GLASNIK MATEMATIČKI
Vol. 47(67)(2012), 61 – 79

SOME APPLICATIONS OF THE *abc*-CONJECTURE TO THE DIOPHANTINE EQUATION $qy^m = f(x)$

Ivica Gusić
University of Zagreb, Croatia

Abstract. Assume that the *abc*-conjecture is true. Let f be a polynomial over $\mathbb{Q}$ of degree $n \geq 2$ and let $m \geq 2$ be an integer such that the curve $y^m = f(x)$ has genus ≥ 2. A. Granville in [3] proved that there is a set of exceptional pairs (m, n) such that if (m, n) is not exceptional, then the equation $dy^m = f(x)$ has only trivial rational solutions, for almost all m-free integers d. We prove that the result can be partially extended on the set of exceptional pairs. For example, we prove that if f is completely reducible over $\mathbb{Q}$ and $n \neq 2$, then the equation $qy^m = f(x)$ has only trivial rational solutions, for all but finitely many prime numbers q.

1. Introduction

Let f be a polynomial over $\mathbb{Q}$ of degree $n \geq 2$ and let $m \geq 2$ be an integer such that the curve $y^m = f(x)$ has genus ≥ 2. Let d be an m-free integer. Assume that the equation $dy^m = f(x)$ has a nontrivial rational solution (i.e., the solution that does not come from a rational root of f). Put $x = \frac{r}{s}$ where r, s are coprime integers. A. Granville proved that, if the *abc*-conjecture is true, then there exists $\delta > 0$ (dependent only on (m, n)) such that

$$|r|, |s| \ll_f |d|^{\delta + o(1)}. \tag{1.1}$$

Using (1.1), he proved that if $\delta < \frac{1}{2}$ then the equation $dy^m = f(x)$ has no nontrivial rational solutions for almost all d (see Corollary 2.5). Unfortunately, there is an infinite set of exceptional pairs (m, n) for which $\delta \geq \frac{1}{2}$ holds. The purpose of this paper is to prove that a similar result is valid for the equations of the type $qy^m = f(x)$ with prime q, even for the exceptional pairs (m, n) (Theorem 4.3 and Theorem 4.5).

2010 *Mathematics Subject Classification.* 11D45, 11D41.
Key words and phrases. abc-conjecture, Diophantine equation.

In Section 2 we describe Granville's results on equation $dy^m = f(x)$ with m-free d (modulo the *abc*-conjecture). In Section 3 we apply (1.1) to a question on diophantine equations with separate variables (Theorem 3.5). In Section 4 we extend Granville's results to the equation $qy^m = f(x)$ with prime q (Theorem 4.3 and Theorem 4.5).

2. The equation $dy^m = f(x)$

In this section we describe Granville's results from [3] concerning the equations $dy^m = f(x)$.

THE *abc*-CONJECTURE (Oesterlé, Masser, Szpiro). *If a, b, c are coprime positive integers satisfying $a + b = c$ then*

$$c \ll \Big(\prod_{p|abc} p\Big)^{1+o(1)}$$

In this paper we need the following important consequence of the abc-conjecture.

LEMMA 2.1. *Assume that the abc-conjecture is true. Suppose that $G \in \mathbb{Z}[X,Y]$ is homogenous, without repeated roots. Then for any coprime integers r, s*

$$\prod_{p|G(r,s)} p \gg_G \max\{|r|, |s|\}^{\deg(G)-2-o(1)}.$$

PROOF. See, for example, [3, Proposition 2.1]. ∎

Using the estimation from Lemma 2.1, A. Granville proved the following result.

LEMMA 2.2. *Assume that the abc-conjecture is true. Let $f \in \mathbb{Z}[X]$ be a polynomial of degree $n \geq 2$ without repeated roots, and let $m \geq 2$ be an integer such that the curve $y^m = f(x)$ has genus $g \geq 2$. Let d be an integer not divisible by the mth power of any prime. Assume that a rational pair (x, y) with $x = \frac{r}{s}$ where r, s are coprime satisfies*

$$dy^m = f(x).$$

Then

$$|r|,\ |s| \ll_f |d|^{\frac{1}{n-1-\frac{\gcd(m,i)+1}{m-1}}+o(1)} \tag{2.1}$$

where $n = k \cdot m + i$ with $1 \leq i \leq m$.

PROOF. In the case $m = 2$, by [3, Theorem 1.1(ii)], we have

$$|r|, |s| \ll |d|^{\frac{1}{2g-2}+o(1)}.$$

Therefore we have to prove that it coincides with (2.1) for $m = 2$. Note that $\ll$ here depends only on f (see [3, Section 2, Proof of Theorem 1.1, for rational points, after Corollary 2.2]). Since the curve $y^2 = f(x)$ is hyperelliptic we have $g = \lfloor \frac{n-1}{2} \rfloor$ (especially, we have $n \geq 5$). We have to prove that $2g - 2 = n - 1 - \frac{\gcd(m,i)+1}{m-1}$. Assume first that n is odd. Then $2g - 2 = n - 3$. On the other side, we have $i = 1$, hence $n-1-\frac{\gcd(m,i)+1}{m-1} = n-1-\frac{1+1}{1} = n-3$. Assume now that n is even. Then $2g - 2 = n - 4$. On the other side, we have $i = 2$, hence $n - 1 - \frac{\gcd(m,i)+1}{m-1} = n - 1 - \frac{2+1}{1} = n - 4$.

In the case $m \geq 3$ the relation (2.1) coincides with (11.1) from [3, Section 11]. □

Remark 2.3. (i) We have seen in the proof of Lemma 2.2, that the condition $g \geq 2$ on the genus of the curve $y^m = f(x)$ for $m = 2$, is equivalent with $n \geq 5$. If $m \geq 3$, then the corresponding curve is superelliptic which genus g satisfies $2g-2 = mn-m-n-\gcd(m,n)$ (see, for example, [7, Exercise A.4.6] or [9, p. 401, formula (4)]). Especially,

(a) if $m = 3$ then $g \geq 2$ if and only if $n \geq 4$,
(b) if $m = 4$ then $g \geq 2$ if and only if $n \geq 3$,
(c) if $m \geq 5$ then $g \geq 2$ for each $n \geq 2$.

(ii) By Lemma 2.2, under the abc-conjecture, the size of a rational solution of the equation $dy^m = f(x)$ depends on the value $\gamma(m,n) := n - 1 - \frac{\gcd(m,i)+1}{m-1}$. It can be easily checked the following:

(a) $\gamma(2,5) = \gamma(2,6) = 2$ and $\gamma(2,n) \geq 3$ for $n \geq 7$,
(b) $\gamma(3,4) = 2$ and $\gamma(3,n) \geq 3$ for $n \geq 5$,
(c) $\gamma(4,3) = \gamma(4,4) = \frac{4}{3}$ and $\gamma(4,n) > 2$ for $n \geq 5$,
(d) $\gamma(5,3) = \frac{3}{2}, \gamma(6,3) = \frac{6}{5}$ and $\frac{6}{5} \leq \gamma(m,3) < 2$ for each $m \geq 4$,
(e) $\gamma(5,2) = \frac{1}{2},\ \gamma(6,2) = \frac{2}{5}$ and $\frac{4}{7} \leq \gamma(m,2) < 1$ for each $m \geq 7$.

Definition 2.4. *We say that a pair (m,n) from Remark 2.3 is exceptional if the condition $\gamma(m,n) \leq 2$ holds.*

Let us fix a positive integer D, and consider an equation $dy^m = f(x)$ with $|d| \leq D$ (as in [3]). Then, if (r,s) is as in Lemma 2.2, we have

$$|r|,\ |s| \ll_f D^{\frac{1}{n-1-\frac{\gcd(m,i)+1}{m-1}}+o(1)}.$$

Since each such (r,s) with $f(\frac{r}{s}) \neq 0$ participates in a unique equation $dy^m = f(x)$ with m-free d, we see that there are $\ll_f D^{\frac{2}{n-1-\frac{\gcd(m,i)+1}{m-1}}+o(1)}$ equations $dy^m = f(x)$ with $|d| \leq D$, that have nontrivial rational solutions. Here, we say that a solution is trivial if it comes from a rational root of f. For the sake of brevity, we will say that $dy^m = f(x)$ has only trivial rational solutions for almost all m-free d, if

$$\lim_{D \to +\infty} \frac{\sharp\{d : |d| \leq D,\ d \text{ is } m-\text{free and } dy^m = f(x) \text{ has a nontriv. sol.}\}}{\sharp\{d : |d| \leq D \text{ and } d \text{ is } m-\text{free}\}} = 0$$

holds. The above discussion leads to the following corollary of Lemma 2.2.

Corollary 2.5 ([3, Cor. 1.2 and sect. 11]). *Let the notation be as in Lemma 2.2. Assume that the curve $y^m = f(x)$ is of genus ≥ 2, and that neither of the following conditions is satisfied*

(i) $n = 5$ *or* $n = 6$, *and* $m = 2$,
(ii) $n = 4$ *and* $m = 3$ *or* $m = 4$,
(iii) $n = 3$ *and* $m \geq 4$,
(iv) $n = 2$ *and* $m \geq 5$.

Then for almost all m-free integers d, the equation

$$dy^m = f(x)$$

has only trivial rational solutions.

Proof. For the convenience of readers we present a proof. Recall first that, by Remark 2.3 (i), if $m = 2$ then $n \geq 5$, if $m = 3$ then $n \geq 4$, and if $m = 4$ then $n \geq 3$. Let us put $\delta := \frac{1}{n-1-\frac{\gcd(m,i)+1}{m-1}}$. By Remark 2.3 (ii), if (m, n) does not satisfy any of conditions (i)-(iv) (i.e., if (m, n) is not exceptional), then $\delta < \frac{1}{2}$. Therefore there exists a real number δ' with $0 < 2\delta' < 1$ such that, for sufficiently large D, there are $\leq D^{2\delta'}$ m-free integers d with $|d| \leq D$, such that the equation $dy^m = f(x)$ has a nontrivial rational solution (note that $\ll$ in (2.1) depends only on f, which is fixed here). It is a classical fact that the set of m-free integers has density $\frac{1}{\zeta(m)}$ (in the set of integers), where ζ denotes the Riemann zeta function (see, for example, [17]). Therefore, for almost all m-free integers d, the equation $dy^m = f(x)$ has only trivial rational solutions. $\square$

3. A question on diophantine equations with separated variables

As an illustration, we apply estimation (2.1) to a question on the diophantine equations with separable variables. Yuri Bilu observed (published in [4, Proposition 3]) that if f is a polynomial over $\mathbb{Q}$ of degree $n \geq 2$, and m is a composite positive integer, then there exists a polynomial g over $\mathbb{Q}$ of degree m, such that the equation $g(y) = f(x)$ has no rational solutions.

Question 3.1. *Let f be a polynomial over $\mathbb{Q}$ of degree $n \geq 2$ and let m be a prime number. Does there exist a polynomial g over $\mathbb{Q}$ of degree m, such that the equation $g(y) = f(x)$ has no rational solutions?*

The answer is positive if $n = 2$, $(m, n) = (2, 3)$, or if $m|n$ (see Proposition 3.4 below). We demonstrate that if the abc-conjecture is true, then the answer is positive in the remaining cases, too (Theorem 3.5).

Definition 3.1. *We say that a subset P of the set of prime numbers has density ρ if*

$$\lim_{X\to\infty} \frac{\sharp\{p \in P : p \leq X\}}{\pi(X)} = \rho,$$

where $\pi(X)$ denotes the number of primes that are $\leq X$.

Lemma 3.2. *Let f be an irreducible polynomial over $\mathbb{Z}$ of degree $n \geq 2$. Then the set of primes p, such that f has no roots modulo p, has the density $\geq \frac{1}{n}$.*

Proof. See for example [15, Theorem 1 and Theorem 2]. $\square$

Remark 3.3. In Question 3.1 we may assume that the polynomial f is $\mathbb{Q}$-irreducible, defined over $\mathbb{Z}$ and monic. Namely the polynomial $\Phi \in \mathbb{Q}[x,t]$, defined by $\Phi(x,t) := f(x) - t$, is irreducible. By the Hilbert irreducibility theorem (see, for example, [14, Theorem 46]), there exists a rational number α such that $\Phi(x,\alpha)$ is $\mathbb{Q}$-irreducible. Since f (from Question 3.1) can be replaced by $f-\alpha$, for each rational α, we may assume that f is $\mathbb{Q}$-irreducible. Since f can be replaced by λf, for each nonzero $\lambda \in \mathbb{Q}$, we may assume that f is defined over $\mathbb{Z}$ (and $\mathbb{Q}$-irreducible). Similarly, if $f(x) = a_n x^n + ... + a_0$, then

$$f(x) = \frac{(a_n x)^n + a_{n-1}(a_n x)^{n-1} + ... + a_1 a_n^{n-2}(a_n x) + a_0 a_n^{n-1}}{a_n^{n-1}}.$$

Therefore we may assume that f is monic.

Proposition 3.4. *Let f be a polynomial over $\mathbb{Q}$ of degree $n \geq 2$ and let m be a prime number. Assume that one of the following conditions holds:*

(i) $n = 2$,
(ii) $(m,n) = (2,3)$,
(iii) $m|n$.

Then there exists a polynomial g over $\mathbb{Q}$ of degree m, such that the equation $g(y) = f(x)$ has no rational solutions.

Proof. (i) The cases $m = 2$ and $m = 3$ follow from the fact that there are affine conics and elliptic curves over $\mathbb{Q}$ without rational points. For $m = 5$ we may use the fact that $4y^5 - 1 = dx^2$ has no rational solutions for infinitely many square-free d, see([11, Theorem 4]), or the fact that the equation $y^5 + A = x^2$ has no rational solutions for $A = -3, -13, -37, -38, -52, ...$ (see [19, Corollary 3.2]). Assume that $m \geq 7$. Let h be a cubic polynomial such that the equation $z^2 = h(y)$ has no rational solutions, and let r be a $\mathbb{Q}$-irreducible polynomial of degree $\frac{m-3}{2}$. Then the equation

$$r(y)^2 h(y) = x^2$$

has no rational solutions.

(ii) By Remark 3.3, we may assume that $f(x) = x^3 + ax^2 + bx + c$ is irreducible. Consider the elliptic curve

$$E : y^2 = x^3 + ax^2 + bx + c.$$

Then there are infinitely many square-free integers d such that the quadratic twist $E_d : dy^2 = x^3+ax^2+bx+c$ has rank zero (see, for example, [12, Corollary 3] and note that elliptic curves over $\mathbb{Q}$ are modular). Now, the positive answer to the question follows from the fact that there are only finitely many square-free d such that E_d has a rational torsion point of order > 2 (see [16, exercise 8.17(d)] or [10, Lemma 5.5] for a proof over number fields).

(iii) By Remark 3.3, we may assume that $f \in \mathbb{Z}[X]$ is irreducible and monic. By Lemma 3.2, there is a prime number p such that f has no roots modulo p. Then the equation $py^m = f(x)$ has no rational solutions. Namely, if (a, b) is a solution, then $a \neq 0$ and $b \neq 0$. Let v_p denote the discrete valuation at p. If $v_p(a) \geq 0$, then $v_p(f(a)) \geq 0$, and so $v_p(f(a)) = 0$. It implies $mv_p(b) = -1$, a contradiction. On the other side, if $v_p(a) < 0$, then $v_p(f(a)) = nv_p(a)$, which implies $mv_p(b)+1 = nv_p(a)$. It is in a contradiction with $m|n$. ∎

Note that Question 3.1 can be stated over any algebraic number field. Using recent results of B. Mazur and K. Rubin ([10]) on the 2-Selmer groups of elliptic curves, it can be proved that the answer is positive in the case $n = 3,\ m = 2$, see [5]. Note also that the statement from Proposition 3.4 holds unconditionally, in contrast to the rest of the article where the results usually depend on the *abc*-conjecture. From this point on, we follow [3].

THEOREM 3.5. *Assume that the abc-conjecture is true. Then the answer to Question 3.1 is positive.*

PROOF. The answer is positive unconditionally for $n = 2$ or $(m, n) = (2, 3)$, or $m|n$ (see Proposition 3.4). By Remark 3.3, in the remaining cases we may assume that $f \in \mathbb{Z}[X]$ is irreducible and monic (especially, f is without repeated roots). We will see that the *abc*-conjecture implies that there is an integer $d \neq 0$ such that the equation

$$dy^m = f(x)$$

has no rational solutions. It follows directly from Corollary 2.5, assuming that (m, n) does not satisfy any of the following conditions

(i) $n = 5$ and $m = 2$,
(ii) $n = 4$ and $m = 3$,
(iii) $n = 3$ and $m \geq 5$.

Assume that one of conditions (i), (ii), (iii) holds. We will show that there is a prime q such that the equation

$$qy^m = f(x)$$

has no rational solutions (in fact we will prove that there is a positive proportion of such primes q). Since f is irreducible there is no trivial solutions. For each rational number $x = \frac{r}{s}$, with relatively prime integers r, s, we have

$$f(\frac{r}{s}) = \frac{s^{m-i}F(r,s)}{s^{(k+1)m}}$$

where $n = k \cdot m + i$ with $1 \leq i \leq m$ and $F(r,s) := s^n f(\frac{r}{s})$. Note that each pair (r,s) determines at most one prime q with

$$qt^m = s^{m-i}F(r,s), \ t \in \mathbb{Z}. \tag{3.1}$$

Each integer solution of (3.1) leads to a rational solution of the equation $qy^m = f(x)$ with $x = \frac{r}{s}$. On the other side, if $qy^m = f(\frac{r}{s})$ holds for some rational y, then $q(ys^{k+1})^m = s^{m-i}F(r,s)$. Since $m \geq 2$ we see that ys^{k+1} is an integer. Therefore, for each (r,s) there is at most one prime number q such that the equation $qy^m = f(x)$ has a rational solution with $x = \frac{r}{s}$. If (r,s) leads to a solution of an equation of type (3.1), then we will say that (r,s) determines the prime number q.

By Remark 2.3, we have $\gamma(2,5) = \gamma(3,4) = 2$ and $\gamma(m,3) \geq \frac{6}{5}$ for each $m \geq 5$. In any case, by (2.1), if (r,s) determines some q, then $|r|, |s| \ll_f q^{\frac{5}{6}+o(1)}$ (note that since m is a prime number and since $m \geq 5$ for $n = 3$, we can find a better estimation, but this one will be sufficient for our purpose). By the definition, it means that for each $\epsilon > 0$ there exists a constant $K_\epsilon > 0$, dependent only on f and ϵ, such that $|r|, \ |s| \leq K_\epsilon q^{\frac{5}{6}+\epsilon}$. Let S be the set of prime numbers p such that f has no roots modulo p. By Lemma 3.2 we know that S has density $\geq \frac{1}{n}$, especially S is infinite. Therefore, there exists $q \in S$ such that $K_\epsilon q^{\frac{5}{6}+\epsilon} < q$ for $\epsilon = 0.01$. We claim that the equation $qy^m = f(x)$ has no nontrivial rational solutions. Contrary, there exist integers r, s, t with $s, t \neq 0$ and r, s coprime such that (3.1) holds. Since $|s| < q$, we see that q does not divide s. Since $q \in S$, we see that q does not divide $F(r,s)$. It is a contradiction. Note that, in fact, we have proved that the equation $qy^m = f(x)$ has no nontrivial rational solutions, for all but finitely many $q \in S$. ∎

4. The equation $qy^m = f(x)$

In this section we assume that f is a polynomial over $\mathbb{Z}$ of degree $n \geq 2$ without repeated roots, and that $m \geq 2$ is such that the genus g of the curve $y^m = f(x)$ is ≥ 2. A. Granville conjectured that a stronger version of Corollary 2.5. holds even for exceptional pairs (m,n). To be more precise, he conjectured that there is a constant κ'_f, such that there are $\sim \kappa'_f D^{\frac{1}{g+1}}$ squarefree integers d with $|d| \leq D$, for which $dy^2 = f(x)$ has a nontrivial rational solution (see [3, Conjecture 1.3(ii)]). He also conjectured that there are $\sim \kappa'_{f,m} D^{\frac{2}{n}}$ squarefree integers d with $|d| \leq D$, for which $dy^m = f(x)$ with

$m \geq 3$, has a nontrivial rational solution (see [3, Section 11, p. 22]). The estimate (2.1) is too weak to prove that conjecture. Nevertheless, it enables us to prove that there are a lot of prime numbers q, such that the equation $qy^m = f(x)$ has no nontrivial rational solutions, even in the exceptional cases (see Theorem 4.3 and Theorem 4.5 for a more precise formulation). Unlike the case of Theorem 3.5, where we could assume that f is $\mathbb{Q}$-irreducible, now we have to consider the reducible polynomials, too. Also, the set of exceptional cases is wider now, since we have to include the equations with $n = 2$, as well as the cases when m is not prime.

For a natural number u, let $d(u)$ denote the number of divisors of u, and let $\omega(u)$ denote the number of distinct prime factors of u. Also, let $p_n\sharp$ denote the n-th primorial number (the product of the first n prime numbers).

LEMMA 4.1. *Let F be an irreducible binary form of degree $\lambda \geq 3$, with rational integer coefficients. Then the number of primitive solutions of the equation $|F(r, s)| = u$ does not exceed $c_1\lambda^{1+\omega(u)}$, where c_1 is an absolute constant (here we say that a solution (r, s) is primitive if r, s are coprime integers).*

PROOF. See [1, Theorem, p. 69-70] □

The following lemma will be used in a part of the proof of Theorem 4.5.

LEMMA 4.2. *Let M denotes arbitrary positive integer.*

(i) *Let $\nu(u)$ denote the number of integer solutions of equation $r^2 + As^2 = u$, with $A, u \in \mathbb{N}$. Then, for $a \in \mathbb{Z}$ and sufficiently large X,*

$$\sum_{1 \leq u \leq X} \nu(au^M) \ll X^{1+o(1)} \ln X.$$

(ii) *Let $\nu_X(u)$ denote the number of integer solutions of equation $r^2 - As^2 = u$, with $|r|, |s| \leq X$, where $A \in \mathbb{N}$ is not a square. Then, for $a \in \mathbb{Z}$ and sufficiently large X, Y,*

$$\sum_{1 \leq u \leq Y} \nu_X(au^M) \ll Y^{1+o(1)} \ln X \ln Y.$$

(iii) *Let F be an irreducible cubic form over $\mathbb{Z}$, and let $\nu(u)$ denote the number of primitive integer solutions of the equation $F(r, s) = u$ (i.e., the solutions with coprime integers r, s). Then, for $a \in \mathbb{Z}$ and sufficiently large X*

$$\sum_{1 \leq u \leq X} \nu(au^M) \ll X(\ln X)^2.$$

PROOF. (i) Let us set $\alpha := r + s\sqrt{-A}$, so that the relation $r^2 + As^2 = u$ becomes $\alpha\overline{\alpha} = u$. If $(\alpha) = \prod \mathcal{P}^{ord_{\mathcal{P}}\alpha}$ is the prime factorization of the ideal (α) in the ring of integers of the quadratic field $\mathbb{Q}(\sqrt{-A})$, then $ord_{\mathcal{P}}\alpha = ord_{P}\overline{\alpha}$.

By the character of extension of rational primes in quadratic number fields, we conclude that there are at most $d(u)$ possibilities for (α). Since the ring of integers has at most six invertible elements, we see that $\nu(u) \ll d(u)$. Note that $d(uv) \le d(u)d(v)$, and $d(u^M) \le M^{\omega(u)}d(u)$ for each u, v, M. Hence,

$$\nu(au^M) \ll d(au^M) \le d(a)d(u^M) \le d(a)M^{\omega(u)}d(u).$$

Using the fact that if k is primorial then $\omega(k) \sim \frac{\ln k}{\ln\ln k}$ (see, for example, [6, p.471]), we get

$$\omega(u) = \omega(p_{\omega(u)}\sharp) \sim \frac{\ln p_{\omega(u)}\sharp}{\ln\ln p_{\omega(u)}\sharp} \le \frac{\ln X}{\ln\ln X}$$

(note that $p_{\omega(u)}\sharp \le u \le X$ and that X is sufficiently large). We see that if X is sufficiently large, then $\omega(u) \le \frac{2\ln X}{\ln\ln X}$. Therefore $M^{\omega(u)} \le M^{\frac{2\ln X}{\ln\ln X}} = (e^{\ln X})^{\frac{2\ln M}{\ln\ln X}} = X^{\frac{2\ln M}{\ln\ln X}} \ll X^{o(1)}$. Summing and using

$$\sum_{1 \le u \le X} d(u) = X\ln X + (2\gamma - 1)X + O(X^\theta),$$

where γ is Euler's constant, and $\theta \le 0.5$ (see [6, p.347-349 and 359] or [8] for a better estimation of θ), we get

$$\sum_{1 \le u \le X} \nu(au^M) \ll \sum_{1 \le u \le X} d(a)M^{\omega(u)}d(u) \ll M^{\frac{2\ln X}{\ln\ln X}} \sum_{1 \le u \le X} d(u) \ll X^{1+o(1)}\ln X.$$

(ii) We have $\nu_X(u) \ll \ln X d(u)$ for sufficiently large X (see [13, Lemma 3] for a more precise estimation). Therefore we may proceed as in (i):
$\sum_{1 \le u \le Y} \nu_X(au^M) \ll \ln X d(a) \sum_{1 \le u \le Y} M^{\omega(u)}d(u) \ll \ln X \cdot Y^{1+o(1)} \ln Y.$

(iii) By Lemma 4.1, we know that there is an absolute constant C such that

$$\nu(u) \le C \cdot 3^{\omega(u)}$$

(see also [18, Theorem 1]). Since $\omega(au^M) \le \omega(a) + \omega(u)$, and

$$\lim_{X\to\infty} \frac{1}{X(\ln X)^2} \sum_{1 \le u \le X} 3^{\omega(u)} = 0.1433...,$$

(see, for example, [2, p.111]), we get

$$\sum_{1 \le u \le X} \nu(au^M) \le \sum_{1 \le u \le X} C \cdot 3^{\omega(a)+\omega(u)} \ll \sum_{1 \le u \le X} 3^{\omega(u)} \ll X(\ln X)^2.$$

□

We will use the estimation (2.1) to prove that the equation $qy^m = f(x)$, with prime q, generally has no nontrivial rational solutions. Note that the set of prime numbers has zero density in the set of m-free numbers. Therefore, Corollary 2.5 provides no direct information about the equations $qy^m = f(x)$. However, if the pair (m, n) is not exceptional (see Definition 2.4 and Remark 2.3), then the argument from the proof of Corollary 2.5 can be applied to prove that there is a set of prime numbers q of density 1, such that the equations $qy^m = f(x)$ has no nontrivial rational solutions. In Theorem 4.3 we will get a stronger result for completely reducible polynomials f. Namely, we will prove that in that case the equation $qy^m = f(x)$ has no nontrivial rational solutions, for all but finitely many prime numbers q (assuming that $n \neq 2$). The proofs of Theorem 4.3 and Theorem 4.5 depend on the value of $\delta := \frac{1}{n-1-\frac{\gcd(m,i)+1}{m-1}}$. The most comfortable situation is when $\delta < \frac{1}{2}$ (i.e., when (m,n) is not exceptional). Less pleasant is when $\frac{1}{2} \leq \delta < 1$, and the unpleasant when $\delta > 1$ (i.e., when $n = 2$).

THEOREM 4.3. *Assume that the abc-conjecture is true. Let $f \in \mathbb{Z}[X]$ be a polynomial of degree $n \geq 2$ without repeated roots, and let $m \geq 2$ be an integer such that the curve $y^m = f(x)$ has genus ≥ 2. Assume that f is completely reducible over $\mathbb{Q}$.*

(a) *If $n \geq 3$, then for all but finitely many primes q the equation $qy^m = f(x)$ has only trivial rational solutions.*
(b) *If $n = 2$ and $m \neq 6$, then there is a set of prime numbers q of density 1 such that the equation $qy^m = f(x)$ has only trivial rational solutions.*

PROOF. (a) Let us put $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$. We can write

$$f(x) = \frac{(a_n x)^n + a_{n-1}(a_n x)^{n-1} + \ldots + a_1 a_n^{n-2}(a_n x) + a_0 a_n^{n-1}}{a_n^{n-1}} = \frac{g(x')}{a_n^{n-1}},$$

where $x' := a_n x$. Set $a_n^{n-1} = bu^m$ where b is m-free integer. Note that g is defined over $\mathbb{Z}$ and monic. We see that it is enough to prove that, for all but finitely many prime numbers q, the equation

$$qby^m = g(x) \tag{4.1}$$

has only trivial rational solutions. Further, since b depends only on f (i.e., since $|b| \ll_f 1$), we may assume that $\gcd(q,b) = 1$ (in other words, we exclude from the consideration a finitely many primes q that divide b). For each rational number $x = \frac{r}{s}$ with relatively prime integers r, s, we have

$$g(\frac{r}{s}) = \frac{s^{m-i}G(r,s)}{s^{(k+1)m}}$$

where $n = k \cdot m + i$ with $1 \leq i \leq m$ and $G(r,s) := s^n g(\frac{r}{s})$ (here we may exclude $r = 0$ since it leads to at most one q). Each pair (r,s) determines at most one prime q with

$$qbt^m = s^{m-i}G(r,s),\ t \in \mathbb{Z}. \tag{4.2}$$

Each integer solution of (4.2) leads to the rational solution of the equation $qby^m = g(x)$ with $x = \frac{r}{s}$. On the other side, if $qby^m = g(\frac{r}{s})$ holds for some rational y, then $qb(ys^{k+1})^m = s^{m-i}G(r,s)$. Since $m \geq 2$, we see that ys^{k+1}

is an integer. Therefore, for each (r, s) there is at most one prime number q such that the equation $qby^m = g(x)$ has a rational solution with $x = \frac{r}{s}$.

Note that all roots of g are integers. Let $G = L_1 \cdot L_2 \cdot \ldots \cdot L_n$ be the product of G on linear factors over $\mathbb{Z}$. Let us put $\delta := \frac{1}{\gamma(m,n)} = \frac{1}{n-1-\frac{\gcd(m,i)+1}{m-1}}$.

Since $n \neq 2$, we have $\gamma(m, n) > 1$ (see Remark 2.3), hence $\delta < 1$. By (2.1), if $qby^m = g(x)$ has a nontrivial rational solution, with $x = \frac{r}{s}$ where r, s are coprime, then

$$|r|, |s| \ll_g |qb|^{\delta+o(1)}.$$

It means that, for each $\epsilon > 0$, there exists $K_\epsilon > 0$, such that $|r|, |s| \leq K_\epsilon |qb|^{\delta+\epsilon}$. Put $L_j(r, s) = r - \alpha_j s,\ j = 1, 2, \ldots, n$ (note that $\alpha_j \in \mathbb{Z}$ for all j). Set $A = \max_j(1 + |\alpha_j|)$ and choose $\epsilon > 0$ such that $\delta + \epsilon < 1$. Assume that $AK_\epsilon|qb|^{\delta+\epsilon} < q$ (it is satisfied for all but finitely many primes q). For such q the equation $qby^m = g(x)$ has no nontrivial rational solutions. Assume contrary, i.e., assume that there is a nontrivial solution with $x = \frac{r}{s}$. Then $q|s^{m-i}$ or $q|L_j(r, s)$ for some j. It is impossible since $q > |s|$ and $q > |L_j(r, s)|$ for all j. Namely, $|L_j(r, s)| = |r - \alpha_j s| \leq |r| + \alpha_j||s| \leq (1 + |\alpha_j|)K_\epsilon|qb|^{\delta+\epsilon} \leq AK_\epsilon|qb|^{\delta+\epsilon} < q$.

(b) We will discuss the case $m = 6$, too. Similarly as in (a), we may consider the corresponding equations $qby^m = g(x)$ and $qbt^m = s^{m-i}G(r, s)$. We have to prove that there is a set of prime numbers q of density 1 such that the equation $qby^m = g(x)$ has no nontrivial rational solutions, provided $m \neq 6$. Here $i = 2$, hence each (r, s) determines at most one prime number q such that

$$qbt^m = s^{m-2}G(r, s),\ t \in \mathbb{Z} \tag{4.3}$$

where $m \geq 5$ and G is a reducible quadratic form without double factors. Since $\gamma(m, n) \leq 1$ we can not apply directly the argument from (a).
Assume that (4.3) holds. By (2.1), and Remark 2.3, (ii)

if $m = 5$ then $|r|,\ |s| \ll_f |qb|^{2+o(1)}$,
if $m = 6$ then $|r|,\ |s| \ll_f |qb|^{2.5+o(1)}$,
if $m \geq 7$ then $|r|,\ |s| \ll_f |qb|^{1.75+o(1)}$.

Therefore, for all but finitely many q we have $|s| < q^3$, especially $v_q(s) < 3$.
After a linear transformation we may assume that $G(r, s) = r(r - \alpha s),\ \alpha \in \mathbb{Z} \setminus \{0\}$. Let D be a sufficiently large real number. We have to estimate the number of primes q with $|qb| \leq D$ such that (4.3) holds, for some (r, s) with r, s coprime. Note that, by (2.1) and Remark 2.3, (ii) we have

if $m = 5$ then $|r|,\ |s| \ll_f D^{2+o(1)}$,
if $m = 6$ then $|r|,\ |s| \ll_f D^{2.5+o(1)}$,
if $m \geq 7$ then $|r|,\ |s| \ll_f D^{1.75+o(1)}$.

We see from (4.3) that there are three possibilities for r, s: $q|s,\ q|r$ or $q|r - \alpha s$. The idea is to estimate the number of each of these possibilities, and to show that the sum is negligible compared to the number of primes q with $|qb| \leq D$. Assume first that $q|s$. Since the integers s and $G(r,s)$ are coprime (we assume that $r \neq 0$), and since we may assume that q does not divide b, by (4.3) we get $1 + mv_q(t) = (m-2)v_q(s)$. It is impossible if m is even, and it implies $v_q(s) \geq 3$ if $m \neq 5$. Therefore, the case with $q|s$ is impossible if q is sufficiently large and $m \neq 5$. It remains to consider the case $m = 5$. By (4.3) and the fact that s and $G(r,s)$ are coprime we get

$$G(r,s) = au^5$$

where $a|b$. Since $\gcd(r, r-\alpha s) \leq |\alpha|$ (for each coprime integers r, s), we get $r = a_1u_1^5$ and $r - \alpha s = a_2u_2^5$, with $u_1, u_2 \in \mathbb{N}$ and $|a_1|, |a_2| \ll_f 1$. In other words, there are finitely many such systems of equations and the number of systems is dependent only on f (for all coprime integers r, s). We see that $u_1^5, u_2^5 \ll_f D^{2+o(1)}$, hence $u_1, u_2 \ll_f D^{0.4+o(1)}$. Therefore (if D is sufficiently large) there are $\ll D^{0.41}$ possibilities both for r and $r - \alpha s$. Since $r - (r - \alpha s) = \alpha s$, we see that there are $\ll_f D^{0.82}$ possibilities for s. We claim that, if D is sufficiently large, then each s determines at most one q with $q \geq D^{0.6}$ (and $q|s$). Contrary we have

$$q_1bt_1^5 = s^3G(r_1,s) \text{ and } q_2bt_2^5 = s^3G(r_2,s),$$

with $q_1 \neq q_2, q_1|s, q_2|s$ and $q_1, q_2 \geq D^{0.6}$ (we may assume that $|b| < q_1$ and $|b| < q_2$). From $q_1|s$ we get $3v_{q_1}(s) = 1 + 5v_{q_1}(t_1)$, hence $v_{q_1}(s) \geq 2$, and similarly for q_2. Therefore, $|s| \geq q_1^2 \cdot q_2^2 \geq D^{2.4}$ (a contradiction with the fact that $|s| \ll_f D^{2+o(1)}$ and that D is sufficiently large). Now we conclude that there are $\ll_f D^{0.82}$ possibilities for q with $q \geq D^{0.6}$. Since there are $< D^{0.6}$ prime numbers q such that $q < D^{0.6}$, we conclude that, for sufficiently large D, there are $\ll_f (D^{0.6} + D^{0.82})$ prime numbers q such that the equation $qbt^m = s^{m-2}G(r,s)$ has a solution with $q|s$.

Assume now that $q|r$. From (4.3) with $G(r,s) = r(r - \alpha s)$ and the fact that r, s and $r - \alpha s, s$ are coprime, we get, for a sufficiently large q,

$$s^{m-2} = a_1u_1^m,\ r - \alpha s = a_2u_2^m,$$

where $u_1, u_2 \in \mathbb{N}$ and $|a_1|, |a_2| \ll_f 1$. As above we see that

if $m = 5$ then $u_2^m \ll_f D^{2+o(1)}$, hence $u_2 \ll_f D^{0.4+o(1)}$,
if $m = 6$ then $u_2^m \ll_f D^{2.5+o(1)}$, hence $u_2 \ll_f D^{0.417+o(1)}$,
if $m \geq 7$ then $u_2^m \ll_f D^{1.75+o(1)}$, hence $u_2 \ll_f D^{0.25+o(1)}$.

Therefore, in any case, there are $\ll D^{0.42}$ possibilities for $r - \alpha s$.

Let us estimate the number of possibilities for s. If m is odd then from $s^{m-2} = a_1u_1^m$ we get $s = b_1v_1^m$ with $|b_1| \ll_f 1$ and $v_1^m \ll_f D^{2+o(1)}$ (hence $1 \leq v_1 \ll_f D^{0.4+o(1)}$). If m is even then we get $s = b_1v_1^{\frac{m}{2}}$ with $|b_1| \ll_f 1$. This is the point when we have to exclude the case $m = 6$ (similarly happens in the case when $q|r - \alpha s$). In Remark 4.4(i), we will explain it in more details. It is easy to see that if $m \neq 6$, then $1 \leq v_1 \ll_f D^{0.4375+o(1)}$. Therefore,

there are $\ll_f D^{0.44}$ possibilities for s (if $m \neq 6$). Combining with $\ll D^{0.42}$ possibilities for $r - \alpha s$, we get that there are $\ll_f D^{0.86}$ possibilities for r. Note that r from (4.3) has at most one prime divisor p with $p \geq D^{0.6}$ (if D is sufficiently large). Contrary, from $qbt^m = s^{m-2}r(r - \alpha s)$ and $|b| \ll_f 1$, there is a common prime divisor p of r and t with $p \geq D^{0.6}$. Therefore $v_p(r) \geq 5$, hence $|r| \geq D^3$, which is in a contradiction with $|r| \ll_f D^{2.5+o(1)}$ (for sufficiently large D). Therefore, in this case, each r determines at most one prime q with $q|r$ and $q \geq D^{0.6}$ (for sufficiently large D). We conclude that there are $\ll_f (D^{0.6} + D^{0.86})$ primes q such that (4.3) holds (with $q|r$, g reducible and $(m, n) \neq (6, 2)$).
Assume, finally, that $q|r - \alpha s$. This case is completely analogous to the case $q|r$, and we get the same estimate.
To finish the proof we have to add numbers of possibilities for q with $q|s$, $q|r$ and $q|r - \alpha s$. We obtain that this sum is $\leq D^{0.9}$ (if D is sufficiently large). Since there are $\sim \frac{\frac{D}{|b|}}{\ln \frac{D}{|b|}}$ prime numbers q with $|qb| \leq D$, and since

$$\lim_{D\to\infty} \frac{\frac{D}{|b| \ln \frac{D}{|b|}} - D^{0.9}}{\frac{D}{|b| \ln \frac{D}{|b|}}} = 1,$$

we conclude that there is a set of prime numbers of density 1, such that the equation $qby^m = g(x)$ has only trivial rational solutions (if g is reducible of degree $n = 2$ and $m = 5$ or $m \geq 7$). $\square$

In the following Remark we will comment the exceptional case $(m, n) = (6, 2)$ with f reducible.

Remark 4.4. (i) In the proof of Theorem 4.3 (b), the case $(m, n) = (6, 2)$ with $q|r$ (similarly with $q|r - \alpha s$), we have obtained the relation $s = b_1 v_1^3$ where $|b_1| \ll_f 1$. Therefore $v_1^3 \ll_f D^{2.5+o(1)}$, hence $1 \leq v_1 \ll_f D^{\frac{5}{6}+o(1)}$. It implies that there are $\ll_f D^{\frac{5}{6}+o(1)}$ possibilities for s. We know that there are $\ll_f D^{\frac{5}{12}+o(1)}$ possibilities for $r - \alpha s$. Therefore, we only can conclude that there are $\ll_f D^{\frac{5}{6}+\frac{5}{12}+o(1)}$ possibilities for r. It is not useful since $\frac{5}{6} + \frac{5}{12} \geq 1$.

(ii) After a linear transformation over $\mathbb{Z}$, we may write $g(x) = x^2 - A^2$ for a positive integer A. Namely, here we have $f(x) = a_2x^2 + a_1x + a_0$ with $a_2, a_1, a_0 \in \mathbb{Z}$ and $a_2 \neq 0$. The equation $qy^6 = f(x)$ can be written in the form $q \cdot 4a_2y^6 = (2a_2x)^2 + 2a_1(2a_2x) + 4a_2a_0$. Since f is reducible, after a linear transformation of x and y over $\mathbb{Z}$, we get $qby^6 = x^2 - A^2$ where b is 6-free and A is a positive integer. It defines the family of hyperelliptic genus two curves with equation $x^2 = qby^6 + A^2$ (here b and A are fixed, while q runs through the set of prime numbers). As we have already seen in (i), our approach does not give any result in this case.

In the case when f has at least one nonlinear $\mathbb{Q}$-irreducible factor we will obtain a weaker result compared with the result from Theorem 4.3. Recall that a pair (m, n) is exceptional if one of the following conditions is satisfied:

(i) $n = 5$ or $n = 6$, and $m = 2$,
(ii) $n = 4$ and $m = 3$ or $m = 4$,
(iii) $n = 3$ and $m \geq 4$,
(iv) $n = 2$ and $m \geq 5$.

In Theorem 4.5 we will say that an exceptional pair (m, n) is conditionally exceptional if one of the following conditions is satisfied:

E_1 $(m, n) \in \{(2, 6), (4, 4), (6, 3)\}$ and f is $\mathbb{Q}$-irreducible.
E_2 $(m, n) = (2, 6)$ and f is a product of a quadratic and a quartic irreducible polynomial over $\mathbb{Q}$.

THEOREM 4.5. *Assume that the abc-conjecture is true. Let $f \in \mathbb{Z}[X]$ be a polynomial of degree $n \geq 2$ without repeated roots having at least one nonlinear irreducible factor over $\mathbb{Q}$. Let $m \geq 2$ be an integer such that the curve $y^m = f(x)$ has genus ≥ 2.*

(a) *Assume that $n \neq 2$ and that (m, n) is not conditionally exceptional (see the above conditions E_1, E_2). Then there exists a set of prime numbers q of density 1 such that the equation $qy^m = f(x)$ has no nontrivial rational solutions.*
(b) *Assume that $n = 2$. Then there exists a set of prime numbers q of density at least $\frac{1}{2}$ such that the equation $qy^m = f(x)$ has no rational solutions.*

PROOF. (a) Similarly as in the proof of Theorem 4.3 we may consider the corresponding equations $qby^m = g(x)$ and $qbt^m = s^{m-i}G(r, s)$. We have to prove that there is a set of prime numbers q of density 1 such that the equation $qby^m = g(x)$ has no nontrivial rational solutions. Let us put

$$\delta := \frac{1}{n - 1 - \frac{\gcd(m,i)+1}{m-1}}.$$

Let D be a sufficiently large real number. We consider the equations of type $qby^m = g(x)$ with $|qb| \leq D$. By (2.1), if $qby^m = g(x)$ has a nontrivial rational solution with $x = \frac{r}{s}$ and with r, s coprime, then

$$|r|, |s| \ll_g |qb|^{\delta + o(1)}.$$

Assume first that (m, n) is not exceptional, i.e., that $\delta < \frac{1}{2}$. Since each (r, s) gives rise to at most one equation, there are $\ll_g |qb|^{2\delta + o(1)}$ prime numbers q such that the equation $qby^m = g(x)$ has a nontrivial rational solution. Since $2\delta < 1$ and since there are $\sim \frac{\frac{D}{|b|}}{\ln \frac{D}{|b|}}$ prime numbers q with $|qb| \leq D$, we conclude, as at the end of the proof of Theorem 4.3, (b), that there is a set of prime numbers q of density 1 such that the equation $qby^m = g(x)$ has no nontrivial rational solutions.

Assume now that (m, n) is exceptional. The proof depends on the reducibility properties of f (or g) over $\mathbb{Q}$, as well as on the value of δ. Since $n \neq 2$ we have $\frac{1}{2} \leq \delta < 1$. We separately consider the cases when $m \neq i$ and when $m = i$ (see the formulation of Lemma 2.2).

Assume that $m \neq i$, i.e, that $(m, n) \neq (2, 6)$ and $(m, n) \neq (4, 4)$. Assume that $qby^m = g(x)$ has a nontrivial rational solution with $x = \frac{r}{s}$ and with r, s coprime. Since s and $G(r, s)$ are coprime, we conclude, by $qbt^m = s^{m-i}G(r, s)$, that $q|s$ or $q|G(r, s)$. Similarly as in the proof of Theorem 4.3, we have that $q > |s|$ for all but finitely many q. Therefore, for sufficiently large q, it must be $q|G(r, s)$. Therefore

$$s^{m-i} = au^m$$

for $u \geq 1$ and $|a| \ll_f 1$. We will separately discuss the cases $(m, n) = (2, 5)$, $(m, n) = (3, 4)$, and $(m, n) = (m, 3)$ with $m \geq 4$.

If $(m, n) = (2, 5)$ then we get $s = au^2$, hence $1 \leq u \ll D^{0.25+0(1)}$ (recall that here $\delta = 0.5$, hence $|s| \ll_f D^{0.5+o(1)}$). Therefore there are $\ll_f D^{0.25+o(1)}$ possibilities for s. Since there are $\ll_f D^{0.5+o(1)}$ possibilities for r, we see that there are $\ll_f D^{0.75+o(1)}$ equations $qby^2 = g(x)$ with $|qb| \leq D$ having a nontrivial rational solution. Therefore there exists a set of prime numbers q of density 1, such that $qy^2 = f(x)$ has no nontrivial rational solutions.

Similarly, if $(m, n) = (3, 4)$ then we get $s^2 = au^3$. It must be $s = a_1v^3$, hence $v \ll D^{\frac{1}{6}+o(1)}$ (recall that here $\delta = \frac{1}{2}$). Therefore we may proceed as for $(m, n) = (2, 5)$.

For $(m, 3)$ with $m \geq 4$ we have $i = 3$, hence $s^{m-3} = au^m$. We will see that this case, for $m \neq 6$, is similar to the case $(m, n) = (2, 5)$. If m is not divisible by 3 we get $s = a_1v^m$ with $v \geq 1$ and $|a_1| \ll_f 1$. Here we get that there are $\ll D^{\frac{\delta}{m}}$ possibilities for s. It is easy to check that $\delta + \frac{\delta}{m} < 1$ for each m (not divisible by 3). Therefore we may proceed as for $(m, n) = (2, 5)$. Let us consider the case when m is divisible by 3. From $s^{m-3} = au^m$ we get $s = a_1v^{\frac{m}{3}}$, with $v \geq 1$ and $|a_1| \ll_f 1$. It implies that there are $\ll D^{\frac{3\delta}{m}}$ possibilities for s. It is easy to check that if $m \geq 9$, then $\delta + \frac{3\delta}{m} < 1$. Therefore, for $m \geq 9$, we can proceed as for $(m, n) = (2, 5)$. The remaining case is $m = 6$, hence $\delta = \frac{5}{6}$. Unfortunately, here we have $\delta + \frac{3\delta}{m} > 1$. It is a reason why we have excluded irreducible polynomials f. Therefore g has a rational root. We may assume that $g(0) = 0$, hence we have $qbt^6 = s^3rK(r, s)$, with quadratic K. Similarly as in the proof of Theorem 4.3, using (2.1), we conclude that q does not divide rs for all sufficiently large q. Since the common factors of r and $K(r, s)$ are bounded by an absolute constant (dependent only on f) we get, for sufficiently large q,

$$r = a_2z^6$$

with $z \geq 1$ and $|a_2| \ll_f 1$ (recall that here we may consider only the primes q not dividing sr). We see that there are $\ll_f D^{\frac{\delta}{6}}$ possibilities for r. Since $\frac{3\delta}{6} + \frac{\delta}{6} < 1$ we are done.

Assume now that $m = i$, i.e, that $(m, n) = (2, 6)$ or $(m, n) = (4, 4)$.

We first consider the case when f has at least one rational root (especially, (m, n) is not conditionally exceptional). Similarly as in the case $(m, n) = (6, 3)$ we may assume that $qbt^m = rK(r, s)$. Similarly as in the proof of Theorem 4.3 we conclude that q does not divide r, for all sufficiently large q. Since the common factors of r and $K(r, s)$ are bounded by an absolute constant (dependent only on f) we get, for sufficiently large q,

$$r = au^m$$

with $u \geq 1$ and $|a| \ll_f 1$. We obtain that there are $\ll_f D^{\frac{\delta}{m}}$ possibilities for r. Since $\delta = \frac{1}{2}$ for $m = 6$ and $\delta = \frac{3}{4}$ for $m = 4$ we see that, in any case, $\delta + \frac{\delta}{m} < \frac{15}{16}$. Therefore there $\ll_f D^{\frac{15}{16}+o(1)}$ equations $qby^m = g(x)$ with $|qb| \leq D$ having nontrivial rational solutions. We are done.

Assume, now, that f has no rational roots. In this case we introduce a new approach with applying Lemma 4.2. Note that we may assume that $g = hk$, where h is Q-irreducible non-linear monic polynomial over $\mathbb{Z}$, and k is a polynomial over $\mathbb{Z}$, which may be irreducible or a product of two irreducible polynomials over $\mathbb{Q}$ (recall that in this case f is not $\mathbb{Q}$-irreducible). Let $G = HK$ be the corresponding factorization. Assume that $qby^m = g(x)$ has a rational solution with $x = \frac{r}{s}$ and with r, s coprime. Then, by (2.1), we have $|r|, |s| \ll_g |qb|^{\delta+o(1)}$. Since h, k are coprime over $\mathbb{Q}$, there exist polynomials h', k' over $\mathbb{Q}$ such that

$$h'h + k'k = 1.$$

Therefore, there exist binary forms H', K' over $\mathbb{Z}$, a non-zero integer b', and a positive integer M such that

$$H'(r, s)H(r, s) + K'(r, s)K(r, s) = b's^M,$$

for all integers r, s with $s \neq 0$. Note that we consider pairs (r, s) with r, s coprime. Therefore, each common divisor of $H(r, s)$ and $K(r, s)$ is a divisor of b'. We separately estimate the possibilities when $q|H(r, s)$ and $q|K(r, s)$.

Assume first that $(m, n) = (4, 4)$, especially $\delta = \frac{3}{4}$. Then H, K are quadratic (recall that we excluded the case when f is irreducible, and that we are in the case when f has no rational roots). If $q|K(r, s)$ and q is sufficiently large, then q does not divide $H(r, s)$, hence

$$H(r, s) = au^4, \tag{4.4}$$

where $a \ll_f 1$ and u is an positive integer. Note that it means that there are finitely many possibilities for a and that the number of the possibilities depends only on g (i.e., on f). Since

$$|r|,\ |s| \ll_f D^{\delta+o(1)},$$

we get $u^4 \ll D^{2\cdot\delta+o(1)}$ for u from (4.4), so $u \ll D^{\frac{3}{8}+o(1)}$. Therefore, if D is sufficiently large, then $u \le D^{0.4}$ for u from (4.4). We have to estimate the number of solutions (r,s) in (4.4) for all possible u and a. After a linear transformation we may assume that $H(r,s) = r^2 + As^2$, with $A \in \mathbb{Z}$.

If $A > 0$ then by Lemma 4.2, (i) (with $M = 4$ and $X = D^{0.4}$), there are $\ll (D^{0.4})^{1+o(1)}$ pairs (r,s), for each fixed a. Since the number of parameters a in (4.4) is bounded by a constant dependent only on f, which is fixed here, we see that there are $\le D^{0.5}$ possibilities for (r,s) (assuming that D is sufficiently large). Since each (r,s) gives rise to at most one prime q, there are $\le D^{0.5}$ prime numbers q with $|qb| \le D$ such that the equation $qby^4 = g(x)$ has a rational solution with $q|K(r,s)$.

If $A < 0$, then by Lemma 4.2, (ii) (with $M = 4$ and $X = Y = D^{0.4}$), we obtain, in a similar way, that there are $\le D^{0.5}$ prime numbers q with $|qb| \le D$ such that the equation $qby^4 = g(x)$ has a rational solution with $q|K(r,s)$.

Similarly we obtain that if D is sufficiently large, then there are $\le D^{0.5}$ prime numbers q, with $|qb| \le D$, such that the equation $qby^4 = g(x)$ has a rational solution with $q|H(r,s)$. Therefore, there are $\le 2D^{0.5}$ prime numbers q, with $|qb| \le D$, such that the equation $qby^4 = g(x)$ has a rational solution. We conclude that there is a set of prime numbers q of density 1 such that the equation $qy^4 = f(x)$ has no rational solutions.

Assume now that $(m,n) = (2,6)$, especially $\delta = \frac{1}{2}$. Recall that we excluded the case when f is irreducible, as well as the case when f is a product of a quadratic and a quartic irreducible polynomials. Recall also, that we are in the case when f has no rational roots. Assume first that H, K are cubic $\mathbb{Q}$-irreducible forms. Analogously as in the case $(m,n) = (4,4)$ we get, using Lemma 4.2, (iii), with $M = 2$ and $X = D^{0.76}$, that there are $\le 2D^{0.8}$ prime numbers q, with $|qb| \le D$, such that the equation $qby^2 = g(x)$ has a rational solution (assuming that D is sufficiently large).

Assume, finally, that H is quadratic and $K = K_1K_2$ is a product of quadratic irreducible forms. If $q|K(r,s)$ then

$$H(r,s) = au^2 \tag{4.5}$$

where $a \ll_f 1$ and u is an positive integer (assuming that q is sufficiently large). It implies that $1 \le u \ll D^{0.5+o(1)}$. On the other side, if $q|H(r,s)$ and q is sufficiently large, then

$$K_1(r,s) = a_1u_1^2$$

where $a_1 \ll_f 1$ and u_1 is an positive integer (note that H, K_1, K_2 are pairwise coprime over $\mathbb{Q}$). We again obtain that $1 \le u_1 \ll D^{0.5+o(1)}$. Therefore we may proceed as in the case $(m,n) = (4,4)$.

(b) Here $n = 2$ and G is an irreducible binary quadratic form of degree $m \geq 5$. Therefore, each (r, s) determines at most one prime number q such that

$$qbt^m = s^{m-2}G(r, s),\ t \in \mathbb{Z}. \tag{4.6}$$

Assume that (4.6) holds. By (2.1), and Remark 2.3, (ii)

if $m = 5$ then $|r|,\ |s| \ll_f |qb|^{2+o(1)}$,
if $m = 6$ then $|r|,\ |s| \ll_f |qb|^{2.5+o(1)}$,
if $m \geq 7$ then $|r|,\ |s| \ll_f |qb|^{1.75+o(1)}$.

Therefore, for all but finitely many q, we have $|s| < q^3$, especially $v_q(s) < 3$.

The set S of primes q, such that the polynomial g has no roots modulo q, has the density $\frac{1}{2}$. We may assume that $G(r, s) = r^2 + As^2$, with $A \in \mathbb{Z} \setminus \{0\}$. Since s and $G(r, s)$ are relatively prime (note that we assume that $r \neq 0$), if $q \in S$ then from (4.6) we have $q|s$. Hence

$$1 + mv_q(t) = (m - 2)v_q(s)$$

(note that we excluded a finitely many prime numbers q that divide b). We see that it is impossible if m is even. If $m \neq 5$ it implies $v_q(s) \geq 3$. Namely, $2v_q(s) + 1 = m(v_q(s) - v_q(t))$, which forces $v_q(s) > 2$ if $m \neq 5$. Therefore, if $m \geq 6$, then for all but finitely many $q \in S$, the equation $qby^m = g(x)$ has no nontrivial rational solutions.

Let us consider the case $m = 5$. Let D be a sufficiently large real number. We consider the equations $qby^5 = g(x)$ with $|qb| \leq D$. By (2.1), Remark 2.3, (ii) and the discussion after Remark 2.3, we see that if $qby^5 = g(x)$ has a nontrivial solution with $x = \frac{r}{s}$ where r, s are coprime, then $|r|,\ |s| \ll_f D^{2+o(1)}$. Assume that $q \in S$. From (4.6) we get $G(r, s) = au^5$ (where $|a| \ll_f 1$, and $u \geq 1$). Since $G(r, s)$ is quadratic in r, s we see that $u^5 \ll_f D^{4+o(1)}$, hence $1 \leq u \ll_f D^{0.8+o(1)}$. By Lemma 4.2, (i) or (ii), with $M = 5$ we see that there are $\leq D^{0.9}$ possibilities for such pairs (r, s) (for sufficiently large D). Similarly as at the end of the proof of Theorem 4.3, (b), we get that there is a set of prime numbers q of the density at least $\frac{1}{2}$, such that $qby^5 = g(x)$ has no rational solutions. ∎

In the following remark we discuss exceptional cases of Theorem 4.5 (the conditionally exceptional cases).

Remark 4.6. (i) Assume that the polynomial f is irreducible and that $(m, n) \in \{(2, 6), (4, 4), (6, 3)\}$. Then by the argument from the proof of Proposition 3.4, (iii), it can be proved unconditionally that there is a set of prime numbers q of density at least $\frac{1}{n}$, such that the equation $qy^m = f(x)$ has no rational solutions.

(ii) Assume that the *abc*-conjecture is true. Let f be a polynomial over $\mathbb{Q}$ of degree $n = 6$. Assume that f is a product of a quadratic and a quartic irreducible polynomial over $\mathbb{Q}$. Using the argument from the proof of Theorem

4.5 (b), it can be proved that there is a set of prime numbers q of density at least $\frac{1}{2}$, such that the equation $qy^2 = f(x)$ has no rational solutions.

Acknowledgements.

The author thanks the referee for several very helpful comments and suggestions.

References

[1] E. Bombieri, W. M. Schmidt, *On Thue's equation*, Invent. Math. **88** (1987), 69–81.
[2] S. R. Finch, Mathematical constants, Cambridge University Press, Cambridge, 2003.
[3] A. Granville, *Rational and integral points on quadratic twists of a given hyperelliptic curve*, Int. Math. Res. Not. IMRN **2007** Art. ID 027, 24pp.
[4] I. Gusić, *A characterization of linear polynomials*, J. Number Theory **115** (2005), 343–347.
[5] I. Gusić, *A remark on Diophantine equation* $f(x) = g(y)$, Glas. Mat. Ser. III **46(66)** (2011), 333–338.
[6] G. H. Hardy, E. M. Wright, An introduction to the theory of numbers, sixth edition, Oxford University Press, Oxford, 2008.
[7] M. Hindry, J. H. Silverman, Diophantine geometry, an introduction, GTM **201**, Springer, 2000.
[8] M. N. Huxley, *Exponential sums and lattice points III.*, Proc. London Math. Soc. **87** (2003), 591–609.
[9] J. C. Koo, *On holomorphic differentials of some algebraic function field of one variable over* **C**, Bull. Austral. Math. Soc. **43** (1991), 399–405.
[10] B. Mazur, K. Rubin, *Ranks of twists of elliptic curves and Hilberts tenth problem*, Invent. Math. **181** (2010), 541–575.
[11] J. Nakagawa, K. Horie, *Elliptic curves with no rational points*, Proc. Amer. Math. Soc. **104** (1988), 20–24.
[12] K. Ono, C. Skinner, *Non-vanishing of quadratic twists of modular L-functions*, Invent. Math. **134** (1998), 651–660.
[13] A. Pethő, V. Ziegler, *Arithmetic progressions on Pell equations*, J. Number Theory **128** (2008), 1389–1409.
[14] A. Schinzel, Polynomials with special regard to reducibility, Cambridge University Press, Cambridge, 2000.
[15] J. P. Serre, *On a theorem of Jordan*, Bull. Amer. Math. Soc. **40** (2003), 429–440.
[16] J. H. Silverman, The arithmetic of elliptic curves, GTM **106**, Springer, Berlin, 1986.
[17] H. M. Stark, *On the asymptotic density of the k-free integers*, Proc. Amer. Math. Soc. **17** (1966), 1211–1214.
[18] C. L. Stewart, *On the number of solutions of polynomial congruences and Thue equation*, J. Amer. Math. Soc. **4** (1991), 793–835.
[19] M. Stoll, *On the arithmetic of the curves* $y^2 = x^l + A$ *and their Jacobians*, J. Reine Angew. Math. **501** (1998), 171–189.

I. Gusić
Faculty of Chemical Engin. and Techn.
University of Zagreb
Marulićev trg 19, 10000 Zagreb
Croatia
E-mail: igusic@fkit.hr

Received: 21.6.2010.
Revised: 2.10.2010. & 2.1.2011. & 30.4.2011.