Nanjing Univ. J. Math. Biquarterly 36 (2019), no. 2, 108-133.

NEW OBSERVATIONS ON PRIMITIVE ROOTS MODULO PRIMES

ZHI-WEI SUN

Abstract. We make many new observations on primitive roots modulo primes. For an odd prime p and an integer c, we establish a theorem concerning $\sum_g(\frac{g+c}{p})$, where g runs over all the primitive roots modulo p among $1,\ldots,p-1$, and $(\frac{\cdot}{p})$ denotes the Legendre symbol. On the basis of our numerical computations, we formulate 35 conjectures involving primitive roots modulo primes. For example, we conjecture that for any prime p there is a primitive root $g<p$ modulo p with $g-1$ a square, 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 quadratic nonresidues modulo primes and primitive prime divisors of some combinatorial sequences. 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 a prime $p>3$.

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. [12, 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 [13] 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.*

2010 *Mathematics Subject Classification.* Primary 11A07, 11A41; Secondary 11A15, 11B39, 11B68, 11L40, 11T99.

Keywords: Primitive root modulo a prime, finite field, quadratic residue, combinatorial sequence, primitive prime divisor.

Supported by the National Natural Science Foundation (grant 11571162) of China.

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

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

has cardinality $\varphi(p-1)$, where φ denotes Euler's totient function. According to [10, p. 377], P. Erdös 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 [19] 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 [8] 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 [6]). 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 Y. Zhang's breakthrough (cf. [20]) on prime gaps.

In 1989 W. B. Han [11] 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 [11]) *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 $f(x)g(x)^k$ $(k = 0, 1, 2, \ldots)$ can be written in the form $cP(x)^d$ with $c \in \mathbb{F}_q$, $1 < d \mid (q-1)$ and $P(x) \in \mathbb{F}_q[x]$. 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 $\omega(q-1)$ the number of distinct prime divisors of $q-1$.*

As a consequence of Theorem 1.1, Han noted that for any finite field $\mathbb{F}_q$ with $q \geqslant 2^{66}$, if $a, b, c \in \mathbb{F}_q$ and $ac(b^2 - 4ac) \neq 0$, 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. [11, 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 $x \in \mathbb{Z}$.

On Oct. 3, 2013, the author [16, A229910] conjectured that for any prime $p > 13$ there is a primitive root g modulo p such that $g + g^{-1}$ is also a primitive root modulo p. Based on Han's work, the author showed in Oct. 2013 (cf. [16, A229910]) that for each $\varepsilon \in \{\pm 1\}$ and for any finite field $\mathbb{F}_q$ with $q > 2^{66}$, there is a primitive element g of $\mathbb{F}_q$ such that $g + \varepsilon g^{-1}$ is also a primitive root of $\mathbb{F}_q$.

In 2018, S.D. Cohen, T. Oliveira e Silva and Sutherland [5] obtained the following further result.

Theorem 1.2. ([5, Corollary 2]) *Let $q > 5$ be a prime power.*

(i) *If $q \notin \{7, 9, 13, 25, 121\}$, then there is a primitive element g of $\mathbb{F}_q$ with $g + g^{-1}$ also primitive.*

(ii) *If $q \notin \{9, 13, 25, 61, 121\}$, then there is a primitive element g of $\mathbb{F}_q$ with $g - g^{-1}$ also primitive.*

For any odd prime p and integer c, we introduce

$$S_p(c) := \sum_{g\in G(p)} \left(\frac{g+c}{p}\right), \tag{1.2}$$

where $(\frac{\cdot}{p})$ denotes the Legendre symbol. Note that if $p \mid c$ then $S_p(c) = -|G(p)| = -\varphi(p-1)$. Concerning $S_p(c)$ we have the following result.

Theorem 1.3. *Let p be any odd prime.*

(i) *We have*

$$S_p(1) = 0. \tag{1.3}$$

(ii) *For any integer $c \in \mathbb{Z}$ with $c \not\equiv 0 \pmod p$, we have*

$$S_p(c) \equiv \left(\frac{c}{p}\right) \sum_{k=0}^{(p-1)/2} \frac{\binom{2k}{k}}{(-4c)^k} \mu\left(\frac{p-1}{(k,p-1)}\right) \frac{\varphi(p-1)}{\varphi((p-1)/(k,p-1))} \pmod p, \tag{1.4}$$

where μ is the Möbius function and $(k, p-1)$ is the greatest common divisor of k and $p-1$.

Proof. (i) For $g \in \{1, \ldots, p-1\}$ let $g^* \in \{1, \ldots, p-1\}$ be the inverse of g modulo p (i.e., $gg^* \equiv 1 \pmod p$). Clearly,

$$S_p(1) = \sum_{g\in G(p)} \left(\frac{g^*+1}{p}\right) = -\sum_{g\in G(p)} \left(\frac{g(g^*+1)}{p}\right) = -\sum_{g\in G(p)} \left(\frac{1+g}{p}\right) = -S_p(1)$$

and thus $S_p(1) = 0$.

(ii) Now let $c\in\mathbb{Z}$ with $c\not\equiv 0 \pmod p$. Observe that

$$\begin{aligned}\sum_{g\in G(p)}(g+c)^{(p-1)/2}&=\sum_{g\in G(p)}\sum_{k=0}^{(p-1)/2}\binom{(p-1)/2}{k}g^kc^{(p-1)/2-k}\\&=\sum_{k=0}^{(p-1)/2}\binom{(p-1)/2}{k}c^{(p-1)/2-k}\sum_{g\in G(p)}g^k\\&\equiv\left(\frac{c}{p}\right)\sum_{k=0}^{(p-1)/2}\frac{\binom{-1/2}{k}}{c^k}\sum_{g\in G(p)}g^k\\&=\left(\frac{c}{p}\right)\sum_{k=0}^{(p-1)/2}\frac{\binom{2k}{k}}{(-4c)^k}\sum_{g\in G(p)}g^k \pmod p.\end{aligned}$$

Fix a primitive root g_0 modulo p. Then

$$\sum_{g\in G(p)}g^k\equiv\sum_{\substack{j=1\\(j,p-1)=1}}^{p-1}g_0^{jk}\equiv\varphi(p-1)\frac{\mu((p-1)/(k,p-1))}{\varphi((p-1)/(k,p-1))} \pmod p$$

via the known evaluations of Ramanujan sums. Therefore the desired (1.4) follows.

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

Corollary 1.1. (i) *For any prime* $p\equiv 1 \pmod 4$, *we have* $S_p(-c)=S_p(c)$ *for all* $c\in\mathbb{Z}$, *in particular* $S_p(-1)=S_p(1)=0$.

(ii) *Let* p *be a Fermat prime and let* $c\in\mathbb{Z}$ *with* $c\not\equiv 0 \pmod p$. *Then*

$$S_p(c)=\frac{1-(\frac{c}{p})}{2}. \tag{1.5}$$

Proof. (i) We now prove the first part. Let $c\in\mathbb{Z}$. If $p\mid c$, then $S_p(-c)=S_p(0)=S_p(c)$.

Now we assume $p\nmid c$. If k is odd, then $(p-1)/(k,p-1)\equiv 0 \pmod 4$ and hence $\mu((p-1)/(k,p-1))=0$. If k is even, then $(-c)^k=c^k$. So, by (1.4) we have $S_p(-c)\equiv S_p(c) \pmod p$. Since

$$|S_p(\pm c)|\leqslant|G(p)|=\varphi(p-1)\leqslant\frac{p-1}{2},$$

we must have $S_p(-c)=S_p(c)$. In particular, $S_p(-1)=S_p(1)=0$ with the aid of (1.3).

(ii) Now we turn to show the second part of Corollary 1.1. Write $p=2^n+1$ with n a power of two. For any positive integer $k<(p-1)/2=2^{n-1}$, we have $(k,p-1)\mid 2^{n-2}$ and hence $\mu((p-1)/(k,p-1))=0$ since $(p-1)/(k,p-1)$ is divisible by 4. Thus, by

(1.4) we have

$$\begin{aligned}\left(\frac{c}{p}\right)S_p(c) \equiv&\varphi(p-1)+\frac{\binom{p-1}{(p-1)/2}}{(-4c)^{(p-1)/2}}\mu(2)\frac{\varphi(p-1)}{\varphi(2)}\\ \equiv&\varphi(p-1)\left(1-\left(\frac{c}{p}\right)\right)=\frac{p-1}{2}\left(1-\left(\frac{c}{p}\right)\right)\equiv\frac{(\frac{c}{p})-1}{2}\pmod p.\end{aligned}$$

Note that $|S_p(c)| \leqslant \varphi(p-1) = (p-1)/2$. Therefore (1.5) holds. □

In view of Erdős' problem, Theorems 1.1-1.2 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 computational 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. In Section 4, we will pose some other conjectures involving primitive roots modulo primes.

Let $(a_n)_{n\geqslant1}$ be a sequence of integers. If no term of the sequence $(a_n)_{n\geqslant1}$ has a prime divisor greater than a given integer $N>1$, then for any prime $q\equiv 1 \pmod{4\prod_{p\leqslant N}p}$ we have $(\frac{a_n}{q})=1$ for all $n=1,2,3,\ldots$. 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 integer sequences with infinitely many terms having primitive prime divisors.

In 1886 A. S. Bang [1] 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 $k\in\{1,\ldots,n-1\}$. In 1892 K. Zsigmondy [21] extended this as follows: If a and b are integers with $a>b>0$ and $(a,b)=1$, then for any integer $n>2$ the number a^n-b^n has a prime divisor not dividing any a^k-b^k with $0<k<n$, unless $a=2$, $b=1$ and $n=6$.

Recall that the Fibonacci numbers are given by

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

Carmichael's theorem (cf. [4]) 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 $0<k<n$. Let $A,B\in\mathbb{Z}$ with $B\neq0$ and $A^2\neq 4B$. The Lucas sequence $u_n=u_n(A,B)$ $(n=0,1,2,\ldots)$ is defined by

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

In 2001 Y. Bilu, G. Hanrot and P. M. Voutier [2] 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 5 we look at various combinatorial sequences of integers or rational numbers 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 $\mathbb{N}=\{0,1,2,\ldots\}$ and $\mathbb{Z}^+=\{1,2,3,\ldots\}$.

2 On Special Quadratic Nonresidues Modulo Primes

Let a be a quadratic residue modulo an odd prime p. How to solve the congruence $x^2 \equiv a \pmod p$ efficiently? By the Tonelli-Shanks Algorithm (cf. R. Crandall and C. Pomerance [7, 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 $m_1, \ldots, m_s$ with $(ad^{m_i})^{2^{s-i}t} \equiv 1 \pmod p$ for all $i = 1, \ldots, s$ in the following way: $m_1 := 0$, and after those $m_1, \ldots, m_i$ (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

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

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 a given odd prime p. According to [7, 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, under the ERH, one can find square roots for quadratic residues modulo the prime p in deterministic, polynomial time.

As the 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 a prime $p > 3$ in deterministic polynomial time.

Conjecture 2.1. (i) (2014-04-26) *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) (2014-04-27) *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) (2014-05-07) *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, for any positive integer n divisible by 3 or 4, there is no square congruent to $F_3 = 2$ modulo n. If $n > 4$ has a prime divisor $p > 3$, and there is a positive Fibonacci number $F_k < p/2$ with $x^2 \not\equiv F_k \pmod p$ for all $x \in \mathbb{Z}$, then $F_k < n/2$ and also $x^2 \not\equiv F_k \pmod n$ for all $x \in \mathbb{Z}$. We have verified part (i) for every $n = 4, 5, \ldots, 3 \times 10^9$. For data and graphs related to Conjecture 2.1(i), one may consult [16, 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 $p < 10^8$, 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) (2014-04-26) *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) (2014-04-27) *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) (2014-05-21) *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(i) for every $n = 3, \ldots, 10^9$, and Conjecture 2.2(iii) for all primes $p < 10^8$. The least Lucas number which is a quadratic nonresidue modulo the prime $p = 167$, is $L_{10} = 123 > 167/2$. 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. (2014-05-11) *Let p be any prime with $p \equiv 1 \pmod 3$. 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 $p < 10^9$ with $p \equiv 1 \pmod 3$; 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. (2014-04-20) *For any prime $p > 7$, there is a prime $q < p$ with $2^q - 1$ a quadratic residue modulo p. Also, for each prime $p > 5$, there exists a prime $q < p$ such that $2^q + 1$ is a quadratic nonresidue modulo p.*

We have verified Conjecture 2.4 for primes p below 10^8; see [16, A235709 and A235712] for related data and graphs. For example, 41 is the least prime $q < 13003$ with $2^q - 1$ a quadratic residue modulo the prime 13003. Note that for the prime $p = 2089$ there is no prime $q < p$ with $2^q + 1$ a primitive root modulo p.

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. (2014-04-23) (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 $g - 1$ an integer square.*

(ii) *For any prime $p > 3$, there is a triangular number $g < p$ which is a primitive root modulo p. Also, every prime $p > 7$ has a primitive root $g < p$ modulo p which is a product of two consecutive integers.*

Remark 3.1. The author verified Conjecture 3.1(i) for all primes $p < 10^7$ in April 2014, and later C. Greathouse [9] extended the verification to all primes below $p < 10^{10}$ in May 2014. The author would like to offer 2,000 RMB as the prize for the first complete solution of Conjecture 3.1(i). Note that for any prime $p > 5$, one of the three numbers $1^2 + 1 = 2$, $2^2 + 1 = 5$ and $3^2 + 1 = 10 = 2 \times 5$ is a quadratic residue modulo p. We have verified Conjecture 3.1(ii) for primes $p < 10^9$. Note that for any prime $p > 3$ one of 1×2, 2×3 and 3×4 is a quadratic residue modulo p. For data and graphs concerning Conjecture 3.1, one may consult [16, 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 [15] proved that if $a \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$ are relatively prime then for any $k \in \mathbb{Z}^+$ there is a positive integer n such that $p_{n+1} \equiv p_{n+2} \equiv \ldots \equiv p_{n+k} \equiv a \pmod{m}$, 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 [17] 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. (2014-05-10) (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.*

(iii) *For any integer $n > 4$, there is a positive integer $k \leqslant n/2$ such that $\prod_{j=1}^k p_j$ is a primitive root modulo p_n.*

Remark 3.2. We have verified part (i) for all odd primes $p < 10^9$, and parts (ii) and (iii) for n up to 10^7. See [16, 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

For each $n \in \mathbb{Z}^+$ let $p(n)$ be the number of ways to write n as a sum of some unordered positive integers with repetitions allowed. This is the well-known partition function. On April 24, 2014 the author conjectured that for any prime q there is a positive integer n with $p(n) < q$ such that $p(n)$ is a primitive root modulo q (cf. [18, Conjecture 4.10(i)]). We have verified this for all primes $q < 10^9$.

Conjecture 3.3. (i) (2014-04-22) *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) (2014-05-09) *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 $3 < p < 10^7$; see [16, A236966] for related data and graphs. For example, for the prime $p = 5336101$, the least prime $q < p/2$ with $2^q - 1$ a primitive root modulo p is 193.

(b) Conjecture 3.3(ii) is very strong! We have verified it for all primes $3 < p < 10^7$; see [16, 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

Conjecture 3.4. (2014-05-11) *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 odd primes $p < 10^8$; see [16, 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

Both Conjecture 3.4 and the following conjecture are more sophisticated than Erdős' Problem mentioned in Section 1.

Conjecture 3.5. (i) (2014-04-21) *For any prime $p > 7$, there exists a prime $q < p$ such that both q and $q!$ are primitive roots modulo p.*

(ii) (2017-08-27) *For any odd prime p, there exists a prime $q < p$ such that q is not only a primitive root modulo p but also a primitive root modulo p_q.*

Remark 3.5. (a) We have verified this conjecture for primes $p < 10^8$; see [16, A236306 and A291615] for related data and graphs. For example, both 3 and $3! = 6$ are primitive roots modulo the prime 17; the number 3 is a primitive root modulo the prime 43 and also a primitive root modulo $p_3 = 5$.

(b) If there are only finitely many primes q with q a primitive root modulo p_q, then for the product P of all such primes q, by Dirichlet's theorem on primes in arithmetic progressions, $p \equiv 1 \pmod{4P}$ for some prime p, hence for any prime $q \mid P$ we have $(\frac{q}{p}) = 1$ (by the law of quadratic reciprocity) and thus q is not a primitive root modulo

p. So Part (ii) of Conjecture 3.4 implies that there are infinitely primes q such that q is a primitive root modulo p_q. For such primes q, see [16, A291657].

Conjecture 3.6. (i) *For any prime p, there are positive integers k and m such that $g = F_kF_m$ is smaller than p and also a primitive root modulo p. Moreover, the set $G(p)$ given by* (1.1) *contains a number of the form ℓF_m with $m \in \mathbb{Z}^+$ and $\ell \in \{F_k : k = 2,3,4\} = \{1,2,3\}$.*

(ii) *For each prime p, there are $k, m \in \mathbb{N}$ such that $g = L_kL_m$ is smaller than p and also a primitive root modulo p.*

Remark 3.6. We have verified parts (i) and (ii) of Conjecture 3.6 for primes p smaller than 5×10^9 and 10^9 respectively. See [16, A331506] for related data. In contrast with Conjectures 2.1(i) and Conjecture 2.2(i), Conjecture 3.6 implies that for any prime p there are $k, m \in \mathbb{N}$ with $F_k < p$ and $L_m < p$ such that $(\frac{F_k}{p}) = (\frac{L_m}{p}) = -1$.

Conjecture 3.7. (2018-05-24) *For any prime $p > 7$, there is a a number $g = 5^k + 10^m$ with $k, m \in \mathbb{N}$ such that g is smaller than p and also a primitive root modulo p.*

Remark 3.7. We have verified this for all primes $7 < p < 10^9$ (cf. [16, A305048]). Our computation suggests that

$$3,\ 5,\ 31,\ 43,\ 241,\ 307,\ 311,\ 421,\ 523,\ 547,\ 607,\ 727,\ 2311,\ 2511,$$
$$2689,\ 6091,\ 9439,\ 13381,\ 55441,\ 56401,\ 66301,\ 6276271$$

are the only values of primes p which has a unique primitive root $g < p$ of the form $5^k + 10^m$ $(k, m \in \mathbb{N})$. For example, for the prime $p = 6276271$, the unique primitive root $g < p$ of the form $5^k + 10^m$ is $5^5 + 10 = 3135$.

Conjecture 3.8. (2018-05-24) (i) *For any odd prime p, the set $G(p)$ given by* (1.1) *contains a number of the form $\binom{2k}{k} + \binom{2m}{m}$ with $k, m \in \mathbb{N}$.*

(ii) *For any odd prime p, the set $G(p)$ given by* (1.1) *contains a number of the form $C_k + C_m$ with $k, m \in \mathbb{N}$, where C_n denotes the n-th Catalan number $\binom{2n}{n}/(n+1)$.*

Remark 3.8. We have verified Conjecture 3.8 for all odd primes $p < 10^9$ (cf. [16, A305030]). For example, $\binom{2}{1} + \binom{8}{4} = 2 + 70 = 72$ is a primitive root modulo the prime 109.

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} $(k = 1, \ldots, (p-3)/2)$ are p-adic integers (this follows from the recurrence for Bernoulli numbers or Kummer's theorem on Bernoulli numbers). The tangent numbers $t_1, t_2, \ldots$ are given by

$$\tan x = \sum_{n=1}^{\infty} t_n \frac{x^{2n-1}}{(2n-1)!} \ \text{ for } |x| < \frac{\pi}{2}.$$

It is known that

$$t_n = (-1)^{n-1} 2^{2n} (2^{2n} - 1) \frac{B_{2n}}{2n} \qquad \text{for all } n \in \mathbb{Z}^+.$$

Conjecture 3.9. (2014-05-07) (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.*

(iii) *For any odd prime p, there is a prime $q < p$ such that the tangent number t_q is a primitive root modulo p.*

Remark 3.9. We have verified Conjecture 3.9 for primes $p < 10^8$; see [16, A242210 and A242213] for related data and graphs.

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

p	5	11	19
$q < p$	2	3	17
B_{q-1}	$-1/2$	$1/6$	$-3617/510$
B_{q-1} mod 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 rational numbers $H_n^{(2)} = \sum_{0<k\leqslant n} 1/k^2$ with $n \in \mathbb{N}$.

Conjecture 3.10. (2014-05-08) *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.*

Remark 3.10. We have verified both parts of Conjecture 3.10 for all primes $5 < p < 10^8$; See [16, A242222 and A242241] for related data and graphs.

Conjecture 3.11. (i) (2014-04-21) *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) (2014-04-22) *For any prime $p > 3$, there exists a prime $q < p/2$ such that the Bell number* $\mathrm{Bell}(q)$ *is a primitive root modulo p, where* $\mathrm{Bell}(q)$ *denotes the number of ways to partition a set of cardinality q.*

(iii) (2014-05-11) *For any prime $p > 3$, there exists a prime $q < p/2$ such that the Franel number $f_{q-1} = \sum_{k=0}^{q}\binom{q-1}{k}^3$ is a primitive root modulo p.*

(iv) *For any prime $p > 3$, there exists a prime $q < p$ such that the T_q is a primitive root modulo p, where the central trinomial coefficient T_q denotes the coefficient of x^q in the expansion of $(x^2 + x + 1)^q$.*

Remark 3.11. We have verified all parts of Conjecture 3.11 for each prime $3 < p < 10^8$. For related data and graphs concerning parts (i)-(ii) of Conjecture 3.11, one may visit [16, A236308 and A237594].

4 Other Conjectures involving Primitive Roots Modulo Primes

The following conjecture was originally motivated by the Chinese Remainder Theorem.

Conjecture 4.1. (2017-08-29) (i) *Let p and q be primes. Then there is a positive integer $g \leqslant \sqrt{4pq+1}$ such that g is a primitive root modulo p and also a primitive root modulo q. We may require further that $g < \sqrt{pq}$ unless $\{p, q\}$ is among the 15 pairs*

$$\{2,3\},\ \{2,11\},\ \{2,13\},\ \{2,59\},\ \{2,131\},\ \{2,181\},$$

$$\{3,7\},\ \{3,31\},\ \{3,79\},\ \{3,191\},\ \{3,199\},\ \{5,271\},\ \{7,11\},\ \{7,13\},\ \{7,71\}.$$

(ii) *Let n be any positive integer. If $q_1, \ldots, q_n$ are primes with* $\max\{q_1, \ldots, q_n\}$ *sufficiently large, then there is a positive integer $g \leqslant n!(q_1 \ldots q_n)^{1/n}$ which is a primitive root modulo q_k for all $k = 1, \ldots, n$.*

Remark 4.1. See [16, A291690] for related data and comments. We have verified part (i) of Conjecture 4.1 for primes $p, q < 2 \times 10^5$. For example, $5 = \sqrt{4 \times 2 \times 3 + 1}$ is the least positive integer which is a primitive root modulo 2 and also a primitive root modulo 3, and $19 = \lfloor\sqrt{4 \times 7 \times 13 + 1}\rfloor$ is the least positive integer which is a primitive root modulo 7 and also a primitive root modulo 13. Our computation for primes smaller than 3515 suggests that if $q_1 \leqslant q_2 \leqslant q_3$ are primes but there is no positive integer $g \leqslant 6\sqrt[3]{q_1q_2q_3}$ which is a primitive root modulo q_i for all $i = 1, 2, 3$, then (q_1, q_2, q_3) must be among the following 13 triples:

$$(3, 5, 43),\ (3, 7, 13),\ (3, 7, 19),\ (3, 7, 67),\ (3, 7, 127),\ (3, 7, 151),\ (3, 7, 421),$$
$$(3, 13, 127),\ (3, 31, 43),\ (5, 13, 31),\ \ (7, 11, 523),\ (7, 23, 127),\ (31, 37, 79).$$

For $(q_1, q_2, q_3, q_4) = (3, 31, 43, 991)$, 1439 is the least positive integer which is a primitive root modulo q_j for all $j = 1, 2, 3, 4$. Note that $1439/(3 \times 31 \times 43 \times 991)^{1/4} \approx 32.25$.

Conjecture 4.2. (2015-08-05) (i) *For any prime $p > 13$, there are distinct positive integers a and b with $a + b < p$ such that $a, b, a + b, ab(a + b)$ are all primitive roots modulo p.*

(ii) *For any prime $p > 13$ with $p \neq 31$, there are $a, b, c \in \{1, \ldots, p-1\}$ with $a^2+b^2 = c^2$ such that abc is a primitive root modulo p.*

Remark 4.2. We have verified parts (i) and (ii) for primes below 10^6 and 10^8 respectively. See [16, A260947 and A260946] for related data.

Conjecture 4.3. (2015-08-06) (i) *For any prime $p > 7$, there exists a right triangle whose three sides are among $1, \ldots, p - 1$ and whose area is a primitive root modulo p.*

(ii) *For any prime $p > 31$, there exists a right triangle whose three sides are among $1, \ldots, p - 1$, and whose perimeter and area are quadratic residues modulo p.*

Remark 4.3. See [16, A260960] for related data and graphs. For example, 6 is a primitive root modulo the prime 17 and 6 is also the area of a right triangle with sides $3, 4, 5$.

Conjecture 4.4. (2014-06-11) *For any $m, N \in \mathbb{Z}^+$, there is a positive integer $n \geqslant N$ such that p_{n+i} is a primitive root modulo p_{n+j} for all $i, j = 0, \ldots, m$ with $i \neq j$.*

Remark 4.4. See [16, A243839] for related data. Via the Maynard-Tao theorem, H. Pan and Z.-W. Sun [14] showed that the Generalized Riemann Hypothesis implies Conjecture 4.4.

Conjecture 4.5. (2017-10-02) *There are infinitely many primes p such that $\phi(p - 1)$ is a primitive root modulo p. Moreover, there is a constant $0.361 < s < 0.362$ such that $\lim_{x\to+\infty} S(x)/(x/\log x) = s$, where $S(x)$ denotes the number of primes $p \leqslant x$ with $\varphi(p - 1)$ a primitive root modulo p.*

Remark 4.5. It is well known that for any prime p there are exactly $\varphi(p-1)$ numbers among $1,\ldots,p-1$ which are primitive roots modulo p. See [16, A293213] for such special primes p with $\varphi(p-1)$ a primitive root modulo p. Among the first 6×10^8 primes, there are exactly 216635723 such special primes. Note that $216635723/(6\times10^8)\approx0.36105954$.

Conjecture 4.6. (2013-10-02) *For any prime $p>7$ with $p\neq 13,29,61$, there are three consecutive integers among $1,\ldots,p-1$ which are primitive roots modulo p.*

Remark 4.6. See [16, A229899] for related data. For example, $19,20,21$ are primitive roots modulo the prime 23.

Conjecture 4.7. (2017-10-01) *Let p be a prime. For any $x\in\mathbb{Z}$, one of $x,x+1,\ldots,x+2\lfloor\sqrt{p+2}\rfloor+2$ is a primitive root modulo p.*

Remark 4.7. We have verified this for all primes $p<10^5$. For example, $2\lfloor\sqrt{79+2}\rfloor+2=20$ and among the integers $8+k$ $(k=0,\ldots,20)$ only 28 is a primitive root modulo 79. Also, $2\lfloor\sqrt{409+2}\rfloor+2=42$, and among the integers $388+k$ $(k=0,\ldots,42)$ only 388 and 430 are primitive roots modulo the prime 409. By [3, Theorem 3], Conjecture 4.7 holds for sufficiently large primes p.

For $a,b,c\in\mathbb{Z}$, we set

$$S_p(a,b,c):=\sum_{g\in G(p)}\left(\frac{ag^2+bg+c}{p}\right),\tag{4.1}$$

where $G(p)$ is given by (1.1). Since the inverse g^* of $g\in G(p)$ modulo p is also a primitive root modulo p, we see that

$$S_p(a,b,c)=\sum_{g\in G(p)}\left(\frac{a(g^*)^2+bg^*+c}{p}\right)=\sum_{g\in G(p)}\left(\frac{a+bg+cg^2}{p}\right)=S_p(c,b,a).$$

Conjecture 4.8. (2013-10-02) *Let $p>11$ be a prime, and let $a,b,c\in\mathbb{Z}$ with $b^2-4ac\not\equiv0\pmod p$. If a or c is not divisible by p, then*

$$|S_p(a,b,c)|<\frac{\sqrt{p}}{2}\log p.\tag{4.2}$$

Remark 4.8. We note that $S_{11}(1,-3,1)/(\sqrt{11}\log 11)\approx0.50296$.

Conjecture 4.9. (2013-10-02) *Let $p>13$ be a prime with $p\neq19,31$, and let a,b,c be integers with a or c not divisible by p. If p does not divide b^2-4ac, then there is a primitive root g modulo p such that ag^2+bg+c is a quadratic residue modulo p, and there is also a primitive root h modulo p such that ah^2+bh+c is a quadratic nonresidue modulo p.*

Remark 4.9. Compare this with a consequence of Theorem 1.1 mentioned in Section 1.

Conjecture 4.10. (2014-04-20) *Let a be any positive integer.*

(i) *For any prime $p > 7$ with $p \neq 13$, there is a primitive root g modulo p^a such that $g + g^{-1}$ is also a primitive root modulo p^a.*

(ii) *For any prime $p > 5$ with $p \neq 13, 61$, there is a primitive root g modulo p^a such that $g - g^{-1}$ is also a primitive root modulo p^a.*

Remark 4.10. Note that Conjecture 4.10 holds for $a = 1$ by Theorem 1.2.

When p and $2p + 1$ are both prime, p is called a Sophie Germain prime.

Conjecture 4.11. (2014-01-17) (i) *Any integer $n > 37$ can be written as $k + m$ with $k, m \in \mathbb{Z}^+$ such that $p = p_k + \varphi(m)$ is a Sophie Germain prime having 2 as a primitive root.*

(ii) *Any integer $n > 7$ can be written as $k + m$ with $k, m \in \mathbb{Z}^+$ such that $p = \varphi(k) + \varphi(m/2) - 1$ is a prime having 2 as a primitive root.*

Remark 4.11. See [16, A235987] for related data and graphs.

5 Primitive Prime Divisors of Some Combinatorial Sequences

Conjecture 5.1. *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 5.1. See [16, A242292] for related data.

Conjecture 5.2. *For any integer $n > 4$, there is a prime p for which $B_{2n} \equiv 0 \pmod p$ but $B_{2k} \not\equiv 0 \pmod p$ for all $0 < k < n$. For each $n = 2, 3, \ldots$, the Euler number E_{2n} has a prime divisor p not dividing any E_{2k} with $0 < k < n$. Also, for every $n = 4, 5, \ldots$ the tangent number t_n has a prime divisor p not dividing any t_k with $0 < k < n$.*

Remark 5.2. See [16, A242193, A242194 and A242195]. In Table 5.1, $p_B(n)$ denotes the least prime p for which $B_{2n} \equiv 0 \pmod p$ but $B_{2k} \not\equiv 0 \pmod p$ for all $0 < k < n$, similarly $p_E(n)$ represents the least prime divisor of E_{2n} not dividing any E_{2k} with $0 < k < n$.

Table 5.1: Least primitive prime 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	2348958052704310825201782857619894774 1
20	137616929	41
21	1520097643918070802691	137
22	59	587
23	23	285528427091
24	653	5516994249383296071214195242422482492286460673697
25	417202699	5639
26	577	53
27	39409	2749
28	113161	5303
29	29	1459879476771247347961031445001033
30	2003	6821509
31	31	101
32	1226592271	25349

Conjecture 5.3. *Let $n > 1$ be an integer. If $n \neq 7$, then there is a prime p for which $H_n \equiv 0 \pmod p$ but $H_k \not\equiv 0 \pmod p$ for all $0 < k < n$. Also, there is a prime p for which $H_n^{(2)} \equiv 0 \pmod p$ but $H_k^{(2)} \not\equiv 0 \pmod p$ for all $0 < k < n$.*

Remark 5.3. For related numerical data, see [16, A242223 and A242241].

Table 5.2: Least primitive prime 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

In Table 5.2, $p_H(n)$ denotes the least prime p for which $H_n \equiv 0 \pmod p$ but $H_k \not\equiv 0 \pmod p$ for all $0 < k < n$, and $p_{H^{(2)}}(n)$ represents the least prime p for which $H_n^{(2)} \equiv 0 \pmod p$ but $H_k^{(2)} \not\equiv 0 \pmod p$ for all $0 < k < n$.

Conjecture 5.4. *For the sequence* $(\mathrm{Bell}(n))_{n>1}$ *of Bell numbers, each term* $\mathrm{Bell}(n)$ *with* $n \geqslant 2$ *has a primitive prime divisor.*

Remark 5.4. See [16, A242171] for related data.

Table 5.3: Least primitive prime divisors $p_b(n)$ of $\mathrm{Bell}(n)$ and $p_f(n)$ of $f_n = \sum_{k=0}^{n}\binom{n}{k}^3$

n	$p_b(n)$	$p_f(n)$
1		2
2	2	5
3	5	7
4	3	173
5	13	563
6	7	13
7	877	41
8	23	369581
9	19	937
10	4639	61
11	22619	23
12	37	29
13	27644437	2141
14	1800937	12148537
15	251	31
16	241	157
17	255755771	59
18	19463	37
19	271	506251
20	61	151
21	24709	3019
22	17	769
23	89	47
24	123419	6730949
25	367	79
26	101	53
27	157	3853
28	67	661
29	75979	138961158000728258971
30	107	1361

Table 5.3 is related to Conjecture 5.4 and the following Conjecture 5.5, where $p_b(n)$ denotes the least prime divisor p of the Bell number Bell(n) which does not divide any Bell(k) with $0 < k < n$, and $p_f(n)$ represents the least prime divisor p of the Franel number $f_n = \sum_{k=0}^n \binom{n}{k}^3$ which does not any f_k with $0 < k < n$.

Conjecture 5.5. *For the sequence $(f_n)_{n\geqslant 1}$ of Franel numbers, each term $f_n = \sum_{k=0}^n \binom{n}{k}^3$ 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 $0 < k < n$.*

Remark 5.5. For related numerical data, see [16, A242171 and A242169].

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 $(x^2 + x + 1)^n$, and the Motzkin number M_n is given by $M_n = \sum_{k=0}^n \binom{n}{2k} C_k$.

Conjecture 5.6. (i) *For the sequence $(T_n)_{n\geqslant 1}$ of central trinomial coefficients, each term T_n with $n > 1$ has a primitive prime divisor.*

(ii) *Each term of the sequence $(M_n)_{n\geqslant 4}$ of Motzkin numbers has a primitive prime divisor.*

Remark 5.6. See [16, A242170] for related data. For integer $n > 1$ let $p_T(n)$ be the least prime factor of T_n which does not divide any of T_k $(0 < k < n)$. Then

$$p_T(2) = 3,\ p_T(3) = 7,\ p_T(4) = 19,\ p_T(5) = 17,\ p_T(6) = 47,\ p_T(7) = 131,\ p_T(8) = 41,$$
$$p_T(9) = 43,\ p_T(10) = 1279,\ p_T(11) = 503,\ p_T(12) = 113,\ p_T(13) = 2917,\ p_T(14) = 569,$$
$$p_T(15) = 198623,\ p_T(16) = 14083,\ p_T(17) = 26693,\ p_T(18) = 201611,\ p_T(19) = 42998951,$$
$$p_T(20) = 41931041,\ p_T(21) = 52635749,\ p_T(22) = 1296973,\ p_T(23) = 169097,$$
$$p_T(24) = 1451,\ p_T(25) = 1304394227,\ p_T(26) = 107,\ p_T(27) = 233,\ p_T(28) = 173.$$

Recall that the central Delannoy numbers D_n $(n \in \mathbb{N})$ and the Apéry numbers A_n $(n \in \mathbb{N})$ are given by

$$D_n := \sum_{k=0}^n \binom{n}{k}\binom{n+k}{k} \quad\text{and}\quad A_n := \sum_{k=0}^n \binom{n}{k}^2\binom{n+k}{k}^2.$$

Conjecture 5.7. *Each term of the sequence $(D_n)_{n\geqslant 1}$ of central Delannoy numbers has a primitive prime divisor. Also, any term of the sequence $(A_n)_{n\geqslant 1}$ of Apéry numbers has a primitive prime divisor.*

Remark 5.7. See [16, A242173] for related data.

Conjecture 5.8. *Each term of the sequence* $(d_n)_{n\geqslant 3}$ *of derangement numbers has a primitive prime divisor, where* $d_n := n!\sum_{k=0}^n \frac{(-1)^k}{k!}$. *Also, any term of the sequence* $(\mathrm{Domb}(n))_{n\geqslant 4}$ *of Domb numbers has a primitive prime divisor, where* $\mathrm{Domb}(n) := \sum_{k=0}^n \binom{n}{k}^2\binom{2k}{k}\binom{2(n-k)}{n-k}$.

Remark 5.8. See [16, A242207] for related data.

Conjecture 5.9. *For* $n\in\mathbb{Z}^+$ *let* $q(n)$ *denote the number of unordered ways to write* n *as a sum of distinct positive integers. Then, for any integer* $n>203$, *the number* $q(n)$ *has a prime divisor* p *not dividing any* $q(k)$ *with* $0<k<n$.

Remark 5.9. See [16, A242180] for related data. It is known that $q(n)\sim e^{\pi\sqrt{n/3}}/(4\sqrt[4]{3n^3})$ as $n\to+\infty$.

Finally, we mention that Conjectures 5.1-5.9 were formulated by the author on May 7, 2014 on the basis of related computations.

Acknowledgments. The initial version of this paper was posted to arXiv in May 2014 with the ID `arXiv:1405.0290`. The author would like to thank Prof. Carl Pomerance and J. Wu for helpful comments.

References

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

[2] 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.

[3] D. A. Burgess, *On character sums and primitive roots*, Proc. London Math. Soc. **12** (1962), 179–192.

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

[5] S. D. Cohen, T. Oliveira e Silva and N. Sutherland, *Linear combinations of primitive elements of a finite field*, Finite Fields Appl. **51** (2018), 388–406.

[6] 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. Comp. **84** (2015), 2979–2986.

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

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

[9] C. Greathouse, *Re: Primitive roots of special forms*, a Message to Number Theory Mailing List, May 1, 2014. `https://listserv.nodak.edu/cgi-bin/wa.exe? A2=NMBRTHRY;f1e44d28.1405&S=`.

[10] R. K. Guy, Unsolved Problems in Number Theory, 3rd Edition, Springer, New York, 2004.

[11] W. B. Han, *Polynomials and primitive roots over finite fields*, Acta Math. Sinica **32** (1989), bo. 1, 110–117.

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

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

[14] H. Pan and Z.-W. Sun, *Consecutive primes and Legendre symbols*, Acta Arith. **190** (2019), 209–220.

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

[16] Z.-W. Sun, Sequences A229899, A229910, A235709, A235712, A236306, A236308, A236966, A235987, A237594, A239957, A239963, A241476, A241492 A241568, A241604, A241675, A242169, A242170, A242171, A242173, A242180, A242193, A242194, A242195, A242207, A242210, A242213, A242222, A242223, A242241, A242248, A242250, A242266, A242277, A242292, A242345, A243839, A260946, A260947, A260960, A261690, A291615, A291657, A293213, A305030, A305048, A331506 in OEIS (On-Line Encyclopedia of Integer Sequences), `http://oeis.org`.

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

[18] Z.-W. Sun, *Problems on combinatorial properties of primes*, in: M. Kaneko, S. Kanemitsu and J. Liu (eds.), Number Theory: Plowing and Starring through High Wave Forms, Proc. 7th China-Japan Seminar (Fukuoka, Oct. 28–Nov. 1, 2013), Ser. Number Theory Appl. 11, World Sci., Singapore, 2015, pp. 169-187.

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

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

[21] K. Zsigmondy, *Zur Theorie der Potenzrest*, J. Monatsh. Math. **3** (1892), 265–284.

Department of Mathematics, Nanjing University, Nanjing 210093, People's Republic of China

E-mail address: `zwsun@nju.edu.cn`