RATIONAL POINTS ON THE SUPERELLIPTIC ERDÖS–SELFRIDGE CURVE OF FIFTH DEGREE

M. LAKHAL AND J. W. SANDER

§1. *Introduction.* By a remarkable result of Erdös and Selfridge [3] in 1975, the diophantine equation

$$y^k = (x+1)(x+2)\cdots(x+m), \tag{1}$$

with integers $k \geqslant 2$ and $m \geqslant 2$, has only the trivial solutions $x = -j$ $(j = 1, \ldots, m)$, $y = 0$. This put an end to the old question whether the product of consecutive positive integers could ever be a perfect power; for a brief account of its history see [7].

From the viewpoint of algebraic geometry (1) represents a so-called superelliptic curve, and it seems to be more natural to ask for *rational* solutions $(x; y)$ instead of integer solutions. Rational points on elliptic curves are well understood, but for general k and m, their nice arithmetic properties fade away. It follows from Faltings's proof [4] of Mordell's conjecture that, for fixed $k > 1, m > 1$ and $k + m > 6$, equation (1) has at most finitely many rational solutions (*cf.* [7]).

It was shown by the second author [7] that, for $k \geqslant 2$ and $2 \leqslant m \leqslant 4$, all rational points $(x; y)$ on the superelliptic curve (1) are the trivial ones with $x = -j$ $(j = 1, \ldots, m)$ and $y = 0$, except for the case $k = m = 2$ where we have exactly those satisfying

$$x = \frac{2c_1^2 - c_2^2}{c_2^2 - c_1^2}, \qquad y = \frac{c_1 c_2}{c_2^2 - c_1^2}$$

with coprime integers $c_1 \neq \pm c_2$. The second author also made the following

CONJECTURE. *For $k \geqslant 2$ and $m \geqslant 2$, all rational points $(x; y)$ on the superelliptic curve (1) are the trivial ones with $x = -j$ $(j = 1, \ldots, m)$ and $y = 0$, except for the case $k = m = 2$ with exactly those satisfying*

$$x = \frac{2c_1^2 - c_2^2}{c_2^2 - c_1^2}, \qquad y = \frac{c_1 c_2}{c_2^2 - c_1^2}$$

with coprime integers $c_1 \neq \pm c_2$.

The purpose of this article is to prove the conjecture for $m = 5$ and all $k \geqslant 2$.

THEOREM. *Let $k \geqslant 2$. Then the only rational points on the superelliptic curve*

$$y^k = (x+1)(x+2)(x+3)(x+4)(x+5) \tag{2}$$

are $(x; 0)$ with $-x \in \{1, 2, 3, 4, 5\}$.

§2. *Notation and preliminary results.* For a positive integer k, let

$$k^* := \begin{cases} k, & \text{for } 5 \nmid k, \\ k/5, & \text{for } 5 \mid k. \end{cases}$$

For arbitrary integers a and b we define the greatest common divisors

$$G_1 = G_1(a, b) := (a, a^2 - 4b^2),$$
$$G_2 = G_2(a, b) := (a^2 - b^2, a^2 - 4b^2).$$

For $(a, b) = 1$ they satisfy

$$G_1(a, b) = (a, 4) \in \{1, 2, 4\}, \tag{3}$$

$$G_2(a, b) = (a^2 - b^2, 3) \in \{1, 3\}. \tag{4}$$

Our proof of the theorem uses results on the solutions of several diophantine equations, all of which are based on the work of Wiles [**9**]. An integral solution $(x; y; z)$ of the equation

$$aX^k + bY^l = cZ^m,$$

with given integers a, b, c and positive integers k, l, m, is called *primitive* if $\gcd(x, y, z) = 1$, and is called *trivial* if $xyz \in \{0, \pm 1\}$.

THEOREM A (RIBET). *Let $p \geqslant 3$ be a prime, and let $2 \leqslant \alpha < p$. Then*

$$X^p + Y^p = 2^\alpha Z^p$$

has only trivial solutions.

Proof. This is part of Ribet's Theorem 3 in [**6**].

THEOREM B (RIBET, DARMON & MEREL). *Let $p \geqslant 3$ be a prime. Then*

$$X^p + Y^p = 2Z^p$$

has only trivial solutions.

Proof. This is part 1 of the main theorem of Darmon and Merel in [**1**].

THEOREM C (POONEN). *The primitive solutions of*

$$X^5 + Y^5 = Z^2$$

are all trivial.

Proof. This result can be found in [5].

THEOREM D (SERRE, RIBET). *For a positive integer α the equation*

$$X^5 + Y^5 = 3^\alpha Z^5$$

has only trivial solutions.

Proof. This is shown in the same fashion as Ribet's Theorem 1 in [6], since Serre's Théorème 2 in [8] also works in the case $L = 3$ and $p = 5$.

§3. *Proof of the main theorem.* According to the possible values of G_1 and G_2 (*cf.* (3) and (4)), the proof of our theorem falls into four parts.

PROPOSITION 1. *Let $k \geqslant 2, a, b = b_1^{k^*} > 0$ and c be integers satisfying $G_2(a, b) = (a, b) = 1$ and*

$$c^k = a(a^2 - b^2)(a^2 - 4b^2). \tag{5}$$

Then $c = 0$.

Proof. Since $(a, b) = 1$, we have $(a, a^2 - b^2) = 1$. Then (5) and $G_2(a, b) = 1$ imply that

$$a^2 - b^2 = c_1^k \quad \text{and} \quad (a^2 - 4b^2)a = c_2^k \tag{6}$$

for some coprime integers c_1, c_2. By (3) we have $G_1|4$, and so we obtain from the second equation in (6) that

$$a = G_1 2^s c_3^k \quad \text{and} \quad a^2 - 4b^2 = G_1 2^t c_4^k \tag{7}$$

for some odd, coprime integers c_3, c_4 satisfying $(c_1, c_3c_4) = 1$, where

$$(s, t) = \begin{cases} (0, 0), & \text{for } G_1 = 1, \\ (0, jk - 2), & \text{for } G_1 = 2, \\ (0, 0), & \text{for } G_1 = 4, 4\|a, \\ (jk - 4, 0), & \text{for } G_1 = 4, 8|a, \end{cases}$$

for a suitable positive integer j. Since $b = b_1^{k^*}$, (6) and (7) yield

$$G_1^2 2^{2s} c_3^{2k} - b_1^{2k^*} = c_1^k$$

in three pairwise coprime terms. Since $G_1|4$ by (3), that is an identity of type

$$2^{2\alpha} X^{2k} - Y^{2k^*} = Z^k \tag{8}$$

with $\alpha = s + \log_2 G_1$.

First, assume that there is a prime $p \notin \{2, 5\}$ dividing k, or $5^2 | k$. Then (8) is of type

$$2^{2\alpha} X^p - Y^p = Z^p$$

in coprime terms for a prime $p \neq 2$. By Theorem A together with Theorem B this has only trivial solutions (more precisely $XYZ = 0$); hence $c_3 c_1 = 0$ and thus $c = 0$. We are left with the case $k = 2^r 5^\varepsilon$ with a non-negative integer r and $\varepsilon \in \{0, 1\}$. For $\varepsilon = 0$ we have $r \geqslant 1$, since $k \geqslant 2$. Therefore (8) is of type

$$2^{2\alpha} X^4 - Y^4 = Z^2,$$

which Euler knew to be unsolvable except for $XYZ = 0$ (*cf.* **[2]**, p. 626). So we only have to deal with the case $\varepsilon = 1$, when (8) is of type

$$2^{2\alpha} X^{10} - Y^2 = Z^5. \tag{9}$$

For $\alpha = 0$, we have an equation of the form $X^5 + Z^5 = Y^2$ in coprime terms, which has only trivial solutions by Theorem C and thus implies that $c = 0$. For $\alpha \geqslant 1$, we have

$$(2^\alpha X^5 - Y, 2^\alpha X^5 + Y) = (2^\alpha X^5 - Y, 2^{\alpha+1} X^5) = 1;$$

hence, by (9),

$$2^\alpha X^5 - Y = Z_1^5 \quad \text{and} \quad 2^\alpha X^5 + Y = Z_2^5.$$

We obtain $2^{\alpha+1} X^5 = Z_1^5 + Z_2^5$ in coprime terms, which again has only trivial solutions by Theorems A and B. This completes the proof of Proposition 1.

Proposition 2. *Let* $k \geqslant 2, a, b = b_1^{k^*} > 0$ *and* c *be integers satisfying* $G_1(a, b) = (a, b) = 1$, $G_2(a, b) = 3$ *and (5). Then* $c = 0$.

Proof. Since $G_1 = (a, 4) = 1$ by (3), we know that $2 \nmid a$, and hence

$$(a - 2b, a + 2b) = (a - 2b, 2a) = (a - 2b, a) = 1. \tag{10}$$

Moreover, $(a, b) = 1$ implies that

$$(a - b, a - 2b) = (a + b, a + 2b) = 1. \tag{11}$$

By the fact that $3 = G_2(a, b) = ((a - b)(a + b), (a - 2b)(a + 2b))$, we have either $(a - b, a + 2b) = 3$, $(a + b, a - 2b) = 1$, or $(a - b, a + 2b) = 1$, $(a + b, a - 2b) = 3$. By the transformation $b \mapsto -b$ each of the two cases turns into the other. Therefore, we may assume without loss of generality that

$$(a - b, a + 2b) = 3 \quad \text{and} \quad (a + b, a - 2b) = 1. \tag{12}$$

Consequently, $(a - b, 3) = 3$, and clearly $(a, (a^2 - b^2)(a^2 - 4b^2)) = G_1 = 1$. By virtue of (5), (10), (11) and (12), we only have to distinguish two cases, namely,

$$\begin{cases} a = c_1^k, \\ a - 2b = c_2^k, \\ a + 2b = 3^{k-1} c_3^k, \\ a^2 - b^2 = 3c_4^k, \end{cases} \tag{13}$$

and

$$\begin{cases} a = c_1^k, \\ a - 2b = c_2^k, \\ a + 2b = 3c_3^k, \\ a^2 - b^2 = 3^{k-1} c_4^k \end{cases} \tag{14}$$

for some pairwise coprime integers c_1, c_2, c_3, c_4 satisfying $2 \not| c_1c_2c_3$ and $3 \not| c_1c_2$.

Since $d := (a+b, a-b) = (a+b, 2) \in \{1, 2\}$, we have

$$(a+b, a(a-b)(a^2-4b^2)) = d.$$

So, by (5), we have in coprime terms

$$a+b = c_5^k \quad \text{or} \quad a+b = 2c_5^k \quad \text{or} \quad a+b = 2^{k-1} c_5^k$$

for a suitable c_5. Both (13) and (14) imply that $a = c_1^k$, and we have $b = b_1^{k^*}$ by definition of b. So we obtain an equation of type

$$X^k + Y^{k^*} = 2^\delta \cdot Z^k \tag{15}$$

in coprime terms and $\delta \in \{0, 1, k-1\}$. If k has an odd prime divisor $p \neq 5$ or $5^2 \mid k$, then (15) has only trivial solutions by Theorems A and B, which all lead to $c = 0$. The same is true in case $4 \mid k$, which was known to Euler (*cf.* **[2]**, p. 626). So we are left with the three exponents $k \in \{2, 5, 10\}$.

For $k \in \{2, 10\}$ we obtain (with $b = b_1^{k^*}$) an equation of type $X^4 - Y^4 = 3Z^2$ in coprime terms from the last identity in (13) or (14), respectively. This equation can be shown to have only trivial solutions by Fermat's method of descent (*cf.* **[2]**, p. 634), or with a simple congruence argument by careful use of the divisibility properties we have.

It remains to consider the unique exponent $k = 5$, which leaves us with four cases according to the two subcases (13) and (14) as well as $d = (a+b, a-b) \in \{1, 2\}$. Let us first examine (13) with $d = 1$. By (12) we have $3 \mid (a-b)$, and thus $3 \not| (a+b)$. It follows from (13) that

$$\begin{cases} a = c_1^5, \\ a - 2b = c_2^5, \\ a + 2b = 3^4 c_3^5, \\ a - b = 3c_6^5, \\ a + b = c_7^5 \end{cases}$$

with coprime integers c_6, c_7. Consequently,

$$b = (a+2b) - (a+b) = 3^4 c_3^5 - c_7^5$$

and

$$3b = (a+b) - (a-2b) = c_7^5 - c_2^5.$$

Comparison of these two implies that

$$(3c_3)^5 - 3c_7^5 = c_7^5 - c_2^5,$$

so that we have an equation of type $X^5 + Y^5 = 4Z^5$, which has only trivial solutions by Theorem A.

In case (13) with $d = 2$ we get

$$a - b = 3 \cdot 2c_6^5 \quad \text{and} \quad a + b = 2^4 c_7^5$$

or

$$a - b = 3 \cdot 2^4 c_6^5 \quad \text{and} \quad a + b = 2c_7^5,$$

which imply that

$$\begin{cases} a = c_1^5, \\ a - 2b = c_2^5, \\ a + 2b = 3^4 c_3^5, \\ a - b = 2 \cdot 3c_6^5, \\ a + b = 2^4 c_7^5, \end{cases} \tag{16}$$

or

$$\begin{cases} a = c_1^5, \\ a - 2b = c_2^5, \\ a + 2b = 3^4 c_3^5, \\ a - b = 2^4 \cdot 3c_6^5, \\ a + b = 2c_7^5. \end{cases} \tag{17}$$

From (16) follow

$$b = (a+2b) - (a+b) = 3^4 c_3^5 - 2^4 c_7^5$$

and

$$3b = (a+b) - (a-2b) = 2^4 c_7^5 - c_2^5,$$

which lead to

$$(3c_3)^5 + c_2^5 = 2(2c_7)^5,$$

an equation having only trivial solutions by Theorem B. In the other situation (17) we similarly obtain

$$(3c_3)^5 + c_2^5 = 8c_7^5,$$

which has only trivial solutions by Theorem A.

In case (14) with $d = 1$ then follow

$$\begin{cases} a = c_1^5, \\ a - 2b = c_2^5, \\ a + 2b = 3c_3^5, \\ a - b = 3^4 c_6^5, \\ a + b = c_7^5, \end{cases}$$

which imply that

$$b = (a - b) - (a - 2b) = 3^4 c_6^5 - c_2^5$$

and

$$3b = (a + b) - (a - 2b) = c_7^5 - c_2^5,$$

thus

$$(3c_6)^5 - c_7^5 = 2c_2^5,$$

having only trivial solutions by Theorem B.

Finally we have to consider (14) with $d = 2$, so that

$$\begin{cases} a = c_1^5, \\ a - 2b = c_2^5, \\ a + 2b = 3c_3^5, \\ a - b = 2 \cdot 3^4 c_6^5, \\ a + b = 2^4 c_7^5, \end{cases} \tag{18}$$

or

$$\begin{cases} a = c_1^5, \\ a - 2b = c_2^5, \\ a + 2b = 3c_3^5, \\ a - b = 2^4 \cdot 3^4 c_6^5, \\ a + b = 2c_7^5. \end{cases} \tag{19}$$

From (18) follows

$$3c_1^5 = 3a = 2(a + b) + (a - 2b) = 2^5 c_7^5 + c_2^5,$$

which means that

$$(2c_7)^5 + c_2^5 = 3c_1^5.$$

This equation of type $X^5 + Y^5 = 3Z^5$ has only trivial solutions by Theorem D. From (19) we obtain

$$c_1^5 = a = 2(a-b) - (a-2b) = 2^5 \cdot 3^4 c_6^5 - c_2^5;$$

hence

$$c_1^5 + c_2^5 = 3^4(2c_6)^5,$$

and again there are only trivial solutions by Theorem D. This proves Proposition 2.

PROPOSITION 3. *Let* $k \geqslant 2, a, b = b_1^{k*} > 0$ *and* c *be integers satisfying* $(a, b) = 1, G_1(a, b) = 2, G_2(a, b) = 3$ *and (5). Then* $c = 0$.

Proof. It follows from $G_1 = (a, a^2 - 4b^2) = 2$ that $2 \| a$. Then (5) implies, by virtue of $(a, a^2 - b^2) = 1$, and $G_2 = (a^2 - b^2, a^2 - 4b^2) = 3$, that

$$a = 2c_1^k \quad \text{and} \quad (a^2 - b^2)(a^2 - 4b^2) = 2^{k-1}c_2^k \tag{20}$$

for some coprime integers c_1 and c_2 with odd c_1. Since $(a, b) = 1$ and $2 \mid a$, we know that

$$(a-b, a+b) = (a-b, 2) = 1. \tag{21}$$

By the condition $G_2 = 3$, we may assume without loss of generality (as in the proof of Proposition 2) that

$$(a-b, a+2b) = 3 \quad \text{and} \quad (a+b, a-2b) = 1. \tag{22}$$

Since $2 \| a$, and thus $2 \nmid b$, we have $a \pm 2b \equiv 0 \bmod 4$, and therefore

$$(a-2b, a+2b) = (a-2b, 4b) = (a-2b, 4) = 4. \tag{23}$$

Now (20), (21), (22) and $(a+b, a+2b) = 1$ imply that

$$a + b = c_3^k, \tag{24}$$

and, with (23) in addition, we necessarily have one of the following four situations:

$$\begin{cases} a - b = 3c_4^k, \\ a - 2b = 2^2 c_5^k, \\ a + 2b = 2^{k-3}3^{k-1}c_6^k, \end{cases} \tag{25}$$

or

$$\begin{cases} a-b=3c_4^k, \\ a-2b=2^{k-3}c_5^k, \\ a+2b=2^2 3^{k-1}c_6^k, \end{cases} \tag{26}$$

or

$$\begin{cases} a-b=3^{k-1}c_4^k, \\ a-2b=2^2c_5^k, \\ a+2b=2^{k-3}3c_6^k, \end{cases} \tag{27}$$

or

$$\begin{cases} a-b=3^{k-1}c_4^k, \\ a-2b=2^{k-3}c_5^k, \\ a+2b=2^2 3c_6^k, \end{cases} \tag{28}$$

where c_3, c_4, c_5 and c_6 are pairwise coprime integers.

First of all, (24), (20) and $b = b_1^{k^*}$ imply that

$$2c_1^k + b_1^{k^*} = c_3^k \tag{29}$$

in coprime terms. For even k this equation is of type $2X^2 + Y^2 = Z^2$ in coprime terms, where $2 \nmid XYZ$ by definition of c_1, c_3 and b_1, since $2\|a$ and $2 \nmid b$. This is contradictory, because $2X^2 + Y^2 \equiv 3 \not\equiv 1 \equiv Z^2 \bmod 4$. For odd k, (29) is an equation of type $X^p + Y^p = 2Z^p$ for some prime $p > 2$, unless $k = 5$, which is the only exponent left by Theorem B.

For $k = 5$ we obtain in both cases (25) and (26)

$$a^2 - 4b^2 = (a-2b)(a+2b) = (2 \cdot 3)^4 (c_5 c_6)^5.$$

With (20) then follows

$$c_1^{10} - b^2 = 2^2 3^4 (c_5 c_6)^5.$$

Since $(c_1, b) = 1$, we have $(c_1^5 - b, c_1^5 + b) = 2$, and we conclude that

$$c_1^5 - b = 2 \cdot 3^4 c_7^5 \quad \text{and} \quad c_1^5 + b = 2c_8^5$$

or

$$c_1^5 - b = 2c_7^5 \quad \text{and} \quad c_1^5 + b = 2 \cdot 3^4 c_8^5$$

for some coprime integers c_7 and c_8. In both cases, addition leads to an equation of type $X^5 - Y^5 = 3^4 Z^5$, which has only trivial solutions by Theorem D.

In the cases (25) and (26), we obtain, for $k = 5$,

$$a^2 - 4b^2 = (a - 2b)(a + 2b) = 2^4 \cdot 3(c_5 c_6)^5.$$

With (20) there follows

$$c_1^{10} - b^2 = 2^2 \cdot 3(c_5 c_6)^5.$$

Again, $(c_1, b) = 1$ implies that $(c_1^5 - b, c_1^5 + b) = 2$, and we conclude that

$$c_1^5 - b = 2 \cdot 3c_7^5 \quad \text{and} \quad c_1^5 + b = 2c_8^5$$

or

$$c_1^5 - b = 2c_7^5 \quad \text{and} \quad c_1^5 + b = 2 \cdot 3c_8^5$$

for some coprime integers c_7 and c_8. In both cases, addition leads to an equation of type $X^5 - Y^5 = 3Z^5$, which has only trivial solutions by Theorem D.

Proposition 4. *Let* $k \geqslant 2, a, b = b_1^{k*} > 0$ *and* c *be integers satisfying* $(a, b) = 1, G_1(a, b) = 4, G_2(a, b) = 3$ *and (5). Then* $c = 0$.

Proof. It follows from $G_1 = (a, a^2 - 4b^2) = 4$ that $4 \mid a$; hence $2 \nmid b$ and so $4 \| (a^2 - 4b^2)$. Then (5) implies, by virtue of $(a, a^2 - b^2) = 1$, that

$$a = 4^{k-1} c_1^k \quad \text{and} \quad (a^2 - b^2)(a^2 - 4b^2) = 4c_2^k \tag{30}$$

for some coprime integers c_1 and c_2 with odd c_2. Since $(a, b) = 1$ and $2 | a$, we know that

$$(a - b, a + b) = (a - b, 2) = 1. \tag{31}$$

By the condition $G_2 = 3$, we may assume without loss of generality (as in the proof of Proposition 2) that

$$(a - b, a + 2b) = 3 \quad \text{and} \quad (a + b, a - 2b) = 1. \tag{32}$$

Now (30), (31), (32), $(a + b, a + 2b) = (a - b, a - 2b) = 1$ and $(a - 2b, a + 2b) = (a - 2b, 2a) = 2$ imply that

$$a + b = c_3^k \quad \text{and} \quad a - 2b = 2c_4^k, \tag{33}$$

and we necessarily have one of the following two situations:

$$a - b = 3c_5^k \quad \text{and} \quad a + 2b = 2 \cdot 3^{k-1} c_6^k \tag{34}$$

or

$$a - b = 3^{k-1} c_5^k \quad \text{and} \quad a + 2b = 2 \cdot 3c_6^k \tag{35}$$

with some pairwise coprime integers c_3, c_4, c_5 and c_6 satisfying $2 \nmid c_3 c_4 c_5 c_6$ and $3 \nmid c_3 c_4$.

From (33), (30) and $b = b_1^{k^*}$, we conclude that

$$4^{k-1}c_1^k + b_1^{k^*} = c_3^k \tag{36}$$

in coprime terms. For even k we consequently have $X^2 + Y^2 \equiv Z^2 \bmod 3$ with $3 \nmid XYZ$ by the definition of c_1, b_1 and c_3 and $3 \mid (a-b)$ by (35), but this congruence cannot hold. For odd k, (36) is an equation of type $X^p - Y^p = 4^{p-1}Z^p = 2^{p-2}(2Z)^p$ for some prime $p > 2$, unless $k = 5$, which is the only exponent left by Theorem A or Theorem B, respectively.

For $k = 5$, we obtain in case (34) with (33)

$$\begin{aligned} 0 &= 3 \cdot 2a - 2 \cdot 3a = 3 \cdot ((a-2b) + (a+2b)) - 2 \cdot ((a-2b) + 2(a+b)) \\ &= 3 \cdot (2c_4^5 + 2 \cdot 3^4 c_6^5) - 2 \cdot (2c_4^5 + 2c_3^5) = 2c_4^5 + 2(3c_6)^5 - 4c_3^5, \end{aligned}$$

i.e., an equation with only trivial solutions by Theorem B. In case (35) for $k = 5$ we obtain with (33)

$$\begin{aligned} 0 &= 3 \cdot 2a - 2 \cdot 3a = 3 \cdot ((a+b) + (a-b)) - 2 \cdot ((a-2b) + 2(a+b)) \\ &= 3 \cdot (c_3^5 + 3^4 c_5^5) - 2 \cdot (2c_4^5 + 2c_3^5) = -c_3^5 + (3c_5)^5 - 4c_4^5, \end{aligned}$$

and we have only trivial solutions by Theorem A. So the proof of Proposition 4 is complete.

Proof of the Theorem. By the transformation $x \mapsto x - 3$ equation (2) turns into

$$y^k = x(x^2 - 1)(x^2 - 4). \tag{37}$$

Since x and y are rational numbers, we have $x = a/b$ and $y = c/d$ for suitable integers $a, b > 0, c$ and $d > 0$ satisfying $(a, b) = (c, d) = 1$. We obtain from (37)

$$\frac{c^k}{d^k} = \frac{a(a^2 - b^2)(a^2 - 4b^2)}{b^5}.$$

By virtue of $(a, b) = (c, d) = 1$ this is equivalent with

$$c^k = a(a^2 - b^2)(a^2 - 4b^2) \quad \text{and} \quad b^5 = d^k. \tag{38}$$

The second identity implies that $b = b_1^{k^*}$ for some positive integer b_1. Since $(a, b) = 1$ it follows from (3) and (4) that Propositions 1–4 cover all possible values of G_1 and G_2. Hence $c = 0$, and consequently $y = 0$ in (2), which proves the theorem.

References

1. H. Darmon and L. Merel, Winding quotients and some variants of Fermat's Last Theorem, *J. reine angew. Math.* 490 (1997), 81–100.
2. L. E. Dickson, *History of the Theory of Numbers*, volume II. Carnegie Institute of Washington, (1919).
3. P. Erdös and J. L. Selfridge, The product of consecutive integers is never a power, *Illinois J. Math.* 19 (1975), 292–301.

4. G. Faltings, Endlichkeitssätze für abelsche Varietäten über Zahlkörpern, *Invent. math.* 73 (1983), 349–366.
5. B. Poonen, Some diophantine equations of the form $x^n + y^n = z^m$, *Acta Arith.* 86 (1998), 193–205.
6. K. A. Ribet, On the equation $a^p + 2^\alpha b^p + c^p = 0$, *Acta Arith.* 79 (1997), 7–16.
7. J. W. Sander, Rational points on a class of superelliptic curves, *J. London Math. Soc* (2) 59 (1999), 422–434.
8. J. P. Serre, Sur les représentations modulaires de degré de *Gal* $(\bar{\mathbb{Q}}/\mathbb{Q})$, *Duke Math. J.* 54 (1987), 179–230.
9. A. Wiles, Modular elliptic curves and Fermat's Last Theorem, *Ann. Math.* 141 (1995), 443–551.

M. Lakhal and J. W. Sander,
Institut für Mathematik,
Universität Hannover,
Welfengarten 1,
30167 Hannover,
Germany.

11D41: *NUMBER THEORY; Diophantine equations; Higher degree equations. Fermat's equation.*

Received on the 11*th of November*, 2002