COMPOSITIO MATHEMATICA

JERZY URBANOWICZ

On diophantine equations involving sums of powers with quadratic characters as coefficients, I

Compositio Mathematica, tome 92, n° 3 (1994), p. 249-271

<http://www.numdam.org/item?id=CM_1994__92_3_249_0>

Compositio Mathematica **92**: 249–271, 1994.

On diophantine equations involving sums of powers with quadratic characters as coefficients, I

JERZY URBANOWICZ*

Institute of Mathematics, Polish Academy of Sciences, ul. Śniadeckich 8, 00-950 Warszawa, Poland

Received 5 February 1993; accepted in revised form 2 June 1993

Introduction

Let d be the discriminant of a quadratic field with the character $\left(\frac{d}{\cdot}\right)$. Put $\delta = |d|$. Set $\eta(5) = \frac{1}{5}$, $\eta(8) = \frac{1}{2}$, and $\eta(d) = 1$, otherwise. If $d > 0$ put $B_{2,\left(\frac{d}{\cdot}\right)} = \eta(d)k_2(d)$. It is known that $k_2(d)$ is equal to the order of the K_2-group of the ring of integers of a quadratic field with the discriminant d (see p. 499 in [10] and Theorems 4.2, 4.3, pp. 31 and 33 in [9]). Write $\xi(-3) = \frac{1}{3}$, $\xi(-4) = \frac{1}{2}$, and $\xi(d) = 1$, otherwise. If $d < 0$, set $-B_{1,\left(\frac{d}{\cdot}\right)} = \xi(d)h(d)$. As usual, $h(d)$ denotes the class number. According to the above remarks the numbers $k_2(d)$ and $h(d)$ are natural. Moreover it is known (see, e.g. [5]) that the first of them is divisible by 4. In this paper $B_{k,\chi}$, resp. $B_{k,\chi}(x)$ denotes as usual the kth Bernoulli number, resp. polynomial belonging to the Dirichlet character χ (see [9]).

In this paper we are going to deal with the equation

$$\sum_{a=1}^{x\delta} \left(\frac{d}{a}\right) a^k = by^z, \tag{1.1}$$

in integers $x \geqslant 1$, $y, z > 1$, where $b \neq 0$ and $k \geqslant 1$ are fixed integers.

K. Dilcher [2] proved that:

'*the equation* (1.1) *has only finitely many integral solutions* $x \geqslant 1$, $y, z > 1$ (*with effective upper bounds for them*)', (D)

if one of the following conditions holds:

(i) k is sufficiently large (without determination of a lower bound),

(ii) $d = -p$, and $p \equiv 3 \pmod 8$ is a prime number, for $k \geqslant 3$, $k \not\equiv 0 \pmod 4$,

*This research was done at Leiden University and supported by the Netherlands Organization for Scientific Research (N.W.O.) grant 611-307-019/018.

(iii) there exists an odd prime number q such that $\left(\frac{d}{q}\right) = -1$, $q \geqslant \frac{2}{5}\sqrt{\delta}\log\delta$ and $k = q$ or $q+1$, for $k \neq 4$,

(iv) $d = -4$, for $k \geqslant 3$, $k \neq 4, 5$.

We are going to extend this list by proving the following:

THEOREM 1. *Let $d < -4$ be the discriminant of an imaginary quadratic field, and let k be an integer with $k \geqslant 3$, $k \neq 4$. Then* (D) *is true if* $\left(\frac{d}{2}\right) \neq 1$ *and* $8 \nmid h(d)$.

REMARK. The conditions of Theorem 1 are satisfied in the following cases. (i), (iii) and (vii) follow from Dirichlet's class number formulas for imaginary quadratic fields. References in the other cases may be found in [5] (in cases (x) and (xiv) see also Corrigendum to [5]). Here p and q are odd primes and $\left(\frac{p}{q}\right)$ denotes the Legendre symbol.

(i) $\delta = p \equiv 3 \pmod 8$,

(ii) (H. Hasse) $\delta = pq \equiv 3 \pmod 8$ and $\left(\frac{p}{q}\right) = -1$,

(iii) $\delta = 4p$, $p \equiv -3 \pmod 8$,

(iv) (P. Barrucand and H. Cohn) $\delta = 4p$, $p \equiv 1 \pmod 8$, $p = u^2 - 2w^2$, $u > 0$, $u \equiv 3 \pmod 4$, $w \equiv 0 \pmod 4$,

(v)–(vi) (E. Brown and A. Pizer) $\delta = 4pq$, $p \equiv q \equiv 3 \pmod 8$, or $\delta = 4pq$, $p \equiv q + 4 \equiv 1 \pmod 8$ and $\left(\frac{p}{q}\right) = -1$,

(vii) $\delta = 8$,

(viii)–(ix) (H. Hasse) $\delta = 8p$, $p \equiv 1 \pmod 8$, $-2p = u^2 - 2w^2$, $w > 0$, $w \not\equiv 1, 3 \pmod 8$, or $\delta = 8p$, $p \equiv -1 \pmod 8$, $-2p = u^2 - 2w^2$, $w > 0$, $w \not\equiv \pm 1 \pmod 8$,

(x)–(xiv) (A. Pizer) $\delta = 8pq$, $p \equiv q \equiv 5 \pmod 8$, or $\delta = 8pq$, $p \equiv -q \equiv 3 \pmod 8$, or $\delta = 8pq$, $p \equiv 1 \pmod 8$, $q \equiv \pm 3 \pmod 8$ and $\left(\frac{p}{q}\right) = -1$, or $\delta = 8pq$, $p \equiv q - 2 \equiv -3 \pmod 8$ and $\left(\frac{p}{q}\right) = -1$, or $\delta = 8pq$, $p \equiv q + 4 \equiv 3 \pmod 8$ and $\left(\frac{p}{q}\right) = -1$.

Hence the theorem holds true in all these cases. Case (i) is Dilcher's case (ii).

The case $\left(\frac{d}{2}\right) = 1$ is more complicated. In this case by generalized Kummer congruences (see, e.g., (1.2) of [7], or the exercise 7.5, p. 141 in [9]), the generalized Bernoulli numbers $B_{k,\left(\frac{d}{\cdot}\right)}$ can be divisible by any powers of 2. Our methods, i.e., congruences modulo powers of 2 used together with results of [7], give in this case only results with restrictions on k.

THEOREM 2. *Let d be the discriminant of an imaginary quadratic field, and let k be an integer with $k \geqslant 3$, $k \neq 4$. Then* (D) *is true in the following cases*:

(i) *if* $\left(\frac{d}{2}\right) = 1$, $8 \nmid h(d)$, $64 \nmid k_2(-4d)$ *with* $k \not\equiv 2 \pmod{16}$,

(ii) *if* $\left(\frac{d}{2}\right) = -1$, $8 \parallel h(d)$ *with the additional condition* $8 \mid h(8d)$,

(iii) *if* $4 \parallel d$, $8 \parallel h(d)$ *with the additional condition* $8 \mid h(2d)$.

By using the methods of this paper one can generalize Theorems 1 and 2. However, the assumptions on d and restrictions on k will be more complicated, especially in the case $8 \mid d$.

With Theorem 2 one can extend the above list. We shall do it only for $\left(\frac{d}{2}\right) = 1$.

REMARK (cf. [5]). The conditions of Theorem 2 in case $\left(\frac{d}{2}\right) = 1$ are satisfied in the following cases. Here p and q are odd primes.

(xv) $\delta = p \equiv 7 \pmod{16}$,

(xvi) $\delta = pq$, $p \equiv -q \equiv 3 \pmod{8}$.

Hence the theorem holds true in all these cases with $k \not\equiv 2 \pmod{16}$.

In order to prove the theorems we use results of [6], [7] and methods of [8] using congruences modulo higher powers of 2, or Eisenstein polynomials with respect to $p = 2$.

2. Generalized Bernoulli numbers and polynomials

For any Dirichlet character χ, set $S_{k,\chi}(x) = \sum_{a=1}^{x-1} \chi(a)a^k$. Write $\chi(-1) = (-1)^\rho$, where $\rho \in \{0, 1\}$. It is well known (see, e.g., [9]) that:

$$B_{k,\chi} = B_{k,\chi}(0), \tag{2.1}$$

$$B_{0,\chi} = 0, \text{ if } \chi \neq 1, \text{ and } B_{0,1} = 1, \tag{2.2}$$

$$\text{if } \chi \neq 1 \text{ then we have: } B_{k,\chi} = 0 \Leftrightarrow k \not\equiv \rho \pmod 2, \tag{2.3}$$

$$B_{k,\chi}(x) = \sum_{i=0}^{k} \binom{k}{i} B_{i,\chi} x^{k-i}, \tag{2.4}$$

$$S_{k,\chi}(fx) = \frac{1}{k+1}\,[B_{k+1,\chi}(fx) - B_{k+1,\chi}], \text{ where } f \text{ denotes the conductor of } \chi. \tag{2.5}$$

3. Auxiliary formulas

Let d be the discriminant of a quadratic field, and let $\left(\frac{d}{\cdot}\right)$ denote the Kronecker symbol. Denote by ρ the number 0, resp. 1, if d is positive, resp. negative. Then $\left(\frac{d}{-1}\right) = (-1)^{\rho}$. For any $s \geqslant 1$, put

$$b_s(d) = \frac{B_{s,\left(\frac{d}{\cdot}\right)}}{s}.$$

For any k, set

$$P_{k+1}(x) = \frac{1}{k+1} \sum_{\substack{1 \leqslant i \leqslant k, \\ i \equiv \rho \pmod 2}} \binom{k+1}{i} B_{i,\left(\frac{d}{\cdot}\right)} (x\delta)^{k+1-i}. \tag{3.1}$$

By (2.1)–(2.5) we can rewrite equation (1.1) in the form

$$P_{k+1}(x) = by^z.$$

Moreover (3.1) implies the formulas:

$$P_{k+1}(x) = \begin{cases} \dfrac{x\delta}{k+1} \displaystyle\sum_{\substack{2-\rho \leqslant i \leqslant k, \\ i \equiv \rho \pmod 2}} \binom{k+1}{i} B_{i,\left(\frac{d}{\cdot}\right)} (x\delta)^{k-i}, & \text{if } k \equiv \rho \pmod 2, \\ \dfrac{(x\delta)^2}{k+1} \displaystyle\sum_{\substack{2-\rho \leqslant i \leqslant k-1, \\ i \equiv \rho \pmod 2}} \binom{k+1}{i} B_{i,\left(\frac{d}{\cdot}\right)} (x\delta)^{k-i-1}, & \text{otherwise.} \end{cases}$$

Hence we get

$$P_{k+1}(x)=\begin{cases} x\delta \sum_{i=1}^{(k+\rho)/2} \binom{k}{2i-\rho-1} b_{2i-\rho}(d)(x\delta)^{k-2i+\rho}, & \text{if } k\equiv\rho \pmod 2, \\ (x\delta)^2 \sum_{i=1}^{(k+\rho-1)/2} \binom{k}{2i-\rho-1} b_{2i-\rho}(d)(x\delta)^{k-2i+\rho-1}, & \text{otherwise.} \end{cases} \tag{3.2}$$

4. LEMMAS

The proofs of Theorems 1 and 2 fall naturally into a sequence of lemmas. In the five lemmas below, let d be the discriminant of an imaginary quadratic field and let k be an odd natural number.

LEMMA 1 (see Cor. 4 to Theorem 1 [7]). *If* $\left(\frac{d}{2}\right) = -1$ *and* $k \geqslant 3$ *then we have*:

(i) $\operatorname{ord}_2 b_k(d) \geqslant 1$,
(ii) $\operatorname{ord}_2 b_k(d) = 1 \Leftrightarrow 2 \nmid h(d) \Leftrightarrow \delta = p \equiv 3 \pmod 8$, *where* p *is a prime number*,
(iii) $\operatorname{ord}_2 b_k(d) = v$, $v = 2$ *or* $3 \Leftrightarrow 2^{v-1} \parallel h(d)$,
(iv) $\operatorname{ord}_2 b_k(d) = 4 \Leftrightarrow \{8 \parallel h(d)$ *and* $[k \equiv 1 \pmod 4$ *of* $(k \equiv 3 \pmod 4$ *and* $8 \mid h(8d))]\}$ *or* $(16 \mid h(d)$ *and* $k \equiv 3 \pmod 4$ *and* $4 \parallel h(8d))$,
(v) $\operatorname{ord}_2 b_k(d) \geqslant 5$, *otherwise.* □

LEMMA 2 (see Cor. 2 to Thm. 2 [6] and Cor. 1, 2 to Thm. 1 [7]). *If* $\left(\frac{d}{2}\right) = 1$ (*so* $16 \mid k_2(-4d)$ *then*) *and* $k \geqslant 3$, *then we have*:

(i) $b_k(d) \equiv -\frac{k-1}{2} k_2(-4d) \pmod{64}$,
(ii) $\operatorname{ord}_2 b_k(d) \geqslant 4$,
(iii) $\operatorname{ord}_2 b_k(d) = 4 \Leftrightarrow 16 \parallel k_2(-4d)$ *and* $k \equiv 3 \pmod 4$,
(iv)) $\operatorname{ord}_2 b_k(d) \geqslant 5$, *otherwise.* □

LEMMA 3 (see Cor. 1 to Thms. 2, 4 [7]). *If* $4 \parallel d$ *then we have*:

(i) $\operatorname{ord}_2 b_k(d) = -1$, *if* $d = -4$, *and* $\operatorname{ord}_2 b_k(d) \geqslant 1$, *if* $d < -4$,
(ii) $\operatorname{ord}_2 b_k(d) - v$, $v = 1, 2, 3 \Leftrightarrow 2^v \parallel h(d)$,
(iii) $\operatorname{ord}_2 b_k(d) \geqslant 4$, *otherwise.* □

LEMMA 4 (see Cor. 2 to Thms. 3, 4 [7]). *If* $8 \mid d$ *and* $k \geqslant 3$ *then we have*:

(i) $\operatorname{ord}_2 b_k(d) \geqslant 0$,

(ii) $\operatorname{ord}_2 b_k(d) = v$, $0 \leqslant v \leqslant 3 \Leftrightarrow 2^v \| h(d)$
(*i.e.*, $\operatorname{ord}_2 b_k(d) = 0 \Leftrightarrow d = -8$),
(iii) $\operatorname{ord}_2 b_k(d) \geqslant 4$, *otherwise.* □

LEMMA 5. *If* $4 \mid d$, $d \neq -4$ *and* $8 \nmid h(d)$ *then for* $k \geqslant 3$ *the congruence*

$$b_k(d) \equiv -h(d) \pmod{2^{\operatorname{ord}_2 h(d)+2}}$$

holds. Moreover if $4 \| d$ *and* $8 \| h(d)$ *then it holds for* $k \geqslant 3$ *provided* $8 \mid h(2d)$.

Proof. First, let $4 \| d$. By the congruence of Theorem 4 [7] the lemma for $8 \nmid h(d)$ follows immediately. Therefore let us assume that $8 \| h(d)$. Write $d = -4d^*$, where d^* is the discriminant of a real quadratic field. Then Theorem 2 [7] states that the numbers $b_k(d)$ are 2-integral. Moreover the following congruence holds:

$$b_k(d) \equiv \alpha_1 k_2(d^*)\eta(d^*) + \alpha_2 h(d) + \alpha_3 h(2d) \pmod{64},$$

where α_i are integers of the form $\alpha_i = p_i k + q_i$, and the numbers p_i and q_i are given by formulas with $\left(\frac{-1}{k}\right)$, $\left(\frac{2}{k}\right)$, $\left(\frac{d^*}{2}\right)$. On the other hand, by Corollary 2 to Theorem 1 [6] the divisibility $8 \| h()d)$ implies $16 \mid k_2(d^*)$ and $4 \mid h(2d)$. Furthermore by the above mentioned formulas for α_i we get $\alpha_1 \equiv 0$, resp. 1 (mod 2), $\alpha_2 \equiv -1$, resp. 1 (mod 4), if $k \equiv 1$, resp. 3 (mod 4), and $\alpha_3 \equiv 0 \pmod 8$. Therefore, if $k \equiv 1 \pmod 4$ then the lemma follows immediately. In the case $k \equiv 3 \pmod 4$ we find that $b_k(d) \equiv k_2(d^*)\eta(d^*) + h(d) \pmod{32}$. Consequently, assuming $b_k(d) \equiv h(d) \pmod{32}$ gives $32 \mid k_2(d^*)$. And so by Corollary 2(iii) to Theorem 1 [6], this together with $8 \| h(d)$ imply $4 \| h(2d)$. Contradiction with the hypothesis $8 \mid h(2d)$.

Next, let $8 \mid d$. Then by Theorem 4 [7], Lemma 5 for $4 \nmid h(d)$ follows immediately. Thus let us assume that $4 \| h(d)$. Write $d = \pm 8d^*$, where d^* is the discriminant of a quadratic field. In the case $d^* < 0$, Theorem 3 [7] states that

$$b_k(d) \equiv \beta_1 k_2(-4d^*) + \beta_2 h(d) + \beta_3 h(d^*)\xi(d^*) \pmod{64},$$

where the integral numbers β_i, $i = 1, 2, 3$ are given in [7]. In this case by Corollary 2 to Theorem 2 [6], the divisibility $4 \| h(d)$ implies $16 \| k_2(-4d^*)$, if $\left(\frac{d^*}{2}\right) = 1$, and $2 \mid h(d^*)$, $8 \mid k_2(-4d^*)$, if $\left(\frac{d^*}{2}\right) = -1$. Hence in the first case we get the lemma immediately, because $\beta_2 \equiv -1 \pmod 4$ and $\beta_3 \equiv 0 \pmod{16}$. If $\left(\frac{d^*}{2}\right) = -1$, then $\beta_1 \equiv 0$, resp. 1 (mod 2), and $\beta_3 \equiv 0$, resp. 4 (mod 8), if

$k \equiv 1$, resp. 3 (mod 4). Furthermore $\beta_2 \equiv -1 \pmod 4$. These give the lemma in case $k \equiv 1 \pmod 4$. In case $k \equiv 3 \pmod 4$ we obtain the congruence

$$b_k(d) \equiv k_2(-4d^*) - h(d) + h(d^*)\xi(d^*) \pmod{16}.$$

Hence assuming $b_k(d) \equiv h(d) \pmod{16}$ gives the congruence

$$2h(d) \equiv k_2(-4d^*) + 4h(d^*)\xi(d^*) \pmod{16}.$$

Thus, if $8 \| k_2(-4d^*)$ then by Corollary 2(iii) to Theorem 2 [6] we get $2 \| h(d^*)$ and $8 \mid h(d)$. Contradiction. Likewise, if $16 \mid k_2(-4d^*)$ then $4 \mid h(d^*)$ and we get $8 \mid h(d)$ again.

Now let $d^* > 0$. In this case, $4 \| h(d)$ implies $8 \mid k_2(d^*)$, $4 \mid h(-4d^*)$. On the other hand Theorem 3 [7] states that

$$b_k(d) \equiv \gamma_1 k_2(d^*)\eta(d^*) + \gamma_2 h(d) + \gamma_3 h(-4d^*) \pmod{64},$$

where $\gamma_1 \equiv 0$, resp. 1 (mod 2), $\gamma_3 \equiv 0$, resp. 2 (mod 4), if $k \equiv 1$, resp. 3 (mod 4), and $\gamma_2 \equiv -1 \pmod 4$. Consequently if $k \equiv 1 \pmod 4$, then the lemma follows at once. If $k \equiv 3 \pmod 4$ then we get the congruence

$$b_k(d) \equiv k_2(d^*)\eta(d^*) - h(d) + 2h(-4d^*) \pmod{16}.$$

Thus, if $b_k(d) \equiv h(d) \pmod{16}$ then we get the congruence

$$2h(d) \equiv k_2(d^*)\eta(d^*) + 2h(-4d^*) \pmod{16}.$$

An analysis similar to that in the previous case gives the lemma. Indeed, if $8 \| k_2(d^*)$ then by Corollary 2(ii) to Theorem 1 [6] we get $4 \| h(-4d^*)$, whence $8 \mid h(d)$. Similarly, if $16 \mid k_2(d^*)$, then by the same corollary we obtain $8 \mid h(-4d^*)$. Hence we get $8 \mid h(d)$, again. This contradiction proves the lemma completely. □

LEMMA 6 (see [1], [3], [4],and [8]). *Let $0 \neq b \in \mathbb{Z}$ and let $P(x) \in \mathbb{Q}[x]$ be a polynomial with at least three zeros of odd multiplicity and for any odd prime p, with at least two zeros of multiplicities relatively prime to p. Then the equation*

$$P(x) = by^z$$

has only finitely many integral solutions $x \geqslant 1$, $y, z > 1$ and these solutions can be effectively determined. □

To simplify writing, we let A_2 stand for the ring of polynomials over $\mathbb{Q}$ with 2-integral coefficients. Further, in several places of the proof of Lemma 9, we are going to use some facts which are easy to check. It is convenient to enunciate them in the following two lemmas:

LEMMA 7. *Let* $\tau_1, \tau_2 \in A_2$ *and* p *be a prime number. Then the implication*

$$\tau_1^p(x) \equiv \tau_2^p(x) \pmod 2 \Rightarrow \tau_1(x) \equiv \tau_2(x) \pmod 2$$

holds.

Proof. Without loss of generality we may assume that τ_1 and τ_2 are monic. We have

$$(\tau_1(x) - \tau_2(x))(\tau_1^{p-1}(x) + \tau_1^{p-2}(x)\tau_2(x) + \cdots + \tau_2^{p-1}(x)) \equiv 0 \pmod 2.$$

Hence in the case $p \geqslant 3$ we get $\tau_1(x) \equiv \tau_2(x) \pmod 2$ at once, because the leading coefficient of the second factor of the left-hand side of the above congruence is equal to $p \not\equiv 0 \pmod 2$. If $p = 2$ then

$$\tau_1^2(x) - \tau_2^2(x) \equiv (\tau_1(x) - \tau_2(x))^2 \pmod 2$$

and the implication is obvious. □

LEMMA 8. *Denote by* $A(m, p)$ *the sum of the digits of* m *written in the base* p. *Let* $k = k_0 + 2k_1 + \cdots + 2^r k_r$ *and* $j = j_0 + 2j_1 + \cdots + 2^r j_r$, where $k_v, j_v \in \{0, 1\}$ *for* $v = 0, 1, \ldots, r$. *Then we have*:

(i) $$\operatorname{ord}_2 \binom{k}{j} = A(j, 2) + A(k - j, 2) - A(k, 2),$$

(ii) $$2 \nmid \binom{k}{j} \Leftrightarrow k_v \geqslant j_v$$

for all $v = 0, 1, \ldots, r$,

(iii) $$\binom{k}{j} \equiv \binom{k}{k - j - 1} \pmod 2,$$

if k *is odd and* j *is even.*

Proof. (i) This follows at once by using the well-known fact that for $m \geqslant 1$ and prime p we have

$$\operatorname{ord}_p(m!) = \frac{m - A(m, p)}{p - 1}.$$

(ii) This follows easily from (i).

(iii) A trivial verification shows that $(j+1)\binom{k}{j} = (k-j)\binom{k}{k-j-1}$.

Hence (iii) of the lemma follows immediately. □

LEMMA 9. *Let k be a natural number, $k \geqslant 3$, $k \neq 4$. Write $k \equiv \kappa \pmod 2$, $\kappa \in \{0, 1\}$. If*

$$f_k(x) = \sum_{i=0}^{(k-2+\kappa)/2} \binom{k}{2i} a_{2i} x^{k-2i-2+\kappa}$$

is a polynomial over $\mathbb{Q}$ with 2-integral coefficients a_{2i} satisfying one of the following conditions:

(i) $2 \nmid a_0$ *and* $a_{2i} \equiv 2 \pmod 4$, *if* $i \geqslant 1$,
(ii) $2 \nmid a_{2i}$ *if* $i \geqslant 0$, *and* $a_{2i} \equiv -a_0 \pmod 4$, *if* $i \geqslant 1$,
(iii) $2 \nmid a_0$ *and* $2^{\operatorname{ord}_2 i+1} \parallel a_{2i}$, *if* $i \geqslant 1$ *and* $k \not\equiv 2 \pmod 8$,
(iv) $2 \nmid a_0$ *and* $2^{\operatorname{ord}_2 i+r} \parallel a_{2i}$, *if* $i \geqslant 1$, $2 \leqslant r \leqslant 5$ *and* $k \not\equiv 2 \pmod{16}$,

then the polynomial $x^{2-\kappa} f_k(x)$ satisfies the hypothesis of Lemma 6.

REMARK. Actually in the cases (i) with $k \not\equiv 0 \pmod 4$, or (ii) for odd k, the polynomial $f_k(x)$ is an Eisenstein polynomial (with respect to $p = 2$).

Proof. (i) First, let us assume that $k \not\equiv 0 \pmod 4$. Then by definition, the leading coefficient of the polynomial $f_k(x)$ is odd, all its other coefficients are even and its constant term is not divisible by 4. Thus this polynomial is of Eisenstein type with respect to $p = 2$, and so irreducible over $\mathbb{Q}$. Hence it satisfies the hypothesis of Lemma 6. The proof for $k \equiv 0 \pmod 4$ not being a power of 2 will work for any k such that k and $k - 1$ are not powers of 2 (with the assumption $f_k(0) \neq 0$ for odd k). In order not to have to check later one case, viz. if $k - 1$ is a power of 2, we assume that $k \not\equiv 1 \pmod 4$. Since the degrees of $f_k(x)$ and of squares of polynomials are even, to prove the lemma it suffices to exclude the cases

$$f_k(x) = qt^p(x) \tag{4.1}$$

for any prime $p \geqslant 2$, $t \in A_2$ and 2-integral $q \in \mathbb{Q}$, and for even k the case

$$f_k(x) = w(x)u^2(x), \tag{4.2}$$

where $w, u \in A_2$ and $\deg w = 2$.

Let us first observe that by $2 \nmid a_0$, $2 \mid a_{2i}$, $i \geqslant 1$ we get the congruence

$$f_k(x) \equiv x^{k-2+\kappa} \pmod 2. \tag{4.3}$$

From (4.1), it follows that $p \mid (k-2+\kappa)$. Moreover, (4.1) and (4.3) together with Lemma 7, give

$$t(x) = x^{(k-2+\kappa)/p} + 2t_1(x). \tag{4.4}$$

where $t_1 \in A_2$. Hence we get the congruence

$$f_k(x) \equiv qx^{k-2+\kappa} + 2pqt_1(x)x^{(k-2+\kappa)/p} \pmod 4 \tag{4.5}$$

with odd q.

On the other hand, if k and $k-1$ are not powers of 2, then by Lemma 8(ii) there exist at least two i, $1 \leqslant i \leqslant \dfrac{k-2+\kappa}{2}$ such that $2 \nmid \binom{k}{2i}$. Furthermore by $\binom{k}{2i} = \binom{k}{k-2i}$ (used for even k), and by $\binom{k}{2i} \equiv \binom{k}{k-2i-1} \pmod 2$ for odd k (see Lemma 8(iii)), it follows that there exist at least two such i, unless $i = \dfrac{k}{4}$, if $k \equiv 0 \pmod 4$, or $i = \dfrac{k-1}{4}$, if $k \equiv 1 \pmod 4$. Set $k = k_0 + 2k_1 + \cdots + 2^r k_r$, where $k_v \in \{0, 1\}$ for $v = 0, 1, \ldots, r$. Then by Lemma 8(i), we have

$$\operatorname{ord}_2 \binom{k}{k/2} = k_0 + k_1 + \cdots + k_r - 1 \geqslant 1,$$

and also

$$\operatorname{ord}_2 \binom{k}{(k-1)/2} = k_0 + k_1 + \cdots + k_r \geqslant 1$$

in both the considered cases. Therefore both

$$\binom{k}{k/2} \quad \text{and} \quad \binom{k}{(k-1)/2}$$

are even. Here we have $k \not\equiv 1 \pmod 4$, so $k-1$ is not a power of 2. Thus the above holds true for $k \not\equiv 1 \pmod 4$ not being a power of 2.

If $p = 2$ then we get a contradiction with (4.5) immediately. So let $p \geqslant 3$. In this case in the left-hand side of the congruence (4.5) we have

$$\frac{k-2+\kappa}{p}(p-1) \geqslant \frac{2}{3}(k-2+\kappa).$$

This inequality contradicts the above again, because for at least one of the numbers $t = 2i$ or $t = k - 2i - \kappa$ we have $k - t - 2 + \kappa < \frac{2}{3}(k-2+\kappa)$. Indeed, if $k - 2i - 2 + \kappa \geqslant \frac{2}{3}(k-2+\kappa)$, i.e., $2i \leqslant \frac{1}{3}(k+\kappa-1)$ then we have

$$\begin{aligned} k-(k-2i-\kappa)-2+\kappa = 2i+2\kappa-2 &\leqslant \tfrac{1}{3}(k+\kappa-1)+2\kappa-2 \\ &= \tfrac{1}{3}k+\tfrac{7}{3}\kappa-\tfrac{7}{3} < \tfrac{2}{3}(k-2+\kappa), \end{aligned}$$

because $k > 5\kappa - 3$.

It remains to consider the case $k = 2^\lambda$, $\lambda \geqslant 3$. Then putting $\mu = \frac{1}{4}k$, by definition of $f_k(x)$ and Lemma 8(i), (ii) we find that

$$f_k(x) \equiv rx^{4\mu-2} + 8x^{3\mu-2} \pm 4x^{2\mu-2} + 8x^{\mu-2} \pmod{16}, \tag{4.6}$$

where r is odd.

This congruence together with (4.5), in the case $p \geqslant 3$ imply $t_1(x) \equiv 0 \pmod 2$. Consequently by (4.1) we get

$$f_k(x) \equiv qx^{4\mu-2} + 4pqt_2(x)x^{(k-2)/p(p-1)} \pmod{16},$$

where $t_2 \in A_2$. This contradicts (4.6) because of the term $8x^{\mu-2}$ and the inequality

$$\frac{k-2}{p}(p-1) \geqslant \frac{2}{3}(k-2) \geqslant \frac{4}{3}(2\mu-1) > \mu-2.$$

Now let us take $p = 2$. Then (4.1) together with (4.4), give the equality

$$f_k(x) = qx^{4\mu-2} + 4qt_1(x)x^{2\mu-1} + 4qt_1^2(x).$$

Let us assume $t_1(x) \equiv x^{l_1} + \cdots + x^{l_m} \pmod 2$, where $l_1 > \cdots > l_m \geqslant 0$ are integers. Then by $2\mu - 1 > 2\mu - 2$ we get $2\mu - 2 = 2l_{s_1}$, i.e., $l_{s_1} = \mu - 1$ for some $1 \leqslant s_1 \leqslant m$. On account of this the polynomial $4qt_1(x)x^{2\mu-1}$ contains the term $\pm 4x^{3\mu-2}$. Hence by (4.6) there must exist $1 \leqslant s_2 \leqslant m$ such that $3\mu - 2 = 2l_{s_2}$, i.e., $l_{s_2} = \frac{3}{2}\mu - 1$. In the same manner we can construct by induction a monotonically increasing sequence of natural numbers

$$l_{s_n} = \frac{2^n - 1}{2^{n-1}} \mu - 1,$$

where

$$n \leqslant \lambda - 1 \quad \text{and} \quad 3\mu - 2 \leqslant 2\mu - 1 + l_{s_n} < 4\mu - 2, \quad \text{if } n \geqslant 1.$$

This sequence is finite, i.e., there exists $n \leqslant \min(\lambda - 1, m)$ such that $2\mu - 1 + l_{s_n} \neq 2l_i$ for all $1 \leqslant i \leqslant m$. Thus the polynomial $f_k(x)$ must contain the term $\pm 4x^s$, where $3\mu - 2 \leqslant s < 4\mu - 2$. This contradicts (4.6).

To finish the proof of (i) of the lemma it remains to exclude (4.2) in the case of even k. Put in (4.2) $w(x) = ax^2 + bx + c$, where a, b, c are 2-integral rational numbers. Then by definition of $f_k(x)$, $b = 0$ and a must be odd. Moreover by (4.3) the polynomial $u(x)$ must be divisible modulo 2 by $x^{(k-4)/2}$, i.e.,

$$u(x) = x^{(k-4)/2} u_1(x) + 2u_2(x). \tag{4.7}$$

where $u_1, u_2 \in A_2$ and all coefficients of the polynomial u_1 are odd. Hence in view of (4.2) we find that

$$f_k(x) \equiv (ax^2 + c)x^{k-4} u_1^2(x) \pmod 4. \tag{4.8}$$

Consequently by (4.3) and $\deg(u_1^2(x) \bmod 4) = \deg(u_1^2(x) \bmod 2)$ we deduce that $\deg(u_1^2(x) \bmod 4) = 0$. Therefore $u_1^2(x) \equiv d \pmod 4$, where d is odd. According to the above the congruence (4.8) now becomes

$$f_k(x) \equiv adx^{k-2} + cdx^{k-4} \pmod 4.$$

This is impossible because by Lemma 8(ii) there must exist at least two terms of $f_k(x)$ with coefficients congruent to 2 modulo 4, unless k is a power of 2. Then, let $k = 2^\lambda$, $\lambda \geqslant 3$.

First of all let us note that without loss of generality we may assume that $u_1(x) = 1$ in (4.7). Indeed since a is odd and c is even, (4.2) together with (4.7) give $\deg u_1^2(x) = 0$, i.e., $u_1(x) = d$. By (4.2) and (4.3), d must be odd. Next by (4.2) and (4.6), c must be divisible by 4. Consequently (4.2) implies the congruence

$$f_k(x) \equiv ax^{4\mu-2} + cx^{4\mu-4} \pm 4x^{2\mu} u_2(x) \pm 4x^2 u_2^2(x) \pmod{16}.$$

Write $u_2(x) \equiv x^{l_1} + \cdots + x^{l_m} \pmod 2$, where $l_1 > \cdots > l_m$. Since $2\mu > 2\mu - 2$, by (4.6) there exists $1 \leqslant s_1 \leqslant m$ such that $2l_{s_1} = 2\mu - 4$, i.e., $l_{s_1} = \mu - 2$. Therefore the polynomial $4x^{2\mu} u_2(x)$ must contain the term $\pm 4x^{3\mu-2}$. In virtue

of that and (4.6) there must exist $1 \leqslant s_2 \leqslant m$ satisfying $3\mu - 4 = 2l_{s_2}$, i.e., $l_{s_2} = \frac{3}{2}\mu - 2$. In the same manner, by induction, we can construct a finite sequence of natural numbers $l_{s_n} = \dfrac{2^n - 1}{2^{n-1}}\,\mu - 2$, where $n \leqslant \lambda - 1$. This sequence is monotonically increasing. Furthermore, by arguments used earlier in the case of (4.1), there must exist $1 \leqslant s_n \leqslant m$ such that $2\mu + l_{s_n} \neq 2l_i$ for all $1 \leqslant i \leqslant m$, and $3\mu - 2 \leqslant 2\mu + l_{s_n} < 4\mu - 2$. Then the polynomial $f_k(x)$ contains the term $\pm 4x^{2\mu + l_{s_n}}$ which is incompatible with (4.6). This completes the proof of (i). □

(ii) (a) The case of even k.

Since $\binom{k}{i} = \binom{k}{k-i}$ and $2 \Big| \binom{k}{i}$ for $2 \nmid i$, we get

$$x^2 f_k(x) \equiv \sum_{\substack{0 \leqslant i \leqslant k-2 \\ 2|i}} \binom{k}{i} x^{k-i} \equiv \sum_{\substack{2 \leqslant i \leqslant k, \\ 2|i}} \binom{k}{i} x^i \equiv \sum_{i=1}^{k} \binom{k}{i} x^i$$

$$\equiv (x+1)^k - 1 \pmod 2.$$

Therefore

$$g_k(x) := (x+1)^2 f_k(x+1) \equiv x^k - 1 \pmod 2. \tag{4.9}$$

Similarly as in the proof of part (i) of the lemma, we are going to exclude the cases (4.1) and (4.2). Writing $k = 2^\lambda k'$, $2 \nmid k'$ we have

$$g_k(x) \equiv (x^{k'} - 1)^{2^\lambda} \pmod 2. \tag{4.10}$$

Thus in order to exclude (4.1) for $k \neq 2^\lambda$ and $p \geqslant 3$ it suffices to notice that the monic polynomial $x^{k'} - 1$ is relatively prime to its derivative modulo 2. Consequently it has only simple zeros. Before we exclude the cases (4.1) (for $p = 2$) and (4.2) for $k \neq 2^\lambda$, we prove the lemma in the case $k = 2^\lambda$, $\lambda \geqslant 3$ which is much easier. Then putting $\mu = \frac{1}{4}k$ by definition we obtain the congruence

$$f_k(x) \equiv rx^{4\mu-2} + 4x^{3\mu-2} \pm 2x^{2\mu-2} + 4x^{\mu-2} \pmod 8$$

(cf. the congruence (4.6)), where r is odd. We apply the same arguments as in the proof of part (i) of the lemma in the same case. First (4.1) together with Lemma 7 (with $\kappa = 0$), and next the congruence (4.5). This congruence gives a contradiction. If $p = 2$ then it is incompatible with the above

congruence because of the term $\pm 2x^{2\mu-2}$ and if $p \geqslant 3$ then because of the inequality

$$\frac{k-2}{p}(p-1) \geqslant \frac{4}{3}(2\mu-1) > 2\mu - 2.$$

In the same manner we exclude (4.2). First, we get the equality (4.7), and next the congruence (4.8). By the above congruence a is odd and $c \equiv 2 \pmod 4$ which contradicts this congruence at once because $k - 4 = 4\mu - 4 > 2\mu - 2$, if $k > 4$.

Now we return to the case $k \neq 2^\lambda$. Let us first note that to exclude (4.1) or (4.2) for the polynomial $f_k(x)$ it suffices to do it for the polynomial $g_k(x)$. Then, let $g_k(x) = qt^2(x)$, where $q \in \mathbb{Q}$ is 2-integral and $t \in A_2$. Since by (4.9) we have $g_k(0) \equiv 1 \pmod 2$, q must be odd. Write $k = 2^\lambda k'$, $2 \nmid k'$ again. Then (4.10) together with Lemma 7, imply

$$t(x) \equiv (x^{k'} - 1)^{2^{\lambda-1}} \equiv x^{k/2} - 1 \pmod 2.$$

Therefore we obtain

$$g_k(x) \equiv qx^k + 2x^{k/2} + q + 2(x^{k/2} + 1)t_1(x) \pmod 4,$$

where $t_1 \in A_2$.

Consequently setting $t_1(x) \equiv x^{l_1} + \cdots + x^{l_m} \pmod 2$, where $l_1 > \cdots > l_m \geqslant 0$ we conclude that

$$g_k(x) \equiv qx^k + 2x^{k/2} + q + 2(x^{l_1} + \cdots + x^{l_m}) + 2(x^{l_1+k/2} + \cdots + x^{l_m+k/2}) \pmod 4. \tag{4.11}$$

Denote by b_j for $0 \leqslant j \leqslant k$ the coefficient of x^j in the polynomial $g_k(x)$. By (4.9) we have

$$g_k(x) = \sum_{i=0}^{(k-2)/2} \binom{k}{2i} a_{2i}(x+1)^{k-2i}. \tag{4.12}$$

Hence we get

$$b_k = a_0, \tag{4.13}$$

and

$$b_0 = \sum_{i=0}^{(k-2)/2} \binom{k}{2i} a_{2i}.$$

Thus by definition we find that

$$b_0 \equiv a_0 \left[1 - \sum_{i=1}^{(k-2)/2} \binom{k}{2i}\right] \equiv a_0(1 - 2^{k-1} - 2) \pmod 4,$$

i.e.,

$$b_0 \equiv -a_0 \pmod 4, \tag{4.14}$$

because $k \geqslant 3$. Applying this to (4.11) gives $l_m = 0$ and the congruence

$$\begin{aligned} g_k(x) \equiv\ & a_0 x^k - a_0 + 2(x^{l_1} + \cdots + x^{l_{m-1}}) \\ & + 2(x^{l_1 + k/2} + \cdots + x^{l_{m-1} + k/2}) \pmod 4. \end{aligned} \tag{4.15}$$

Moreover from (4.12) it follows that for $0 < j < k$

$$b_j = \sum_{i=0}^{[(k-j)/2]} \binom{k}{2i}\binom{k-2i}{j} a_{2i} = \binom{k}{j} \sum_{i=0}^{[(k-j)/2]} \binom{k-j}{2i} a_{2i},$$

since by induction we have

$$\binom{k}{2i}\binom{k-2i}{j} = \binom{k}{k-2i}\binom{k-2i}{j} = \binom{k}{j}\binom{k-j}{k-2i-j}.$$

Therefore we conclude that

$$b_j \equiv a_0 \binom{k}{j}\left[1 - \sum_{i=1}^{[(k-j)/2]} \binom{k-j}{2i}\right] \equiv a_0 \binom{k}{j}(2 - 2^{k-j-1}) \pmod 4,$$

and hence

$$b_j \equiv 2\binom{k}{j} \pmod 4, \tag{4.16}$$

if $j \leqslant k - 3$, and $b_{k-2} \equiv 0 \pmod 4$, $b_{k-1} \equiv k \pmod 4$, because a_0 is odd and k is even.

Since k is not a power of 2, by Lemma 8(ii) there exists even $0 < j < k$ such that $2 \nmid \binom{k}{j}$. Thus $b_j \equiv 2 \pmod 4$, and hence by (4.15) $b_{j+k/2} \equiv 2 \pmod 4$, i.e., $2 \nmid \binom{k}{j+k/2}$. If $2^\lambda \| k$ and $2 \nmid \binom{k}{j}$, then by Lemma 8(ii) we have $2^\lambda \| j$. Moreover $2\lambda - 1 \| \frac{k}{2}$, and so $2^{\lambda-1} \| j + \frac{k}{2}$, too. Thus by Lemma 8(ii) we get $2 \| \binom{k}{j+k/2}$. Contradiction.

Finally let

$$g_k(x) = w(x)u^2(x), \tag{4.17}$$

where $w(x) = ax^2 + bx + c$, $w, u \in A_2$ and $a \neq 0$. Let us first notice that by (4.9) (i.e., by $g_k(0) \equiv 1 \pmod 2$), c must be odd. Next, by $2 \nmid b_k = a_0$ we have $2 \nmid a$. Moreover let us observe that b must be even. Otherwise the polynomial $x^k - 1$, and in consequence the polynomial $x^{k-1} + \cdots + x + 1$ would be divisible modulo 2 by the polynomial $x^2 + x + 1$. Then $3 \mid k$ and we get

$$\begin{aligned} u^2(x) &\equiv (x+1)(x^{k-3} + x^{k-6} + \cdots + x^3 + 1) \\ &\equiv x^{k-2} + x^{k-3} + x^{k-5} + x^{k-6} + \cdots + x + 1 \pmod 2. \end{aligned}$$

This congruence is impossible if $k - 2 \geqslant 1$, i.e., $k \geqslant 3$ because of the terms with the odd exponents. Further, if b is even, then by (4.9) we get the congruence

$$(x^{k/2} + 1)^2 \equiv [(x+1)u(x)]^2 \pmod 2.$$

Hence by Lemma 7 we obtain

$$x^{k/2} + 1 \equiv (x+1)u(x) \pmod 2.$$

Consequently we get

$$u(x) \equiv x^{k/2-1} + x^{k/2-2} + \cdots + x + 1 \pmod 2.$$

Therefore we find that

$$u^2(x) \equiv x^{k-2} + x^{k-4} + \cdots + x^2 + 1 + 2\sum_t p_t x^t \pmod 4,$$

where p_t is the number of solutions (i, j) of the equation $i + j = k - t$ with $1 \leqslant i < j \leqslant \frac{k}{2}$.

Moreover it is not difficult to see that $p_t = \left[\frac{k-t}{2}\right]$. Thus (4.17) together with (4.13) and (4.14), give the congruence

$$g_k(x) \equiv a_0 x^k - a_0 + h_k(x) + b(x^{k-1} + x^{k-3} + \cdots + x) \pmod 4, \qquad (4.18)$$

where

$$h_k(x) := 2\sum_{t=1}^{k-3}\left[\frac{k-t}{2}\right]x^{t+2} + 2\sum_{t=1}^{k-3}\left[\frac{k-t}{2}\right]x^t.$$

On the other hand, since

$$\left[\frac{k-t+2}{2}\right] + \left[\frac{k-t}{2}\right] = \begin{cases} k-t+1, & \text{if } t \text{ is even,} \\ k-t, & \text{if } t \text{ is odd,} \end{cases}$$

we observe that

$$\begin{aligned} h_k(x) &= 2\sum_{t=3}^{k-1}\left[\frac{k-t+2}{2}\right]x^t + 2\sum_{t=1}^{k-3}\left[\frac{k-t}{2}\right]x^t \\ &= 2\sum_{\substack{3 \leqslant t \leqslant k-3, \\ 2 \mid t}} (k-t+1)x^t + 2\sum_{\substack{3 \leqslant t \leqslant k-3, \\ 2 \nmid t}} (k-t)x^t \\ &\quad + (k-2)x + (k-2)x^2 + 4x^{k-2} + 2x^{k-1}. \end{aligned}$$

Consequently, we have the congruence

$$h_k(x) \equiv 2\sum_{t=3}^{k-3} x^t + (k-2)x + (k-2)x^2 + 2x^{k-1} \pmod 4. \qquad (4.19)$$

On the other hand (4.16) implies $b_2 \equiv k \pmod 4$. This contradicts (4.18) and (4.19) which give $b_2 \equiv k - 2 \pmod 4$.

The case of even k of (ii) is proved. □

(b) The case of odd k.

We shall prove that the polynomial $g_k(x)$ defined by

$$g_k(x) = f_k(x + 1)$$

is an Eisenstein polynomial (and so irreducible over $\mathbb{Q}$) with respect to $p = 2$.

By definition we have

$$g_k(x) = \sum_{i=0}^{(k-1)/2} \binom{k}{2i} a_{2i}(x+1)^{k-2i-1}. \tag{4.20}$$

Thus denoting by b_j (for $0 \leqslant j \leqslant k-1$) the coefficient of x^j in the polynomial $g_k(x)$ we get

$$b_{k-1} = a_0. \tag{4.21}$$

Moreover by definition we find that

$$b_0 = \sum_{i=0}^{(k-1)/2} \binom{k}{2i} a_{2i} \equiv a_0 \left[1 - \sum_{i=1}^{(k-1)/2} \binom{k}{2i}\right] \equiv a_0(2 - 2^{k-1}) \pmod 4,$$

and so for $k \geqslant 3$ we get

$$b_0 \equiv 2 \pmod 4.$$

By virtue of that and (4.21), the proof will be completed as soon as we can show that b_j for $1 \leqslant j \leqslant k-2$ are even. Indeed by (4.20) and the congruence $\binom{k}{2i} \equiv \binom{k}{k-2i-1} \pmod 2$ (see Lemma 8(iii)), it may be concluded that

$$\begin{aligned} b_j &= \sum_{i=0}^{[(k-j-1)/2]} \binom{k}{2i}\binom{k-2i-1}{j} a_{2i} \equiv \sum_{i=0}^{[(k-j-1)/2]} \binom{k}{k-2i-1}\binom{k-2i-1}{j} \\ &= \binom{k}{j} \sum_{i=0}^{[(k-j-1)/2]} \binom{k-j}{k-2i-1-j} \pmod 2. \end{aligned}$$

Therefore putting $j \equiv \theta \pmod 2$, $\theta \in \{0, 1\}$ we get

$$b_j \equiv \binom{k}{j} \sum_{i=0}^{(k-j-1-\theta)/2} \binom{k-j}{2i+\theta} \equiv \binom{k}{j} 2^{k-j-1} \equiv 0 \pmod 2,$$

if $j \leqslant k-2$, as required.

Part (ii) of the lemma is proved completely. □

(iii), (iv) Our task is to exclude the cases (4.1) and (4.2) again. We first turn to the case (4.1). Then we have the congruence (4.3), and by Lemma

7 we get the equality (4.4). Let us consider the power $t^p(x)$ of the right-hand side of (4.1). Denoting $m = \min_{0 \leqslant i \leqslant (k-2-\kappa)/2} \operatorname{ord}_2 \binom{k}{2i}$, by definition of $f_k(x)$ all coefficients of the polynomial $2qx^{(k-2+\kappa)/p(p-1)}t_1(x)$ must be divisible by 2^{r+m}. Therefore by $2 \nmid q$ all coefficients of the polynomial $t_1(x)$ must be divisible by 2^{r+m-1}. Hence for any $s \geqslant 2$, all coefficients of the polynomial $t_1^s(x)$ are divisible by $2^{s(r+m-1)}$. Now applying (4.4) to (4.1) gives, for $r \geqslant 1$, the congruence

$$f_k(x) \equiv qx^{k-2+\kappa} + 2pqx^{(k-2+\kappa)/p(p-1)}t_1(x) \pmod{2^{r+m+1}}, \tag{4.22}$$

which is even modulo 2^{r+m+2}, if $r \geqslant 2$. Indeed, all coefficients of the polynomial $2^s qx^{(k-2+\kappa)/p(p-s)}t_1^s(x)$ are divisible by 2^t, where $t = s + s(r+m-1) = s(r+m)$. Thus $t \geqslant r+m+1$, resp. $\geqslant r+m+2$, if $r \geqslant 1$, resp. $\geqslant 2$, because $(s-1)(r+m) \geqslant 1$, resp. $\geqslant 2$, if $r \geqslant 1$, resp. $\geqslant 2$. Moreover the polynomial $2qx^{(k-2+\kappa)/p(p-1)}t_1(x)$ modulo 2^{r+m+1} (resp. 2^{r+m+2}) must contain all terms of $f_k(x)$ with coefficients exactly divisible by 2^{r+m} (resp. by 2^{r+m+1}), if $r \geqslant 1$ (resp. $\geqslant 2$).

On the other hand, if $k \not\equiv 2, 3 \pmod 4$ then by $\binom{k}{i} = \binom{k}{k-i}$ (used for even k) and by $\binom{k}{i} \equiv \binom{k}{k-i-1} \pmod{2^{m+1}}$ for odd k (see Lemma 8(iii)), at least one of such terms is of degree less than $(k-2+\kappa)/2$. By the congruence (4.22) this contradicts the inequality $(k-2+\kappa)/p(p-1) \geqslant (k-2+\kappa)/2$. Let us consider the cases $k \equiv 2, 3 \pmod 4$ then. If $k \equiv 3 \pmod 4$ then for the constant term of $f_k(x)$ we have $2^{r+m} \parallel ka_{k-1}$. This gives a contradiction with the congruence (4.22) because of the inequality $\dfrac{k-1}{p}(p-1) \geqslant \dfrac{k-2}{2} \geqslant 1$. If $k \equiv -2 \pmod 8$ then we have $2^{r+m+1} \left\| \binom{k}{2} a_{k-2} \right.$ (for the constant term), and $2^{r+m} \left\| \binom{k}{4} a_{k-4} \right.$ (for the coefficient of x^2 of $f_k(x)$). This gives a contradiction with (4.22) (considered modulo 2^{r+m+2}, resp. 2^{r+m+1}) and the inequality

$$\frac{k-2}{p}(p-1) \geqslant \frac{k-2}{2} > 0, \text{ resp. } > 2.$$

If $k \equiv -6 \pmod{16}$, then we have $2^{r+m+1} \left\| \binom{k}{4} a_{k-4} \right.$. We obtain a contradiction with the congruence (4.22) modulo 2^{r+m+2}.

Our next concern will be the case (4.2). Again let us put in (4.2)

$w(x) = ax^2 + bx + c$ with 2-integral rational a, b, c and $a \neq 0$. We have $b = 0, 2 \nmid a$ and obtain an equality similar to (4.7) for the polynomial $u(x)$. Here $u(x) = x^{(k-4+\kappa)/2} + 2u_2(x)$, where $u_2 \in A_2$, because without loss of generality we may assume $u_1(x) = 1$, again. Furthermore, by the term $cx^{k-4+\kappa}$ we have $2^{r+m} | c$. Therefore (4.2) implies the congruence

$$f_k(x) \equiv ax^{k-2+\kappa} + cx^{k-4+\kappa} + 2u_2(x)x^{(k+\kappa)/2} + 4au_2^2(x)x^2 + 2\gamma c u_2(x)x^{(k-4+\kappa)/2} \pmod{2^{r+m+1+\gamma}}, \tag{4.23}$$

where $\gamma \in \{0, 1\}$.

From this it may be assumed that all coefficients of the polynomial $u_2(x)$ modulo $2^{r+m+1+\gamma}$ are exactly divisible by 2^{r+m-1}, if $\gamma = 0$, or by 2^{r+m-1} or 2^{r+m}, if $\gamma = 1$.

Let $k \not\equiv 2, 3 \pmod 4$. Then similarly as in the case of (4.1) the terms with coefficients divisible by the same power of 2 occur in pairs. Moreover only one of the terms of each such pair can be a term of the polynomial $2u_2(x)x^{(k+\kappa)/2}$. Thus the other must be contained in the polynomial $4au_2^2(x)x^2$. Therefore the polynomial $u_2^2(x)$ has a coefficient exactly divisible by 2^{r+m-3} consequently the polynomial $u_2(x)$ must have two coefficients exactly divisible by 2^s, and resp. by 2^t with $s + t = r + m - 3$, or one coefficient exactly divisible by 2^s, where $2s = r + m - 3$. We get a contradiction, because all the coefficients of $u_2(x)$ are exactly divisible by 2^{r+m-1}. The same reasoning as earlier applies also to the case $k \equiv 3 \pmod 4$ and $k \equiv -2 \pmod 8$. Then we use the congruence (4.23) with $\gamma = 1$. It remains to exclude (4.2) for $k \equiv -6 \pmod{16}$. Then by the congruence (4.23) with $\gamma = 1$, the constant term of $u_2^2(x)$ is exactly divisible by 2^{r+m-1}. Therefore the polynomial $u_2(x)$ has to have a coefficient exactly divisible by $2^{r+m-1/2}$. Contradiction. This completes the proof of Lemma 9. □

5. Proofs of the theorems

The proofs of the theorems will be divided into the cases: $2 \nmid d$, $4 \parallel d$, or $8 \mid d$. Each of these cases falls naturally into two subcases according to k is odd or even. We shall use Lemma 6 for the polynomial

$$f_k(x) := 2^{-\mathrm{ord}_2 h(d)} x^{\kappa-2} P_{k+1}(x\delta^{-1}) \in \mathbb{Q}[x],$$

where $k \equiv \kappa \pmod 2$, $\kappa \in \{0, 1\}$, and by (3.2) in the case of negative d we have

$$P_{k+1}(x) = \begin{cases} x\delta\Big[-h(d)\xi(d)(x\delta)^{k-1} + \binom{k}{2} b_3(d)(x\delta)^{k-3} + \cdots \\ \quad + \binom{k}{k-3} b_{k-2}(d)(x\delta)^2 + k b_k(d)\Big], & \text{if } k \text{ is odd,} \\ (x\delta)^2\Big[-h(d)\xi(d)(x\delta)^{k-2} + \binom{k}{2} b_3(d)(x\delta)^{k-4} + \cdots \\ \quad + \binom{k}{k-4} b_{k-3}(d)(x\delta)^2 + \binom{k}{k-2} b_{k-1}(d)\Big] & \text{if } k \text{ is even.} \end{cases}$$

(5.1)

By Lemmas 1–4 and the assumptions on d of both the theorems we have

$$\operatorname{ord}_2 b_k(d) \geqslant \operatorname{ord}_2 h(d).$$

Therefore putting in the above defined polynomial $f_k(x)$

$$a_{2i} = 2^{-\operatorname{ord}_2 h(d)} b_{2i+1}(d),$$

if $i \geqslant 0$, the a_{2i} are 2-integral rational numbers and by (5.1) this polynomial is of the same form as the polynomial defined in Lemma 6. We consider the three cases:

1. If $\left(\frac{d}{2}\right) = -1$ and $8 \nmid h(d)$, or $8 \parallel h(d)$ and $8 \mid h(8d)$, then by Lemma 1 we put $a_{2i} \equiv 2 \pmod 4$, if $i \geqslant 1$. Moreover by definition we have $2 \nmid a_0$. Therefore the above defined polynomial $f_k(x)$ satisfies the assumptions of (i) of Lemma 9, and by this lemma of Lemma 6. Consequently by Lemma 5 both the theorems follow in this case. □
2. If $4 \mid d$ then by Lemmas 3 (if $4 \parallel d$) or 4 (if $8 \mid d$) the a_{2i} are odd, if $i \geqslant 0$. Furthermore, if $8 \nmid h(d)$ or $8 \parallel h(d)$, $8 \mid h(2d)$ in the case of $4 \parallel d$, then Lemma 5 implies the congruence $a_{2i} \equiv -a_0 \pmod 4$, if $i \geqslant 1$. Thus the polynomial $f_k(x)$ satisfies the hypothesis (ii) of Lemma 9, and hence the hypothesis of Lemma 6. □
3. If $\left(\frac{d}{2}\right) = 1$, then by Lemma 2 we can control the divisibility of some of $b_k(d)$ by powers of 2 only in the case of $64 \nmid k_2(-4d)$. In this case $f_k(x)$ satisfies the hypothesis (iii) of Lemma 9 with

$$r := \operatorname{ord}_2 k_2(-4d) - \operatorname{ord}_2 h(d).$$

Let us note that small values of $\operatorname{ord}_2 h(d)$ and of $\operatorname{ord}_2 k_2(-4d)$ are in case $\left(\frac{d}{2}\right) = 1$ independent of each other and all supposed values of r in Lemma 9(iii), (iv) are possible. Again Theorem 2(i) follows from Lemma 9 and Lemma 6. □

6. The case $R \neq 0$

K. Dilcher [2] also proved that the equation

$$\left(\frac{d}{1}\right) 1^k + \left(\frac{d}{2}\right) 2^k + \cdots + \left(\frac{d}{x\delta}\right) (x\delta)^k + R(x) = by^z \tag{6.1}$$

has only finitely many integral solutions $x \geqslant 1$, $y, z > 1$ with $R = R_k \in \mathbb{Z}[x]$ satisfying the following condition:

$$\lim_{k \to \infty} \frac{(2\pi)^k \mid R_k(x)\mid}{\delta^k (k-1)!} = 0 \tag{6.2}$$

for any x, if k is sufficiently large. We considered the equation (6.1) only with $R = 0$, although our methods also give results for this equation with some polynomials $R \in 2^{\mu} x^{\vartheta} \mathbb{Z}[\delta x]$, where $\mu \leqslant 6$ depends only on moduli of congruences used in the proof of Lemma 9 and $\vartheta \leqslant 2$. Consequently the assumption (6.2) seems to be rather a consequence of methods used in [2].

Acknowledgement

The author wishes to thank Professor R. Tijdeman for his stimulating comments and useful suggestions and A. Chmura for correcting inaccuracies in an earlier draft of this paper.

References

[1] B. Brindza: On S-integral solutions of the equation $f(x) = y^m$. *Acta Math. Acad. Sci. Hungar.* 44 (1984) 133–139.
[2] K. Dilcher: On a diophantine equation involving quadratic characters. *Compositio Math.* 57 (1986) 383–403.
[3] W. J. Leveque: On the equation $y^m = f(x)$. *Acta Arith.* 9 (1964) 209–219.
[4] A. Schinzel and R. Tijdeman: On the equation $y^m = f(x)$. *Acta Arith.* 31 (1976) 199–204.

[5] J. Urbanowicz: On the 2-primary part of a conjecture of Birch-Tate. *Acta Arith.* 43 (1983) 69–81 and Corr., to appear.

[6] J. Urbanowicz: Connections between $B_{2,\chi}$ for even quadratic characters χ and class numbers of appropriate imaginary quadratic fields. I. *Compositio Math.* 75 (1990) 247–270.

[7] J. Urbanowicz: On some new congruences between generalized Bernoulli numbers. I. Publications Math. de la Fac. des Sci. de Besançon, Theorie des Nombres, Années 1990/1991.

[8] M. Voorhoeve, K. Győry and R. Tijdeman: On the diophantine equation $1^k + 2^k + \cdots + x^k + R(x) = y^z$. *Acta Math.* 143 (1979) 1–8 and Corr. 159 (1987) 151–152.

[9] L. Washington: *Introduction to Cyclotomic Fields.* Springer-Verlag, Berlin, Heidelberg, New York, 1982.

[10] A. Wiles: The Iwasawa conjecture for totally real fields. *Ann. of Math.* 131 (1990) 493–540.