ACTA ARITHMETICA
137.2 (2009)

Two conjectures by Zhi-Hong Sun

by

Constantin N. Beli (Bucureşti)

Let ε be an algebraic integer in $\mathbb{Q}(\sqrt{d})$, where $d > 1$ is square-free, and let $p > 2$ be a prime with $p \nmid d$ and $p \nmid \mathrm{N}(\varepsilon)$, where $\mathrm{N} : \mathbb{Q}(\sqrt{d}) \to \mathbb{Q}$ is the norm map. It is well known that $\varepsilon^{p-1} \equiv 1 \pmod p$ if $p \equiv 1 \pmod 4$ and $\varepsilon^{p+1} \equiv \mathrm{N}(\varepsilon) \pmod p$ if $p \equiv 3 \pmod 4$.

The next problem is to find $\varepsilon^{(p\pm1)/2} \bmod p$. If $\left(\frac{d}{p}\right) = \left(\frac{\mathrm{N}(\varepsilon)}{p}\right) = 1$ then $\left(\frac{\varepsilon}{p}\right)$ is defined and we have $\varepsilon^{(p-1)/2} \equiv \left(\frac{\varepsilon}{p}\right) \pmod p$ so the problem is equivalent to finding the Legendre symbol $\left(\frac{\varepsilon}{p}\right)$. A particular case with a long history is when $\varepsilon = \varepsilon_d$, the fundamental unit of $\mathbb{Q}(\sqrt{d})$ and $\mathrm{N}(\varepsilon_d) = -1$. The problem of finding $\left(\frac{\varepsilon_d}{p}\right)$ when $\mathrm{N}(\varepsilon_d) = -1$ for primes p with $\left(\frac{-1}{p}\right) = \left(\frac{d}{p}\right) = 1$ was first considered in 1942, when Aigner and Reichardt showed that if $p \equiv 1 \pmod 8$ then $\varepsilon_2 = 1 + \sqrt{2}$ is a quadratic residue modulo p if and only if $p = x^2 + 32y^2$ for some $x, y \in \mathbb{Z}$. Various mathematicians have obtained similar results for other fundamental units ε_d of norm -1. The problem was finally settled by Z. H. Sun [S1], who determined the value of $\varepsilon^{(p-(-1/p))/2} \bmod p$, where ε is an arbitrary integer in $\mathbb{Q}(\sqrt{d})$, in the case when $\left(\frac{-d}{p}\right) = 1$. Sun's result, just as the results obtained before him, is given in terms of x, y satisfying $f(x, y) = p$, where $f = AX^2 + 2BXY + CY^2$ is a quadratic form with $\det f = B^2 - AC = -k^2 d$ and k is a (bounded) positive integer. The fact that p can be represented by one of these quadratic forms is ensured by the fact that $\left(\frac{-d}{p}\right) = 1$.

The next level of difficulty is to calculate $\varepsilon^{(p-(-1/p))/4} \bmod p$, again when $\left(\frac{-d}{p}\right) = 1$. In this paper we restrict ourselves to the case when $p \equiv 3 \pmod 4$, i.e. $\left(\frac{-1}{p}\right) = \left(\frac{d}{p}\right) = -1$, and we determine $\varepsilon^{(p+1)/4} \bmod p$. We solve two conjectures by Z. H. Sun regarding the value of $\varepsilon_5^{(p+1)/4} \bmod p$, where $\varepsilon_5 = (1 + \sqrt{5})/2$, for $p \equiv 3, 7 \pmod{20}$, and the value of $\varepsilon_3^{(p+1)/8} \bmod p$, where $\varepsilon_3 = 2 + \sqrt{3}$, for $p \equiv 7 \pmod{24}$. Apparently the second conjec-

2000 *Mathematics Subject Classification*: 11B50, 11R37, 11A15, 11B39.
Key words and phrases: Fibonacci and Lucas numbers, congruences, class field theory.

DOI: 10.4064/aa137-2-1

ture is one level of difficulty up because of the denominator 8. However, if we note that $2+\sqrt{3} = (1+\sqrt{3})^2/2$ then the problem reduces to finding $(1+\sqrt{3})^{(p+1)/4} \bmod p$.

The conjecture regarding $(2+\sqrt{3})^{(p+1)/8}$ is related to a problem involving the sequence S_k given by $S_1 = 4$, $S_{k+1} = S_k^2 - 2$, from the Lucas–Lehmer test, which is mentioned in [G, A3]. If $M_p = 2^p - 1$ is a Mersenne prime then $p \mid S_{p-1} = S_{p-2}^2 - 2$ so $S_{p-2}^2 \equiv 2 \equiv 2^{p+1} \pmod{2^p-1}$, so $S_{p-2} \equiv \pm 2^{(p+1)/2} \pmod{M_p}$. The problem is to determine the $\pm$ sign. We have $S_k = (2+\sqrt{3})^{2^{k-1}} + (2-\sqrt{3})^{2^{k-1}} = 2V_{2^{k-1}}$, where V_n is given by the formula $V_n + U_n\sqrt{3} = (2+\sqrt{3})^n$. Therefore we want to know the $\pm$ sign for which $2V_{(M_p+1)/8} = 2V_{2^{p-3}} = S_{p-2} \equiv \pm 2^{(p+1)/2} \pmod{M_p}$. Since $M_p \equiv 7 \pmod 8$ we have $\left(\frac{-1}{M_p}\right) = -1$ and $\left(\frac{2}{M_p}\right) = 1$. Thus the $\pm$ sign equals $\left(\frac{S_{p-2}}{M_p}\right) = \left(\frac{V_{(M_p+1)/8}}{M_p}\right)$. Sun's conjecture gives the quadratic residues mod p for both $V_{(p+1)/8}$ and $U_{(p+1)/8}$ for any $p \equiv 7 \pmod{24}$ and it allows us to determine $(2+\sqrt{3})^{(p+1)/8} \bmod p$. As a consequence, our $\pm$ sign is $(-1)^{(x^2-4)/32}$, where $M_p = x^2 + 3y^2$ with $x, y \in \mathbb{Z}$.

The methods we use are from class field theory. Given a number field F and a (possibly archimedian) prime $\mathfrak{p}$ of F, for any $x \in F$ we denote by $x_\mathfrak{p}$ its image in $F_\mathfrak{p}$. When there is no danger of confusion we simply write x instead of $x_\mathfrak{p}$. If E/F is a finite abelian extension and $\mathfrak{P}$ is a prime of E lying over $\mathfrak{p}$ then we denote by $\left(\frac{\cdot, E/F}{\mathfrak{p}}\right) : F_\mathfrak{p}^\times \to \mathrm{Gal}(E/F)$ the Artin map and by $(\cdot, E_\mathfrak{P}/F_\mathfrak{p}) : F_\mathfrak{p}^\times \to \mathrm{Gal}(E_\mathfrak{P}/F_\mathfrak{p})$ the local Artin map. If we identify $\mathrm{Gal}(E_\mathfrak{P}/F_\mathfrak{p})$ with its image in $\mathrm{Gal}(E/F)$ then $\left(\frac{a, E/F}{\mathfrak{p}}\right) = (a, E_\mathfrak{P}/F_\mathfrak{p})$ for any $a \in F_\mathfrak{p}^\times$.

1. $F_{(p+1)/4}$ and $L_{(p+1)/4} \bmod p$ for $p \equiv 3, 7 \pmod{20}$. Let F_n, L_n be the Fibonacci and Lucas sequences given by $F_0 = 0$, $F_1 = 1$ and $F_{n+1} = F_{n-1} + F_n$ and by $L_0 = 2$, $L_1 = 1$ and $L_{n+1} = L_{n-1} + L_n$. We have

$$\frac{L_n + F_n\sqrt{5}}{2} = \left(\frac{1+\sqrt{5}}{2}\right)^n.$$

In [S1, Conjecture 5.2] Z. H. Sun proposed the following conjecture:

Conjecture 1.1 (Z. H. Sun, 2003). *If $p \equiv 3, 7 \pmod{20}$ is a prime with $2p = x^2 + 5y^2$ for some integers x, y then*

$$F_{(p+1)/4} \equiv \begin{cases} 2(-1)^{[(p-5)/10]} 10^{(p-3)/4} \pmod p & \text{if } y \equiv \pm(p-1)/2 \pmod 8, \\ -2(-1)^{[(p-5)/10]} 10^{(p-3)/4} \pmod p & \text{if } y \not\equiv \pm(p-1)/2 \pmod 8. \end{cases}$$

By [SS, Corollary 2(iii)] we have

$$F_{(p+1)/4} L_{(p+1)/4} = F_{(p+1)/2} \equiv 2(-1)^{[(p-5)/10]} 5^{(p-3)/4} \pmod p.$$

Therefore the conjecture above is equivalent to:

$$L_{(p+1)/4} \equiv \begin{cases} (-2)^{(p+1)/4} \pmod p & \text{if } y \equiv \pm(p-1)/2 \pmod 8, \\ -(-2)^{(p+1)/4} \pmod p & \text{if } y \not\equiv \pm(p-1)/2 \pmod 8. \end{cases}$$

We have $p \equiv 3 \pmod 4$ and $p \equiv 2, 3 \pmod 5$ so $\left(\frac{-1}{p}\right) = \left(\frac{5}{p}\right) = -1$.

1.2. Since $(L_n + F_n\sqrt{5})/2 = \varepsilon^n$, where $\varepsilon := (1+\sqrt{5})/2$, we have to evaluate $\varepsilon^{(p+1)/4} \bmod p$. We have $\left(\frac{5}{p}\right) = -1$ so p is inert in $\mathbb{Q}(\sqrt{5})$. Since $p \nmid \varepsilon$ the conjugate of ε, $\overline{\varepsilon} := (1-\sqrt{5})/2$, is given by the Frobenius automorphism $\overline{\varepsilon} = \Phi_p(\varepsilon) \equiv \varepsilon^p \pmod p$. Thus $\varepsilon^{p+1} \equiv \varepsilon\overline{\varepsilon} = -1 \pmod p$.

Note that $(p-1)/2$ is odd so

$$\left(p+1, \frac{p^2-1}{8}\right) = \frac{p+1}{4}\left(4, \frac{p-1}{2}\right) = \frac{p+1}{4}.$$

Thus if we also know $\varepsilon^{(p^2-1)/8} \bmod p$ then we know $\varepsilon^{(p+1)/4} \bmod p$. More precisely, if $p \equiv 3 \pmod 8$ then

$$\frac{p+1}{4} = \frac{p^2-1}{8} - (p+1)\cdot\frac{p-3}{8}$$

so

$$\varepsilon^{(p+1)/4} = \varepsilon^{(p^2-1)/8}(\varepsilon^{p+1})^{-(p-3)/8} \equiv (-1)^{(p-3)/8}\varepsilon^{(p^2-1)/8} \pmod p,$$

while if $p \equiv 7 \pmod 8$ then

$$\frac{p+1}{4} = -\frac{p^2-1}{8} + (p+1)\cdot\frac{p+1}{8}$$

so

$$\varepsilon^{(p+1)/4} = \varepsilon^{-(p^2-1)/8}(\varepsilon^{p+1})^{(p+1)/8} \equiv (-1)^{(p+1)/8}\varepsilon^{-(p^2-1)/8} \pmod p.$$

We will obtain $\varepsilon^{(p^2-1)/8} \bmod p$ in terms of some Hilbert symbol of order 8. To do this we will construct a cyclic extension of order 8 of $F := \mathbb{Q}(\sqrt{5})$.

Since $\left(\frac{-1}{p}\right) = -1$ we have either $\left(\frac{2}{p}\right) = 1$ (if $p \equiv 7 \pmod 8$) or $\left(\frac{-2}{p}\right) = 1$ (if $p \equiv 3 \pmod 8$). This implies that we can write $2p = u^2 - 2v^2$ if $p \equiv 7 \pmod 8$ or $2p = u^2 + 2v^2$ if $p \equiv 3 \pmod 8$.

Let $F = \mathbb{Q}(\sqrt{5})$ and $E = F(\zeta) = F(i, \sqrt{2})$, where $\zeta := \zeta_8 = (1+i)/\sqrt{2}$. Note that the morphisms $\zeta \mapsto \zeta^k$ with $k \in \mathbb{Z}_8^\times$ behave as follows: $\zeta \mapsto \zeta$ is the identity; $\zeta \mapsto \zeta^3$ is given by $i \mapsto -i$ and $\sqrt{2} \mapsto -\sqrt{2}$; $\zeta \mapsto \zeta^5$ is given by $i \mapsto i$ and $\sqrt{2} \mapsto -\sqrt{2}$; $\zeta \mapsto \zeta^7$ is given by $i \mapsto -i$ and $\sqrt{2} \mapsto \sqrt{2}$.

Define $A_1 \in E$ by

$$A_1 = \begin{cases} 2p(x + y\sqrt{5}\,i)^2(u + v\sqrt{2}\,i)^4 & \text{if } p \equiv 3 \pmod 8, \\ 2p(x + y\sqrt{5}\,i)^6(u + v\sqrt{2})^4 & \text{if } p \equiv 7 \pmod 8. \end{cases}$$

Note that $\sqrt{2p} \notin E = \mathbb{Q}(i, \sqrt{5}, \sqrt{2})$ so A_1 is not a square in E. For $k \in \mathbb{Z}_8^\times$ we denote by A_k the image of A_1 under the automorphism $\zeta \mapsto \zeta^k$ from $\mathrm{Gal}(E/F)$.

Let $L = E(\sqrt[8]{A_1})$. Since $\mu_8 \subset E$ and A_1 is not a square in E we have $\mathrm{Gal}(L/E) = \langle\sigma\rangle \cong \mathbb{Z}_8$, where $\sigma \in \mathrm{Gal}(L/E)$ is given by $\sqrt[8]{A_1} \mapsto \zeta \sqrt[8]{A_1}$.

LEMMA 1.3. *The extension L/F is Galois and* $\mathrm{Gal}(L/F) \cong \mathbb{Z}_8^\times \times \mathbb{Z}_8$.

Proof. First we prove that L/F is normal. Define $\alpha_1 = \sqrt[8]{A_1}$. Let $\overline{F}$ be some algebraic closure of F containing L and let $\alpha \in \overline{F}$ be some conjugate of α_1 over F. Then α^8 is a conjugate of $\alpha_1^8 = A_1$ over F so it is of the form A_k with $k \in \mathbb{Z}_8^\times$. We show that for any $k \in \mathbb{Z}_8^\times$, $k \neq 1$, we have $A_k = \alpha_k^8$, where

$$\alpha_3 = \begin{cases} \alpha_1^3(x + y\sqrt{5}\,i)^{-1}(u + v\sqrt{2}\,i)^{-1} & \text{if } p \equiv 3 \pmod 8, \\ \alpha_1^3 \cdot 2p(x + y\sqrt{5}\,i)^{-3}(u + v\sqrt{2})^{-2} & \text{if } p \equiv 7 \pmod 8, \end{cases}$$

$$\alpha_5 = \begin{cases} \alpha_1^5(x + y\sqrt{5}\,i)^{-1}(u + v\sqrt{2}\,i)^{-3} & \text{if } p \equiv 3 \pmod 8, \\ \alpha_1^5(x + y\sqrt{5}\,i)^{-3}(u + v\sqrt{2})^{-3} & \text{if } p \equiv 7 \pmod 8, \end{cases}$$

$$\alpha_7 = \begin{cases} 2p\alpha_1^{-1} = \alpha_1^7(x + y\sqrt{5}\,i)^{-2}(u + v\sqrt{2}\,i)^{-4} & \text{if } p \equiv 3 \pmod 8, \\ 2p(u + v\sqrt{2})\alpha_1^{-1} = \alpha_1^7(x + y\sqrt{5}\,i)^{-6}(u + v\sqrt{2})^{-3} & \text{if } p \equiv 7 \pmod 8. \end{cases}$$

The proof is straightforward and it uses the relations $\alpha_1^8 = A_1$, $2p = (x+y\sqrt{5}\,i)(x-y\sqrt{5}\,i)$ and $2p = (u+v\sqrt{2}\,i)(u-v\sqrt{2}\,i)$ or $(u+v\sqrt{2})(u-v\sqrt{2})$, corresponding to $p \equiv 3 \pmod 8$ or $p \equiv 7 \pmod 8$, respectively, and also the way the morphisms $\zeta \mapsto \zeta^k$ from $\mathrm{Gal}(E/F)$ act on $\sqrt{2}$ and i. For illustration we give the argument for α_5 when $p \equiv 3 \pmod 8$. Since the morphism $\zeta \mapsto \zeta^5$ is given by $i \mapsto i$ and $\sqrt{2} \mapsto -\sqrt{2}$ we have

$$\begin{aligned} A_5 &= 2p(x + y\sqrt{5}\,i)^2(u - v\sqrt{2}\,i)^4 = (2p)^5(x + y\sqrt{5}\,i)^2(u + v\sqrt{2}\,i)^{-4} \\ &= A_1^5(x + y\sqrt{5}\,i)^{-8}(u + v\sqrt{2}\,i)^{-24} = \alpha_3^8, \end{aligned}$$

where $\alpha_5 = \alpha_1^5(x + y\sqrt{5}\,i)^{-1}(u + v\sqrt{2}\,i)^{-3}$.

In all cases we have $\alpha^8 = A_k = \alpha_k^8$ for some $\alpha_k \in L$, with $k \in \mathbb{Z}_8^\times$. Therefore $\alpha = \zeta^l\alpha_k$ for some l so $\alpha \in L$. So the 32 conjugates of α_1 over F are $\zeta^l\alpha_k$ with $k \in \mathbb{Z}_8^\times$ and $l \in \mathbb{Z}_8$.

Let $\phi \in \mathrm{Gal}(L/F)$. Then $\phi_{|E}$ is of the form $\zeta \mapsto \zeta^k$ with $k \in \mathbb{Z}_8^\times$. It follows that $\phi(\alpha_1)^8 = \phi(A_1) = A_k = \alpha_k^8$ so $\phi(\alpha_1) = \zeta^l\alpha_k$ for some l. Therefore the 32 elements of $\mathrm{Gal}(L/F)$ are given by $\zeta \mapsto \zeta^k$, $\alpha_1 \mapsto \zeta^l\alpha_k$ with $k \in \mathbb{Z}_8^\times$, $l \in \mathbb{Z}_8$. For $k \in \mathbb{Z}_8^\times$ we denote by τ_k the morphism $\zeta \mapsto \zeta^k$, $\alpha_1 \mapsto \alpha_k$.

Let $H = \{\tau_k \mid k \in \mathbb{Z}_8^\times\}$. We now prove that H is a subgroup of $\mathrm{Gal}(L/F)$, the mapping $k \mapsto \tau_k$ defines an isomorphism between $\mathbb{Z}_8^\times$ and H, and $\mathrm{Gal}(L/F)$ is the internal direct product of its subgroups H and $\mathrm{Gal}(L/E) = \langle\sigma\rangle$. To do this we have to prove that $H \cap \mathrm{Gal}(L/E) = \{1\}$, $\tau_k\sigma = \sigma\tau_k$ for

$k \in \mathbb{Z}_8^\times$, and $\tau_k\tau_l = \tau_{kl}$ for $k, l \in \mathbb{Z}_8^\times$. (In fact, for the second assertion we only need to prove that $\tau_3^2 = \tau_5^2 = \tau_7^2 = 1$ and $\tau_3\tau_5 = \tau_7$.)

If $\phi \in H \cap \mathrm{Gal}(L/E)$ then $\phi = \tau_k = \sigma^l$ for some $k \in \mathbb{Z}_8^\times$ and $l \in \mathbb{Z}_8$. It follows that $\alpha_k = \tau_k(\alpha_1) = \sigma^l(\alpha_1) = \zeta^l\alpha_1$ so $A_k = \alpha_k^8 = (\zeta^l\alpha_1)^8 = A_1$. Hence $k = 1$ and we have $\phi = \tau_1 = 1$.

For the second assertion we note that in all cases we have $\alpha_k = \alpha_1^k a$ for some $a \in E$. Now $\tau_k\sigma(\zeta) = \tau_k(\zeta) = \zeta^k$ and $\sigma\tau_k(\zeta) = \sigma(\zeta^k) = \zeta^k$. Also $\tau_k\sigma(\alpha_1) = \tau_k(\zeta\alpha_1) = \zeta^k\alpha_k$ and $\sigma\tau_k(\alpha_1) = \sigma(\alpha_k) = \sigma(\alpha_1^k a) = (\zeta\alpha_1)^k a = \zeta^k\alpha_k$. So $\tau_k\sigma = \sigma\tau_k$.

The proof of the third assertion is more laborious as it involves many cases. We first prove that $\tau_3\tau_5 = \tau_7$ when $p \equiv 3 \pmod 8$. Since $\tau_k(\zeta) = \zeta^k$ we have $\tau_3\tau_5(\zeta) = \zeta^{15} = \zeta^7 = \tau_7(\zeta)$. Also

$$\begin{aligned}
\tau_3\tau_5(\alpha_1) = \tau_3(\alpha_5) &= \tau_3(\alpha_1^5(x + y\sqrt{5}\,i)^{-1}(u + v\sqrt{2}\,i)^{-3}) \\
&= \alpha_3^5(x - y\sqrt{5}\,i)^{-1}(u + v\sqrt{2}\,i)^{-3} \\
&= (\alpha_1^3(x + y\sqrt{5}\,i)^{-1}(u + v\sqrt{2}\,i)^{-1})^5(2p)^{-1}(x + y\sqrt{5}\,i)(u + v\sqrt{2}\,i)^{-3} \\
&= \alpha_1^{15}(2p)^{-1}(x + y\sqrt{5}\,i)^{-4}(u + v\sqrt{2}\,i)^{-8} \\
&= \alpha_1^7(x + y\sqrt{5}\,i)^{-2}(u + v\sqrt{2}\,i)^{-4} = \alpha_7 = \tau_7(\alpha_1).
\end{aligned}$$

So $\tau_3\tau_5 = \tau_7$. (Recall that $\tau_{3|E}$ is given by $\zeta \mapsto \zeta^3$, i.e. by $i \mapsto -i$, $\sqrt{2} \mapsto -\sqrt{2}$. Also $\alpha_1^8 = A_1 = 2p(x + y\sqrt{5}\,i)^2(u + v\sqrt{2}\,i)^4$.)

The proof of $\tau_k\tau_l = \tau_{kl}$ in all the other cases is quite straightforward if we follow the pattern above. The reason why it always works is the following: We have $\tau_k\tau_l(\zeta) = \tau_k(\zeta^l) = \zeta^{kl}$. As seen above, this implies that $\tau_k\tau_l(\alpha_1)$ is of the form $\zeta^j\alpha_{kl}$ for some j. But in calculating $\tau_k\tau_l(\alpha_1)$, as well as $\tau_{kl}(\alpha_1) = \alpha_{kl}$, ζ is not involved. (We only have the factors $x \pm y\sqrt{5}\,i$, $u \pm v\sqrt{2}\,i$ (if $p \equiv 3 \pmod 8$), $u \pm v\sqrt{2}$ (if $p \equiv 7 \pmod 8$), $2p$ and α_1.) Therefore we must have $j = 0$. Hence $\tau_k\tau_l$ is given by $\zeta \mapsto \zeta^{kl}$, $\alpha_1 \mapsto \alpha_{kl}$ so it is equal to τ_{kl}.

Consequently, $\mathrm{Gal}(L/F) = H \times \mathrm{Gal}(L/E) \cong \mathbb{Z}_8^\times \times \mathbb{Z}_8$. ∎

Let $K = L^H$. Then $\mathrm{Gal}(K/F) \cong \mathrm{Gal}(L/F)/H = \langle \sigma H \rangle \cong \mathbb{Z}_8$, the isomorphism being given by $\phi_{|K} \mapsto \phi H$. We denote by $\chi_0 : \mathrm{Gal}(K/F) \to \mu_8$ the isomorphism given by $\sigma^k_{|K} \mapsto \zeta^k$. It induces a character $\chi : \mathrm{Gal}(L/F) \to \mu_8$ given by the composition with $\mathrm{Gal}(L/F) \to \mathrm{Gal}(K/F)$. For any $\sigma^k\tau_l \in \mathrm{Gal}(L/F)$ we have $\chi(\sigma^k\tau_l) = \zeta^k$. We obtain

$$\prod_{\mathfrak{q}} \left(\frac{\varepsilon, L/F}{\mathfrak{q}}\right) = 1 \quad \text{so} \quad \chi\left(\prod_{\mathfrak{q}} \left(\frac{\varepsilon, L/F}{\mathfrak{q}}\right)\right) = 1.$$

Note that $\sigma^k(\alpha_1) = \zeta^k\alpha_1$ so for any $\phi \in \langle\sigma\rangle = \mathrm{Gal}(L/E)$ we have $\chi(\phi) = \phi(\alpha_1)/\alpha_1$.

Since $\left(\frac{5}{p}\right) = -1$ the extension $F/\mathbb{Q}$ is inert at p. Let $\mathfrak{p}$ be the prime of F lying over p, i.e. $\mathfrak{p} = p\mathcal{O}_F$. Now $-1, 2$ are units in $\mathbb{Q}_p$ so they are in the square class modulo p of either 1 or 5. In both cases they are squares in $F_\mathfrak{p}$. Therefore the prime $\mathfrak{p}$ splits completely in $E = F(i, \sqrt{2})$. Now $(x+y\sqrt{5}\,i)(x-y\sqrt{5}\,i) = 2p$ and either $(u + v\sqrt{2}\,i)(u - v\sqrt{2}\,i) = 2p$ or $(u + v\sqrt{2})(u - v\sqrt{2}) = 2p$ (according as $p \equiv 3$ or $7 \pmod 8$). So for every prime $\mathfrak{P}$ of E lying over $\mathfrak{p}$ exactly one of $x \pm y\sqrt{5}\,i$ and exactly one of $u \pm v\sqrt{2}\,i$ or $u \pm v\sqrt{2}$ belongs to $\mathfrak{P}$. Of the four primes of E that lie over $\mathfrak{p}$ we choose the one for which $x - y\sqrt{5}\,i \in \mathfrak{P}$, and $u - v\sqrt{2}\,i \in \mathfrak{P}$ or $u - v\sqrt{2} \in \mathfrak{P}$, corresponding to $p \equiv 3$ or $7 \pmod 8$.

Denote by $\infty_\pm$ the two archimedian primes of F corresponding to the embeddings $F \hookrightarrow \mathbb{R}$ given by $\sqrt{5} \mapsto \pm\sqrt{5}$.

Lemma 1.4.

(i) $\chi\left(\left(\dfrac{\varepsilon, L/F}{\mathfrak{p}}\right)\right) \equiv \varepsilon^{-(p^2-1)/8} \pmod{\mathfrak{P}}$.

(ii) $\chi\left(\left(\dfrac{\varepsilon, L/F}{\infty_-}\right)\right) = \begin{cases} 1 & \text{if } p \equiv 3 \pmod 8, \\ \operatorname{sgn}(u) & \text{if } p \equiv 7 \pmod 8. \end{cases}$

(iii) $\chi\left(\left(\dfrac{\varepsilon, L/F}{\mathfrak{q}}\right)\right) = 1$ *if* $\mathfrak{q} \neq \mathfrak{p}, \infty_-$ *and* $\mathfrak{q} \nmid 2$.

Proof. (i) Since $\mathfrak{p}$ splits in E we have $[E_\mathfrak{P} : F_\mathfrak{p}] = 1$ so $N_{E_\mathfrak{P}/F_\mathfrak{p}}\varepsilon = \varepsilon$ so $\left(\frac{\varepsilon, L/F}{\mathfrak{p}}\right) = \left(\frac{\varepsilon, L/E}{\mathfrak{P}}\right) \in \operatorname{Gal}(L/E)$. It follows that

$$\chi\left(\left(\frac{\varepsilon, L/F}{\mathfrak{p}}\right)\right) = \chi\left(\left(\frac{\varepsilon, L/E}{\mathfrak{P}}\right)\right) = \left(\frac{\varepsilon, L/E}{\mathfrak{P}}\right)(\alpha_1)/\alpha_1$$
$$= \left(\frac{\varepsilon, A_1}{\mathfrak{P}}\right)_8 = \left(\frac{A_1, \varepsilon}{\mathfrak{P}}\right)_8^{-1}.$$

(Recall that $L = E(\alpha_1)$ and we have $\alpha_1^8 = A_1 \in E$ and $\mu_8 \subset E$.)

Note that ε is a unit in $E_\mathfrak{P}$ so $\left(\frac{A_1, \varepsilon}{\mathfrak{P}}\right)_8 \equiv \varepsilon^{(\mathrm{N}\mathfrak{P}^{\operatorname{ord}_\mathfrak{P} A_1}-1)/8} \pmod{\mathfrak{P}}$. But $E_\mathfrak{P} \cong F_\mathfrak{p}$ is an unramified extension of degree 2 of $\mathbb{Q}_p$ so $\operatorname{ord}_\mathfrak{P} p = 1$ and $\mathrm{N}\mathfrak{P} = p^2$. Since also $x+y\sqrt{5}\,i \notin \mathfrak{P}$ and either $u+v\sqrt{2}\,i \notin \mathfrak{P}$ or $u+v\sqrt{2} \notin \mathfrak{P}$, depending on whether $p \equiv 3$ or $7 \pmod 8$, we get $\operatorname{ord}_\mathfrak{P} A_1 = 1$. Therefore

$$\chi\left(\left(\frac{\varepsilon, L/F}{\mathfrak{p}}\right)\right) = \left(\frac{A_1, \varepsilon}{\mathfrak{P}}\right)_8^{-1} \equiv \varepsilon^{-(p^2-1)/8} \pmod{\mathfrak{P}}.$$

(ii) Let $\mathfrak{q} = \infty_-$ and let $\mathfrak{Q}$ be the infinite prime of $E = F(\zeta)$ lying over $\mathfrak{q}$ corresponding to an embedding of E in $\mathbb{C}$ given by $\zeta \mapsto \zeta$ (i.e. the embedding of $E = \mathbb{Q}(\sqrt{5}, i, \sqrt{2})$ in $\mathbb{C}$ given by $\sqrt{5} \mapsto -\sqrt{5}$, $i \mapsto i$, $\sqrt{2} \mapsto \sqrt{2}$). Finally, we extend $\mathfrak{Q}$ to a prime $\mathcal{Q}$ of L.

We have $F_{\mathfrak{q}} \cong \mathbb{R}$ and $E_{\mathfrak{Q}} \cong L_{\mathcal{Q}} \cong \mathbb{C}$. Moreover, $\varepsilon_{\mathfrak{q}} = (1-\sqrt{5})/2 < 0$ so if $\phi = \left(\frac{\varepsilon, L/F}{\mathfrak{q}}\right)$ then ϕ corresponds to c, the conjugacy automorphism from $\mathrm{Gal}(L_{\mathcal{Q}}/F_{\mathfrak{q}}) \cong \mathrm{Gal}(\mathbb{C}/\mathbb{R})$. So we want to know what automorphism $\phi \in \mathrm{Gal}(L/F)$ corresponds to $c \in \mathrm{Gal}(L_{\mathcal{Q}}/F_{\mathfrak{q}})$. First note that $\phi(\zeta) = c(\zeta) = \overline{\zeta} = \zeta^7 = \tau_7(\zeta)$. Thus $\phi_{|E} = \tau_{7|E}$. It follows that $\phi \in \tau_7 \mathrm{Gal}(L/E) = \tau_7\langle\sigma\rangle$. So $\phi = \sigma^k\tau_7$ for some $k \in \mathbb{Z}_8$. We have $\chi(\phi) = \zeta^k$.

If $p \equiv 3 \pmod 8$ then $\phi(\alpha_1) = \sigma^k\tau_7(\alpha_1) = \sigma^k(2p\alpha_1^{-1}) = 2p\zeta^{-k}\alpha_1^{-1}$. On the other hand, $\phi(\alpha_1) = c(\alpha_1) = \overline{\alpha}_1$. Hence $\alpha_1\overline{\alpha}_1 = 2p\zeta^{-k}$. Since $\alpha_1\overline{\alpha}_1 \in \mathbb{R}_+$ and $\zeta^{-k} \in \mu_8$ we must have $\zeta^{-k} = 1$ so $\chi\left(\left(\frac{\varepsilon, L/F}{\mathfrak{q}}\right)\right) = \zeta^k = 1$, as claimed. The proof in the case when $p \equiv 7 \pmod 8$ is similar but this time $\alpha_7 = 2p(u + v\sqrt{2})\alpha_1$ so we get $\alpha_1\overline{\alpha}_1 = 2p(u+v\sqrt{2})\zeta^{-k}$. So $\alpha_1\overline{\alpha}_1 \in \mathbb{R}_+$ and $\zeta^{-k} \in \mu_8$ will imply this time $\zeta^{-k} = \mathrm{sgn}(u+v\sqrt{2})$. Thus $\chi\left(\left(\frac{\varepsilon, L/F}{\mathfrak{q}}\right)\right) = \zeta^k = \mathrm{sgn}(u+v\sqrt{2})$. But $u^2 - 2v^2 = 2p > 0$ so $|u| > |v\sqrt{2}|$. Hence $\mathrm{sgn}(u+v\sqrt{2}) = \mathrm{sgn}(u)$ and we get the desired result.

(iii) If $\mathfrak{q} = \infty_+$ then $\varepsilon_{\mathfrak{q}} = (1+\sqrt{5})/2 > 0$ so $\left(\frac{\varepsilon, L/F}{\mathfrak{q}}\right) = 1_L$. If $\mathfrak{q}$ is non-archimedian lying over $q \neq 2, p$ then $\mathfrak{q}$ does not ramify in $E = F(\zeta)$. If $\mathfrak{Q}$ is a prime of E lying over $\mathfrak{q}$ then $\mathfrak{Q}$ does not ramify in $L = E(\sqrt[8]{A_1})$ because A_1 is a unit in $E_{\mathfrak{Q}}$. This happens because A_1 divides a power of $2p$ and $(2p, q) = 1$. (If $p \equiv 3 \pmod 8$ we have $x + y\sqrt{5}\,i \,|\, 2p$ and $u + v\sqrt{2}\,i \,|\, 2p$ so $A_1 = 2p(x+y\sqrt{5}\,i)^2(u+v\sqrt{2}\,i)^4$ divides $(2p)^7$. Similarly, if $p \equiv 7 \pmod 8$ then $A_1 = 2p(x + y\sqrt{5}\,i)^6(u + v\sqrt{2})^4$ divides $(2p)^{11}$.) Hence $\mathfrak{q}$ does not ramify in L. Since ε is a unit in F we have again $\left(\frac{\varepsilon, L/F}{\mathfrak{q}}\right) = 1_L$. Therefore $\chi\left(\left(\frac{\varepsilon, L/F}{\mathfrak{q}}\right)\right) = 1$. ∎

1.5. By Lemma 1.4 the relation $\prod_{\mathfrak{q}} \chi\left(\left(\frac{\varepsilon, L/F}{\mathfrak{q}}\right)\right) = 1$ implies

$$\varepsilon^{(p^2-1)/8} \equiv \begin{cases} \chi\left(\left(\dfrac{\varepsilon, L/F}{\mathfrak{q}}\right)\right) \pmod{\mathfrak{P}} & \text{if } p \equiv 3 \pmod 8, \\ \mathrm{sgn}(u)\chi\left(\left(\dfrac{\varepsilon, L/F}{\mathfrak{q}}\right)\right) \pmod{\mathfrak{P}} & \text{if } p \equiv 7 \pmod 8, \end{cases}$$

where $\mathfrak{q}$ is the only prime of F lying over 2. (The prime 2 is inert in $F = \mathbb{Q}(\sqrt{5})$.)

Unfortunately, calculating the local Artin map $\left(\frac{\varepsilon, L/F}{\mathfrak{q}}\right)$ is very difficult since $\mathfrak{q}$ ramifies in L. In order to circumvent this impediment we show that if $p' \equiv 3, 7 \pmod{20}$ is another prime and $x', y', u', v', L', \chi'$ are the x, y, u, v, L, χ corresponding to p', and p, x, y, u, v are close enough to p', x', y', u', v' in the 2-adic topology, then $\chi\left(\left(\frac{\varepsilon, L/F}{\mathfrak{q}}\right)\right) = \chi\left(\left(\frac{\varepsilon, L'/F}{\mathfrak{q}}\right)\right)$. Next we show that if $p \equiv p' \pmod{16}$ and $y \equiv \pm y' \pmod 8$, then our conjecture is true for p iff it is true for p'. Hence we reduce the proof to a finite number of p's.

LEMMA 1.6. *Let k be a finite extension of $\mathbb{Q}_2$, $\mathcal{O}$ its ring of integers, $\mathfrak{m}$ the maximal ideal of $\mathcal{O}$, and $\mathcal{O}^\times = \mathcal{O} \setminus \mathfrak{m}$ the group of units. Let $j \geq 1$.*

(i) *If $\alpha \in 2^{j+1}\mathfrak{m}$ then there is $\beta \in 2\mathfrak{m}$ such that $1 + \alpha = (1 + \beta)^{2^j}$.*
(ii) *If $\alpha \in 2^{j+1}\mathcal{O}^\times$ and the extension $k/\mathbb{Q}_2$ is totally ramified then there is $\beta \in 2\mathfrak{m}$ such that $1 + \alpha = 5^{2^{j-1}}(1 + \beta)^{2^j}$.*

Proof. We use the following well known result: If $\alpha \in 4\mathfrak{m}$ then $1 + \alpha$ is a square in k and $1 + \alpha = (1 + \beta)^2$ for some β with $\beta\mathcal{O} = \frac{1}{2}\alpha\mathcal{O}$. More precisely, $\beta \in \frac{1}{2}\alpha(1 + \mathfrak{m})$. One way to prove this is to show that there is a sequence $\beta_0, \beta_1, \ldots$ with $\beta_0 = \frac{1}{2}\alpha$ such that $(1 + \beta_n)^2 \equiv 1 + \alpha \pmod{\alpha\mathfrak{m}^{n+1}}$ and $\beta_n \equiv \beta_{n+1} \pmod{\frac{1}{2}\alpha\mathfrak{m}^{n+1}}$ and then take $\beta = \lim \beta_n$.

We use induction on j. Take $j = 1$. For (i) we have $\alpha \in 4\mathfrak{m}$ and, by the result above, $1 + \alpha = (1 + \beta)^2$ for some β such that $\beta\mathcal{O} = \frac{1}{2}\alpha\mathcal{O}$. But $\alpha \in 4\mathfrak{m}$ so $\beta \in 2\mathfrak{m}$. For (ii) we have $\alpha \in 4\mathcal{O}^\times$ so $\alpha = 4\eta$ for some $\eta \in \mathcal{O}^\times$. We now use the fact that $k/\mathbb{Q}_2$ is a totally ramified extension so its inertia degree $[\mathcal{O}/\mathfrak{m} : \mathbb{Z}/2\mathbb{Z}]$ is 1. Thus $\mathcal{O}/\mathfrak{m} \cong \mathbb{Z}/2\mathbb{Z} = \{\widehat{0}, \widehat{1}\}$. Since $\eta \notin \mathfrak{m}$ we have $\widehat{\eta} \neq \widehat{0}$ so $\widehat{\eta} = \widehat{1}$. It follows that $\eta \equiv 1 \pmod{\mathfrak{m}}$, which implies $1 + \alpha = 1 + 4\eta \equiv 5 \pmod{4\mathfrak{m}}$ so $5^{-1}(1 + \alpha) \equiv 1 \pmod{4\mathfrak{m}}$. Hence $5^{-1}(1 + \alpha) = 1 + \alpha_1$ for some $\alpha_1 \in 4\mathfrak{m}$. By (i) we have $1 + \alpha_1 = (1 + \beta)^2$ for some $\beta \in 2\mathfrak{m}$ so $1 + \alpha = 5(1 + \beta)^2$.

Let now $j > 1$. We have $\alpha \in 2^{j+1}\mathfrak{m}$ or $2^{j+1}\mathcal{O}^\times$. In both cases $\alpha \in 2^{j+1}\mathcal{O} \subseteq 4\mathfrak{m}$. This implies that $1 + \alpha = (1 + \gamma)^2$ for some γ such that $\gamma\mathcal{O} = \frac{1}{2}\alpha\mathcal{O}$. In the case of (i) this implies $\gamma \in 2^j\mathfrak{m}$, while in the case of (ii), $\gamma \in 2^j\mathcal{O}^\times$. By the induction hypothesis we have $1 + \gamma = (1 + \beta)^{2^{j-1}}$ or $5^{2^{j-2}}(1 + \beta)^{2^{j-1}}$, respectively, for some $\beta \in 2\mathfrak{m}$. Since $1 + \alpha = (1 + \gamma)^2$ we get the desired results. ∎

1.7. Suppose now that p, p' are two primes $\equiv 3, 7 \pmod{20}$ and assume that $p \equiv p' \pmod{16}$ and $y \equiv \pm y' \pmod 8$.

From $x^2 + 5y^2 = u^2 \pm 2v^2 = 2p$ we see that x, y, v are odd and u is even.

If $p \equiv 3 \pmod 8$ then $u^2 = 2p - 2v^2 \equiv 2 \cdot 3 - 2 \cdot 1 = 4 \pmod 8$ so $4 \nmid u$.

If $p \equiv 7 \pmod 8$ then $u^2 = 2p + 2v^2 \equiv 2 \cdot 3 + 2 \cdot 1 \equiv 0 \pmod 8$ so $4 \mid u$. We reduce to the case when $8 \mid u$. If $u \equiv 4 \pmod 8$ then we replace u, v with $u_1 = 3u + 4v$ and $v_1 = 2u + 3v$. ($3 + 2\sqrt{2}$ is a unit of norm 1 in $\mathbb{Z}[\sqrt{2}]$ and $(u + v\sqrt{2})(3 + 2\sqrt{2}) = u_1 + v_1\sqrt{2}$.) Since $u \equiv 4 \pmod 8$ and v is odd we have $8 \mid 3u + 4v = u_1$.

Similarly for x', y', u', v'.

Since x, y, v, x', y', v' are all odd we may assume, after multiplying x, y, v with ± 1, that $x, y, v \equiv x', y', v' \pmod 4$. If $p \equiv p' \equiv 3 \pmod 8$ then $u/2, u'/2$ are odd, so after multiplying u with ± 1, we may assume that $u/2 \equiv u'/2 \pmod 4$ so $u \equiv u' \pmod 8$. The same happens if $p \equiv p' \equiv 7$

(mod 8), when both u, u' are multiples of 8. Since $x \equiv x'$ (mod 4) and x is odd we have $x + x' \equiv 2x \equiv 2$ (mod 4), and similarly for $y + y'$ and $v + v'$.

We have $2p \equiv 2p'$ (mod 32) so $x^2 + 5y^2 \equiv x'^2 + 5y'^2$ (mod 32) and $u^2 \pm 2v^2 \equiv u'^2 \pm 2v'^2$ (mod 32).

If $p \equiv p' \equiv 3$ (mod 8) then $u/2$ and $u'/2$ are odd so $u^2/4 \equiv u'^2/4 \equiv 1$ (mod 8). Thus $u^2 \equiv u'^2$ (mod 32). The same happens if $p \equiv 7$ (mod 8), when $8 \mid u, u'$. Together with $u^2 \pm 2v^2 \equiv u'^2 \pm 2v'^2$ (mod 32), this implies $v^2 \equiv v'^2$ (mod 16). Since $16 \mid v^2 - v'^2$ and $v + v' \equiv 2$ (mod 4) we have $8 \mid v - v'$ so $v \equiv v'$ (mod 8).

Since $y \equiv y'$ (mod 4) and $y \equiv \pm y'$ (mod 8) we have $y \equiv y'$ (mod 8). This implies that $y^2 \equiv y'^2$ (mod 16). (We have $2 \mid y + y'$ and $8 \mid y - y'$ so $16 \mid y^2 - y'^2$.) Since $x^2 + 5y^2 \equiv x'^2 + 5y'^2$ (mod 32) and $y^2 \equiv y'^2$ (mod 16) we have $x^2 \equiv x'^2$ (mod 16). Thus $16 \mid x^2 - x'^2$ and $x + x' \equiv 2$ (mod 4) so $8 \mid x - x'$. Let $x' - x = 8a$ and $y' - y = 8b$. Then

$$\begin{aligned} x^2 + 5y^2 \equiv x'^2 + 5y'^2 &= (x + 8a)^2 + 5(y + 8b)^2 \\ &\equiv x^2 + 16xa + 5y^2 + 80yb \pmod{32} \end{aligned}$$

so $2 \mid xa + 5yb$. But x, y are odd so we get $a \equiv b$ (mod 2).

In conclusion, we reduced to the case when $x, y, u, v \equiv x', y', u', v'$ (mod 8), and if $x - x' = 8a$ and $y - y' = 8b$, then $a \equiv b$ (mod 2). Also x, y, v, x', y', v' are odd, and if $p \equiv p' \equiv 3$ (mod 8), then $u/2, u'/2$ are odd as well.

Note that 2 is inert in $F = \mathbb{Q}(\sqrt{5})$ and is totally ramified in $\mathbb{Q}(\zeta) = \mathbb{Q}(i, \sqrt{2})$, so in $E = F(\zeta) = \mathbb{Q}(\sqrt{5}, i, \sqrt{2})$ there is only one prime $\mathfrak{Q}$ over 2 with ramification index $e_{\mathfrak{Q}/2} = 4$. Let $\mathfrak{q}_1, \mathfrak{q}_2$ be the primes of $\mathbb{Q}(\sqrt{5}\,i)$ and $\mathbb{Q}(\sqrt{2}\,i)$ (if $p \equiv 3$ (mod 8)) or $\mathbb{Q}(\sqrt{2})$ (if $p \equiv 7$ (mod 8)) lying over 2. We have $e_{\mathfrak{q}_1/2} = e_{\mathfrak{q}_2/2} = 2$ so $e_{\mathfrak{Q}/\mathfrak{q}_1} = e_{\mathfrak{Q}/\mathfrak{q}_2} = 2$.

Denote by $\mathcal{O}_\mathfrak{q}$ the ring of integers in $F_\mathfrak{q}$ and by $\widetilde{\mathfrak{q}} = \mathfrak{q}\mathcal{O}_\mathfrak{q}$ the maximal ideal of $\mathcal{O}_\mathfrak{q}$. We do the same for $\mathfrak{q}_1, \mathfrak{q}_2, \mathfrak{Q}$. Also denote by $\mathcal{O}_2$ the ring of integers in $\mathbb{Q}_2$ and by $\widetilde{2} = 2\mathcal{O}_2$ the maximal ideal of $\mathcal{O}_2$.

LEMMA 1.8. *If A_1' is the A_1 corresponding to p' then $A_1' = (\sqrt{5}^s t)^8 A_1$ for some integer s and some $t \in 1 + 2\widetilde{\mathfrak{Q}}$.*

Proof. If $p \equiv 3$ (mod 8) then $\widetilde{\mathfrak{q}}_2$ is generated by $\sqrt{2}\,i$. Since u is even and v is odd we have $\operatorname{ord}_{\widetilde{\mathfrak{q}}_2}(u + v\sqrt{2}\,i) = 1$. Now $8 \mid u' - u$ and $8 \mid v' - v$ so $(u' + v'\sqrt{2}\,i) - (u + v\sqrt{2}\,i) = (u' - u) + (v' - v)\sqrt{2}\,i \in 8\mathcal{O}_{\mathfrak{q}_2}$. Together with $\operatorname{ord}_{\widetilde{\mathfrak{q}}_2}(u + v\sqrt{2}\,i) = 1$, this implies that

$$\frac{u' + v'\sqrt{2}\,i}{u + v\sqrt{2}\,i} - 1 \in 8\widetilde{\mathfrak{q}}_2^{-1} = 4\widetilde{\mathfrak{q}}_2.$$

By Lemma 1.6(i) applied to $k = \mathbb{Q}(\sqrt{2}\,i)_{\mathfrak{q}_2}$, we get

$$\frac{u'+v'\sqrt{2}\,i}{u+v\sqrt{2}\,i}=t_1^2 \quad \text{with } t_1\in 1+2\widetilde{\mathfrak{q}}_2\subset 1+2\widetilde{\mathfrak{Q}}.$$

Similarly for $(u'+v'\sqrt{2})/(u+v\sqrt{2})$ when $p\equiv 7 \pmod 8$.

We have $\mathrm{N}_{\mathbb{Q}(\sqrt{5}\,i)_{\mathfrak{q}_1}/\mathbb{Q}_2}(x+y\sqrt{5}\,i)=2p$ so $\mathrm{ord}_{\widetilde{\mathfrak{q}}_1}(x+y\sqrt{5}\,i)=\frac{1}{2}\,\mathrm{ord}_{\widetilde{\mathfrak{q}}_1}\,2p=1$. Now $(x'+y'\sqrt{5}\,i)-(x+y\sqrt{5}\,i)=8a+8b\sqrt{5}\,i$, where $a,b\in\mathbb{Z}$ have the same parity. But $\mathrm{N}_{\mathbb{Q}(\sqrt{5}\,i)_{\mathfrak{q}_1}/\mathbb{Q}_2}(a+b\sqrt{5}\,i)=a^2+5b^2$ is even so $a+b\sqrt{5}\,i\in\widetilde{\mathfrak{q}}_1$. It follows that $(x'+y'\sqrt{5}\,i)-(x+y\sqrt{5}\,i)\in 8\widetilde{\mathfrak{q}}_1$, which, together with $\mathrm{ord}_{\widetilde{\mathfrak{q}}_1}(x+y\sqrt{5}\,i)=1$, implies that

$$\frac{x'+y'\sqrt{5}\,i}{x+y\sqrt{5}\,i}-1\in 8\mathcal{O}_{\mathfrak{q}_1}.$$

By Lemma 1.6(i) and (ii) applied to $k=\mathbb{Q}(\sqrt{5}\,i)_{\mathfrak{q}_1}$, this implies that

$$\frac{x'+y'\sqrt{5}\,i}{x+y\sqrt{5}\,i}=5^{2s_2}t_2^4,\quad \text{where}\quad s_2\in\{0,1\},\ t_2\in 1+2\widetilde{\mathfrak{q}}_1\subset 1+2\widetilde{\mathfrak{Q}}.$$

Since $p\equiv p' \pmod{16}$ we have $p'/p\in 1+16\mathcal{O}_2$. By Lemma 1.6(i) and (ii) applied to $k=\mathbb{Q}_2$, we have $p'/p=5^{4s_3}t_3^8$ where $s_3\in\{0,1\}$ and $t_3\in 1+2\widetilde{2}\subset 1+2\widetilde{\mathfrak{Q}}$.

If $p\equiv 3 \pmod 8$ then

$$A_1'/A_1=5^{4s_3}t_3^8(5^{2s_2}t_2^4)^2(t_1^2)^4=(\sqrt{5}^{\,s}t)^8$$

with $s=s_3+s_2$ and $t=t_3t_2t_1$. If $p\equiv 7 \pmod 8$ then

$$A_1'/A_1=5^{4s_3}t_3^8(5^{2s_2}t_2^4)^6(t_1^2)^4=(\sqrt{5}^{\,s}t)^8$$

with $s=s_3+3s_2$ and $t=t_3t_2^3t_1$. Since t_1,t_2,t_3 belong to $1+2\widetilde{\mathfrak{Q}}$, so does t. ∎

Lemma 1.9. *We have*

$$\chi\biggl(\Bigl(\frac{\varepsilon,L/F}{\mathfrak{q}}\Bigr)\biggr)=\chi'\biggl(\Bigl(\frac{\varepsilon,L'/F}{\mathfrak{q}}\Bigr)\biggr).$$

Proof. Let $\phi=\bigl(\frac{\varepsilon,L/F}{\mathfrak{q}}\bigr)$. Then $\phi=(\varepsilon,L_{\mathcal{Q}}/F_{\mathfrak{q}})$, where $\mathcal{Q}$ is a prime of L over $\mathfrak{Q}$, so over $\mathfrak{q}$. Since $-1,2\in\mathbb{Q}_2$ and $\mathrm{N}_{\mathbb{Q}(\sqrt{5})_{\mathfrak{q}}/\mathbb{Q}_2}(\varepsilon)=-1$ we have

$$\left(\frac{\varepsilon,-1}{\mathfrak{q}}\right)=\left(\frac{-1,-1}{2}\right)=-1\quad\text{and}\quad\left(\frac{\varepsilon,2}{\mathfrak{q}}\right)=\left(\frac{-1,2}{2}\right)=1$$

so $\phi(i)=-i$ and $\phi(\sqrt{2})=\sqrt{2}$. It follows that $\phi(\zeta)=\overline{\zeta}=\zeta^{-1}=\zeta^7=\tau_7(\zeta)$. So $\phi_{|E}=\tau_{7|E}$, which implies that $\phi\in\tau_7\mathrm{Gal}(L/E)=\tau_7\langle\sigma\rangle$. So $\phi=\sigma^k\tau_7$ for some $k\in\mathbb{Z}_8$. We have $\chi(\phi)=\chi(\sigma^k\tau_7)=\zeta^k$.

We have $\tau_7(\alpha_1)=\alpha_7=2p\alpha_1^{-1}$ or $2p(u+v\sqrt{2})\alpha_1^{-1}$, corresponding to $p\equiv 3$ or $7 \pmod 8$. So $\phi(\alpha_1)=\sigma^k\tau_7(\alpha_1)=\sigma^k(2p\alpha_1^{-1})=2p\zeta^{-k}\alpha_1^{-1}$ or $\phi(\alpha_1)=2p(u+v\sqrt{2})\zeta^{-k}\alpha_1^{-1}$, respectively.

We make the same reasoning for p'. Denote by $\phi', \mathcal{Q}', k'$ the $\phi, \mathcal{Q}, k$ corresponding to p'. Our goal is to prove that $\zeta^k = \zeta^{k'}$.

We have $L_{\mathcal{Q}} = E_{\mathfrak{Q}}(\alpha_1)$, $\alpha_1^8 = A_1 \in E_{\mathfrak{Q}}$, and $\mu_8 \subset E_{\mathfrak{Q}}$. It follows that $L_{\mathcal{Q}}$ is the splitting field of $X^8 - A_1 \in E_{\mathfrak{Q}}[X]$. Similarly $L'_{\mathcal{Q}'}$ is the splitting field of $X^8 - A'_1$. By Lemma 1.8 we have $A'_1 = B^8 A_1$, where $B = \sqrt{5}^s t \in E_{\mathfrak{Q}}$, so $L'_{\mathcal{Q}'} \cong L_{\mathcal{Q}}$. Let $\psi : L'_{\mathcal{Q}'} \to L_{\mathcal{Q}}$ be an isomorphism with $\psi_{|E_{\mathfrak{Q}}} = 1_{E_{\mathfrak{Q}}}$. We have $(\psi(\alpha'_1))^8 = \psi(A'_1) = A'_1 = B^8 A_1 = (B\alpha_1)^8$ so $\psi(\alpha'_1) = \zeta^l B\alpha_1$ for some integer l.

Now $\phi = (\varepsilon, \psi(L'_{\mathcal{Q}'})/E_{\mathfrak{Q}}) = \psi(\varepsilon, L'_{\mathcal{Q}'}/E_{\mathfrak{Q}})\psi^{-1} = \psi\phi'\psi^{-1}$ so $\phi\psi = \psi'\phi$. In particular, $\phi(\psi(\alpha'_1)) = \psi(\phi'(\alpha'_1))$. But if $p \equiv 3 \pmod 8$ then

$$\phi(\psi(\alpha'_1)) = \phi(\zeta^l B\alpha_1) = \zeta^{-l}\phi(B) \cdot 2p\zeta^{-k}\alpha_1^{-1},$$
$$\psi(\phi'(\alpha'_1)) = \psi(2p'\zeta^{-k'}{\alpha'_1}^{-1}) = 2p'\zeta^{-k'}\zeta^{-l}B^{-1}\alpha_1^{-1}.$$

It follows that $\zeta^{k'-k} = \frac{p'}{p}(B\phi(B))^{-1}$. We have $B = \sqrt{5}^s t$ so $B\phi(B) = 5^s t\phi(t)$. By Lemma 1.8, t belongs to $1 + 2\widetilde{\mathfrak{Q}}$ and so does its conjugate, $\phi(t)$. Since also $5 \in 1+4\mathcal{O}_2 \subset 1+2\widetilde{\mathfrak{Q}}$ we get $B\phi(B) \in 1+2\widetilde{\mathfrak{Q}}$, which, together with $p'/p \in 1 + 16\mathcal{O}_2 \subset 1 + 2\widetilde{\mathfrak{Q}}$, implies $\zeta^{k'-k} \in 1 + 2\widetilde{\mathfrak{Q}}$. By a similar reasoning, if $p \equiv 7 \pmod 8$ we have

$$\zeta^{k'-k} = \frac{p'}{p} \cdot \frac{u' + v'\sqrt{2}}{u + v\sqrt{2}} (B\phi(B))^{-1}.$$

Since

$$\frac{u' + v'\sqrt{2}}{u + v\sqrt{2}} \in 1 + 4\widetilde{\mathfrak{q}}_2 \subset 1 + 2\widetilde{\mathfrak{Q}}$$

(see the proof of Lemma 1.8) we get again $\zeta^{k'-k} \in 1 + 2\widetilde{\mathfrak{Q}}$.

We have $\zeta^{k'-k} \in 1 + 2\widetilde{\mathfrak{Q}}$ so $1 - \zeta^{k'-k} \in 2\widetilde{\mathfrak{Q}}$, which implies $\zeta^{k'-k} = 1$. (If $\eta \in \mu_8$, $\eta \neq 1$, then $1 - \eta \,|\, 2$ so $1 - \eta \notin 2\widetilde{\mathfrak{Q}}$.) Thus $\zeta^{k'} = \zeta^k$. ∎

Lemma 1.10.

(i) *If* $p \equiv 3 \pmod 8$ *then*

$$\left(\frac{x}{p}\right) = \left(\frac{x,14}{2}\right)\left(\frac{2p}{5}\right)_4, \qquad \left(\frac{y}{p}\right) = \left(\frac{y,6}{2}\right),$$
$$\left(\frac{u}{p}\right) = \left(\frac{u,3}{2}\right), \qquad \left(\frac{v}{p}\right) = \left(\frac{v,6}{2}\right).$$

(ii) *If* $p \equiv 7 \pmod 8$ *then*

$$\left(\frac{x}{p}\right) = \left(\frac{x,6}{2}\right)\left(\frac{2p}{5}\right)_4, \qquad \left(\frac{y}{p}\right) = \left(\frac{y,14}{2}\right),$$
$$\left(\frac{u}{p}\right) = \operatorname{sgn}(u), \qquad \left(\frac{v}{p}\right) = \left(\frac{v,14}{2}\right).$$

Proof. Note that $p \nmid xyuv$.

Let $q \neq 2, 5, p$ be a prime. If $q \mid x$, then $2p = x^2 + 5y^2 \equiv 5y^2 \pmod q$. Hence $\left(\frac{10p}{q}\right) = 1$, which implies $\left(\frac{x,10p}{q}\right) = 1$. The same happens if $q \nmid x$, when both x and $10p$ are units in $\mathbb{Q}_q$. We also have $10p > 0$ so $\left(\frac{x,10p}{\infty}\right) = 1$. By Hilbert's reciprocity law we get

$$\left(\frac{x}{p}\right) = \left(\frac{x, 10p}{p}\right) = \left(\frac{x, 10p}{2}\right)\left(\frac{x, 10p}{5}\right).$$

But $5 \nmid x$ so $\left(\frac{x,10p}{5}\right) = \left(\frac{x}{5}\right)$. Since $2p = x^2 + 5y^2 \equiv x^2 \pmod 5$ and $\left(\frac{-1}{5}\right) = 1$, the quartic residue symbol $\left(\frac{2p}{5}\right)_4$ is defined and is equal to $\left(\frac{x}{5}\right)$. Hence

$$\left(\frac{x}{p}\right) = \left(\frac{x, 10p}{2}\right)\left(\frac{2p}{5}\right)_4.$$

But if $p \equiv 3$ or $7 \pmod 8$ then modulo $\mathbb{Q}_2^{\times 2}$ we have $10p = 14$ or 6, respectively. This yields the formulas for $\left(\frac{x}{p}\right)$ in (i) and (ii).

Similarly if $q \neq 2, p$ is a prime then either $q \mid y$ so $2p = x^2 + 5y^2 \equiv x^2 \pmod q$ so $\left(\frac{2p}{q}\right) = 1$ so $\left(\frac{y,2p}{q}\right) = 1$, or $q \nmid y$ so again $\left(\frac{y,2p}{q}\right) = 1$. Also $2p > 0$ so $\left(\frac{y,2p}{\infty}\right) = 1$. Hence $\left(\frac{y}{p}\right) = \left(\frac{y,2p}{p}\right) = \left(\frac{y,2p}{2}\right)$. By the same proof $\left(\frac{v}{p}\right) = \left(\frac{v,2p}{2}\right)$ (in both cases when $u^2 \pm 2v^2 = 2p$). But if $p \equiv 3$ or $7 \pmod 8$ then $2p = 6$ or 14, respectively, in $\mathbb{Q}_2^{\times}/\mathbb{Q}_2^{\times 2}$. This gives the formulas for $\left(\frac{y}{p}\right)$ and $\left(\frac{v}{p}\right)$ in (i) and (ii).

If $p \equiv 3 \pmod 8$ then for any prime $q \neq 2, p$ we have either $q \mid u$ so $2p \equiv u^2 + 2v^2 \equiv 2v^2 \pmod p$ and so $\left(\frac{p}{q}\right) = 1$ so $\left(\frac{u,p}{q}\right) = 1$, or $q \nmid u$ and again $\left(\frac{u,p}{q}\right) = 1$. Similarly if $p \equiv 7 \pmod 8$ then $2p = u^2 - 2v^2$ implies $\left(\frac{u,-p}{q}\right) = 1$ for $q \neq 2, p$ prime. If $p \equiv 3 \pmod 8$ then $p > 0$ so $\left(\frac{u,p}{\infty}\right) = 1$ and so

$$\left(\frac{u}{p}\right) = \left(\frac{u, p}{p}\right) = \left(\frac{u, p}{2}\right) = \left(\frac{u, 3}{2}\right).$$

If $p \equiv 7 \pmod 8$ then $-p \in \mathbb{Q}_2^{\times 2}$ so $\left(\frac{u,-p}{2}\right) = 1$. We get

$$\left(\frac{u}{p}\right) = \left(\frac{u, -p}{p}\right) = \left(\frac{u, -p}{\infty}\right) = \operatorname{sgn}(u). \ \blacksquare$$

REMARK 1.11. If s, t are p-adic units and $s \equiv \pm t \pmod p$ then

$$s \equiv \left(\frac{st}{p}\right) t \pmod p.$$

Indeed, if $s \equiv t \pmod p$ then $\left(\frac{st}{p}\right) = 1$, while if $s \equiv -t \pmod p$ then $\left(\frac{st}{p}\right) = \left(\frac{-1}{p}\right) = -1$. Also note that, since $\left(\frac{-1}{p}\right) = -1$, we have $\left(\frac{\alpha}{p}\right) = \alpha$ if $\alpha \in \{\pm 1\}$.

LEMMA 1.12. *Let $\alpha,\beta\in\{\pm1\}$ and let s,t be integers in $\mathbb{Q}_p$ such that $s+t\sqrt{5}\equiv\frac{\alpha+\beta i}{\sqrt{2}}\pmod{\widetilde{\mathfrak{P}}}$.*

(i) *If $p\equiv3\pmod 8$ then*

$$s\equiv-2^{(p-3)/4}\left(\frac{u,3}{2}\right)\left(\frac{v,6}{2}\right)\beta\pmod p,$$

$$t\equiv-10^{(p-3)/4}\left(\frac{x,14}{2}\right)\left(\frac{y,6}{2}\right)\left(\frac{u,3}{2}\right)\left(\frac{v,6}{2}\right)\left(\frac{2p}{5}\right)_4\alpha\pmod p.$$

(ii) *If $p\equiv7\pmod 8$ then*

$$s\equiv2^{(p-3)/4}\left(\frac{v,14}{2}\right)\operatorname{sgn}(u)\alpha\pmod p,$$

$$t\equiv10^{(p-3)/4}\left(\frac{x,6}{2}\right)\left(\frac{y,14}{2}\right)\left(\frac{v,14}{2}\right)\left(\frac{2p}{5}\right)_4\operatorname{sgn}(u)\beta\pmod p.$$

Proof. (i) We have $p\nmid xyuv$ and $x-y\sqrt{5}\,i,u-v\sqrt{2}\,i\in\widetilde{\mathfrak{P}}$ so $x\equiv y\sqrt{5}\,i\pmod{\widetilde{\mathfrak{P}}}$ and $u\equiv v\sqrt{2}\,i\pmod{\widetilde{\mathfrak{P}}}$. It follows that

$$\frac{i}{\sqrt{2}}\equiv-\frac{v}{u}\pmod{\widetilde{\mathfrak{P}}},\qquad\frac{1}{\sqrt{2}}\equiv-\frac{yv}{xu}\sqrt{5}\pmod{\widetilde{\mathfrak{P}}}.$$

Hence

$$s+t\sqrt{5}\equiv\frac{\alpha+\beta i}{\sqrt{2}}\equiv-\alpha\,\frac{yv}{xu}\sqrt{5}-\beta\,\frac{v}{u}\pmod{\widetilde{\mathfrak{P}}}.$$

Since both sides belong to $F_{\mathfrak{p}}$, the congruence will also hold modulo $\widetilde{\mathfrak{p}}$. This implies

$$s\equiv-\beta\,\frac{v}{u}\pmod p,\qquad t\equiv-\alpha\,\frac{yv}{xu}\pmod p.$$

We have

$$s\equiv-\beta\,\frac{v}{u}\equiv\frac{\beta i}{\sqrt{2}}\pmod{\widetilde{\mathfrak{P}}},\qquad t\sqrt{5}\equiv-\alpha\,\frac{yv}{xu}\sqrt{5}\equiv\frac{\alpha}{\sqrt{2}}\pmod{\widetilde{\mathfrak{P}}}.$$

Taking squares yields $s^2\equiv-\frac12\pmod{\widetilde{\mathfrak{P}}}$ and $5t^2\equiv\frac12\pmod{\widetilde{\mathfrak{P}}}$ so $t^2\equiv\frac{1}{10}\pmod{\widetilde{\mathfrak{P}}}$. Since all sides belong to $\mathbb{Q}_p$, these congruences will also hold modulo p. It follows that $\left(\frac{-2}{p}\right)=\left(\frac{10}{p}\right)=1$ and so $(-2)^{(p-1)/2}\equiv10^{(p-1)/2}\equiv1\pmod p$. Thus $s^2\equiv\frac{1}{-2}\equiv((-2)^{(p-3)/4})^2\pmod p$ so $s\equiv\pm(-2)^{(p-3)/4}$ and similarly $t\equiv\pm10^{(p-3)/4}\pmod p$.

By Lemma 1.10 and Remark 1.11 we have

$$s\equiv\left(\frac{(-2)^{(p-3)/4}s}{p}\right)(-2)^{(p-3)/4}=\left(\frac{s}{p}\right)2^{(p-3)/4}$$

$$=\left(\frac{-uv\beta}{p}\right)2^{(p-3)/4}=-2^{(p-3)/4}\left(\frac{u,3}{2}\right)\left(\frac{v,6}{2}\right)\beta\pmod p.$$

(Note that $(p-3)/4$ is even.) Similarly

$$t \equiv \left(\frac{10^{(p-3)/4}t}{p}\right)10^{(p-3)/4} = \left(\frac{t}{p}\right)10^{(p-3)/4} = \left(\frac{-xyuv\alpha}{p}\right)10^{(p-3)/4}$$
$$= -10^{(p-3)/4}\left(\frac{x,14}{2}\right)\left(\frac{y,6}{2}\right)\left(\frac{u,3}{2}\right)\left(\frac{v,6}{2}\right)\left(\frac{2p}{5}\right)_4\alpha \pmod p.$$

If $p \equiv 7 \pmod 8$ then again $x \equiv y\sqrt{5}\,i \pmod{\widetilde{\mathfrak{P}}}$ but $u \equiv v\sqrt{2} \pmod{\widetilde{\mathfrak{P}}}$. So this time

$$\frac{1}{\sqrt{2}} \equiv \frac{v}{u} \pmod{\widetilde{\mathfrak{P}}}, \qquad \frac{i}{\sqrt{2}} \equiv -\frac{yv}{xu}\sqrt{5}.$$

We get

$$s + t\sqrt{5} \equiv \frac{v}{u}\,\alpha - \frac{yv}{xu}\sqrt{5} \pmod{\widetilde{\mathfrak{P}}}$$

so

$$s \equiv \frac{v}{u}\,\alpha \pmod p \quad \text{and} \quad t \equiv -\frac{yv}{xu}\,\beta \pmod p.$$

Now

$$s \equiv \alpha\,\frac{v}{u} \equiv \frac{\alpha}{\sqrt{2}} \pmod{\widetilde{\mathfrak{P}}}, \qquad t\sqrt{5} \equiv -\beta\,\frac{yv}{xu}\sqrt{5} \equiv \frac{\beta i}{\sqrt{2}} \pmod{\widetilde{\mathfrak{P}}}.$$

Just as for the case when $p \equiv 3 \pmod 8$, we get $s^2 \equiv \frac{1}{2} \pmod p$ and $5t^2 \equiv -\frac{1}{2} \pmod p$ and so $t^2 \equiv -\frac{1}{10} \pmod p$, which, by the same argument, will imply

$$s \equiv \left(\frac{s}{p}\right)2^{(p-3)/4} \equiv \left(\frac{uv\alpha}{p}\right) = \left(\frac{v,14}{2}\right)\operatorname{sgn}(u)\alpha \pmod p$$

and

$$t \equiv \left(\frac{t}{p}\right)(-10)^{(p-3)/4} \equiv -\left(\frac{-xyuv\beta}{p}\right)10^{(p-3)/4}$$
$$= 10^{(p-3)/4}\left(\frac{x,6}{2}\right)\left(\frac{y,14}{2}\right)\left(\frac{v,14}{2}\right)\left(\frac{2p}{5}\right)_4\operatorname{sgn}(u)\beta \pmod p,$$

as claimed. (Note that this time $(p-3)/4$ is odd so $(-10)^{(p-3)/4} = -10^{(p-3)/4}$.) ∎

Lemma 1.13. *We have*

$$F_{(p+1)/4} \equiv 2\cdot 10^{(p-3)/4}\left(\frac{2p}{5}\right)_4 A \pmod p, \qquad L_{(p+1)/4} \equiv 2^{(p+1)/4}B \pmod p,$$

where $A, B \in \{\pm 1\}$ *depend only on* $p \bmod 16$ *and* $\pm y \bmod 8$.

Proof. As seen in 1.2, $\varepsilon^{p+1} \equiv -1 \pmod{\mathfrak{p}}$. This congruence also holds modulo $\mathfrak{P}$ so $\varepsilon^{(p+1)/4} \equiv \eta \pmod{\mathfrak{P}}$ for some primitive $\eta \in \mu_8$.

By 1.2 we have

$$\varepsilon^{(p+1)/4} \equiv \begin{cases} (-1)^{(p-3)/8}\varepsilon^{(p^2-1)/8} \pmod p & \text{if } p \equiv 3 \pmod 8, \\ (-1)^{(p+1)/8}\varepsilon^{-(p^2-1)/8} \pmod p & \text{if } p \equiv 7 \pmod 8. \end{cases}$$

These congruences also hold modulo $\mathfrak{P}$. Together with 1.5 they imply that $\varepsilon^{(p+1)/4} \equiv \nu \pmod{\mathfrak{P}}$, where $\nu \in \mu_8$ is given by

$$\nu = \begin{cases} (-1)^{(p-3)/8}\chi\Big(\Big(\dfrac{\varepsilon, L/F}{\mathfrak{q}}\Big)\Big) & \text{if } p \equiv 3 \pmod 8, \\ (-1)^{(p+1)/8}\operatorname{sgn}(u)\chi\Big(\Big(\dfrac{\varepsilon, L/F}{\mathfrak{q}}\Big)\Big)^{-1} & \text{if } p \equiv 7 \pmod 8. \end{cases}$$

It follows that $\eta \equiv \nu \pmod{\mathfrak{P}}$, which implies that $\eta = \nu$. (If $\eta_1, \eta_2 \in \mu_8$ and $\eta_1 \equiv \eta_2 \pmod{\mathfrak{P}}$ then $\eta_1 = \eta_2$ since otherwise $\eta_1 - \eta_2 \mid 2$ so $\eta_1 - \eta_2 \notin \mathfrak{P}$.) In particular, since $\eta = \nu$ is primitive in μ_8, so is $\chi\big(\big(\frac{\varepsilon, L/F}{\mathfrak{q}}\big)\big)$.

Let $\chi\big(\big(\frac{\varepsilon, L/F}{\mathfrak{q}}\big)\big) = (\alpha + \beta i)/\sqrt{2}$. We have

$$\frac{L_{(p+1)/4}}{2} + \frac{F_{(p+1)/4}}{2}\sqrt{5} = \varepsilon^{(p+1)/4} \equiv \eta \pmod{\widetilde{\mathfrak{P}}},$$

where

$$\eta = (-1)^{(p-3)/8}\,\frac{\alpha + \beta i}{\sqrt{2}} \quad \text{if } p \equiv 3 \pmod 8$$

and

$$\eta = (-1)^{(p+1)/8}\operatorname{sgn}(u)\left(\frac{\alpha + \beta i}{\sqrt{2}}\right)^{-1} = (-1)^{(p+1)/8}\operatorname{sgn}(u)\left(\frac{\alpha - \beta i}{\sqrt{2}}\right)$$

if $p \equiv 7 \pmod 8$. By Lemma 1.12 this implies that

$$\frac{F_{(p+1)/4}}{2} \equiv 10^{(p-3)/4}\left(\frac{2p}{5}\right)_4 A \pmod p, \qquad \frac{L_{(p+1)/4}}{2} \equiv 2^{(p-3)/4}B \pmod p,$$

where $A, B \in \{\pm 1\}$ are given by

$$A = \begin{cases} -(-1)^{(p-3)/8}\Big(\dfrac{x,14}{2}\Big)\Big(\dfrac{y,6}{2}\Big)\Big(\dfrac{u,3}{2}\Big)\Big(\dfrac{v,6}{2}\Big)\alpha & \text{if } p \equiv 3 \pmod 8, \\ -(-1)^{(p+1)/8}\Big(\dfrac{x,6}{2}\Big)\Big(\dfrac{y,14}{2}\Big)\Big(\dfrac{v,14}{2}\Big)\beta & \text{if } p \equiv 7 \pmod 8, \end{cases}$$

and

$$B = \begin{cases} -(-1)^{(p-3)/8}\Big(\dfrac{u,3}{2}\Big)\Big(\dfrac{v,6}{2}\Big)\beta & \text{if } p \equiv 3 \pmod 8, \\ (-1)^{(p+1)/8}\Big(\dfrac{v,14}{2}\Big)\alpha & \text{if } p \equiv 7 \pmod 8. \end{cases}$$

We still have to prove that A, B depend only on $p \bmod 16$ and $\pm y \bmod 8$. Suppose that $p \equiv p' \pmod{16}$ and $y \equiv \pm y' \pmod 8$. Denote by α', β', A', B' the α, β, A, B corresponding to p'. We have to prove that $A = A'$ and

$B = B'$. By 1.7 we can restrict ourselves to the case when $x, y, u, v \equiv x', y', u', v' \pmod 8$. Also x, y, v, x', y', v' are odd and, if $p \equiv 3 \pmod 8$, then $u/2, u'/2$ are odd integers. This implies that $xx', yy', vv' \in \mathbb{Q}_2^{\times 2}$. Moreover, if $p \equiv 3 \pmod 8$, then $u/2, u'/2$ are odd and $u/2 \equiv u'/2 \pmod 4$ so $uu' \in \mathbb{Q}_2^{\times 2} \cup 5\mathbb{Q}_2^{\times 2}$.

To prove that $A = A'$ we show that the various factors that occur in A are equal to the similar factors from A', and similarly for $B = B'$. By Lemma 1.9 we have $\chi\big(\big(\frac{\varepsilon, L/F}{\mathfrak{q}}\big)\big) = \chi'\big(\big(\frac{\varepsilon, L'/F}{\mathfrak{q}}\big)\big)$ so $\alpha = \alpha'$ and $\beta = \beta'$.

If $p \equiv p' \equiv 3 \pmod 8$ then $p \equiv p' \pmod{16}$ implies that $(-1)^{(p-3)/8} = (-1)^{(p'-3)/8}$. From $xx', yy', vv' \in \mathbb{Q}_2^{\times 2}$ and $uu' \in \mathbb{Q}_2^{\times 2} \cup 5\mathbb{Q}_2^{\times 2}$ we also have

$$\left(\frac{xx', 14}{2}\right) = \left(\frac{yy', 6}{2}\right) = \left(\frac{uu', 3}{2}\right) = \left(\frac{vv', 6}{2}\right) = 1$$

so

$$\left(\frac{x, 14}{2}\right) = \left(\frac{x', 14}{2}\right), \quad \left(\frac{y, 6}{2}\right) = \left(\frac{y', 6}{2}\right),$$
$$\left(\frac{u, 3}{2}\right) = \left(\frac{u', 3}{2}\right), \quad \left(\frac{v, 6}{2}\right) = \left(\frac{v', 6}{2}\right).$$

Together with $\alpha = \alpha'$ and $\beta = \beta'$, these imply $A = A'$ and $B = B'$.

If $p \equiv p' \equiv 7 \pmod 8$ then $p \equiv p' \pmod{16}$ implies that $(-1)^{(p-3)/8} = (-1)^{(p'-3)/8}$ and $xx', yy', vv' \in \mathbb{Q}_2^{\times 2}$ implies that

$$\left(\frac{xx', 6}{2}\right) = \left(\frac{yy', 14}{2}\right) = \left(\frac{vv', 14}{2}\right) = 1$$

so

$$\left(\frac{x, 6}{2}\right) = \left(\frac{x', 6}{2}\right), \quad \left(\frac{y, 14}{2}\right) = \left(\frac{y', 14}{2}\right), \quad \left(\frac{v, 14}{2}\right) = \left(\frac{v', 14}{2}\right).$$

Together with $\alpha = \alpha'$ and $\beta = \beta'$, these imply $A = A'$ and $B = B'$. ∎

Proof of Conjecture 1.1. Note that the factor $(-1)^{[(p-5)/10]}$ which appears in the expression for $F_{(p+1)/4} \bmod p$ is equal to $-\big(\frac{2p}{5}\big)_4$. (If $p \equiv 3 \pmod{20}$ they are both -1; if $p \equiv 7 \pmod{20}$ they are both 1.) Therefore Sun's conjecture states that $F_{(p+1)/4} \equiv 2 \cdot 10^{(p-3)/4}\big(\frac{2p}{5}\big)_4 A \pmod p$ and $L_{(p+1)/4} \equiv 2^{(p+1)/4} B \pmod p$ where

$$A = \begin{cases} -1 & \text{if } y \equiv \pm\frac{p-1}{2} \pmod 8, \\ 1 & \text{if } y \not\equiv \pm\frac{p-1}{2} \pmod 8, \end{cases}$$

$$B = \begin{cases} (-1)^{(p+1)/4} & \text{if } y \equiv \pm\frac{p-1}{2} \pmod 8, \\ (-1)^{(p-3)/4} & \text{if } y \not\equiv \pm\frac{p-1}{2} \pmod 8. \end{cases}$$

Obviously A, B defined this way depend only on $p \bmod 16$ and $\pm y \bmod 8$. In view of Lemma 1.13 the conjecture has to be verified only for a set of

primes p such that p covers all the possible remainders modulo 16, namely $3, 7, 11, 15$, and $\pm y$ covers the odd remainders modulo 8, i.e. ± 1 and ± 3. One can check that $3, 7, 23, 43, 47, 67, 107, 127$ cover all eight possibilities. (We have $2 \cdot 3 = 1^2 + 5 \cdot 1^2$, $2 \cdot 7 = 3^2 + 5 \cdot 1^2$, $2 \cdot 23 = 1^2 + 5 \cdot 3^2$, $2 \cdot 43 = 9^2 + 5 \cdot 1^2$, $2 \cdot 47 = 7^2 + 5 \cdot 3^2$, $2 \cdot 67 = 3^2 + 5 \cdot 5^2$, $2 \cdot 107 = 13^2 + 5 \cdot 3^2$ and $2 \cdot 127 = 3^2 + 5 \cdot 7^2$.) But Sun checked the conjecture for primes up to 3000, including these.

2. $(2+\sqrt{3})^{(p+1)/8} \bmod p$ **when** $p \equiv 7 \pmod{24}$**.** Let

$$V_n + U_n\sqrt{3} = (2+\sqrt{3})^{(p+1)/4}.$$

CONJECTURE 2.1 (Z. H. Sun, 1988). *If p is a prime, $p \equiv 7 \pmod{24}$, and $x, y \in \mathbb{Z}$ with $x \equiv 1 \pmod 3$ such that $x^2 + 3y^2 = p$, then*

$$\left(\frac{U_{(p+1)/8}}{p}\right) = (-1)^{((x+4)^2-4)/32}, \qquad \left(\frac{V_{(p+1)/8}}{p}\right) = (-1)^{(x^2-4)/32}.$$

Note that $x^2 + 3y^2 = p \equiv 7 \pmod 8$ implies that y is odd and $x \equiv 2 \pmod 4$. Therefore

$$(-1)^{((-x+4)^2-4)/32} = -(-1)^{((x+4)^2-4)/32},$$
$$(-1)^{((-x)^2-4)/32} = (-1)^{(x^2-4)/32}.$$

Since also $\left(\frac{-x}{3}\right) = -\left(\frac{x}{3}\right)$ we can remove the condition $x \equiv 1 \pmod 3$, provided that we replace $(-1)^{((x+4)^2-4)/32}$ by $(-1)^{((x+4)^2-4)/32}\left(\frac{x}{3}\right)$. (If $x \equiv 2 \pmod 3$ then replacing x by $-x$ will not change the outcome of the two formulas.)

By Lemma 2.11 these will yield some formula for $(2+\sqrt{3})^{(p+1)/8} \bmod p$:

$$U_{(p+1)/8} \equiv -(-1)^{((x+4)^2-4)/32} 6^{(p-3)/4} \left(\frac{x}{3}\right) \pmod p,$$
$$V_{(p+1)/8} \equiv (-1)^{(x^2-4)/32} 2^{(p-3)/4} \pmod p.$$

An alternative formula for $(2+\sqrt{3})^{(p+1)/8} \bmod p$ is provided in [L, Exercise 9.9, p. 315], but it also involves writing p as $p = c^2 + 6d^2 = e^2 - 2f^2$ with $c, d, e, f \in \mathbb{Z}$.

We will also prove a related result regarding $(2+\sqrt{3})^{(p+5)/8} \bmod p$ when $p \equiv 19 \pmod{24}$.

THEOREM 2.2. *If $p \equiv 19 \pmod{24}$ is a prime and $p = x^2 + 3y^2$ then*

$$U_{(p+5)/8} \equiv \begin{cases} (-1)^{(x+p+1)/8} 6^{(p-3)/4} \left(\dfrac{x}{3}\right) \pmod p & \text{if } 8 \nmid x, \\ (-1)^{(x+p+5)/8} 2^{(p-3)/4} \pmod p & \text{if } 8 \mid x, \end{cases}$$

and

$$V_{(p+5)/8} \equiv \begin{cases} (-1)^{(x+p+1)/8} \cdot 3 \cdot 6^{(p-3)/4} \left(\dfrac{x}{3}\right) \pmod p & \text{if } 8 \nmid x, \\ (-1)^{(x+p+5)/8} 2^{(p-3)/4} \pmod p & \text{if } 8 \mid x. \end{cases}$$

REMARK. Since $x^2+3y^2 = p \equiv 3 \pmod 8$ we have $4 \mid x$. If $x \equiv 4 \pmod 8$ then $(x+p+1)/8 \in \mathbb{Z}$ so the formulas above in the case $8 \nmid x$ make sense. Moreover, $(x+p+1)/8$ and $(-x+p+1)/8$ have opposite parities, which, together with $\left(\frac{-x}{3}\right) = -\left(\frac{x}{3}\right)$, implies $(-1)^{(x+p+1)/8}\left(\frac{x}{3}\right) = (-1)^{(-x+p+1)/8}\left(\frac{-x}{3}\right)$. So the formulas from Theorem 2.2 are preserved if we replace x by $-x$.

If $8 \mid x$ then $(x+p+5)/8 \in \mathbb{Z}$ and $(x+p+5)/8 \equiv (-x+p+5)/8 \pmod 2$ so again the formulas from Theorem 2.2 make sense and they do not change if we replace x by $-x$.

2.3. We will treat the two problems together. Note that $p \equiv 7, 19 \pmod{24}$ means $p \equiv 7 \pmod{12}$. We have $p \equiv 1 \pmod 3$ and the two cases, $p \equiv 3, 19 \pmod{24}$, correspond to $p \equiv 3, 7 \pmod 8$ respectively.

We have $2+\sqrt{3} = (1+\sqrt{3})^2/2$. Let $\varepsilon = 2+\sqrt{3}$ and $\varepsilon' = 1+\sqrt{3}$ and denote by $\overline{\varepsilon}, \overline{\varepsilon}'$ their conjugates. We have $\left(\frac{3}{p}\right) = -1$ so p is inert in $\mathbb{Q}(\sqrt{3})$. As in §1, we obtain $\varepsilon^{p+1} \equiv \varepsilon\overline{\varepsilon} = 1 \pmod p$ and $\varepsilon'^{p+1} \equiv \varepsilon'\overline{\varepsilon}' = -2 \pmod p$. We reduce our problem to finding $\varepsilon'^{(p^2-1)/8} \bmod p$.

If $p \equiv 7 \pmod 8$ then $\varepsilon^{(p+1)/8} = 2^{-(p+1)/8}\varepsilon'^{(p+1)/4}$. But, as in 1.2, we have

$$\varepsilon'^{(p+1)/4} \equiv \varepsilon'^{-(p^2-1)/8}(\varepsilon'^{p+1})^{(p+1)/8} \equiv (-2)^{(p+1)/8}\varepsilon^{-(p^2-1)/2} \pmod p.$$

It follows that

$$\varepsilon^{(p+1)/8} \equiv (-1)^{(p+1)/8}\varepsilon'^{-(p^2-1)/8} \pmod p.$$

If $p \equiv 3 \pmod 8$ then

$$\varepsilon^{(p+5)/8} = 2^{-(p+5)/8}\varepsilon'^{(p+5)/4} = 2^{-(p+5)/8}(1+\sqrt{3})\varepsilon'^{(p+1)/4}.$$

As in 1.2, we also have

$$\varepsilon'^{(p+1)/4} \equiv \varepsilon'^{(p^2-1)/8}(\varepsilon'^{p+1})^{-(p-3)/8} \equiv (-2)^{-(p-3)/8}\varepsilon'^{(p^2-1)/8} \pmod p.$$

It follows that

$$\varepsilon^{(p+5)/8} \equiv (-1)^{(p-3)/8}2^{-(p+1)/4}(1+\sqrt{3})\varepsilon'^{(p^2-1)/8} \pmod p.$$

Theorem 2.2 can be stated as:

$$\begin{aligned} \varepsilon^{(p+5)/8} &= V_{(p+5)/8} + U_{(p+5)/8}\sqrt{3} \\ &\equiv \begin{cases} (-1)^{(x+p+1)/8} 6^{(p-3)/4} \left(\dfrac{x}{3}\right)(3+\sqrt{3}) \pmod p & \text{if } 8 \nmid x, \\ (-1)^{(x+p+5)/8} 2^{(p-3)/4}(1+\sqrt{3}) \pmod p & \text{if } 8 \mid x. \end{cases} \end{aligned}$$

Since $\varepsilon^{(p+5)/8} \equiv (-1)^{(p-3)/8} 2^{-(p+1)/4}(1+\sqrt{3})\varepsilon'^{(p^2-1)/8} \pmod p$ this is equivalent to

$$\varepsilon'^{(p^2-1)/8} \equiv \begin{cases} (-1)^{(x-4)/8} 3^{(p-3)/4}\left(\dfrac{x}{3}\right)\sqrt{3} \pmod p & \text{if } 8 \nmid x, \\ (-1)^{x/8} \pmod p & \text{if } 8 \mid x. \end{cases}$$

(Here we use the fact that $\left(\frac{2}{p}\right) = -1$ so $2^{(p+1)/4}6^{(p-3)/4} = 2^{(p-1)/2}3^{(p-3)/4} \equiv -3^{(p-3)/4} \pmod p$ and $2^{(p+1)/4}2^{(p-3)/4} = 2^{(p-1)/2} \equiv -1 \pmod p$.)

From now on, the proof follows the pattern from §1. We write $p = u^2+2v^2$ if $p \equiv 3 \pmod 8$ and $p = u^2 - 2v^2$ if $p \equiv 7 \pmod 8$. Note that the relations $p = x^2 + 3y^2 = u^2 \pm 2v^2$ are similar to $2p = x^2 + 5y^2 = u^2 \pm 2v^2$ from §1. Therefore we can repeat the definitions and results from §1 with $\mathbb{Q}(\sqrt{5})$, $2p$ and $x \pm y\sqrt{5}\,i$ replaced by $\mathbb{Q}(\sqrt{3})$, p and $x \pm y\sqrt{3}\,i$. So we take $F = \mathbb{Q}(\sqrt{3})$ and $E = F(\zeta) = \mathbb{Q}(\sqrt{3}, \sqrt{2}, i)$. We define $L = E(\sqrt[8]{A_1})$, where $A_1 \in E$ is given by

$$A_1 = \begin{cases} p(x + y\sqrt{3}\,i)^2(u + v\sqrt{2}\,i)^4 & \text{if } p \equiv 3 \pmod 8, \\ p(x + y\sqrt{3}\,i)^6(u + v\sqrt{2})^4 & \text{if } p \equiv 7 \pmod 8. \end{cases}$$

Again $\mathrm{Gal}(L/E) = \langle\sigma\rangle \cong \mathbb{Z}_8$ where σ is given by $\sqrt[8]{A_1} \mapsto \zeta\sqrt[8]{A_1}$. For $k \in \mathbb{Z}_8^\times$ define A_k and α_k similarly to the proof of Lemma 1.3. The analogue of Lemma 1.3 will hold so $\mathrm{Gal}(L/F) \cong \mathbb{Z}_8^\times \times \mathbb{Z}_8$. More precisely, $\mathrm{Gal}(L/F)$ is the internal direct product of its subgroups $H = \{\tau_k \mid k \in \mathbb{Z}_8^\times\}$ and $\langle\sigma\rangle$.

Just as in §1 we define $\chi : \mathrm{Gal}(L/F) \to \mu_8$ by $\sigma^k\tau_l \mapsto \zeta^k$.

Define $\mathfrak{p}, \mathfrak{P}$ and $\infty_\pm$ as in §1. By a proof similar to that of Lemma 1.4 we have:

Lemma 2.4.

(i) $\chi\left(\left(\dfrac{\varepsilon', L/F}{\mathfrak{p}}\right)\right) \equiv \varepsilon'^{-(p^2-1)/8} \pmod{\mathfrak{P}}$.

(ii) $\chi\left(\left(\dfrac{\varepsilon', L/F}{\infty_-}\right)\right) = \begin{cases} 1 & \text{if } p \equiv 3 \pmod 8, \\ \mathrm{sgn}(u) & \text{if } p \equiv 7 \pmod 8. \end{cases}$

(iii) $\chi\left(\left(\dfrac{\varepsilon', L/F}{\mathfrak{q}}\right)\right) = 1$ *if* $\mathfrak{q} \neq \mathfrak{p}, \infty_-$ *and* $\mathfrak{q} \nmid 2$.

(Note that for (ii) we use the fact that $\varepsilon'_{\infty_-} = 1 - \sqrt{3} < 0$, and for (iii) the fact that $\varepsilon'_{\infty_+} = 1+\sqrt{3} > 0$ and $\varepsilon' \mid 2$ so it is a unit at all nonarchimedian primes $\mathfrak{q}$ with $\mathfrak{q} \nmid 2$.)

So $\varepsilon'^{(p^2-1)/8} \equiv \chi\big(\big(\frac{\varepsilon', L/F}{\mathfrak{q}}\big)\big)$ or $\mathrm{sgn}(u)\chi\big(\big(\frac{\varepsilon', L/F}{\mathfrak{q}}\big)\big) \pmod{\mathfrak{P}}$, according as $p \equiv 3$ or $7 \pmod 8$, where $\mathfrak{q}$ is the prime of $\mathbb{Q}(\sqrt{3})$ over 2.

2.5. We now take another prime $p' \equiv 7 \pmod{12}$ and let x', y', u', v' be the corresponding x, y, u, v. Assume that $p \equiv p' \pmod{16}$ and either $x \equiv x' \pmod{16}$ or $x \equiv x' \equiv 0 \pmod 8$.

Since $u^2 \pm 2v^2 = x^2 + 3y^2 = p \equiv 3 \pmod 4$ we see that x is even and y, u, v are odd, and similarly for x', y', u', v'. By multiplying y, u, v with ± 1 we may assume that $y, u, v \equiv y', u', v' \pmod 4$. This implies that $y + y' \equiv u + u' \equiv v + v' \equiv 2 \pmod 4$.

Since v, v' are odd, we have $v^2 \equiv v'^2 \equiv 1 \pmod 8$. Together with $u^2 \pm 2v^2 = p \equiv p' = u'^2 \pm 2v'^2 \pmod{16}$, this implies $u^2 \equiv u'^2 \pmod{16}$. Since $16 \,|\, u'^2 - u^2$ and $u' + u \equiv 2 \pmod 4$, we get $8 \,|\, u' - u$.

If $x \equiv x' \pmod{16}$ then $16 \,|\, x - x'$ and $x + x'$ is even so $32 \,|\, x^2 - x'^2$. The same happens if $x \equiv x' \equiv 0 \pmod 8$. This implies that $3(y'^2 - y^2) = p' - p + x^2 - x'^2 \equiv p' - p \pmod{32}$. Since $16 \,|\, p' - p$ we have $16 \,|\, y'^2 - y^2$ and $32 \,|\, y'^2 - y^2$ iff $32 \,|\, p' - p$. But $y' + y \equiv 2 \pmod 4$ so $8 \,|\, y' - y$ and $16 \,|\, y' - y$ iff $32 \,|\, p' - p$.

Also note that if $p \equiv 3 \pmod 8$ then $x^2 + 3y^2 = p$ implies that $4 \,|\, x$, while if $p \equiv 7 \pmod 8$ then $x \equiv 2 \pmod 4$; and similarly for x'. In particular, if $p \equiv p' \equiv 7 \pmod 8$ then $x \equiv x' \pmod{16}$ since we cannot have $x \equiv x' \equiv 0 \pmod 8$.

We now prove the analogue of Lemma 1.8. Let $\mathfrak{Q}, \mathfrak{q}_1, \mathfrak{q}_2$ be the only primes of $E, \mathbb{Q}(\sqrt{3}\,i)$ and $\mathbb{Q}(\sqrt{2}\,i)$ or $\mathbb{Q}(\sqrt{2})$ lying over 2. Define $\widetilde{\mathfrak{Q}}, \widetilde{\mathfrak{q}}_1, \widetilde{\mathfrak{q}}_2$ and $\widetilde{2}$ as in §1.

LEMMA 2.6. *If A_1' is the A_1 corresponding to p', then $A_1' = (\sqrt{3}^s t)^8 A_1$ for some $t \in 1 + 2\widetilde{\mathfrak{Q}}$, where $s = 0$ if $x \equiv x' \pmod{16}$ and $s = 1$ otherwise.*

Proof. Note that $u + \sqrt{2}\,i$ (or $u + v\sqrt{2}$), $x + y\sqrt{3}\,i \,|\, p$, which is odd, so $u + \sqrt{2}\,i$ (or $u + v\sqrt{2}$), $x + y\sqrt{3}\,i, p$ are units in $\mathcal{O}_{\mathfrak{q}_2}, \mathcal{O}_{\mathfrak{q}_1}, \mathcal{O}_2$ respectively.

Suppose that $p \equiv 3 \pmod 8$. Then $\mathfrak{q}_2$ is generated by $\sqrt{2}\,i$. Since $8 \,|\, u' - u$ and $4 \,|\, v' - v$, we have $(u' + v'\sqrt{2}\,i) - (u + v\sqrt{2}\,i) = (u' - u) + (v' - v)\sqrt{2}\,i \in 4\mathfrak{q}_2$. Since also $u + v\sqrt{2}\,i \in \mathcal{O}_{\mathfrak{q}_2}^\times$ we get

$$\frac{u' + v'\sqrt{2}\,i}{u + v\sqrt{2}\,i} - 1 \in 4\widetilde{\mathfrak{q}}_2.$$

By Lemma 1.6(i) we have

$$\frac{u' + v'\sqrt{2}\,i}{u + v\sqrt{2}\,i} = t_1^2 \quad \text{for some } t_1 \in 1 + 2\widetilde{\mathfrak{q}}_2 \subset 1 + 2\widetilde{\mathfrak{Q}}.$$

Similarly for $\frac{u' + v'\sqrt{2}}{u + v\sqrt{2}}$ when $p \equiv 7 \pmod 8$.

We have $x \equiv x' \pmod 8$ and $y \equiv y' \pmod 8$. If $x + y \equiv x' + y' \pmod{16}$ then we can write $x - x' = 8a$ and $y - y' = 8b$ with $a + b$ even. This implies that $\mathrm{N}_{\mathbb{Q}(\sqrt{3}\,i)_{\mathfrak{q}_1}/\mathbb{Q}_2}(a + b\sqrt{3}\,i) = a^2 + 3b^2$ is even so $a + b\sqrt{3}\,i \in \mathfrak{q}_1$ so $(x' + y'\sqrt{3}\,i) - (x + y\sqrt{3}\,i) = 8(a + b\sqrt{3}\,i) \in 8\widetilde{\mathfrak{q}}_1$. Since also $x + y\sqrt{3}\,i \in \mathcal{O}_{\mathfrak{q}_1}^\times$

we have

$$\frac{x'+y'\sqrt{3}\,i}{x+y\sqrt{3}\,i}-1\in 8\widetilde{\mathfrak{q}}_1.$$

By Lemma 1.6(i) applied to $k=\mathbb{Q}(\sqrt{3}\,i)_{\mathfrak{q}_1}$ we get

$$\frac{x'+y'\sqrt{3}\,i}{x+y\sqrt{3}\,i}=t_2^4\quad\text{for some } t_2\in 1+2\widetilde{\mathfrak{q}}_1\subset 1+2\widetilde{\mathfrak{Q}}.$$

If $x+y\not\equiv x'+y'\pmod{16}$ then $x'+y'\equiv x+y+8\pmod{16}$. Note that $x+y$ is odd so $9x+9y\equiv x+y+8\equiv x'+y'\pmod{16}$. Since also $9x\equiv x\equiv x'\pmod 8$ and $9y\equiv y\equiv y'\pmod 8$, by a similar reasoning to the one above, we get

$$\frac{x'+y'\sqrt{3}\,i}{9x+9y\sqrt{3}\,i}=t_2^4,\quad\text{so}\quad\frac{x'+y'\sqrt{3}\,i}{x+y\sqrt{3}\,i}=9t_2^4,\quad\text{for some } t_2\in 1+2\widetilde{\mathfrak{Q}}.$$

In conclusion,

$$\frac{x'+y'\sqrt{3}\,i}{x+y\sqrt{3}\,i}=3^{2s_2}t_2^4\quad\text{with } t_2\in 1+2\widetilde{\mathfrak{Q}},$$

where $s_2=0$ if $x+y\equiv x'+y'\pmod{16}$ and $s_2=1$ if $x+y\equiv x'+y'+8\pmod{16}$.

If $p\equiv p'\pmod{32}$ then $p'-p\in 32\mathcal{O}_2=16\widetilde{2}$, which, together with $p\in\mathcal{O}_2^\times$, implies that $p'/p-1\in 16\widetilde{2}$. By Lemma 1.6(i) applied to $k=\mathbb{Q}_2$ we get $p'/p=t_3^8$ for some $t_3\in 1+2\widetilde{2}\subset 1+2\widetilde{\mathfrak{Q}}$. If $p\not\equiv p'\pmod{32}$ then $p'\equiv p+16\pmod{16}$. But p is odd so $81p\equiv p+80\equiv p+16\equiv p'\pmod{32}$. As in the previous case, we get $p'/81p=t_3^8$, so $p'/p=81t_3^8$ for some $t_3\in 1+2\widetilde{\mathfrak{Q}}$. For short, $p'/p=3^{4s_3}t_3^8$ with $t_3\in 1+2\widetilde{\mathfrak{Q}}$, where $s_3=0$ if $p\equiv p'\pmod{32}$ and $s_3=1$ if $p\equiv p'+16\pmod{32}$.

If $p\equiv 3\pmod 8$ then

$$\begin{aligned}\frac{A_1'}{A_1}&=\frac{p'}{p}\left(\frac{x'+y'\sqrt{3}\,i}{x+y\sqrt{3}\,i}\right)^2\left(\frac{u'+v'\sqrt{2}\,i}{u+v\sqrt{2}\,i}\right)^4\\&=3^{4s_3}t_3^8(3^{2s_2}t_2^4)^2(t_1^2)^4=3^{4(s_3+s_2)}(t_3t_2t_1)^8.\end{aligned}$$

If $p\equiv 7\pmod 8$ then

$$\begin{aligned}\frac{A_1'}{A_1}&=\frac{p'}{p}\left(\frac{x'+y'\sqrt{3}\,i}{x+y\sqrt{3}\,i}\right)^6\left(\frac{u'+v'\sqrt{2}}{u+v\sqrt{2}}\right)^4\\&=3^{4s_3}t_3^8(3^{2s_2}t_2^4)^6(t_1^2)^4=3^{4(s_3+3s_2)}(t_3t_2^3t_1)^8.\end{aligned}$$

By 2.5 we have either $p\equiv p'\pmod{32}$ and $y\equiv y'\pmod{16}$, or $p\equiv p'+16\pmod{32}$ and $y\equiv y'+8\pmod{16}$. We now consider separately the cases $x\equiv x'\pmod{16}$ and $x\equiv x'+8\pmod{16}$.

If $x \equiv x' \pmod{16}$ then either $p \equiv p' \pmod{32}$ and $x+y \equiv x'+y' \pmod{16}$, or $p \equiv p'+16 \pmod{32}$ and $x+y \equiv x'+y'+8 \pmod{16}$. This implies that either $s_3 = s_2 = 0$ or $s_3 = s_2 = 1$. If $p \equiv 3 \pmod 8$ then

$$\frac{A_1'}{A_1} = 3^{4(s_3+s_2)}(t_3t_2t_1)^8 = \begin{cases} (t_3t_2t_1)^8 \text{ or} \\ 3^8(t_3t_2t_1)^8 = (-3t_3t_2t_1)^8. \end{cases}$$

If $p \equiv 7 \pmod 8$ then

$$\frac{A_1'}{A_1} = 3^{4(s_3+3s_2)}(t_3t_2^3t_1)^8 = \begin{cases} (t_3t_2^3t_1)^8 \text{ or} \\ 3^{16}(t_3t_2^3t_1)^8 = (9t_3t_2^3t_1)^8. \end{cases}$$

Thus $A_1'/A_1 = t^8$, where $t = t_3t_2t_1, -3t_3t_2t_1, t_3t_2^3t_1$ or $9t_3t_2^3t_1$. But $t_3, t_2, t_1 \in 1+2\widetilde{\mathfrak{Q}}$ and also $-3, 9 \in 1+4\mathcal{O}_2 \subset 1+2\widetilde{\mathfrak{Q}}$. So in all four cases we have $t \in 1+2\widetilde{\mathfrak{Q}}$.

If $x \equiv x'+8 \pmod{16}$ then either $p \equiv p' \pmod{32}$ and $x+y \equiv x'+y'+8 \pmod{16}$, or $p \equiv p'+16 \pmod{32}$ and $x+y \equiv x'+y' \pmod{16}$. This implies that either $s_3 = 0, s_2 = 1$ or $s_3 = 1, s_2 = 0$. Since $x \not\equiv x' \pmod{16}$ we must have $x \equiv x' \equiv 0 \pmod 8$ so $p = x^2+3y^2 \equiv 3 \pmod 8$. We get

$$\frac{A_1'}{A_1} = 3^{4(s_3+s_2)}(t_3t_2t_1)^8 = 3^4(t_3t_2t_1)^8 = (\sqrt{3}\,t)^8, \quad \text{where} \quad t = t_3t_2t_1.$$

But t_3, t_2, t_1 belong to $1+2\widetilde{\mathfrak{Q}}$ and so does t. ∎

Let E', χ' be the E, χ corresponding to p'.

Lemma 2.7. *We have*

$$\chi\left(\left(\frac{\varepsilon', L/F}{\mathfrak{q}}\right)\right) = (-1)^{(x'-x)/8}\chi'\left(\left(\frac{\varepsilon', L'/F}{\mathfrak{q}}\right)\right).$$

(*Note that if* $p \equiv p' \equiv 7 \pmod 8$ *then by* 2.5, $x \equiv x' \pmod{16}$ *so the factor* $(-1)^{(x'-x)/8}$ *can be dropped in the formula above.*)

Proof. Let $\phi = \chi\big(\big(\frac{\varepsilon', L/F}{\mathfrak{q}}\big)\big)$. We have $\mathrm{N}_{\mathbb{Q}(\sqrt{3})_{\mathfrak{q}}/\mathbb{Q}_2}(\varepsilon') = -2$ so

$$\left(\frac{\varepsilon', -1}{\mathfrak{q}}\right) = \left(\frac{-2, -1}{2}\right) = -1, \qquad \left(\frac{\varepsilon', 2}{\mathfrak{q}}\right) = \left(\frac{-2, 2}{2}\right) = 1.$$

Thus $\phi(i) = -i$ and $\phi(\sqrt{2}) = \sqrt{2}$ and so $\phi(\zeta) = \overline{\zeta} = \zeta^7$.

Now the proof follows that of Lemma 1.9. We have $A_1' = B^8A_1$, where $B = \sqrt{3}^s t$. If $\chi\big(\big(\frac{\varepsilon', L/F}{\mathfrak{q}}\big)\big) = \zeta^k$ and $\chi'\big(\big(\frac{\varepsilon', L'/F}{\mathfrak{q}}\big)\big) = \zeta^{k'}$, then we have to prove that $\zeta^{k'-k} = (-1)^{(x'-x)/8}$. By the same proof as for Lemma 1.9 we have

$$\zeta^{k'-k} = \frac{p'}{p}\,(B\phi(B))^{-1} \quad \text{or} \quad \frac{p'}{p} \cdot \frac{u'+v'\sqrt{2}}{u+v\sqrt{2}}\,(B\phi(B))^{-1},$$

according as $p \equiv 3$ or $7 \pmod 8$. Now $p \equiv p' \pmod{16}$, so $p'/p \in 1+16\mathcal{O}_2 \subset 1+2\widetilde{\mathfrak{Q}}$, and if $p \equiv 7 \pmod 8$, then

$$\frac{u'+v'\sqrt{2}}{u+v\sqrt{2}} \in 1+4\widetilde{\mathfrak{q}}_2 \subset 1+2\widetilde{\mathfrak{Q}}.$$

On the other hand, $B = \sqrt{3}^s t$ so $B\phi(B) = 3^s t\phi(t)$. By Lemma 2.6, t belongs to $1+2\widetilde{\mathfrak{Q}}$ and so does its conjugate $\phi(t)$. In the case $x \equiv x' \pmod{16}$, when $(-1)^{(x'-x)/8} = 1$, we have $s = 0$ so $(B\phi(B))^{-1} = (t\phi(t))^{-1} \in 1+2\widetilde{\mathfrak{Q}}$. This implies that $\zeta^{k'-k} \in 1+2\widetilde{\mathfrak{Q}}$ and so $\zeta^{k'-k} = 1$. In the case $x \equiv x'+8 \pmod{16}$, when $(-1)^{(x'-x)/8} = -1$, we have $s = 1$ so $3(B\phi(B))^{-1} = (t\phi(t))^{-1} \in 1+2\widetilde{\mathfrak{Q}}$. It follows that $3\zeta^{k'-k} \in 1+2\widetilde{\mathfrak{Q}}$. Together with $4\zeta^{k'-k} \in 4\mathcal{O}_{\mathfrak{Q}} \subset 2\widetilde{\mathfrak{Q}}$, this implies by subtraction that $-\zeta^{k'-k} \in 1+2\widetilde{\mathfrak{Q}}$ and so $-\zeta^{k'-k} = 1$. ∎

LEMMA 2.8.

(i) *If* $p \equiv 3 \pmod 8$ *then*

$$\left(\frac{x}{p}\right) = \left(\frac{x}{3}\right), \qquad \left(\frac{y}{p}\right) = \left(\frac{y,3}{2}\right).$$

(ii) *If* $p \equiv 7 \pmod 8$ *then*

$$\left(\frac{x}{p}\right) = \left(\frac{x,5}{2}\right)\left(\frac{x}{3}\right), \qquad \left(\frac{y}{p}\right) = \left(\frac{y,7}{2}\right),$$
$$\left(\frac{u}{p}\right) = \left(\frac{u,2}{2}\right)\operatorname{sgn}(u), \qquad \left(\frac{v}{p}\right) = \left(\frac{v,7}{2}\right).$$

Proof. As in the proof of Lemma 1.10, the relation $x^2+3y^2 = p$ implies $\left(\frac{x,3p}{q}\right) = 1$ for $q \neq 2,3,p$ and $\left(\frac{y,p}{q}\right) = 1$ for $q \neq 2,p$. Also $\left(\frac{x,3p}{\infty}\right) = \left(\frac{y,p}{\infty}\right) = 1$. Therefore

$$\left(\frac{x}{p}\right) = \left(\frac{x,3p}{p}\right) = \left(\frac{x,3p}{2}\right)\left(\frac{x,3p}{3}\right) = \left(\frac{x,3p}{2}\right)\left(\frac{x}{3}\right), \ \left(\frac{y}{p}\right) = \left(\frac{y,p}{p}\right) = \left(\frac{y,p}{2}\right).$$

If $p \equiv 3 \pmod 8$ then $\left(\frac{x,3p}{2}\right) = 1$ and $\left(\frac{y,p}{2}\right) = \left(\frac{y,3}{2}\right)$. If $p \equiv 7 \pmod 8$ then $\left(\frac{x,3p}{2}\right) = \left(\frac{x,5}{2}\right)$ and $\left(\frac{y,p}{2}\right) = \left(\frac{y,7}{2}\right)$. This yields the formulas for $\left(\frac{x}{p}\right)$ and $\left(\frac{y}{p}\right)$ from (i) and (ii).

If $p \equiv 7 \pmod 8$ then $u^2-2v^2 = p$ implies $\left(\frac{u,-2p}{q}\right) = 1$ and $\left(\frac{v,p}{q}\right) = 1$ for $q \neq 2,p$. Also $\left(\frac{v,p}{\infty}\right) = 1$. Hence

$$\left(\frac{u}{p}\right) = \left(\frac{u,-2p}{p}\right) = \left(\frac{u,-2p}{2}\right)\left(\frac{u,-2p}{\infty}\right) = \left(\frac{u,2}{2}\right)\operatorname{sgn}(u),$$
$$\left(\frac{v}{p}\right) = \left(\frac{v,p}{2}\right) = \left(\frac{v,7}{2}\right). \ ∎$$

LEMMA 2.9. *Let* $s,t \in \mathcal{O}_p$, $\alpha,\beta \in \{\pm 1\}$.

(i) *If* $p \equiv 7 \pmod 8$ *and* $s + t\sqrt{3} \equiv \frac{\alpha+\beta i}{\sqrt{2}} \pmod{\widetilde{\mathfrak{P}}}$ *then*

$$s \equiv \left(\frac{s}{p}\right) 2^{(p-3)/4} \pmod p \quad \textit{and} \quad t \equiv -\left(\frac{t}{p}\right) 6^{(p-3)/4} \pmod p.$$

Also

$$\left(\frac{s}{p}\right) = \left(\frac{uv}{p}\right)\alpha \quad \textit{and} \quad \left(\frac{t}{p}\right) = -\left(\frac{xyuv}{p}\right)\beta.$$

(ii) *If* $p \equiv 3 \pmod 8$ *and* $s + t\sqrt{3} \equiv \beta i \pmod{\widetilde{\mathfrak{P}}}$ *then* $s \equiv 0 \pmod p$ *and* $t \equiv \left(\frac{t}{p}\right) 3^{(p-3)/4} \pmod p$. *Also* $\left(\frac{t}{p}\right) = -\left(\frac{xy}{p}\right)\beta$.

Proof. (i) We have $x - y\sqrt{3}\,i, u - v\sqrt{2} \in \widetilde{\mathfrak{P}}$ so $x \equiv y\sqrt{3}\,i \pmod{\widetilde{\mathfrak{P}}}$ and $u \equiv v\sqrt{2} \pmod{\widetilde{\mathfrak{P}}}$. Since also $p \nmid xyuv$, we have

$$\frac{1}{\sqrt{2}} \equiv \frac{v}{u} \pmod{\widetilde{\mathfrak{P}}} \quad \text{and} \quad \frac{i}{\sqrt{2}} \equiv -\frac{yv}{xu}\sqrt{3} \pmod{\widetilde{\mathfrak{P}}}.$$

Therefore

$$s + t\sqrt{3} \equiv \frac{\alpha+\beta i}{\sqrt{2}} \equiv \alpha\frac{v}{u} - \beta\frac{yv}{xu}\sqrt{3} \pmod{\widetilde{\mathfrak{P}}}.$$

Since both sides belong to $F_{\mathfrak{p}}$, the congruence will also hold modulo $\widetilde{\mathfrak{p}}$ so

$$s \equiv \alpha\frac{v}{u} \pmod p, \qquad t \equiv -\beta\frac{yv}{xu} \pmod p.$$

By Remark 1.11 we get

$$\left(\frac{s}{p}\right) = \left(\frac{uv\alpha}{p}\right) = \left(\frac{uv}{p}\right)\alpha, \qquad \left(\frac{t}{p}\right) = \left(\frac{-xyuv\beta}{p}\right) = -\left(\frac{xyuv}{p}\right)\beta.$$

We have

$$s \equiv \alpha\frac{v}{u} \equiv \frac{\alpha}{\sqrt{2}} \pmod{\widetilde{\mathfrak{P}}}, \qquad t\sqrt{3} \equiv -\beta\frac{yv}{xu}\sqrt{3} \equiv \frac{\beta i}{\sqrt{2}} \pmod{\widetilde{\mathfrak{P}}}$$

so $s^2 \equiv \frac{1}{2} \pmod{\widetilde{\mathfrak{P}}}$ and $3t^2 \equiv -\frac{1}{2} \pmod{\widetilde{\mathfrak{P}}}$. Since both sides belong to $\mathbb{Q}_p$, these congruences also hold modulo p. Consequently, $s^2 \equiv \frac{1}{2} \pmod p$ and $t^2 \equiv -\frac{1}{6} \pmod p$. It follows that $\left(\frac{2}{p}\right) = \left(\frac{-6}{p}\right) = 1$ so $2^{(p-1)/2} \equiv (-6)^{(p-1)/2} \equiv 1 \pmod p$. Therefore $s^2 \equiv \frac{1}{2} \equiv (2^{(p-3)/4})^2 \pmod p$ and so $s \equiv \pm 2^{(p-3)/4} \pmod p$. By Remark 1.11 we have

$$s \equiv \left(\frac{2^{(p-3)/4}s}{p}\right) 2^{(p-3)/4} = \left(\frac{s}{p}\right) 2^{(p-3)/4} \pmod p.$$

Similarly

$$t \equiv \left(\frac{t}{p}\right)(-6)^{(p-3)/4} = -\left(\frac{t}{p}\right) 6^{(p-3)/4} \pmod p.$$

(Note that $p \equiv 7 \pmod 8$ so $(p-3)/4$ is odd.)

(ii) The congruence $x \equiv y\sqrt{3}\,i \pmod{\widetilde{\mathfrak{P}}}$ implies $i \equiv -\frac{y}{x}\sqrt{3} \pmod{\widetilde{\mathfrak{P}}}$ so $s + t\sqrt{3} \equiv -\beta\frac{y}{x}\sqrt{3} \pmod{\widetilde{\mathfrak{P}}}$. It follows that $s \equiv 0 \pmod p$ and $t \equiv -\beta\frac{y}{x} \pmod p$. By Remark 1.11,

$$\left(\frac{t}{p}\right) = \left(\frac{-xy\beta}{p}\right) = -\left(\frac{xy}{p}\right)\beta.$$

We have $t\sqrt{3} \equiv -\beta\frac{y}{x}\sqrt{3} \equiv \beta i \pmod{\widetilde{\mathfrak{P}}}$ so $3t^2 \equiv -1 \pmod{\widetilde{\mathfrak{P}}}$. This implies $t^2 \equiv -\frac{1}{3} \pmod p$. We have $\left(\frac{-3}{p}\right) = 1$ so $(-3)^{(p-1)/2} \equiv 1 \pmod p$. Thus $t^2 \equiv -\frac{1}{3} \equiv ((-3)^{(p-3)/4})^2 \pmod p$ so $t \equiv \pm(-3)^{(p-3)/4} \pmod p$. By Remark 1.11 we have

$$t \equiv \left(\frac{(-3)^{(p-3)/4}t}{p}\right)(-3)^{(p-3)/4} = \left(\frac{t}{p}\right)3^{(p-3)/4} \pmod p.$$

(Note that $p \equiv 3 \pmod 8$ so $(p-3)/4$ is even.) ∎

2.10. By 2.3 we have $\varepsilon'^{p+1} \equiv -2 \pmod p$ so

$$\varepsilon'^{(p^2-1)/2} \equiv (-2)^{(p-1)/2} = \left(\frac{-2}{p}\right) \pmod p$$

and this congruence also holds modulo $\widetilde{\mathfrak{P}}$. If $p \equiv 3 \pmod 8$ then $\varepsilon'^{(p^2-1)/2} \equiv 1 \pmod{\widetilde{\mathfrak{P}}}$ so $\varepsilon'^{(p^2-1)/8} \equiv \eta \pmod{\widetilde{\mathfrak{P}}}$ for some $\eta \in \mu_4$. If $p \equiv 7 \pmod 8$ then $\varepsilon'^{(p^2-1)/2} \equiv -1 \pmod{\widetilde{\mathfrak{P}}}$ so $\varepsilon'^{(p^2-1)/8} \equiv \eta \pmod{\widetilde{\mathfrak{P}}}$ for some primitive $\eta \in \mu_8$.

If $p \equiv 3 \pmod 8$ then by Lemma 2.4 we have

$$\varepsilon'^{(p^2-1)/2} \equiv \chi\left(\left(\frac{\varepsilon', L/F}{\mathfrak{q}}\right)\right) \pmod{\widetilde{\mathfrak{P}}}$$

so $\eta = \chi\big(\big(\frac{\varepsilon', L/F}{\mathfrak{q}}\big)\big)$. (If $\eta, \eta' \in \mu_8$ and $\eta \equiv \eta' \pmod{\widetilde{\mathfrak{P}}}$ then $\eta = \eta'$ since otherwise $\eta - \eta' \mid 2$ so $\eta - \eta' \notin \widetilde{\mathfrak{P}}$.) Similarly if $\mathfrak{p} \equiv 7 \pmod 8$ then $\eta = \operatorname{sgn}(u)\chi\big(\big(\frac{\varepsilon', L/F}{\mathfrak{q}}\big)\big)$. It follows that $\chi\big(\big(\frac{\varepsilon', L/F}{\mathfrak{q}}\big)\big)$ is primitive in μ_8 if $p \equiv 3 \pmod 8$ and it belongs to μ_4 if $p \equiv 7 \pmod 8$.

LEMMA 2.11. *If $p \equiv 7 \pmod{24}$ then*

$$U_{(p+1)/8} \equiv -\left(\frac{U_{(p+1)/8}}{p}\right)6^{(p-3)/4} \pmod p,$$

$$V_{(p+1)/8} \equiv \left(\frac{V_{(p+1)/8}}{p}\right)2^{(p-3)/4} \pmod p.$$

Also

$$\left(\frac{U_{(p+1)/8}}{p}\right) = A\left(\frac{x}{3}\right), \qquad \left(\frac{V_{(p+1)/8}}{p}\right) = B,$$

where A and B are two functions of $p \bmod 16$ and $x \bmod 16$, A is odd and B is even in the variable x.

Proof. We have

$$\varepsilon'^{(p^2-1)/8} \equiv \operatorname{sgn}(u)\chi\bigg(\Big(\frac{\varepsilon', L/F}{\mathfrak{q}}\Big)\bigg) \pmod{\widetilde{\mathfrak{P}}}$$

and, by 2.3, $\varepsilon^{(p+1)/8} \equiv (-1)^{(p+1)/8}\varepsilon'^{-(p^2-1)/8} \pmod p$. Thus

$$\varepsilon^{(p+1)/8} \equiv \operatorname{sgn}(u)(-1)^{(p+1)/8}\chi\bigg(\Big(\frac{\varepsilon', L/F}{\mathfrak{q}}\Big)\bigg)^{-1} \pmod{\widetilde{\mathfrak{P}}}.$$

By 2.10, $(-1)^{(p+1)/8}\chi\big(\big(\frac{\varepsilon', L/F}{\mathfrak{q}}\big)\big)^{-1}$ is primitive in μ_8 so it can be written as $(\alpha+\beta i)/\sqrt{2}$ for some $\alpha, \beta \in \{\pm 1\}$. Hence

$$V_{(p+1)/8} + U_{(p+1)/8}\sqrt{3} = \varepsilon^{(p+1)/8} \equiv \frac{\alpha \operatorname{sgn}(u) + \beta \operatorname{sgn}(u) i}{\sqrt{2}} \pmod{\widetilde{\mathfrak{P}}}.$$

By Lemma 2.9(i) we have

$$V_{(p+1)/8} \equiv \bigg(\frac{V_{(p+1)/8}}{p}\bigg) 2^{(p-3)/4} \pmod p,$$
$$U_{(p+1)/8} \equiv -\bigg(\frac{U_{(p+1)/8}}{p}\bigg) 6^{(p-3)/4} \pmod p.$$

Also

$$\bigg(\frac{V_{(p+1)/8}}{p}\bigg) = \bigg(\frac{uv}{p}\bigg)\alpha \operatorname{sgn}(u) = B,$$
$$\bigg(\frac{U_{(p+1)/8}}{p}\bigg) = -\bigg(\frac{xyuv}{p}\bigg)\beta \operatorname{sgn}(u) = A\bigg(\frac{x}{3}\bigg),$$

where

$$B = \bigg(\frac{u,2}{2}\bigg)\bigg(\frac{v,7}{2}\bigg)\alpha, \qquad A = -\bigg(\frac{x,5}{2}\bigg)\bigg(\frac{y,7}{2}\bigg)\bigg(\frac{u,2}{2}\bigg)\bigg(\frac{v,7}{2}\bigg)\beta.$$

(See Lemma 2.8(ii).)

We now prove that A, B depend only on $p \bmod 16$ and $x \bmod 16$. Let $p' \equiv 7 \pmod{24}$ be another prime such that $p' \equiv p \pmod{16}$ and $x' \equiv x \pmod{16}$. We keep the reductions of 2.5. Let α', β', A', B' be the α, β, A, B corresponding to p'. In order to prove that $A' = A$ we show that the factors of A' are equal to the similar factors of A, and the same for $B' = B$. By Lemma 2.7 we have $\chi'\big(\big(\frac{\varepsilon', L'/F}{\mathfrak{q}}\big)\big) = \chi\big(\big(\frac{\varepsilon', L/F}{\mathfrak{q}}\big)\big)$. Since $p \equiv p' \pmod{16}$ we also have $(-1)^{(p'+1)/8} = (-1)^{(p+1)/8}$ and so

$$(-1)^{(p'+1)/8}\chi'\bigg(\Big(\frac{\varepsilon', L'/F}{\mathfrak{q}}\Big)\bigg) = (-1)^{(p+1)/8}\chi\bigg(\Big(\frac{\varepsilon', L/F}{\mathfrak{q}}\Big)\bigg),$$

which implies that $\alpha' = \alpha$ and $\beta' = \beta$. We still have to prove that

$$\left(\frac{x',5}{2}\right) = \left(\frac{x,5}{2}\right), \quad \left(\frac{y',7}{2}\right) = \left(\frac{y,7}{2}\right),$$
$$\left(\frac{u',2}{2}\right) = \left(\frac{u,2}{2}\right), \quad \left(\frac{v',7}{2}\right) = \left(\frac{v,7}{2}\right),$$

i.e. that

$$\left(\frac{xx',5}{2}\right) = \left(\frac{yy',7}{2}\right) = \left(\frac{uu',2}{2}\right) = \left(\frac{vv',7}{2}\right) = 1.$$

But this follows from $xx', yy', uu' \in \mathbb{Q}_2^{\times 2}$ and $vv' \in \mathbb{Q}_2^{\times 2} \cup 5\mathbb{Q}_2^{\times 2}$. (By 2.5, $x/2, x'/2, y, y', u, u', v, v'$ are all odd, and $x/2 \equiv x'/2 \pmod 8$, $y \equiv y' \pmod 8$, $u \equiv u' \pmod 8$ and $v \equiv v' \pmod 4$.)

Finally, note that if $x^2 + 3y^2 = p$ then also $(-x)^2 + 3y^2 = p$. Since $\left(\frac{U_{(p+1)/8}}{p}\right)$ and $\left(\frac{V_{(p+1)/8}}{p}\right)$ are independent of how we write p as $x^2 + 3y^2$ we must have $A(x,p)\left(\frac{x}{3}\right) = A(-x,p)\left(\frac{-x}{3}\right)$ and $B(x,p) = B(-x,p)$. So A is odd and B is even in the variable x. ∎

Proof of Conjecture 2.1. With the notation of 2.3, we have to prove that $A = (-1)^{((x+4)^2-4)/32}$ and $B = (-1)^{(x^2-4)/32}$. It is easy to verify that the mappings $x \mapsto (-1)^{((x+4)^2-4)/32}$ and $x \mapsto (-1)^{(x^2-4)/32}$, defined on integers $x \equiv 2 \pmod 4$, depend only on $x \bmod 16$, and they are odd and even, respectively. In view of Lemma 2.10, the two equalities need to be verified for a set of primes $p \equiv 7 \pmod{24}$ such that p covers all possible remainders modulo 16, namely $7, 15$ and $\pm x$ all possible remainders modulo 16, namely ± 2 and ± 6. But the primes $7, 31, 103, 127$ cover all four possibilities. (We have $7 = 2^2 + 3 \cdot 1^2$, $31 = 2^2 + 3 \cdot 3^2$, $103 = 10^2 + 3 \cdot 1^2$ and $127 = 10^2 + 3 \cdot 3^2$.) It is easy to see that Sun's conjecture is true at these primes.

Proof of Theorem 2.2. Suppose that $p \equiv 19 \pmod p$ and let $s + t\sqrt{3} = \varepsilon'^{(p^2-1)/8}$. By 2.3, Theorem 2.2 is equivalent to

$$s + t\sqrt{3} \equiv \begin{cases} (-1)^{(x-4)/8} 3^{(p-3)/4} \left(\dfrac{x}{3}\right)\sqrt{3} \pmod p & \text{if } 8 \nmid x, \\ (-1)^{x/8} \pmod p & \text{if } 8 \mid x. \end{cases}$$

We have

$$\varepsilon'^{(p^2-1)/8} \equiv \chi\left(\left(\frac{\varepsilon', L/F}{\mathfrak{q}}\right)\right) \pmod{\widetilde{\mathfrak{P}}}.$$

By 2.10, $\chi\left(\left(\frac{\varepsilon', L/F}{\mathfrak{q}}\right)\right) \in \mu_4$ so it equals $\alpha = \pm 1$ or βi with $\beta = \pm 1$. In the first case $s + t\sqrt{3} \equiv \alpha \pmod{\widetilde{\mathfrak{P}}}$ implies $s + t\sqrt{3} \equiv \alpha \pmod p$, as both sides belong to F. In the second case $s + t\sqrt{3} \equiv \alpha \pmod{\widetilde{\mathfrak{P}}}$ implies by Lemmas 2.9(ii) and 2.8(i) that $s \equiv 0 \pmod p$ and

$$t \equiv -\left(\frac{xy}{p}\right)3^{(p-3)/4}\beta = -\left(\frac{y,3}{2}\right)\beta \cdot 3^{(p-3)/4}\left(\frac{x}{3}\right)$$

so

$$s + t\sqrt{3} \equiv -\left(\frac{y,3}{2}\right)\beta \cdot 3^{(p-3)/4}\left(\frac{x}{3}\right)\sqrt{3} \pmod{p}.$$

It follows that Theorem 2.2 is equivalent to

$$\chi\left(\left(\frac{\varepsilon', L/F}{\mathfrak{q}}\right)\right) = \eta = \begin{cases} -(-1)^{(x-4)/8}\left(\dfrac{y,3}{2}\right)i & \text{if } 8 \nmid x, \\ (-1)^{x/8} & \text{if } 8 \mid x. \end{cases}$$

Let now $p' \equiv 19 \pmod{24}$ be another prime. We use the notations from 2.5 and Lemma 2.7.

LEMMA 2.12. *If* $p \equiv p' \pmod{16}$ *and* $x \equiv x' \pmod 8$ *then the conclusion of Theorem* 2.2 *holds for* p *iff it holds for* p'.

Proof. By 2.5 we have $4 \mid x, x'$ so $x \equiv x' \equiv 0$ or $4 \pmod 8$. We consider the two cases.

If $x \equiv x' \equiv 4 \pmod 8$ then $x/4, x'/4$ are odd integers. By multiplying x with ± 1, we may assume that $x/4 \equiv x'/4 \pmod 4$ so $x \equiv x' \pmod{16}$. We also have $p \equiv p' \pmod{16}$ so we may apply the reductions of 2.5. By Lemma 2.7 we have $\chi\big(\big(\frac{\varepsilon', L/F}{\mathfrak{q}}\big)\big) = \chi'\big(\big(\frac{\varepsilon', L'/F}{\mathfrak{q}}\big)\big)$. Now Theorem 2.2 for p and p' is equivalent to

$$\chi\left(\left(\frac{\varepsilon', L/F}{\mathfrak{q}}\right)\right) = -(-1)^{(x-4)/8}\left(\frac{y,2}{p}\right)i,$$
$$\chi'\left(\left(\frac{\varepsilon', L'/F}{\mathfrak{q}}\right)\right) = -(-1)^{(x'-4)/8}\left(\frac{y',2}{p}\right)i,$$

so in order to prove that the two statements are equivalent it is enough to prove that

$$-(-1)^{(x-4)/8}\left(\frac{y,2}{p}\right)i = -(-1)^{(x'-4)/8}\left(\frac{y',2}{p}\right)i.$$

But $x \equiv x' \pmod{16}$ so $(-1)^{(x-4)/8} = (-1)^{(x'-4)/8}$, so we still need $\big(\frac{y,3}{2}\big) = \big(\frac{y',3}{2}\big)$. This follows from the fact that y, y' are odd and $y \equiv y' \pmod 8$ so they are in the same square class in $\mathbb{Q}_2^\times$.

If $x \equiv x' \equiv 0 \pmod 8$ then again we can apply the reductions of 2.5. Theorem 2.2 for p and p' is equivalent to

$$\chi\left(\left(\frac{\varepsilon', L/F}{\mathfrak{q}}\right)\right) = (-1)^{x/8}, \quad \chi'\left(\left(\frac{\varepsilon', L'/F}{\mathfrak{q}}\right)\right) = (-1)^{x'/8}.$$

The two statements are equivalent because by Lemma 2.7 we have

$$\chi\left(\left(\frac{\varepsilon', L/F}{\mathfrak{q}}\right)\right) = (-1)^{(x'-x)/8}\chi'\left(\left(\frac{\varepsilon', L'/F}{\mathfrak{q}}\right)\right). \blacksquare$$

So it is enough to check Theorem 2.2 for a set of primes $p \equiv 19 \pmod{24}$ such that p covers all the possible remainders modulo 16, namely 3 and 11, and x covers all the possible remainders modulo 8, namely 0 and 4. The primes $19, 43, 67$ and 139 cover all four possibilities. (We have $19 = 4^2+3\cdot 1^2$, $43 = 4^2 + 3 \cdot 3^2$, $67 = 8^2 + 3 \cdot 1^2$ and $139 = 8^2 + 3 \cdot 5^2$.)

3. Related problems. Throughout this section $d > 1$ is a square-free integer and ε is an integer of $\mathbb{Q}(\sqrt{d})$. For the time being we assume that $d > 2$. If $p \equiv 3 \pmod 4$ is a prime with $\left(\frac{d}{p}\right) = -1$ then $\left(\frac{-d}{p}\right) = 1$ so p can be written as $p = f(x, y)$ with $x, y \in \mathbb{Z}$, where $f(x, y) = ax^2 + bxy + cy^2$ is a quadratic form with the discriminant $b^2 - 4ac = -d$ or $-4d$, according as $-d \equiv 1 \pmod 4$ or $-d \equiv 2, 3 \pmod 4$. For any prime q (including $q = \infty$) we denote by f_q the localized of f at q.

We want to determine $\varepsilon^{(p+1)/4} \bmod p$ in terms of x and y. We could also determine the value modulo p for $\varepsilon^{(p+1)/8}$ if $p \equiv 7 \pmod 8$ and for $\varepsilon^{(p+5)/8}$ if $p \equiv 3 \pmod 8$ assuming that $\varepsilon = \varepsilon_d$ is the fundamental unit of $\mathbb{Q}(\sqrt{d})$ and the norm of ε is 1. In this case, as in §2, we can write $\varepsilon = \varepsilon'^2/m$ for some integer ε' in $\mathbb{Q}(\sqrt{d})$, and $m \in \mathbb{Z}^\times$. We can take for example $\varepsilon' = 1 + \varepsilon$, and since $\varepsilon\overline{\varepsilon} = \mathrm{N}\varepsilon = 1$, we have $\varepsilon = \varepsilon'/\overline{\varepsilon}' = \varepsilon'^2/m$, where $m = \varepsilon'\overline{\varepsilon}' = \mathrm{N}\varepsilon'$. Then if $p \equiv 7 \pmod 8$ we have $\varepsilon^{(p+1)/8} = m^{-(p+1)/8}\varepsilon'^{(p+1)/4}$, while if $p \equiv 3 \pmod 8$ then $\varepsilon^{(p+5)/8} = m^{-(p+5)/8}\varepsilon'\varepsilon'^{(p+1)/4}$, so in both cases we have to determine $\varepsilon'^{(p+1)/4} \bmod p$.

As in 1.2 or 2.3, we reduce our problem to finding $\varepsilon^{(p^2-1)/8} \bmod p$. Namely, we have $\varepsilon^{p+1} \equiv N \pmod p$ and so

$$\varepsilon^{(p+1)/4} \equiv \begin{cases} N^{-(p-3)/8}\varepsilon^{(p^2-1)/8} \pmod p & \text{if } p \equiv 3 \pmod p, \\ N^{(p+1)/8}\varepsilon^{-(p^2-1)/8} \pmod p & \text{if } p \equiv 7 \pmod p, \end{cases}$$

where $N = \mathrm{N}\varepsilon = \varepsilon\overline{\varepsilon}$.

We consider the two cases $p \equiv 3$ or $7 \pmod 8$ separately. Note that besides the condition that the discriminant b^2-4ac is $-d$ or $-4d$, f should also represent numbers $\equiv 3$ or $7 \pmod 8$. This is equivalent to the fact that f_2 represents 3 or -1, respectively. We claim that the rational quadratic form $F(x, y, u, v) = f(x, y) - (u^2 \pm 2v^2)$, where the sign is $+$ if $p \equiv 3 \pmod 8$ and $-$ if $p \equiv 7 \pmod 8$, is isotropic. By the Hasse–Minkowski theorem we have to prove this statement locally. Since f is positive definite F will be indefinite and so F_∞ is isotropic. If $q > 2$ is a prime with $q \nmid d$ then F_q is unimodular so isotropic. If $q > 2$ and $q \mid d$ then F_q is isotropic because $\det F = \pm 2d \neq 1$ in $\mathbb{Q}_q^\times/(\mathbb{Q}_q^\times)^2$. Finally, if $q = 2$ and $p \equiv 3 \pmod 8$ then F_2 is isotropic because both $f_2(x, y)$ and $u^2 + 2v^2$ represent 3, while if $p \equiv 7 \pmod 8$ then F_2 is isotropic because both $f_2(x, y)$ and $u^2 - 2v^2$ represent -1.

Let $(x_1, y_1, u_1, v_1) \in \mathbb{Q}^4 \setminus \{(0,0,0,0)\}$ with $F(x_1, y_1, u_1, v_1) = 0$. Since both $f(x,y)$ and $u^2 \pm 2v^2$ are anisotropic we have $(x_1, y_1), (u_1, v_1) \neq (0,0)$ so $f(x_1, y_1) = u_1^2 \pm 2v_1^2 =: a' \neq 0$. By multiplying x_1, y_1, u_1, v_1 with a proper rational number we may assume that $x_1, y_1 \in \mathbb{Z}$ and $(x_1, y_1) = 1$. Hence f represents a' primitively, which implies that $f(x,y) = g(x', y')$, where the mapping $(x,y) \mapsto (x', y')$ belongs to $\mathrm{SL}(2,\mathbb{Z})$ and g has the form $g(x', y') = a'x'^2 + b'xy + by'^2$ and has the same discriminant as f.

Let now p be a prime, $p \nmid a'$, with $p \equiv 3 \pmod 4$ and $\left(\frac{d}{p}\right) = -1$, that is representable by f. We write $p = f(x,y) = u^2 \pm 2v^2$. Then

$$a'p = a'g(x', y') = \left(a'x' + \frac{b'}{2}\, y'\right)^2 + \frac{4a'c' - b'^2}{4}\, y'^2.$$

But $b'^2 - 4a'c' = -d$ or $-4d$, according as $-d \equiv 1 \pmod 4$ or $-d \equiv 2, 3 \pmod 4$. Hence $p = X^2 + dY^2$, where $X = a'x' + \frac{b'}{2}y'$ and $Y = \frac{1}{2}y'$ or y', respectively. Note that X, Y are linear combinations of x', y', and hence of x, y. We also have $a'p = (u_1^2 \pm 2v_1^2)(u^2 \pm 2v^2) = U^2 \pm 2V^2$, where $U = u_1u \mp v_1v$ and $V = u_1v + v_1u$.

Note that the relations $a'p = X^2 + dY^2 = U^2 \pm 2V^2$ resemble $2p = x^2 + 5y^2 = u^2 \pm 2v^2$ from §1. Therefore the reasoning follows the same pattern but with $\mathbb{Q}(\sqrt{5})$, $2p$, $x \pm y\sqrt{5}\, i$, $u \pm v\sqrt{2}$ and $u \pm v\sqrt{2}\, i$ replaced by $\mathbb{Q}(\sqrt{d})$, $a'p$, $X \pm Y\sqrt{d}\, i$, $U \pm V\sqrt{2}$ and $U \pm V\sqrt{2}\, i$. Hence we define the fields $F = \mathbb{Q}(\sqrt{d})$, $E = F(\zeta) = \mathbb{Q}(\sqrt{d}, \sqrt{2}, i)$, where $\zeta := \zeta_8$ and $L = E(\sqrt[8]{A_1})$, where

$$A_1 = \begin{cases} a'p(X + Y\sqrt{d}\, i)^2(U + V\sqrt{2}\, i)^4 & \text{if } p \equiv 3 \pmod 8, \\ a'p(X + Y\sqrt{d}\, i)^6(U + V\sqrt{2})^4 & \text{if } p \equiv 7 \pmod 8. \end{cases}$$

The analogue of Lemma 1.3 holds and, with the notation of §1, we define again $\chi : \mathrm{Gal}(L/F) \to \mu_8$ by $\sigma^k\tau_l \mapsto \zeta^k$.

Since $\left(\frac{d}{p}\right) = -1$, p is inert in F and we denote by $\mathfrak{p}$ the only prime of F over p. As in §1, $\mathfrak{p}$ splits completely in E and we denote by $\mathfrak{P}$ the prime of E over $\mathfrak{p}$ for which $\mathrm{ord}_{\mathfrak{P}}(X - Y\sqrt{d}\, i) = 1$ and $\mathrm{ord}_{\mathfrak{P}}(U - V\sqrt{2}\, i) = 1$ or $\mathrm{ord}_{\mathfrak{P}}(U - V\sqrt{2}) = 1$, according as $p \equiv 3$ or $7 \pmod 8$.

By the same proof as for Lemma 1.4(i) we get

$$\chi\left(\left(\frac{\varepsilon, L/F}{\mathfrak{p}}\right)\right) \equiv \varepsilon^{-(p^2-1)/8} \quad \text{so} \quad \varepsilon^{(p^2-1)/8} \equiv \prod_{\mathfrak{q} \neq \mathfrak{p}} \chi\left(\left(\frac{\varepsilon, L/F}{\mathfrak{q}}\right)\right)$$

modulo $\mathfrak{P}$. So, in principle, the value of $\varepsilon^{(p^2-1)/8} \bmod \mathfrak{P}$ can be determined and hence we can get $\varepsilon^{(p^2-1)/8} \bmod p$ by a reasoning similar to that from Lemmas 1.12 and 2.9. The difficulty is that the factors $\chi\left(\left(\frac{\varepsilon, L/F}{\mathfrak{q}}\right)\right)$ with $\mathfrak{q} \neq \mathfrak{p}$ may be $\neq 1$ not only for $\mathfrak{q} = \infty_\pm$ or for $\mathfrak{q} \mid 2$ but also for primes $\mathfrak{q} \mid \varepsilon$. It is not clear at this time if in all cases the final answer can be given in terms of x and y alone, as in §1 and §2, or if it has to involve also u and v.

The case $d = 2$ is different and somewhat easier because if $F = \mathbb{Q}(\sqrt{2})$ and $E = F(\sqrt{2}, \zeta)$ then $\mathrm{Gal}(E/F) \cong \mathbb{Z}_2$, unlike the case $d > 2$, when $\mathrm{Gal}(E/F) \cong \mathbb{Z}_8^\times \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. A particular case was conjectured by Z. H. Sun in 1988 (see also [S1, Conjecture 5.1]) and later solved in [S2] and involves the value of $(1+\sqrt{2})^{(p+1)/4} \bmod p$ for primes $p \equiv 3 \pmod 8$ and is given in terms of x, y, where $p = x^2 + 2y^2$.

The condition that $p \equiv 3 \pmod 4$ and $\left(\frac{2}{p}\right) = -1$ is equivalent to $p \equiv 3 \pmod 8$ so it implies that $p = x^2 + 2y^2$ for some $x, y \in \mathbb{Z}$. We define $F = \mathbb{Q}(\sqrt{2})$, $E = \mathbb{Q}(\zeta) = \mathbb{Q}(\sqrt{2}, i)$ and $L = E(\sqrt[8]{A})$ where $A = p(x+y\sqrt{2}\,i)^2$. The group $\mathrm{Gal}(E/F)$ is generated by the automorphism $\sqrt{2} \mapsto \sqrt{2}$, $i \mapsto -i$, which coincides with the automorphism $\zeta \mapsto \zeta^3$ of $\mathrm{Gal}(E/\mathbb{Q})$. We also have $\mathrm{Gal}(L/E) = \langle\sigma\rangle \cong \mathbb{Z}_8$, where σ is given by $\sqrt[8]{A} \mapsto \zeta\sqrt[8]{A}$.

LEMMA 3.1. *The extension L/F is Galois and* $\mathrm{Gal}(L/F) \cong \mathbb{Z}_2 \times \mathbb{Z}_8$.

Proof. We prove that L/F is normal. Let $\alpha = \sqrt[8]{A}$ and let β be some conjugate of α over F in some algebraic closure of F. Then β^8 is a conjugate of $\alpha^8 = A$ over F so $\beta^8 \in \{A, A'\}$, where $A' = p(x - y\sqrt{2}\,i)^2$. Since $p = (x + y\sqrt{2}\,i)(x - y\sqrt{2}\,i)$ we have

$$A' = p^3(x + y\sqrt{2}\,i)^{-2} = A^3(x + y\sqrt{2}\,i)^{-8} = \alpha'^8,$$

where $\alpha' = \alpha^3(x + y\sqrt{2}\,i)^{-1} \in L$. If $\beta^8 = A$ then $\beta = \zeta^k\alpha \in L$, while if $\beta^8 = A'$ then $\beta = \zeta^k\alpha' \in L$ for some k. So L/F is normal.

Let now $\phi \in \mathrm{Gal}(L/F)$. Then $\phi_{|E} \in \mathrm{Gal}(E/F)$ so is given by $\zeta \mapsto \zeta$ or $\zeta \mapsto \zeta^3$. If $\phi(\zeta) = \zeta$ then $\phi(\alpha)^8 = \phi(A) = A$ so $\phi(\alpha) = \zeta^k\alpha$, i.e. $\phi = \sigma^k$ for some k. If $\phi(\zeta) = \zeta^3$ then $\phi(\alpha)^8 = \phi(A) = A'$ and hence $\phi(\alpha) = \zeta^k\alpha'$ for some k. So the 16 automorphisms of L over F are given by $\zeta \mapsto \zeta$ and $\alpha \mapsto \zeta^k\alpha$ or $\zeta \mapsto \zeta^3$ and $\alpha \mapsto \zeta^k\alpha'$ with $k \in \mathbb{Z}_8$. We denote by τ the automorphism $\zeta \mapsto \zeta^3$, $\alpha \mapsto \alpha'$.

We claim that $\langle\tau\rangle \cong \mathbb{Z}_2$ and $\mathrm{Gal}(L/F)$ is the internal direct product of $\langle\tau\rangle$ and $\mathrm{Gal}(L/E) = \langle\sigma\rangle$ and so it is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_8$. We have to show that $\tau^2 = 1$, $\tau\sigma = \sigma\tau$ and $\langle\tau\rangle \cap \langle\sigma\rangle = \{1\}$. For the first condition we have $\tau(\zeta) = \zeta^3$ so $\tau^2(\zeta) = \zeta^9 = \zeta$ and

$$\begin{aligned}\tau^2(\alpha) &= \tau(\alpha') = \tau(\alpha^3(x + y\sqrt{2})^{-1}) = \alpha'^3(x - y\sqrt{2}\,i)^{-1}\\ &= \alpha^9(x + y\sqrt{2})^{-3}(x - y\sqrt{2}\,i)^{-1} = \alpha p(x + y\sqrt{2}\,i)^{-1}(x - y\sqrt{2}\,i)^{-1} = \alpha.\end{aligned}$$

(Recall that $\alpha^8 = A = p(x + y\sqrt{2}\,i)^2$.) So $\tau^2 = 1$. For the second condition $\tau\sigma(\zeta) = \tau(\zeta) = \zeta^3$ and $\sigma\tau(\zeta) = \sigma(\zeta^3) = \zeta^3$. Also

$$\begin{aligned}\tau\sigma(\alpha) &= \tau(\zeta\alpha) = \zeta^3\alpha' = \zeta^3\alpha^3(x + y\sqrt{2}\,i)^{-1},\\ \sigma\tau(\alpha) &= \sigma(\alpha') = \sigma(\alpha^3(x + y\sqrt{2}\,i)^{-1}) = \zeta^3\alpha^3(x + y\sqrt{2}\,i)^{-1}.\end{aligned}$$

So $\tau\sigma = \sigma\tau$. Finally, the third condition follows from the fact that $\tau(\zeta) \neq \zeta$ so $\tau \notin \mathrm{Gal}(L/E) = \langle\sigma\rangle$. ∎

We define $\chi : \mathrm{Gal}(L/F) \to \mu_8$ by $\sigma^k\tau_l \mapsto \zeta^k$. As in §1, $\chi(\phi) = \phi(\alpha)/\alpha$ if $\phi \in \langle\sigma\rangle = \mathrm{Gal}(L/E)$.

Since $\left(\frac{2}{p}\right) = -1$ we see that p is inert in F. Let $\mathfrak{p}$ be the prime of F over p. Since $\left(\frac{-2}{p}\right) = 1$ we infer that -2 is a square in $\mathbb{Q}_p$ and so in $F_\mathfrak{p}$. Thus $\mathfrak{p}$ splits in E. Since $(x + y\sqrt{2}\,i)(x - y\sqrt{2}\,i) = p$ each of $x \pm y\sqrt{2}\,i$ belongs to one of the two primes of E over $\mathfrak{p}$. We denote by $\mathfrak{P}$ the prime of E over p such that $x - y\sqrt{2}\,i \in \mathfrak{P}$.

By the same proof as for Lemma 1.4(i) (with α instead of α_1) we get $\chi\big(\big(\frac{\varepsilon, L/F}{\mathfrak{p}}\big)\big) \equiv \varepsilon^{-(p^2-1)/8} \pmod{\mathfrak{P}}$ and then we follow the same reasoning as in the case $d > 2$.

We have $\chi\big(\big(\frac{\varepsilon, L/F}{\mathfrak{p}}\big)\big) \in \mu_8$ so it has the form α, βi or $(\alpha + \beta i)/\sqrt{2}$ with $\alpha, \beta = \pm 1$. The value of $\varepsilon^{-(p^2-1)/8} \bmod p$ can be found from $\varepsilon^{-(p^2-1)/8} \bmod \mathfrak{P}$ by using the following lemma.

LEMMA 3.2. *Let s, t be p-adic integers and $\alpha, \beta \in \{\pm 1\}$.*

(i) *If $s + t\sqrt{2} \equiv \alpha \pmod{\widetilde{\mathfrak{P}}}$ then $s \equiv \alpha \pmod p$ and $t \equiv 0 \pmod p$.*
(ii) *If $s + t\sqrt{2} \equiv \beta i \pmod{\widetilde{\mathfrak{P}}}$ then $s \equiv 0 \pmod p$ and $t \equiv -\beta\frac{y}{x} \pmod p$.*
(iii) *If $s + t\sqrt{2} \equiv \frac{\alpha+\beta i}{\sqrt{2}} \pmod{\widetilde{\mathfrak{P}}}$ then $s \equiv -\beta\frac{y}{x} \pmod p$ and $t \equiv \frac{1}{2}\alpha \pmod p$.*

Proof. We have $x - y\sqrt{2}\,i \in \widetilde{\mathfrak{P}}$ so $x \equiv y\sqrt{2}\,i \pmod{\widetilde{\mathfrak{P}}}$. Since $p \nmid xy$ we get $i \equiv -\frac{y}{x}\sqrt{2} \pmod{\widetilde{\mathfrak{P}}}$ and $\frac{i}{\sqrt{2}} \equiv -\frac{y}{x} \pmod{\widetilde{\mathfrak{P}}}$. It follows that $\beta i \equiv -\beta\frac{y}{x}\sqrt{2} \pmod{\widetilde{\mathfrak{P}}}$ and

$$\frac{\alpha + \beta i}{\sqrt{2}} = \frac{1}{2}\alpha\sqrt{2} + \beta\frac{i}{\sqrt{2}} \equiv \frac{1}{2}\alpha\sqrt{2} - \beta\frac{y}{x} \pmod{\widetilde{\mathfrak{P}}}.$$

Therefore the congruences from the hypotheses of (i)–(iii) can be written as $s + t\sqrt{2} \equiv \alpha$, $-\beta\frac{y}{x}\sqrt{2}$ or $-\beta\frac{y}{x} + \frac{1}{2}\alpha\sqrt{2} \pmod{\widetilde{\mathfrak{P}}}$, respectively. Since both sides of these congruences belong to $F_\mathfrak{p}$ they will also hold modulo $\widetilde{\mathfrak{p}}$. ∎

References

[G] R. K. Guy, *Unsolved Problems in Number Theory*, 2nd ed., Springer, New York, 1994.

[L] F. Lemmermeyer, *Reciprocity Laws*: *From Euler to Eisenstein*, Springer, Berlin, 2000.

[S1] Z. H. Sun, *Values of Lucas sequences modulo primes*, Rocky Mountain J. Math. 33 (2003), 1123–1145.

[S2] Z. H. Sun, *Quartic, octic residues and Lucas sequences*, preprint.
[SS] Z. H. Sun and Z. W. Sun, *Fibonacci numbers and Fermat's last theorem*, Acta Arith. 60 (1992), 371–388.

Institute of Mathematics "Simion Stoilow"
of the Romanian Academy
21 Calea Grivitei St.
010702 Bucureşti, Sector 1, Romania
E-mail: Constantin.Beli@imar.ro, raspopitu1@yahoo.com

Received on 9.4.2007
and in revised form on 1.10.2008 (5428)