J. Number Theory 133(2013), no. 8, 2794–2812.

ON FUNCTIONS TAKING ONLY PRIME VALUES

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. For $n = 1, 2, 3, \ldots$ define $S(n)$ as the smallest integer $m > 1$ such that those $2k(k-1) \bmod m$ for $k = 1, \ldots, n$ are pairwise distinct; we show that $S(n)$ is the least prime greater than $2n-2$ and hence the value set of the function $S(n)$ is exactly the set of all prime numbers. For every $n = 4, 5, \ldots$, we prove that the least prime $p > 3n$ with $p \equiv 1 \pmod 3$ is just the least positive integer m such that $18k(3k-1)$ $(k = 1, \ldots, n)$ are pairwise distinct modulo m. For $d \in \{4, 6, 12\}$ and $n = 3, 4, \ldots$, we show that the least prime $p \geqslant 2n-1$ with $p \equiv -1 \pmod d$ is the smallest integer m such that those $(2k-1)^d$ for $k = 1, \ldots, n$ are pairwise distinct modulo m. We also pose several challenging conjectures on primes. For example, we find a surprising recurrence for primes, namely, for every $n = 10, 11, \ldots$ the $(n+1)$-th prime p_{n+1} is just the least positive integer m such that $2s_k^2$ $(k = 1, \ldots, n)$ are pairwise distinct modulo m where $s_k = \sum_{j=1}^k (-1)^{k-j} p_j$. We also conjecture that for any positive integer m there are consecutive primes $p_k, \ldots, p_n$ $(k < n)$ not exceeding $2m + 2.2\sqrt{m}$ such that $m = p_n - p_{n-1} + \cdots + (-1)^{n-k} p_k$.

1. Introduction

Prime numbers play a central role in number theory (see the excellent book [CP] on primes by R. Crandall and C. Pomerance). It is known that there is no non-constant polynomial with integer coefficients, even in several variables, which takes only prime values. Many mathematicians ever tried in vain to find a nontrivial number -theoretic function whose values are always primes. In 1947 W. H. Mills [Mi] showed that there exists a real number A such that $\lfloor A^{3^n} \rfloor$ is prime for any $n = 1, 2, 3, \ldots$; unfortunately such a constant A cannot be effectively found.

In 2012, the author conjectured that for any $m = 12, 13, \ldots$ the largest positive integer n with $\binom{2k}{k}$ $(k = 1, \ldots, n)$ pairwise distinct modulo m does not exceed $0.6\sqrt{m}\log m$. Motivated by this, he made the following conjecture.

2010 *Mathematics Subject Classification.* Primary 11A41, 11Y11; Secondary 05A10, 11A07, 11B75, 11N13.

Keywords. Primes, congruences, functions taking only prime values.

Supported by the National Natural Science Foundation (grant 11171140) of China.

Conjecture 1.1. (i) ([S12a]) *For $n \in \mathbb{Z}^+ = \{1, 2, 3, \ldots\}$ define $s(n)$ as the smallest integer $m > 1$ such that*

$$\binom{2k}{k} \quad (k = 1, \ldots, n)$$

are pairwise distinct modulo m. Then all those $s(1), s(2), \ldots$ are primes!

(ii) ([S12b]) *For $n \in \mathbb{Z}^+$ let $t(n)$ denote the least integer $m > 1$ such that*

$$|\{k! \bmod m : \ k = 1, \ldots, n\}| = n.$$

Then $t(n)$ is prime with the only exception $t(5) = 10$.

The author verified both parts of Conjecture 1.1 for $n \leqslant 2000$. Later, Laurent Bartholdi and Qing-Hu Hou verified parts (i) and (ii) of Conjecture 1.1 for all $n \in [2001, 5000]$ and $n \in [2001, 10000]$ respectively.

In 1985 L. K. Arnold, S. J. Benkoski and B. J. McCabe [ABM] defined $D(n)$ for $n \in \mathbb{Z}^+$ as the smallest positive integer m such that $1^2, 2^2, \ldots, n^2$ are pairwise distinct modulo m, and they showed that if $n > 4$ then $D(n)$ is the smallest integer $m \geqslant 2n$ such that m is p or $2p$ with p an odd prime. (Note that if $p = 2q + 1$ with p and q both prime then the prime p is not contained in the range $\{D(n) : \ n \in \mathbb{Z}^+\}$.) This stimulated later studies of characterizing

$$D_f(n) := \min\{m \in \mathbb{Z}^+ : \ f(1), f(2), \ldots, f(n) \text{ are distinct modulo } m\}$$

for some special polynomials $f(x) \in \mathbb{Z}[x]$ including powers of x and Dickson polynomials of degrees relatively prime to 6 (see, e.g., [BSW, MM, Z] and the references therein). However, the value sets of those D_f considered in papers along this line are usually somewhat complicated and they contain infinitely many composite numbers. Note also that $D_f(1)$ is just 1, not a prime.

Now we present a simple function whose set of values is exactly the set of all prime numbers.

Theorem 1.1. (i) *For $n \in \mathbb{Z}^+$ let $S(n)$ denote the smallest integer $m > 1$ such that those $2k(k-1)$ mod m for $k = 1, \ldots, n$ are pairwise distinct. Then $S(n)$ is the least prime greater than $2n - 2$.*

(ii) *For $n \in \mathbb{Z}^+$ let $T(n)$ denote the least integer $m > 1$ such that those $k(k-1)$ mod m with $1 \leqslant k \leqslant n$ are pairwise distinct. Then we have*

$$T(n) = \min\{m \geqslant 2n - 1 : \ m \text{ is a prime or a positive power of } 2\}. \tag{1.1}$$

Remark 1.1. (a) The way to generate all primes via Theorem 1.1(i) is simple in concept, but it has no advantage in algorithm. Nevertheless, Theorem 1.1(i) is of certain theoretical interest since it provides a surprising new characterization of primes.

(b) By modifying our proof of Theorem 1.1(i), we are also able to show that for any $d, n \in \mathbb{Z}^+$ with $n \geqslant \lfloor d/2 \rfloor + 4$ the least prime $p \geqslant 2n + d$ is just the smallest $m \in \mathbb{Z}^+$ such that $2k(k + d)$ $(k = 1, \ldots, n)$ are pairwise distinct modulo m. (Similar results hold for $d \in \{0, -2\}$ and $n \in \{5, 6, \ldots\}$.)

Below are four more related theorems.

Theorem 1.2. (i) *For any positive integer n, the number $2^{\lceil \log_2 n\rceil}$ (the least power of two not smaller than n) is the least positive integer m such that those $k(k-1)/2$ $(k=1,\ldots,n)$ are pairwise distinct modulo m.*

(ii) *Let $d\in\{2,3\}$ and $n\in\mathbb{Z}^+$. Take the smallest positive integer m such that $|\{k(dk-1) \bmod m:\ k=1,\ldots,n\}|=n$. Then m is the least power of d not smaller than n, i.e., $m=d^{\lceil \log_d n\rceil}$.*

(iii) *Let $n\in\{4,5,\ldots\}$ and take the least positive integer m such that $18k(3k-1)$ $(k=1,\ldots,n)$ are pairwise distinct modulo m. Then m is the least prime $p>3n$ with $p\equiv 1 \pmod 3$.*

Remark 1.2. We are also able to prove some other results similar to those in Theorem 1.2. For example, for each $n=5,6,7,\ldots$ the first prime $p\equiv -1 \pmod 3$ after $3n$ is just the least $m\in\mathbb{Z}^+$ such that those $18k(3k+1)$ $(k=1,\ldots,n)$ are pairwise distinct modulo m. Also, if $f(n)$ denotes the least $m\in\mathbb{Z}^+$ with $|\{4k(4k-1) \bmod m:\ k=1,\ldots,n\}|=n$ and $g(n)$ denotes the least $m\in\mathbb{Z}^+$ with $|\{4k(4k+1) \bmod m:\ k=1,\ldots,n\}|=n$, then $f(n)$ with $n\geqslant 5$ is the least prime $p>(8n-4)/3$ with $p\equiv 1 \pmod 4$, and $g(n)$ with $n\geqslant 6$ is the least prime $p>(8n-2)/3$ with $p\equiv -1 \pmod 4$.

Theorem 1.3. *For $d,n\in\mathbb{Z}^+$ let $\lambda_d(n)$ be the smallest integer $m>1$ such that those $(2k-1)^d$ $(k=1,\ldots,n)$ are pairwise distinct modulo m. Then $\lambda_d(n)$ with $d\in\{4,6,12\}$ and $n>2$ is the least prime $p\geqslant 2n-1$ with $p\equiv -1 \pmod d$.*

Theorem 1.4. *Let q be an odd prime. Then the smallest integer $m>1$ such that those $k^q(k-1)^q$ $(k=1,\ldots,n)$ are pairwise distinct modulo m, is just the least prime $p\geqslant 2n-1$ with $p\not\equiv 1 \pmod q$.*

Theorem 1.5. *Define $s_n=\sum_{k=1}^n(-1)^{n-k}p_k$ for all $n\in\mathbb{Z}^+$, where p_k denotes the k-th prime. Then, for any $n\in\mathbb{Z}^+$ those $2s_k^2$ $(k=1,\ldots,n)$ are pairwise distinct modulo p_{n+1}.*

Remark 1.3. All terms of the sequence $s_1,s_2,s_2,\ldots$ are positive integers. In fact, if $n\in\mathbb{Z}^+$ is even then $s_n=\sum_{k=1}^{n/2}(p_{2k}-p_{2k-1})>0$; if $n\in\mathbb{Z}^+$ is odd then $s_n=\sum_{k=1}^{(n-1)/2}(p_{2k+1}-p_{2k})+p_1>0$. Here we list the values of $s_1,\ldots,s_{15}$.

$$s_1=2,\ s_2=1,\ s_3=4,\ s_4=3,\ s_5=8,\ s_6=5,\ s_7=12,\ s_8=7,$$
$$s_9=16,\ s_{10}=13,\ s_{11}=18,\ s_{12}=19,\ s_{13}=22,\ s_{14}=21,\ s_{15}=26.$$

The sequence $0,s_1,s_2,\ldots$ was first introduced by N.J.A. Sloane and J. H. Conway [SC]. We conjecture that for any integers $m>0$ and r there are infinitely many $n\in\mathbb{Z}^+$ with $s_n\equiv r \pmod m$.

In the next section we will present two auxiliary theorems. Section 3 is devoted to our proofs of Theorems 1.1 and 1.2. In Section 4 we will show Theorems 1.3-1.5.

Motivated by Theorem 1.5 we raise the following conjecture on recurrence for primes which allows us to compute p_{n+1} in terms of $p_1,\ldots,p_n$.

Conjecture 1.2. *Let $n \in \mathbb{Z}^+$ with $n \neq 1, 2, 4, 9$. Then p_{n+1} is the smallest positive integer m such that those $2s_k^2$ $(k = 1, \ldots, n)$ are pairwise distinct modulo m.*

Remark 1.4. (a) We have verified Conjecture 1.2 for all $n \leqslant 10^5$. Note that 9 is the least $m \in \mathbb{Z}^+$ with $2s_1^2, 2s_2^2, 2s_3^2, 2s_4^2$ pairwise distinct modulo m, and 25 is the least $m \in \mathbb{Z}^+$ with $|\{2s_k^2 \bmod m : \ k = 1, \ldots, 9\}| = 9$.

(b) Define $b(n)$ as the least power of two modulo which $s_1, \ldots, s_n$ are pairwise incongruent. We conjecture that $b(n)$ is the least $m \in \mathbb{Z}^+$ such that $2s_k^2 - s_k$ $(k = 1, \ldots, n)$ are pairwise distinct modulo m, and moreover $\{b(n) : n \in \mathbb{Z}^+\} = \{2^a : a = 0, 1, 2, \ldots\}$.

Inspired by Conjecture 1.2, we find the following surprising conjecture on representations of integers by alternating sums of consecutive primes.

Conjecture 1.3. *For any positive integer m, there are consecutive primes $p_k, \ldots, p_n$ $(k < n)$ not exceeding $2m + 2.2\sqrt{m}$ such that*

$$m = p_n - p_{n-1} + \cdots + (-1)^{n-k} p_k.$$

Remark 1.5. We also conjecture that $2m + 2.2\sqrt{m}$ in Conjecture 1.3 can be replaced by $m + 4.6\sqrt{m}$ if m is odd. If the upper bound $2m + 2.2\sqrt{m}$ is replaced by $3m$, then we may require additionally that $p_k - 1$ and $p_n + 1$ are both practical numbers (cf. [S13]). We have verified Conjecture 1.3 for $m = 1, \ldots, 10^5$. To illustrate the conjecture, we look at a few concrete examples:

$$1 = 3 - 2, \quad 2 = 5 - 3, \quad 3 = 7 - 5 + 3 - 2, \quad 4 = 11 - 7, \quad 5 = 7 - 5 + 3,$$
$$8 = 11 - 7 + 5 - 3 + 2, \quad 11 = 19 - 17 + 13 - 11 + 7,$$
$$20 = 41 - 37 + 31 - 29 + 23 - 19 + 17 - 13 + 11 - 7 + 5 - 3,$$
$$303 = p_{76} - p_{75} + \cdots - p_{53} + p_{52} \ \text{ with } p_{76} = 383 = 303 + \lfloor 4.6\sqrt{303} \rfloor,$$
$$2382 = p_{652} - p_{651} + \cdots + p_{44} - p_{43} \ \text{ with } p_{652} = 4871 = 2 \cdot 2382 + \lfloor 2.2\sqrt{2382} \rfloor.$$

The author would like to offer 1000 US dollars as the prize for the first correct proof of Conjecture 1.3. We also have some other conjectures on representations involving alternating sums of consecutive primes, for example, every $m = 3, 4, \ldots$ can be written in the form $p + s_n$, where p is a Sophie Germain prime and n is a positive integer.

We also have a conjecture involving sums of consecutive primes.

Conjecture 1.4. *For $k \in \mathbb{Z}^+$ let S_k denote the sum of the first k primes $p_1, \ldots, p_k$.*

(i) *For $n \in \mathbb{Z}^+$ define $S^+(n)$ as the least integer $m > 1$ such that m divides none of $S_i! + S_j!$ with $1 \leqslant i < j \leqslant n$. Then $S^+(n)$ is always a prime, and $S^+(n) < S_n$ for every $n = 2, 3, 4, \ldots$.*

(ii) *For $n\in\mathbb{Z}^+$ define $S^-(n)$ as the least integer $m>1$ such that m divides none of those $S_i!-S_j!$ with $1\leqslant i<j\leqslant n$. Then $S^-(n)$ is always a prime, and $S^-(n)<S_n$ for every $n=2,3,4,\ldots$.*

(iii) *For any positive integer n not dividing 6, the least integer $m>1$ such that $2S_k^2$ $(k=1,\ldots,n)$ are pairwise distinct modulo m is a prime smaller than n^2.*

Remark 1.6. When $n>1$, clearly $S_n!\pm S_{n-1}!\equiv 0 \pmod m$ for any $m=1,\ldots,S_{n-1}$, and hence both $S^+(n)$ and $S^-(n)$ are greater than S_{n-1}. Thus, by the conjecture we should have $S^+(n)<S_n<S^+(n+1)$ and $S^-(n)<S_n<S^-(n+1)$ for all $n=2,3,\ldots$. Conjecture 1.4 implies that for any $n=2,3,\ldots$ the interval (S_{n-1},S_n) contains the primes $S^+(n)$ and $S^-(n)$, which are actually very close to S_{n-1}. However, it seems very challenging to prove that (S_n,S_{n+1}) contains a prime for any $n\in\mathbb{Z}^+$. Note that

$$S_n\sim\sum_{k=1}^n k\log k\sim\int_1^n x\log x dx=\frac{x^2}{2}\log x\bigg|_1^n-\int_1^n\frac{x^2}{2}(\log x)'dx\sim\frac{n^2}{2}\log n$$

as $n\to+\infty$, and the Legendre conjecture asserts that the interval $(n^2,(n+1)^2)$ contains a prime for any $n\in\mathbb{Z}^+$. We conjecture that the number of primes in the interval (S_n,S_{n+1}) is asymptotically equivalent to $cn/2$ as $n\to+\infty$, where $c\geqslant 1$ is a constant (whose value is probably 1).

Our following conjecture allows us to produce primes via products of consecutive primes.

Conjecture 1.5. *For $k\in\mathbb{Z}^+$ let P_k denote the product of the first k primes $p_1,\ldots,p_k$.*

(i) *For $n\in\mathbb{Z}^+$ define $w_1(n)$ as the least integer $m>1$ such that m divides none of those P_i-P_j with $1\leqslant i<j\leqslant n$. Then $w_1(n)$ is always a prime.*

(ii) *For $n\in\mathbb{Z}^+$ define $w_2(n)$ as the least integer $m>1$ such that m divides none of those P_i+P_j with $1\leqslant i<j\leqslant n$. Then $w_2(n)$ is always a prime.*

(iii) *We have $w_1(n)<n^2$ and $w_2(n)<n^2$ for all $n=2,3,4,\ldots$.*

Remark 1.7. (a) Clearly $w_i(n)\leqslant w_i(n+1)$ for $i=1,2$ and $n\in\mathbb{Z}^+$. Since $P_1,\ldots,P_n$ are pairwise distinct modulo $w_1(n)$, we have $w_1(n)\geqslant n$ and hence $W_1=\{w_1(n):\ n\in\mathbb{Z}^+\}$ is an infinite set. For any integer $m>1$, there is an odd prime $p_n\equiv -1 \pmod m$ and hence $P_{n-1}+P_n=P_{n-1}(1+p_n)\equiv 0 \pmod m$. Thus $W_2=\{w_2(n):\ n\in\mathbb{Z}^+\}$ is also infinite. If $w_i(n)=p_k$, then $k\geqslant n$ since $P_k\pm P_{k+1}\equiv 0 \pmod{p_k}$. Thus it follows from Conjecture 1.5(ii) that $w_2(n)>n$ for all $n\in\mathbb{Z}^+$, in other words, for each $n=2,3,4,\ldots$ there are $1\leqslant j<k\leqslant n$ such that $P_j+P_k\equiv 0 \pmod n$. For $n=2,3,4,\ldots$ we conjecture further that $P_n\equiv P_j\equiv -P_k \pmod n$ for some $j,k\in\{1,\ldots,n-1\}$. This seems simple but we are unable to prove it.

(b) The author [S12c] listed values of $w_1(n)$ for $n = 1, \ldots, 1172$, and values of $w_2(n)$ for $n = 1, \ldots, 258$. Later W. B. Hart [H] reported that he had verified Conjecture 1.5 for all $n \leqslant 10^5$.

A prime is said to be of the first kind (or the second kind) if it belongs to $W_1 = \{w_1(n) : n \in \mathbb{Z}^+\}$ (or $W_2 = \{w_2(n) : n \in \mathbb{Z}^+\}$, resp.). Here we list the first 20 primes of each kind.

Primes of the first kind: 2, 3, 5, 11, 23, 29, 37, 41, 47, 73, 131, 151, 199, 223, 271, 281, 353, 457, 641, 643, ...

Primes of the second kind: 2, 3, 5, 7, 11, 19, 23, 47, 59, 61, 71, 101, 113, 223, 487, 661, 719, 811, 947, 1327, ...

The famous Artin conjecture for primitive roots states that if an integer a is neither -1 nor a square then there are infinitely many primes p having a as a primitive root modulo p. This is open for any particular value of a. Concerning Artin's conjecture the reader may consult the excellent survey of R. Murty [Mu] and the book [IR, p. 47]. In Section 5 we will present more conjectures which are similar to Conjecture 1.1 or related to the Artin conjecture.

2. Two auxiliary theorems

Theorem 2.1. *Let $m > 1$ and $n > 1$ be integers such that those $k(k-1)$ for $k = 1, \ldots, n$ are pairwise distinct modulo m.*

(i) *We have $m \geqslant 2n - 1$.*

(ii) *If $n \geqslant 15$ and $m \leqslant 2.4n$, then m is a prime or a power of two.*

Proof of Theorem 2.1(i). Suppose on the contrary that $m \leqslant 2n - 2$. Then $n \geqslant m/2 + 1$. If m is even, then

$$\left(\frac{m}{2}+1\right)\left(\frac{m}{2}+1-1\right) - \frac{m}{2}\left(\frac{m}{2}-1\right) = m \equiv 0 \pmod{m}.$$

If m is odd, then $(m+3)/2 \leqslant n$ and

$$\frac{m+3}{2}\left(\frac{m+3}{2}-1\right) - \frac{m-1}{2}\left(\frac{m-1}{2}-1\right) = 2m \equiv 0 \pmod{m}.$$

So we get a contradiction as desired. □

The next task in this section is to prove Theorem 2.1(ii). In the following two lemmas, we fix $n \geqslant 15$ and $m \in [2n-1, 2.4n]$ and assume that those $k(k-1)$ mod m $(1 \leqslant k \leqslant n)$ are pairwise distinct.

Lemma 2.1. *$m \neq 2p$ for any odd prime p.*

Proof. Suppose that $m = 2p$ with p an odd prime. Note that

$$\frac{p+3}{2}\left(\frac{p+3}{2}-1\right) - \frac{p-1}{2}\left(\frac{p-1}{2}-1\right) = 2p \equiv 0 \pmod{2p}.$$

and hence $(p+3)/2 > n$. So $2n - 1 \leqslant p = m/2 \leqslant 1.2n$, which is impossible. □

Lemma 2.2. *$p^2 \nmid m$ for any odd prime p.*

Proof. Suppose that $m = p^2 q$ with p an odd prime and $q \in \mathbb{Z}^+$. Set $k = (p+1)/2$ and $l = k + pq \leqslant 2pq$. Then

$$l(l-1) - k(k-1) = (l-k)(l+k-1) = pq(pq + 2k - 1) \equiv 0 \pmod{p^2 q}$$

and hence we must have $2pq > n$. If $p > 3$, then

$$n < \frac{2m}{p} \leqslant \frac{2}{5} m \leqslant \frac{2}{5} \times 2.4n < n$$

which is impossible. When $p = 3$, we also have a contradiction since $l = 2+3q = 2 + m/3 \leqslant 2 + 0.8n \leqslant n$. $\square$

Proof of Theorem 2.1(ii). Suppose that $n \geqslant 15$ and $m \leqslant 2.4n$. We want to deduce a contradiction under the assumption that m is neither a prime nor a power of two.

By Lemmas 2.1 and 2.2, we may write $m = pq$ with p an odd prime, $q > 2$ and $p \nmid q$.

Take an integer $k \in [1, q/(2,q)]$ such that

$$k \equiv \frac{1-p}{2} \left(\bmod \frac{q}{(2,q)}\right),$$

where $(2, q)$ is the greatest common divisor of 2 and q. Set $l = k + p$. Then

$$l(l-1) - k(k-1) = p(2k - 1 + p) \equiv 0 \pmod{pq}.$$

If $2 \mid q$, then $q \geqslant 4$ and hence

$$l \leqslant p + \frac{q}{2} = \frac{m}{q} + \frac{m}{2p} \leqslant \frac{m}{4} + \frac{m}{6} = \frac{5}{12} m \leqslant \frac{5}{12} \times 2.4n = n$$

which contradicts the property of m. Thus $2 \nmid q$ and

$$l \leqslant p + q = \frac{m}{p} + \frac{m}{q} \leqslant \left(\frac{1}{p} + \frac{1}{q}\right) 2.4n.$$

If both p and q are greater than 3, then

$$\frac{1}{p} + \frac{1}{q} \leqslant \frac{2}{5} < \frac{5}{12}$$

and hence $l < \frac{5}{12} 2.4n = n$ which leads to a contradiction. So m cannot have two distinct prime divisors greater than 3. In view of Lemma 2.2, we may assume that $m = pq$ with $q = 3$. Note that

$$l \leqslant p + q = \frac{m}{3} + 3 \leqslant \frac{2.4n}{3} + 3 = 0.8n + 3 \leqslant n$$

since $n \geqslant 15$. So we get a contradiction.

In view of the above, we have completed the proof of Theorem 2.1. $\square$

Theorem 2.2. *Let $n>1$ and $m\geqslant 2n-1$ be integers.*

(i) *Suppose that m is a prime or a power of two. Then $k(k-1)\not\equiv l(l-1) \pmod m$ for any $1\leqslant k<l\leqslant n$.*

(ii) *If m is a power of two not exceeding $2.4n$, then $2k(k-1)\equiv 2l(l-1) \pmod m$ for some $1\leqslant k<l\leqslant n$.*

Proof. (i) To prove part (i) we distinguish two cases.

Case 1. $m=2^a$ for some $a\in\mathbb{Z}^+$.

In this case, $n\leqslant (m+1)/2=2^{a-1}+1/2$ and hence $n\leqslant 2^{a-1}$. For any $1\leqslant k<l\leqslant n$, we have $0<l-k<n\leqslant 2^{a-1}$ and $0<l+k-1<2n\leqslant 2^a$, hence

$$l(l-1)-k(k-1)=(l-k)(l+k-1)\not\equiv 0 \pmod{2^a}$$

since one of $l-k$ and $l+k-1$ is odd.

Case 2. m equals an odd prime p.

If $1\leqslant k<l\leqslant n$, then $0<l-k<n\leqslant (p+1)/2<p$ and $l+k-1<2n-1\leqslant p$, therefore

$$l(l-1)-k(k-1)=(l-k)(l+k-1)\not\equiv 0 \pmod p.$$

(ii) As $2k(k-1)\equiv 0 \pmod 4$ for any $k=1,\ldots,n$, we just assume that $m=2^a$ with $a>2$. Take $k=2^{a-2}$ and $l=k+1$. Then

$$2l(l-1)-2k(k-1)=2(2^{a-2}+1)2^{a-2}-2\times 2^{a-2}(2^{a-2}-1)=2^a\equiv 0 \pmod{2^a}$$

and $k<l=2^{a-2}+1<2^a/2.4\leqslant n$.

Combining the above we have completed the proof. □

3. Proofs of Theorems 1.1 and 1.2

As in Theorem 1.1, let $S(n)$ (or $T(n)$) denote the least integer $m>1$ such that those $2k(k-1)$ (or $k(k-1)$, resp.) for $k=1,\ldots,n$ are pairwise distinct modulo m.

Lemma 3.1. *For any positive integer n we have $2n-1\leqslant T(n)\leqslant S(n)\leqslant 2.4n$.*

Proof. The case $n=1$ is trivial since $S(1)=T(1)=2$. Below we assume $n\geqslant 2$.

As those $2k(k-1)$ ($k=1,\ldots,n$) are pairwise distinct modulo $S(n)$, those $k(k-1)$ ($k=1,\ldots,n$) are also pairwise distinct modulo $S(n)$ and hence $S(n)\geqslant T(n)$. Note that $T(n)\geqslant 2n-1$ by Theorem 2.1(i).

By J. Nagura [N], for $m=25,26,\ldots$ the interval $[m,1.2m]$ contains a prime. Thus, if $n\geqslant 13$ then there is a prime in the interval $[2n-1,2.4n]$. For $n=2,\ldots,12$ we can easily check that the interval $[2n-1,2.4n]$ does contain primes. By P. Dusart [D, Section 4], for $x\geqslant 3275$ there is a prime p such that

$$x\leqslant p\leqslant x\left(1+\frac{1}{2\log^2 x}\right)\leqslant x\left(1+\frac{1}{2\log^2 3275}\right)<1.01x;$$

this provides another way to show that $[2n-1, 2.4n]$ contains at least a prime. So there exists an odd prime $p \in [2n-1, 2.4n]$ and hence $S(n) \leqslant p \leqslant 2.4n$ by Theorem 2.2(i). (For $1 \leqslant k < l \leqslant n$, clearly $k(k-1) \not\equiv l(l-1) \pmod p$ if and only if $2k(k-1) \not\equiv 2l(l-1) \pmod p$.) We are done. $\Box$

Proof of Theorem 1.1. We want to prove that $S(n)$ is the least prime greater than $2n-2$ and $T(n)$ is the least integer $m \geqslant 2n-1$ with m a prime or a positive power of 2. For $n = 1, \ldots, 14$ these can be easily verified.

Now assume that $n \geqslant 15$. By Lemma 3.1, Theorem 2.1(ii) and Theorem 2.2(ii), $S(n)$ must be an odd prime in the interval $[2n-1, 2.4n]$. In view of Theorem 2.2(i), $S(n)$ is the least prime greater than $2n-2$.

By Lemma 3.1, $T(n) \in [2n-1, 2.4n]$. Applying Theorem 2.1(ii) we see that $T(n)$ is either a prime or a power of two. Combining this with Theorem 2.2(i) we immediately get (1.1). $\Box$

Proof of Theorem 1.2(i). Let $n \in \mathbb{Z}^+$ and take the smallest positive integer m such that those $k(k-1)/2$ $(1 \leqslant k \leqslant n)$ are pairwise distinct modulo m. We want to prove that $m = 2^h$ where $h := \lceil \log_2 n \rceil$. This is trivial when $n = 1$.

Below we let $n > 1$ and hence $h > 0$. Note that $2^{h-1} < n \leqslant 2^h$.

Clearly $m \geqslant n$. As $2^{h+1} > 2n-1$, by Theorem 2.2(i), those $k(k-1)$ $(k = 1, \ldots, n)$ are pairwise distinct modulo 2^{h+1}. It follows that $m \leqslant 2^h < 2n$. If m is odd, then $m \leqslant 2n-3$ and

$$\frac{1}{2} \cdot \frac{m+3}{2}\left(\frac{m+3}{2} - 1\right) - \frac{1}{2} \cdot \frac{m-1}{2}\left(\frac{m-1}{2} - 1\right) = m \equiv 0 \pmod m.$$

So m must be even.

Suppose that $m \neq 2^h$. Then m has the form $2p^a q$ with p an odd prime, $a, q \in \mathbb{Z}^+$ and $p \nmid q$. Let k be the least positive residue of $(1-p^a)/2 \bmod 2q$ and set $l = k + p^a$. Observe that

$$l(l-1) - k(k-1) = (l-k)(l+k-1) = p^a(2k-1+p^a) \equiv 0 \pmod{4p^a q}$$

and thus $l(l-1)/2 \equiv k(k-1)/2 \pmod m$. Clearly,

$$l \leqslant 2q + p^a = \frac{m}{p^a} + \frac{m}{2q} < \left(\frac{2}{p^a} + \frac{1}{q}\right) n.$$

Thus we must have

$$\frac{2}{p^a} + \frac{1}{q} > 1$$

and hence $q < 3$. Thus $m = 2p^a$ or $m = 4 \times 3 = 12$. When $n \leqslant 12$ we can easily check that $m \neq 12$. For $n > 12$ we have $m \geqslant n > 12$. Therefore $m = 2p^a$.

Note that $m/2 + 1 \leqslant n$. If $p^a \equiv 1 \pmod 4$, then

$$\frac{p^a(p^a-1)}{2} - \frac{1(1-1)}{2} = 2p^a \frac{p^a-1}{4} \equiv 0 \pmod{2p^a}$$

and $p^a = m/2 < n$; if $p^a \equiv 3 \pmod 4$, then

$$\frac{(p^a+1)p^a}{2} - \frac{1(1-1)}{2} = 2p^a\frac{p^a+1}{4} \equiv 0 \pmod{2p^a}$$

and $p^a + 1 = m/2 + 1 \leqslant n$. So we get a contradiction.

The proof of Theorem 1.2(i) is now complete. $\square$

Proof of Theorem 1.2(ii). Fix $d \in \{2, 3\}$ and $n \in \mathbb{Z}^+$, and take the least $m \in \mathbb{Z}^+$ such that those $k(dk-1)$ $(k = 1, \ldots, n)$ are pairwise distinct modulo m. We want to prove that $m = d^{\lceil \log_d n \rceil}$. This can be easily verified in the case $n \leqslant 7$.

Below we assume $n > 7$ and hence $m \geqslant n \geqslant 8$. Suppose that $d^{h-1} < n \leqslant d^h$ where $h \in \mathbb{Z}^+$. For $1 \leqslant k < l \leqslant n$, clearly $0 < l - k < n \leqslant d^h$ and hence

$$l(dl-1) - k(dk-1) = (l-k)(d(l+k)-1) \not\equiv 0 \pmod{d^h}.$$

Thus $m \leqslant d^h < dn$.

When $m \equiv -1 \pmod d$, we have $1 < l = (m+1)/d - 1 < (m+1)/d \leqslant n$ and

$$l(dl-1) - 1(d\cdot 1-1) = \left(\frac{m+1}{d} - 1\right)((m+1-d)-1) - (d-1) \equiv 0 \pmod m,$$

which contradicts the choice of m. So we have $m \not\equiv -1 \pmod d$. When $d = 3$ and $m \equiv 1 \pmod d$, for $k = (m-1)/3$ and $l = (m+2)/3$, we have $1 \leqslant k < l \leqslant n$ and

$$l(dl-1) - k(dk-1) = (l-k)(d(l+k)-1) = 2m \equiv 0 \pmod m,$$

which also contradicts the choice of m. Therefore $m \not\equiv \pm 1 \pmod d$ and hence $d \mid m$.

Write $m = d^a q$ with $a, q \in \mathbb{Z}^+$ and $d \nmid q$. Set $\delta = d^a - \varepsilon_q$, where

$$\varepsilon_q = \begin{cases} -(\frac{-1}{q}) & \text{if } d = 2 \text{ and } a = 1, \\ (\frac{-1}{q}) & \text{if } d = 2 \text{ and } a \geqslant 2, \\ (\frac{q}{3}) & \text{if } d = 3, \end{cases}$$

and $(-)$ denotes the Legendre symbol. Note that

$$\frac{\delta q + 1}{d} = d^{a-1}q - \frac{\varepsilon_q q - 1}{d} \in \mathbb{Z} \text{ and } \frac{\delta q+1}{d} \equiv d^a \pmod 2.$$

Thus both

$$k = \frac{1}{2}\left(\frac{\delta q+1}{d} - d^a\right) \text{ and } l = \frac{1}{2}\left(\frac{\delta q+1}{d} + d^a\right)$$

are integers, and

$$l(dl-1)-k(dk-1)=(l-k)(d(l+k)-1)=d^a(\delta q)\equiv 0 \pmod{m}.$$

As

$$\frac{\delta q+1}{d}+d^a\leqslant d^{a-1}q+\frac{q+1}{d}+d^a=\frac{m+1}{d}+\frac{m}{d^{a+1}}+\frac{m}{q}$$

and $m<dn$, we have

$$2l<n+\frac{n}{d^a}+\frac{dn}{q}.$$

Case 1. $q\geqslant d+1$.

As $6(2\cdot 6-1)-2(2\cdot 2-1)=60=5(3\cdot 5-1)-2(3\cdot 2-1)$, we have $m\nmid 60$. If $a=1$, then $q>5$, hence

$$\frac{\delta q+1}{d}\geqslant\frac{(d-1)q+1}{d}>\frac{5(d-1)-1}{d}=d$$

and

$$2l<n+\frac{n}{d}+\frac{dn}{q}\leqslant n+\frac{n}{2}+\frac{3n}{6}=2n.$$

When $a\geqslant 2$, we have $q>d+(d-1)/(d^a-1)$ and hence

$$\frac{\delta q+1}{d}=d^{a-1}q-\frac{\varepsilon_q q-1}{d}\geqslant d^{a-1}q-\frac{q-1}{d}=\frac{(d^a-1)q+1}{d}>d^a,$$

also

$$2l<n+\frac{n}{d^a}+\frac{dn}{q}\leqslant n\left(1+\frac{1}{d^2}+\frac{d}{d+1}\right)\leqslant 2n.$$

So, we always have $1\leqslant k<l\leqslant n$ and hence we get a contradiction by the definition of m.

Case 2. $q<d$.

If $q=1$, then $d^{h-1}<n\leqslant m=d^a\leqslant d^h$ and hence $m=d^h$ as desired.

Now suppose that $q>1$. As $q<d\leqslant 3$ we must have $q=2$ and $d=3$. Since $3^{h-1}<n\leqslant m=2\cdot 3^a\leqslant 3^h$, we get $a=h-1$ and hence $3^a+1\leqslant n$. Observe that

$$(3^a+1)(3(3^a+1)-1)-1(3\cdot 1-1)=3^a(3(3^a+2)-1)\equiv 0 \pmod{2\cdot 3^a}.$$

This contradicts that $m=2\cdot 3^a$.

Combining the above we have completed the proof of Theorem 1.2(ii). $\square$

Lemma 3.2 ([RR, Theorem 1]). *Let $d \in \{1, \ldots, 72\}$, and $r \in \mathbb{Z}$ with $(r, d) = 1$. For $x \geqslant 10^{10}$ and $\varepsilon = 0.023269$, we have*

$$(1-\varepsilon)\frac{x}{\varphi(d)} \leqslant \theta(x; r, d) \leqslant (1+\varepsilon)\frac{x}{\varphi(d)},$$

where φ is Euler's totient function and $\theta(x; r, d) := \sum_{p \leqslant x,\ p \equiv r \ (\mathrm{mod}\ d)} \log p$ with p prime.

Proof of Theorem 1.2(iii). Let $n > 3$ be an integer and take the least $m \in \mathbb{Z}^+$ with $|\{18k(3k-1) \bmod m :\ k = 1, \ldots, n\}| = n$. We want to prove that m is the least prime $p > 3n$ with $p \equiv 1 \pmod 3$. For $4 \leqslant n \leqslant 36$ one can verify the desired result directly.

Below we assume $n > 36$. Let $\varepsilon = 0.023269$. If $3n \geqslant 10^{10}$, then $3.433(1 - \varepsilon) > 3(1 + \varepsilon)$ and hence $\theta(3.433n; 1, 3) > \theta(3n; 1, 3)$ by Lemma 3.2, therefore $(3n, 3.433n]$ contains a prime $p \equiv 1 \pmod 3$. For $n = 37, \ldots, \lfloor 10^{10}/3 \rfloor$ one can easily verify (using a computer) that the interval $(3n, 3.433n]$ contains at least a prime congruent to 1 modulo 3. (Note also that in 1932 R. Breusch [Br] refined the Bertrand Postulate confirmed by Chebyshev by showing that for any $x \geqslant 7$ the interval $(x, 2x)$ contains a prime congruent to 1 modulo 3.)

If p is a prime in $(3n, 3.433n]$ with $p \equiv 1 \pmod 3$, then for $1 \leqslant k < l \leqslant n$ we have

$$18l(3l-1) - 18k(3k-1) = 18(l-k)(3(l+k)-1) \not\equiv 0 \pmod p$$

since $1 \leqslant l - k < n < p$ and $p \neq 3(l + k) - 1 < 6n - 1 < 2p$. Therefore $n \leqslant m \leqslant 3.433n$.

Assume that $m_0 = m/(18, m) < 3n$. As $m \geqslant n > 36$ we have $m_0 > 2$. If $m_0 \equiv 1 \pmod 3$, then for $k = (m_0 - 1)/3$ and $l = (m_0 + 2)/3 \leqslant n$ we have $l(3l - 1) \equiv k(3k - 1) \pmod{m_0}$ and hence $18l(3l - 1) \equiv 18k(3k - 1) \pmod m$ which leads to a contradiction. As $4(3 \cdot 4 - 1) \equiv 3(3 \cdot 3 - 1) \pmod 5$, we cannot have $m_0 = 5$ since $k(3k - 1)$ $(k = 1, \ldots, n)$ are pairwise distinct modulo m_0. If $m_0 > 5$ and $m_0 \equiv 2 \pmod 3$, then for $k = 1 < l = (m_0 - 2)/3 \leqslant n$, we have $l(3l - 1) \equiv k(3k - 1) \pmod{m_0}$ which leads to a contradiction. Therefore $3 \mid m_0$. Write $m_0 = 3^a q$ with $a, q \in \mathbb{Z}^+$ and $3 \nmid q$. If $q > 1$, then we may argue as in cases 1 and 2 in the proof of Theorem 1.2(ii) with $d = 3$ to get a contradiction. So $m_0 = 3^a$, and hence m or $m/2$ is a power of 3. Suppose $3^{h-1} < n \leqslant 3^h$ with $h \in \mathbb{Z}^+$. Then $m \in \{3^h, 3^{h+1}, 2 \cdot 3^h, 2 \cdot 3^{h-1}\}$ since $n \leqslant m \leqslant 3.433n$. For $k = 1 < l = 3^{h-1} + 1 \leqslant n$ we clearly have $m \mid 18(l - k)$ and hence $18l(3l - 1) \equiv 18k(3k - 1) \pmod m$ which leads to a contradiction.

By the above, we must have $m_0 \geqslant 3n$. As $m/2 < 3n$ we must have $(18, m) = 1$ and $m \geqslant 3n$. If $p \in [3n, 3.433n]$ is a prime with $p \equiv 2 \pmod 3$, then for $k = (p - 5)/6$ and $l = (p + 7)/6$ we have $1 \leqslant k < l \leqslant n$ and $18l(3l - 1) \equiv 18k(3k - 1) \pmod p$.

Now it remains to show that m cannot be a composite number in $[3n, 3.433n]$. Suppose that $m = cd$ with $c, d \in \{2, 3, \ldots\}$. As $(m, 18) = 1$, we have $(c, 6) =$

$(d,6)=1$. Take $k\in[1,d]$ such that $k\equiv((1+2d(\frac{d}{3}))/3-c)/2 \pmod d$, and set $l=k+c$. Note that $l(3l-1)-k(3k-1)=(l-k)(3(l+k)-1)\equiv 0 \pmod m$. Clearly

$$l=k+c\leqslant c+d=\frac{m}{d}+\frac{m}{c}\leqslant 3.433n\left(\frac{1}{c}+\frac{1}{d}\right)\leqslant n$$

since $m=cd\geqslant n>36$ and $1/3.433\geqslant\max\{1/5+1/11,1/7+1/7\}$. So we get a contradiction. □

4. Proofs of Theorems 1.3-1.5

Lemma 4.1. *Let $d\in\{4,6,12\}$ and $n\in\mathbb{Z}^+$. Then $[2n-1,2.4n]$ contains at least a prime $p\equiv -1 \pmod d$ except for $n\in E(d)$, where*

$$E(4)=\{1,7,17\},\quad E(6)=\{1,2,4,7,16,17\}$$

and

$$E(12)=\{1,2,3,4,7,8,9,13,14,15,16,17,18,19,43,44,67,68,69\}.$$

Proof. Note that $\varepsilon:=0.023269<1/11$. If $n\geqslant 10^{10}/2$, then by Lemma 3.2 we have

$$\theta(2.4n;-1,d)\geqslant(1-\varepsilon)\frac{2.4n}{\varphi(d)}>(1+\varepsilon)\frac{2n}{\varphi(d)}\geqslant\theta(2n;-1,d),$$

and hence $(2n,2.4n]$ contains at least a prime $p\equiv -1 \pmod d$. It can be easily verified that for $n<10^{10}/2$ the interval $[2n-1,2.4n]$ contains a prime $p\equiv -1 \pmod d$ except for $n\in E(d)$. We are done. □

Lemma 4.2. *Suppose that $p>3$ is a prime in $[2n-1,2.4n]$ where $n>2$ is an integer. For $d\in\{4,6,12\}$, those $(2k-1)^d$ with $1\leqslant k\leqslant n$ are pairwise distinct modulo p if and only if $p\equiv -1 \pmod d$.*

Proof. For $1\leqslant k<l\leqslant n$, we clearly have

$$(2l-1)^4-(2k-1)^4=((2l-1)^2-(2k-1)^2)((2l-1)^2+(2k-1)^2),$$

$$\begin{aligned}&(2l-1)^6-(2k-1)^6=((2l-1)^3-(2k-1)^3)((2l-1)^3+(2k-1)^3)\\=&((2l-1)^2-(2k-1)^2)((2l-1)^2+(2k-1)(2l-1)+(2k-1)^2)\\&\times((2l-1)^2-(2k-1)(2l-1)+(2k-1)^2)\end{aligned}$$

and

$$\begin{aligned}&(2l-1)^6+(2k-1)^6\\=&((2l-1)^2+(2k-1)^2)((2l-1)^4-(2k-1)^2(2l-1)^2+(2k-1)^4).\end{aligned}$$

Note that

$$(2l-1)^2-(2k-1)^2=4(l-k)(l+k-1)\not\equiv 0 \pmod p$$

since $0<l-k<l+k-1<2n-1\leqslant p$. If $(2l-1)^2+(2k-1)^2\equiv 0 \pmod p$, then -1 is a quadratic residue mod p and hence $p\equiv 1 \pmod 4$. For $\delta\in\{\pm 1\}$, if

$$4((2l-1)^2+\delta(2l-1)(2k-1)+(2k-1)^2)=(2(2l-1)+\delta(2k-1))^2+3(2k-1)^2$$

is divisible by p, then -3 is a quadratic residue mod p and hence $p\equiv 1 \pmod 6$. Similarly, if $(2l-1)^4-(2k-1)^2(2l-1)^2+(2k-1)^4\equiv 0 \pmod p$ then $p\equiv 1 \pmod 6$.

By the above, for any $d\in\{4,6,12\}$, if $p\equiv -1 \pmod d$ then those $(2k-1)^d$ with $k=1,\ldots,n$ are pairwise distinct modulo p.

Now we handle the case $p\equiv 1 \pmod 4$. It is well known that $p=x^2+y^2$ for some integers $x>y>0$ and hence $2p=(x+y)^2+(x-y)^2$ with $x\pm y$ odd. Take $k=(x-y+1)/2$ and $l=(x+y+1)/2$. Clearly $2l-1=x+y\leqslant\sqrt{2p}\leqslant\sqrt{4.8n}<2n$ and hence $1\leqslant k<l\leqslant n$. As $(2l-1)^2\equiv -(2k-1)^2 \pmod p$, we have $(2l-1)^4\equiv(2k-1)^4 \pmod p$ and $(2l-1)^{12}\equiv(2k-1)^{12} \pmod p$.

Now we assume $p\equiv 1 \pmod 3$. It is known that $p=u^2+3v^2$ for some $u,v\in\mathbb{Z}^+$ with $u\not\equiv v \pmod 2$. Write $u+v=2l-1$ and $|u-v|=\delta(v-u)=2k-1$. Clearly $k,l\in\mathbb{Z}^+$ and $k<l$. Since $4p=(u-3v)^2+3(u+v)^2$, we have

$$u+v\leqslant\sqrt{\frac{4p}{3}}\leqslant 2\sqrt{\frac{2.4n}{3}}<2n$$

and hence $l\leqslant n$. Observe that

$$\begin{aligned}&(2l-1)^2+\delta(2l-1)(2k-1)+(2k-1)^2\\ =&(u+v)^2+(u+v)(v-u)+(u-v)^2=u^2+3v^2\equiv 0 \pmod p.\end{aligned}$$

So we have $(2l-1)^6\equiv(2k-1)^6 \pmod p$ and $(2l-1)^{12}\equiv(2k-1)^{12} \pmod p$.

Combining the above we have finished the proof of Lemma 4.2. □

Proof of Theorem 1.3. Fix $d\in\{4,6,12\}$ and $n\in\{3,4,\ldots\}$. We want to prove that $\lambda_d(n)$ (the least integer $m>1$ with $|\{(2k-1)^d \bmod m:\ k=1,\ldots,n\}|=n$) is just the least prime $p\geqslant 2n-1$ with $p\equiv -1 \pmod d$.

If $n\leqslant 14$ or $n\in E(d)$, then we can easily verify the desired result. Below we simply assume $n\geqslant 15$ and $n\notin E(d)$.

For $1\leqslant k<l\leqslant n$, clearly $(2l-1)^d-(2k-1)^d$ is a multiple of $(2l-1)^2-(2k-1)^2=4l(l-1)-4k(k-1)$. If those $(2k-1)^d$ with $1\leqslant k\leqslant n$ are pairwise distinct modulo an integer $m>1$, then so are those $k(k-1)$ $(k=1,\ldots,n)$ and hence $m\geqslant 2n-1$ by Theorem 2.1(i). Therefore $\lambda_d(n)\geqslant 2n-1$.

By Lemma 4.1, $[2n-1,2.4n]$ contains a prime $p\equiv -1 \pmod d$ and hence $\lambda_d(n)\leqslant p\leqslant 2.4n$ by Lemma 4.2. As those $2k(k-1)$ $(k=1,\ldots,n)$ are pairwise distinct mod $\lambda_d(n)$, by Theorem 2.1(ii) and Theorem 2.2(ii), $\lambda_d(n)$ must be a prime. In view of Lemma 4.2, $\lambda_d(n)$ is the least prime $p\in[2n-1,2.4n]$ with $p\equiv -1 \pmod d$.

So far we have completed the proof of Theorem 1.3. □

Lemma 4.3. *For any odd prime q and positive integer n, the interval $[2n-1, 2.4n]$ contains at least a prime $p \not\equiv 1 \pmod q$ unless $n \leqslant 17$ and $q < 2.4n$.*

Proof. By the proof of Lemma 3.1, $[2n-1, 2.4n]$ contains a prime p. If $p \equiv 1 \pmod q$ then $q \leqslant p-1 < 2.4n$.

Clearly $[2 \cdot 1 - 1, 2.4]$ contains the prime $2 \not\equiv 1 \pmod q$. When $n > 1$, the interval $[2n-1, 2.4n]$ contains an odd prime p. If $q \geqslant 1.2n$ then $1 + 2q > 2.4n$ and hence $p \not\equiv 1 \pmod q$. Below we assume $q < 1.2n$.

We first handle the case $q \leqslant 53$. As in Lemma 4.1 we can employ [RR, Theorem 1.1] to deduce that $(2n, 2.4n]$ contains a prime $p \equiv -1 \pmod q$ for $n \geqslant 10^{10}/2$. For $n \in [18, 10^{10}/2]$ we can easily check that $[2n-1, 2.4n]$ indeed contains a prime $p \not\equiv 1 \pmod q$.

Now assume that $q \geqslant 59$. Set $x := 2.4n$. Then $q < x/2$. By the Brun-Titchmarsh theorem (cf. [MV] or [CP, p. 43]) in analytic number theory, we have

$$\pi(x; 1, q) := |\{p \leqslant x : \ p \text{ is a prime and } p \equiv 1 \pmod q\}| \leqslant \frac{2x}{\varphi(q)\log(x/q)}.$$

Thus, if $q \leqslant \sqrt{x}$ then

$$\pi(x; 1, q) \leqslant \frac{2x}{(q-1)\log\sqrt{x}} \leqslant \frac{4x}{58\log x} = \frac{2}{29} \times \frac{x}{\log x};$$

if $\sqrt{x} < q \leqslant x/2$ then

$$\pi(x; 1, q) \leqslant \frac{2x}{(\sqrt{x}-1)\log 2}.$$

Note that $(\sqrt{x}-1)\log 2 > 29\log x$ when $n \geqslant 114895$.

Assume $n > 148000$. By the above,

$$\pi(x; 1, q) \leqslant \frac{2}{29} \times \frac{x}{\log x}. \tag{4.1}$$

Since $x = 2.4n > 599$, by [D, Section 4] we have

$$\pi(x) := \pi(x; 1, 1) \geqslant \frac{x}{\log x}\left(1 + \frac{0.992}{\log x}\right) > \frac{x}{\log x}$$

and

$$\begin{aligned}\pi(2n) \leqslant& \frac{2n}{\log(2n)}\left(1 + \frac{1.2762}{\log(2n)}\right) \\ \leqslant& \frac{2n}{\log(2n)}\left(1 + \frac{1.2762}{\log(2 \times 148001)}\right) < \frac{2.202602n}{\log(2n)}.\end{aligned}$$

Thus

$$\pi(2.4n)-\pi(2n)>\frac{2.4n}{\log(2.4n)}-\frac{2.202602n}{\log(2n)}. \tag{4.2}$$

Since

$$\begin{aligned}\left(\frac{27}{29}\times 2.4-2.202602\right)\log n &\geqslant \left(\frac{27}{29}\times 2.4-2.202602\right)\log 148001\\ &>0.3795>2.202602\log 2.4-\frac{27}{29}\times 2.4\log 2,\end{aligned}$$

we have the inequality

$$\left(1-\frac{2}{29}\right)\frac{2.4}{\log n+\log 2.4}>\frac{2.202602}{\log n+\log 2}. \tag{4.3}$$

Combining (4.1)–(4.3) we obtain $\pi(2.4n)-\pi(2n)>\pi(2.4n;1,q)$. So $[2n-1,2.4n]$ contains a prime $p\not\equiv 1 \pmod q$.

When $18\leqslant n\leqslant 148000$ and $59\leqslant q<1.2n$, we can easily verify the desired result using a computer.

So far we have proved Lemma 4.3. $\square$

Proof of Theorem 1.4. Fix an odd prime q and let $D_q(n)$ denote the smallest integer $m>1$ such that those $k^q(k-1)^q$ $(k=1,\ldots,n)$ are pairwise distinct modulo m. We want to prove that $D_q(n)$ is just the least prime $p\geqslant 2n-1$ with $p\not\equiv 1 \pmod q$. This is trivial for $n=1$, so we just let $n>1$.

As those $k(k-1)$ mod $D_q(n)$ with $1\leqslant k\leqslant n$ are pairwise distinct, we have $2<2n-1\leqslant T(n)\leqslant D_q(n)$ by Theorem 1.1(ii).

If $n\leqslant 17$ and $q<2.4n$, then we can easily verify the desired result directly. Below we let $n\geqslant 18$ or $q\geqslant 2.4n$. By Lemma 4.3, the interval $[2n-1,2.4n]$ contains a prime $p\not\equiv 1 \pmod q$.

Let p be any prime in $[2n-1,2.4n]$. If $l^q(l-1)^q\equiv k^q(k-1)^q \pmod p$ for some $1\leqslant k<l\leqslant n\leqslant (p+1)/2$, then $p\nmid k(k-1)$,

$$\left(\frac{l(l-1)}{k(k-1)}\right)^q\equiv 1 \pmod p \ \text{ and } \ \left(\frac{l(l-1)}{k(k-1)}\right)^{(q,p-1)}\equiv 1 \pmod p; \tag{4.4}$$

as $l(l-1)\not\equiv k(k-1) \pmod p$ by Theorem 2.2(i), (4.4) implies that $(q,p-1)>1$ and hence $p\equiv 1 \pmod q$. Conversely, if $p\equiv 1 \pmod q$, then $q<p\leqslant 2.4n$ and $n\geqslant 18$, hence those $k^q(k-1)^q$ with $1\leqslant k\leqslant n$ cannot be pairwise distinct modulo p since we only have $(p-1)/q\leqslant (p-1)/3\leqslant (2.4n-1)/3<n-1$ q-th power residue modulo p.

In view of the above, $D_q(n)$ does not exceed the least prime $p\in[2n-1,2.4n]$ with $p\not\equiv 1 \pmod q$. If $D_q(n)=2^a w$ with $a\geqslant 3$ and $2\nmid w$, then

$$(2^{a-2}w(2^{a-2}w-1))^q\equiv (1(1-1))^q \pmod{2^a w}$$

and also $1 < 2^{a-2}w = D_q(n)/4 \leqslant 0.6n < n$. So $8 \nmid D_q(n)$. If $D_q(n) = 2^a w$ with $a \in \{1, 2\}$ and $2 \nmid w$, then those $k^q(k-1)^q$ $(k = 1, \ldots, n)$ are pairwise distinct modulo $w < D_q(n)$ since $8 \mid k^q(k-1)^q$ for all $k = 1, \ldots, n$. Thus $D_q(n)$ cannot be even. If $n \geqslant 15$, then $D_q(n)$ must be a prime by Theorem 2.1(ii), and hence it is just the least prime $p \geqslant 2n-1$ with $p \not\equiv 1 \pmod q$.

Now we handle the remaining case $2 \leqslant n \leqslant 14$ and $q \geqslant 2.4n$. Note that any prime in $[2n-1, 2.4n]$ is not congruent to 1 modulo q. For each $n =$ 2, 3, 4, 6, 7, 9, 10, 12, clearly $2n-1$ is prime and hence $D_q(n)$ is the least prime in $[2n-1, 2.4n]$. As $2 + 9/3 = 5$, we have $3^2 \nmid D_q(5)$ by the proof of Lemma 2.2, hence $D_q(5)$ is the least prime 11 after $2 \cdot 5 - 1 = 9$. (Note that $D_q(5) \neq 10$ since 10 is even.) Since $15/3+3 = 8$ and $21/3+3 < 11$, by the proof of Theorem 2.1(ii) we have $D_q(8) \neq 3 \cdot 5$ and $D_q(11) \neq 3 \cdot 7$, hence $D_q(8) = 17$ and $D_q(11) = 23$ as desired. For $n = 13, 14$, as $2 + D_q(n)/3 \leqslant 2 + 0.8n \leqslant n$, by the proof of Lemma 2.2 we have $p^2 \nmid D_q(n)$ for any odd prime p, hence $D_q(n) \neq 25, 27$. Note also that $D_q(n) \neq 26, 28$. So $D_q(13) = D_q(14) = 29$ as desired.

The proof of Theorem 1.4 is now complete. □

Lemma 4.4. *All those* $s_n = \sum_{k=1}^n (-1)^{n-k} p_k$ $(n = 1, 2, 3, \ldots)$ *are pairwise distinct, and also* $s_n \leqslant p_n$ *for all* $n \in \mathbb{Z}^+$.

Proof. Obviously $s_1 = p_1 = 2$. For $n = 2, 3, 4, \ldots$, we clearly have $s_n + s_{n-1} = p_n$ and hence $s_n < p_n$ since $s_{n-1} > 0$.

Now we show that $s_n \neq s_k$ for any $1 \leqslant k < n$ (see also [SC] for this simple observation). If $n-k$ is even, then

$$s_n - s_k = (p_n - p_{n-1}) + \cdots + (p_{k+2} - p_{k+1}) > 0.$$

When $n-k$ is odd, we have

$$s_n - s_k = \sum_{l=k+1}^{n} (-1)^{n-l} p_l - 2\sum_{j=1}^{k} (-1)^{k-j} p_j \equiv n - k \not\equiv 0 \pmod 2.$$

The proof of Lemma 4.4 is now complete. □

Proof of Theorem 1.5. Let $k, l \in \{1, \ldots, n\}$ with $k \neq l$. We want to show that

$$2s_l^2 - 2s_k^2 = 2(s_l + s_k)(s_l - s_k) \not\equiv 0 \pmod{p_{n+1}}.$$

By Lemma 4.4, $s_k \neq s_l$ and $|s_k - s_l| \leqslant \max\{s_k, s_l\} \leqslant \max\{p_k, p_l\} \leqslant p_n < p_{n+1}$, therefore $s_k \not\equiv s_l \pmod{p_{n+1}}$.

As $s_k + s_l \leqslant p_k + p_l \leqslant 2p_n < 2p_{n+1}$, it remains to prove that $s_k + s_l \neq p_{n+1}$. Without loss of generality we assume that $k < l$. If $l - k$ is even, then

$$s_l + s_k = \sum_{j=k+1}^{l} (-1)^{l-j} p_j + 2s_k \equiv l - k \equiv 0 \pmod 2$$

and hence $s_k + s_l \neq p_{n+1}$. If $l-k$ is odd, then

$$s_l+s_k = \sum_{j=k+1}^{l}(-1)^{l-j}p_j = p_l - \sum_{0<j\leqslant(l-k-1)/2}(p_{l-2j+1}-p_{l-2j}) \leqslant p_l \leqslant p_n < p_{n+1}.$$

So we do have $s_k + s_l \neq p_{n+1}$ as desired.

In view of the above we have completed the proof of Theorem 1.5. $\square$

5. More conjectures

Motivated by Conjecture 1.1, here we pose more conjectures for further research.

Conjecture 5.1. (i) *For the functions $s(n)$ and $t(n)$ in Conjecture* 1.1*, we have $s(n) < n^2$ and $t(n) \leqslant n^2/2$ for all $n = 2, 3, 4, \ldots$.*

(ii) *The number of primes not exceeding x in the set $S = \{s(1), s(2), s(3), \ldots\}$ is $o(\sqrt{x})$ and even $O(\sqrt{x}/\log^3 x)$ as $x \to +\infty$.*

(iii) *If we replace $k!$ in Conjecture* 1.1(ii) *by $(k+1)!$ or $(2k)!$, then the modified $t(n)$ is always a prime.*

Remark 5.1. It seems that if we replace $\binom{2k}{k}$ in the definition of $s(n)$ by $2^{k!}$ or $2^k!$ or 2^{2^k} then the modified $s(n)$ also takes only prime values.

Conjecture 5.2. *Let n be a positive integer.*

(i) *The least integer $m > 1$ such that $|\{(k^2-k)! \bmod m :\ k = 1, \ldots, n\}| = n$ is a prime in the interval $((n-1)(n-2), n(n-1))$ for every $n = 3, 4, \ldots$.*

(ii) *The least integer $m > 1$ such that $n! \not\equiv k! \pmod m$ for all $0 < k < n$ is a prime not exceeding $2n$ except for $n = 4, 6$.*

Remark 5.2. For any positive integer n, the interval $[n, 2n]$ contains at least a prime by the Bertrand Postulate proved by Chebyshev, but Legendre's conjecture that $(n^2, (n+1)^2)$ contains a prime remains unsolved.

Conjecture 5.3. *Let $a \in \mathbb{Z}$ with $|a| > 1$. For $n \in \mathbb{Z}^+$ define $f_a(n)$ as the least integer $m > 1$ such that those a^k $(k = 1, \ldots, n)$ are pairwise distinct modulo m. Then there is a positive integer $n_0(a)$ such that for any integer $n \geqslant n_0(a)$, the number $f_a(n)$ is the least prime $p > n$ having a as a primitive root modulo p if a is not a square, and $f_a(n)$ is the least prime $p > 2n$ such that $a, a^2, \ldots, a^{(p-1)/2}$ are pairwise distinct modulo p if a is a square. In particular, we may take $n_0(-2) = 3$, $n_0(-3) = n_0(5) = 1$, and $n_0(9) = n_0(25) = 2$.*

Let A and B be integers. The Lucas sequence $u_n = u_n(A, B)$ $(n \in \mathbb{N} = \{0, 1, 2, \ldots\})$ and its companion sequence $v_n = v_n(A, B)$ $(n \in \mathbb{N})$ are defined as follows:

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

and

$$v_0 = 2,\ v_1 = A,\ \text{and}\ v_{n+1} = Av_n - Bv_{n-1}\ (n = 1, 2, 3, \ldots).$$

It is well known that

$$(\alpha - \beta)u_n = \alpha^n - \beta^n \quad \text{and} \quad v_n = \alpha^n + \beta^n \quad \text{for all } n \in \mathbb{N},$$

where $\alpha = (A + \sqrt{\Delta})/2$ and $\beta = (A - \sqrt{\Delta})/2$ are the two roots of the equation $x^2 - Ax + B = 0$ with $\Delta = A^2 - 4B$. It is also known that if p is an odd prime not dividing B then $p \mid u_{p-(\frac{\Delta}{p})}$ (see, e.g., [S06]), where $(-)$ is the Legendre symbol. Note that

$$u_{2n} = u_n v_n = Au_n(A^2 - 2B, B^2) \quad \text{and} \quad v_{2n} = v_n(A^2 - 2B, B^2)$$

for all $n \in \mathbb{N}$. Those $F_n = u_n(1, -1)$ and $L_n = v_n(1, -1)$ are Fibonacci numbers and Lucas numbers respectively, and also $F_{2n} = u_n(3, 1)$ and $L_{2n} = v_n(3, 1)$.

Clearly an integer a is a primitive root modulo an odd prime p if and only if those $v_k(a + 1, a) = a^k + 1$ $(k = 1, ..., p - 1)$ are pairwise distinct modulo p. Motivated by the Artin conjecture, we raise the following new conjecture.

Conjecture 5.4. *Let A be an integer with $|A| > 2$.*

(i) *If $2+A$ is not a square, then there are infinitely many odd primes $p \nmid A^2-4$ such that those $v_k(A, 1) \bmod p$ for $k = 1, ..., (p-(\frac{A^2-4}{p}))/2$ are pairwise distinct.*

(ii) *If $2 - A$ is not a square, then there are infinitely many odd primes $p \nmid A^2 - 4$ such that those $u_k(A, 1) \bmod p$ for $k = 1, ..., (p - (\frac{A^2-4}{p}))/2$ are pairwise distinct.*

Inspired by Conjecture 5.3, we pose the following challenging conjecture which implies part (i) of Conjecture 5.4.

Conjecture 5.5. *Let A be an integer with $|A| > 2$. For $n \in \mathbb{Z}^+$ define $t_A(n)$ as the smallest integer $m > 1$ such that those $v_k(A, 1) \bmod m$ for $k = 1, \ldots, n$ are pairwise distinct. Then $t_A(n)$ is prime for any sufficiently large integer n ($n > 2|A|$ might suffice). When $A+2$ is not a square, there is a positive integer $N_0(A)$ such that for any integer $n \geqslant N_0(A)$, the number $t_A(n)$ is the smallest odd prime $p \nmid A^2 - 4$ such that $p - (\frac{A^2-4}{p}) \geqslant 2n$ and those $v_k(A, 1) \bmod p$ $(k = 1, \ldots, (p - (\frac{A^2-4}{p}))/2)$ are pairwise distinct. In particular, we may take $N_0(3) = 6$, $N_0(-3) = 7$, and $N_0(\pm 4) = N_0(\pm 10) = 3$.*

Remark 5.3. Note that $v_k(3, 1) = L_{2k}$ and $v_k(-3, 1) = (-1)^k L_{2k}$ for any $k \in \mathbb{Z}^+$. Also, [S02] contains the congruence

$$T_{(p-(\frac{3}{p}))/2} \equiv 2\left(\frac{6}{p}\right) \pmod{p^2} \quad \text{for any prime } p > 3,$$

where $T_n := v_n(4, 1)$.

Recall that S_n denotes the sum of the first n primes. Our following conjecture is a refinement of the Artin conjecture.

Conjecture 5.6. *If $a \in \mathbb{Z}$ is neither -1 nor a square, then there is a positive integer n_0 such that for any integer $n \geqslant n_0$ the least integer $m > 1$ such that $|\{a^{S_k} \bmod m:\ k = 1, \ldots, n\}| = n$ is a prime p having a as a primitive root modulo p. In particular, we may take $n_0 = 1$ for $a = -3$.*

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

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

It is well known that $E_{2n+1} = 0$ for all $n \in \mathbb{N}$ and

$$\sec x = \sum_{n=0}^{\infty} (-1)^n E_{2n} \frac{x^{2n}}{(2n)!} \quad \left(|x| < \frac{\pi}{2}\right).$$

Conjecture 5.7. (i) *For $n \in \mathbb{Z}^+$ let $e(n)$ be the least integer $m > 1$ such that E_{2k} $(k = 1, \ldots, n)$ are pairwise distinct modulo m. Then we have $e(n) = 2^{\lceil \log_2 n \rceil + 1}$ with the only exceptions as follows:*

$$\begin{aligned} &e(3) = 7,\ e(5) = e(6) = 13,\ e(9) = e(10) = 25,\ e(17) = 47,\\ &e(18) = e(19) = e(20) = e(21) = 7^2, \quad e(65) = \cdots = e(78) = 13^2,\\ &e(1025) = e(1026) = e(1027) = e(1028) = e(1029) = e(1030) = 5^5. \end{aligned}$$

(ii) *For $n \in \mathbb{Z}^+$ let $e^*(n)$ be the least integer $m > 1$ such that $2E_{2n} \not\equiv 2E_{2k} \pmod{m}$ for all $0 < k < n$. Then $e^*(n)$ is a prime in the interval $[2n, 3n]$ with the only exceptions as follows:*

$$e^*(4) = 13,\ e^*(7) = 23,\ e^*(10) = 5^2,\ e^*(55) = 11^2.$$

Remark 5.4. With the help of the Stern congruence for Euler numbers (see, e.g., S. S. Wagstaff [W] and the author [S05]), we can easily show that $\log_2 e(n) \leqslant \lceil \log_2 n \rceil + 1$. Also, it is known (cf. [B]) that for any $n \in \mathbb{Z}^+$ the interval $[2n, 3n]$ contains at least a prime.

Acknowledgments. The author would like to thank Prof. N. Koblitz, C. Pomerance, P. Moree, and Dr. O. Gerard and H. Pan, and the referee for their helpful comments.

References

[ABM] L. K. Arnold, S. J. Benkoski and B. J. McCabe, *The discriminator (a simple application of Bertrand's postulate)*, Amer. Math. Monthly **92** (1985), 275–277.

[B] M. El Bachraoui, *Primes in the interval* $[2n, 3n]$, Int. J. Contemp. Math. Sci. **1** (2006), 617–621.

[BSW] P. S. Bremser, P. D. Schumer and L. C. Washington, *A note on the incongruence of consecutive integers to a fixed power*, J. Number Theory **35** (1990), 105–108.

[Br] R. Breusch, *Zur Verallgemeinerung des Bertrandschen Postulates, dass zwischen x und $2x$ stets Primzahlen liegen*, Math. Z. **34** (1932), 505–526.

[CP] R. Crandall and C. Pomerance, *Prime Numbers: A Computational Perspective*, 2nd Edition, Springer, New York, 2005.

[D] P. Dusart, *The kth prime is greater than $k(\log k + \log\log k - 1)$ for $k \geqslant 2$*, Math. Comp. **68** (1999), 411–415.

[H] W. B. Hart, *Re: A new conjecture on primes*, a message to Number Theory List, April 14, 2012. `http://listserv.nodak.edu/cgi-bin/wa.exe?A2=NMBRTHRY;57b2e5f8.1204`.

[IR] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory, 2nd Edition*, Springer, New York, 1990.

[Mi] W. H. Mills, *A prime-representing function*, Bull. Amer. Math. Soc. **53** (1947), 604.

[MV] H. Montgomery and R. Vaughan, *The large sieve*, Mathematica **20** (1973), 119–134.

[MM] P. Moree and G. L. Mullen, *Dickson polynomial discriminators*, J. Number Theory **59** (1996), 88–105.

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

[N] J. Nagura, *On the interval containing at least one prime number*, Proc. Japan Acad. Ser. A **28** (1952), 177–181.

[RR] O. Ramaré and R. Rumely, *Primes in arithmetic progressions*, Math. Comp. **65** (1996), 397–425.

[SC] N.J.A. Sloane and J. H. Conway, Sequence A008347 in OEIS (On-Line Encyclopedia of Integer Sequences), `http://oeis.org/A008347`.

[S02] Z. W. Sun, On the sum $\sum_{k\equiv r\,(\mathrm{mod}\ m)}\binom{n}{k}$ and related congruences, Israel J. Math. **128** (2002), 135–156.

[S05] Z. W. Sun, *On Euler numbers modulo powers of two*, J. Number Theory **115** (2005), 371–380.

[S06] Z. W. Sun, *Binomial coefficients and quadratic fields*, Proc. Amer. Math. Soc. **134** (2006), 2213–2222.

[S12a] Z. W. Sun, *A function taking only prime values*, a message to Number Theory List on Feb. 21, 2012. `http://listserv.nodak.edu/cgi-bin/wa.exe?A2=ind1202&L=NMBRTHRY&T=0&P=4035`.

[S12b] Z. W. Sun, Sequence A208494 in OEIS (On-Line Encyclopedia of Integer Sequences), posted in Feb. 2012, `http://oeis.org/A208494`.

[S12c] Z. W. Sun, Sequences A210144 and A210186 in OEIS (On-Line Encyclopedia of Integer Sequences), posted in March 2012, `http://oeis.org`.

[S13] Z. W. Sun, Sequences A222579 and A222580 in OEIS (On-Line Encyclopedia of Integer Sequences), posted in Feb. 2013, `http://oeis.org`.

[W] S. S. Wagstaff, Jr., *Prime divisors of the Bernoulli and Euler numbers*, in: Number Theory for the Millennium, III (Urbana, IL, 2000), 357–374, A K Peters, Natick, MA, 2002.

[Z] M. Zieve, *A note on the discriminator*, J. Number Theory **73** (1998), 122–138.