On attaching coordinates of Gaussian prime torsion points of $y^2 = x^3 + x$ to $\mathbb{Q}(i)$

Gordan Savin and David Quarfoot

March 29, 2010

1 Background

One of the natural questions that arises in the study of abstract algebra is to describe all the abelian extensions of $\mathbb{Q}$. The celebrated Kronecker-Weber Theorem largely answers this question by proving that any finite abelian extension of $\mathbb{Q}$ is contained in some cyclotomic extension, $\mathbb{Q}(\zeta_n)$, where n depends on the given extension. Thus, by understanding cyclotomic extensions, which are a managable and simpler set of objects, one, in effect, understands all finite abelian extensions of $\mathbb{Q}$.

Perhaps the next most natural base field to consider is $\mathbb{Q}(i)$. In asking the same question, one again is met with a pleasant, albeit more complicated, result. We have:

Theorem 1.1. *Let $C : y^2 = x^3 + x$ and $F/\mathbb{Q}(i)$ be any finite abelian extension. Then, there exists $n \geq 1$ such that $F \subset \mathbb{Q}(i)(C[n])$ where $C[n]$ is the collection of x and y coordinates of the n-torsion (nonidentity) points on C.*

While these results may seem markedly different at first, when viewed under the right lens, they are quite similar. In the first case, if we define $\lambda_n : \mathbb{C}^\times \to \mathbb{C}^\times$ by $\lambda_n(z) = z^n$, then the cyclotomic extension $\mathbb{Q}(\zeta_n) = \mathbb{Q}(\ker(\lambda_n))$. Likewise, in the second setting, define $\lambda_n : C \to C$ via $\lambda_n(P) = nP$, and we see that the above theorem states $F \subset \mathbb{Q}(i)(\ker(\lambda_n))$. So, in both cases, we may encapsulate any finite abelian extension of our base field in a composite of our base field and the kernel of a certain map on a certain space.

In the case of extensions of $\mathbb{Q}$, one may define an injective homomorphism $\rho : (\mathbb{Z}/n\mathbb{Z})^\times \to Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ via the rule $\rho(\bar{a}) = \sigma_a$ where $\sigma_a : \mathbb{Q}(\zeta_n) \to \mathbb{Q}(\zeta_n)$ via $\sigma_a(\zeta_n) = \zeta_n^a$. Showing this map is onto, however, requires knowing that the nth cyclotomic polynomial is irreducible over $\mathbb{Q}$, which, in the case of $n = p$, a prime, is seen readily through Eisenstein's criterion with an index shift trick. This results implies $|Gal(\mathbb{Q}(\zeta_p)/\mathbb{Q})| = [\mathbb{Q}(\zeta_p) : \mathbb{Q}] = \varphi(p) = p - 1$. In the material to follow, we work to derive analogies of these results in the more complex setting of abelian extensions of $\mathbb{Q}(i)$.

2 Set Up

We begin by defining a collection of polynomials $\psi_n \in \mathbb{Z}[x, y]$ based on the curve $C : y^2 = x^3 + x$ via the following recursive definitions:

$$\psi_0 = 1, \psi_1 = 1, \psi_2 = 2y, \psi_3 = 3x^4 + 6x^2 - 1, \psi_4 = 2y(2x^6 + 10x^4 - 10x^2 - 2)$$
$$\psi_{2n+1} = \psi_{n+2}\psi_n^3 - \psi_{n-1}\psi_{n+1}^3, n \geq 2$$
$$2y\psi_{2n} = \psi_n(\psi_{n+2}\psi_{n-1}^2 - \psi_{n-2}\psi_{n+1}^2), n \geq 3$$

In addition, we define the polynomials:

$$\varphi_n = x\psi_n^2 - \psi_{n+1}\psi_{n-1}, n \geq 2$$

$$4y\omega_n = \psi_{n+2}\psi_{n-1}^2 - \psi_{n-2}\psi_{n+1}^2, n \geq 2$$

The most important properties of these polynomials, which were proved in the last submitted homework set, are the following:

Lemma 2.1. *Given the above setup:*
(a) All the $\psi_n, \varphi_n, \omega_n$ are in $\mathbb{Z}[x, y]$.
(b) If n is odd, $\psi_n, \varphi_n, y^{-1}\omega_n$ are in $\mathbb{Z}[x, y^2]$. If n is even, then $(2y)^{-1}\psi_n, \varphi_n, \omega_n$ are in $\mathbb{Z}[x, y^2]$. In these cases, we may replace y^2 with $x^3 + x$ and get a polynomial just in x.
(c) As polynomials in x, we have that:

$$\varphi_n(x) = x^{n^2} + \textit{lower degree terms}$$
$$\psi_n(x)^2 = n^2 x^{n^2-1} + \textit{lower degree terms}$$

(d) For any $P = (x, y) \in C$, we have $nP = \left(\frac{\varphi_n(P)}{\psi_n(P)^2}, \frac{\omega_n(P)}{\psi_n(P)^3}\right)$.
(e) If $P = (x, y) \in C(\mathbb{C})$, then nP is the identity if and only if $\psi_n(x)^2 = 0$.

A computer program readily finds these polynomials for small values of n:

$\psi_1(x) = 1$

$\psi_2(x) = 2y$

$\psi_3(x) = 3x^4 + 6x^2 - 1$

$\psi_4(x) = (2y)(2x^6 + 10x^4 - 10x^2 - 2)$

$\psi_5(x) = 5x^{12} + 62x^{10} - 105x^8 - 300x^6 - 125x^4 - 50x^2 + 1$

$\psi_6(x) = (2y)(3x^{16} + 72x^{14} - 364x^{12} - 1288x^{10} - 942x^8 - 1288x^6 - 364x^4 + 72x^2 + 3)$

$\psi_7(x) = 7x^{24} + 308x^{22} - 2954x^{20} - 19852x^{18} - 35231x^{16} - 82264x^{14} - 111916x^{12} - 42168x^{10} + 15673x^8 + 14756x^6 + 1302x^4 + 196x^2 - 1$

...

$\psi_{11}(x) = 11x^{60} + 2794x^{58} - 207691x^{56} - 5092956x^{54} - 28366041x^{52} - 815789634x^{50} - 5391243935x^{48} - 7864445336x^{46} + 50897017743x^{44} + 387221579866x^{42} + 1197743580033x^{40} + 2175830922716x^{38} + 3223489742187x^{36} + 5384207244702x^{34} + 8608181312269x^{32} + 9712525647792x^{30} + 6610669151537x^{28} + 1890240552750x^{26} - 1084042069649x^{24} -$

$1642552094436x^{22} - 948497199067x^{20} - 291359180310x^{18} - 57392757037x^{16} -$
$14323974808x^{14} - 3974726283x^{12} - 385382514x^{10} - 5093605x^{8} +$
$2923492x^{6} + 33033x^{4} + 1210x^{2} - 1$

...

$\psi_{13}(x) = 13x^{84} + 6370x^{82} - 966771x^{80} - 40172008x^{78} - 302574974x^{76} - 25746637540x^{74} -$
$256749753910x^{72} - 58238066536x^{70} + 13732966612261x^{68} + 154178038516762x^{66} +$
$785812055225821x^{64} + 2479277700934112x^{62} + 7665898221693816x^{60} + 29291279621875024x^{58} +$
$99093094080008600x^{56} + 234510906536697440x^{54} + 360106370579869018x^{52} +$
$292227204652497764x^{50} - 150573378043884614x^{48} - 968698282925133488x^{46} -$
$1823536524411131348x^{44} - 2182258606767553496x^{42} - 1860316858105594980x^{40} -$
$1248291077679739184x^{38} - 797540307628030798x^{36} - 562197483577820636x^{34} -$
$380108964428406590x^{32} - 197635149662855840x^{30} - 68542512916164040x^{28} -$
$12834604373175472x^{26} + 726553759796696x^{24} + 1469150719590112x^{22} +$
$534618582761913x^{20} + 94168981334714x^{18} + 8722781334553x^{16} + 894973190488x^{14} +$
$179986452386x^{12} + 10357000732x^{10} + 168733994x^{8} - 21130408x^{6} - 113399x^{4} - 2366x^{2} + 1$

3 Irreducibility Results

In analyzing the extension degrees created by attaching the coordinates of torsion points, we proceed in two cases. First, let p be a prime with $p \equiv 3(4)$, so p remains prime in $\mathbb{Z}[i]$ Here we claim that the polynomial ψ_p is irreducible over $\mathbb{Q}[i]$. Since $(p) \subset \mathbb{Z}[i]$ is a prime ideal, we aim to use Eisenstein's criterion on the coefficients of ψ_p. One may show via induction that the constant term of $\psi_n(x)$ is ± 1 if n is odd. Thus, if some nonconstant coefficient of ψ_p is not divisible by p, then reducing this polynomial mod p produces a nonconstant polynomial which will have a root in some extension of $\mathbb{F}_p$, say $\mathbb{F}_{p^k}$. This root provides a p-torsion point, thus showing that p divides $|E_{p^k}|$, where E_{p^k} is the group of points on $y^2 = x^3 + x$ in $\mathbb{F}_{p^k}$. The size of this group is well known (see Koblitz pp. 40 and 61, e.g.). If k is odd, then $p^k \equiv 3(4)$, and so $|E_{p^k}| = p^k + 1$, and since $p \not| p^k + 1$, we have a contradiction. (Note: while Koblitz examines $|E_{p^k}|$ for $y^2 = x^3 - n^2 x$, his proof requires only that y^2 equals an odd function, thus applying to our elliptic curve.) If k is even, we have that $|E_{p^k}| = p^k + 1 - \alpha^{k/2} - \bar{\alpha}^{k/2}$ where α is a Gaussian integer of norm p^2 satisfying a certain congruence condition. Given the only possibilities for α are $p, ip, -p, -ip$, we again have a contradiction in all cases. (Again, slight alterations are needed in Koblitz's proof which deals with the curve $y^2 = x^3 - n^2 x$.) These results are immediately seen in the cases of ψ_3 and ψ_7 listed above, where all the nonconstant terms are divisible by 3 and 7 respectively.

In the case of p prime with $p \equiv 1(4)$, we know that p does not remain prime in $\mathbb{Z}[i]$, and we may write $p = \pi\bar{\pi}$ where $\pi = a + bi$ with $a^2 + b^2 = p$. In this case, the polynomial ψ_p will not be irreducible, and will have, as two of its irreducible factors, the polynomials ψ_π and $\psi_{\bar{\pi}}$, which represent the polynomials in x whose roots are the x-coordinates of the π-torsion (resp. $\bar{\pi}$-torsion) points on C. To find a formula for ψ_π observe that if $(a + bi)P$ equals the identity, then $-bi(x, y) = a(x, y)$. Since we are working over $\mathbb{Q}(i)$, we know that multiplication by i and the addition-b-times homomorphism commute (p. 205, Silverman and Tate). Thus, $a(x, y) = ib(x, -y)$, and so, using the complex multiplication of $y^2 = x^3 + x$

(one of the reasons this curve is the focus of our attention), we have

$$\left(\frac{\varphi_a(x,y)}{\psi_a(x,y)^2}, \frac{\omega_a(x,y)}{\psi_a(x,y)^3}\right) = \left(-\frac{\varphi_b(x,-y)}{\psi_b(x,-y)^2}, -i\frac{\omega_b(x,-y)}{\psi_b(x,-y)^3}\right).$$

We focus our attention on the x-coordinates of this expression, for if these agree, then the y-coordinates will agree or differ by a minus sign (a situation addressed below). Next, observe that since the φ's and ψ^2's are polynomials only in x, we may ignore the y (or $-y$) input. In addition, note that if $\psi_b(x) = 0$, then we have that $\text{ord}(x,y)|b$. Since $(a+bi)(x,y)$ is the identity, then so is $a(x,y)$, and thus $\text{ord}(x,y)|a$. Given that $a^2+b^2 = p$, we must have $\text{ord}(x,y) = 1$, a case we can ignore, since the roots of the ψ polynomials are precisely for nonidentity points. Thus, we may assume that both $\psi_a(x)^2$ and $\psi_b(x)^2$ are nonzero, and thus cross-multiply the first coordinates of the above expression to obtain $\Phi = \varphi_a\psi_b^2 + \varphi_b\psi_a^2 = 0$. Part ($c$) of the above lemma reveals that the leading term of Φ is $x^{a^2}b^2x^{b^2-1} + x^{b^2}a^2x^{a^2-1} = (b^2+a^2)x^{a^2+b^2-1} = px^{p-1}$.

Now, not every root of $\Phi(x)$ corresponds to a π-torsion point, for, as noted above, it is possible that the x-coordinates of the critical equation agree, but not the y-coordinates. In the case they do agree, we see (x,y) is π-torsion. If not, then starting the calculation with $a-bi$ instead of $a+bi$ yields an identical relation in the first coordinate, and an extra minus sign in the second coordinate. This shows that each root of $\Phi(x)$ either corresponds to a π-torsion point or a $\bar{\pi}$-torsion point. In addition, for a fixed pair (x,y) we know: (x,y) is π-torsion $\Leftrightarrow$ $(x,-y)$ is π-torsion $\Leftrightarrow$ $(\bar{x},\bar{y})$ is $\bar{\pi}$-torsion $\Leftrightarrow$ $(\bar{x},-\bar{y})$ is $\bar{\pi}$-torsion. Thus we have an equal number of π and $\bar{\pi}$-torsion points, and so we may write $\Phi(x) = \psi_\pi(x)\psi_{\bar{\pi}}(x)$ where the leading coefficient of ψ_π is $\eta x^{(p-1)/2}$ and for $\psi_{\bar{\pi}}$ we have $\epsilon x^{(p-1)/2}$ where $\eta\epsilon = p$.

We now show that ψ_π is Eisenstein in the Gaussian prime π. This will imply that $\pi|\eta$, and a similar argument shows $\bar{\pi}|\epsilon$. Since $\eta\epsilon = p$, we know $\eta = \pi$, up to associates, and thus have a clearer picture of ψ_π. Before proceeding, we observe two things. First, since ψ_p has ± 1 as a constant term, ψ_π will have some unit of $\mathbb{Z}[i]$ as its constant term. In particular, it has a nonzero constant term. Second, if we factor $\psi_\pi(x)$ over $\mathbb{C}$ (not over $\mathbb{Q}(i)$), we may write the factorization as $\eta\prod(x-a_i)$, where the a_i's are the roots of ψ_π. Given the above relationship between π and $\bar{\pi}$-torsion points, we see that $\psi_{\bar{\pi}}$ must factor as $\epsilon\prod(x-\bar{a}_i)$.

For the irreducibility, we proceed by contradiction: if π does not divide each nonconstant term in ψ_π, then we get a π-torsion point mod π, i.e. in $\mathbb{Z}[i]/(\pi) \cong \mathbb{F}_p$. But noting the factorizations of ψ_π and $\psi_{\bar{\pi}}$, we also get a $\bar{\pi}$-torsion point mod $\bar{\pi}$. These two torsion points generate a total of p^2-1 nonidentity p-torsion points mod p, an impossibility given that the reduction of ψ_p mod p has degree less than $(p^2-1)/2$ (note: each x value gives rise to two y values) since its leading coefficient is divisible by p from the above lemma. This shows the irreducibility and confirms the leading coefficients of ψ_π and $\psi_{\bar{\pi}}$. Thus, we know that $\psi_p = \psi_\pi \cdot \psi_{\bar{\pi}} \cdot \text{another polynomial} = (\pi x^{(p-1)/2}+\ldots)(\bar{\pi}x^{(p-1)/2}+\ldots)(x^{(p-1)^2/2}+\ldots)$. Indeed, using Mathematica, we may factor our above expressions for $\psi_5(x)$ and $\psi_{13}(x)$ over $\mathbb{Q}[i]$. We have:

$$\begin{aligned}\psi_5(x) = {} & ((1+2i)x^2+1)\cdot \\ & ((1-2i)x^2+1)\cdot \\ & (x^8+12x^6-26x^4-52x^2+1).\end{aligned}$$

$$
\begin{aligned}
\psi_{13}(x) = &((2+3i)x^6 + (4-7i)x^4 + (10-11i)x^2 - i)\cdot \\
&((2-3i)x^6 + (4+7i)x^4 + (10+11i)x^2 + i)\cdot \\
&(x^{72} + 492x^{70} - 73386x^{68} + \ldots + 1).
\end{aligned}
$$

(Note that, for example: $4+7i = (2-3i)(-1+2i)$ and $10+11i = (2-3i)(-1+4i)$.)

4 Conclusion

We are now in a position to prove our main result.

Theorem 4.1. *Let $\omega \in \mathbb{Z}[i]$ be prime. Let K_ω be the field obtained by adjoining the x and y-coordinates of the nonidentity ω-torsion points on the elliptic curve $C : y^2 = x^3 + x$ to the base field $\mathbb{Q}(i)$. Then, $[K_\omega : \mathbb{Q}(i)] = N(\omega) - 1$, where N is the norm function on $\mathbb{Z}[i]$.*

Proof: We begin with the case $\omega = 1+i$ (its associates follow similarly). If $(1+i)P$ is the identity, then we find that $(x, y) = (-x, -iy)$, so $(x, y) = (0, 0)$. Since this is the only nonidentity torsion point, we have $K_\omega = \mathbb{Q}(i)$, and thus $[K_\omega : \mathbb{Q}(i)] = 1 = N(1+i) - 1$.

For the other cases, note first that attaching all the x and y-coordinates is the same as attaching a single pair, for the collection of ω torsion points, E_ω, is isomorphic to $\mathbb{Z}[i]/(\omega)$ as a $\mathbb{Z}[i]$ module. So, we may set $E_\omega = \mathbb{Z}[i] \cdot P$ where $P = (x, y)$ is the point we focus on adjoining to $\mathbb{Q}(i)$. Now, observe that adjoining y to $\mathbb{Q}(i, x)$ creates a degree 2 extension because of the following observations. First, $y^2 = x^3 + x$, so the extension is of degree at most 2. Second, note that the homomorphism sending $(x, y) \to (x, -y)$ on C gives rise to a element of $Gal(K_\omega/\mathbb{Q}(i))$ that fixes x but not y. (Note: We can be sure that $(x, y) \neq (x, -y)$, because if not, then $y = 0$, and we are not in the case of points whose order divides 2.) We now proceed in two cases, using the irreducibility results from above:

Case 1: $\omega = p \equiv 3(4)$
We have: $[K_\omega : \mathbb{Q}(i)] = [\mathbb{Q}(i, x, y) : \mathbb{Q}(i, x)] \cdot [\mathbb{Q}(i, x) : \mathbb{Q}(i)] = 2 \cdot \dfrac{p^2 - 1}{2} = N(\omega) - 1.$

Case 2: $\omega = a + bi$ where $N(\omega) = p \equiv 1(4)$
We have: $[K_\omega : \mathbb{Q}(i)] = [\mathbb{Q}(i, x, y) : \mathbb{Q}(i, x)] \cdot [\mathbb{Q}(i, x) : \mathbb{Q}(i)] = 2 \cdot \dfrac{p - 1}{2} = N(\omega) - 1.$ □

Finally, observe that this theorem generalizes the case of adjoining the roots of the equation $x^p - 1 = 0$ to the base field $\mathbb{Q}$. In this setting, as above, one must only adjoin a single x-value, ζ_p, and the irreducibility of Φ_p shows $[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p - 1 = N(p) - 1$, where $N(p) = |p|$ is the norm function on $\mathbb{Z}$.