Math. Comp. 78(2009), no. 267, 1853–1866.

COVERS OF THE INTEGERS WITH ODD MODULI AND THEIR APPLICATIONS TO THE FORMS $x^m - 2^n$ AND $x^2 - F_{3n}/2$

KE-JIAN WU[1] AND ZHI-WEI SUN[2,*]

[1]Department of Mathematics, Zhanjiang Normal University
Zhanjiang 524048, People's Republic of China
kjwu328@yahoo.com.cn

[2]Department of Mathematics, Nanjing University
Nanjing 210093, People's Republic of China
zwsun@nju.edu.cn
http://math.nju.edu.cn/∼zwsun

ABSTRACT. In this paper we construct a cover $\{a_s(\bmod\ n_s)\}_{s=1}^k$ of $\mathbb{Z}$ with odd moduli such that there are distinct primes $p_1, \ldots, p_k$ dividing $2^{n_1} - 1, \ldots, 2^{n_k} - 1$ respectively. Using this cover we show that for any positive integer m divisible by none of 3, 5, 7, 11, 13 there exists an infinite arithmetic progression of positive odd integers the mth powers of whose terms are never of the form $2^n \pm p^a$ with $a, n \in \{0, 1, 2, \ldots\}$ and p a prime. We also construct another cover of $\mathbb{Z}$ with odd moduli and use it to prove that $x^2 - F_{3n}/2$ has at least two distinct prime factors whenever $n \in \{0, 1, 2, \ldots\}$ and $x \equiv a \pmod M$, where $\{F_i\}_{i\geqslant 0}$ is the Fibonacci sequence, and a and M are suitable positive integers having 80 decimal digits.

1. INTRODUCTION

For $a \in \mathbb{Z}$ and $n \in \mathbb{Z}^+ = \{1, 2, 3, \ldots\}$ we let

$$a(n) = \{x \in \mathbb{Z} : x \equiv a \,(\bmod\, n)\}$$

which is a residue class modulo n. A finite system

$$A = \{a_s(n_s)\}_{s=1}^k \tag{1.1}$$

of residue classes is said to be a *cover* of $\mathbb{Z}$ if every integer belongs to some members of A. Obviously (1.1) covers all the integers if it covers $0, 1, \ldots, N_A - 1$ where

Keywords: Cover of the integers, arithmetic progression, Fibonacci sequence, prime divisor.

2000 *Mathematics Subject Classification.* Primary 11B25; Secondary 11A07, 11A41, 11B39, 11D61, 11Y99.

*This author is responsible for communications, and supported by the National Natural Science Foundation (grant 10871087) of China.

$N_A = [n_1, \dots, n_k]$ is the least common multiple of the moduli $n_1, \dots, n_k$. The reader is referred to [Gu] for problems and results on covers of $\mathbb{Z}$ and to [FFKPY] for a recent breakthrough in the field. In this paper we are only interested in applications of covers.

By a known result of Bang [B] (see also Zsigmondy [Z] and Birkhoff and Vandiver [BV]), for each integer $n > 1$ with $n \neq 6$, there exists a prime factor of $2^n - 1$ not dividing $2^m - 1$ for any $0 < m < n$; such a prime is called a *primitive prime divisor of* $2^n - 1$. P. Erdős, who introduced covers of $\mathbb{Z}$ in the early 1930s, constructed the following cover (cf. [E])

$$A_0 = \{0(2),\ 0(3),\ 1(4),\ 3(8),\ 7(12),\ 23(24)\}$$

whose moduli are distinct, greater than one and different from 6. It is easy to check that $2^2 - 1, 2^3 - 1, 2^4 - 1, 2^8 - 1, 2^{12} - 1, 2^{24} - 1$ have primitive prime divisors $3, 7, 5, 17, 13, 241$ respectively. Using the cover A_0 and the Chinese Remainder Theorem, Erdős showed that any integer x satisfying the congruences

$$\begin{cases} x \equiv 2^0 \pmod{3}, \\ x \equiv 2^0 \pmod{7}, \\ x \equiv 2^1 \pmod{5}, \\ x \equiv 2^3 \pmod{17}, \\ x \equiv 2^7 \pmod{13}, \\ x \equiv 2^{23} \pmod{241} \end{cases}$$

and the additional congruences $x \equiv 1 \pmod{2}$ and $x \equiv 3 \pmod{31}$ cannot be written in the form $2^n + p$ with $n \in \mathbb{N} = \{0, 1, 2, \dots\}$ and p a prime. The reader may consult [SY] for a refinement of this result. By improving the work of Cohen and Selfridge [CS], Sun [S00] showed that for any integer

$$x \equiv 47867742232066880047611079 \left(\bmod\ \prod_{p \in P} p\right)$$

with

$$P = \{2,\ 3,\ 5,\ 7,\ 11,\ 13,\ 17,\ 19,\ 31,\ 37,\ 41,\ 61,\ 73,\ 97,\ 109,\ 151,\ 241,\ 257,\ 331\},$$

we have $x \neq \pm p^a \pm q^b$ where p, q are primes and $a, b \in \mathbb{N}$. In 2005, Luca and Stănică [LS] constructed a cover of $\mathbb{Z}$ to show that if n is sufficiently large and $n \equiv 1807873 \pmod{3543120}$ then $F_n \neq p^a + q^b$ with p, q prime numbers and $a, b \in \mathbb{N}$, where the Fibonacci sequence $\{F_n\}_{n \geqslant 0}$ is given by

$$F_0 = 0,\ F_1 = 1,\ \text{and } F_{n+1} = F_n + F_{n-1} \text{ for } n = 1, 2, 3, \dots .$$

A famous conjecture of Erdős and J. L. Selfridge states that there does not exist a cover of $\mathbb{Z}$ with all the moduli odd, distinct and greater than one. There is little progress on this open conjecture (cf. [Gu] and [GS]). In contrast, we have the following theorem.

Theorem 1.1. *There exists a cover* $A_1 = \{a_s(n_s)\}_{s=1}^{173}$ *of* $\mathbb{Z}$ *with all the moduli greater than one and dividing the odd number*

$$3^3 \times 5^2 \times 7 \times 11 \times 13 = 675675,$$

for which there are distinct primes $p_1, \ldots, p_{173}$ *greater than* 5 *such that each* p_s $(1 \leqslant s \leqslant 173)$ *is a primitive prime divisor of* $2^{n_s} - 1$.

Theorem 1.1 has the following application.

Theorem 1.2. *Let* N *be any positive integer. Then there is a residue class consisting of odd numbers such that for each nonnegative* x *in the residue class and each* $m \in \{1, \ldots, N\}$ *divisible by none of* 3, 5, 7, 11, 13, *the number* $x^m - 2^n$ *with* $n \in \mathbb{N}$ *always has at least two distinct prime factors.*

Remark 1.1. Let $m \in \mathbb{Z}^+$. Chen [C] conjectured that there are infinitely many positive odd numbers x such that $x^m - 2^n$ with $n \in \mathbb{Z}^+$ always has at least two distinct prime factors, and he was able to prove this when $m \equiv 1 \pmod 2$ or $m \equiv \pm 2 \pmod{12}$. The conjecture is particularly difficult when m is a high power of 2. In a recent preprint [FFK], Filaseta, Finch and Kozek confirmed the conjecture for $m = 4, 6$ with the help of a deep result of Darmon and Granville [DG] on generalized Fermat equations; they also showed that there exist infinitely many integers $x \in \{1, 3^8, 5^8, \ldots\}$ such that $x^m 2^n + 1$ with $n \in \mathbb{Z}^+$ always has at least two distinct prime divisors.

Recall that $\{F_n\}_{n \geqslant 0}$ is the Fibonacci sequence. Set $u_n = F_{3n}/2$ for $n \in \mathbb{N}$. Clearly, $u_0 = 0$, $u_1 = 1$, and

$$\begin{aligned} u_{n+1} =& \frac{F_{3n+3}}{2} = \frac{F_{3n+1} + (F_{3n+1} + F_{3n})}{2} \\ =& F_{3n+1} + u_n = F_{3n-1} + 3u_n \\ =& 4u_n + \frac{2F_{3n-1} - F_{3n}}{2} \\ =& 4u_n + \frac{F_{3n-1} - F_{3n-2}}{2} \\ =& 4u_n + u_{n-1} \end{aligned}$$

for every $n = 1, 2, 3, \ldots$.

Now we give the third theorem which is of a new type and will be proved on the basis of certain cover of $\mathbb{Z}$ with odd moduli.

Theorem 1.3. *Let*

$$\begin{aligned} a =& 31207386885274502188173522132023665167365193670823768\text{-} \\ & 2341853548563549188738642 75 \end{aligned}$$

and

$$M = 368128524439220711844024989130760705031462298208612115\text{-}$$
$$583470788713547837448507 78.$$

Then, for any $x \equiv a \pmod{M}$ *and* $n \in \mathbb{N}$, *the number* $x^2 - F_{3n}/2$ *has at least two distinct prime divisors.*

Remark 1.2. (a) Actually our proof of Theorem 1.3 yields the following stronger result: Whenever $y \in a^2(M)$ and $n \in \mathbb{N}$, the number $y - F_{3n}/2$ has at least two distinct prime divisors.

(b) In view of Theorem 1.3, it is interesting to study the diophantine equation $x^2 - F_{3n}/2 = \pm p^a$ with $a, n, x \in \mathbb{N}$ and p a prime, or the equation $F_{3n} = 2x^2 \pm dy^2$ with d equal to 1 or 2 or twice an odd prime. The related equation $F_n = x^2 + dy^2$ has been investigated by Ballot and Luca [BL].

The second author has the following conjecture.

Conjecture 1.1. *Let* m *be any positive integer. Then there exist* $b, d \in \mathbb{Z}^+$ *such that whenever* $x \in b^m(d)$ *and* $n \in \mathbb{N}$ *the number* $x - F_n$ *has at least two distinct prime divisors. Also, there are odd integer* b *and even number* $d \in \mathbb{Z}^+$ *such that whenever* $x \in b^m(d)$ *and* $n \in \mathbb{N}$ *the number* $x - 2^n$ *has at least two distinct prime divisors.*

Remark 1.3. (a) We are unable to prove Conjecture 1.1 since it is difficult for us to construct a suitable cover of $\mathbb{Z}$ for the purpose.

(b) In 2006, Bugeaud, Mignotte and Siksek [BMS] showed that the only powers in the Fibonacci sequence are

$$F_0 = 0,\ F_1 = F_2 = 1,\ F_6 = 2^3 \text{ and } F_{12} = 12^2.$$

It seems challenging to solve the diophantine equation $x^m - F_n = \pm p^a$ with $a, n, x \in \mathbb{N}$, $m > 1$, and p a prime.

We are going to show Theorems 1.1–1.3 in Sections 2–4 respectively.

2. Proving Theorem 1.1 via constructions

Proof of Theorem 1.1. Let $a_1(n_1), \ldots, a_{173}(n_{173})$ be the following 173 residue classes respectively.

0(3), 1(5), 0(7), 1(9), 7(11), 8(11), 7(13), 8(15), 19(21), 17(25), 22(25), 25(27), 23(33), 29(35), 30(35), 14(39), 17(39), 4(45), 13(45), 0(55), 25(55), 50(55), 25(63), 52(63), 9(65), 2(75), 32(75), 13(77), 41(91), 62(91), 76(91), 5(99), 65(99), 86(99), 44(105), 59(105), 89(105), 31(117), 43(117), 83(117), 103(117), 35(135), 43(135), 88(135), 26(143), 86(143), 125(143), 35(165), 37(175), 87(175), 162(175), 34(189), 53(189), 155(195), 85(225), 130(225), 157(225), 202(225), 137(231), 158(231), 104(273), 146(273), 188(273), 65(275), 175(275), 152(297), 218(297), 79(315), 284(315), 295(315), 87(325), 112(325), 162(325), 16(351), 44(351), 97(351), 286(351), 313(351), 15(385), 225(385), 290(385), 191(429), 203(429), 284(429), 34(455), 454(455), 130(495), 230(495), 395(495), 179(525), 362(525), 445(525), 494(525), 335(585), 355(585), 412(585), 490(585), 7(675), 232(675), 277(675), 502(675), 200(693), 257(693), 515(693), 445(715), 500(715), 555(715), 356(819), 538(819), 629(819), 100(825), 145(825), 265(825), 475(825), 179(945), 494(945), 562(975), 637(975), 662(975), 862(975), 937(975), 115(1001), 808(1001), 5(1155), 809(1155), 845(1155), 950(1155), 614(1287), 742(1287), 1010(1287), 767(1365), 977(1365), 1235(1365), 350(1485), 220(1575), 662(1575), 1012(1575), 1390(1575), 470(1755), 580(1755), 610(1755), 880(1755), 564(1925), 949(1925), 1089(1925), 1334(1925), 1474(1925), 1859(1925), 202(2079), 895(2079), 911(2079), 1105(2145), 1670(2145), 1012(2275), 1362(2275), 1537(2275), 647(2457), 853(2457), 1210(2457), 1214(2457), 2365(2457), 2384(2457), 670(2475), 2245(2475), 2290(2475), 2264(3003), 1390(3465), 416(3861), 3195(5005), 1600(5775), 2920(6435), 7825(10395), 583939(675675).

It is easy to check that the least common multiple of $n_1, \dots, n_{173}$ is the odd number

$$3^3 \times 5^2 \times 7 \times 11 \times 13 = 675675.$$

Since $A_1 = \{a_s(n_s)\}_{s=1}^{173}$ covers $0, \dots, 675674$, it covers all the integers.

Using the software *Mathematica* and the main tables of [BLSTW, pp. 1–59], below we associate each $n \in \{n_1, \dots, n_{173}\}$ with m_n distinct primitive prime divisors $p_{n,1}, \dots, p_{n,m_n}$ of $2^n - 1$ and write $n : p_{n,1}, \dots, p_{n,m_n}$ for this, where m_n is the number of occurrences of n among the moduli $n_1, \dots, n_{173}$. For those

$$n \in \{1485, 3003, 3465, 3861, 5005, 5775, 6435, 10395, 675675\},$$

as $m_n = 1$ we just need one primitive prime divisor of $2^n - 1$ whose existence is guaranteed by Bang's theorem; but they are too large to be included in the following list.

3: 7; 5: 31; 7: 127; 9: 73; 11: 23, 89; 13: 8191;
15: 151; 21: 337; 25: 601, 1801; 27: 262657;
33: 599479; 35: 71, 122921; 39: 79, 121369; 45: 631, 23311;
55: 881, 3191, 201961; 63: 92737, 649657; 65: 145295143558111;
75: 100801, 10567201; 77: 581283643249112959;
91: 911, 112901153, 23140471537; 99: 199, 153649, 33057806959;
105: 29191, 106681, 152041; 117: 937, 6553, 86113, 7830118297;
135: 271, 348031, 49971617830801;
143: 724153, 158822951431, 5782172113400990737;
165: 20485688352973804867602 31;
175: 39551, 60816001, 535347624791488552837151;
189: 1560007, 207617485544258392970753527;
195: 1343041968450992625728145733 51;
225: 115201, 617401, 1348206751, 13861369826299351;
231: 463, 4982397651178256151338302204762057;
273: 108749551, 4093204977277417, 86977595801949844993;
275: 382027665134363932751, 4074891477354886815033308087379995347151;
297: 8950393, 1708866188231417380818309508072927716483135994 33;
315: 870031, 983431, 29728307155963706810228435378401;
325: 7151, 51879585551, 4613679391936953610429590532014122532260339 7396-44049093601;
351: 446473, 29121769, 571890896913727, 93715008807883087, 150832426800 17-3710177;
385: 55441, 1971764055031, 310553416811904444781267197559651345711 5147-3925765532041;
429: 17286204937, 106510771775654289288280258 6807, 16783351554928582788-5461382441449;
455: 200201, 47747974536083438032709889843322140983517825277475774 5602-83916249038566366768546 31;
495: 991, 33420293476473795143859474 6151, 608477715953763579655053686 37-41698483921;
525: 4201, 7351, 181165951, 3259855088755275876696070972226675571162 2113-9090131514801;
585: 2400314671, 339175003117573351, 2553752153166985215 91, 272833453603-459286533929980571253533 2071;
675: 1605151, 109427008539847839039559084 1401, 28424962631886476400 8979-4561760551, 4703900385034768551806279419427610 32401;
693: 289511839, 2868251407519807, 32259495750896115565329957738135 85269-0689819443677192184896969820547798379289023 23497;

715: 249602191565465311, 598887853030285391, 404371560247021095769621126905156405733487840189392571928708658758227326311683873284821544141641506240647137 11;

819: 2681001528674743, 2195163317271456972493 08031, 2149497317930391319-0133458460563964459380529075838941297352657742148160962406273546512257;

825: 702948566745151, 9115784422509601, 410831665424727139790492285217 7-568560929751, 10124924126024061560521761223037698180014266940 1;

945: 1243395210785469499143045214993922 41, 893712833189249887135446424-72309024678004403189516730060412595564942724011446583991926781827601;

975: 1951, 8837728285481551, 2615596668478972288500 1, 166376338119230863-5718252801, 4294500770439625509689707482842762056791217143467781867769 93-9979855730352201;

1001: 6007, 69527446946369608514121790903949092 07;

1155: 2311, 6250631311, 494224324441, 260078892331205274324088366772886 7-9019962160653438459960757841691207916601913191239370820827703893645439 3-545946152508951;

1287: 216217, 71477407, 141968533929529744009;

1365: 469561, 52393016292934591, 2224981001722824694441;

1575: 82013401, 32758188751, 76641458269269601, 764384916291005220555242-939647951;

1755: 3511, 196911, 4242734772486358591, 854883655194091009 51;

1925: 11551, 13167001, 1891705201, 5591298184498951, 292615400703113951, 5627063397043739893603449551;

2079: 4159, 16633, 80932047967;

2145: 96001053721, 347878768688881;

2275: 218401, 28319200001, 1970116306308855665077103351;

2457: 565111, 1410319, 21287449, 41194063, 167511687756624289 27, 178613107-4995391292297656133027144291751;

2475: 4951, 143551, 1086033846151.

Observe that $p_{n,j} > 5$ for all $n \in \{n_1, \ldots, n_{173}\}$ and $1 \leqslant j \leqslant m_n$. In view of the above, Theorem 1.1 has been proved. $\square$

3. Proof of Theorem 1.2

Recall that an odd prime p is called a Wieferich prime if $2^{p-1} \equiv 1 \pmod{p^2}$. The only known Wieferich primes are 1093 and 3511, and there are no others below 1.25×10^{15} (cf. [R, p. 230]).

Suppose that $n \neq 6$ is an integer greater than than one, and p is a primitive prime divisor of $2^n - 1$. Then n is the order of 2 mod p and hence $p-1$ is a multiple of n by Fermat's little theorem. Thus $2^n - 1 \mid 2^{p-1} - 1$, and hence $p^2 \nmid 2^n - 1$ if p is not a Wieferich prime.

Let $A_1=\{a_s(n_s)\}_{s=1}^{173}$ and $p_1,\ldots,p_{173}$ be as described in Theorem 1.1. For each $s=1,\ldots,173$ let q_s be a primitive prime divisor of $2^{p_s^2}-1$. Then $p_1,\ldots,p_{173}$, $q_1,\ldots,q_{173}$ are distinct odd primes since $\{p_1^2,\ldots,p_{173}^2\}\cap\{n_1,\ldots,n_{173}\}=\emptyset$.

For each $s=1,\ldots,173$ let α_s be the largest positive integer with $p_s^{\alpha_s}\mid 2^{n_s}-1$. Since 3511 is the only Wieferich prime in the set $\{p_1,\ldots,p_{173}\}$, we have $\alpha_s=1$ if $p_s\neq 3511$. In the case $p_s=3511$, we have $\alpha_s=2$ since $3511^2\mid 2^{3510}-1$ but $3511^3\nmid 2^{3510}-1$.

Let $M=2^{2L}\prod_{s=1}^{173}p_s^{\alpha_s+2}q_s$, where L is the smallest positive integer satisfying

$$2^L-1>\max\{16N,p_1^{\alpha_1+1},\ldots,p_{173}^{\alpha_{173}+1}\}.$$

By the Chinese Remainder Theorem, there exists a unique $a\in\{1,\ldots,M\}$ such that

$$1+3\cdot 2^L(2^{2L})\cap\bigcap_{s=1}^{173}\left(x_s^{b_s}(p_s^{\alpha_s+2})\cap y_s^{b_s}(q_s)\right)=a(M).$$

Let $m\leqslant N$ be a positive integer relatively prime to $3\cdot5\cdot7\cdot11\cdot13=15015$, and write $m=2^\alpha m_0$ with $\alpha\in\mathbb{N}$, $m_0\in\mathbb{Z}^+$ and $2\nmid m_0$. Let $s\in\{1,\ldots,173\}$. Since n_s is a divisor of $3^3\cdot5^2\cdot7\cdot11\cdot13=675675$, we have $\gcd(m,n_s)=1$ and hence $m_0b_s\equiv a_s\pmod{n_s}$ for some $b_s\in\mathbb{N}$.

As the order of 2 mod p_s is the odd number n_s, n_s divides $(p_s-1)/\gcd(2^\alpha,p_s-1)$ and hence

$$2^{(p_s-1)/\gcd(2^\alpha,\ p_s-1)}\equiv 1\pmod{p_s},\ 2^{p_s(p_s-1)/\gcd(2^\alpha,\ p_s-1)}\equiv 1\pmod{p_s^2},\ \ldots.$$

Since there is a primitive root modulo $p_s^{\alpha_s+2}$ and

$$2^{\varphi(p_s^{\alpha_s+2})/\gcd(2^\alpha,\varphi(p_s^{\alpha_s+2}))}=2^{p_s^{\alpha_s+1}(p_s-1)/\gcd(2^\alpha,p_s-1)}\equiv 1\pmod{p_s^{\alpha_s+2}}$$

(where φ is Euler's totient function), by [IR, Proposition 4.2.1] there exists $x_s\in\mathbb{Z}$ with $x_s^{2^\alpha}\equiv 2\pmod{p_s^{\alpha_s+2}}$. Similarly, the order p_s^2 of 2 mod q_s divides $(q_s-1)/\gcd(2^\alpha,q_s-1)$, therefore $2^{(q_s-1)/\gcd(2^\alpha,q_s-1)}\equiv 1\pmod{q_s}$ and hence $y_s^{2^\alpha}\equiv 2\pmod{q_s}$ for some $y_s\in\mathbb{Z}$.

Let $x\geqslant 0$ be an element of $a(M)$. As A_1 is a cover of $\mathbb{Z}$, for any $n\in\mathbb{N}$ there is an $s\in\{1,\ldots,173\}$ such that $n\equiv a_s\pmod{n_s}$. Clearly

$$x^m\equiv(x_s^{b_s})^m=(x_s^{2^\alpha})^{m_0b_s}\equiv 2^{m_0b_s}\pmod{p_s^{\alpha_s+2}},$$

thus

$$x^m-2^n\equiv 2^{m_0b_s}-2^{a_s}\equiv 0\pmod{p_s^{\alpha_s}}$$

since $2^{n_s}\equiv 1\pmod{p_s^{\alpha_s}}$ and $m_0b_s\equiv a_s\pmod{n_s}$.

As $16m\leqslant 16N<2^L-1$ and $x\equiv 1+3\cdot 2^L\pmod{2^{2L}}$, we have $|x^m-2^n|\geqslant 2^L-1>p_s^{\alpha_s+1}$ by [C, Lemma 1]. So $|x^m-2^n|\neq 0,p_s^{\alpha_s},p_s^{\alpha_s+1}$. If x^m-2^n is not divisible by $p_s^{\alpha_s+2}$, then it must have at least two distinct prime divisors.

Now we assume that $x^m - 2^n \equiv 0 \pmod{p_s^{\alpha_s+2}}$. Note that $2^n \equiv x^m \equiv 2^{m_0 b_s} \pmod{p_s^{\alpha_s+2}}$. Since n_s is the order of 2 mod $p_s^{\alpha_s}$ and not the order of 2 mod $p_s^{\alpha_s+1}$, by [C, Corollary 3] we have $2^n \equiv 2^{m_0 b_s} \pmod{q_s}$. Thus

$$x^m - 2^n \equiv (y_s^{b_s})^{2^\alpha m_0} - 2^{m_0 b_s} \equiv 0 \pmod{q_s}$$

and so the nonzero integer $x^m - 2^n$ has at least two distinct prime divisors (including p_s and q_s).

By the above, we have proved the desired result. □

Remark 3.1. Given $m, n \in \mathbb{Z}^+$ and an odd prime p, the equation $x^m - 2^n = p^b$ with $b, x \in \mathbb{N}$ only has finitely many solutions. As observed by the referee, this is a consequence of the Darmon-Granville theorem in [DG]. In the case $m = 2$, all the finitely many solutions are effectively computable by the algorithms given by Weger [W].

4. Proof of Theorem 1.3

Lemma 4.1. *Let $c \in \mathbb{Z}^+$, and define $\{U_n\}_{n\geqslant 0}$ by*

$$U_0 = 0,\ U_1 = 1,\ \textit{and } U_{n+1} = cU_n + U_{n-1} \textit{ for } n = 1, 2, 3, \ldots .$$

Suppose that $n > 0$ is an integer with $n \equiv 2 \pmod 4$ and p is a prime divisor of U_n which divides none of $U_1, \ldots, U_{n-1}$. Then $U_{kn+r} \equiv U_r \pmod p$ for all $k \in \mathbb{N}$ and $r \in \{0, \ldots, n-1\}$.

Proof. By [HS, Lemma 2], $U_{n+1} \equiv -(-1)^{n/2} = 1 \pmod p$. If $k \in \mathbb{N}$ and $r \in \{0, \ldots, n-1\}$, then $U_{kn+r} \equiv U_{n+1}^k U_r \pmod{U_n}$ by [HS, Lemma 3] or [S92, Lemma 2], therefore $U_{kn+r} \equiv U_r \pmod p$. □

Proof of Theorem 1.3. Let $b_1(m_1), \ldots, b_{24}(m_{24})$ be the following 24 residue classes:

$$\begin{gathered}1(3),\ 2(5),\ 3(5),\ 4(7),\ 6(7),\ 0(9),\ 5(15),\ 11(15),\ 9(21),\ 12(21),\\ 1(35),\ 14(35),\ 24(35),\ 29(35),\ 6(45),\ 15(45),\ 29(45),\ 30(45),\\ 5(63),\ 23(63),\ 44(63),\ 66(105),\ 21(315),\ 89(315).\end{gathered}$$

It is easy to check that $\{b_t(m_t)\}_{t=1}^{24}$ forms a cover of $\mathbb{Z}$ with odd moduli. Set $m_0 = 1$. Then

$$B = \{1(2m_0), 2b_1(2m_1), \ldots, 2b_{24}(2m_{24})\}$$

is a cover of $\mathbb{Z}$ with all the moduli congruent to 2 mod 4.

Let $u_n = F_{3n}/2$ for $n \in \mathbb{N}$. As we mentioned in Section 1, $u_0 = 0$, $u_1 = 1$ and $u_{n+1} = 4u_n + u_{n-1}$ for $n = 1, 2, 3, \ldots$. For a prime p and an integer $n > 0$, we call p a *primitive prime divisor of* u_n if $p \mid u_n$ but $p \nmid u_k$ for those $0 < k < n$.

Let $p_0, \dots, p_{24}$ be the following 25 distinct primes respectively:

2, 19, 31, 11, 211, 29, 5779, 541, 181, 31249, 1009, 767131, 21211, 911,
71, 119611, 42391, 271, 811, 379, 912871, 85429, 631, 69931, 17011.

One can easily verify that each p_t $(0 \leqslant t \leqslant 24)$ is a primitive prime divisor of u_{2m_t}.

The residue class $a(M)$ in Theorem 1.3 is actually the intersection of the following 25 residue classes with the moduli $p_0, \dots, p_{24}$ respectively:

$$1(2),\ 2(19),\ 14(31),\ 4(11),\ 94(211),\ 5(29),\ 0(5779),\ 156(541),\ 76(181),$$
$$10727(31249),\ 501(1009),\ 2(767131),\ 7199(21211),\ 257(911),\ 30(71),$$
$$13909(119611),\ 9054(42391),\ 85(271),\ 292(811),\ 72(379),\ 80065(912871),$$
$$40368(85429),\ 205(631),\ 19928(69931),\ 497(17011).$$

It is known that the only solutions of the diophantine equation $F_n = 2x^2$ with $n, x \in \mathbb{N}$ are $(n, x) = (0,0), (3,1), (6,2)$. (Cf. [Co, Theorem 4].) Let x be any integer in the residue class $a(M)$. Then $|x| > 2$ and hence $x^2 \neq u_n = F_{3n}/2$ for all $n \in \mathbb{N}$. With the help of Lemma 4.1 in the case $c = 4$, one can check that $x^2 \equiv u_1 = 1 \pmod{p_0}$ and $x^2 \equiv u_{2b_t} \pmod{p_t}$ for all $t = 1, \dots, 24$.

Let n be any nonnegative integer. As B forms a cover of $\mathbb{Z}$, $n \equiv 1 \pmod{2m_0}$ or $n \equiv 2b_t \pmod{2m_t}$ for some $1 \leqslant t \leqslant 24$. By Lemma 4.1 with $c = 4$, if $n \equiv 1 \pmod{2m_0}$ then $u_n \equiv u_1 = 1 \pmod{p_0}$ and hence $x^2 - u_n \equiv x^2 - 1 \equiv 0 \pmod{p_0}$; if $n \equiv 2b_t \pmod{2m_t}$ then $u_n \equiv u_{2b_t} \pmod{p_t}$ and hence $x^2 - u_n \equiv x^2 - u_{2b_t} \equiv 0 \pmod{p_t}$. Thus, it remains to show that for any given $a, b \in \mathbb{N}$ we can deduce a contradiction if $x^2 - u_{1+2m_0a} = \pm 2^b$ or $x^2 - u_{2b_t+2m_ta} = \pm p_t^b$ for some $1 \leqslant t \leqslant 24$.

Case 4.0. $x^2 - u_{1+2a} = \pm 2^b$.

As $p_2 = 31$ and $p_3 = 11$ are primitive prime divisors of $u_{2m_2} = u_{2m_3} = u_{10}$, and

$$u_1 = 1,\ u_3 = 17,\ u_5 = 305,\ u_7 = 5473,\ u_9 = 98209$$

have residues $1, -14, -5, -14, 1$ modulo 31 and residues $1, -5, -3, -5, 1$ modulo 11 respectively. If $2a + 1 \not\equiv 5 \pmod{10}$, then by Lemma 4.1 we have

$$x^2 - u_{1+2a} \equiv 10 - 1, 10 - (-14) \not\equiv \pm 1, \pm 2, \pm 4, \pm 8, \pm 16 \pmod{31}$$

which contradicts $x^2 - u_{1+2a} = \pm 2^b$. (Note that $2^5 \equiv 1 \pmod{31}$.) So $2a + 1 \equiv 5 \pmod{10}$. It follows that

$$x^2 - u_{1+2a} \equiv 10 - (-5) \equiv -2^4 \pmod{31} \text{ and } x^2 - u_{1+2a} \equiv 5 - (-3) = 2^3 \pmod{11}.$$

Thus $x^2 - u_{1+2a}$ can only be -2^b with $b \equiv 4 \pmod 5$, which cannot be congruent to 2^3 mod 11. (Note that $2^5 \equiv -1 \pmod{11}$.) So we have a contradiction.

`Case 4.1.` $x^2 - u_{2+6a} = \pm 19^b$.

Observe that

$$u_0 = 0,\ u_2 = 4,\ u_4 = 72,\ u_6 = 1292,\ u_8 = 23184$$

have residues $0, 4, -5, 5, -4$ modulo 11 and $0, 4, 10, -10, -4$ modulo 31 respectively. Also, $19^b \equiv 2^{3b} \equiv \pm 1, \pm 2, \pm 4, \pm 3, \pm 5 \pmod{11}$ and $19^5 \equiv (-2^2 \cdot 3)^5 \equiv -3^5 \equiv 5 \pmod{31}$.

If $2 + 6a \equiv 0 \pmod{10}$, then

$$x^2 - u_{2+6a} \equiv 5 - 0 \equiv 19^8, -19^3 \pmod{11}$$

and hence $x^2 - u_{2+6a} = (-1)^{d-1} 19^{3+5d}$ for some $d \in \mathbb{N}$, this leads to a contradiction since $x^2 - u_{2+6a} \equiv 10 - 0 \pmod{31}$ but

$$19^{3+5d} \equiv 8 \times 5^d \equiv 8, 9, 14 \not\equiv \pm 10 \pmod{31}.$$

Now we handle the case $2 + 6a \equiv 2 \pmod{10}$. Since 181 is a primitive prime divisor of u_{30}, and $6a \equiv 0 \pmod{30}$ and $19^2 \equiv -1 \pmod{181}$, we have

$$x^2 - u_{2+6a} \equiv 76^2 - u_2 \equiv -20 \not\equiv \pm 19^b \pmod{181}$$

which leads a contradiction.

If $2 + 6a \equiv 4 \pmod{10}$, then $x^2 - u_{2+6a} \equiv 10 - 10 = 0 \pmod{31}$. If $2 + 6a \equiv 6 \pmod{10}$, then $x^2 - u_{2+6a} \equiv 5 - 5 = 0 \pmod{11}$. So, when $2 + 6a \equiv 4, 6 \pmod{10}$ we get a contradiction since $x^2 - u_{2+6a} = \pm 19^b$.

If $2 + 6a \equiv 8 \pmod{10}$, then $x^2 - u_{2+6a} \equiv 5 - (-4) \equiv 19^2, -19^7 \pmod{11}$ and hence $x^2 - u_{2+6a} = (-1)^d 19^{2+5d}$ for some $d \in \mathbb{N}$, this leads a contradiction since $x^2 - u_{2+6a} \equiv 10 - (-4) \equiv -11 \times 10 \pmod{31}$ but

$$19^{2+5d} \equiv -11 \times 5^d \equiv -11, -11 \times 5, -11 \times (-6) \not\equiv \pm 11 \times 10 \pmod{31}.$$

`Case 4.2.` $x^2 - u_{4+10a} = \pm 31^b$.

As $x^2 - u_{4+10a} \equiv 5 - u_4 \equiv 5 - (-5) \equiv -1 \pmod{11}$ and $31^b \equiv (-2)^b \equiv 1, -2, 4, -8, 16 \pmod{11}$, we must have $x^2 - u_{4+10a} = -31^b$ with $b \equiv 0 \pmod 5$. As $31^5 \equiv 2^3 = 8 \pmod{19}$, $31^b \equiv 8^{b/5} \equiv \pm 1, \pm 8, \pm 7 \pmod{19}$. If $3 \nmid a$, then $4 + 10a \equiv 0, 2 \pmod 6$ and hence

$$x^2 - u_{4+10a} \equiv 4 - u_0, 4 - u_2 \equiv 4, 0 \not\equiv -31^b \pmod{19}.$$

Thus $a = 3c$ for some $c \in \mathbb{N}$. As

$$-8^{b/5} \equiv -31^b = x^2 - u_{4+10a} \equiv 4 - u_4 = 4 - 72 \equiv 8 \pmod{19},$$

we have $b/5-1\equiv 3 \pmod 6$ and hence $b=20+30d$ for some $d\in\mathbb{N}$. As $31^{10}\equiv -1 \pmod{181}$, we have $31^b=31^{20+30d}\equiv(-1)^{2+3d}=(-1)^d \pmod{181}$. On the other hand,

$$-31^b=x^2-u_{4+10a}=x^2-u_{4+30c}\equiv 76^2-u_4\equiv -16-72=-88 \pmod{181}.$$

So we get a contradiction.

`Case 4.3.` $x^2-u_{6+10a}=\pm 11^b$.

As $x^2-u_{6+10a}\equiv 10-(-10)\equiv -11 \pmod{31}$, and the order of 11 mod 31 is 30, we have $x^2-u_{6+10a}=(-1)^{d-1}11^{1+15d}$ for some $d\in\mathbb{N}$. Since $11^{15}\equiv(-8)^{15}=(-2^9)^5\equiv 1 \pmod{19}$, we have $x^2-u_{6+10a}\equiv\pm 11 \pmod{19}$.

If $6+10a\equiv 0,2 \pmod 6$, then

$$x^2-u_{6+10a}\equiv 4-u_0, 4-u_2\not\equiv\pm 11 \pmod{19}.$$

So $6+10a\equiv 4 \pmod 6$, i.e., $a=1+3c$ for some $c\in\mathbb{N}$. Therefore

$$x^2-u_{6+10a}=x^2-u_{16+30c}\equiv -16-u_{16}\equiv -16-47\equiv -11\times 88 \pmod{181}.$$

Note that

$$(-11)^{15d}\equiv(-49)^d\equiv 1,\ -49,\ 48\not\equiv 88 \pmod{181}.$$

As $x^2-u_{6+10a}=(-11)^{1+15d}$, we get a contradiction.

`Case 4.4.` $x^2-u_{8+14a}=\pm 211^b$.

As $p_5=29$ is a primitive divisor of $u_{2m_5}=u_{14}$, we have $x^2-u_{8+14a}\equiv 25-u_8\equiv 25-13=12 \pmod{29}$.

Since 2 is a primitive root mod 29, $211\equiv 2^3 \pmod{29}$, $2^{3\times 21}\equiv 2^7\equiv 12 \pmod{29}$, and $2^{3\times 7}\equiv 12^3\equiv -12 \pmod{29}$, we have $x^2-u_{8+14a}=(-1)^{d-1}211^{7+14d}$ for some $d\in\mathbb{N}$.

Observe that

$$\begin{aligned}x^2-u_{8+14a}&\equiv 10-u_0, 10-u_2, 10-u_4, 10-u_6, 10-u_8,\\ &\equiv 10-0, 10-4, 10-10, 10-(-10), 10-(-4) \pmod{31}.\end{aligned}$$

Clearly $211\equiv 5^2 \pmod{31}$ and $5^3\equiv 1 \pmod{31}$, thus

$$211^{7+14d}\equiv 5^{14+28d}\equiv 5^{2+d}\equiv -6,\ 1,\ 5 \pmod{31}.$$

Therefore $2\mid d$, $3\mid d$ and $8+14a\equiv 2 \pmod{10}$. It follows that $a=1+5c$ for some $c\in\mathbb{N}$ and $d=6e$ for some $e\in\mathbb{N}$.

Note that

$$x^2-u_{8+14(1+5c)}\equiv x^2-u_2\equiv 5-4=1 \pmod{11}$$

and

$$(-1)^{d-1}211^{7+14d} \equiv -2^{7(1+12e)} \equiv -2^{7(1+2e)} \pmod{11}.$$

So $2^{7(1+2e)} \equiv -1 \equiv 2^5 \pmod{11}$, hence $7(1+2e) \equiv 5 \equiv 35 \pmod{10}$ and thus $e \equiv 2 \pmod{5}$. Therefore $7+14d \equiv 7+84\times 2 \equiv 35 \pmod{140}$ and hence

$$211^{7+14d} \equiv (-2)^{35} \equiv \left(\frac{-2}{71}\right) = -\left(\frac{2}{71}\right) = -1 \pmod{71}$$

by the theory of quadratic residues, but

$$x^2 - u_{8+14a} = x^2 - u_{22+70c} \equiv 30^2 - u_{22} = 900 - 13888945017644 \equiv 14 \pmod{71},$$

so we get a contradiction from the equality $x^2 - u_{8+14a} = -211^{7+14d}$.

Case 4.5. $x^2 - u_{12+14a} = \pm 29^b$.

As $29^b \equiv (-2)^b \equiv \pm1, \pm2, \pm4, \pm8, \pm16 \pmod{31}$, $x^2 \equiv 14^2 \equiv 10 \pmod{31}$ and

$$u_{12+14a} \equiv u_0, u_2, u_4, u_6, u_8 \equiv 0, 4, 10, -10, -4 \pmod{31},$$

we have $x^2 - u_{12+14a} \not\equiv \pm 29^b \pmod{31}$. So, a contradiction occurs.

Case 4.6. $x^2 - u_{0+18a} = \pm 5779^b$.

As $x^2 - u_{18a} \equiv 2^2 - u_0 = 4 \pmod{19}$, $5779 \equiv 3 \pmod{19}$ and the order of 3 mod 19 equals 18, we have $x^2 - u_{18a} = (-1)^{d-1}5779^{5+9d} = (-5779)^{5+9d}$ for some $d \in \mathbb{N}$.

Note that

$$(-5779)^{9d} \equiv (-13)^{9d} \equiv (2^2)^{3d} \equiv 2^d \equiv 1,\ 2,\ 4,\ 8,\ 16 \pmod{31}$$

and $5779^5 \equiv 13^5 \equiv 6 \pmod{31}$. Thus

$$x^2 - (-5779)^{5+9d} \equiv 10 + 6 \times 2^d \equiv -15,\ -9,\ 3,\ -4,\ 13 \pmod{31}$$

while $u_{18a} \equiv u_0, u_2, u_4, u_6, u_8 \equiv 0, 4, 10, -10, -4 \pmod{31}$. As $u_{18a} = x^2 - (-5779)^{5+9d}$, we must have $18a \equiv 8 \pmod{10}$ and $d = 3 + 5e$ for some $e \in \mathbb{N}$.

Observe that $x^2 - u_{18a} \equiv 5 - u_8 \equiv -2 \pmod{11}$ but

$$(-5779)^{5+9d} \equiv (-2^2)^{5+9(3+5e)} = (-1)^e 2^{64+90e} \equiv (-1)^e 2^4 \not\equiv -2 \pmod{11}.$$

So a contradiction occurs.

Case 4.7. $x^2 - u_{10+30a} = \pm 541^b$.

As $x^2 - u_{10+30a} \equiv 5 - u_0 \equiv 5 \pmod{11}$ and

$$541^b \equiv 2^b \equiv \pm1, \pm2, \pm3, \pm4, \pm8, \pm16 \pmod{11},$$

$x^2 - u_{10+30a} = (-1)^d 541^{4+5d}$ for some $d \in \mathbb{N}$, and hence we have a contradiction since $x^2 - u_{10+30a} \equiv 10 - u_0 = 10 \pmod{31}$ but

$$541^{4+5d} \equiv (2 \times 7)^{4+5d} \equiv 7 \times 5^d \equiv 7,\ 7 \times 5,\ 7 \times (-6) \not\equiv \pm 10 \pmod{31}.$$

`Case 4.8.` $x^2 - u_{22+30a} = \pm 181^b$.

As $x^2 - u_{22+30a} \equiv 5 - u_2 = 5 - 4 \pmod{11}$ and $181^b \equiv 5^b \equiv 1, 5, 3, 4, -2 \pmod{11}$, we have $x^2 - u_{22+30a} = 181^b$ with $b = 5d$ for some $d \in \mathbb{N}$. Since $x^2 - u_{22+30a} \equiv x^2 - u_2 \equiv 10 - 4 = 6 \pmod{31}$ and $181^{5d} \equiv (-5)^{5d} \equiv 6^d \equiv 1, 6, 5, -1, -6, -5 \pmod{31}$, $d = 1 + 6e$ for some $e \in \mathbb{N}$. Note that $x^2 - u_{22+30a} \equiv 4 - u_4 = 4 - 72 \equiv 8 \pmod{19}$ but

$$181^{5d} \equiv (-9)^{5d} = (-3^{10})^d \equiv 3^d = 3^{1+6e} \equiv 3 \times 7^e \equiv 3,\ 2,\ -5 \not\equiv 8 \pmod{19}.$$

`Case 4.9.` $x^2 - u_{18+42a} = \pm 31249^b$.

Note that $31249^b \equiv 1^b = 1 \pmod{31}$, $x^2 \equiv 10 \pmod{31}$ and also

$$u_{18+42a} \equiv u_0, u_2, u_4, u_6, u_8 \equiv 0,\ 4,\ 10,\ -10,\ -4 \pmod{31}.$$

Therefore $x^2 - u_{18+42a} \not\equiv \pm 31249^b \pmod{31}$.

`Case 4.10.` $x^2 - u_{24+42a} = \pm 1009^b$.

As $x^2 - u_{24+42a} \equiv 4 - u_0 = 4 \pmod{19}$, $1009 \equiv 2 \pmod{19}$ and 2 is a primitive root modulo 19, we have $x^2 - u_{24+42a} = (-1)^d 1009^{2+9d} = (-1009)^{2+9d}$ for some $d \in \mathbb{N}$. Observe that $u_{10} = 416020$ and $x^2 - u_{24+42a} \equiv 25 - u_{10} \equiv 10 \pmod{29}$. But $6^7 \equiv -1 \pmod{29}$ and hence

$$(-1009)^{2+9d} \equiv 6^{2+9d} \equiv \pm 1,\ \pm 6,\ \pm 7,\ \pm 13,\ \pm 9,\ \pm 4,\ \pm 5 \not\equiv 10 \pmod{29}.$$

So we get a contradiction.

`Case 4.11.` $x^2 - u_{2+70a} = \pm 767131^b$.

Observe that $x^2 - u_{2+70a} \equiv 5^2 - u_2 \equiv -8 \pmod{29}$ and

$$767131^b \equiv (-6)^b \equiv 1,\ -6,\ 7,\ -13,\ -9,\ -4,\ -5 \pmod{29}.$$

So a contradiction occurs.

`Case 4.12.` $x^2 - u_{28+70a} = \pm 21211^b$.

As $28 + 70a \equiv 0 \pmod{14}$, we have $x^2 - u_{28+70a} \equiv 5^2 - u_0 \equiv -4 \pmod{29}$. On the other hand,

$$21211^b \equiv \pm 12^b \equiv \pm 1,\ \pm 12 \pmod{29}.$$

Thus we have a contradiction.

`Case 4.13.` $x^2 - u_{48+70a} = \pm 911^b$.

Note that $x^2 - u_{48+70a} \equiv 5^2 - u_6 = 25 - 1292 \equiv 9 \pmod{29}$ but $911^b \equiv 12^b \equiv \pm1, \pm12 \pmod{29}$.

`Case 4.14.` $x^2 - u_{58+70a} = \pm 71^b$.
Observe that $x^2 - u_{58+70a} \equiv 5^2 - u_2 \equiv -8 \pmod{29}$ but

$$71^b \equiv 13^b \equiv \pm1,\ \pm13,\ \pm5,\ \pm7,\ \pm4,\ \pm6,\ \pm9 \pmod{29}.$$

`Case 4.15.` $x^2 - u_{12+90a} = \pm 119611^b$.
Since $x^2 - u_{12+90a} \equiv 4 - u_0 \equiv 4 \pmod{19}$ and

$$119611^b \equiv 6^b \equiv 1,\ 6,\ -2,\ 7,\ 4,\ 5,\ -8,\ 9,\ -3 \pmod{19},$$

we must have $x^2 - u_{12+90a} = 119611^b$ with $b = 4 + 9d$ for some $d \in \mathbb{N}$. Note that $x^2 - u_{12+90a} \equiv 10 - u_2 = 6 \equiv 10 \times 13 \pmod{31}$, but

$$119611^{4+9d} \equiv 13^{4+9d} \equiv 10(-2)^d \pmod{31}$$

with $(-2)^d \equiv \pm1, \pm2, \pm4, \pm8, \pm16 \not\equiv 13 \pmod{31}$. So we have a contradiction.

`Case 4.16.` $x^2 - u_{30+90a} = \pm 42391^b$.
As $x^2 - u_{30+90a} \equiv 4 - u_0 = 4 \pmod{19}$, $42391 \equiv 2 \pmod{19}$ and 2 is a primitive root mod 19, we have $x^2 - u_{30+90a} = (-1)^d 42391^{2+9d}$ for some $d \in \mathbb{N}$.
Note that $x^2 - u_{30+90a} \equiv 10 - 0 \pmod{31}$ and

$$(-42391)^{2+9d} \equiv (-14)^{2+9d} \equiv 10(-2^4)^{3d} \equiv 10(-1)^d 2^{2d} \pmod{31}.$$

Since the only residues of powers of 2 modulo 31 are 1, 2, 4, 8, 16, we must have $x^2 - u_{30+90a} = (-42391)^{2+9d}$ with d divisible by both 5 and 2. Write $d = 10e$ with $e \in \mathbb{N}$. Then

$$x^2 - u_{30+90a} = 42391^{2+90e} \equiv (-3)^{2+90e} \equiv 9 \pmod{11},$$

which contradicts the fact $x^2 - u_{30+90a} \equiv 5 - u_0 = 5 \pmod{11}$.

`Case 4.17.` $x^2 - u_{58+90a} = \pm 271^b$.
Note that $x^2 - u_{58+90a} \equiv 10 - u_8 \equiv 14 \pmod{31}$ while

$$271^b \equiv (-2)^{3b} \equiv \pm1,\ \pm2,\ \pm4,\ \pm8,\ \pm16 \pmod{31}.$$

`Case 4.18.` $x^2 - u_{60+90a} = \pm 811^b$.
As $x^2 - u_{60+90a} \equiv 10 - u_0 = 10 \pmod{31}$ and $811^b \equiv 5^b \equiv 1, 5, 25 \pmod{31}$. we have a contradiction.

`Case 4.19.` $x^2 - u_{10+126a} = \pm 379^b$.

Note that $x^2 - u_{10+126a} \equiv 2^2 - u_4 = 4 - 72 \equiv 8 \pmod{19}$ but $379^b \equiv (-1)^b \equiv \pm 1 \pmod{19}$.

`Case 4.20`. $x^2 - u_{46+126a} = \pm 912871^b$.

Since $x^2 - u_{46+126a} \equiv 2^2 - u_4 \equiv 2^3 \pmod{19}$, $912871^b \equiv 2^{4b} \pmod{19}$ and the order of 2 mod 19 is 18, we must have $x^2 - u_{46+126a} = -912871^b$ with $b = 3 + 9d$ for some $d \in \mathbb{N}$. Note that $x^2 - u_{46+126a} \equiv 5^2 - u_4 = 25 - 72 \equiv 11 \pmod{29}$ but

$$912871^{3+9d} \equiv 3^{2(3+9d)} \equiv 4^{1+3d} \equiv \pm 1,\ \pm 4,\ \pm 13,\ \pm 6,\ \pm 5,\ \pm 9,\ \pm 7 \pmod{29}.$$

So we have a contradiction.

`Case 4.21`. $x^2 - u_{88+126a} = \pm 85429^b$.

Observe that $x^2 - u_{88+126a} \equiv 5^2 - u_4 \equiv 11 \pmod{29}$ but

$$85429^b \equiv (-5)^b \equiv 1,\ -5,\ -4,\ -9,\ -13,\ 7,\ -6 \pmod{29}.$$

So a contradiction occurs.

`Case 4.22`. $x^2 - u_{132+210a} = \pm 631^b$.

Note that $x^2 - u_{132+210a} \equiv 4^2 - u_2 \equiv 1 \pmod{11}$ and $631 \equiv 2^2 \pmod{11}$. Since $2^5 \equiv -1 \pmod{11}$ and $2^{10} \equiv 1 \pmod{11}$, we must have $x^2 - u_{132+210a} = 631^b$ with $b = 5d$ for some $d \in \mathbb{N}$. As $x^2 - u_{132+210a} \equiv 10 - u_2 = 6 \pmod{31}$, $631^5 \equiv (-2^2 \times 5)^5 \equiv -5^2 \equiv 6 \pmod{31}$ and the order of 6 mod 31 is 6, we can write $d = 1 + 6e$ with $e \in \mathbb{N}$. Thus

$$x^2 - u_{132+210a} = 631^{5+30e} \equiv (2^2)^{5+30e} \equiv (-2)^{1+6e} \equiv -2,\ 5,\ -3 \pmod{19}.$$

On the other hand, $x^2 - u_{132+210a} \equiv 4 - u_0 = 4 \pmod{19}$. This leads to a contradiction.

`Case 4.23`. $x^2 - u_{42+630a} = \pm 69931^b$.

As $42 + 630a \equiv 0 \pmod 6$, we have $x^2 - u_{42+630a} \equiv 2^2 - u_0 = 4 \pmod{19}$. On the other hand, $69931^b \equiv (-2)^{3b} \equiv 1,\ -8,\ 7 \pmod{19}$. So we get a contradiction.

`Case 4.24`. $x^2 - u_{178+630a} = \pm 17011^b$.

Since $178 + 630a \equiv 10 \pmod{14}$, we have

$$x^2 - u_{178+630a} \equiv 5^2 - u_{10} = 25 - 416020 \equiv 10 \pmod{29}.$$

Note that $17011^b \equiv (-12)^b \equiv \pm 1,\ \pm 12 \pmod{29}$. So a contradiction occurs.

In view of the above, we have completed the proof of Theorem 1.3. □

Acknowledgment. The authors would like to thank the referee for some helpful comments.

References

[BL] C. Ballot and F. Luca, *On the equation $x^2 + dy^2 = F_n$*, Acta Arith. **127** (2007), 145–155.

[B] A. S. Bang, *Taltheoretiske Undersgelser*, Tidsskrift for Mat. **4** (1886), no. 5, 70–80, 130–137.

[BV] G. D. Birkhoff and H. S. Vandiver, *On the integral divisors of $a^n - b^n$*, Ann. of Math. **5** (1904), 173–180.

[BLSTW] J. Brillhart, D. H. Lehmer, J. L. Selfridge, B. Tuckerman, and S. S. Wagstaff, Jr., *Factorizations of $b^n \pm 1$, $b = 2, 3, 5, 6, 7, 10, 11, 12$ up to High Powers*, 3rd ed., Contemporary Mathematics 22, Amer. Math, Soc., Providence, RI, 2002.

[BMS] Y. Bugeaud, M. Mignotte and S. Siksek, *Classical and modular approaches to exponential Diophantine equations. I. Fibonacci and Lucas perfect powers*, Ann. of Math. (2) **163** (2006), 969–1018.

[C] Y.-G. Chen, *On integers of the forms $k^r - 2^n$ and $k^r 2^n + 1$*, J. Number Theory **98** (2003), 310–319.

[CS] F. Cohen and J. L. Selfridge, *Not every number is the sum or difference of two prime powers*, Math. Comput. **29** (1975), 79–81.

[Co] J. H. E. Cohn, *Square Fibonacci numbers, etc.*, Fibonacci Quart. **2** (1964), 109–113.

[DG] H. Darmon and A. Granville, *On the equations $z^m = F(x, y)$ and $Ax^p + By^q = Cz^r$*, Bull. London Math. Soc. **27** (1995), 513–544.

[E] P. Erdős, *On integers of the form $2^k + p$ and some related problems*, Summa Brasil. Math. **2** (1950), 113–123.

[FFK] M. Filaseta, C. Finch and M. Kozek, *On powers associated with Sierpiński numbers, Riesel numbers and Polignac's conjecture*, J. Number Theory **128** (2008), 1916–1940.

[FFKPY] M. Filaseta, K. Ford, S. Konyagin, C. Pomerance and G. Yu, *Sieving by large integers and covering systems of congruences*, J. Amer. Math. Soc. **20** (2007), 495–517.

[GS] S. Guo and Z. W. Sun, *On odd covering systems with distinct moduli*, Adv. in Appl. Math. **35** (2005), 182–187.

[Gu] R. K. Guy, *Unsolved Problems in Number Theory*, Third edition, Springer, New York, 2004, Section A19, B21, F13.

[HS] H. Hu and Z. W. Sun, *An extension of Lucas' theorem*, Proc. Amer. Math. Soc. **129** (2001), 3471–3478.

[IR] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, Second edition, Grad. Texts in Math. 84, Springer, New York, 1990.

[LS] F. Luca and P. Stănică, *Fibonacci numbers that are not sums of two prime powers*, Proc. Amer. Math. Soc. **133** (2005), 1887–1890.

[R] P. Ribenboim, *The Little Book of Bigger Primes*, 2nd ed., Springer, New York, 2004.

[S92] Z. W. Sun, *Reduction of unknowns in Diophantine representations*, Sci. China Ser. A **35** (1992), no. 3, 257–269.

[S00] Z. W. Sun, *On integers not of the form $\pm p^a \pm q^b$*, Proc. Amer. Math. Soc. **128** (2000), 997–1002.

[SY] Z. W. Sun and S. M. Yang, *A note on integers of the form $2^n + cp$*, Proc. Edinburgh Math. Soc. **45** (2002), 155–160.

[W] B. M. M. de Weger, *Algorithms for Diophantine Equations*, CWI Tract, Vol. 65, Stichting Mathematisch Centrum, Centrum voor Wiskunde en Informatica, Amsterdam, 1989.

[Z] K. Zsigmondy, *Zur Theorie der Potenzreste*, Monatsh. Math. **3** (1892), 265–284.