NEW OBSERVATIONS ON PRIMITIVE ROOTS MODULO PRIMES

ZHI-WEI SUN

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

ABSTRACT. On the basis of our numerical computations, we make many new observations on primitive roots modulo primes. For example, we conjecture that for any odd prime p there is a primitive root $g < p$ modulo p which is the sum of the first n primes for some $n > 0$, and that for any prime $p > 3$ there is a prime $q < p$ with the Bernoulli number B_{q-1} a primitive root modulo p. We also make related observations on primitive prime divisors of many combinatorial sequences and quadratic nonresidues modulo primes. For example, based on heuristic arguments we conjecture that for any prime $p > 3$ there exists a Fibonacci number $F_k < p/2$ which is a quadratic nonresidue modulo p. This implies that there is a deterministic polynomial time algorithm to find square roots of quadratic residues modulo an odd prime p.

1. INTRODUCTION

Let p be any prime. It is well known that $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} = \{\bar{a} = a+p\mathbb{Z} : a \in \mathbb{Z}\}$ is a field and $\mathbb{F}_p^* = \mathbb{F}_p \setminus \{0\}$ is a cyclic group of order $p-1$. A rational p-adic integer g is called a *primitive root* modulo p if $\bar{g} = g \bmod p$ is a generator of $\mathbb{F}_p^*$. The standard proof of the existence of a primitive root modulo p (cf. [IR, p. 40]) is nonconstructive, and it provides no way to find an explicit primitive root modulo p.

The most famous unsolved problem on primitive roots modulo primes is the following conjecture posed by E. Artin in 1927 (see [M] for a survey of results towards Artin's conjecture).

Artin's Conjecture. *If $g \in \mathbb{Z}$ is neither -1 nor a square, then there are infinitely many primes p such that g is a primitive root modulo p.*

Let p be an odd prime. It is well known that the set

$$G(p) := \{g \in \{1, \ldots, p-1\} : g \text{ is a primitive root modulo } p\}| \qquad (1.1)$$

has cardinality $\varphi(p-1)$, where φ denotes Euler's totient function. According to [Gu, p. 377], P. Erdős ever asked the following open question.

Erdős' Problem. *Whether for any sufficiently large prime p there exists a prime $q < p$ which is a primitive root modulo p?*

Let $q > 1$ be a prime power. For the finite field $\mathbb{F}_q$ of order q, the multiplicative group $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$ is a cyclic group of order $q-1$ and any generator of this group is called a primitive root (or primitive element) of the field $\mathbb{F}_q$. In 1971 E. Vegh [V] guessed that if $q > 61$ then any element of $\mathbb{F}_q$ can be written as a difference of two primitive roots of $\mathbb{F}_q$. In 1984 S. W. Golomb [G] conjectured that any nonzero element of $\mathbb{F}_q$ can be expressed as a sum of two primitive roots of $\mathbb{F}_q$. After many earlier efforts to prove Vegh's and Golomb's conjectures and their linear extensions , it is now known that if $q > 61$ and $a, b, c \in \mathbb{F}_q^*$ then there always exist primitive roots g and h of $\mathbb{F}_q$ with $a = bg + ch$ (see the introduction part of the recent paper [COT]). In particular, this implies that for any prime $p > 61$ the set $G(p)$ defined in (1.1) contains two consecutive integers. In contrast, the twin prime conjecture still remains unsolved despite the recent breakthrough on prime gaps made by Y. Zhang [Z].

In 1989 W. B. Han [H] studied extensions of Vegh's and Golomb's conjectures to polynomials over finite fields. Using Weil's theorem on character sums, he established the following general theorem.

Theorem 1.1 (Han [H])**.** *Let $q > 1$ be a prime power. Let $f(x)$ and $g(x)$ be polynomials over the finite field $\mathbb{F}_q$ such that none of $g(x)$ and $f(x)g(x)^k$ ($k = 0, 1, 2, \dots$) can be written in the form $ch(x)^d$ with $c \in \mathbb{F}_q$, $1 < d \mid (q-1)$ and $h(x) \in \mathbb{F}_q[x]$. Let m be the number of distinct zeroes of $f(x)$ in the splitting field of $f(x)$, and let n be the number of distinct zeroes of $g(x)$ in the splitting field of $g(x)$. If $\sqrt{q} \geqslant (m + n - 1)4^{\omega(q-1)}$, then for some $a \in \mathbb{F}_q$ both $f(a)$ and $g(a)$ are primitive roots of $\mathbb{F}_q$, where $\omega(q-1)$ denotes the number of distinct prime divisors of $q - 1$.*

As a consequence of his theorem, Han noted that for any $a, b, c \in \mathbb{F}_q$ with $ac(b^2 - 4ac) \neq 0$, if $q \geqslant 2^{66}$ then there is a primitive root $g \in \mathbb{F}_q$ with $ag^2 + bg + c$ also a primitive root of $\mathbb{F}_q$ (cf. [H, Corollary 3]). In particular, for any prime $p > 2^{66}$ there is a primitive root g modulo p such that $g^2 + 1$ is also a primitive root modulo p. In contrast, it is unproven that there are infinitely many primes of the form $x^2 + 1$ with $x \in \mathbb{Z}$.

In view of Erdős' problem, Han's above work and various problems on primes of special forms, we are led to consider whether primitive roots modulo primes can take certain special forms. In Section 3 we will pose various conjectures in this direction based on our computation checks. Since any primitive root modulo an odd prime p must be a quadratic nonresidue modulo p, in Section 2 we will investigate quadratic nonresidues modulo primes of certain special forms armed with heuristic arguments.

Let $(a_n)_{n \geqslant 1}$ be a sequence of integers. If no term of the sequence $(a_n)_{n \geqslant 1}$ has a prime divisor greater than a given number N, then we should not expect that the sequence contains quadratic nonresidues modulo any sufficiently large prime p. If a prime p divides the n-th term a_n but it does not divide any previous term a_k with $0 < k < n$, then p is called a *primitive prime divisor* of the term a_n. For our purposes, we are interested in those sequences with infinitely many terms having primitive prime divisors.

In 1886 A. S. Bang [B] proved that for any integer $n > 1$ with $n \neq 6$ the number $2^n - 1$ has a prime divisor not dividing any $2^k - 1$ with $k \in \{1, \dots, n-1\}$. In 1892 K. Zsigmondy [Zs] extended this as follows: If a and b are relatively positive integers with $a > b$, then for any integer $n > 2$ the number $a^n - b^n$ has a prime divisor not dividing any $a^k - b^k$ with $0 < k < n$ except for the case $a = 2$, $b = 1$ and $n = 6$.

Recall that the Fibonacci numbers are given by

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

Carmichael's theorem (cf. [C]) asserts that for any integer $n > 12$ the n-th Fibonacci number F_n has a prime divisor p which does not divide any previous Fibonacci number F_k with $0 < k < n$. For $A, B \in \mathbb{Z}$ with $B \neq 0$ and $A^2 \neq 4B$, the Lucas sequence $u_n = u_n(A, B)$ $(n = 0, 1, 2, \dots)$ is defined by

$$u_0 = 0, \ u_1 = 1, \ \text{and} \ u_{n+1} = Au_n - Bu_{n-1} \ \text{for} \ n = 1, 2, 3, \dots.$$

In 2001 Y. Bilu, G. Hanrot and P. M. Voutier [BHV] finally proved that for any integer $n > 30$ the term $u_n(A, B)$ has prime divisor not dividing any previous term $u_k(A, B)$ with $0 < k < n$.

In Section 4 we look at various combinatorial sequences of integers or rationals to see whether larger terms have primitive prime divisors. This leads us to generate some tables on primitive prime divisors and formulate various conjectures in this direction.

Throughout this paper, we set $\mathbb{N} = \{0, 1, 2, \dots\}$ and $\mathbb{Z}^+ = \{1, 2, 3, \dots\}$.

2. ON FIBONACCI QUADRATIC RESIDUES MODULO PRIMES

Let p be an odd prime and a be any quadratic residue modulo p. How to solve the congruence $x^2 \equiv a \pmod{p}$ quickly? By the Tonelli-Shanks Algorithm (cf. R. Crandall and C. Pomerance [CP, pp. 93-95]), if we know a quadratic nonresidue $d \in \mathbb{Z}$ modulo p then one can solve $x^2 \equiv a \pmod{p}$ efficiently as follows:

Write $p - 1 = 2^s t$ with $s, t \in \mathbb{Z}^+$ and $2 \nmid t$, and find even integers $m_1, \dots, m_s$ with $(ad^{m_i})^{2^{s-i}t} \equiv 1 \pmod{p}$ for all $i = 1, \dots, s$ in the following way: $m_1 := 0$, and after those $m_1, \dots, m_i$ (with $1 \leqslant i < s$) have been chosen we select $m_{i+1} \in \{m_i, m_i + 2^i\}$ such that $(ad^{m_{i+1}})^{2^{s-i-1}t} \equiv 1 \pmod{p}$. Note

that $((ad^{m_i})^{2^{s-i-1}t})^2 \equiv 1 \pmod{p}$ and hence $(ad^{m_i})^{2^{s-i-1}t} \equiv \pm 1 \pmod{p}$. If $(ad^{m_i})^{2^{s-i-1}t} \equiv -1 \pmod{p}$, then

$$(ad^{m_i+2^i})^{2^{s-1-i}t} \equiv -d^{2^{s-1}t} = -d^{(p-1)/2} \equiv 1 \pmod{p}.$$

As $(ad^{m_s})^t \equiv 1 \pmod{p}$, we have $x^2 \equiv a \pmod{p}$ with $x = \pm a^{(t+1)/2}(d^t)^{m_s/2}$.

However, there is no known deterministic, polynomial time algorithm for finding a quadratic nonresidue d modulo the odd prime p. According to [CP, pp. 93-95], under the Extended Riemann Hypothesis for algebraic fields, it can be shown that there is a positive quadratic nonresidue $d < 2\log^2 p$; and so an exhaustive search to this limit succeeds in finding a quadratic nonresidue in polynomial time. Thus, on the ERH, one can find square roots for quadratic residues modulo the prime p in deterministic, polynomial time.

As Fibonacci numbers grow exponentially, part (i) of our following conjecture is particularly interesting since it implies that we can find square roots for quadratic residues modulo any odd prime p in deterministic, polynomial time.

Conjecture 2.1. (i) *For any integer $n > 4$, there is a Fibonacci number $f < n/2$ with $x^2 \equiv f \pmod{n}$ for no integer x.*

(ii) *For any odd prime p, let $f(p)$ be the least Fibonacci number with $(\frac{f(p)}{p}) = -1$. Then $f(p) = o(p^{0.7})$ as $p \to \infty$. Moreover, we have $f(p) = O(p^c)$ for any $c > c_0 = \log_2 \frac{1+\sqrt{5}}{2} \approx 0.694$.*

(iii) *For any prime p, there exists a positive integer $k \leqslant \sqrt{p+2}+2$ such that $F_k + 1$ is a primitive root modulo p.*

Conjecture 2.1(i) can be reduced to the case when n is prime. In fact, if $n = 3$ or $4 \mid n$, then no square is congruent to $F_3 = 2$ modulo n. If $n > 4$ has an odd prime divisor p, and there is a positive Fibonacci number $F_k < p$ with $x^2 \not\equiv F_k \pmod{p}$ for all $x \in \mathbb{Z}$, then $F_k < p \leqslant n/2$ and also $x^2 \not\equiv F_k \pmod{n}$ for all $x \in \mathbb{Z}$. We have verified part (i) for all primes p with $3 < p < 3 \times 10^9$. For data and graphs related to Conjecture 2.1(i), one may consult [S, A241568, A241604 and A241675].

As for part (ii) of Conjecture 2.1, we don't have a rigorous proof but it seems reasonable in view of the following heuristic arguments.

Heuristic Arguments for Conjecture 2.1(ii). In light of Carmichael's theorem on primitive prime divisors of Fibonacci numbers, we may think that a positive Fibonacci number not exceeding p^c is a quadratic residue modulo p with 'probability' $1/2$. Roughly speaking, there are about

$$\frac{\log_2 p^c}{\log_2 \frac{1+\sqrt{5}}{2}} = \frac{c}{c_0} \log_2 p$$

positive Fibonacci numbers not exceeding p^c. So we might expect that all positive Fibonacci numbers not exceeding p^c are quadratic residues modulo p

with probability

$$\left(\frac{1}{2}\right)^{(\log_2 p)c/c_0} = \frac{1}{p^{c/c_0}}.$$

As $\sum_p p^{-c/c_0}$ converges, it seems reasonable to think that there are finitely many primes p for which all positive Fibonacci numbers not exceeding p^c are quadratic residues modulo p. So the guess $f(p) = O(p^c)$ probably holds.

We have verified Conjecture 2.1(iii) for all primes $p < 5 \times 10^6$, and observed that no Fibonacci number is a primitive root modulo the prime 3001. Note that for any integer $n > 1$ there is a Fibonacci number F_k with $F_k + 1 \equiv 0 \pmod{n}$. In fact, by the Pigeonhole Principle, there are $0 \leqslant i < j \leqslant n^2$ such that $F_i \equiv F_j$ $\pmod{n}$ and $F_{i+1} \equiv F_{j+1} \pmod{n}$, and hence $F_{j-i} \equiv F_0 = 0 \pmod{n}$ and $F_{j-i+1} \equiv F_1 = 1 \pmod{n}$. Clearly $k = j - i - 2 > 0$ since $F_1 = F_2 = 1 \not\equiv 0$ $\pmod{n}$, and

$$F_k = F_{k+2} - (F_{k+3} - F_{k+2}) = 2F_{k+2} - F_{k+3} = 2F_{j-i} - F_{j-i+1} \equiv -1 \pmod{n}.$$

Recall that the Lucas numbers $L_0, L_1, L_2, \ldots$ are defined by

$$L_0 = 2, \ L_1 = 1, \ \text{and} \ L_{n+1} = L_n + L_{n-1} \ (n = 1, 2, 3, \ldots).$$

It is well known that

$$L_n = \left(\frac{1 + \sqrt{5}}{2}\right)^n + \left(\frac{1 - \sqrt{5}}{2}\right)^n \quad \text{for all } n \in \mathbb{N}.$$

Our following conjecture is similar to Conjecture 2.1.

Conjecture 2.2. (i) *For any integer $n > 2$, there is a Lucas number $L_k < n$ such that $x^2 \not\equiv L_k \pmod{n}$ for all $x \in \mathbb{Z}$.*

(ii) *For any odd prime p, let $\ell(p)$ be the least Lucas number with $(\frac{\ell(p)}{p}) = -1$. Then $\ell(p) = o(p^{0.7})$ as $p \to \infty$. Moreover, we have $\ell(p) = O(p^c)$ for any $c > \log_2 \frac{1+\sqrt{5}}{2} \approx 0.694$.*

(iii) *For any prime p, there exists a positive integer $k < \sqrt{p} + 2$ such that $L_k + 1$ is a primitive root modulo p.*

We have verified Conjecture 2.2(iii) for all primes $p < 10^7$. Note that no Lucas number is a primitive root modulo the prime 28657. Also, for any integer $n > 1$ there is a positive integer $j < n^2$ such that $L_j \equiv L_0 = 2 \pmod{n}$ and $L_{j+1} \equiv L_1 = 1 \pmod{n}$, and hence $L_{j-1} = L_{j+1} - L_j \equiv 1 - 2 = -1 \pmod{n}$.

The following conjecture similar to Conjectures 2.1 and 2.2 is concerned with cubic nonresidues modulo primes. For a prime $p \equiv 1 \pmod{3}$, it seems reasonable to think that $2^k - 1$ is a cubic nonresidue modulo p with probability $2/3 = 1/1.5$.

Conjecture 2.3. *Let p be any prime with $p \equiv 1$ (mod 3). Then, there is a positive integer k with $2^k - 1 < p/2$ such that $2^k - 1$ is a cubic nonresidue modulo p. Moreover, for any $c > \log 1.5 / \log 2 \approx 0.585$ we have $s(p) = O(p^c)$, where $s(p)$ denotes the least positive cubic nonresidue modulo p in the form $2^k - 1$ with $k \in \mathbb{Z}^+$.*

We have verified the first assertion in Conjecture 2.3 for all primes below 5×10^6; for example, the least positive cubic nonresidue modulo the prime $p = 4667629$ in the form $2^k - 1$ is $2^{15} - 1 = 32767$. The second assertion in Conjecture 2.3 sounds reasonable by heuristic arguments.

To conclude this section, we pose one more conjecture.

Conjecture 2.4. *For each prime $p > 5$, there exists a prime $q < p$ such that $2^q + 1$ is a quadratic nonresidue modulo p.*

Note that for the prime $p = 2089$ there is no prime $q < p$ with $2^q + 1$ a primitive root modulo p. We have verified Conjecture 2.4 for all primes p with $5 < p < 10^8$; see [S, A235712] for related data and graphs.

3. ON PRIMITIVE ROOTS OF SPECIAL FORMS

As we mentioned in Section 1, it is known that for any sufficiently large prime p there is a primitive root modulo p in the form $x^2 + 1$ with $x \in \mathbb{Z}$. Part (i) of our following conjecture is stronger than this.

Conjecture 3.1. (i) *Every prime p has a primitive root $g < p$ modulo p of the form $k^2 + 1$. In other words, for any prime p, there is a primitive root $0 < g < p$ modulo p with $g - 1$ a square.*

(ii) *For any prime $p > 3$, there is a triangular number $g < p$ which is a primitive root modulo p. Also, every prime $p > 11$ has a primitive root $g < p$ modulo p which is a product of two consecutive integers.*

Remark 3.1. We have verified Conjecture 3.1(i) for all primes below 10^7. For data and graphs concerning Conjecture 3.1, one may consult [S, A239957, A241476, A239963 and A241492].

Table 3.1: Primes p with unique primitive root g of the form $k^2 + 1 < p$

p	2	3	5	7	11	13	31	71	79	151
k	1	1	1	2	1	1	4	8	6	9
$g = k^2 + 1$	2	2	2	5	2	2	17	65	37	82

In 2000 D.K.L. Shiu [Sh] proved that if a and $m > 0$ are relatively prime then for any positive integer k there is a positive integer n such that $p_{n+1} \equiv p_{n+2} \equiv \ldots \equiv p_{n+k} \equiv a$ (mod m), where p_j denotes the j-th prime. This remarkable

result implies that the set $\{S_n = \sum_{k=1}^n p_k : n = 1, 2, 3, \ldots\}$ contains a complete system of residues modulo any positive integer m. In [S13a] the author conjectured that the set $\{s_n = \sum_{k=1}^n (-1)^{n-k} p_k : n = 1, 2, 3, \ldots\}$ also contains a complete system of residues modulo any positive integer m. Motivated by these we pose the following conjecture.

Conjecture 3.2. (i) *For any odd prime p, there is a primitive root $g < p$ modulo p in the form $S_n = \sum_{k=1}^n p_k$ with $n \in \mathbb{Z}^+$.*

(ii) *For any integer $n > 1$, there is a number $k \in \{1, \ldots, n\}$ such that $s_k = \sum_{j=1}^k (-1)^{k-j} p_j$ is a primitive root modulo p_n.*

Remark 3.2. We have verified part (i) for all odd primes $p < 10^7$, and part (ii) for all $n = 2, \ldots, 250000$. See [S, A242266 and A242277] for related data and graphs.

Table 3.2: Primes p with unique primitive root g of the form $\sum_{k=1}^n p_k < p$

p	3	5	7	11	13	31	71	127	241
n	1	1	2	1	1	4	5	7	10
$g = \sum_{k=1}^n p_k$	2	2	5	2	2	17	28	58	129

Conjecture 3.3. (i) *For any prime $p > 3$, there exists a prime $q < p/2$ such that the Mersenne number $M_q = 2^q - 1$ is a primitive root modulo p.*

(ii) *For any prime $p > 7$, there exists a prime $q < p/2$ such that $q!$ is a primitive root modulo p.*

(iii) *For any prime $p > 3$, there exists a positive integer $g < p$ such that g, $2^g - 1$ and $(g-1)!$ are all primitive roots modulo p.*

Remark 3.3. (a) We have verified Conjecture 3.3(i) for all primes $p < 10^7$; see [S, A236966] for related data and graphs. For each prime p with $3 < p < 10^7$, the least prime $q < p/2$ with $2^q - 1$ a primitive root modulo p is at most 193. For the prime $p = 5336101$, the least prime $q < p/2$ with $2^q - 1$ a primitive root modulo p is 193. For related data and graphs concerning Conjecture 3.3(ii) 1.3, one may visit [S, A237112].

(b) Conjecture 3.3(iii) is very strong! We have verified it for all primes below 10^6; see [S, A242248 and A242250] for related data and graphs.

Table 3.3: Primes p with unique $0 < g < p$ such that
g, $2^g - 1$ and $(g-1)!$ are all primitive roots mod p

p	5	7	11	13	19	23	31	43	67	79
g	3	5	8	11	13	21	12	34	41	53
$2^g - 1 \bmod p$	2	3	2	6	2	11	3	20	11	30
$(g-1)! \bmod p$	2	3	2	6	10	11	22	29	44	47

The following conjecture is much stronger than Erdős' Problem mentioned in Section 1.

Conjecture 3.4. *For any odd prime p, there exists a prime $q < p$ such that both q and $2^q - q$ are primitive roots modulo p.*

Remark 3.4. We have verified this conjecture for all odd primes below 10^6; see [S, A242345] for related data and graphs.

Table 3.4: Primes p with unique prime $q < p$ such that
both q and $2^q - q$ are primitive roots modulo p

p	$q < p$	$2^q - q \bmod p$
3	2	2
5	2	2
7	3	5
11	2	2
13	2	2
19	2	2
23	19	7
29	2	2
31	11	22
43	3	5
61	2	2
71	67	13
73	31	58
79	59	29
97	71	74
127	43	86
151	71	14

Recall that the Bernoulli numbers $B_0, B_1, B_2, \ldots$ are rational numbers defined by

$$B_0 = 1 \quad \text{and} \quad \sum_{k=0}^{n} \binom{n+1}{k} B_k = 0 \ \text{ for all } n = 1, 2, 3, \ldots,$$

and the Euler numbers $E_0, E_1, E_2, \ldots$ are integers defined by

$$E_0 = 1 \quad \text{and} \quad \sum_{\substack{k=0 \\ 2 \mid n-k}}^{n} \binom{n}{k} E_k = 0 \ \text{ for all } n = 1, 2, 3, \ldots.$$

It is well known that $B_{2n+1} = E_{2n-1} = 0$ for all $n = 1, 2, 3, \ldots$. For any prime $p > 3$ it is well known that all the Bernoulli numbers

$$B_{2k} \quad \left(k = 1, \ldots, \frac{p-3}{2} \right)$$

are p-adic integers (this follows from the recurrence for Bernoulli numbers or Kummer's theorem on Bernoulli numbers.

Conjecture 3.5. (i) *For any prime $p > 3$, there exists a prime $q < p$ such that the Bernoulli number B_{q-1} is a primitive root modulo p.*

(ii) *For any prime $p > 13$, there exists a prime $q < p$ such that the Euler number E_{q-1} is a primitive root modulo p.*

Remark 3.5. We have verified part (i) for all primes p with $3 < p < 6 \times 10^6$; see [S, A242210 and A242213] for related data and graphs. We have also checked part (ii) for all primes p with $13 < p < 10^6$.

<div align="center">

Table 3.5: Primes p with unique prime $q < p$ such that
B_{q-1} is a primitive root modulo p

</div>

p	5	11	19
$q < p$	2	3	17
B_{q-1}	$-1/2$	$1/6$	$-3617/510$
$B_{q-1} \bmod p$	2	2	15

Recall that those rational numbers $H_n = \sum_{0 < k \leqslant n} 1/k$ $(n = 0, 1, 2, \ldots)$ are called harmonic numbers. The second-order harmonic numbers are those rationals $H_n^{(2)} = \sum_{0 < k \leqslant n} 1/k^2$ with $n \in \mathbb{N}$.

Conjecture 3.6. *Let $p > 5$ be a prime.*

(i) *There exists a prime $q \leqslant (p+1)/2$ such that H_{q-1} is a primitive root modulo p.*

(ii) *There exists a prime $q \leqslant (p-1)/2$ such that $H_{q-1}^{(2)}$ is a primitive root modulo p.*

Conjecture 3.7. (i) *For any prime $p > 3$, there exists a prime $q < p/2$ such that the Catalan number $C_q = \binom{2q}{q}/(q+1)$ is a primitive root modulo p.*

(ii) *For any prime $p > 3$, there exists a prime $q < p/2$ such that the Bell number b_q is a primitive root modulo p, where b_q denotes the number of ways to partition a set of cardinality q.*

(iii) *For any prime $p > 3$, there exists a prime $q < p/2$ such that the Franel number $f_q = \sum_{k=0}^{q} \binom{q}{k}^3$ is a primitive root modulo p.*

Remark 3.7. For related data and graphs concerning parts (i)-(ii) of Conjecture 3.7, one may visit [S, A236308 and A237594].

4. Primitive prime divisors of some combinatorial sequences

Conjecture 4.1. *For any integer $n > 1$ with $n \neq 5, 16$, the number $2^n - n$ has a prime divisor p not dividing any $2^k - k$ with $0 < k < n$.*

Remark 4.1. See [S, 242292] for related data.

Conjecture 4.2. *For any integer $n > 4$, there is a prime p for which $B_{2n} \equiv 0$ (mod p) but $B_{2k} \not\equiv 0$ (mod p) for all $0 < k < n$. Also, for any integer $n > 1$, the Euler number E_{2n} has a prime divisor p which does not divide any E_{2k} with $0 < k < n$.*

Remark 4.2. For related numerical data, one may see [S, A242193 and A242194]. In Table 4.1, $p_B(n)$ denotes the least prime p for which $B_{2n} \equiv 0$ (mod p) but $B_{2k} \not\equiv 0$ (mod p) for all $0 < k < n$, similarly $p_E(n)$ represents the least prime divisor of p_{2n} which does not divide any E_{2k} with $0 < k < n$.

Conjecture 4.3. (i) *For any integer $n > 1$ with $n \neq 7$, there is a prime p for which $H_n \equiv 0$ (mod p) but $H_k \not\equiv 0$ (mod p) for all $0 < k < n$.*

(ii) *For any integer $n > 1$, there is a prime p for which $H_n^{(2)} \equiv 0$ (mod p) but $H_k^{(2)} \not\equiv 0$ (mod p) for all $0 < k < n$.*

Remark 4.3. For related numerical data, see [S, A242223 and A242241]. In Table 4.2, $p_H(n)$ denotes the least prime p for which $H_n \equiv 0$ (mod p) but $H_k \not\equiv 0$ (mod p) for all $0 < k < n$, and $p_H^{(2)}(n)$ represents the least prime p for which $H_n^{(2)} \equiv 0$ (mod p) but $H_k^{(2)} \not\equiv 0$ (mod p) for all $0 < k < n$.

Conjecture 4.4. *For the sequence $\{f_n\}_{n \geqslant 1}$ of Franel numbers, each term f_n with $n \in \mathbb{Z}^+$ has a primitive prime divisor. For the sequence $\{f_n^{(4)}\}_{n \geqslant 1}$ of the fourth-order Franel numbers with $f_n^{(4)} = \sum_{k=0}^n \binom{n}{k}^4$, each term $f_n^{(4)}$ with $n \in \mathbb{Z}^+$ has a primitive prime divisor. In general, for any integer $r > 2$, if $n \in \mathbb{Z}^+$ is large enough then $f_n^{(r)} = \sum_{k=0}^n \binom{n}{k}^r$ has a prime divisor p not dividing any $f_k^{(r)}$ with $0 < k < n$.*

For each $n \in \mathbb{N}$ the central trinomial coefficient

$$T_n = \sum_{k=0}^{\lfloor n/2 \rfloor} \binom{n}{2k}\binom{2k}{k}$$

is the coefficient of x^n in the expansion of $(x^2 + x + 1)^n$.

Conjecture 4.5. *For the sequence $\{T_n\}_{n \geqslant 1}$ of central trinomial coefficients, each term T_n with $n > 1$ has a primitive prime divisor.*

We have many other conjectures similar to Conjectures 4.1-4.5.

Table 4.1: Least primitive divisors $p_B(n)$ of B_{2n} and $p_E(n)$ of E_{2n}

n	$p_B(n)$	$p_E(n)$
2		5
3		61
4		277
5	5	19
6	691	13
7	7	47
8	3617	17
9	43867	79
10	283	41737
11	11	31
12	103	2137
13	13	67
14	9349	29
15	1721	15669721
16	37	930157
17	17	4153
18	26315271553053477373	37
19	19	23489580527043108252017828576198947741
20	137616929	41
21	15200976439180708002691	137
22	59	587
23	23	285528427091
24	653	55169942493832960712141952424224824922864606733697
25	417202699	5639
26	577	53
27	39409	2749
28	113161	5303
29	29	145987947677124734796103144500103
30	2003	6821509
31	31	101
32	1226592271	25349

ZHI-WEI SUN

Table 4.2: Least primitive divisors $p_H(n)$ of H_n and $p_{H^{(2)}}(n)$ of $H_n^{(2)}$

n	$p_H(n)$	$p_{H^{(2)}}(n)$
2	3	5
3	11	7
4	5	41
5	137	11
6	7	13
7		266681
8	761	17
9	7129	19
10	61	178939
11	97	23
12	13	18500393
13	29	40799043101
14	1049	29
15	41233	31
16	17	619
17	37	601
18	19	8821
19	7440427	86364397717734821
20	11167027	421950627598601
21	18858053	2621
22	23	295831
23	583859	47
24	577	2237
25	109	157
26	34395742267	53
27	521	307
28	375035183	7741
29	4990290163	6823
30	31	61
31	2667653736673	205883
32	2917	487

References

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

[BHV] Y. Bilu, G. Hanrot and P. M. Voutier, *Existence of primitive divisors of Lucas and Lehmer numbers*, J. Reine Angew. Math. **539** (2001), 75–122.

[C]   R. D. Carmichael, *On the numerical factors of the arithmetic forms $\alpha^n + \beta^n$*, Annals of Math. **15** (1913), 30–70.

[COT] S. D. Cohen, T. Oliveira e Silva and T. Trudgian, *A proof of the conjecture of Cohen and Mullen on sums of primitive roots*, Math. Com., to appear. `arXiv:1402.2724`.

[CP]   R. Crandall and C. Pomerance, *Prime Numbers: A Computational Perspective*, Springer, New York, 2001.

[G]   S. W. Golomb, *Algebraic constructions for Costas arrays*, J. Combin. Theory Ser. A **37** (1984), 13–21.

[Gu]   R. K. Guy, *Unsolved Problems in Number Theory* (3rd, ed.), Springer, 2004.

[H]   W. B. Han, *Polynomials and primitive roots over finite fields*, Acta Math. Sinica **32** (1989), no. 1, 110–117.

[IR]   K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory (2nd Edition), Grad. Texts in Math. 84,*, Springer, New York, 1990.

[M]   R. Murthy, *Artin's conjecture for primitive roots*, Math. Intelligencer **10** (1988), 59–67.

[Sh]   D. K. L. Shiu, *Strings of congruent primes*, J. London Math. Soc. **61** (2000), 359–373.

[S]   Z.-W. Sun, Sequences A235712, A236308, A236966, A237112, A237594, A239957, A239963, A241476, A241492 A241568, A241604, A241675, A242193, A242194, A242210, A242213, A242222, A242223, A242266, A242277 in OEIS (On-Line Encyclopedia of Integer Sequences), `http://oeis.org`.

[S13a] Z.-W. Sun, *On functions taking only prime values*, J. Number Theory **133** (2013), 2794–2812.

[S13b] Z.-W. Sun, *Some new problems in additive combinatorics*, preprint, `arXiv:1309.1679`.

[S14]   Z.-W. Sun, *Problems on combinatorial properties of primes*, preprint, `arXiv:1402.6641`.

[V]   E. Vegh, *A note on the distribution of the primitive roots of a prime*, J. Number Theory **3** (1971), 13–18.

[Z]   Y. Zhang, *Bounded gaps between primes*, Annals of Math. **179** (2014), 1121–1174.

[Zs]   K. Zsigmondy, *Zur Theorie der Potenzrest*, J. Monatsh. Math. **3** (1892), 265-C284.