Rational points on algebraic curves
Lecture V, March 19, 1999

Ed Schaefer, Santa Clara University

Abstract:

In this last talk, we solve the three motivating problems. To finish the proof that the only integers that are simultaneously the product of two and of three consecutive integers, requires showing that the Mordell-Weil rank of the associated elliptic curve is 1. The second problem is to find the longest sequence of squares in arithmetic progression. The third problem is to say what we can about solutions of the equation $y^2 = x^5 + 1$ in number fields.

REVIEW

Let C be defined by the equation $y^q = f(x)$, over the number field K, which contains the qth roots of unity. We assume that q is prime and that $f(x) \in \mathcal{O}_K[X]$ is monic, separable, and $q \not| d$, the degree of f. The genus is $(q-1)(d-1)/2$. Let $\phi = 1-\zeta_q$ and $L = K[T]/(f(T))$. We have

$$\begin{array}{ccccc} J(K)/\phi J(K) & \stackrel{x-T}{\hookrightarrow} & \ker : L(S,q) & \stackrel{\text{norm}}{\to} & K^*/K^{*q} \\ \downarrow & & \downarrow & & \\ \prod_{\mathfrak{p}\in S} J(K_\mathfrak{p})/\phi J(K_\mathfrak{p}) & \stackrel{x-T}{\hookrightarrow} & \prod_{\mathfrak{p}\in S} L_\mathfrak{p}^*/L_\mathfrak{p}^{*q} & & \end{array}$$

where $L(S,q)$ is the subgroup of L^*/L^{*q} unramified outside $S = \{\mathfrak{p}|q, \mathfrak{p}|\Delta f, \mathfrak{p} = \infty \text{ if } q = 2\}$. We let $L_\mathfrak{p} = L \otimes_K K_\mathfrak{p}$.

Proposition. If $C : y^2 = f(x)/\mathbf{R}$, then $\dim J(\mathbf{R})/2J(\mathbf{R}) = \dim J(\mathbf{R})[2] - g$.

FIRST PROBLEM.

When is the product of two consecutive integers equal to the product of three consecutive integers? We use the elliptic curve $v^2+v = u^3-u/\mathbf{Q}$. It remains to show that $E(\mathbf{Q}) \cong \mathbf{Z}$ and $(u,v) = (0,0)$ generates. We have already shown that $E(\mathbf{Q})_{\text{tors}} = 0$. We change equations so that it is of the form $y^2 = f(x)$ and get $E : y^2 = x^3 - 16x + 16$ where $y = 8v + 4, x = 4u$. We have $q = 2$, and $\phi = 1 - (-1) = 2$.

Drawing this elliptic curve, we see that the three points of order 2 are the points on the line $y = 0$. They all have real coordinates. Let $L = \mathbf{Q}[T]/(T^3 - 16T + 16)$. It is a number field. It is isomorphic to the field of definition of any one of the 2-torsion points. We have $S = \{\infty, 2, 37\}$ and

$$\begin{array}{ccccc} E(\mathbf{Q})/2E(\mathbf{Q}) & \stackrel{x-T}{\hookrightarrow} & \ker : L(S,2) & \stackrel{\text{norm}}{\to} & \mathbf{Q}^*/\mathbf{Q}^{*2} \\ \downarrow & & \downarrow \prod \beta_p & & \\ \prod_{p=\infty,2,37} E(\mathbf{Q}_p)/2E(\mathbf{Q}_p) & \stackrel{x-T}{\hookrightarrow} & \prod_{p=\infty,2,37} L_p^*/L_p^{*2}. & & \end{array}$$

First let us describe $\ker : L(S,2) \stackrel{\text{norm}}{\to} \mathbf{Q}^*/\mathbf{Q}^{*2}$. The field L has class number 1. It is totally real and so has unit rank 2. The unit group is generated by $-1, \frac{T}{2} - 1$, and $\frac{T^2}{4} + T - 1$. We have the following factorizations of the ideals generated by 2 and 37: $(2) = (\frac{T}{2})^3, (37) = (3 + T)(27T^2 - \frac{227T}{2} + 91)^2$. Therefore, $L(S,2) = \langle -1, \frac{T}{2} - 1, \frac{T^2}{4} + T - 1, \frac{T}{2}, 3 + T, 27T^2 - \frac{227T}{2} + 91\rangle$. The norms of those elements are $-1, 1, -1, -2, -37, 37$, respectively. Since $(-1)(3 + T)(27T^2 - \frac{227T}{2} + 91)^2) = \frac{65T^2}{2} - \frac{365T}{2} + 159$, the kernel of the norm is $\langle \frac{T}{2}-1, -\frac{T^2}{4}-T+1, \frac{65T^2}{2}-\frac{365T}{2}+159\rangle$. For brevity, we will rename those $\langle \alpha_1, \alpha_2, \alpha_3\rangle$, respectively.

For simplicity, since there will be no obstruction in finding $E(\mathbf{Q})/2E(\mathbf{Q})$, we will not talk in terms of Selmer groups, but instead, find $E(\mathbf{Q})/2E(\mathbf{Q})$ directly. We will do the same in the remaining two examples.

Recall there is the rational point $(0,0)$ on $v^2+v=u^3-u$. That is $(x,y)=(0,4)$. Recall $E\cong \mathrm{Jac}(E)$ by $P\mapsto [P-\mathcal{O}]$. We will now replace E by its Jacobian, and by abuse of notation we write $[(0,4)-\mathcal{O}]\in E(\mathbf{Q})$. We have $(x-T)[(0,4)-\infty]=-T\equiv \alpha_2 \bmod L^{*2}$. So $\langle\alpha_2\rangle \subset (x-T)(E(\mathbf{Q})/2E(\mathbf{Q}))\subset \langle \alpha_1,\alpha_2,\alpha_3\rangle$.

Now $\dim E(\mathbf{R})/2E(\mathbf{R}) = \dim E(\mathbf{R})[2]-g=2-1=1$. We have

$$L_\infty = \frac{\mathbf{R}[T]}{(T^3-16T+16)} \cong \frac{\mathbf{R}[T]}{(T+4.4)} \oplus \frac{\mathbf{R}[T]}{(T-1.1)} \oplus \frac{\mathbf{R}[T]}{(T-3.4)} \cong \mathbf{R}\oplus\mathbf{R}\oplus\mathbf{R}$$

where $T\mapsto (T,T,T)\mapsto(-4.4,1.1,3.4)$. So $L_\infty^*/L_\infty^{*2}\cong(\mathbf{R}^*/\mathbf{R}^{*2})^3=\langle -1\rangle^3$. We have

$$\begin{array}{rcccc} E(\mathbf{R})/2E(\mathbf{R}) \hookrightarrow & L_\infty^*/L_\infty^{*2} \cong \mathbf{R}^*/\mathbf{R}^{*2} & \oplus\mathbf{R}^*/\mathbf{R}^{*2} & \oplus\mathbf{R}^*/\mathbf{R}^{*2} \\ \text{by} & x+4.4 & x-1.1 & x-3.4 \\ [(0,4)-\infty]\mapsto & 4.4\equiv 1 & -1.1\equiv -1 & -3.4\equiv -1. \end{array}$$

Since the image of $[(0,4)-\infty]$ is non-trivial, this divisor class generates $E(\mathbf{R})/2E(\mathbf{R})$.

Let us consider the map β_∞.

$$\begin{array}{rccc} L^*/L^{*2}\mapsto & \mathbf{R}^*/\mathbf{R}^{*2} & \oplus\mathbf{R}^*/\mathbf{R}^{*2} & \oplus\mathbf{R}^*/\mathbf{R}^{*2} \\ T\mapsto & -4.4 & 1.1 & 3.4 \\ \alpha_1=\frac{T}{2}-1\mapsto & -1 & -1 & 1 \\ \alpha_2\mapsto & 1 & -1 & -1 \\ \alpha_3\mapsto & 1 & -1 & -1 \end{array}$$

We see that $\beta_\infty(\alpha_1)\not\subset (x-T)(E(\mathbf{R})/2E(\mathbf{R}))$. Thus $(x-T)(E(\mathbf{Q})/2E(\mathbf{Q}))\subset\langle\alpha_2,\alpha_3\rangle$.

Since L_2 is a cubic, totally ramified extension of $\mathbf{Q}_2$, $\dim E(\mathbf{Q}_2)[2]=0$. Thus $\dim E(\mathbf{Q}_2)/2E(\mathbf{Q}_2)=g[\mathbf{Q}_2:\mathbf{Q}_2(\mu_2)]+\dim E(\mathbf{Q}_2)[2]=1$.

$$\begin{array}{rc} E(\mathbf{Q}_2)/2E(\mathbf{Q}_2) \overset{x-T}{\hookrightarrow} & L_2^*/L_2^{*2} \\ [(0,4)-\mathcal{O}]\mapsto & -T=\alpha_2\notin L_2^{*2} \end{array}$$

So $[(0,4)-\mathcal{O}]$ generates $E(\mathbf{Q}_2)/2E(\mathbf{Q}_2)$ and the image is generated by α_2. Now $\alpha_3\neq 1,\alpha_2 \bmod L_2^{*2}$, thus $\langle\alpha_2\rangle\subset(x-T)(E(\mathbf{Q})/2E(\mathbf{Q}))\subset\langle\alpha_2\rangle$ and $\dim E(\mathbf{Q})/2E(\mathbf{Q})=1$. Since $E(\mathbf{Q})_{\mathrm{tors}}=0$, we have $E(\mathbf{Q})\cong\mathbf{Z}$. We do not even need to check at the prime 37.

Lastly we must show that $P=(u,v)=(0,0)$ generates $E(\mathbf{Q})$. I will sketch the proof as we have not yet developed the tools for this. Since the non-identity component of $E(\mathbf{R})$ contains rational points, the generator must be on the non-identity component. Recall that we proved in the first lecture, that if R is a rational, non-integer point, then $2R$ is also. This is true for any multiple, not just doubles. Thus, since there are rational integer points, the generator must be an integer point. The only integer points on the non-identity component are $\pm P, \pm 3P$. Thus P generates $E(\mathbf{Q})$.

SECOND PROBLEM.

The integers $1, 25, 49$ are squares in arithmetic progression. How long can such a sequence be? Let A^2, B^2, C^2, D^2 be integer squares in arithmetic progression. Then $A^2+C^2=2B^2$

and $B^2 + D^2 = 2C^2$. This is an intersection of two surfaces in $\mathbf{P}^3$. It is a curve of genus 1 with a rational point, so it is an elliptic curve over $\mathbf{Q}$. There are eight trivial rational points $[\pm 1 : 1 : \pm 1 : \pm 1]$ (corresponding to the four squares being the same).

We would like to write the curve as y^2 =cubic. We first dehomogenize with respect to B. Let $a = A/B, c = C/B, d = D/B$. Then we have $a^2 + c^2 = 2, 1 + d^2 = 2c^2$. We need to remove a variable, in order to get a plane curve. We do this by parametrizing $a^2 + c^2 = 2$. The other point of intersection of the line with slope m through $(a, c) = (1, -1)$ is

$$(a, c) = \left(\frac{m^2 + 2m - 1}{m^2 + 1}, \frac{m^2 - 2m - 1}{m^2 + 1} \right).$$

This induces a bijection between rational points on $a^2 + c^2 = 2$ and rational slopes m. We replace c in $1 + d^2 = 2c^2$ and get

$$d^2(m^2 + 1)^2 = m^4 - 8m^3 + 2m^2 + 8m + 1$$

Let $v = d(m^2 + 1)$, then $v^2 = m^4 - 8m^3 + 2m^2 + 8m + 1$.

The following trick will get us an equation of the form y^2 =cubic. It works since the leading coefficient of the quartic polynomial in m is a square. We find a quadratic in m whose square agrees with the quartic polynomial at the highest three coefficients: $v^2 = (m^2 - 4m - 7)^2 - 48m - 48$.

$$\begin{aligned} \text{Let } t = &\ v + (m^2 - 4m - 7) \text{ then} \\ \tfrac{-48m-48}{t} = &\ v - (m^2 - 4m - 7). \end{aligned}$$

So

$$t - \left(\frac{-48m - 48}{t} \right) = 2(m^2 - 4m - 7)$$

Multiply both sides by t^2 and we get $t^3 + (48m + 48)t = 2t^2(m^2 - 4m - 7)$. Let $s = mt$ and we have $t^3 + 48s + 48t = 2s^2 - 8st - 14t^2$. We complete the square with respect to s and get $t^3 + 22t^2 + 144t + 288 = 2(s - (4t + 24))^2$. Let $t = 2x$ and $s - (4t + 24) = 2y$. Then we get $E : y^2 = (x + 2)(x + 3)(x + 6)$.

This induces isomorphism of curves over $\mathbf{Q}$. The eight trivial rational points map to $\mathcal{O}$, $(-2, 0), (-3, 0), (-6, 0), (0, \pm 6), (-4, \pm 2)$. These points form a subgroup of $E(\mathbf{Q})$ isomorphic to $\mathbf{Z}/4\mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z}$. We have $S = \{\infty, 2, 3\}$; so 5 and 7 are primes of good reduction of E. We have $\#E(\mathbf{F}_5) = 8$ and $\#E(\mathbf{F}_7) = 8$ so $\#E(\mathbf{Q})_{\text{tors}} = 8$.

$$L = \frac{\mathbf{Q}[T]}{((T + 2)(T + 3)(T + 6))} \cong \frac{\mathbf{Q}[T]}{(T + 2)} \oplus \frac{\mathbf{Q}[T]}{(T + 3)} \oplus \frac{\mathbf{Q}[T]}{(T + 6)} \cong \mathbf{Q} \oplus \mathbf{Q} \oplus \mathbf{Q}$$

by

$$T \mapsto (T, T, T) \mapsto (-2, -3, -6).$$

We also have $L^*/L^{*2} \cong (\mathbf{Q}^*/\mathbf{Q}^{*2})^3$. So $L(S, 2) \cong (\langle -1, 2, 3 \rangle \bmod \mathbf{Q}^{*2})^3$. The norm is the product of coordinates; so the kernel of the norm is those triples whose coordinate product is a square.

We have

$$\begin{array}{ccc} E(\mathbf{Q})/2E(\mathbf{Q}) & \overset{x-T}{\hookrightarrow} & \ker : \langle -1,2,3\rangle^3 \overset{\text{norm}}{\rightarrow} \mathbf{Q}^*/\mathbf{Q}^{*2} \\ \downarrow & & \downarrow \prod \beta_p \\ \prod_{p=\infty,2,3} E(\mathbf{Q}_p)/2E(\mathbf{Q}_p) & \overset{x-T}{\hookrightarrow} & \prod_{p=\infty,2,3} L_p^*/L_p^{*2}. \end{array}$$

Let us find the image of the known rational divisor classes. This gives a lower bound on $(x-T)(E(\mathbf{Q})/2E(\mathbf{Q}))$. We again replace E by degree 0 divisor classes.

$$\begin{array}{rccc} E(\mathbf{Q})/2E(\mathbf{Q}) \hookrightarrow & \langle -1,2,3\rangle & \oplus\langle -1,2,3\rangle & \oplus\langle -1,2,3\rangle \\ \text{by} & x+2 & x+3 & x+6 \\ [(0,6)-\mathcal{O}] \mapsto & 2 & 3 & 6 \\ [(-6,0)-\mathcal{O}] \mapsto & -1 & -3 & 3 \end{array}$$

Let us now work at the prime 2. We have $\dim E(\mathbf{Q}_2)/2E(\mathbf{Q}_2) = g[\mathbf{Q}_2 : \mathbf{Q}_2(\mu_2)] + \dim E(\mathbf{Q}_2)[2] = 1\cdot 1+2 = 3$. We also have $L_2 = \mathbf{Q}_2[T]/((T+2)(T+3)(T+6)) \cong \mathbf{Q}_2\oplus\mathbf{Q}_2\oplus\mathbf{Q}_2$ and $L_2^*/L_2^{*2} \cong \langle -1,2,3\rangle^3$. So β_2 is injective.

$$\begin{array}{rccc} E(\mathbf{Q}_2)/2E(\mathbf{Q}_2) \hookrightarrow & \langle -1,2,3\rangle & \oplus\langle -1,2,3\rangle & \oplus\langle -1,2,3\rangle \\ \text{by} & x+2 & x+3 & x+6 \\ [(0,6)-\mathcal{O}] \mapsto & 2 & 3 & 6 \\ [(-6,0)-\mathcal{O}] \mapsto & -1 & -3 & 3 \\ [(-3/4,\alpha)-\mathcal{O}] \mapsto & -3 & 1 & -3. \end{array}$$

So $\langle (2,3,6),(-1,-3,3)\rangle \subset (x-T)(E(\mathbf{Q})/2E(\mathbf{Q})) \subset \langle (2,3,6),(-1,-3,3),(-3,1,-3)\rangle$. Now $\dim E(\mathbf{R})/2E(\mathbf{R}) = \dim E(\mathbf{R})[2] - g = 2-1 = 1$. We have

$$\begin{array}{rccc} E(\mathbf{R})/2E(\mathbf{R}) \hookrightarrow & \langle -1\rangle & \oplus\langle -1\rangle & \oplus\langle -1\rangle \\ \text{by} & x+2 & x+3 & x+6 \\ [(-6,0)-\mathcal{O}] \mapsto & -1 & -1 & 1. \end{array}$$

So $(-3,1,-3) \notin (x-T)(E(\mathbf{Q})/2E(\mathbf{Q}))$. Thus $\dim E(\mathbf{Q})/2E(\mathbf{Q}) = 2$ and $E(\mathbf{Q})/2E(\mathbf{Q})$ is all torsion. Hence $\#E(\mathbf{Q}) = 8$. So there are no more rational points. If four integer squares are in arithmetic progression, then they are the same.

THIRD PROBLEM.

It has been known for a long time that the equation $y^2 = x^5+1$ has only trivial integer solutions $(-1,0)$, $(0,\pm 1)$. What can we say about other rational solutions and solutions in other number fields?

Let $C : y^2 = x^5 + 1/\mathbf{Q}$. Let J be its Jacobian and let $D = [(0,1)+(-1,0)-2\infty] \in J(\mathbf{Q})$. We have

$$\begin{array}{ll} D = [(0,1)+(-1,0)-2\infty], & 2D = [2(0,1)-2\infty], \\ 3D = [(1+i,1-2i)+(1-i,1+2i)-2\infty], & 4D = [(0,-1)+\infty-2\infty], \\ 5D = [(-1,0)+\infty-2\infty], & 6D = [(0,1)+\infty-2\infty], \\ 7D = [(1+i,-1+2i)+(1-i,-1-2i)-2\infty], & 8D = [2(0,-1)-2\infty], \\ 9D = [(0,-1)+(-1,0)-2\infty], & 10D = [2\infty-2\infty] = 0. \end{array}$$

We can get $2D$ from D by noting $\mathrm{div}(x+1) = 2(-1,0)-2\infty$. We showed $D+2D = 3D$ in the second lecture. Let us find $J(\mathbf{Q})_{\text{tors}}$. If p is a prime of good reduction of C then $\#J(\mathbf{F}_p) = 1/2(\#C(\mathbf{F}_p)^2 + \#C(\mathbf{F}_{p^2})) - p$. The only primes of bad reduction of C are 2 and 5. We have $\#J(\mathbf{F}_3) = 10$ and $\#J(\mathbf{F}_7) = 50$ so $J(\mathbf{Q})_{\text{tors}} \cong \mathbf{Z}/10\mathbf{Z}$. To find the Mordell-Weil rank of $J(\mathbf{Q})$, we can use the endomorphisms 2 or $1-\zeta_5$ of J. Since we have done two examples using the multiplication-by-2 map already, let us use $1-\zeta_5$.

We have $C: x^5=(y+1)(y-1)$. Let $\zeta=\zeta_5$ and $K=\mathbf{Q}(\zeta)$. Let $\phi=1-\zeta\in\mathrm{End}(J)$. We have $\dim J[\phi]=d-1=1$ and $J[\phi]=\langle[(0,1)-\infty]\rangle$. Let $\mathfrak{r}=1-\zeta\in K$ (a prime above 5). We have $S=\{2,\mathfrak{r}\}$ and $L=K[T]/((T+1)(T-1))\cong K\oplus K$ by $T\mapsto(-1,1)$. The field K has class number 1 and fundamental unit $1+\zeta$. So $L(S,5)=(\langle\zeta,1+\zeta,2,\mathfrak{r}\rangle \bmod K^{*5})^2$.

$$\begin{array}{ccc} J(K)/\phi J(K) & \overset{y-T}{\hookrightarrow} & \ker : L(S,5)\overset{\text{norm}}{\to} K^*/K^{*5} \\ \downarrow & & \downarrow \prod\beta_{\mathfrak{p}} \\ \prod_{\mathfrak{p}=2,\mathfrak{r}} J(K_{\mathfrak{p}})/\phi J(K_{\mathfrak{p}}) & \overset{y-T}{\hookrightarrow} & \prod_{\mathfrak{p}=2,\mathfrak{r}} L_{\mathfrak{p}}^*/L_{\mathfrak{p}}^{*5}. \end{array}$$

We have $\ker : L(S,5)\overset{\text{norm}}{\to} K^*/K^{*5}\cong\langle(\zeta,\zeta^4),\,(1+\zeta,(1+\zeta)^4),\,(2,16),\,(\mathfrak{r},\mathfrak{r}^4)\rangle$. Let us find the image of a known rational divisor class. This gives a lower bound on $(x-T)(J(K)/\phi J(K))$.

$$\begin{array}{rccc} J(K)/\phi J(K)\hookrightarrow & K^*/K^{*5} & \oplus K^*/K^{*5} \\ \text{by} & y+1 & y-1 \\ [(0,1)-\infty]\mapsto & 2 & 16 \end{array}$$

Now let us check at the prime $\mathfrak{r}$. We have $K_{\mathfrak{r}}^*/K_{\mathfrak{r}}^{*5}=\langle\mathfrak{r},1+\mathfrak{r},1+\mathfrak{r}^2,1+\mathfrak{r}^3,1+\mathfrak{r}^4,1+\mathfrak{r}^5\rangle$ $=\langle a,b,c,d,e,f\rangle$. Let us consider the map $\beta_{\mathfrak{r}}$. We have the following equivalence of vectors: $[\zeta,1+\zeta,2,\mathfrak{r}]\equiv[b^4c^4e^4,b^2c^4d^2e^4,e^3f,a] \bmod K_{\mathfrak{r}}^{*5}$.
Now $\dim J(K_{\mathfrak{r}})/\phi J(K_{\mathfrak{r}})=g\cdot[K_{\mathfrak{r}}:\mathbf{Q}_5(\zeta)]+\dim J(K_{\mathfrak{r}})[\phi]=2\cdot1+1=3$ and we have

$$\begin{array}{rccc} J(K_{\mathfrak{r}})/\phi J(K_{\mathfrak{r}})\hookrightarrow & L_{\mathfrak{r}}^*/L_{\mathfrak{r}}^{*5}\cong K_{\mathfrak{r}}^*/K_{\mathfrak{r}}^{*5} & \oplus K_{\mathfrak{r}}^*/K_{\mathfrak{r}}^{*5} \\ \text{by} & y+1 & y-1 \\ [(x_1,\mathfrak{r}^3)-\infty]\mapsto & d & d^4 \\ [(x_2,\mathfrak{r}^4)-\infty]\mapsto & e & e^4 \\ [(x_3,\mathfrak{r}^5)-\infty]\mapsto & f & f^4. \end{array}$$

We see that $\beta_{\mathfrak{r}}^{-1}$ of the image of $J(K_{\mathfrak{r}})/\phi J(K_{\mathfrak{r}})$ is generated by the image of $[(0,1)-\infty]$. So $\dim J(K)/\phi J(K)=1$. We have

$$(5-1)(\dim J(K)/\phi J(K)-\dim J(K)[\phi])=0=\text{MW rank}(J(K)).$$

Since the Mordell-Weil rank of $J(K)$ is 0, the Mordell-Weil rank of $J(\mathbf{Q})$ is also 0. So $J(\mathbf{Q})\cong\mathbf{Z}/10\mathbf{Z}$.

Recall that every divisor class contains a unique divisor of the form $P+Q-2\infty$ except for the trivial class. It contains divisors of the form $(a,b)+(a,-b)-2\infty$. Let $P\in C(\mathbf{Q})$. Then $[P+\infty-2\infty]$ must appear in list. So $C(\mathbf{Q})=\{\infty,(-1,0),(0,\pm1)\}$. Let P be defined over a quadratic extension of $\mathbf{Q}$ and let $\overline{P}$ be its conjugate. Then $[P+\overline{P}-2\infty]$ must appear in our list unless $P=(a,b)$, $\overline{P}=(a,-b)$ so $a\in\mathbf{Q}$. Thus the only other points of C, with coordinates in a quadratic extension of $\mathbf{Q}$, are $(1+i,\pm(1-2i))$, $(1-i,\pm(1+2i))$ and those with $x\in\mathbf{Q}$.