# Algebraic points of low degree on the Fermat quintic 

by<br>Matthew Klassen (Tacoma, Wa.) and Pavlos Tzermias (Bellaterra)

1. Introduction. The Fermat quintic is the smooth plane curve with projective equation

$$
F_{5}=\left\{(X, Y, Z) \in P^{2}(\overline{\mathbb{Q}}): X^{5}+Y^{5}=Z^{5}\right\}
$$

In this paper, which is based on [4] and [7], we characterize all rational points on $F_{5}$ over all number fields of degree at most 6 over $\mathbb{Q}$.

It is well known that there are exactly three $\mathbb{Q}$-rational points on $F_{5}$, namely

$$
Q_{0}=(0,1,1), \quad Q_{1}=(1,0,1), \quad \infty=(-1,1,0)
$$

Also let $\eta$ be a primitive 6 th root of 1 in $\overline{\mathbb{Q}}$ and let $\bar{\eta}$ denote the complex conjugate of $\eta$. Consider the following quadratic points on $F_{5}$ :

$$
P=(\eta, \bar{\eta}, 1), \quad \bar{P}=(\bar{\eta}, \eta, 1)
$$

Note that all of the above five points lie on the line

$$
L: \quad X+Y=Z
$$

For a positive integer $d$, let $\Gamma_{\mathbb{Q}, d}$ denote the union of all extensions of $\mathbb{Q}$ of degree at most $d$. Gross and Rohrlich have proved in [3] that

$$
F_{5}\left(\Gamma_{\mathbb{Q}, 2}\right)=\left\{Q_{0}, Q_{1}, \infty, P, \bar{P}\right\} .
$$

Now we define "trivial points" of higher degree, i.e. points which can be obtained from the points of $F_{5}\left(\Gamma_{\mathbb{Q}, 2}\right)$.

Let $R_{1}$ be a point of degree $k$ over $\mathbb{Q}$. We denote by $R_{1}, \ldots, R_{k}$ the conjugates of $R_{1}$ over $\mathbb{Q}$. Also let $L^{\prime}$ denote any plane $\mathbb{Q}$-rational line and $P^{\prime}$ any of the three $\mathbb{Q}$-rational points $Q_{0}, Q_{1}, \infty$. Further, denote by $C^{\prime}$ any plane $\mathbb{Q}$-rational conic which has contact of order 2 with $F_{5}$ at one of the pairs of points $\left(Q_{0}, \infty\right),\left(Q_{1}, \infty\right),\left(Q_{0}, Q_{1}\right)$ or $(P, \bar{P})$. For such a conic $C^{\prime}$, let $t\left(C^{\prime}\right)$ denote the effective divisor $2 Q_{0}+2 Q \infty, 2 Q_{1}+2 \infty, 2 Q_{0}+2 Q_{1}$ or $2 P+2 \bar{P}$, respectively.

[^0]Definition. Let notation be as in the previous paragraph. A point $R_{1}$ on $F_{5}$ of degree $k=4,5$ or 6 will be called a trivial point if $R_{1}+\ldots+R_{k}$ is of the form $F_{5} \cdot L^{\prime}-P^{\prime}, F_{5} \cdot L^{\prime}$ or $F_{5} \cdot C^{\prime}-t\left(C^{\prime}\right)$, respectively.

The main result in this paper is the following theorem:
Theorem 1. $F_{5}\left(\Gamma_{\mathbb{Q}, 6}\right)$ consists of $Q_{0}, Q_{1}, \infty, P, \bar{P}$ and the trivial points of degrees 4,5 and 6 . In particular, there are no points of degree 3 on $F_{5}$.

The paper is organized as follows: In Section 2 , we compute the group $J_{5}(\mathbb{Q})$ of $\mathbb{Q}$-rational points on the Jacobian $J_{5}$ of $F_{5}$. We show that $J_{5}(\mathbb{Q})$ is a group isomorphic to $(\mathbb{Z} / 5 \mathbb{Z})^{2}$ and we exhibit its generators. In Section 3, we prove some auxiliary results that will be needed for the proof of Theorem 1. In Section 4, we prove Theorem 1 using the results of the previous sections. Finally, in Section 5, we formulate an extension of Fermat's conjecture and discuss related results.
2. The $\mathbb{Q}$-rational points on $J_{5}$. Let $K$ be the cyclotomic field obtained by adjoining a primitive 5 th root of unity $\zeta$ to $\mathbb{Q}$. Also let $\varepsilon$ be a primitive 10 th root of unity such that $\varepsilon^{2}=\zeta$ (for example, let $\varepsilon=-\zeta^{3}$ ). Following [6], we note the following $K$-rational points on $F_{5}$ :

$$
a_{j}=\left(0, \zeta^{j}, 1\right), \quad b_{j}=\left(\zeta^{j}, 0,1\right), \quad c_{j}=\left(\varepsilon \zeta^{j}, 1,0\right)
$$

where $0 \leq j \leq 4$. These points will be referred to as points at infinity on $F_{5}$. Observe that $Q_{0}=a_{0}, Q_{1}=b_{0}$ and $\infty=c_{2}$.

Let $J_{5}^{\infty}$ denote the subgroup of $J_{5}$ consisting of those divisor classes of degree 0 which can be represented by a divisor supported on the points at infinity on $F_{5}$. In [6], Rohrlich has determined the structure of $J_{5}^{\infty}$. It is a group isomorphic to $(\mathbb{Z} / 5 \mathbb{Z})^{8}$. In [7] we proved that $J_{5}(K)=J_{5}^{\infty}$. From this we deduced the following theorem, whose proof was only sketched in [7]:

Theorem 2. $J_{5}(\mathbb{Q})$ is a group isomorphic to $(\mathbb{Z} / 5 \mathbb{Z})^{2}$. The divisor classes $\left[a_{0}-c_{2}\right]$ and $\left[b_{0}-c_{2}\right]$ form a basis for $J_{5}(\mathbb{Q})$ as a $\mathbb{Z} / 5 \mathbb{Z}$-vector space.

Since the proof of our main result depends crucially on Theorem 2, we will give a detailed proof of the latter in this section. It clearly suffices to determine which elements of $J_{5}^{\infty}$ remain invariant under the action of a generator of the Galois group $\operatorname{Gal}(K / \mathbb{Q})$. We will make use of the following result, due to Rohrlich:

Theorem 3 ([6], Corollary 1). A divisor of degree 0 supported on the points at infinity on $F_{5}$ is principal if and only if, mod 5 , it is in the span of

$$
\sum_{j=0}^{4} a_{j}, \quad \sum_{j=0}^{4} b_{j}, \quad \sum_{j=0}^{4} c_{j}
$$

$$
\sum_{j=0}^{4} j\left(a_{j}+b_{j}\right), \quad \sum_{j=0}^{4} j\left(b_{j}+c_{j}\right), \quad \sum_{j=0}^{4} j(j+1)\left(a_{j}+b_{j}+c_{j}\right) .
$$

Proof of Theorem 2. Consider the generator $g \in \operatorname{Gal}(K / \mathbb{Q})$ given by $\varepsilon \mapsto \varepsilon^{3}$. Then $\zeta \mapsto \zeta^{3}$. We immediately see that

$$
\begin{array}{lllll}
a_{0}^{g}=a_{0}, & a_{1}^{g}=a_{3}, & a_{2}^{g}=a_{1}, & a_{3}^{g}=a_{4}, & a_{4}^{g}=a_{2}, \\
b_{0}^{g}=b_{0}, & b_{1}^{g}=b_{3}, & b_{2}^{g}=b_{1}, & b_{3}^{g}=b_{4}, & b_{4}^{g}=b_{2}, \\
c_{0}^{g}=c_{1}, & c_{1}^{g}=c_{4}, & c_{2}^{g}=c_{2}, & c_{3}^{g}=c_{0}, & c_{4}^{g}=c_{3} .
\end{array}
$$

Now, by [6], for any element of $J_{5}^{\infty}$, we can choose a representative of the form

$$
\begin{aligned}
D= & x_{1}\left(a_{0}-a_{1}\right)+x_{2}\left(a_{0}-a_{2}\right)+x_{3}\left(a_{0}-a_{3}\right)+x_{4}\left(a_{0}-a_{4}\right) \\
& +y_{1}\left(b_{0}-b_{1}\right)+y_{2}\left(b_{0}-b_{2}\right)+y_{3}\left(b_{0}-b_{3}\right)+y_{4}\left(b_{0}-b_{4}\right) \\
& +z_{1}\left(c_{2}-c_{0}\right)+z_{2}\left(c_{2}-c_{1}\right)+z_{3}\left(c_{2}-c_{3}\right)+z_{4}\left(c_{2}-c_{4}\right) \\
& +s\left(a_{0}-c_{2}\right)+t\left(b_{0}-c_{2}\right),
\end{aligned}
$$

for integers $s, t, x_{j}, y_{j}, z_{j}, 1 \leq j \leq 4$. Therefore,

$$
\begin{aligned}
D^{g}-D= & \left(x_{1}-x_{2}\right) a_{1}+\left(x_{2}-x_{4}\right) a_{2}+\left(x_{3}-x_{1}\right) a_{3}+\left(x_{4}-x_{3}\right) a_{4} \\
& +\left(y_{1}-y_{2}\right) b_{1}+\left(y_{2}-y_{4}\right) b_{2}+\left(y_{3}-y_{1}\right) b_{3}+\left(y_{4}-y_{3}\right) b_{4} \\
& +\left(z_{1}-z_{3}\right) c_{0}+\left(z_{2}-z_{1}\right) c_{1}+\left(z_{3}-z_{4}\right) c_{3}+\left(z_{4}-z_{2}\right) c_{4} .
\end{aligned}
$$

Now since $[D] \in J_{5}(\mathbb{Q})$, the divisor $D^{g}-D$ is principal. By Theorem 3, there exist integers $l_{1}, \ldots, l_{6}$ such that, $\bmod 5$,

$$
\begin{aligned}
D^{g}-D= & l_{1} \sum_{j=0}^{4} a_{j}+l_{2} \sum_{j=0}^{4} b_{j}+l_{3} \sum_{j=0}^{4} c_{j} \\
& +l_{4} \sum_{j=0}^{4} j\left(a_{j}+b_{j}\right)+l_{5} \sum_{j=0}^{4} j\left(b_{j}+c_{j}\right) \\
& +l_{6} \sum_{j=0}^{4} j(j+1)\left(a_{j}+b_{j}+c_{j}\right) .
\end{aligned}
$$

Comparing the coefficients of $a_{0}, b_{0}, c_{0}, a_{4}, b_{4}, a_{2}$ in both expressions for $D^{g}-D$, we get (always mod 5)

$$
\begin{aligned}
l_{1} & =l_{2}=0, \\
l_{3} & =z_{1}-z_{3} \\
l_{4} & =x_{3}-x_{4} \\
l_{5} & =y_{3}-y_{4}+x_{4}-x_{3}, \\
l_{6} & =x_{4}-2 x_{3}+x_{2} .
\end{aligned}
$$

Using the above relations and comparing the coefficients of all points at infinity in the two expressions for $D^{g}-D$, we get (always mod 5)

$$
\begin{aligned}
x_{1} & =2 x_{3}+x_{4}-2 x_{2} \\
y_{1} & =3 y_{3}+3 y_{4}+3 x_{4}-x_{3}+3 x_{2} \\
y_{2} & =2 y_{3}-y_{4}+x_{4}-2 x_{3}+x_{2} \\
z_{2} & =z_{1}-y_{3}+y_{4}+x_{2}-x_{3} \\
z_{3} & =z_{1}+2 y_{3}-2 y_{4}+x_{3}-2 x_{4}+x_{2} \\
z_{4} & =z_{1}+y_{3}-y_{4}-x_{3}+x_{4}
\end{aligned}
$$

Therefore, mod 5 , we have

$$
\begin{aligned}
D- & s\left(a_{0}-c_{2}\right)-t\left(b_{0}-c_{2}\right) \\
= & \left(2 x_{4}-2 x_{3}-x_{2}\right) a_{0}+\left(2 x_{2}-x_{4}-2 x_{3}\right) a_{1}-x_{2} a_{2}-x_{3} a_{3}-x_{4} a_{4} \\
& +\left(y_{3}-2 y_{4}-x_{4}+2 x_{3}-x_{2}\right) b_{0}+\left(2 y_{3}+2 y_{4}+2 x_{4}+x_{3}+2 x_{2}\right) b_{1} \\
& +\left(-2 y_{3}+y_{4}-x_{4}+2 x_{3}-x_{2}\right) b_{2}-y_{3} b_{3}-y_{4} b_{4}-z_{1} c_{0} \\
& +\left(-z_{1}+y_{3}-y_{4}-x_{2}+x_{3}\right) c_{1}+\left(-z_{1}+2 y_{3}-2 y_{4}+2 x_{2}-x_{3}-x_{4}\right) c_{2} \\
& +\left(-z_{1}-2 y_{3}+2 y_{4}-x_{3}+2 x_{4}-x_{2}\right) c_{3}+\left(-z_{1}-y_{3}+y_{4}+x_{3}-x_{4}\right) c_{4} .
\end{aligned}
$$

It is now a straightforward task to verify that the right-hand side of the latter equality is equal, $\bmod 5$, to the linear combination

$$
\begin{aligned}
& \left(2 x_{4}-2 x_{3}-x_{2}\right) \sum_{j=0}^{4} a_{j}+\left(y_{3}-2 y_{4}-x_{4}+2 x_{3}-x_{2}\right) \sum_{j=0}^{4} b_{j}+\left(-z_{1}\right) \sum_{j=0}^{4} c_{j} \\
& \quad+\left(-2 x_{4}-2 x_{3}-x_{2}\right) \sum_{j=0}^{4} j\left(a_{j}+b_{j}\right)+\left(y_{3}-y_{4}-x_{3}+x_{4}\right) \sum_{j=0}^{4} j\left(b_{j}+c_{j}\right) \\
& \quad+\left(2 x_{2}+x_{3}+2 x_{4}\right) \sum_{j=0}^{4} j(j+1)\left(a_{j}+b_{j}+c_{j}\right) .
\end{aligned}
$$

By Theorem 3, we see immediately that $[D]=s\left[a_{0}-c_{2}\right]+t\left[b_{0}-c_{2}\right]$. This proves that every $\mathbb{Q}$-rational point on $J_{5}$ is a linear combination of the classes $a_{0}-c_{2}$ and $b_{0}-c_{2}$. Using Theorem 3, it is easy to check that these two divisor classes are linearly independent over $\mathbb{Z} / 5 \mathbb{Z}$. This completes the proof of Theorem 2.
3. Linear series on the Fermat quintic. In the proof of Theorem 1 we will make use of an explicit description of equivalence classes of divisors of degree 6 on a smooth plane quintic $C$, i.e. a nonsingular plane curve of degree 5 (and hence of genus 6 ). Since the complete linear series are just
the fibers of the Abel-Jacobi map

$$
f^{(6)}: C^{(6)} \rightarrow J(C)
$$

we will describe them from this point of view. (This material is well known, but we include it here for completeness. For more general results of this type concerning base-point free pencils, consult [1].)

Let $x$ be a point of $J(C)$, let $f_{x}$ be the fiber $\left(f^{(6)}\right)^{-1}(x)$, and let $D \in f_{x}$. Then we will show that $f_{x}$ has one of the following types:
$f_{x}=\{D\}, r(D)=0$ (a single divisor);
(f1) $\quad f_{x}=|D|, r(D)=1$, and $D$ contains 4 collinear points (i.e. there are base-points $P_{1}$ and $P_{2}$ of $|D|$ such that $\left|D-P_{1}-P_{2}\right|$ is a $g_{4}^{1}$ induced by a pencil of lines through a fixed point on $C$ ); $f_{x}=|D|$ and $D$ contains 5 collinear points (i.e. there is a base-point $P_{1}$ of $|D|$ such that $\left|D-P_{1}\right|$ is the unique $g_{5}^{2}$ cut out by lines on $\left.C\right)$; $f_{x}=|D|$ and $D$ consists of 6 points on a conic (i.e. $|D|$ is the $g_{6}^{1}$ induced by a pencil of conics through 4 fixed points on $C$ ).
Lemma 1. If $C$ is a smooth plane quintic, then the fibers of the Abel-Jacobi map $f^{(6)}: C^{(6)} \rightarrow J(C)$ are completely described by the cases (f0)-(f3) above.

Proof. The proof can be broken down into cases. First, let $D$ be an effective divisor of degree 6 on $C$. Then either $r(D)=0$ or $r(D)>0$. We only need to show that if $r(D)>0$ then we are in one of the cases (f1)-(f3) above. We will observe below that the points of $D$ lie on a conic. Then either this conic is irreducible (no 3 points of $D$ lie on a line), or the conic is reducible in which case we will let $k=k(D) \geq 3$ denote the maximum number of collinear points of $D$. The cases then break down as follows: irreducible or reducible and $k=3$ yields (f3); reducible and $k=4$ or $k=5$ yields (f1) or (f2), respectively. We now proceed with the proof.

By Clifford's theorem, $r(D) \leq 2$. We use the Riemann-Roch Theorem in the form $r-i=d-g$, so $r(D)=i(D)$, where $i(D)$ is the number of linearly independent holomorphic differentials $\omega$ on $C$ such that $(\omega) \geq D$. Now the canonical series on $C$ is cut out by the linear system of conics in the plane. So for $r(D)>0$ the points of $D$ lie on a conic. If the conic is irreducible, then it is the unique conic containing the six points of $D$, and hence there is only one differential $\omega$ on $C$ such that $(\omega) \geq D$. So $r(D)=i(D)=1$. Now let $D^{\prime}=(\omega)-D$. Then the complete linear series $|D|$ consists precisely of those divisors which lie on a conic which also passes through the 4 points of $D^{\prime}$. If the conic consists of two lines, then in the case where 3 points of $D$ lie on each line, this is again the unique conic containing the six points of $D$, and the argument is the same as before. This describes the case ( f 3 ) above.

Next, suppose that the conic is reducible, and also that $k \geq 4$ of the points of $D$ lie on one of the lines of this conic. Then it follows by similar arguments that the cases $k=4$ and $k=5$ describe the cases (f1) and (f2) above respectively. This completes the proof of the lemma.

Now we will give a list of divisor classes for $J_{5}(\mathbb{Q})$ according to the four types of the lemma. Our list captures all the geometric information that we will need in the sequel.

Remark. We wish to emphasize at this point that, in the following list, the symbols $L^{\prime}$ and $C^{\prime}$ are as in the definition of trivial points, except that they are not assumed to be $\mathbb{Q}$-rational any more.

Type (f2):

$$
\begin{array}{ll}
D_{1}=6 \infty & \left|D_{1}\right|=\left\{D=\infty+F_{5} \cdot L^{\prime}\right\} \\
D_{2}=6 Q_{0} & \left|D_{2}\right|=\left\{D=Q_{0}+F_{5} \cdot L^{\prime}\right\} \\
D_{3}=6 Q_{1} & \left|D_{3}\right|=\left\{D=Q_{1}+F_{5} \cdot L^{\prime}\right\}
\end{array}
$$

Type (f1):

$$
\begin{aligned}
& D_{4}=Q_{0}+Q_{1}+4 \infty \quad\left|D_{4}\right|=\left\{D=Q_{0}+Q_{1}+\left(F_{5} \cdot L^{\prime}-\infty\right)\right\} \\
& D_{5}=Q_{0}+4 Q_{1}+\infty \quad\left|D_{5}\right|=\left\{D=Q_{0}+\infty+\left(F_{5} \cdot L^{\prime}-Q_{1}\right)\right\} \\
& D_{6}=4 Q_{0}+Q_{1}+\infty \quad\left|D_{6}\right|=\left\{D=Q_{1}+\infty+\left(F_{5} \cdot L^{\prime}-Q_{0}\right)\right\} \\
& D_{7}=P+\bar{P}+4 \infty \quad\left|D_{7}\right|=\left\{D=P+\bar{P}+\left(F_{5} \cdot L^{\prime}-\infty\right)\right\} \\
& D_{8}=P+\bar{P}+4 Q_{0} \quad\left|D_{8}\right|=\left\{D=P+\bar{P}+\left(F_{5} \cdot L^{\prime}-Q_{0}\right)\right\} \\
& D_{9}=P+\bar{P}+4 Q_{1} \quad\left|D_{9}\right|=\left\{D=P+\bar{P}+\left(F_{5} \cdot L^{\prime}-Q_{1}\right)\right\} \\
& D_{10}=2 Q_{0}+4 Q_{1} \quad\left|D_{10}\right|=\left\{D=2 Q_{0}+\left(F_{5} \cdot L^{\prime}-Q_{1}\right)\right\} \\
& D_{11}=4 Q_{0}+2 Q_{1} \quad\left|D_{11}\right|=\left\{D=2 Q_{1}+\left(F_{5} \cdot L^{\prime}-Q_{0}\right)\right\} \\
& D_{12}=2 Q_{0}+4 \infty \quad\left|D_{12}\right|=\left\{D=2 Q_{0}+\left(F_{5} \cdot L^{\prime}-\infty\right)\right\} \\
& D_{13}=4 Q_{0}+2 \infty \quad\left|D_{13}\right|=\left\{D=2 \infty+\left(F_{5} \cdot L^{\prime}-Q_{0}\right)\right\} \\
& D_{14}=2 Q_{1}+4 \infty \quad\left|D_{14}\right|=\left\{D=2 Q_{1}+\left(F_{5} \cdot L^{\prime}-\infty\right)\right\} \\
& D_{15}=4 Q_{1}+2 \infty \quad\left|D_{15}\right|=\left\{D=2 \infty+\left(F_{5} \cdot L^{\prime}-Q_{1}\right)\right\}
\end{aligned}
$$

Type (f3):

$$
\begin{array}{ll}
D_{16}=3 Q_{0}+3 Q_{1} & \left|D_{16}\right|=\left\{D=F_{5} \cdot C^{\prime}-\left(2 Q_{0}+2 Q_{1}\right)\right\} \\
D_{17}=3 Q_{0}+3 \infty & \left|D_{17}\right|=\left\{D=F_{5} \cdot C^{\prime}-\left(2 Q_{0}+2 \infty\right)\right\} \\
D_{18}=3 Q_{1}+3 \infty & \left|D_{18}\right|=\left\{D=F_{5} \cdot C^{\prime}-\left(2 Q_{1}+2 \infty\right)\right\} \\
D_{19}=2 Q_{0}+2 Q_{1}+2 \infty & \left|D_{19}\right|=\left\{D=F_{5} \cdot C^{\prime}-(2 P+2 \bar{P})\right\}
\end{array}
$$

Type (f0):

$$
\begin{aligned}
& D_{20}=3 Q_{0}+Q_{1}+2 \infty \\
& D_{21}=3 Q_{0}+2 Q_{1}+\infty \\
& D_{22}=Q_{0}+3 Q_{1}+2 \infty \\
& D_{23}=2 Q_{0}+3 Q_{1}+\infty \\
& D_{24}=2 Q_{0}+Q_{1}+3 \infty \\
& D_{25}=Q_{0}+2 Q_{1}+3 \infty
\end{aligned}
$$

Lemma 1 now shows that Theorem 2 can be rephrased as follows:
Proposition 1. $J_{5}(\mathbb{Q})=\left\{[D-6 \infty]: D=D_{1}, \ldots, D_{25}\right\}$.
4. Proof of Theorem 3. Let $L_{0}, L_{1}$ and $L_{\infty}$ denote the tangent lines to $F_{5}$ at $Q_{0}, Q_{1}$ and $\infty$, respectively. It is easy to check that they all have contact of order 5 with $F_{5}$ at the corresponding points.

Now let $R_{1}$ be a point of degree $k=3,4,5$ or 6 over $\mathbb{Q}$. Consider the $\mathbb{Q}$-rational divisor $D=R_{1}+\ldots+R_{k}+(6-k) \infty$. By the previous section, $D$ lies in one of the complete linear series $\left|D_{i}\right|$, for $1 \leq i \leq 25$.

First we will show that there are no cubic points on $F_{5}$. Suppose that $R_{1}, R_{2}$ and $R_{3}$ are conjugate points of degree 3 on $F_{5}$. Let $D=R_{1}+R_{2}+$ $R_{3}+3 \infty$. Clearly $D$ is not one of the divisors of type (f0), so we must show that $D$ is not linearly equivalent to one of the divisors $D_{1}-D_{19}$. Suppose this were the case. In the case of type (f2), we get $F_{5} \cdot L^{\prime} \geq 2 \infty$ and thus $L^{\prime}=L_{\infty}$. For the case of type (f1), $R_{1}+R_{2}+R_{3}$ cannot be part of the base locus, otherwise it would contain quadratic or rational points. So then $F_{5} \cdot L^{\prime}=R_{1}+R_{2}+R_{3}+\infty+P^{\prime}$ for some $\mathbb{Q}$-rational point $P^{\prime}$ and thus $L^{\prime}$ is either $L_{\infty}$ or $L$. For the case of type (f3), we have $F_{5} C^{\prime} \geq 3 \infty$, which implies that $C^{\prime}$ is reducible and contains $L_{\infty}$ (by Lemma 2.3.2 of [5]). Therefore $C^{\prime}$ must pass through $2 Q_{0}+2 \infty$ or $2 Q_{1}+2 \infty$ and hence $R_{1}+R_{2}+R_{3}$ is equal to $3 Q_{0}$ or $3 Q_{1}$.

Next, we show that there are only the trivial points of degrees 4,5 , and 6 . We will again proceed by cases, and we will assume that in each case $D$ is in one of the indicated equivalence classes. Our conclusions will then always be that $R_{1}$ would be forced to have lower degree or that it is indeed a trivial point. We will abbreviate these conclusions by (lower degree) or (trivial points). The following lemma will be tacitly used whenever the conclusion is "(trivial points)".

Lemma 2. Let $L^{\prime}$ denote a plane line and $C^{\prime}$ a plane conic. Let $D$ be an effective $\mathbb{Q}$-rational divisor on $F_{5}$ of degree $k=4,5$ or 6 such that $D<F_{5} \cdot L^{\prime}, D=F_{5} . L^{\prime}$ or $D<F_{5} . C^{\prime}$ respectively. Then the corresponding line $L^{\prime}$ or conic $C^{\prime}$ is $\mathbb{Q}$-rational.

Proof. Let $\sigma \in \operatorname{Gal}(\overline{\mathbb{Q}} / \mathbb{Q})$. If $D=F_{5} . C^{\prime}-E$, where $C^{\prime}$ is a conic and $E$ is an effective divisor of degree 4 , then $D=D^{\sigma}=F_{5} . C^{\prime \sigma}-E^{\sigma}$. Therefore, $C^{\prime}$ and $C^{\prime \sigma}$ have at least 6 points in common. Since a conic is uniquely determined by 5 points, we get $C^{\prime}=C^{\prime \sigma}$. The proof for the case of lines is similar.

Now we proceed with the final part of the proof of Theorem 1. Because of Lemma $2, L^{\prime}, C^{\prime}$ and $P^{\prime}$ are exactly as in the definition of trivial points:
(i) $k=4, D=R_{1}+R_{2}+R_{3}+R_{4}+2 \infty$ :

Type (f2): Either some $R_{i}=P^{\prime}$ (lower degree), or $R_{1}+R_{2}+R_{3}+$ $R_{4}+\infty=F_{5} . L^{\prime}$ (trivial points).

Type (f1): We get either some $R_{i}$ is in the base locus (lower degree), or that the $R_{i}$ are all on $L^{\prime}$ (trivial points).

Type (f3): In cases $16-19$ we get $F_{5} . C^{\prime} \geq 2 \infty+2 Q_{0}+2 Q_{1}$, or $4 \infty+2 Q_{0}$, or $4 \infty+2 Q_{1}$, or $2 \infty+2 P+2 \bar{P}$. In each case $C^{\prime}$ reduces to a pair of rational lines (lower degree).
(ii) $k=5, D=R_{1}+R_{2}+R_{3}+R_{4}+R_{5}+\infty$ :

Type (f2): Either some $R_{i}=P^{\prime}$ (lower degree), or $R_{1}+R_{2}+R_{3}+$ $R_{4}+R_{5}=F_{5} \cdot L^{\prime}$ (trivial points).

Type (f1): Some $R_{i}$ is in the base locus (lower degree).
Type (f3): $C^{\prime}$ goes through $\infty$ and one of $2 \infty, Q_{0}+Q_{1}$, or $P+\bar{P}$. In each case $C^{\prime}$ reduces to a pair of rational lines (lower degree).
(iii) $k=6, D=R_{1}+R_{2}+R_{3}+R_{4}+R_{5}+R_{6}$ :

Type (f2): Some $R_{i}=P^{\prime}$ (lower degree).
Type (f1): Some $R_{i}$ is in the base locus (lower degree).
Type (f3): $D=F_{5} . C^{\prime}$ (trivial points).
5. An extension of Fermat's conjecture. Theorem 1 shows, in particular, that all points $P \in F_{5}(M)$, where $M$ is a number field such that $[M: \mathbb{Q}] \leq 3$, lie on the line $X+Y=Z$. It is interesting to ask whether this is true in more generality. We therefore formulate the following conjecture, which extends Fermat's conjecture (now a theorem of Wiles):

Conjecture. Let $p$ be an odd prime and let $F_{p}$ denote the Fermat curve of degree $p$. If $P \in F_{p}(M)$ for a number field $M$ such that $[M: \mathbb{Q}] \leq p-2$, then $P$ lies on the line $X+Y=Z$.

We wish to conclude this paper by discussing some limited evidence for the above conjecture:

Fermat and Euler have proved this conjecture for $p=3$. The case $p=5$ is handled by Theorem 1. For $p \leq 11$, Gross and Rohrlich ([3]) have proved a
similar assertion for $[M: \mathbb{Q}] \leq(p-1) / 2$. Moreover, from a general theorem of Debarre and Klassen $([2])$, it follows that the set $F_{p}\left(\Gamma_{\mathbb{Q}, p-2}\right)$ is finite for all odd primes $p$.

## References

[1] M. Coppens, A study of the schemes $W_{e}^{1}$ of smooth plane curves, in: Proc. 1st Belgian-Spanish Week on Algebra and Geometry, R.U.C.A., 1988, 29-63.
[2] O. Debarre and M. Klassen, Points of low degree on smooth plane curves, J. Reine Angew. Math. 446 (1994), 81-87.
[3] B. Gross and D. Rohrlich, Some results on the Mordell-Weil group of the Jacobian of the Fermat curve, Invent. Math. 44 (1978), 201-224.
[4] M. Klassen, Algebraic points of low degree on curves of low rank, Ph.D. thesis, University of Arizona, 1993.
[5] M. Namba, Families of Meromorphic Functions on Compact Riemann Surfaces, Lecture Notes in Math. 767, Springer, Berlin, 1979.
[6] D. Rohrlich, Points at infinity on the Fermat curves, Invent. Math. 39 (1977), 95-127.
[7] P. Tzermias, Mordell-Weil groups of the Jacobian of the 5-th Fermat curve, Proc. Amer. Math. Soc. 125 (1997), 663-668.

Department of Mathematics Pacific Lutheran University Tacoma, Washington 98447 U.S.A.

E-mail: matcat@seanet.com

Centre de Recerca Matemàtica Institut d'Estudis Catalans Apartat 50 E-08193 Bellaterra, Spain
E-mail: tzermias@crm.es


[^0]:    1991 Mathematics Subject Classification: Primary 11G30; Secondary 14H25, 14H45.

