$ then it does follow that ξ_i is non-trivial and we can conclude that 2^e divides the exponent of $Ш(E_p)$.

Results attributed to A. Genocchi and L. Bastien (see [Dic20, Chapter XVI] and [Tun83]) essentially establish

$$W(1) = \{p \text{ prime} : p \equiv 1 \pmod 8\}, \tag{1.3a}$$

$$W(2) = \left\{p \text{ prime} : p \equiv 1 \pmod 8 \text{ and } \left(\frac{1+i}{p}\right) = 1\right\}. \tag{1.3b}$$

In the statement below, we use the same $\delta_p, \mathfrak{p}_p$ as in Theorem A. Furthermore, let ζ be a primitive eighth root of unity. For $p \equiv 1 \pmod 8$, we have that $\zeta \in \mathbb{Q}_p$. We prove

Theorem B.

$$\text{(1.3c)}\quad W(3) = \left\{ p \textit{ prime} : p \equiv 1 \ (\mathrm{mod}\ 8) \textit{ and } \left(\frac{1+i}{p}\right) = \left(\frac{\zeta\alpha\delta_p}{\mathfrak{p}_p}\right) = 1 \right\}.$$

While the criteria in Theorems A and B do not immediately guarantee that there are infinitely many primes satisfying them, the fact that the descriptions do not completely agree allows us to conclude:

Corollary 1.1. *At least one of $W(3)$ and $V(4)$ is infinite.*

Proof. Note that $W(2) = V(3)$ contains infinitely many primes p satisfying $p \equiv 9 \pmod{16}$. For these primes we have $\left(\frac{\zeta}{p}\right) = -1$, which is exactly the symbol by which the descriptions of $V(4)$ and $W(3)$ differ. Therefore we have either $p \in V(4)$ or $p \in W(3)$. It follows that at least one set must be infinite. ■

In Section 2 we derive some more results along these lines. Here let us conclude with noting that the criteria for $W(3)$ and $V(4)$ are easy to test computationally for individual primes.

Remark 1.2. It is easy to compute with a computer algebra system that $10^{200} + 16737$ is the first prime beyond 10^{200} such that $p \in V(3) = W(2)$ but $p \notin V(4), W(3)$, and that $q = 10^{200} + 28729$ is the first such prime with $q \in V(4)$ but $q \notin W(3)$. In particular neither prime is *congruent*.

2. Implications.

Just from equations (1.3a) and (1.3b) it follows that there are infinitely many primes $p \in W(1) \setminus W(2)$. Hence there are infinitely many primes p with $(\mathbb{Z}/2\mathbb{Z})^2 \hookrightarrow Ш(E_p)$.

Note that elliptic curves of rank bigger than 1 seem very rare, so one would expect that for most $p \in W(2)$ it is still the case that at least one ξ_i is non-trivial. Indeed, the discussion in [RS02, Section 7] suggests that the following is plausible.

Assumption 2.1 (Goldfeld for primes). The primes p for which $E_p(\mathbb{Q})$ has rank at least 2 have asymptotic density 0 in the set of all primes.

With this assumption, equation (1.3b) would imply that there are infinitely many p for which $\mathbb{Z}/4 \hookrightarrow Ш(E_p)$. If in addition we assume that only the trivial element in $Ш(E_p)$ is totally divisible, then [DD10, Corollary 4.20] implies that the parity conjecture holds for E_p. This would exclude the possibility that $E_p(\mathbb{Q})$ has rank 1 for $p \equiv 1 \pmod 8$ and we deduce that for infinitely many p we have $(\mathbb{Z}/4)^2 \hookrightarrow Ш(E_p)$.

Numerical data suggest that $V(4)$ has asymptotic density $1/2$ in $V(3)$. Indeed, it has been conjectured [CL83, CL84] that such a density exists, but to our knowledge this conjecture is still open. Comparison of our descriptions of $V(4)$ and $W(3)$ shows that $W(3)$ would have an asymptotic density if and only if $V(4)$ has one. At least one would expect that $V(4)$ and $W(3)$ are both infinite. We can combine Theorems A and B to prove half of that.

Corollary 2.2. *At least one of the following statements is true:*

(a) *There are infinitely many primes p such that $(\mathbb{Z}/4)^2 \hookrightarrow Ш(E_p)$.*
(b) *There are infinitely many primes p such that $16 \mid h(-4p)$.*

Proof. The first statement holds for primes $p \in W(2) \setminus W(3)$, while the second statement holds for primes $p \in V(4)$. The intersections of $V(4)$ and $W(3)$ with $p \equiv 1 \pmod{16}$ coincide. If $V(4)$ were finite then there would be only finitely many primes in $W(3)$ that satisfy $p \equiv 1 \pmod{16}$. Since $W(2)$ contains infinitely many such primes, the corollary follows. ■

Again, using Assumption 2.1 we can obtain a stronger, conditional result.

Corollary 2.3. *Under Assumption* 2.1, *at least one of the following statements is true:*

(a) *There are infinitely many primes p such that $\mathbb{Z}/8 \hookrightarrow Ш(E_p)$.*
(b) *There are infinitely many primes p such that $16 \mid h(-4p)$.*

Proof. The first statement follows if $W(3)$ contains a set of positive asymptotic density in the primes and the second follows if $V(4)$ is infinite. When restricted to primes $p \equiv 9 \pmod{16}$, the two sets are complementary in $V(3) = W(2)$. Hence if $V(4)$ contains only finitely many primes congruent to 9 modulo 16, then $W(3)$ does contain a positive density set. The corollary follows. ■

3. Some related modular results. Observations going back to Gauss (see [Dic23, Chapter VI]) link class numbers to coefficients of modular forms of weight 3/2, in particular the cube of the classical *Jacobi Θ-series.* We write

$$\sum_{n=0}^{\infty} r(n)q^n = \Theta(q)^3 = \Big(\sum_{n=-\infty}^{\infty} q^{n^2}\Big)^3.$$

The class number relation relevant for our problem is that for primes $p \equiv 1 \pmod 4$ we have

$$h(-4p) = \frac{r(p)}{12}.$$

The other coefficients relate to class groups as well. For any particular p one can use this relation, or other methods, to compute $h(-4p)$ and hence decide for which e one has $p \in V(e)$, at least in principle.

For the *congruent number* problem, Tunnell [Tun83] identified a specific modular form

$$\sum a_n q^n \in S_{3/2}(\tilde{\Gamma}_0(128))$$

such that for odd n, $a_n \neq 0$ implies that n is not congruent. He also gives another form for even n. His result relies on Waldspurger's work on the Shimura correspondence and the part of the Birch–Swinnerton-Dyer conjecture (BSD) proved by Coates–Wiles. Tunnell also observes that the full BSD-conjecture implies that for non-congruent primes p we have

$$\#\text{Ш}(E_p) = \tfrac{1}{4}a_p^2.$$

Further, Rubin's work [Rub87] imposes severe restrictions on the values that $\#\text{Ш}(E_p)/a_p^2$ can take, but it does not provide any information on $\operatorname{ord}_2(\#\text{Ш}(E_p)/a_p^2)$. Therefore, even though the analytic approach does provide means to prove that numbers are not *congruent*, it requires unproven parts of BSD to provide any results for Question B.

It is also worth noting that for neither question would analytic approaches be feasible to answer questions for primes in the range of Remark 1.2. This is not too surprising, since the analytic approaches would find the integers $h(-4p)$ (unconditionally) and $\#\text{Ш}(E_p)$ (conditionally), whereas Theorems A and B only provide information on the valuation at 2 of those integers.

4. Preliminaries. When K is a number field, we write $\mathcal{O}_K$ for its ring of integers and $\mathcal{O}_K^\times$ for its group of units. We write $\operatorname{Cl}(K) = \operatorname{Cl}(\mathcal{O}_K)$ for its ideal class group. When S is a finite set of places of K, we write $\mathcal{O}_{K,S}$ for the ring of S-integers.

If $\mathfrak{p} \subset \mathcal{O}_K$ is a prime ideal, we write

$$\left(\frac{\cdot}{\mathfrak{p}}\right) : \mathcal{O}_K/\mathfrak{p} \to \{0, \pm 1\}$$

for the associated quadratic character on the residue field, extended by setting $\left(\frac{0}{\mathfrak{p}}\right) = 0$. When $\mathfrak{p}$ is a principal ideal generated by $\pi \in \mathcal{O}_K$, we write $\left(\frac{\cdot}{\pi}\right) = \left(\frac{\cdot}{\mathfrak{p}}\right)$. For an element $\alpha \in \mathcal{O}_K$ we write $\left(\frac{\alpha}{\mathfrak{p}}\right)$ for the quadratic character of the natural image of α in $\mathcal{O}_K/\mathfrak{p}$. When $\mathfrak{p}$ is completely split over a rational prime p, we denote $\left(\frac{\alpha}{\mathfrak{p}}\right) = \left(\frac{\alpha}{p}\right)$ if the value of the symbol is the same for all $\mathfrak{p}$ dividing $p\mathcal{O}_K$. In this case the symbol can be computed by taking any element $\alpha' \in \mathbb{F}_p$ that is a root of the minimal polynomial of α modulo p and computing the Legendre symbol $\left(\frac{\alpha'}{p}\right)$.

In what follows we need a variety of number fields. We fix notation and names for these fields. Let p be a rational prime. We consider the following extensions:

$$\begin{tikzcd}
& H_2 = \mathbb{Q}(\sqrt{1+i}, \sqrt{p}) \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
K_1 = \mathbb{Q}(\sqrt{1+i}) \arrow[d, dash] & H_1 = \mathbb{Q}(i, \sqrt{p}) \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & L_1 \arrow[d, dash] \\
K_0 = \mathbb{Q}(i) \arrow[dr, dash] & H_0 = \mathbb{Q}(\sqrt{-p}) \arrow[d, dash] & L_0 = \mathbb{Q}(\sqrt{p}) \arrow[dl, dash] \\
& \mathbb{Q} &
\end{tikzcd}$$

If $p \neq 2$ then L_1 can be described as the unique quartic subfield of H_2 that contains $\sqrt{p(1+i)}$.

The choice $p = 2$ plays a special role. We fix separate names M_i for H_i and N_0 for L_0. Note that M_2 is Galois over $\mathbb{Q}$ and that it contains two conjugate subfields isomorphic to K_1. We identify K_1 with one of them. We write N_1 for one of the non-normal quartic subfields containing N_0.

We will conduct some involved computations in M_2 and its subfields. Some of these computations depend on the conjugates chosen. To avoid confusion, we fix a generator β for M_2, satisfying the relation

$$\beta^8 - 4\beta^7 + 12\beta^6 - 20\beta^5 + 24\beta^4 - 20\beta^3 + 12\beta^2 - 4\beta + 1 = 0.$$

We write

$$\begin{aligned}
\beta' &:= \tfrac{1}{7}(\beta^7 + 2\beta^6 + 3\beta^5 + 5\beta^4 + 5\beta^3 + 3\beta^2 + 2\beta + 1),\\
\alpha &:= -9\beta' + 7\beta^6 - 9\beta^5 + 25\beta^4 - 14\beta^3 + 19\beta^2 - 4\beta + 2,\\
\zeta &:= -11\beta' + 9\beta^6 - 12\beta^5 + 33\beta^4 - 18\beta^3 + 23\beta^2 - 5\beta + 3,\\
i &:= \zeta^2 = \alpha^2 - 1,\\
\epsilon &:= -8\beta' + 6\beta^6 - 7\beta^5 + 19\beta^4 - 7\beta^3 + 10\beta^2,\\
\eta &:= \epsilon^3 + \epsilon^2 - \epsilon = \zeta\beta^2,\\
\sqrt{2} &:= \epsilon^2 - 1,
\end{aligned}$$

which fixes embeddings of $K_1 = \mathbb{Q}(\alpha)$ and $N_1 = \mathbb{Q}(\epsilon)$ into M_2. Note that $\mathrm{Aut}(M_2/\mathbb{Q}) = D_4$, the dihedral group of order 8. We denote by σ the involution of M_2 that leaves N_1 fixed and by τ the involution that leaves K_1 fixed. Then $\langle\sigma, \tau\rangle = \mathrm{Aut}(M_2/\mathbb{Q})$, and we write $\rho = (\sigma\tau)^2$ for the central involution of $\mathrm{Aut}(M_2/\mathbb{Q})$ which leaves M_1 fixed. The unit groups of the rings of integers of these fields are $\mathcal{O}_{K_1}^\times = \langle i, \alpha + 1\rangle$, $\mathcal{O}_{N_1}^\times = \langle -1, \epsilon, \eta\rangle$ and $\mathcal{O}_{M_2}^\times = \langle \zeta, \alpha + 1, \epsilon, \beta\rangle$.

We will find use for the following elementary lemmas which have undoubtedly been stated and proved many times, but for which we were unable to locate a reference.

Lemma 4.1. *Let $p \equiv 1 \pmod 8$ be a prime and suppose that $x, y, D \in \mathbb{Z}$ with $p \nmid D$ and*

$$x^2 - Dy^2 = p.$$

Then for $\gamma^2 \equiv D \pmod p$ we have either $x + \gamma y \equiv 0 \pmod p$ or

$$\left(\frac{\gamma(x+\gamma y)}{p}\right) = 1$$

Proof. We thank Soroosh Yazdani for pointing out the following proof. Note that $x^2 - Dy^2 \equiv (x+\gamma y)(x-\gamma y) \equiv 0 \pmod p$, so either $x+\gamma y \equiv 0 \pmod p$ or $x - \gamma y \equiv 0 \pmod p$. The lemma holds in the former case, so we assume the latter. Then

$$x(x+\gamma y) \equiv \gamma y(x+\gamma y) \pmod p \quad \text{and} \quad 2x \equiv (x+\gamma y) \pmod p.$$

It follows that

$$\left(\frac{2\gamma y(x+\gamma y)}{p}\right) = 1.$$

We are left with establishing that $\left(\frac{2y}{p}\right) = 1$. For any prime q dividing y we have $x^2 \equiv p \pmod q$, so $\left(\frac{p}{q}\right) = 1$. Since $p \equiv 1 \pmod 8$, quadratic reciprocity gives us $\left(\frac{q}{p}\right) = 1$ and $\left(\frac{-1}{p}\right) = \left(\frac{2}{p}\right) = 1$, so $2y$ is a product of squares modulo p and therefore a square modulo p itself. ∎

Lemma 4.2. *Let $\pi \in \mathbb{Z}[i]$ be a prime element satisfying $\pi \equiv 1 \pmod{2\mathbb{Z}[i]}$, $\mathrm{Norm}_{\mathbb{Z}[i]/\mathbb{Z}}(\pi) \equiv 1 \pmod 8$ and $\left(\frac{1+i}{\pi}\right) = 1$. Suppose that $x, y, D \in \mathbb{Z}[i]$ with $\pi \nmid D$ and $x^2 - Dy^2 = \pi$. Then for $\gamma^2 \equiv D \pmod p$ we have either $x + \gamma y \equiv 0 \pmod \pi$ or*

$$\left(\frac{\gamma(x+\gamma y)}{\pi}\right) = 1.$$

Proof. Note that quadratic reciprocity for $\mathbb{Z}[i]$ (established by Gauss and Dirichlet [Lem00, Proposition 5.1]) says that if $\pi, \lambda \in \mathbb{Z}[i]$ are distinct prime elements satisfying $\pi, \lambda \equiv 1 \pmod{2\mathbb{Z}[i]}$ then $\left(\frac{\lambda}{\pi}\right) = \left(\frac{\pi}{\lambda}\right)$. We can write $y = i^a(1+i)^b\lambda_1^{e_1}\cdots\lambda_r^{e_2}$, where $\lambda_1, \ldots, \lambda_r \in \mathbb{Z}[i]$ are prime elements satisfying $\lambda_j \equiv 1 \pmod{2\mathbb{Z}[i]}$ (we can ensure this by multiplying by i if necessary). It follows that $\left(\frac{\lambda_j}{\pi}\right) = \left(\frac{\pi}{\lambda_j}\right)$. The conditions in the lemma ensure that $\left(\frac{i}{\pi}\right) = \left(\frac{1+i}{\pi}\right) = 1$. This establishes the required ingredients to complete the proof in the same way as for Lemma 4.1. ∎

5. Class groups as local-global obstructions. There are various ways to prove (1.1b) and (1.1c). The proofs we give here are based on norm-form equations and are in the spirit of Gauss's treatment of genus theory. The lack of reference should not be construed as a claim to priority, but rather as evidence that it is hard to find a reference for such elementary facts. These methods have the great benefit that the techniques readily apply over extensions of the base ring as well. Doing so appears to provide a novel ingredient and allows us to prove something about $V(4)$. First we introduce some terminology and an elementary lemma that links solutions to norm-form equations to divisibility in class groups.

Let R be a principal ideal domain of characteristic different from 2 and let k be its field of fractions. Suppose $d \in R$ is a non-square. Let $L = k(\sqrt{d})$ and let $\mathcal{O}_L \subset L$ be the integral closure of R in L. We write $\mathrm{Cl}(\mathcal{O}_L)$ for the ideal class group of $\mathcal{O}_L$.

Definition 5.1. We say that a pair $(x, y) \in k \times k$ is *$\sqrt{d}$-primitive* if the principal fractional ideal $(x+y\sqrt{d})\mathcal{O}_L$ is integral and is not contained in the extension of any proper ideal from R to $\mathcal{O}_L$, i.e. for all $a \in R$ we have

$$(x + y\sqrt{d})\mathcal{O}_L \subset a\mathcal{O}_L \text{ if and only if } a \text{ is a unit in } R.$$

The definition ensures that for a $\sqrt{d}$-primitive pair (x, y), the principal ideal $(x + y\sqrt{d})\mathcal{O}_L$ is not divisible by any prime ideals that are inert for $\mathcal{O}_L/R$, and that if a split prime $\mathfrak{q}$ divides $(x + y\sqrt{d})\mathcal{O}_L$ then the conjugate prime does not. This means that we can read off the exponents in the ideal factorization of $(x+y\sqrt{d})\mathcal{O}_L$ from its norm $(x^2-dy^2)R$. Since R is a principal ideal domain, this corresponds to the factorization of x^2-dy^2 as an element of R.

Remark 5.2. If $\{1, \sqrt{d}\}$ forms an R-basis of $\mathcal{O}_L$ then a pair (x, y) is $\sqrt{d}$-primitive if and only if $x, y \in R$ and $xR + yR = R$. In particular, if $R = \mathbb{Z}$ and d is squarefree and $d \equiv 3 \pmod 4$ then (x, y) is $\sqrt{d}$-primitive if and only if $x, y \in \mathbb{Z}$ with $\gcd(x, y) = 1$, which is the usual meaning of *primitive.*

Lemma 5.3. *Let R be a principal ideal domain of characteristic different from 2 and with field of fractions k. Let $L = k(\sqrt{d})$ be a quadratic extension of k and let $\mathcal{O}_L$ be the integral closure of R in L. Let $\mathfrak{p} \subset \mathcal{O}_L$ be a prime ideal with norm pR. We have*

$$[\mathfrak{p}] \in n\,\mathrm{Cl}(\mathcal{O}_L)$$

if and only if there is a unit $u \in R^\times$ such that the equation

$$x^2 - dy^2 = upz^n$$

has a solution $x, y, z \in k$ with (x, y) a $\sqrt{d}$-primitive pair.

Proof. First suppose we have a solution with (x, y) a $\sqrt{d}$-primitive pair. We denote the ideal factorization of the principal ideal generated by $x+y\sqrt{d}$ by

$$(x + y\sqrt{d})\mathcal{O}_L = \mathfrak{p}^{e_0} \prod_{i=1}^{r} \mathfrak{q}_i^{e_i}. \tag{5.1}$$

The primitivity condition guarantees that none of the $\mathfrak{p}$ and $\mathfrak{q}_i$ are extensions of ideals in R, so each is either split or ramified. That means that $\mathrm{Norm}(\mathfrak{q}_i) = q_i R$ for some prime element q_i. Furthermore, note that if $\mathfrak{q}_i$ and $\mathfrak{q}_j$ have the same norm, then $\mathfrak{q}_i\mathfrak{q}_j = q_i\mathcal{O}_L$, which would contradict the primitivity of x, y.

Taking norms of both sides of (5.1) we find for some unit $u \in R^\times$ that

$$x^2 - dy^2 = up^{e_0} \prod_{i=1}^{r} q_i^{e_i} = upz^n.$$

Unique factorization gives $e_0 \equiv 1 \pmod{n}$ and $e_i \equiv 0 \pmod{n}$ for $i = 1, \ldots, r$. Since the left hand side of (5.1) is a principal ideal, we get the following identity in $\mathrm{Cl}(\mathcal{O}_L)$:

$$0 = [\mathfrak{p}^{e_0}\mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_r^{e_r}] = [\mathfrak{p}] + [\mathfrak{p}^{e_0-1}\mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_r^{e_r}] = [\mathfrak{p}] + n[\mathfrak{a}],$$

where $\mathfrak{a} = \mathfrak{p}^{(e_0-1)/n}\mathfrak{q}_1^{e_1/n} \cdots \mathfrak{q}_r^{e_r/n}$. This establishes one direction of the proof.

For the converse, let $\mathfrak{a} \subset \mathcal{O}_L$ be an ideal such that $[\mathfrak{p}] = -n[\mathfrak{a}]$. This uses the fact that $\mathcal{O}_L$ is a Dedekind domain, so all ideal classes are represented by integral ideals. In fact, we can represent all ideal classes while avoiding a finite set of primes, so we can assume that $\mathrm{Norm}_{L/k}(\mathfrak{a})$ is not divisible by p. Note that inert ideals are principal and that conjugate primes represent inverse classes, so without loss of generality we have $\mathfrak{a} = \mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_r^{e_r}$, where the $\mathfrak{q}_i$ are split or ramified prime ideals and have distinct norms. Then $\mathfrak{p}\mathfrak{a}^n$ is principal, so $\mathfrak{p}\mathfrak{a}^n = (x+y\sqrt{d})\mathcal{O}_L$, where our assumptions on $\mathfrak{a}$ ensure that (x, y) is a primitive pair. By picking $z \in R$ such that $zR = N(\mathfrak{a})$, we obtain a solution as desired. ∎

Proof of (1.1b). We apply Lemma 5.3 with $k = \mathbb{Q}$, $L = H_0 = \mathbb{Q}(\sqrt{-p})$ and $\mathfrak{p} = \mathfrak{t}$ the ramified prime ideal of $\mathcal{O}_L$ over 2. We have already established that the class of $\mathfrak{t}$ has order 2. We see that $p \in V(2)$ if and only if the equation

$$x^2 + py^2 = 2z^2 \tag{5.2}$$

has a solution such that (x, y) is $\sqrt{-p}$-primitive. A priori, we also need to consider the equation $x^2 + py^2 = -2z^2$ but that obviously does not have primitive solutions.

Since equation (5.2) is homogeneous, any non-zero solution is proportional to a $\sqrt{-p}$-primitive solution. Furthermore, the Hasse–Minkowski theorem guarantees that this equation has a solution if and only if it has solutions everywhere locally.

For solvability at p one needs the fact that 2 is a square modulo p, and for solvability at 2 the fact that p is a square modulo 4. These conditions are met if and only if $p \equiv 1 \pmod 8$. ∎

Proof of (1.1c). Lemma 5.3 gives $p \in V(3)$ if and only if there are $x, y, z \in \mathbb{Z}$ with $\gcd(x, y, z) = 1$ such that

$$x^2 + py^2 = 2z^4.$$

We observe that this implies that x, y are both odd and rewrite this as

$$-py^2 = (x - \sqrt{2}\, z^2)(x + \sqrt{2}\, z^2).$$

Let $N_0 = \mathbb{Q}(\sqrt{2})$. We write τ for conjugation of $N_0/\mathbb{Q}$, so for $\alpha = u + v\sqrt{2}$, we have ${}^\tau\alpha = u - v\sqrt{2}$.

Since obviously $V(3) \subset V(2)$, we can assume that $p \equiv 1 \pmod 8$ by (1.1b). Hence p is split in N_0. Furthermore, since $\mathcal{O}_{N_0}$ is a principal ideal domain and the fundamental unit $\epsilon = 1 + \sqrt{2}$ has norm -1, we have an element $\pi \in \mathcal{O}_{N_0}$ such that $\pi\,{}^\tau\pi = -p$. Primitivity implies that there is a $\gamma \in \mathcal{O}_{N_0}$ with $\gamma \notin \sqrt{2}\,\mathcal{O}_{N_0}$ such that

$$\begin{cases} (x - z^2\sqrt{2}) = \pm\pi\gamma^2, \\ (x + z^2\sqrt{2}) = \pm\,{}^\tau\pi\,{}^\tau\gamma^2. \end{cases}$$

From this equation we derive that

$$\pm 2\sqrt{2}\, z^2 = {}^\tau\pi\,{}^\tau\gamma^2 - \pi\gamma^2. \tag{5.3}$$

Local solvability at 2 forces the sign choice. Local solvability at $\pi\mathcal{O}_L$ implies that

$$\left(\frac{\sqrt{2}\,{}^\tau\pi}{\pi\mathcal{O}_L}\right) = 1. \tag{5.4}$$

Conversely, if we write $\gamma = s + t\sqrt{2}$ and collect coefficients with respect to $\sqrt{2}$ in (5.3) then we get a conic in s, t, z with solutions everywhere locally and hence globally. With some further standard calculations we can also check that we can find a point satisfying the appropriate primitivity conditions.

In order to simplify the symbol above, note that Lemma 4.1 implies that $\left(\frac{\sqrt{2}(1+\sqrt{2})^\tau\pi}{\pi}\right) = 1$. Furthermore, with the right choice of conjugates, one has $(1 + \sqrt{2})(1 + i) = (\zeta^3 - 1)^2$. Together this yields

$$\left(\frac{\sqrt{2}\,{}^\tau\pi}{\pi\mathcal{O}_L}\right) = \left(\frac{1+\sqrt{2}}{p}\right) = \left(\frac{1+i}{p}\right), \tag{5.5}$$

where the fact that $p \equiv 1 \pmod 8$ guarantees that the symbol is independent of choice of conjugate. ∎

Note that in the above two arguments, we obtained a criterion for $p \in V(e)$ for $e = 2, 3$ by reducing the condition in Lemma 5.3 to the existence of a rational point on some conic, which is entirely determined by local conditions. We can handle the two cases above with p as a parameter because the extensions involved in deriving the relevant conics are independent of p. For higher e this does not seem to be the case anymore and this approach does not seem to have much benefit over computing $\mathrm{Cl}(\mathbb{Q}(\sqrt{-p}))$ directly.

The following corollary to a classical result by Dirichlet (1842) allows us to link the class groups of $H_0 = \mathbb{Q}(\sqrt{-p})$ and $H_1 = \mathbb{Q}(\sqrt{p}, i)$. We can then consider H_1 as a quadratic extension of $K_0 = \mathbb{Q}(i)$, whose ring of integers is a principal ideal domain. This allows us to apply Lemma 5.3 to obtain an alternative proof for (1.1c) and derive a new criterion for $p \in V(4)$.

Proposition 5.4 ([Coh78, Corollary 19.8c]). *Let $p > 0$ be a prime, let $h' = \#\,\mathrm{Cl}(\mathbb{Q}(\sqrt{p}))$, let $h_0 = \#\,\mathrm{Cl}(\mathbb{Q}(\sqrt{-p}))$ and let $h_1 = \#\,\mathrm{Cl}(\mathbb{Q}(i, \sqrt{-p}))$. Then*

$$h_1 = \begin{cases} \frac{1}{2} h_0 h' & \text{if } p \equiv 1 \pmod 4, \\ h_0 h' & \text{if } p \equiv 3 \pmod 4 \text{ or } p = 2. \end{cases}$$

For a prime satisfying $p \equiv 1 \pmod 8$ we observe that h' is odd by Gauss's genus theory. Note that 2 ramifies in $K_0 = \mathbb{Q}(i)$ and splits in $L_0 = \mathbb{Q}(\sqrt{p})$. That means that H_1 has two primes $\mathfrak{t}_1, \mathfrak{t}_2$ over 2, each of ramification index 2. Furthermore, since h' is odd, we see that $[\mathfrak{t}_1^2]$ and $[\mathfrak{t}_2^2]$ have odd order in the class group.

Extension of ideals from $\mathcal{O}_{H_0}$ to $\mathcal{O}_{H_1}$ gives a homomorphism

$$\mathrm{Cl}(H_0)[2^\infty] \to \mathrm{Cl}(H_1)[2^\infty]$$

and it is easy to check that the kernel is of order 2. In view of Proposition 5.4 this means that the map is surjective and thence that $\mathrm{Cl}(H_1)[2^\infty]$ is cyclic. The last fact also follows from applying genus theory to the relative extension H_1/L_0.

Lemma 5.5. *Let $p \equiv 1 \pmod 8$ be a rational prime and let $e \geq 2$. We have $p \in V(e)$ if and only if the equation*

$$x^2 + py^2 = (1+i)z^{2^{e-2}} \tag{5.6}$$

has a solution $x, y, z \in \mathbb{Q}(i)$ with

$$(x - iy)\mathbb{Z}[i] + 2y\mathbb{Z}[i] = \mathbb{Z}[i].$$

Proof. Lemma 5.3 with $(L, R, \mathfrak{p}, d, p)$ taken to be $(H_1, \mathbb{Z}[i], \mathfrak{t}_1, p, 1+i)$ (a shift in symbols used seems unavoidable here) links the equation in the lemma to the question whether $[\mathfrak{t}_1] \in 2^{e-2}\,\mathrm{Cl}(H_1)$ and hence whether $p \in V(e)$. For $x \in \mathbb{Q}(i)$ we write ${}^\sigma x$ for its conjugate over $\mathbb{Q}$. Note that if (x, y) gives rise to a solution then $({}^\sigma x, {}^\sigma y), (ix, iy), ({}^\sigma(ix), {}^\sigma(iy))$ give rise to solutions to $x^2 + py^2 = u(1+i)z^{2^{e-2}}$ where $u = i, -1, -i$. Therefore, the choice of the unit u in Lemma 5.3 does not affect solvability of the equation.

Note that $\{1, \frac{1}{2}(\sqrt{-p}+i)\}$ is a $\mathbb{Z}[i]$-basis of $\mathcal{O}_{H_1}$. Therefore, (x,y) is a $\sqrt{-p}$-primitive pair in $\mathbb{Z}[i]$ if

$$x + y\sqrt{-p} = u + v\frac{\sqrt{-p}+i}{2},$$

with $u, v \in \mathbb{Z}[i]$ and $\gcd(u,v) = 1$. That corresponds to the condition given in the lemma. ■

Alternative proof of (1.1c). Since $V(3) \subset V(2)$, we can assume that $p \in V(2)$ and hence that $p \equiv 1 \pmod 8$. Lemma 5.5 implies that a necessary condition for $p \in V(3)$ is that

$$\left(\frac{i+1}{p}\right) = 1$$

for both choices of i, because otherwise the conic given by (5.6) does not even have local points at a place above p. However, note that

$$\left(\frac{1+i}{p}\right)\left(\frac{1-i}{p}\right) = \left(\frac{2}{p}\right) = 1$$

because $p \equiv 1 \pmod 8$. Hence, the symbol does not depend on the choice of i. Furthermore, we can check that at $(1+i)\mathbb{Z}[i]$ there is no local obstruction to primitive solutions. The Hasse–Minkowski theorem once again guarantees the existence of rational solutions, and the homogeneity of the equation allows us to derive primitive solutions from that. Therefore, the condition is also sufficient. ■

Proof of Theorem A. Let us assume that $p \in V(3)$. By Lemma 5.5 we deduce that $p \in V(4)$ if and only if we have a solution $x, y, z \in \mathbb{Q}(i)$ to

$$-py^2 = x^2 - (1+i)z^4$$

satisfying the additional conditions stated. We adopt the notation from Section 4 and factor this equation over K_1 to obtain

$$\begin{cases} x + z^2\alpha = \delta\xi_1^2, \\ x - z^2\alpha = {}^{\rho}\delta\,{}^{\rho}\xi_1^2, \end{cases}$$

for some δ representing a class in $K_1^\times/(K_1^{\times 2})$ such that $N_{K_1/K_0}(\delta) \in -pK_0^{\times 2}$. Our primitivity condition together with the fact that 2 is completely ramified in K_1 implies that δ can be represented by an algebraic integer that is a unit outside the primes above p.

Our conditions on p ensure that p is completely split in K_1. Let $u, v \in \mathbb{Z}$ be such that $p = u^2 + v^2$ and suppose that $\pi_1, \ldots, \pi_4 \in \mathcal{O}_{K_1}$ are such that $\mathrm{Norm}_{K_1/\mathbb{Q}}(\pi_i) = p$ and $\pi_1\pi_2 = u + iv$ and $\pi_3\pi_4 = u - iv$. The unit group of $\mathcal{O}_{K_1}$ is generated by $\{i, 1+\alpha\}$. Since $\mathrm{Norm}_{K_1/\mathbb{Q}(i)}(1+\alpha) = -1$ is not a square, the possible values for δ are

$$\pi_1\pi_3,\ \pi_1\pi_4,\ \pi_2\pi_3,\ \pi_2\pi_4,\ i\pi_1\pi_3,\ i\pi_1\pi_4,\ i\pi_2\pi_3,\ i\pi_2\pi_4.$$

A necessary condition for $p \in V(4)$ is that

$$2z^2\alpha = \delta\xi_1^2 - {}^{\rho}\delta\, {}^{\rho}\xi_1^2 \tag{5.7}$$

has solutions everywhere locally. Noting that i is a square modulo p, we see that there must be $j, k \in \{1, \ldots, 4\}$ with $\{j, k\} \neq \{1, 2\}, \{3, 4\}$ such that for all l we have

$$\left(\frac{\pi_j\pi_k\alpha}{\pi_l}\right) \neq -1.$$

However, note that Lemma 4.1 yields identities such as

$$\left(\frac{\pi_1\pi_2}{\pi_3}\right) = \left(\frac{u+iv}{\pi_3}\right) = \left(\frac{i}{\pi_3}\right) = 1,$$

which allow us to deduce that the value does not depend on the actual choices of j, k, l as long as $l \notin \{j, k\}$. Note that ${}^{\rho}\delta\delta$ is a square locally at the prime above 2, so we do not get any local obstructions there either. Therefore, the condition in the theorem is sufficient for (5.7) to have points everywhere locally and hence globally. Checking that these points also give rise to primitive solutions is routine. ∎

6. Congruent numbers: the first step.

All classical results on congruent primes can be obtained via straightforward 2-(isogeny) descent on either E_p or one of its 2-isogenous curves. See for instance [Hem06]. We only state the parts that are important for our subsequent analysis:

(i) If $p \equiv 3 \pmod 8$ then $\mathrm{rk}\, E_p(\mathbb{Q}) = 0$ and $\text{Ш}(E_p/\mathbb{Q})[2] = 0$.

(ii) If $p \equiv 5, 7 \pmod 8$ then $\mathrm{rk}\, E_p(\mathbb{Q}) \leq 1$. In fact, Monsky [Mon90], based on Heegner [Hee52], establishes equality and hence $\text{Ш}(E_p/\mathbb{Q})[2] = 0$.

(iii) If $p \equiv 1 \pmod 8$ then $\mathrm{rk}\, E_p(\mathbb{Q}) \leq 2$.

In the last case, $p \equiv 1 \pmod 8$, some further work shows that the homogeneous spaces from (1.2) are everywhere locally solvable and that rational points on them would give rise to independent points on E_p. We analyze when this can be the case for $C_{p,1}$ and $C_{p,2}$.

Lemma 6.1. *Let $p \equiv 1 \pmod 8$ be a prime. Then $C_{p,1}$ has a rational point if and only if the following curve has one:*

$$D_{p,1}\colon v^2 = p(u^4 - 4u^3 - 6u^2 - 12u - 7).$$

Furthermore, $D_{p,1}$ has points everywhere locally if and only if $\left(\frac{1+i}{p}\right) = 1$.

Proof. For any rational point on $C_{p,1}$ there exists a value δ (determined up to squares) such that the point lifts to

$$D_{p,1}\colon \begin{cases} w^2 = \delta(x^2+2x-1), \\ v^2 = \dfrac{p}{\delta}(x^2-2x-1). \end{cases}$$

With some elementary resultant computation, one can show that it is sufficient to consider $\delta \in \{\pm 1, \pm 2, \pm p, \pm 2p\}$, and a straightforward local computation shows that for $\delta \in \{\pm 2, \pm 2p\}$ the curve does not have $\mathbb{Q}_2$-points.

Furthermore, the automorphisms of $C_{p,1}$ corresponding to $x \mapsto 1/x$ and $x \mapsto -x$ show that the remaining values for δ all lead to isomorphic curves, so it is sufficient to consider $\delta = 1$.

We parametrize the first conic by $(x,w) = \bigl(\frac{u^2+1}{2(u+1)}, \frac{u^2+2u-1}{2(u+1)}\bigr)$. Substituting this parametrization into the second conic yields the given model of $D_{p,1}$.

Note that since $p \equiv 1 \pmod 8$, the local solvability of $D_{p,1}$ over $\mathbb{Q}_2$ does not depend on p. Similarly, because $p > 0$, the local solvability over $\mathbb{R}$ does not depend on p either. Given that $D_{p,1}$ has good reduction at all other primes, the only obstruction to local solvability can be at p. Note that if $(u_0, v_0) \in D_{p,1}(\mathbb{Q}_p)$ then we need that $\operatorname{ord}_p(u_0^4 - 4u_0^3 - 6u_0^2 - 12u_0 - 7)$ is odd. For this we need that the quartic has a root in $\mathbb{Q}_p$. Note that

$$u^4 - 4u^3 - 6u^2 - 12u - 7 = (u^2 - 2(1+\sqrt{2})u - 1 - \sqrt{2})(u^2 - 2(1-\sqrt{2})u - 1 + \sqrt{2})$$

and that the quadratics on the right hand side have discriminants $16(1 \pm \sqrt{2})$. Furthermore, since $p \equiv 1 \pmod 8$ we have $\sqrt{2} \in \mathbb{Q}_p$, so $D_{p,1}(\mathbb{Q}_p)$ is nonempty if and only if

$$\left(\frac{1+\sqrt{2}}{p}\right) = \left(\frac{1+i}{p}\right) = 1;$$

see (5.5) for the reason why the first equality holds. ■

Lemma 6.2. *Let $p \equiv 1 \pmod 8$ be a prime. Then $C_{p,2}$ has a rational point if and only if the following curve has one:*

$$D_{p,2}\colon v^2 = p(u^4 - 4u^3 + 24u + 20).$$

Furthermore, the curve $D_{p,2}$ has points everywhere locally if and only if $\bigl(\frac{i+1}{p}\bigr) = 1$.

Proof. A rational point on $C_{p,2}$ lifts, for some δ, to

$$D_{p,2}\colon \begin{cases} w^2 = \delta(x^2-2x+2), \\ v^2 = \dfrac{p}{\delta}(x^2+2x+2). \end{cases}$$

The first conic only has real solutions if $\delta > 0$, and with an elementary resultant computation one can show it is sufficient to consider $\delta \in \{1, p, 2, 2p\}$. Furthermore, the automorphisms of C_p corresponding to $x \mapsto 1/x$ and

$x \mapsto -x$ show that all choices lead to isomorphic curves, so it is sufficient to consider $\delta = 1$.

We parametrize the first conic by $(x,w) = \left(\frac{2-u^2}{2u+2}, \frac{u^2+2u+2}{2u+2}\right)$. Substitution into the second yields the given model of $D_{p,2}$.

For $p \equiv 1 \pmod 8$, the curve $D_{p,2}$ has points at all primes outside p. For a point $(u_0, v_0) \in D_{p,2}(\mathbb{Q}_p)$ we need $\operatorname{ord}_p(u_0^4 - 4u_0^3 + 24u_0 + 20)$ to be odd, so the quartic should have a root in $\mathbb{Q}_p$. Note that

$$u^4 - 4u^3 + 24u + 20 = (u^2 - (2-2i)u - 4 + 2i)(u^2 - (2+2i)u - 4 - 2i)$$

and that the discriminants of the quadrics on the left hand side are, respectively, $(1+i)^9$ and $-i(1+i)^9$. The statement in the lemma follows by considering when these are squares in $\mathbb{Q}_p$. ∎

Either of Lemmas 6.1 and 6.2 establishes that primes $p \equiv 1 \pmod 8$ for which $\left(\frac{1+i}{p}\right) = -1$ are *not* congruent. This result is already mentioned in [Bas15] and [Tun83]. In order to interpret these results in terms of Question B, we briefly review the relations between isogenies and Tate–Shafarevich groups in the next section.

7. Sha and isogenies. In this section, we review the conditions under which we can conclude the existence of 2^e-torsion in $Ш(E)$ by exhibiting 2^{e-1}-torsion in $Ш(E')$ for an appropriate 2-isogenous elliptic curve E'. We use part of the proof that the truth of the Birch and Swinnerton-Dyer conjecture is constant in isogeny classes (see [Cas65] or [Mil06, I.7]).

Let E be an elliptic curve over a number field k and let $\phi\colon E \to E'$ be an isogeny. Since elliptic curves are self-dual, we can interpret the isogeny dual to ϕ as $\phi^\vee\colon E' \to E$. Suppose that $m = \deg(\phi)$. Then the multiplication-by-m homomorphism on E factorizes as $m = \phi^\vee \circ \phi$.

Note that elements of $Ш(E)$ are represented by principal homogeneous spaces C, so they have a free transitive E-action. We can use this together with an isogeny $\phi : E \to E'$ to induce a homomorphism

$$\phi\colon Ш(E) \to Ш(E'), \qquad C \mapsto C/\ker(\phi).$$

We write $Ш(E)[\phi]$ for its kernel.

For any abelian group A we define its *divisible subgroup* to be

$$A_{\text{div}} := \{a \in A : a \in mA \text{ for all } m = 1, 2, \ldots\}$$

and write $A_{\text{nd}} := A/A_{\text{div}}$. General results from descent show that the p-primary parts of $Ш(E)_{\text{nd}}$ are all finite.

The Cassels–Tate pairing yields non-degenerate, alternating pairings

$$\begin{tikzcd}
Ш(E)_{\mathrm{nd}} \arrow[d, "\phi"] & \times & Ш(E)_{\mathrm{nd}} \arrow[r] & \mathbb{Q}/\mathbb{Z} \\
Ш(E')_{\mathrm{nd}} & \times & Ш(E')_{\mathrm{nd}} \arrow[u, "\phi^\vee"'] \arrow[r] & \mathbb{Q}/\mathbb{Z}
\end{tikzcd}$$

with the diagram commuting in the sense that

$$\langle \phi\xi, \xi' \rangle_{E'} = \langle \xi, \phi^\vee \xi' \rangle_E.$$

In particular, the pairing induces an alternating, non-degenerate pairing

$$Ш(E')_{\mathrm{nd}}[\phi^\vee] \times Ш(E')_{\mathrm{nd}}/\phi Ш(E)_{\mathrm{nd}} \to \mathbb{Q}/\mathbb{Z}. \tag{7.1}$$

LEMMA 7.1. *Let $\phi : E \to E'$ be a p-isogeny between elliptic curves over a number field k. Suppose that $Ш(E')[\phi^\vee] = 0$. Let $\xi \in Ш(E)[p]$ and let $\xi' \in Ш(E')[p]$ be such that $\phi^\vee(\xi') = \xi$. Then*

$$\xi' \in p^{e-1}Ш(E') \quad \textit{implies that} \quad \xi \in p^e Ш(E).$$

More generally, if $Ш(E')$ has elements of order p^e then $Ш(E)$ has elements of order p^{e+1}.

Proof. Note that the first statement in the lemma is trivially true if $\xi' = 0$, or more generally, if ξ' is divisible. Let us assume that $\xi'' \in Ш(E')$ is such that $\xi' = p^{e-1}\xi''$. From the pairing (7.1) we see that $Ш(E')[\phi^\vee] = 0$ implies that $\phi\colon Ш(E) \to Ш(E')$ is surjective, so there is a $\xi''' \in Ш(E)$ such that $\phi(\xi''') = \xi''$. It follows that

$$\xi = \phi^\vee \circ p^{e-1} \circ \phi \xi''' = p^e \xi''',$$

which gives the statement in the lemma.

For the general observation, let $\xi'' \in Ш(E')$ be an element of order p^e, let $\xi' = p^{e-1}\xi''$ and let $\xi = \phi^\vee \xi'$. Then ξ is an element of order p that is divisible by p^e. This proves the statement. ■

8. Results from isogeny descents. The curves $D_{p,i}$ arising in Lemmas 6.1 and 6.2 are principal homogeneous spaces for the elliptic curves

$$E_{p,1}\colon y^2 = x^3 + 4p^2x, \quad E_{p,2}\colon y^2 = x^3 + 6px^2 + p^2x$$

respectively. There are 2-isogenies $\phi_i\colon E_p \to E_{p,i}$.

Proof of (1.3b). The following discussion holds for $i = 1$ or $i = 2$. We do not give details here (see [Sil86, Proposition X.4.9]), but a 2-isogeny descent on the pair $(E_p, E_{p,i})$ for a prime $p \equiv 1 \pmod 8$ implies that $\operatorname{rk} E_p(\mathbb{Q}) \le 2$ as expected and that $Ш(E_{p,i})[\phi_i^\vee] = 0$ (the homogeneous spaces found there correspond to the 2-torsion of E_p). It is perhaps worth noting that for the third 2-isogenous curve $E_{p,3} : y^2 = x^3 - px^2 + p^2x$, this is *not* the case.

As established before, the curve $C_{p,i}$ represents a class ξ_i in $Ш(E)[2]$. Note that since $2 = \phi_{p,i}^\vee \circ \phi_{p,i}$, divisibility of ξ_i by 2 implies that there is an everywhere locally solvable homogeneous space of $E_{p,i}$ that covers $C_{p,i}$. Lemma 6.1 or 6.2 shows that this must be $D_{p,i}$, so if $\left(\frac{1+i}{p}\right) = -1$ then ξ_i is not divisible by 2 and $Ш(E_p)[2^\infty] = (\mathbb{Z}/2\mathbb{Z})^2$ and $p \in W(1) \setminus W(2)$.

If $\left(\frac{1+i}{p}\right) = 1$ then the class ξ' of $D_{p,i}$ in $Ш(E_{p,i})$ satisfies $\phi_i^\vee(\xi') = \xi_i$, so ξ_i is indeed divisible by 2, so $p \in W(2)$. ∎

On the other hand, if $\left(\frac{1+i}{p}\right) = 1$ then Lemma 7.1 implies that ξ_i is divisible by 2. If we can find conditions on p such that the class of $D_{p,i}$ is not divisible by 2 in $Ш(E_{p,i})$ then we classify when ξ_i is divisible by 2 but not by 4 and hence when p is not congruent and $Ш(E_p)[2^\infty] = (\mathbb{Z}/4\mathbb{Z})^2$.

The reason to concentrate on $D_{p,1}$ and $D_{p,2}$ is that we can write down nice quartic models for them without using any properties of p. Other homogeneous spaces would arise in a similar way, but the conic that requires parametrization in order to arrive at a quartic model may only be parametrizable if certain arithmetic conditions on p are taken into account, i.e., that it is a prime $p \equiv 1 \pmod 8$. We will see in the next section how the nice models of $D_{p,1}$ and $D_{p,2}$ allow us to make one further step.

9. Second descents.

Let p be a prime satisfying $p \equiv 1 \pmod 8$ and $\left(\frac{1+i}{p}\right) = 1$. In this section, we perform a second descent on the curves $D_{p,1}$ and $D_{p,2}$ to determine if their classes are divisible by 2 in $Ш(E_{p,1})$ and $Ш(E_{p,2})$. For any particular p, this is a completely standard procedure which can be executed automatically by several computer algebra systems. We give some details here because we do the calculation for an unspecified p, which is not completely automated.

We quickly review the parts of the method we have to refer to explicitly. The method we use is largely as suggested in [MSS96]. However, we neglect to explicitly construct the coverings. See also [BS09].

We consider the smooth projective curve corresponding to the affine model

$$D\colon y^2 = f(x)$$

where $f(x)$ is a square-free quartic polynomial over a field k of characteristic 0. If the leading coefficient of $f(x)$ is a square in k then D has k-rational points P with $x(P) = \infty$. We denote these points by ∞^+ and ∞^-, where the ± superscript provides an arbitrary but fixed label.

The curve D is a homogeneous space of an elliptic curve E, and invariant theory of binary quartic forms provides a degree 4 map $D \to E$, equipping D with a torsor structure under $E[2]$ with base E. If k is a number field and D has points everywhere locally then D represents a class in $Ш(E)[2]$.

Let

$$L = k[\theta] = k[x]/(f(x)).$$

We consider the map

$$\begin{aligned} \mu_k\colon \quad D(k) &\to L^\times/L^{\times 2}k^\times, \\ (x_0,y_0) &\mapsto x_0-\theta \quad \text{ if } y_0 \neq 0, \\ (x_0,0) &\mapsto (x_0-\theta) + \left.\frac{f(x)}{(x-x_0)}\right|_{x=\theta}, \\ P &\mapsto 1 \quad \text{if } P = \infty^{\pm}. \end{aligned}$$

For $k=\mathbb{Q}$ and a place v of k we write $L_v = L\otimes\mathbb{Q}_v$ and consider the natural map $\rho_v : L^\times/L^{\times 2}\mathbb{Q} \to L_v^\times/L_v^{\times 2}\mathbb{Q}_v^\times$. We define

$$\mathrm{Sel}^2_{\text{fake}}(D/\mathbb{Q}) = \{c \in L^\times/L^{\times 2}k^\times : \rho_v(c) \in \operatorname{im}\mu_{k_v} \text{ for all places } v\}.$$

We observe that the class of D is divisible by 2 in $Ш(E)$ if and only if $\mathrm{Sel}^2_{\text{fake}}(D/\mathbb{Q})$ is non-empty.

Let S be the set of places of k containing 2, the places at infinity, the places where coefficients of f are not integral and the places where $\operatorname{disc}(f)$ is not a unit. We write $\mathcal{O}_{L,S}$ for the subring of L of elements that are integral at all places v outside S.

In our cases, L is a number field where $\mathcal{O}_{L,S}$ has class number 1. In those cases, $\mathrm{Sel}^2_{\text{fake}}(D/\mathbb{Q})$ can be represented by elements in the finitely generated multiplicative group $\mathcal{O}_{L,S}^\times$. Furthermore, for such elements δ we only have to check some norm conditions and that $\rho_v(\delta) \in \operatorname{im}\mu_{k_v}$ for the places $v \in S$ in order to conclude that $\delta \in \mathrm{Sel}^2_{\text{fake}}(D/\mathbb{Q})$.

Finally, if $f(x)$ has a root in k_v then $\#\operatorname{im}\mu_{k_v} = \#\frac{E[2](k_v)}{|2|_v}$, and if $f(x)$ has no root in k_v then $\#\operatorname{im}\mu_{k_v} = \frac{\#E[2](k_v)}{2|2|_v}$.

We use the notation for K_0, K_1 and their elements as introduced in Section 4.

Proposition 9.1. *Let* $p \equiv 1 \pmod 8$ *be a prime satisfying* $\left(\frac{1+i}{p}\right)=1$. *Let* $\delta=\delta_p \in K_1 = \mathbb{Q}(\sqrt{1+i})$ *be an algebraic integer such that* $\mathrm{Norm}_{K_1/\mathbb{Q}(i)}(\delta) = p$ *and* $\mathfrak{p}$ *is a prime ideal above* p *such that* $\delta \notin \mathfrak{p}$. *Then the following are equivalent:*

(i) *The class of* $D_{p,1}$ *in* $Ш(E_{p,1})$ *is divisible by* 2.
(ii) *The class of* $D_{p,2}$ *in* $Ш(E_{p,2})$ *is divisible by* 2.
(iii) $\left(\dfrac{\delta\zeta\sqrt{1+i}}{\mathfrak{p}}\right) = 1.$

Proof. (i)⇔(iii). We compute $\mathrm{Sel}^2_{\text{fake}}(D_{p,1})$ as sketched above. We have $f(x) = p(x^4-4x^3-6x^2-12x-7)$ and $L = N_1$.

We can take $S = \{2, p, \infty\}$. Since 2 and p are completely ramified and split respectively, we have four prime ideals $\mathfrak{p}_1, \dots, \mathfrak{p}_4$ of $\mathcal{O}_{N_1}$ above p. We choose generators for them in the following way. Let $\pi \in \mathcal{O}_{M_2}$ be a generator of a prime ideal of $\mathcal{O}_{M_2}$ above p. Since $\mathcal{O}_{M_2}^\times$ surjects onto $(\mathcal{O}_{M_1}/2\mathcal{O}_{M_1})^\times$, we can assume that $\pi \equiv 1 \pmod{2\mathcal{O}_{M_1}}$. We define

$$\pi_1 = \pi\, {}^{\sigma}\pi, \qquad \pi_2 = {}^{\rho}\pi\, {}^{\sigma\rho}\pi, \qquad \pi_3 = {}^{\tau}\pi\, {}^{\sigma\tau}\pi, \qquad \pi_4 = {}^{\tau\sigma}\pi\, {}^{\sigma\tau\sigma}\pi$$

and write $\mathfrak{p}_i = \pi_i \mathcal{O}_{N_1}$. Let $\iota : M_2 \to \mathbb{Q}_p$ be the completion corresponding to $\pi\mathcal{O}_{M_2}$. We identify M_2 with its image under ι. The completions $\iota_1, \dots, \iota_4 : N_1 \to \mathbb{Q}_p$ with respect to $\mathfrak{p}_i$ are induced by $\iota, \iota\rho, \iota\tau\sigma, \iota\sigma\tau$ respectively.

From $\mathrm{Norm}_{N_1/\mathbb{Q}}(\epsilon + 1) = -2$ we know that

$$\mathcal{O}_{L,S}^\times = \langle -1, \epsilon, \eta, \epsilon + 1, \pi_1, \dots, \pi_4 \rangle.$$

Furthermore, $\pi_2\pi_3\pi_4 = p/\pi_1$, so π_1 and $\pi_2\pi_3\pi_4$ represent the same class in $\mathcal{O}_{L,S}^\times / \mathcal{O}_{L,S}^{\times 2}\mathbb{Q}^\times$. It is straightforward to check that classes in $\mathrm{Sel}^2_{\mathrm{fake}}(D_{p,1})$ must be represented by S-integers that have norm in $p\mathbb{Q}^{\times 2}$. This means that a full set of representatives for $\mathrm{Sel}^2_{\mathrm{fake}}(D_{p,1})$ can be found in

$$\{\pi_i, \eta\pi_i : i = 1, \dots, 4\}. \tag{9.1}$$

Note that p is a square at 2, so $\mathrm{im}\,\mu_{\mathbb{Q}_2}$ is independent of p. We see that $f(x)$ is irreducible over $\mathbb{Q}_2$ and that $\#E_{p,1}[2](\mathbb{Q}_2) = 2$, so $\#\,\mathrm{im}\,\mu_{\mathbb{Q}_2} = 2$. We compute that

$$\ker\left(N\colon \frac{L_2^\times}{L_2^{\times 2}\mathbb{Q}_2^\times} \to \frac{\mathbb{Q}_2^\times}{\mathbb{Q}_2^{\times 2}}\right) \simeq (\mathbb{Z}/2\mathbb{Z})^2$$

and that the images of $(0, \sqrt{-7p}), \infty^+ \in D_{p,1}(\mathbb{Q}_2)$ form $\mathrm{im}\,\mu_{\mathbb{Q}_2}$. We find that it can be represented by $\{1, \epsilon^2\} + 2\mathcal{O}_{N_1}$. Our earlier normalization ensures that $\pi_i \equiv 1 \pmod{2\mathcal{O}_{N_1}}$ and computation shows that $\eta \not\equiv \epsilon^2 \pmod{2\mathcal{O}_{N_1}}$, so from (9.1) only $\{\pi_1, \dots, \pi_4\}$ maps to $\mathrm{im}\,\mu_{\mathbb{Q}_2}$.

Let $\theta = \epsilon^2 - 2\epsilon$ be a root of $f(x)$ in N_1. We know that $f(x)$ splits completely over $\mathbb{Q}_p$. Let $\theta_1 = \iota_1\theta, \dots, \theta_4 = \iota_4\theta$ be the roots of $f(x)$ in $\mathbb{Q}_p$. We fix $L \to L_p \simeq (\mathbb{Q}_p)^4$ by $x \mapsto (\iota_1 x, \dots, \iota_4 x)$.

We have $\#E_{p,1}[2](\mathbb{Q}_p) = 4$. It is straightforward to check that $\mathrm{im}\,\mu_{\mathbb{Q}_p}$ is represented by $\{(\theta_1, 0), \dots, (\theta_4, 0)\}$, which in L_p gives

$$\begin{aligned}
&(p(\theta_1-\theta_2)(\theta_1-\theta_3)(\theta_1-\theta_4), (\theta_1-\theta_2), (\theta_1-\theta_3), (\theta_1-\theta_4)),\\
&((\theta_2-\theta_1), p(\theta_2-\theta_1)(\theta_2-\theta_3)(\theta_2-\theta_4), (\theta_2-\theta_3), (\theta_2-\theta_4)),\\
&((\theta_3-\theta_1), (\theta_3-\theta_2), p(\theta_3-\theta_1)(\theta_3-\theta_2)(\theta_3-\theta_4), (\theta_3-\theta_4)),\\
&((\theta_4-\theta_1), (\theta_4-\theta_2), (\theta_4-\theta_3), p(\theta_4-\theta_1)(\theta_4-\theta_2)(\theta_4-\theta_3)).
\end{aligned} \tag{9.2}$$

If π_1 represents a class in $\mathrm{Sel}^2_{\mathrm{fake}}(D_{p,1})$, then based on valuations, π_1 and the first element listed in (9.2) must represent the same class modulo $L_p^{\times 2}\mathbb{Q}_p^\times$. That means that

$$\left(\frac{{}^{\rho}\pi_1\, {}^{\tau\sigma}\pi_1\, {}^{\sigma\tau}\pi_1(\theta_1-\theta_2)(\theta_1-\theta_3)(\theta_1-\theta_4)}{\pi}\right) = \left(\frac{{}^{\rho}\pi_1(\theta_1-\theta_2)}{\pi}\right)$$
$$= \left(\frac{{}^{\tau\sigma}\pi_1(\theta_1-\theta_3)}{\pi}\right) = \left(\frac{{}^{\sigma\tau}\pi_1(\theta_1-\theta_4)}{\pi}\right).$$

We notice that the first and last equalities lead to

$$\left(\frac{{}^{\tau}\pi\, {}^{\tau\sigma}\pi\, {}^{\sigma\tau}\pi\, {}^{\sigma\tau\sigma}\pi(\theta_1-\theta_3)(\theta_1-\theta_4)}{\pi}\right) = \left(\frac{\mathrm{Norm}_{M_2/N_0}({}^{\tau}\pi)\sqrt{2}}{\pi}\right) = 1,$$

which always holds by Lemma 4.1. By equating the second and the last symbol we obtain

$$\left(\frac{{}^{\rho}\pi\, {}^{\rho\sigma}\pi\, {}^{\sigma\tau}\pi\, {}^{\sigma\tau\sigma}\pi(\theta_1-\theta_2)(\theta_1-\theta_4)}{\pi}\right) = \left(\frac{\mathrm{Norm}_{M_2/K_1}({}^{\rho}\pi\, {}^{\sigma\tau}\pi)\zeta\alpha}{\pi}\right).$$

It is straightforward to check that $\delta = \mathrm{Norm}_{M_2/K_1}({}^{\rho}\pi\, {}^{\sigma\tau}\pi)$ satisfies the definition set out in the proposition, so this establishes that π_1 represents an element in $\mathrm{Sel}^2_{\mathrm{fake}}(D_{p,1})$ if and only if p satisfies condition (iii). The same conclusion holds for the other π_i by symmetry.

(ii)⇔(iii). We follow the strategy used for the first equivalence. We choose $\pi \in \mathcal{O}_{M_2}$ in the same way and consider

$$\pi_1 = \pi\, {}^{\tau}\pi, \qquad \pi_2 = {}^{\rho}\pi\, {}^{\tau\rho}\pi, \qquad \pi_3 = {}^{\sigma}\pi\, {}^{\tau\sigma}\pi, \qquad \pi_4 = {}^{\sigma\tau}\pi\, {}^{\tau\sigma\tau}\pi.$$

The four prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_4$ of $\mathcal{O}_{K_1}$ above p are generated by the π_i above, and the completions $K_1 \to \mathbb{Q}_p$ with respect to $\mathfrak{p}_i$ are induced by the same embeddings $\iota, \iota\rho, \iota\tau\sigma, \iota\sigma\tau$ as before.

We have $f(x) = p(x^4 - 4x^3 + 24x + 20)$ and $L = K_1$ and $\theta = \alpha^2 - 2\alpha$. We can take $S = \{2, p, \infty\}$ and we have

$$\mathcal{O}_{K_1,S}^\times = \langle i, \alpha+1, \alpha, \pi_1, \ldots, \pi_4\rangle.$$

Note that $i = \alpha^4/2 \in K_1^{\times 2}\mathbb{Q}^\times$, so for representing $\mathrm{Sel}^2_{\mathrm{fake}}(D_{p,2})$ we can ignore multiplication by i. Norm considerations show that a full set of representatives can be taken from the set

$$\{\pi_1, \ldots, \pi_4, (\alpha+1)\pi_1, \ldots, (\alpha+1)\pi_4\}.$$

A computation as before shows that the images of $\infty^+, (1, \sqrt{41p}) \in D(\mathbb{Q}_2)$ form $\operatorname{im}\mu_{\mathbb{Q}_2}$, represented by $\{1, i\} + 2\mathcal{O}_{N_1}$. Since $\alpha+1 \not\equiv i \pmod{2\mathcal{O}_{K_1}}$, we find that $\mathrm{Sel}^2_{\mathrm{fake}}(D_{p,2})$ can be represented by elements from $\{\pi_1, \ldots, \pi_4\}$.

By setting $\theta_j = \iota_j\theta$ we see that $\operatorname{im}\mu_{\mathbb{Q}_p}$ is represented by the same formulas (9.2). Based on valuations, π_1 can only represent the element corresponding to the first element there. For π_1 to represent the same class in $L_p^{\times 2}/\mathbb{Q}_p^\times$, we need that

$$\left(\frac{{}^{\rho}\pi_1\,{}^{\tau\sigma}\pi_1\,{}^{\sigma\tau}\pi_1(\theta_1-\theta_2)(\theta_1-\theta_3)(\theta_1-\theta_4)}{\pi}\right)$$
$$=\left(\frac{{}^{\rho}\pi_1(\theta_1-\theta_2)}{\pi}\right)=\left(\frac{{}^{\tau\sigma}\pi_1(\theta_1-\theta_3)}{\pi}\right)=\left(\frac{{}^{\sigma\tau}\pi_1(\theta_1-\theta_4)}{\pi}\right).$$

The first and last equalities, together with $(\theta_1-\theta_3)(\theta_1-\theta_4)$ being a square, yield

$$\left(\frac{{}^{\tau\sigma}\pi\,{}^{\tau\sigma\tau}\pi\,{}^{\sigma\tau}\pi\,{}^{\sigma}\pi(\theta_1-\theta_3)(\theta_1-\theta_4)}{\pi}\right)=\left(\frac{\mathrm{Norm}_{M_2/K_0}({}^{\sigma}\pi)}{\pi}\right)=1,$$

which holds by Lemma 4.1. Equating the second and the fourth term yields

$$\left(\frac{{}^{\rho}\pi\,{}^{\sigma\tau\sigma}\pi\,{}^{\sigma}\pi\,{}^{\sigma\tau}\pi\zeta\alpha}{\pi}\right)=1. \tag{9.3}$$

From Lemma 4.2 with $D=i$ and $\gamma=\zeta$ we obtain

$$\left(\frac{{}^{\tau}\pi\,{}^{\sigma\tau\sigma}\pi}{\pi}\right)=\left(\frac{\mathrm{Norm}_{M_2/M_1}({}^{\tau}\pi)}{\pi}\right)=\left(\frac{\zeta}{\pi}\right).$$

Another application of Lemma 4.1 gives

$$\left(\frac{{}^{\sigma\tau}\pi\,{}^{\tau}\pi\,{}^{\tau\sigma}\pi\,{}^{\sigma\tau\sigma}\pi}{\pi}\right)=\left(\frac{\mathrm{Norm}_{M_2/N_0}({}^{\tau}\pi)}{\pi}\right)=\left(\frac{\sqrt{2}}{\pi}\right)=\left(\frac{\zeta}{\pi}\right).$$

Multiplying these with (9.3) shows that it is equivalent to

$$\left(\frac{{}^{\rho}\pi\,{}^{\sigma\tau\sigma}\pi\,{}^{\sigma}\pi\,{}^{\tau\sigma}\pi\zeta\alpha}{\pi}\right)=1,$$

which is the condition stated in the proposition. Conditions for the other π_i follow by symmetry. ∎

Proof of Theorem B. We assume $p \in W(2)$. With Lemma 7.1 and the results of Section 8 we have established that $[C_{p,i}] \in 4Ш(E_p)$ if and only if $D_{p,i} \in 2Ш(E_{p,i})$. This is exactly what either of the equivalences (i)⇔(iii) and (ii)⇔(iii) in Proposition 9.1 establishes. ∎

10. Comparison of the methods. This section gives an informal comparison of the methods of proof of Theorems A and B. They share some important characteristics and naturally the question arises to what extent a framework can be constructed in which both are applications of the same principle. A full answer is beyond the scope of this article (see for instance [CTX09]) but we do sketch why Theorem A is *not* directly related to an isogeny.

Both questions can be interpreted in terms of local-global obstructions to rational or integral points on principal homogeneous spaces under algebraic groups. The congruent number problem is directly formulated in this language. We have the homogeneous spaces $C_{p,i}$ and $D_{p,i}$ under E_p and $E_{p,i}$ respectively. In our case, for non-*congruent* primes $p \equiv 1 \pmod 8$ and assuming that $Ш(E_p)$ is finite, Lemma 7.1 yields $\#Ш(E_p) = 4\#Ш(E_{p,i})$, which means that analysis of the 2- and 4-torsion in $\#Ш(E_{p,i})$ allows us to obtain information about 4- and 8-torsion in $Ш(E_p)$. There is a long history of exploiting isogenies to obtain information about $Ш(E)$ for elliptic curves E; see [Kra83].

For the class number problem, we consider integer points on $C\colon x^2 + py^2 = 2$. The affine scheme described by this equation is a principal homogeneous space under the algebraic group scheme T that describes the kernel of the norm map $\mathrm{Norm}\colon \mathbb{Q}(\sqrt{-p})^\times \to \mathbb{Q}^\times$. The fact that C has integer points everywhere locally follows from the fact that there is an ideal $\mathfrak{t}$ of norm 2, and the fact that C does not have global integer points follows from the fact that $\mathfrak{t}$ is not a principal ideal.

The fundamental step that allows us to prove Theorem A is to base extend to $\mathbb{Z}[i]$. Here C does acquire an integer point and we are led to consider essentially the homogeneous space $D\colon x^2 + py^2 = 1 + i$ under $T' = T \times_{\mathbb{Z}} \mathbb{Z}[i]$ instead (noting that at $1 + i$, the modified notion of primitivity actually describes a slightly different space than the model given here). Proposition 5.4 allows us to relate the information back to the quantities we are originally interested in.

Note that in the latter case, the two algebraic group schemes T and T' are *not* isogenous. They are not even defined over the same base. For elliptic curves one can also use base extensions to kill part of Ш; see for instance [Kra81]. This leads to particular instances of *Mazur visibility* [CM00]. See [Bru04] for an explicit description of these ideas regarding $Ш(E)[2]$ for elliptic curves E.

We searched for a proof of Theorem B based on visibility but were unable to find an appropriate base extension or auxiliary elliptic curve that would work for all relevant p.

Acknowledgements. We would like to thank Peter Stevenhagen for pointing out the similarities between the results for congruent numbers and those for imaginary quadratic class groups. Furthermore, we thank Soroosh Yazdani for useful discussions about Lemma 4.1, Tom Archibald for discussions about the history of the subject, Jeffrey Lagarias for useful comments and Alexa van der Waall for general discussions and suggestions.

Research of the first author is supported by NSERC.

References

[BC69] P. Barrucand and H. Cohn, *Note on primes of type $x^2 + 32y^2$, class number, and residuacity*, J. Reine Angew. Math. 238 (1969), 67–70.

[Bas15] L. Bastien, *Nombres congruents*, Intermédiaire des Math. 22 (1915), 231–232.

[Bru04] N. Bruin, *Visualising* Sha[2] *in Abelian surfaces*, Math. Comp. 73 (2004), 1459–1476.

[BS09] N. Bruin and M. Stoll, *Two-cover descent on hyperelliptic curves*, Math. Comp. 78 (2009), 2347–2370.

[Cas62] J. W. S. Cassels, *Arithmetic on curves of genus 1. IV. Proof of the Hauptvermutung*, J. Reine Angew. Math. 211 (1962), 95–112.

[Cas65] J. W. S. Cassels, *Arithmetic on curves of genus 1. VIII. On conjectures of Birch and Swinnerton-Dyer*, J. Reine Angew. Math. 217 (1965), 180–199.

[Coh78] H. Cohn, *A Classical Invitation to Algebraic Numbers and Class Fields*, Springer, New York, 1978.

[CL83] H. Cohn and J. C. Lagarias, *On the existence of fields governing the 2-invariants of the classgroup of* $\mathbf{Q}(\sqrt{dp})$ *as p varies*, Math. Comp. 41 (1983), 711–730.

[CL84] H. Cohn and J. C. Lagarias, *Is there a density for the set of primes p such that the class number of* $\mathbf{Q}(\sqrt{-p})$ *is divisible by 16?*, in: Topics in Classical Number Theory, Budapest, 1981, Vol. I, Colloq. Math. Soc. János Bolyai 34, North-Holland, Amsterdam, 1984, 257–280.

[CTX09] J.-L. Colliot-Thélène and F. Xu, *Brauer–Manin obstruction for integral points of homogeneous spaces and representation by integral quadratic forms*, Compos. Math. 145 (2009), 309–363.

[CM00] J. E. Cremona and B. Mazur, *Visualizing elements in the Shafarevich–Tate group*, Experiment. Math. 9 (2000), 13–28.

[Dic20] L. Dickson and E. Leonard, *History of the Theory of Numbers. Vol. II: Diophantine Analysis*, Carnegie Institution of Washington, Washington, DC, 1920.

[Dic23] L. Dickson and E. Leonard, *History of the Theory of Numbers. Vol. III: Quadratic and Higher Forms*, Carnegie Institution of Washington, Washington, DC, 1923.

[DD10] T. Dokchitser and V. Dokchitser, *On the Birch–Swinnerton-Dyer quotients modulo squares*, Ann. of Math. (2) 172 (2010), 567–596.

[Hee52] K. Heegner, *Diophantische Analysis und Modulfunktionen*, Math. Z. 56 (1952), 227–253.

[Hem06] B. Hemenway, *On recognizing congruent primes*, M.Sc. thesis, Simon Fraser Univ., 2006; http://ir.lib.sfu.ca/handle/1892/3791.

[Kra81] K. Kramer, *Arithmetic of elliptic curves upon quadratic extension*, Trans. Amer. Math. Soc. 264 (1981), 121–135.

[Kra83] K. Kramer, *A family of semistable elliptic curves with large Tate–Shafarevitch groups*, Proc. Amer. Math. Soc. 89 (1983), 379–386.

[Lem00] F. Lemmermeyer, *Reciprocity Laws, From Euler to Eisenstein*, Springer Monogr. Math., Springer, Berlin, 2000.

[MSS96] J. R. Merriman, S. Siksek and N. P. Smart, *Explicit 4-descents on an elliptic curve*, Acta Arith. 77 (1996), 385–404.

[Mil06] J. S. Milne, *Arithmetic Duality Theorems*, 2nd ed., BookSurge, Charleston, SC, 2006.

[Mon90] P. Monsky, *Mock Heegner points and congruent numbers*, Math. Z. 204 (1990), 45–67.

[Rub87] K. Rubin, *Tate–Shafarevich groups and L-functions of elliptic curves with complex multiplication*, Invent. Math. 89 (1987), 527–559.

[RS02] K. Rubin and A. Silverberg, *Ranks of elliptic curves*, Bull. Amer. Math. Soc. (N.S.) 39 (2002), 455–474.

[Sil86] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Grad. Texts in Math. 106, Springer, New York, 1986.

[Ste93] P. Stevenhagen, *Divisibility by 2-powers of certain quadratic class numbers*, J. Number Theory 43 (1993), 1–19.

[Tun83] J. B. Tunnell, *A classical Diophantine problem and modular forms of weight* 3/2, Invent. Math. 72 (1983), 323–334.

Nils Bruin
Department of Mathematics
Simon Fraser University
Burnaby, BC V5A 1S6, Canada
E-mail: nbruin@sfu.ca
http://www.cecm.sfu.ca/˜nbruin

Brett Hemenway
Department of Mathematics
University of Michigan
Ann Arbor, MI 48109-1043, U.S.A.

Received on 22.7.2012
and in revised form on 14.12.2012 (7135)