ACTA ARITHMETICA
126.3 (2007)

Compact integers and factorials

by

VLADIMIR SHEVELEV (Beer-Sheva)

1. Introduction. In [7], it was asked whether for every fixed positive integer k there exists a positive integer n so that, in the prime power factorization of $n!$, the first k primes appear with even exponents. This question was answered in the affirmative by D. Berend in [3]. In fact, Berend proved more in two aspects. First, he proved that, for arbitrary fixed $k, d \in \mathbb{N}$, there exist infinitely many numbers n so that, in the prime factorization of $n!$, the first k primes appear with exponents divisible by d. In particular, all these exponents may be divisible by 2^m for an arbitrary m. Secondly, he proved that, for fixed $k \geq 1$ and $d \geq 2$, there exists a computable constant $C(k, d)$, depending only on k, d, such that every interval of length $C(k, d)$ of positive numbers contains a positive integer n with the above property. Some natural extensions of Berend's results were obtained in [5], [6], [9], [13].

In this paper we consider factorials whose factorization

$$n! = 2^{e_2(n)} 3^{e_3(n)} \cdots p_k^{e_{p_k}(n)}$$

is special from the point of view of one or more primes. It is easy to show that $e_2(n)$ is a power of 2 infinitely often. This raises the following questions.

QUESTION 1. *Let p be any odd prime. Is $e_p(n)$ a power of 2 infinitely often?*

It is plausible that the answer is affirmative. However, we have not been able to prove this. Most of this paper is devoted to the following question and related issues.

QUESTION 2. *Let p be any odd prime. Do there exist infinitely many positive integers n for which both $e_2(n)$ and $e_p(n)$ are powers of 2?*

2000 *Mathematics Subject Classification*: Primary 11A51; Secondary 11B65, 11D61, 11N05.

Key words and phrases: factorization of factorials, square-free integers, diophantine equations, distribution of primes in short intervals.

The article is partly supported by a grant of the Gil'adi Foundation of the Israeli Ministry of Absorption.

One of the main results of this paper is that the answer here is negative. We mention that this result is almost trivial for non-Fermat primes, but is trickier for Fermat primes.

Our results may be reformulated using Fermi–Dirac arithmetic ([14]). In this arithmetic, the role of primes in classical arithmetic is played by the multiplicative basis of so-called FD-primes,

$$Q = \{p^{2^{k-1}} : p \in P,\ k \in \mathbb{N}\} = \{2, 3, 4, 5, 7, 9, 11, 13, 16, 17, \ldots\},$$

where P denotes the set of all primes. Every positive integer $n \geq 2$ may be written uniquely in the form $n = q_1 \cdots q_k$, where $q_1, \ldots, q_k$ are distinct FD-primes, and we shall write $Q_n = \{q_1, \ldots, q_k\}$ in this case. We put $Q_1 = \emptyset$.

Definition 1. A positive integer n is *compact* if all elements of Q_n are relatively prime.

Denote the set of all compact numbers by C. It is convenient to suppose that $1 \in C$. In Theorem 1 we find the density of the set C, along with an error term for its counting function.

It is easy to see that the set

$$C^! = \{n \in \mathbb{N} : n! \in C\}$$

is finite. In fact, if n is sufficiently large, then the interval $(n/4, n/3)$ contains a prime p, and it is easy to verify that $p^3 \parallel n!$, i.e. $e_p(n) = 3$. Below we obtain the following result: $C^! = \{1, 2, 3, 6, 7, 10, 11\}$.

Definition 2. Let p be a fixed prime. A positive integer n divisible by p is *p-compact* if the set Q_n contains a single power of p.

Denote the set of p-compact numbers by C_p and put

$$C_p^! = \{n \in \mathbb{N} : n! \in C_p\}.$$

Our answer to Question 2 may be rephrased as the statement that, for each prime $p \geq 3$ the set $C_2^! \cap C_p^!$ is finite. Moreover, we obtain an explicit formula for $|C_2^! \cap C_p^!|$. In our approach, we are led to consider various exponential diophantine equations. Our formula for the size of $C_2^! \cap C_p^!$ also allows us to compute the lower and upper densities of those sets of primes for which this size assumes any specific value. Moreover, we obtain an estimate for the least prime for which this set is of some given size. Our estimates depend on the up-to-date results regarding the number of primes in short intervals.

In Section 2 we present the main results. Sections 3–8 are devoted to the proofs. In Section 9 we provide some numerical results. Finally, in Section 10 we pose several questions for further research.

2. The main results. Let

$$c(x) = \sum_{i \le x,\, i \in C} 1, \qquad c_p(x) = \sum_{i \le x,\, i \in C_p} 1.$$

THEOREM 1.

(i) *For every* $x \ge 1$,

$$c(x) = \lambda x + R(x),$$

where

$$\lambda = \frac{6}{\pi^2} \prod_{p \in P} \left(1 + \frac{1}{p+1} \sum_{i=1}^{\infty} p^{-(2^i - 1)}\right) = 0.872497\ldots,$$

$$|R(x)| \le \begin{cases} k_1(\log x + k_2)\sqrt{x} & \text{if } x \le 4 \cdot 10^{19}, \\ k_1\left(\log x + k_2 + e^{k_3 \frac{\sqrt{\log x}}{\log\log\sqrt{x}}} \log \dfrac{x}{4 \cdot 10^{19}}\right)\sqrt{x} & \text{if } x > 4 \cdot 10^{19}, \end{cases}$$

with $k_1 = 28.841303\ldots$, $k_2 = 0.152970\ldots$, $k_3 = 5.263054\ldots$.

(ii) *For any fixed prime* p,

$$c_p(x) = \beta_p x + O(\log\log x)$$

with the constant in $O(\ldots)$ *equal to* $1/\log 2$, *where*

$$\beta_p = \frac{p-1}{p} \sum_{i=0}^{\infty} p^{-2^i}.$$

THEOREM 2.

$$|C_2^! \cap C_q^!| = \begin{cases} 7, & q = 3,\ q = 5, \\ 6, & q = 7, \\ 5, & q = (2^{4k+1} + 3)/5,\ \ k \ge 2, \\ 4, & q = 2^{2^{k-1}} + 1,\ \ k \ge 3, \\ 3, & q = 2^k + 3,\ \ k \ge 3, \\ 2\left(1 + \left\lfloor \log_2 \dfrac{q-5}{2^k - q} \right\rfloor\right), & 2^{k-1} + 3 < q \le 2^k - 1,\ \ k \ge 4, \\ & q \ne (2^{k+2} + 3)/5. \end{cases}$$

THEOREM 3. *For a fixed* $t \in \mathbb{N}$,

$$|\{q \in P,\, q \le 2^m : |C_2^! \cap C_q^!| = 2t\}| \sim \frac{2^t}{(2^{t-1} + 1)(2^t + 1)}\, \pi(2^m);$$

moreover,

$$\limsup_{n \to \infty} \frac{|\{q \in P,\, q \le n : |C_2^! \cap C_q^!| = 2t\}|}{\pi(n)} = \frac{1}{2^{t-1} + 1},$$

$$\liminf_{n \to \infty} \frac{|\{q \in P,\, q \le n : |C_2^! \cap C_q^!| = 2t\}|}{\pi(n)} = \frac{1}{2^t + 1}.$$

THEOREM 4. *For sufficiently large k, as q varies over $(2^{k-1}+3, 2^k-1)$:*

(i) *$|C_2^! \cap C_q^!|$ assumes all even values in the interval $[2, 0.95k-2]$;*

(ii) *the number of primes $q \in (2^{k-1}+3, 2^k-1)$ for which $|C_2^! \cap C_q^!| = 2t$ with $t \in [1, 0.475k-1]$ is not less than*

$$\frac{0.09}{\log 2}\,\frac{2^{0.525(k-1)}}{k}.$$

REMARK 1. The proof depends on the estimates regarding the number of primes in short intervals [2]. Improvements in these estimates will imply corresponding improvements in Theorem 4, namely that $|C_2^! \cap C_q^!|$ assumes all even values in a larger interval.

For a given $t \in \mathbb{N}$ consider the function

$$q(t) = \min\{q \in P : |C_2^! \cap C_q^!| = 2t\}.$$

THEOREM 5. *For sufficiently large t,*

$$2^t - 1 \le q(t) \le 2^{\lceil 40t/19 \rceil}.$$

REMARK 2. Similarly to Remark 1 improvements in the above mentioned estimates will imply corresponding improvements of the upper bound for $q(t)$.

3. Proof of Theorem 1. Let r be a fixed square-free number. Consider the auxiliary function $\beta_r(x)$, defined as the number of positive integers not exceeding x, not divisible by the square of any prime, except perhaps the prime divisors of r.

LEMMA 1. *For every $x \ge 1$,*

$$\beta_r(x) = \frac{6}{\pi^2}\prod_{p|r}\left(1-\frac{1}{p^2}\right)^{-1} x + \varrho(x),$$

where $|\varrho(x)| \le 3.5\sqrt{x}$.

Proof. By inclusion-exclusion

$$\beta_r(x) = \lfloor x \rfloor - \sum_{\substack{p \le x \\ p \nmid r}} \left\lfloor \frac{x}{p^2} \right\rfloor + \sum_{\substack{p<q\le x \\ p,q \nmid r}} \left\lfloor \frac{x}{p^2q^2} \right\rfloor - \cdots \tag{1}$$

$$= \sum_{i \le x} \sum_{\substack{d^2 | i \\ (d,r)=1}} \mu(d) = \sum_{\substack{d \le \sqrt{x} \\ (d,r)=1}} \mu(d) \sum_{\substack{i \le x \\ d^2 | i}} 1$$

$$= \sum_{\substack{d \le \sqrt{x} \\ (d,r)=1}} \mu(d) \left\lfloor \frac{x}{d^2} \right\rfloor = x \sum_{\substack{d \le \sqrt{x} \\ (d,r)=1}} \frac{\mu(d)}{d^2} + R(x),$$

where

$$|R(x)| \le \frac{1}{2} \sum_{d \le \sqrt{x}} |\mu(d)| + o(\sqrt{x}) = \frac{1}{2}\beta_1(\sqrt{x}) + o(\sqrt{x}). \tag{2}$$

The coefficient 1/2 in (2) follows from the well known estimate $|\sum_{n\le x}\mu(n)| = o(x)$ (see [17]). Now

$$\begin{aligned}\sum_{\substack{d=1\\(d,r)=1}}^{\infty} \frac{\mu(d)}{d^2} &= \prod_{\substack{p\in P\\ p\nmid r}}\Big(1-\frac{1}{p^2}\Big) = \prod_{p\in P}\Big(1-\frac{1}{p^2}\Big)\prod_{p\mid r}\Big(1-\frac{1}{p^2}\Big)^{-1}\\ &= \frac{6}{\pi^2}\prod_{p\mid r}\Big(1-\frac{1}{p^2}\Big)^{-1},\end{aligned}$$

and therefore

$$\sum_{\substack{d\le\sqrt{x}\\(d,r)=1}} \frac{\mu(d)}{d^2} = \frac{6}{\pi^2}\prod_{p\mid r}\Big(1-\frac{1}{p^2}\Big)^{-1} - \sum_{\substack{d>\sqrt{x}\\(d,r)=1}} \frac{\mu(d)}{d^2}. \tag{3}$$

We estimate the second term on the right-hand side trivially:

$$\Big|\sum_{\substack{d>\sqrt{x}\\(d,r)=1}} \frac{\mu(d)}{d^2}\Big| \le \sum_{d\ge\lfloor\sqrt{x}\rfloor+1}\frac{1}{d^2} \le \int_{\lfloor\sqrt{x}\rfloor}^{\infty}\frac{dt}{t^2} = \frac{1}{\lfloor\sqrt{x}\rfloor}. \tag{4}$$

It is easy to see that $\sup_{x\ge1}\sqrt{x}/\lfloor\sqrt{x}\rfloor = \sqrt{3.99\ldots}/1 = 2$. So, by (4),

$$x\Big|\sum_{\substack{d>\sqrt{x}\\(d,r)=1}} \frac{\mu(d)}{d^2}\Big| \le 2\sqrt{x}. \tag{5}$$

Taking into account that in (2) $o(\sqrt{x}) \le \sqrt{x}$ for $x \ge 1$, by (1)–(5), for every x we have

$$\beta_r(x) = \frac{6}{\pi^2}\prod_{p\mid r}\Big(1-\frac{1}{p^2}\Big)^{-1} x + \varrho(x)$$

where $|\varrho(x)| \le \sqrt{x}(1/2+1+2) = 3.5\sqrt{x}$. ■

REMARK 3. It follows from the proof of Lemma 1 that for x large enough we have $\varrho(x) \le (1 + 3/\pi^2 + \varepsilon)\sqrt{x}$.

For a fixed square-free number r, denote by B_r the set of square-free numbers n for which $(n, r) = 1$, and put

$$b_r(x) = |B_r \cap \{1, 2, \ldots, x\}|.$$

In particular, $B = B_1$ is the set of all square-free numbers.

Lemma 2.
$$b_r(x) = \frac{6r}{\pi^2}\prod_{p|r}(p+1)^{-1}x + R_r(x),$$
where for every $x \geq 1$ *and every* $r \in B$,
$$|R_r(x)| \leq \begin{cases} 57.682607\ldots\sqrt{x} & \text{if } r \leq N, \\ 57.682607\ldots e^{7.443083\ldots\frac{\sqrt{\log r}}{\log\log r}}\sqrt{x} & \text{if } r \geq N+1, \end{cases}$$
where $N = 6469693229$.

Proof. Consider the function $\lambda : P \to \{1,2\}$ defined by
$$\lambda(p) = \begin{cases} 1, & p \mid r, \\ 2, & p \nmid r. \end{cases}$$
By inclusion-exclusion
$$b_r(x) = \lfloor x\rfloor - \sum_{p\leq x}\left\lfloor \frac{x}{p^{\lambda(p)}}\right\rfloor + \sum_{p<q\leq x}\left\lfloor \frac{x}{p^{\lambda(p)}q^{\lambda(p)}}\right\rfloor - \cdots, \tag{6}$$
where all sums are over primes only. It follows from (6) that
$$\begin{aligned}
b_r(x) = &\Bigg(\lfloor x\rfloor - \sum_{\substack{p\leq x\\ p\nmid r}}\left\lfloor\frac{x}{p^2}\right\rfloor + \sum_{\substack{p<q\leq x\\ p,q\nmid r}}\left\lfloor\frac{x^2}{p^2q^2}\right\rfloor - \cdots\Bigg)\\
&- \sum_{p_1|r}\Bigg(\left\lfloor\frac{x}{p_1}\right\rfloor - \sum_{\substack{p\leq x\\ p\nmid r}}\left\lfloor\frac{x}{p_1}/p^2\right\rfloor + \sum_{\substack{p<q\leq x\\ p,q\nmid r}}\left\lfloor\frac{x}{p_1}/p^2q^2\right\rfloor - \cdots\Bigg)\\
&+ \sum_{p_1<p_2\colon p_1p_2|r}\Bigg(\left\lfloor\frac{x}{p_1p_2}\right\rfloor - \sum_{\substack{p\leq x\\ p\nmid r}}\left\lfloor\frac{x}{p_1p_2}/p^2\right\rfloor + \sum_{\substack{p<q\leq x\\ p,q\nmid r}}\left\lfloor\frac{x}{p_1p_2}/p^2q^2\right\rfloor - \cdots\Bigg)\\
&- \cdots\\
= &\sum_{d|r}\mu(d)\beta_r\left(\frac{x}{d}\right).
\end{aligned}$$
Therefore, by Lemma 1,
$$\begin{aligned}
b_r(x) &= \frac{6}{\pi^2}\prod_{p|r}\left(1-\frac{1}{p^2}\right)^{-1}x\sum_{d|r}\frac{\mu(d)}{d} + R_r(x)\\
&= \frac{6}{\pi^2}\prod_{p|r}\left(1-\frac{1}{p^2}\right)^{-1}\prod_{p|r}\left(1-\frac{1}{p}\right)x + R_r(x)\\
&= \frac{6}{\pi^2}\prod_{p|r}\frac{p}{p+1}x + R_r(x) = \frac{6r}{\pi^2}\prod_{p|r}(p+1)^{-1}x + R_r(x),
\end{aligned} \tag{7}$$

where

$$|R_r(x)| \le 3.5\sqrt{x}\sum_{d|r}\frac{1}{\sqrt{d}} = 3.5\prod_{p|r}\Big(1+\frac{1}{\sqrt{p}}\Big)\sqrt{x}. \tag{8}$$

Let $w(r)$ denote the number of prime divisors of r. If $w(r) \le 9$, then

$$\prod_{p|r}\Big(1+\frac{1}{\sqrt{p}}\Big) \le \prod_{2\le p\le 23}\Big(1+\frac{1}{\sqrt{p}}\Big) = 16.480745\ldots.$$

If $w(r) \ge 10$, then $r \ge \prod_{2\le p\le 29} p = 6469693230$. Put $m = p_{w(r)} \ge 29$.

For $m \ge 29$, as is well known (cf. [16]), $\prod_{2\le p\le m} p > 2^m$. Therefore, if $w(r) \ge 10$, then $2^m < \prod_{p|r} p = r$, i.e. $m < \log_2 r$. Taking into account that the nth prime satisfies $p_n \ge n\log n$, and $\pi(m) \le 1.6m/\log m$ for every $m \ge 2$ (cf. [16]), we have

$$\begin{aligned}\log\prod_{p|r}\Big(1+\frac{1}{\sqrt{p}}\Big) &- \log\prod_{p\le 23}\Big(1+\frac{1}{\sqrt{p}}\Big) \\ &\le \log\prod_{p\le m}\Big(1+\frac{1}{\sqrt{p}}\Big) - \log\prod_{p\le 23}\Big(1+\frac{1}{\sqrt{p}}\Big) \le \sum_{29\le p\le m}\frac{1}{\sqrt{p}} \\ &= \sum_{n\,:\,29\le p_n\le m}\frac{1}{\sqrt{p_n}} \le \sum_{n=10}^{\pi(m)}\frac{1}{\sqrt{n\log n}} \\ &\le \int_9^{1.6m/\log m}\frac{dt}{\sqrt{t\log t}} = \int_9^{1.6m/\log m}\frac{t^{1/4}}{\sqrt{\log t}}\,\frac{dt}{t^{3/4}}.\end{aligned} \tag{9}$$

Notice that for $t > e^2$ the function $t^{1/4}/\sqrt{\log t}$ increases. Therefore, since for $m \ge 9$ we have $\log\log m < \frac{1}{3}\log(1.6m)$,

$$\begin{aligned}\log\prod_{p|r}\Big(1+\frac{1}{\sqrt{p}}\Big) &- \log 16.480745\ldots \\ &\le \Big(1.6\,\frac{m}{\log m}\Big)^{1/4}(\log 1.6+\log m-\log\log m)^{-1/2}\int_9^{1.6m/\log m}\frac{dt}{t^{3/4}} \\ &\le 4\Big(1.6\,\frac{m}{\log m}\Big)^{1/2}\Big(\frac{2}{3}\log m\Big)^{-1/2} \\ &= 4\sqrt{24}\,\frac{m^{1/2}}{\log m} < 4\sqrt{\frac{2.4}{\log 2}}\,\frac{\sqrt{\log r}}{\log\log r}.\end{aligned}$$

Thus, for $N = 6469693229$ and every $r \in B$,

$$\prod_{p|r}\left(1+\frac{1}{\sqrt{p}}\right) \le \begin{cases} 16.480745\ldots & \text{if } r \le N, \\ 16.480745\ldots e^{7.443083\ldots\frac{\sqrt{\log r}}{\log\log r}} & \text{if } r \ge N+1. \end{cases}$$

By (7) and (8) we obtain the conclusion of the lemma. ∎

Now we can complete the proof of Theorem 1(i). Let $a \ge 1$ be a compact number. Denote by $r(a)$ the product of all prime divisors of a; set $r(1) = 1$. Consider, further, the subset $C^{(a)}$ of the compact numbers of the form $a^2 s$, where $a \in C$ and $s \in B_{r(a)}$. It is evident that, if $a_1 \ne a_2$, then $C^{(a_1)} \cap C^{(a_2)} = \emptyset$, and therefore $C = \bigcup_{a\in C} C^a$, where the union is disjoint. Consequently, by Lemma 2,

$$\begin{aligned} (10) \qquad c(x) &= b_1(x) + \sum_{2\le a\le\sqrt{x},\, a\in C} b_r(a)\left(\frac{x}{a^2}\right) \\ &= \frac{6}{\pi^2}\Bigg(1+\sum_{\substack{2\le a\le\sqrt{x}\\ a\in C}}\prod_{p|r(a)}\left(1-\frac{1}{p+1}\right)\frac{1}{a^2}\Bigg)x + R^*(x), \end{aligned}$$

where

$$\begin{aligned} |R^*(x)| &\le 3.5\sqrt{x} + \sum_{\substack{2\le a\le\sqrt{x}\\ a\in C}}\left|R_{r(a)}\left(\frac{x}{a^2}\right)\right| \\ &\le 3.5\sqrt{x} + \sum_{\substack{2\le a\le\sqrt{x}\,:\, r(a)=N\\ a\in C}}\left|R_{r(a)}\left(\frac{x}{a^2}\right)\right| + \sum_{\substack{a\le\sqrt{x}\,:\, r(a)\ge N+1\\ a\in C}}\left|R_{r(a)}\left(\frac{x}{a^2}\right)\right| \end{aligned}$$

with $N = 6469693229$. Therefore, if $x \le N^2$, then

$$|R^*(x)| \le (3.5 + k_1\log x)\sqrt{x},$$

where $k_1 = 28.841303\ldots$. If $x > N^2$, then

$$\begin{aligned} |R^*(x)| &\le (3.5 + k_1\log x)\sqrt{x} \\ &\quad + k_1\sqrt{x}\sum_{\substack{a\le\sqrt{x}\,:\, r(a)\ge N+1\\ a\in C}}\frac{1}{a}\, e^{7.443083\ldots\frac{\sqrt{\log r(a)}}{\log\log r(a)}}, \end{aligned}$$

where the last sum does not exceed

$$\sum_{N+1\le a\le\sqrt{x}\,:\, r(a)\ge N+1}\frac{1}{a}\, e^{7.443083\ldots\frac{\sqrt{\log a}}{\log\log a}} \le e^{k_3\frac{\sqrt{\log x}}{\log\log\sqrt{x}}}\log\frac{\sqrt{x}}{N}$$

with $k_3 = 7.443083/\sqrt{2} = 5.263054\ldots$.

Moreover, if we replace in (10) the sum $\sum_{a\le\sqrt{x},\, a\in C}$ by $\sum_{a\in C}$, then the error does not exceed (see (4))

$$\frac{6x}{\pi^2}\sum_{n>\sqrt{x}}\frac{1}{n^2}\le\frac{6}{\pi^2}\left(\sup_{x\ge 4}\frac{\sqrt{x}}{\lfloor\sqrt{x}\rfloor}\right)\sqrt{x}=\frac{6}{\pi^2}\,\frac{\sqrt{8.999\dots}}{2}\,\sqrt{x}=0.911890\dots\sqrt{x}.$$

Thus,

$$c(x)=\frac{6x}{\pi^2}\sum_{a\in C}\prod_{p\mid r(a)}\left(1-\frac{1}{p+1}\right)\frac{1}{a^2}+R(x), \tag{11}$$

where $R(x)=R^*(x)+0.911890\dots\sqrt{x}$. Hence

$$|R(x)|\le\begin{cases} k_1(\log x+k_2)\sqrt{x} & \text{if } x\le N^2,\\ k_1\left(\log x+k_2+e^{k_3\frac{\sqrt{\log x}}{\log\log\sqrt{x}}}\log\dfrac{x}{N^2}\right)\sqrt{x} & \text{if } x>N^2,\end{cases} \tag{12}$$

with $N=6469693229$, $k_1=28.841303\dots$, $k_2=(3.5+0.911890\dots)/k_1=0.152970\dots$, $k_3=5.263054\dots$.

It remains to evaluate the sum (11). For a fixed $l\in B$, denote by $C(l)$ the set of all compact numbers a with $r(a)=l$. By (11),

$$c(x)=\frac{6x}{\pi^2}\sum_{l\in B}\prod_{p\mid l}\left(1-\frac{1}{p+1}\right)\sum_{a\in C(l)}\frac{1}{a^2}+R(x). \tag{13}$$

Consider the function $A:\mathbb{N}\to\mathbb{R}$ given by

$$A(l)=\begin{cases}\displaystyle\sum_{a\in C(l)}1/a^2, & l\in B,\\ 0, & l\notin B.\end{cases}$$

It is evident that, if $l_1,l_2\in B$ and $(l_1,l_2)=1$, then

$$A(l_1l_2)=\sum_{a\in C(l_1l_2)}\frac{1}{a^2}=\sum_{a\in C(l_1)}\frac{1}{a^2}\sum_{a\in C(l_2)}\frac{1}{a^2}=A(l_1)A(l_2).$$

It follows that $A(l)$ is a multiplicative function. Hence the function f defined by

$$f(l)=\prod_{p\mid l}\left(1-\frac{1}{p+1}\right)A(l)$$

is also multiplicative. Consequently ([4, p. 103]),

$$\sum_{n=1}^{\infty}f(n)=\prod_{p\in P}(1+f(p)+f(p^2)+\cdots). \tag{14}$$

Since $f(p^k) = 0$ for $k \geq 2$, by (13) we have

$$\begin{aligned} c(x) &= \frac{6x}{\pi^2} \sum_{l=1}^{\infty} f(l) + R(x) = \frac{6x}{\pi^2} \prod_{p \in P} (1 + f(p)) + R(x) \\ &= \frac{6x}{\pi^2} \prod_{p \in P} \left(1 + \left(1 - \frac{1}{p+1}\right)\left(\frac{1}{p^2} + \frac{1}{p^4} + \frac{1}{p^8} + \cdots\right)\right) + R(x) \\ &= \frac{6}{\pi^2} \prod_{p \in P} \left(1 + \frac{1}{p+1}\left(\frac{1}{p} + \frac{1}{p^3} + \frac{1}{p^7} + \frac{1}{p^{15}} + \cdots\right)\right) x + R(x). \end{aligned}$$

Employing the estimate of $R(x)$ given by (12) (with $4 \cdot 10^{19} < N^2$), we obtain assertion (i) of the theorem.

To prove (ii), note that it is evident that

$$\begin{aligned} c_p(n) &= \left(\left\lfloor \frac{n}{p} \right\rfloor - \left\lfloor \frac{n}{p^2} \right\rfloor\right) + \left(\left\lfloor \frac{n}{p^2} \right\rfloor - \left\lfloor \frac{n}{p^3} \right\rfloor\right) + \left(\left\lfloor \frac{n}{p^4} \right\rfloor - \left\lfloor \frac{n}{p^5} \right\rfloor\right) + \cdots \\ &= \left(\left\lfloor \frac{n}{p} \right\rfloor - \left\lfloor \frac{n}{p^3} \right\rfloor\right) + \left(\left\lfloor \frac{n}{p^4} \right\rfloor - \left\lfloor \frac{n}{p^5} \right\rfloor\right) + \cdots . \end{aligned}$$

Let

$$p^{2^{d-1}} \leq n < p^{2^d}, \qquad d \in \mathbb{N}.$$

If $d \geq 2$ we have exactly $d - 1$ nonzero terms in brackets. Since

$$d - 1 \leq \frac{\log\log n - \log\log p}{\log 2},$$

we have

$$c_p(n) = \frac{n}{p} - \frac{n}{p^2} + \frac{n}{p^2} - \frac{n}{p^3} + \cdots + \frac{n}{p^{2^{d-1}}} - \frac{n}{p^{2^d+1}} + O(\log\log n),$$

where the constant in $O(\ldots)$ equals $1/\log 2$. Hence

$$\begin{aligned} c_p(n) &= n\,\frac{p-1}{p}\left(\frac{1}{p} + \frac{1}{p^2} + \frac{1}{p^4} + \cdots + \frac{1}{p^{2^{d-1}}}\right) + O(\log\log n) \\ &= n\,\frac{p-1}{p} \sum_{i=0}^{\infty} p^{-2^i} - n\,\frac{p-1}{p} \sum_{i=d}^{\infty} p^{-2^i} + O(\log\log n), \end{aligned}$$

and it suffices to notice that

$$n\,\frac{p-1}{p} \sum_{i=d}^{\infty} p^{-2^i} < \frac{p-1}{p}\left(1 + \frac{1}{p} + \frac{1}{p^2} + \cdots\right) = 1.$$

This completes the proof. ■

Remark 4. In Theorem 1(i), we can reduce k_3 to $\sqrt{2}+\varepsilon$ (at the expense of enlarging k_1). In fact, for small $\delta > 0$ and large enough $m = m(\delta) = e^{2.25/\delta^2}$, according to B. Rosser [12], $\prod_{2 \leq p \leq m} p > e^{(1-4\delta^2/3)m}$, and we can replace (9) by

$$\log \prod_{p\le m}\left(1+\frac{1}{\sqrt{p}}\right) \le K(\delta) + \int\limits_{e^{1/2\delta}}^{m/(\log m-4)} \frac{t^{\delta}}{\sqrt{\log t}}\,\frac{dt}{t^{1/2+\delta}}, \qquad m > m(\delta)$$

($m(\delta)$ was chosen with something to spare to satisfy the technical inequality $(1-3\delta)\log m < (1-2\delta)((\log m - 4)(\log(\log m - 4)))^{1/2}$). Then we obtain for $x \ge 3$, instead of (12),

$$R(x) \le K_\varepsilon \sqrt{x}\, e^{(\sqrt{2}+\varepsilon)\frac{(\log x)^{1/2}}{\log\log x}} \log x.$$

It can be shown that we can take $K_\varepsilon = e^{e^{21\varepsilon^{-2}}}$.

4. Proof of Theorem 2

4.1. *Auxiliary propositions.* Denote by $\sigma_g(n)$ the sum of digits in the base g representation of $n \in \mathbb{N}$.

LEMMA 3 ([11]).

$$\sigma_g(n) = n - (g-1)\sum_{t\ge 1}\left\lfloor \frac{n}{gt} \right\rfloor, \qquad n \in \mathbb{N}.$$

By Lemma 3 we may express n in terms of $\sigma_p(n)$ and the exponent $e_p(n)$ for which $p^{e_p(n)} \| n!$:

$$n = (p-1)e_p(n) + \sigma_p(n). \tag{15}$$

In [11], the estimate $\sigma_g(n) \le (g-1)\log_g(gn)$ is proved. The following lemma improves this bound, which will be useful later.

LEMMA 4.

$$\sigma_g(n) \le (g-1)\log_g(n+1).$$

Proof. Let $\sigma_g(n) \equiv r \pmod{g-1}$, where $0 \le r \le g-2$. Given any k, the smallest n for which $\sigma_g(n) = (g-1)k + r$ is

$$\begin{aligned} n &= rg^k + (g-1)(g^{k-1} + g^{k-2} + \cdots + 1) = (r+1)g^k - 1 \\ &= (r+1)g^{(\sigma_g(n)-r)/(g-1)} - 1. \end{aligned}$$

Hence for every n we have

$$\sigma_g(n) \le r + (g-1)\log_g(n+1) - (g-1)\log_g(r+1).$$

Now for $r = 0$ the lemma follows directly, while for $r \ge 1$ we have $r \le (g-1)\log(r+1)/\log g$, and so $1 \le r \le g-2$, since $x/\log(x+1)$ increases at least for $x \ge 1$. ∎

From Lemmas 3 and 4 we obtain the following estimate.

COROLLARY 1. *$e_p(n) = n/(p-1) + R_p(n)$, where $-\log_p(n+1) \le R_p(n) < 0$.*

Proposition 1. *For $n \ge 6$ we have $n \in C_2^!$ if and only if there exists an $\alpha \ge 2$ such that $n = 2^\alpha + 2$ or $n = 2^\alpha + 3$.*

Proof. If n is of the required form, then

$$e_2(n) = 2^{\alpha-1} + 1 + 2^{\alpha-2} + \cdots + 1 = 2^\alpha, \qquad \alpha \ge 2,$$

and thus $n \in C_2^!$.

Now assume that $n \in C_2^!$, $n \ge 6$. By (15) there exists some $\alpha \in \mathbb{N}$ so that $e_2(n) = 2^\alpha$ and

$$n = e_2(n) + \sigma_2(n) = 2^\alpha + \sigma_2(n). \tag{16}$$

Further, by Lemma 4,

$$\sigma_2(n) \le \lfloor \log_2(n+1) \rfloor < n/2, \qquad n \ge 6.$$

Therefore, by (16) we have $2^\alpha < n < 2^\alpha + n/2$ and consequently $2^\alpha < n < 2^{\alpha+1}$, so that $\alpha = \lfloor \log_2 n \rfloor$. Taking this into account, we apply σ_2 to both sides of (16):

$$\sigma_2(n) = \sigma_2(2^{\lfloor \log_2 n \rfloor} + \sigma_2(n)). \tag{17}$$

Since $\sigma_2(n) \le 1 + \lfloor \log_2(n) \rfloor < 2^{\lfloor \log_2(n) \rfloor}$, by (17) we have

$$\sigma_2(n) = 1 + \sigma_2(\sigma_2(n)), \qquad n \ge 6. \tag{18}$$

Now by (18), and Lemma 3 for $g = 2$,

$$\sigma_2(n) = 1 + \sigma_2(n) - \sum_{t \ge 1} \left\lfloor \frac{\sigma_2(n)}{2^t} \right\rfloor$$

and therefore $\sum_{t \ge 1} \lfloor \sigma_2(n)/2^t \rfloor = 1$. It follows that $\sigma_2(n) = 2$ or 3, and (16) implies that $n = 2^\alpha + 2$ or $n = 2^\alpha + 3$. ∎

Proposition 2. *If q is an odd prime, then $|C_2^! \cap C_q^!| \ge 2$.*

Proof. If $q = 3$, then $3, 6 \in C_2^! \cap C_3^!$. Let $q \ge 5$. Put $k = \lceil \log_2(q+1) \rceil$. Then $k \ge 3$ and $2^{k-1} + 1 \le q \le 2^k - 1$. If $q = 2^{k-1} + 1$, then by Proposition 1 we have $q + 1$, $q + 2 \in C_2^! \cap C_q^!$. If $q \ge 2^{k-1} + 3$, then $2q \ge 2^k + 6$ and

$$q + 3 \le 2^k + 2 < 2^k + 3 < 2q.$$

Therefore, $\lfloor (2^k + 2)/q \rfloor = \lfloor (2^k + 3)/q \rfloor = 1$, i.e. $2^k + 2$, $2^k + 3 \in C_2^! \cap C_q^!$. ∎

Later we shall see that the minimal q for which $|C_2^! \cap C_q^!| = 2$ is $q = 37$.

Proposition 3. *If $p < q$ are primes so that $(q-1)/(p-1)$ is not a power of 2, then the set $C_p^! \cap C_q^!$ is finite. Moreover, if $n \in C_p^! \cap C_q^!$, then*

$$n < 2\left(1 + \frac{\log 2}{2\log q - 1}\right) q^2 - 1.$$

Proof. We have $(p-1)/\log p < (q-1)/\log q$, whence

$$(p-1)\log_p(n+1) < (q-1)\log_q(n+1), \qquad n \in \mathbb{N}.$$

Therefore, by Lemma 4,

$$\max(\sigma_p(n), \sigma_q(n)) \le (q-1)\log_q(n+1), \tag{19}$$

and we find

$$\frac{n-(q-1)\log_q(n+1)}{n-1} < \frac{n-\sigma_p(n)}{n-\sigma_q(n)} < \frac{n-1}{n-(q-1)\log_q(n+1)}. \tag{20}$$

Notice that the function

$$\gamma_q(x) = \frac{\log_q x}{x+q-2}$$

decreases for $x > \max(q-2, e^2)$. Let α be the positive root of the equation $\log 2 + \alpha/2 - \alpha^2/8 = \alpha \log q$. Then $\alpha < 1$ and we have

$$\log(2+\alpha) = \log 2 + \log\left(1+\frac{\alpha}{2}\right) < \log 2 + \frac{\alpha}{2} - \frac{\alpha^2}{4} + \frac{\alpha^2}{8} = \alpha \log q,$$

i.e. $\log_q(2+\alpha) < \alpha$, and

$$\gamma_q((2+\alpha)q^2) = \frac{2+\log_q(2+\alpha)}{(2+\alpha)q^2+q-2} < \frac{1}{q^2}.$$

Therefore, for $n \ge (2+\alpha)q^2 - 1$ we have $\gamma_q(n+1) < 1/q^2$ and consequently $q\log_q(n+1) < (n+q-1)/q$. By (20),

$$\frac{n-\sigma_p(n)}{n-\sigma_q(n)} < \frac{n-1}{n-n/q-1+1/q} = \frac{q}{q-1},$$

and

$$\frac{n-\sigma_p(n)}{n-\sigma_q(n)} > \frac{q-1}{q} > \frac{q-2}{q}.$$

Thus

$$q-2 < (q-1)\,\frac{n-\sigma_p(n)}{n-\sigma_q(n)} < q. \tag{21}$$

Further, since $n \in C_p^! \cap C_q^!$, there exist nonnegative integers α, β so that $e_p(n) = 2^\alpha$, $e_q(n) = 2^\beta$, where $\alpha \ge \beta$, and according to (15) we have $n - \sigma_p(n) = (p-1)2^\alpha$ and $n - \sigma_q(n) = (q-1)2^\beta$.

Consequently, by (21) we obtain $q-2 < (p-1)2^{\alpha-\beta} < q$, whence $(p-1)2^{\alpha-\beta} = q-1$, which is a contradiction. Therefore, $n < (2+\alpha)q^2 - 1$.

It remains to notice that

$$\begin{aligned}\alpha &= 2(((2\log q-1)^2+2\log 2)^{1/2}-(2\log q-1))\\ &= 2(2\log q-1)\left(\left(1+\frac{2\log 2}{(2\log q-1)^2}\right)^{1/2}-1\right)\\ &< 2(2\log q-1)\,\frac{\log 2}{(2\log q-1)^2}=\frac{2\log 2}{2\log q-1},\end{aligned}$$

and the proposition follows. ■

COROLLARY 2. *If $p=2$ and q is a non-Fermat prime, then for $n\in C_2^!\cap C_q^!$ we have*

$$n\in\left(q,2\left(1+\frac{\log 2}{2\log q-1}\right)q^2-1\right).$$

In spite of the fact that the upper bound in Proposition 3 is quite convenient, the numerical experiments show that the value of the maximal element of the set $C_p^!\cap C_q^!$ depends on the distance between $(q-1)/(p-1)$ and the nearest power of 2 (see Table 2). Now we shall give an estimate which is more sensitive to this factor.

PROPOSITION 4. *Under the conditions of Proposition* 3, *we have*

$$\frac{n}{\log(n+1)}\le \max(a(p,q),b(p,q))\quad \textit{for } n\in C_p^!\cap C_q^!,$$

where

$$\begin{aligned}a(p,q)&=\frac{p-1}{\log p}\,(1-2^{-\{\log_2\frac{q-1}{p-1}\}})^{-1},\\ b(p,q)&=\frac{q-1}{\log q}\,(1-2^{\{\log_2\frac{q-1}{p-1}\}-1})^{-1},\end{aligned}$$

and $\{x\}$ denotes the fractional part of x.

Proof. For $n\in C_p^!\cap C_q^!$ there exist $\alpha\ge\beta$, $\alpha,\beta\in\mathbb{Z}_+$, so that $e_p(n)=2^\alpha$, $e_q(n)=2^\beta$, and by Corollary 1 we have

$$\begin{aligned}\frac{n}{p-1}-\log_p(n+1)&\le 2^\alpha<\frac{n}{p-1},\\ \frac{n}{q-1}-\log_q(n+1)&\le 2^\beta<\frac{n}{q-1}.\end{aligned}$$

Therefore

$$\frac{q-1}{p-1}\left(1-(p-1)\,\frac{\log_p(n+1)}{n}\right)\le 2^{\alpha-\beta}\le\frac{q-1}{p-1}\left(1-(q-1)\,\frac{\log_q(n+1)}{n}\right)^{-1},$$

whence

$$\alpha-\beta+\log_2\biggl(1-(q-1)\,\frac{\log_q(n+1)}{n}\biggr)\le\log_2\frac{q-1}{p-1}\le\alpha-\beta+\log_2\biggl(1-(p-1)\,\frac{\log_p(n+1)}{n}\biggr).\tag{22}$$

Notice that

$$b(p,q)>\frac{q-1}{\log q}\biggl(1-\frac{1}{2}\biggr)^{-1}=\frac{2(q-1)}{\log q}.$$

Consequently, if $n/\log(n+1)\le 2(q-1)/\log q$, then the conclusion of the proposition is satisfied trivially. Let now $n/\log(n+1)>2(q-1)/\log q$ (and certainly $n/\log(n+1)>2(p-1)/\log p$). Then

$$\log_2\biggl(1-(q-1)\,\frac{\log_q(n+1)}{n}\biggr)>-1,$$
$$\log_2\biggl(1-(p-1)\,\frac{\log_p(n+1)}{n}\biggr)>-1.$$

By (22),

$$\alpha-\beta-1<\log_2\frac{q-1}{p-1}<\alpha-\beta+1.$$

We distinguish between two cases:

Case 1: $\lfloor\log_2\frac{q-1}{p-1}\rfloor=\alpha-\beta-1$. By the left inequality in (22) we have

$$\alpha-\beta+\log_2\biggl(1-(q-1)\,\frac{\log_q(n+1)}{n}\biggr)\le\alpha-\beta-1+\biggl\{\log_2\frac{q-1}{p-1}\biggr\},$$

which implies $n/\log(n+1)\le b(p,q)$, and the proposition follows.

Case 2: $\lfloor\log_2\frac{q-1}{p-1}\rfloor=\alpha-\beta$. By the right inequality in (22) we have

$$\alpha-\beta+\biggl\{\log_2\frac{q-1}{p-1}\biggr\}\le\alpha-\beta-\log_2\biggl(1-(p-1)\,\frac{\log_p(n+1)}{n}\biggr),$$

so that $n/\log(n+1)\le a(p,q)$, and the proposition again follows. ∎

Proposition 5.

(i) *If $p<q$ are primes such that $(q-1)/(p-1)$ is a power of* 2, *then $n\in C_p^!\cap C_q^!$ if $n\in C_p^!$ and $\sigma_p(n)=\sigma_q(n)$. For $n\ge q^2$ the converse implication holds as well.*

(ii) *If $n\ge 4$, $p=2$ and q is a Fermat prime, then $n\in C_2^!\cap C_q^!$ if and only if $n\in C_2^!$ and $\sigma_2(n)=\sigma_q(n)$.*

Proof. (i) If $n\in C_p^!$ and $\sigma_p(n)=\sigma_q(n)$ then by (15) there exists a nonnegative integer α such that

$$n=(p-1)2^\alpha+\sigma_q(n).$$

Moreover, by assumption, there exists $\gamma \in \mathbb{N}$ so that $(q-1)/(p-1) = 2^\gamma$. Therefore, by (19) and (15),

$$n = (q-1)2^{\alpha-\gamma} + \sigma_q(n) = (q-1)e_q(n) + \sigma_q(n),$$

and hence $e_q(n) = 2^{\alpha-\gamma}$ and $n \in C_p^! \cap C_q^!$.

Conversely, if $n \in C_p^! \cap C_q^!$, then by (15) there exist nonnegative integers α and β so that

$$2^\alpha(p-1) + \sigma_p(n) = 2^\beta(q-1) + \sigma_q(n) = n \tag{23}$$

under the condition $(q-1)/(p-1) = 2^\gamma$. Therefore, by (23),

$$\frac{n-\sigma_p(n)}{n-\sigma_q(n)} = 2^{\alpha-\beta-\gamma}. \tag{24}$$

Furthermore,

$$1 \le \sigma_p(n) \le (p-1)\lfloor \log_p(n+1) \rfloor. \tag{25}$$

Therefore, by (24)–(25),

$$\frac{n-(p-1)\lfloor \log_p(n+1) \rfloor}{n-1} \le 2^{\alpha-\beta-\gamma} \le \frac{n-1}{n-(q-1)\lfloor \log_q(n+1) \rfloor}. \tag{26}$$

Notice that the function $(\log_p x)/x$ decreases for $x > e$. Since $2/p^2 \le 1/2(p-1)$ for $p \ge 2$, we have

$$\frac{\log_p(n+1)}{n+1} < \frac{2}{p^2} \le \frac{1}{2(p-1)} \quad \text{for } n > p^2-1,$$

which yields

$$(p-1)\lfloor \log_p(n+1) \rfloor < \frac{n+1}{2}.$$

For $n > q^2-1$ we also have $(q-1)\lfloor \log_q(n+1) \rfloor < (n+1)/2$, and by (26), $1/2 < 2^{\alpha-\beta-\gamma} \le 2$. Now (24) implies $\sigma_p(n) = \sigma_q(n)$.

(ii) Let $p = 2$ and q be of the form 2^k+1. Since $\sigma_2(n) \ne \sigma_q(n)$ for $n = 4, 5$, and $4, 5 \notin C_2^!$, we suppose that $\max(6, q) \le n < q^2$, and $n \in C_2^! \cap C_q^!$. By Proposition 1 there exists an $\alpha \ge 2$ so that $n = 2^\alpha + i$, where $i = 2$ or 3. Since $\alpha \ge k$, put $\alpha = k+t$, $t \ge 0$. Notice that

$$e_q(n) = \left\lfloor \frac{n}{q} \right\rfloor = \left\lfloor \frac{2^{k+t}+i}{2^k+1} \right\rfloor,$$

where $i = 2$ or 3. For $t \ge 2$ we evidently have $2^{t-1}+1 \le \frac{2^{k+t}+i}{2^k+1} < 2^t$, which contradicts the fact that $n \in C_q^!$.

Therefore, consider $t = 0$ and $t = 1$ only. We obtain four numbers

$$2^k+2 = q+1, \quad 2^k+3 = q+2, \quad 2^{k+1}+2 = 2q, \quad 2^{k+1}+3 = 2q+1,$$

belonging to $C_2^! \cap C_q^!$, and for each of them $\sigma_2(n) = \sigma_q(n)$. ∎

Notice that for $n = 3 \in C_2^! \cap C_3^!$, we have $\sigma_2(3) \neq \sigma_3(3)$.

As an important consequence we obtain the following statement.

PROPOSITION 6. *Let q be a Fermat prime.*

(i) *For $\alpha \geq 2$, we have $2^\alpha + 2 \in C_q^!$ if and only if the diophantine equation*

$$q^x + q^y = 2^\alpha + 2 \tag{27}$$

is solvable in nonnegative integers x, y.

(ii) *For $\alpha \geq 2$ we have $2^\alpha + 3 \in C_q^!$ if and only if the diophantine equation*

$$q^x + q^y + q^z = 2^\alpha + 3 \tag{28}$$

is solvable in nonnegative integers x, y, z.

Proof. Follows from Propositions 1 and 5. ∎

Thus, to describe the set $C_2^! \cap C_q^!$ for a Fermat prime q, it suffices to find all solutions of (28) in nonnegative integers.

4.2. *Proof of Theorem 2 for non-Fermat primes.* We start with several lemmas.

LEMMA 5. *Let q be an odd non-Fermat prime so that $2^{k-1} + 3 \leq q < 2^k$ for some $k \geq 3$. If some number n of the form $n = 2^{k+l} + i$, where $i = 2$ or 3, belongs to $C_q^!$, then $0 \leq l \leq k - 1$.*

Proof. Notice that $l \geq 0$, as otherwise $n < q$ and $n \notin C_q^!$. Put $\Delta = 2^k - q$. Now,

$$1 \leq \Delta \leq 2^k - 2^{k-1} - 3 = 2^{k-1} - 3 \leq q - 6. \tag{29}$$

Furthermore,

$$n = 2^{k+l} + i = 2^l(2^k - \Delta) + 2^l\Delta + i = 2^l q + (2^l\Delta + i). \tag{30}$$

Since, by Proposition 1, $n \in C_2^!$, we have $n \in C_2^! \cap C_q^!$, and, by Corollary 1, $n \leq 3q^2 - 1$. Therefore,

$$e_q(n) = \left\lfloor \frac{n}{q} \right\rfloor + \left\lfloor \frac{n}{q^2} \right\rfloor \leq \left\lfloor \frac{n}{q} \right\rfloor + 2. \tag{31}$$

Suppose that $l \geq k$. Then $q < 2^k \leq 2^l$, and by (30),

$$e_q(n) \geq \left\lfloor \frac{n}{q} \right\rfloor \geq 2^l + 1. \tag{32}$$

On the other hand, by (29)–(31) we have

$$\begin{aligned} e_q(n) &\leq 2^l + \left\lfloor \frac{2^l\Delta + 3}{q} \right\rfloor + 2 \leq 2^l + 2 + \left\lfloor \frac{2^l(2^{k-1} - 3) + 3}{q} \right\rfloor \\ &< 2^l + 2 + \left\lfloor 2^l - \frac{3 \cdot 2^l}{2^{k-1} + 3} \right\rfloor \leq 2^{l+1} + 2 - \frac{3 \cdot 2^k}{2^{k-1} + 2^{k-1}} = 2^{l+1} - 1. \end{aligned} \tag{33}$$

Now (32)–(33) contradict the condition $n \in C_q^!$. Thus, $l \leq k - 1$. ∎

LEMMA 6. *Under the conditions of Lemma* 5, *the number* $n = 2^{k+l} + i$, *where* $i = 2$ *or* 3, *belongs to* $C_q^!$ *if and only if* $2^l \Delta + i < q$.

Proof. If $2^l \Delta + i < q$, then by (30),

$$e_q(n) = 2^l + \left\lfloor \frac{2^l}{q} \right\rfloor = 2^l,$$

i.e., $n \in C_q^!$.

Conversely, let $n \in C_q^!$. We distinguish between two cases:

CASE a: $l = k - 1$. We have $n = 2^{2k-1} + i \in C_2^! \cap C_q^!$, where $i = 2$ or 3. Hence

$$\left\lfloor \frac{n}{q^2} \right\rfloor \le \left\lfloor \frac{2^{2k-1} + 3}{(2^{k-1} + 3)^2} \right\rfloor \le 1. \tag{34}$$

By (29), (30) and (34),

$$e_q(n) \le 2^{k-1} + \left\lfloor \frac{2^{k-1}\Delta + i}{q} \right\rfloor + 1 \le 2^{k-1} + \left\lfloor \frac{2^{k-1}(q-6) + i}{q} \right\rfloor + 1. \tag{35}$$

Since $q \le 2^k - 1$, and the function $(2^{k-1}(x-6) + i)/x$ increases,

$$\frac{2^{k-1}(q-6) + i}{q} \le \frac{2^{k-1}(2^k - 7) + 3}{2^k - 1} < 2^{k-1} - 1.$$

Therefore, by (35),

$$e_q(n) \le 2^{k-1} + 2^{k-1} - 2 + 1 = 2^k - 1. \tag{36}$$

On the other hand, by (30),

$$e_q(n) \ge 2^{k-1} + \left\lfloor \frac{2^{k-1}\Delta + i}{q} \right\rfloor. \tag{37}$$

If $2^{k-1}\Delta + i \ge q$, then (36)–(37) imply $2^{k-1} + 1 \le e_q(n) \le 2^k - 1$, which contradicts the condition $n \in C_q^!$.

CASE b: $l \le k - 2$. Now $n \le 2^{2k-2} + 3$, and instead of (32) we obtain $\lfloor n/q^2 \rfloor = 0$, and therefore instead of (35) we find that

$$e_q(n) \le 2^l + \left\lfloor \frac{2^l(q-6) + 3}{q} \right\rfloor \le 2^l + (2^l - 1) = 2^{l+1} - 1. \tag{38}$$

On the other hand, by (30),

$$e_q(n) = 2^l + \left\lfloor \frac{2^l \Delta + i}{q} \right\rfloor \tag{39}$$

and again we conclude that, if $2^l \Delta + i \ge q$, then (38)–(39) contradict the condition $n \in C_q^!$. ∎

Now we need an additional technical lemma.

Lemma 7. *The diophantine equation*

$$n(2^m+1) = 2^{k+m}+3, \quad m \geq 0,\ k \geq 0,\ n \in \mathbb{N}, \tag{40}$$

has only the following solutions:

1) $k=0$, $m=0$, $n=2$.
2) $k \equiv 3 \pmod 4$, $m=2$, $n=(2^{k+2}+3)/5$.

Proof. Let

$$k = rm+s, \quad 0 \leq s < m.$$

It is easy to see that

$$(2^m+1)\sum_{i=0}^{\lfloor k/m \rfloor}(-1)^i 2^{k-mi} = 2^{k+m}+(-1)^r 2^s, \quad m \geq 1.$$

Therefore,

$$2^{k+m}+3 \equiv (-1)^{r+1}2^s+3 \pmod{2^m+1}, \quad m \geq 1. \tag{41}$$

If (40) is valid, then by (41),

$$(-1)^{r+1}2^s+3 \equiv 0 \pmod{2^m+1}. \tag{42}$$

If r in (42) is even, then $2^s-3 \equiv 0 \pmod{2^m+1}$. This is impossible, since $2^s-3 < 2^m+1$ and $2^5-3 \neq 0$. If the r is odd, then $2^s+3 \equiv 0 \pmod{2^m+1}$, $m \geq 1$. If here $m \geq 3$, then $2^s+3 \leq 2^{m-1}+3 < 2^m+1$. Therefore, $m \leq 2$, and in addition the case $m=1$ is impossible. If $m=2$, from (40) we find $n=(2^{k+2}+3)/5$. Also notice that if in (40) we have $m=0$, then $2n=2^k+3$, so that $k=0$ and $n=2$. ∎

Now we are able to complete the proof of Theorem 2 in the case of a non-Fermat prime q.

1) Let $q=2^{k-1}+3$. First suppose that $k \geq 4$, i.e., $q \geq 11$. Then by Lemma 6, we have $2^{k+l}+i \in C_2^! \cap C_q^!$, $i=2,3$, $l \geq 0$, if and only if $\Delta \cdot 2^l + i < q = 2^{k-1}+3$, where $\Delta = 2^{k-1}-3$. Thus,

$$(2^{k-1}-3)2^l \leq 2^{k-1}+2-i, \quad i=2,3. \tag{43}$$

If $l \geq 1$, this is impossible for $k \geq 4$. Therefore $l=0$ and we have two elements from $C_2^! \cap C_q^!$, namely

$$2^k+2 = 2q-4 \quad \text{and} \quad 2^k+3 = 2q-3.$$

Moreover, in this case $q = 2^{k-1}+3 \in C_2^! \cap C_q^!$. Thus, if $k \geq 4$,

$$C_2^! \cap C_q^! = \{q, 2q-4, 3q-3\}.$$

It remains to deal with the case $q=7$, $k=3$. Here (43) is satisfied if $2^l \leq 6-i$, i.e., $l=0,1$ for $i=2,3$ and $l=2$ for $i=2$. That gives five numbers from $C_2^! \cap C_7^!$: 10, 11, 18, 19 and 34. Moreover, $7 \in C_2^! \cap C_7^!$. Thus $|C_2^! \cap C_7^!| = 6$.

As a simple consequence we obtain the following statement.

PROPOSITION 7.

$$C^! = \{1, 2, 3, 6, 7, 10, 11\}.$$

Proof. It is sufficient to consider the numbers 1, 2, 3, 4, 5, 6, 7, 10, 11, 18, 19, 34. ∎

2) Let $q = (2^{k+2} + 3)/5$, where $k \equiv 3 \pmod 4$. The smallest $q > 7$ of this kind is $q = 103$, obtained for $k = 7$. The smallest $q > 103$ is $q = 6710887$, obtained for $k = 23$. Let $k \geq 7$. Here

$$\Delta = 2^k - \frac{2^{k+2} + 3}{5} = \frac{2^k - 3}{5}.$$

Now by Lemma 6 we have $2^{k+l} + i \in C_2 \cap C_q$, $i = 2, 3$, $l \geq 0$, if and only if

$$\Delta \cdot 2^l + i = \frac{2^{k+l} - 3 \cdot 2^l + 5i}{5} < q = \frac{2^{k+2} + 3}{5}, \qquad k \geq 7.$$

Hence $l \leq 2$, and in the case $l = 2$,

$$2^{k+2} + i < 2^{k+2} + 3$$

and $i = 2$. Thus we have exactly five suitable numbers:

$$\begin{aligned} l = 0: &\qquad n_1 = 2^k + 2 = \frac{5q + 5}{4}, \qquad n_2 = 2^k + 3 = \frac{5q + 9}{4}, \\ l = 1: &\qquad n_3 = 2^k + 2 = \frac{5q + 1}{2}, \qquad n_4 = 2^{k+1} + 3 = \frac{5q + 3}{2}, \\ l = 2: &\qquad n_5 = 2^{k+2} + 2 = 5q - 1, \end{aligned}$$

so that $|C_2^! \cap C_q^!| = 5$.

3) Let $q \geq 2^{k-1} + 5$ and $q \neq (2^{k+2} + 3)/5$. First of all, we will show that in this case $|C_2^! \cap C_q^!|$ is even. To this end, it suffices to show that the inequality $\Delta \cdot 2^l + 2 < q$ implies $\Delta \cdot 2^l + 3 < q$. Indeed, if $\Delta \cdot 2^l + 3 = q$ or $(2^k - q) \cdot 2^l + 3 = q$, then

$$q(2^l + 1) = 2^{k+l} + 3,$$

and by Lemma 7 we have $l = 2$, $q = (2^{k+2} + 3)/5$, where $k \equiv 3 \pmod 4$. This contradicts the assumption. Therefore, by Lemma 6, $2^{k+l} + i \in C_2^! \cap C_q^!$ if and only if $(2^k - q)2^l + 3 < q$. Notice that $l = 0$ is trivially a suitable case, which gives two numbers from $C_2^! \cap C_q^!$, namely, $2^k + 2$ and $2^k + 3$. In the case of $l \geq 1$, the inequality $(2^k - q)2^l + 3 < q$ implies $(2^k - q)2^l \leq q - 5$. Thus, $n \in C_2^! \cap C_q^!$ if and only if $n = 2^{k+l} + i$, where $i = 2$ or 3, and $0 \leq l \leq \left\lfloor \log_2 \frac{q-5}{2^k - q} \right\rfloor$. Therefore

$$|C_2^! \cap C_q^!| = 2\left(1 + \left\lfloor \log_2 \frac{q - 5}{2^k - q} \right\rfloor\right). \tag{44}$$

This completes the proof of Theorem 2 when q is a non-Fermat prime. ∎

4.3. *Proof of Theorem 2 when q is a Fermat prime.* According to Proposition 6, we need to investigate the diophantine equation

$$2^\alpha + 3 = q^x + q^y + q^z \tag{45}$$

in nonnegative integers α, x, y, z, where q is a Fermat prime.

We need the following result of G. C. Gerono (1871).

PROPOSITION 8 (see [15, p. 374]). *The diophantine equation $2^\alpha + 1 = g^x$ for $\alpha \geq 2$, $x \geq 2$, $g \geq 2$, has the only solution $\alpha = 3$, $x = 2$, $g = 3$.*

Taking into account this result, we break up the investigation of (45) into the following cases:

1. $q \geq 17$, $x, y, z \geq 1$,
2. $q \geq 17$, $z = 0$, $x \neq y$
   (except the solution $\alpha = 1 + \log_2(q-1)$, $x = y = 1$),
3. $q = 3$, $z = 0$, $x \neq y$
   (except the solutions $\alpha = 2$, $x = y = 1$; $\alpha = 3$, $x = y = 2$),
4. $q = 5$, $z = 0$, $x \neq y$ (except the solution $\alpha = 3$, $x = y = 1$),
5. $q = 5$, $x, y, z \geq 1$.

4.3.1. CASE 1: $q \geq 17$, $x, y, z \geq 1$. We start with the following straightforward lemma.

LEMMA 8. *If $q = 2^{2^{h-1}} + 1$, $h \geq 3$, then the subgroup of $(\mathbb{Z}/q\mathbb{Z})^*$ generated by 2 is*

$$\{2^j : 0 \leq j \leq 2^{h-1}\} \cup \{q - 2^j : 1 \leq j \leq 2^{h-1}\}.$$

PROPOSITION 9. *If $q \geq 17$ is a Fermat prime, then* (45) *has no solutions with $x, y, z \geq 1$.*

Proof. It is sufficient to prove that $2^\alpha + 3$ is not divisible by q. Let $q = 2^{2^{h-1}} + 1$, $h \geq 3$. If $2^m + 3 \equiv 0 \pmod q$ then -3 is generated by 2 in $(\mathbb{Z}/q\mathbb{Z})^*$. Using Lemma 8, we easily see that the only possibility is $h = 2$.

4.3.2. CASE 2: $q \geq 17$, $z = 0$, $x \neq y$.

LEMMA 9. *If $q = 2^{2^{h-1}}$, $h \geq 3$, is a Fermat prime, then q divides $2^m + 1$ if and only if $m = 2^h k - 2^{h-1}$ for some $k \in \mathbb{N}$.*

Proof. Follows from the connection between j and $2^j \pmod m$, which is implicit in Lemma 8. ∎

Suppose now that in (45) we have $z = 0$, $x, y \geq 1$, $x \neq y$, $q = 2^{2^{h-1}} + 1$, $h \geq 3$. Then $q \mid 2^{\alpha-1} + 1$, and by Lemma 9 we have

$$\alpha = 2^h(k-1) + 2^{h-1} + 1$$

for some $k \geq 1$, so that

$$2(2^{2^h k - 2^{h-1}} + 1) = (2^{2^{h-1}} + 1)^x + (2^{2^{h-1}} + 1)^y. \tag{46}$$

If $k = 1$, then

$$2 = (2^{2^{h-1}} + 1)^{x-1} + (2^{2^{h-1}} + 1)^{y-1},$$

whence $x = y = 1$, contradicting the assumption $x \neq y$. Hence $k \geq 2$. Consequently, $2^h k - 2^{h-1} \geq 2^{h+1} - 2^{h-1} > 2^h$, so that (46) yields

$$2 \equiv 2^{2^{h-1}} x + 2^{2^{h-1}} y + 2 \pmod{2^{2^h}}.$$

Thus

$$x + y \equiv 0 \pmod{2^{2^{h-1}}}, \tag{47}$$

and in particular x and y have the same parity.

Suppose that, in (46), x and y are both even. Taking (46) modulo 3, we obtain

$$\begin{aligned} 2 &\neq (2^{2^{h-1}} + 1)^x + (2^{2^{h-1}} + 1)^y \\ &= ((2^{2^{h-1}} + 2) - 1)^x + ((2^{2^{h-1}} + 2) - 1)^y \\ &= (2(2^{2^{h-1}} + 1) - 1)^x + (2(2^{2^{h-1}} + 1) - 1)^y \equiv 2 \pmod 3, \end{aligned}$$

which is a contradiction. Thus, x and y are both odd. Let $x = 2l - 1$, $y = 2m - 1$, $l, m \in \mathbb{N}$. By (47),

$$l + m \equiv 1 \pmod{2^{2^{h-1}-1}}.$$

Hence, l and m have different parities. Moreover, by (46),

$$2(2^{2^h k - 2^{h-1}} + 1)(2^{2^{h-1}} + 1) = ((2^{2^{h-1}} + 1)^2)^l + ((2^{2^{h-1}} + 1)^2)^m. \tag{48}$$

Notice that, since $h \geq 3$, we have $2^{2^{h-1}} + 1 = (2^4)^{2^{h-3}} + 1 \equiv 2 \pmod 5$. Therefore $(2^{2^{h-1}} + 1)^2 \equiv -1 \pmod 5$, and according to (48), since l and m have different parities, we have $0 \equiv 2^{2^h k - 2^{h-1}} + 1 = 2^{2^{h-1}(2k-1)} + 1 = ((2^4)^{2^{h-3}})^{2k-1} + 1 \equiv 2 \pmod 5$. This contradiction shows that (45) has no solutions with $z = 0$, $x \geq 1$, $y \geq 1$ and $x \neq y$. A simple sorting out of other possibilities gives the following.

PROPOSITION 10. *If $q \geq 17$ is a Fermat prime then* (45) *has only the following solutions* (*up to permutation of x, y, z*):

- $x = 1$, $y = 0$, $z = 0$, $\alpha = \log_2(q - 1)$;
- $x = y = 1$, $z = 0$, $\alpha = \log_2(q - 1)$.

4.3.3. CASE 3: $q = 3$, $z = 0$, $x \neq y$. Here we investigate the equation

$$2^\alpha + 2 = 3^x + 3^y. \tag{49}$$

Since

$$2^{\alpha-1} + 1 = (3 - 1)^{\alpha-1} + 1 \equiv \begin{cases} 0 \pmod 3, & \alpha \equiv 0 \pmod 2, \\ 2 \pmod 3, & \alpha \equiv 1 \pmod 2, \end{cases}$$

α in (49) is even: $\alpha = 2t$, $t \geq 2$. Rewrite (49) as

$$4^t + 2 = 3^x + 3^y, \quad t \geq 2,\ x, y \geq 1,\ x \neq y. \tag{50}$$

Suppose that, say, $x > y$. Suppose x, y have distinct parities. Then

$$3^x + 3^y = 3^y(3 \cdot 3^{x-y-1} + 1) \equiv 0 \pmod 4,$$

which contradicts (50). Next, suppose x, y are both odd. Then

$$3^x + 3^y - 2 = 3(3^{x-1} + 3^{x-1}) - 2 = 3(9^{(x-1)/2} + 9^{(x-1)/2}) - 2 \equiv 4 \pmod 8,$$

which is again impossible in (50). It follows that x, y are both even, say, $x = 2r$, $y = 2u$. Substitute this in (50):

$$4^t + 2 = 9^r + 9^u \quad (r > u \geq 1,\ t \geq 2). \tag{51}$$

Writing $t = 3s + i$, where $s \geq 0$ and $i = 1, 2, 3$, we easily obtain $2^{2i-1} + 1 \equiv 0 \pmod 9$. Thus $i = 2$ and $t = 3s + 2$, and instead of (51) we consider the equation

$$2^{6s+4} + 2 = 9^r + 9^u, \quad r > u \geq 1,\ s \geq 0, \tag{52}$$

whence

$$4 \equiv 2^r + 2^u \pmod 7.$$

Since $2^1 \equiv 2$, $2^2 \equiv 4$, $2^3 \equiv 1 \pmod 7$, it follows that $r \equiv u \equiv 1 \pmod 3$.

Put $r = 3v + 1$, $u = 3w + 1$, $v > w \geq 0$. Then by (52),

$$4^{3s+2} + 2 = 9^{3v+1} + 9^{3w+1}, \quad v > w \geq 0,\ s \geq 0. \tag{53}$$

By taking this modulo 5 we have

$$(-1)^s + 2 \equiv (-1)^{v+1} + (-1)^{w+1} \pmod 5.$$

Therefore, v and w have the same parity; moreover, v and w are even, and s is also even.

Put $s = 2\sigma$, $v = 2\nu$, $w = 2\omega$. Then by (53),

$$4^{6\sigma+2} + 2 = 9^{6\nu+1} + 9^{6\omega+1}, \quad \nu > \omega \geq 0. \tag{54}$$

Let us write (54) in the form

$$16 \cdot 8^{4\sigma} + 2 = 9(27^{4\nu} + 27^{4\omega}), \quad \nu > \omega \geq 0. \tag{55}$$

Now by taking this modulo 19 we have

$$-3 \cdot 8^{4\sigma} + 2 \equiv 9(8^{4\nu} + 8^{4\omega}) \pmod{19}.$$

Taking into account that

$$8^4 = 64^2 \equiv 7^2 \equiv 11 \pmod{19},$$

we have

$$9(11^\nu + 11^\omega) + 3 \cdot 11^\sigma \equiv 2 \pmod{19}. \tag{56}$$

Since $11^1 \equiv 11$, $11^2 \equiv 7$, $11^3 \equiv 1$; $9 \cdot 11^1 \equiv 4$, $9 \cdot 11^2 \equiv 6$, $9 \cdot 11^3 \equiv 9$; $3 \cdot 11^1 \equiv 14$, $3 \cdot 11^2 \equiv 2$, $3 \cdot 11^3 \equiv 3 \pmod{19}$, we see that the unique possibility in (56) is $\sigma \equiv \nu \equiv \omega \equiv 0 \pmod 3$. Finally, put $\nu = 3\beta$, $\omega = 3\gamma$, $\sigma = 3\delta$, $\beta > \gamma \geq 0$. By (54) we have

$$2^{36\delta+4} + 2 = 3^{36\beta+2} + 3^{36\gamma+2}, \qquad \beta > \gamma \geq 0.$$

Consider two cases:

1) $\gamma = 0,\ \beta \geq 1$. Then

$$2^{36\delta+4} \equiv 7 \pmod{27}, \quad \text{i.e.} \quad 16 \cdot 4^{\varphi(27)\delta} \equiv 7 \pmod{27},$$

whence $16 \equiv 7 \pmod{27}$. We have a contradiction.

2) $\gamma \geq 1,\ \beta \geq 2$. Then

$$2^{36\delta+4} \equiv 25 \pmod{27}, \quad \text{i.e.} \quad 16 \cdot 4^{\varphi(27)\delta} \equiv 25 \pmod{27},$$

whence $16 \equiv 25 \pmod{27}$. Again we have a contradiction. Consequently, we have proved the following statement.

Proposition 11. *The diophantine equation* (49): $2^\alpha + 2 = 3^x + 3^y$ *does not have solutions in* $x \geq 1$, $y \geq 1$, $x \neq y$.

By a simple sorting out of the possibilities not included in Proposition 11, using Proposition 8, we obtain the following consequence.

Corollary 3. *If* $x, y \geq 0$, $\alpha \geq 2$ *then the diophantine equation* $2^\alpha + 2 = 3^x + 3^y$ *has only the following solutions*:

- $\alpha = 4$, $x = y = 2$;
- $\alpha = 3$, $x = 2$, $y = 0$; $\alpha = 3$, $x = 0$, $y = 2$;
- $\alpha = 2$, $x = y = 1$.

4.3.4. Case 4: $q = 5$, $z = 0$, $x \neq y$. Here we investigate the equation

$$2^\alpha + 2 = 5^x + 5^y, \qquad x, y \geq 1,\ x \neq y,\ \alpha \geq 5. \tag{57}$$

(It is evident that for $\alpha \leq 4$, (57) has no solutions in $x \geq 1$, $y \geq 1$, $x \neq y$.) Since modulo 5 we have $2^1 \equiv 2$, $2^2 \equiv 4$, $2^3 \equiv 3$, $2^4 \equiv 1$, it follows that in (57), $\alpha = 4k + 3$, $k \geq 1$. Thus by (57),

$$2^{4k+3} + 2 = 5^x + 5^y, \qquad k \geq 1,\ x \geq 1,\ y \geq 1,\ x \neq y. \tag{58}$$

By taking this modulo 16 we have

$$2 \equiv (4+1)^x + (4+1)^y \equiv (x+y) + 2 \pmod{16}.$$

Therefore, $x + y \equiv 0 \pmod 4$, and x, y have the same parity. Taking now (58) modulo 3, we have

$$1 \equiv (6-1)^x + (6-1)^y \equiv 2(-1)^x \pmod 3.$$

Consequently, both x and y are odd.

Put $x = 2l - 1,\ y = 2m - 1$. Then $l + m \equiv 1 \pmod 2$. Now instead of (58) we have

$$(59)\qquad 2^{4k+3} + 2 = 5^{2l-1} + 5^{2m-1}, \qquad k \geq 1,\, l \geq 1,\, m \geq 1,\ l \neq m,\, l + m \equiv 1 \pmod 2,$$

i.e. $5(2^{4k+3} + 2) = 25^l + 25^m$. By taking this modulo 13 we immediately obtain

$$(60)\qquad 2^{4k+2} + 1 \equiv 0, \quad \text{i.e.} \quad 4^{2k+1} \equiv 12,\ 4^{2k} \equiv 3 \pmod{13},\ k \geq 1.$$

Since modulo 13 we have

$$4^1 \equiv 4, \quad 4^2 \equiv 3, \quad 4^3 \equiv 12, \quad 4^4 \equiv 9, \quad 4^5 \equiv 10, \quad 4^6 \equiv 1,$$

from (60) we obtain

$$2k \equiv 2 \pmod 6, \quad \text{i.e.} \quad k \equiv 1 \pmod 3.$$

Put $k = 3r + 1,\ r \geq 0$. Then by (59),

$$(61)\qquad 2^{12r+7}+2 = 5^{2l-1}+5^{2m-1}, \qquad l \geq 1,\, m \geq 1,\, l \neq m,\, l+m \equiv 1 \pmod 2.$$

Further, by taking this modulo 7 we have

$$4 \equiv -2^{2l-1} - 2^{2m-1}, \quad \text{i.e.} \quad 4^l + 4^m \equiv 6 \pmod 7.$$

Since $4^1 \equiv 4,\ 4^2 \equiv 2,\ 4^3 \equiv 1 \pmod 7$, it follows that either $l \equiv 1,\ m \equiv 2 \pmod 3$ or $l \equiv 2,\ m \equiv 1 \pmod 3$. By symmetry it suffices to consider only the first possibility. Put $l = 3u + 1,\ m = 3v + 2,\ u, v \geq 0$. Since in (61), $l + m \equiv 1 \pmod 2$, we have $u + v \equiv 0 \pmod 2$, and by (61) we obtain

$$(62)\qquad 2^{12r+7} + 2 = 5^{6u+1} + 5^{6v+3}, \qquad r, u, v \geq 0,\ u + v \equiv 0 \pmod 2.$$

We shall write (62) in the form

$$2^{12r+7} + 2 = 5 \cdot 125^{2u} + 125^{2v+1}.$$

Since $125 \equiv -8 \pmod{19}$, we have

$$2^{12r+7} + 2 \equiv 5 \cdot 2^{6u} - 2^{6v+3} \pmod{19}.$$

Since $2^6 \equiv 7 \pmod{19}$, we obtain $2 \cdot 7^{2r+1} + 2 \equiv 5 \cdot 7^u - 8 \cdot 7^v \pmod{19}$, i.e.

$$(63)\qquad 7^{2r+1} + 7^{u+1} + 4 \cdot 7^v \equiv 18 \pmod{19}, \qquad r, u, v \geq 0,\ u + v \equiv 0 \pmod 2.$$

Notice that modulo 19 we have $7^1 \equiv 7,\ 7^2 \equiv 11,\ 7^3 \equiv 1;\ 4 \cdot 7^1 \equiv 9,\ 4 \cdot 7^2 \equiv 6,\ 4 \cdot 7^3 \equiv 4$. Consequently, as is easy to check, we have only three cases in (63):

(a) $2r + 1 \equiv 0,\ u \equiv 1,\ v \equiv 2 \pmod 3$,
(b) $2r + 1 \equiv 2,\ u \equiv 2,\ v \equiv 2 \pmod 3$,
(c) $2r + 1 \equiv 1,\ u \equiv 0,\ v \equiv 0 \pmod 3$.

CASE (a). Put $2r+1 = 3(2\lambda+1)$, i.e. $r = 3\lambda+1,\ u = 3\xi+1,\ v = 3\eta+2,\ \lambda, \xi, \eta \geq 0$.

Since $u+v\equiv 0 \pmod 2$, we have $\xi+\eta\equiv 1 \pmod 2$. By (62),

$$2^{36\lambda+19}+2=5^{18\xi+7}+5^{18\eta+15}. \tag{64}$$

By taking this modulo 125 we have $2^{36\lambda+18}\equiv -1 \pmod{125}$.

Since $\min\{\alpha\ge 1 : 2^\alpha\equiv -1 \pmod{125}\}=50$ and $\varphi(125)=100$ we have

$$36\lambda+18\equiv 50 \pmod{100}, \quad \text{i.e.} \quad 9\lambda\equiv 8 \pmod{25}. \tag{65}$$

On the other hand, notice that $5^6+1=15626=2\cdot 13\cdot 601$ and $5^6\equiv -1 \pmod{601}$. Now by (64) we have

$$2^{36\lambda+19}+2=5(5^6)^{3\xi+1}+125(5^6)^{3\eta+2}\equiv 5(-1)^{\xi+1}+125(-1)^\eta \pmod{601}.$$

Taking into account that $\xi+\eta\equiv 1 \pmod 2$, we conclude that, modulo 601,

$$2^{36\lambda+19}+2\equiv\begin{cases}130, & \eta \text{ is even},\\ -130, & \eta \text{ is odd},\end{cases}$$

i.e.

$$2^{36\lambda+18}\equiv\begin{cases}64, & \eta \text{ is even},\\ -66, & \eta \text{ is odd}.\end{cases} \tag{66}$$

Now notice that all residues of powers of 2 modulo 601 are:

$$\begin{gathered} 2^i,\ i=1,2,\dots,9;\ \ 2^{10}\equiv 423,\ \ 2^{11}\equiv 245,\ \ 2^{12}\equiv 490,\ \ 2^{13}\equiv 379,\\ \begin{array}{llll} 2^{14}\equiv 157, & 2^{15}\equiv 314, & 2^{16}\equiv 27, & 2^{17}\equiv 54,\\ 2^{18}\equiv 108, & 2^{19}\equiv 216, & 2^{20}\equiv 432, & 2^{21}\equiv 263,\\ 2^{22}\equiv 526, & 2^{23}\equiv 451, & 2^{24}\equiv 301, & 2^{25}\equiv 1. \end{array}\end{gathered}$$

Now we see that in (66) the residue $-66\equiv 535 \pmod{601}$ is impossible. Therefore η is even and $2^{36\lambda+12}\equiv 1 \pmod{601}$, so $36\lambda+12\equiv 0 \pmod{25}$, hence $9\lambda\equiv -3 \pmod{25}$. That contradicts (65).

Case (b). Put $2r+1=3(2\lambda+1)+2$, i.e. $r=3\lambda+2$, $u=3\xi+2$, $v=3\eta+2$, $\lambda,\xi,\eta\ge 0$. Since $u+v\equiv 0 \pmod 2$, we have $\xi+\eta\equiv 0 \pmod 2$. By (62),

$$2^{36\lambda+31}+2=5^{18\xi+13}+5^{18\eta+15}. \tag{67}$$

By taking this modulo 125 we have $2^{36\lambda+30}\equiv -1 \pmod{125}$. Consequently, as in Case (a) we obtain

$$36\lambda+30\equiv 50 \pmod{100}, \quad \text{i.e.} \quad 9\lambda\equiv 5 \pmod{25}. \tag{68}$$

On the other hand, again, since $5^6\equiv -1 \pmod{601}$, by (67) we have

$$2^{36\lambda+31}+2=5(5^6)^{3\xi+2}+125(5^6)^{3\eta+2}\equiv 5(-1)^{\xi}+125(-1)^\eta \pmod{601}.$$

Taking into account that $\xi+\eta\equiv 0 \pmod 2$, we conclude that

$$2^{36\lambda+31}+2\equiv\begin{cases}130, & \eta \text{ is even},\\ -130, & \eta \text{ is odd},\end{cases}$$

and as in Case (a) we find that η is even and

$$2^{36\lambda+24} \equiv 64 \pmod{601}, \qquad 36\lambda + 24 \equiv 0 \pmod{25},$$

i.e. $9\lambda \equiv -6 \pmod{25}$. That contradicts (68).

Case (c). Put $2r + 1 = 3(2\lambda) + 1$, i.e. $r = 3\lambda$, and $u = 3\xi$, $v = 3\eta$, $\lambda, \xi, \eta \geq 0$. Since $u + v \equiv 0 \pmod 2$, we have $\xi + \eta \equiv 0 \pmod 2$. By (62),

$$2^{36\lambda+7} + 2 = 5^{18\xi+1} + 5^{18\eta+3}. \tag{69}$$

Here we consider two subcases: (c′) $\xi \geq 1$, (c″) $\xi = 0$.

Subcase (c′): $\xi \geq 1$. By taking (69) modulo 125 we find

$$2^{36\lambda+6} \equiv -1 \pmod{125}.$$

Therefore, as above $36\lambda + 6 \equiv 50 \pmod{100}$ and so

$$9\lambda \equiv 11 \pmod{25}. \tag{70}$$

On the other hand, by (69) we have

$$2^{36\lambda+7} + 2 = 5(5^6)^{3\xi} + 125(5^6)^{3\eta} \equiv 5(-1)^{\xi} + 125(-1)^{\eta} \pmod{601}$$

and

$$2^{36\lambda+7} + 2 \equiv \begin{cases} 130, & \eta \text{ is even,} \\ -130, & \eta \text{ is odd.} \end{cases}$$

As above we find that η is even and $2^{36\lambda} \equiv 1 \pmod{601}$. Consequently, $36\lambda \equiv 0 \pmod{25}$. This contradicts (70).

Subcase (c″): $\xi = 0$. By (69),

$$2^{36\lambda+7} - 3 = 5^{18\eta+3}. \tag{71}$$

This equation is a special case of the following equation considered in [1]:

$$1 + 2^a = 3^b 5^c + 2^d 3^e 5^f$$

for $a = 36\lambda + 7$, $b = 0$, $c = 18\eta + 3$, $d = 2$, $e = f = 0$. Since $a \geq 7$, $c \geq 3$, by [1] the equation (71) has only the solution $\lambda = 0$, $\eta = 0$.

Thus, we proved

Proposition 12. *The diophantine equation* (57): $2^\lambda + 2 = 5^x + 5^y$ *has only the following solution*: $\lambda = 7$, $x = 3$, $y = 1$, *in* $\lambda \geq 2$, $x > y \geq 1$.

4.3.5. Case 5: $q = 5$, $x, y, z \geq 1$. Here we investigate the equation

$$2^\alpha + 3 = 5^x + 5^y + 5^z, \qquad x, y, z \geq 1, \ \alpha \geq 4. \tag{72}$$

Since in (72), $2^\alpha \equiv 2 \pmod 5$, we obtain $\lambda = 4t + 1$, $t \geq 1$. Thus,

$$2^{4t+1} + 3 = 5^x + 5^y + 5^z, \qquad t, x, y, z \geq 1. \tag{73}$$

By taking this modulo 3 we have

$$2 \equiv (-1)^x + (-1)^y + (-1)^z \pmod 3.$$

By symmetry, it is sufficient to consider the case: $x \equiv 0$, $y \equiv z \equiv 1 \pmod 2$. Put $x = 2k$, $y = 2l - 1$, $z = 2m - 1$. Then by (73),

$$2^{4t+1} + 3 = 5^{2k} + 5^{2l-1} + 5^{2m-1}, \quad t, k, l, m \geq 1. \tag{74}$$

After multiplying (74) by 5, we consider it modulo 13:

$$10 \cdot 16^t + 2 \equiv -8(-1)^k + (-1)^l + (-1)^m,$$

i.e.

$$16^{t+1} - 2 \equiv 8(-1)^k + (-1)^{l+1} + (-1)^{m+1} \pmod{13}.$$

Taking into account that $16^1 \equiv 3$, $16^2 \equiv 9$, $16^3 \equiv 1 \pmod{13}$, notice that the expression $8(-1)^k + (-1)^{l+1} + (-1)^{m+1} + 2$ gives a residue of a power of 16 only in case when k, l, m are odd; therefore $t \equiv 1 \pmod 3$. Put $k = 2a+1$, $l = 2b + 1$, $m = 2c + 1$, $t = 3d + 1$, $a, b, c, d \geq 0$. Then by (74),

$$2^{12d+5} + 3 = 5^{4a+2} + 5^{4b+1} + 5^{4c+1}, \quad a, b, c, d \geq 0. \tag{75}$$

Modulo 7 this gives $0 \equiv 2^{4a+2} - 2^{4b+1} - 2^{4c+1}$, i.e., since $2^4 \equiv 2 \pmod 7$,

$$2^{a+1} \equiv 2^b + 2^c \pmod 7.$$

Since $2^1 \equiv 2,\ 2^2 \equiv 4,\ 2^3 \equiv 1 \pmod 7$, we evidently have three possibilities:

(a) $a \equiv b \equiv c \equiv 1 \pmod 3$,
(b) $a \equiv b \equiv c \equiv 2 \pmod 3$,
(c) $a \equiv b \equiv c \equiv 0 \pmod 3$.

Let us consider each of them.

(a) $a \equiv b \equiv c \equiv 1 \pmod 3$. Put $a = 3\beta + 1$, $b = 3\gamma + 1$, $c = 3\delta + 1$, $\beta, \gamma, \delta \geq 0$. By (75) we have

$$2^{12d+5} + 3 = 5^{12\beta+6} + 5^{12\gamma+5} + 5^{12\delta+5}, \quad \beta, \gamma, \delta \geq 0.$$

Since $5^6 \equiv -1 \pmod{601}$, we have $2^{12d+5} \equiv -1 + 2 \cdot 5^5 - 3 \equiv 236 \pmod{601}$. However, the number 236 does not appear among the residues of powers of 2 modulo 601 (see above). We have a contradiction.

(b) $a \equiv b \equiv c \equiv 2 \pmod 3$. Put $a = 3\beta + 2$, $b = 3\gamma + 2$, $c = 3\delta + 2$, $\beta, \gamma, \delta \geq 0$. By (75) we have

$$2^{12d+5} + 3 = 5^{12\beta+10} + 5^{12\gamma+9} + 5^{12\delta+9}, \quad \beta, \gamma, \delta \geq 0.$$

By taking this modulo 601 we have $2^{12d+5} \equiv 5^{10} + 2 \cdot 5^9 - 3 = -5^4 - 2 \cdot 5^3 - 3 \equiv 324 \pmod{601}$. We again obtain a contradiction.

(c) $a \equiv b \equiv c \equiv 0 \pmod 3$. Put $a = 3\beta$, $b = 3\gamma$, $c = 3\delta$, $\beta, \gamma, \delta \geq 0$. By (75) we have

$$2^{12d+5} + 3 = 5^{12\beta+2} + 5^{12\gamma+1} + 5^{12\delta+1}, \quad \beta, \gamma, \delta \geq 0. \tag{76}$$

By taking this modulo 601 we have $2^{12d+5} \equiv 25 + 10 - 3 \equiv 32 \pmod{601}$. Thus $12d \equiv 0 \pmod{25}$, and so $d \equiv 0 \pmod{25}$. Put $d = 25\lambda$, $\lambda \ge 0$. By (76),

$$2^{300\lambda+5} + 3 = 5^{12\beta+2} + 5^{12\gamma+1} + 5^{12\delta+1}, \qquad \lambda, \beta, \gamma, \delta \ge 0.$$

Now we show that γ or δ is 0. Indeed, if $\gamma, \delta \ge 1$, then $2^{300\lambda+5} \equiv -3 \pmod{25}$. Consequently, $300\lambda + 5 \equiv 17 \pmod{20}$. This is a contradiction. By symmetry we can further suppose that $\delta = 0$ in (76). We have

$$2^{300\lambda+5} - 2 = 5^{12\beta+2} + 5^{12\gamma+1}, \qquad \lambda, \beta, \gamma \ge 0. \tag{77}$$

Now we show that also $\gamma = 0$. Indeed, if $\gamma \ge 1$ then taking this modulo 25 gives

$$2^{300\lambda+5} \equiv 2 \pmod{25}, \qquad \text{so} \quad 300\lambda + 5 \equiv 1 \pmod{20}.$$

Again we obtain a contradiction.

Thus, $\gamma = 0$ in (77). Therefore

$$2^{300\lambda+5} - 7 = 5^{12\beta+2}.$$

If $\beta \ge 1$, then

$$2^{300\lambda+5} \equiv 7 \pmod{125}.$$

Notice that $\min\{\alpha \ge 1 : 2^\alpha \equiv 7 \pmod{125}\} = 85$. Since $\varphi(125) = 100$, we have $300\lambda + 5 \equiv 85 \pmod{100}$, and so $5 \equiv 85 \pmod{100}$. Again we have a contradiction. Therefore in (74), $\beta = 0$, $2^{300\lambda+5} = 32$, and $\lambda = 0$. Hence, we proved the following statement.

PROPOSITION 13. *The diophantine equation* (72): $2^\alpha + 3 = 5^x + 5^y + 5^z$ *has the only solution*: $\alpha = 5$, $x = 2$, $y = 1$, $z = 1$ *in* $x \ge y \ge z \ge 1$, $\alpha \ge 4$.

By a simple sorting out of the possibilities not included in Propositions 12, 13, using Proposition 8 we obtain

COROLLARY 4. *The diophantine equation* $2^\alpha + 3 = 5^x + 5^y + 5^z$ *has only the following solutions* (*up to a permutation of* x, y, z):

- $\alpha = 7$, $x = 3$, $y = 1$, $z = 0$;
- $\alpha = 5$, $x = 2$, $y = 1$, $z = 1$;
- $\alpha = 3$, $x = 1$, $y = 1$, $z = 0$;
- $\alpha = 2$, $x = 1$, $y = 0$, $z = 0$.

Now we are able to complete the proof of Theorem 2 when q is a Fermat prime in the following more detailed form:

PROPOSITION 14.

(i) *If* $q \ge 17$ *is a Fermat prime, then* $C_2^! \cap C_q^! = \{q+1, q+2, 2q, 2q+1\}$.
(ii) $C_2^! \cap C_3^! = \{3, 6, 7, 10, 11, 18, 19\}$.
(iii) $C_2^! \cap C_5^! = \{6, 7, 10, 11, 35, 130, 131\}$.

Proof. (i) According to Propositions 6 and 10 the solution $x = 1$, $y = 0$, $z = 0$, $\alpha = \log_2(q-1)$ of (45) (or its permutation) corresponds to the elements $q+1$, $q+2$ of $C_2^! \cap C_q^!$, while the solution $x = 1$, $y = 1$, $z = 0$, $\alpha = \log_2(q-1)$ (or its permutation) corresponds to the elements $2q$, $2q+1$.

(ii) According to Proposition 6 and Corollary 3 the solution $\alpha = 4$, $x = y = 2$, $z = 0$ of (45) (or its permutation) corresponds to the elements $18, 19$ of $C_2^! \cap C_3^!$; the solution $\alpha = 2$, $x = y = 1$, $z = 0$ (or its permutations) corresponds to $6, 7$, while the solution $\alpha = 3$, $x = 2$, $y = z = 0$ (or its permutation) corresponds to $10, 11$. Finally, notice that by Proposition 1 the numbers ≤ 5 are considered separately. Among them only $3 \in C_2^! \cap C_3^!$.

(iii) According to Proposition 6 and Corollary 4 the solution $\alpha = 7$, $x = 3$, $y = 1$, $z = 0$ (or its permutation) of (45) corresponds to the elements $130, 131$ of $C_2^! \cap C_5^!$; the solution $\alpha = 5$, $x = 2$, $y = 1$, $z = 1$ (or its permutation) corresponds to 35; the solution $\alpha = 3$, $x = 1$, $y = 1$, $z = 0$ (or its permutation) corresponds to $10, 11$, while the solution $\alpha = 2$, $x = 1$, $y = 1$, $z = 0$ (or its permutation) corresponds to $6, 7$. Finally, $5 \notin C_2^! \cap C_5^!$. This completes the proof of Theorem 2. ∎

5. Proof of Theorem 3. 1) Let q be a prime in the interval $[2^{k-1}+5, 2^k-1]$, $q \neq (2^{k+2}+3)/5$. By Theorem 2, $|C_2^! \cap C_q^!| = 2t$ if and only if $2^{t-1} \leq (q-5)/(2^k-q) < 2^t$, or

$$\frac{2^{k+t-1}+5}{2^{t-1}+1} \leq q < \frac{2^{k+t}+5}{2^t+1}, \qquad k \geq 3. \tag{78}$$

Put

$$\frac{2^{k+t-1}+5}{2^{t-1}+1} = x, \qquad \frac{2^{k+t}+5}{2^t+1} = x + \triangle x.$$

Then

$$\triangle x = \frac{2^{k+t-1} - 5 \cdot 2^{t-1}}{(2^{t-1}+1)(2^t+1)} \sim \frac{1}{2^t+1}\, x \qquad (k \to \infty).$$

By the prime number theorem, for $\lambda = 1/(2^t+1)$,

$$\pi(x + \triangle x) - \pi(x) \sim \frac{\lambda x}{\log x} \qquad (x \to \infty).$$

Therefore, the number of primes q in $[2^{k-1}+5, 2^k-1]$ for which $|C_2^! \cap C_q^!| = 2t$ is

$$\frac{\lambda x}{\pi(2^{k-1}) \log x} \sim \frac{2^{k+t-1}}{(2^t+1)(2^{t-1}+1)} \cdot \frac{k-1}{2^{k-1}(k+t-1)}$$
$$\sim \frac{2^t}{(2^{t-1}+1)(2^t+1)} \qquad (k \to \infty),$$

whence the first formula of Theorem 3 evidently follows.

Remark 5. In particular, we see that

$$\sum_{t=1}^{\infty} \frac{2^t}{(2^{t-1}+1)(2^t+1)} = 1.$$

It also follows directly that

$$\begin{aligned}\sum_{t=1}^{\infty} \frac{2^t}{(2^{t-1}+1)(2^t+1)} &= 2\sum_{t=1}^{\infty}\left(\frac{1}{2^{t-1}+1} - \frac{1}{2^t+1}\right)\\ &= 2\left(\frac{1}{2} - \frac{1}{3} + \frac{1}{3} - \frac{1}{5} + \frac{1}{5} - \cdots\right).\end{aligned}$$

2) Further, by (78) the lim sup on the left-hand side of the second formula of Theorem 3 is attained for the sequence

$$n'_m = \left\lfloor \frac{2^{m+t}+5}{2^t+1} \right\rfloor,$$

while the lim inf of the same expression is attained for the sequence

$$n''_m = \left\lfloor \frac{2^{m-1+t}+5}{2^{t-1}+1} \right\rfloor.$$

Thus we have

$$\begin{aligned}&\limsup_{n\to\infty} \frac{|\{q \in P,\ q \le n : |C_2^! \cap C_q^!| = 2t\}|}{\pi(n)}\\ &= \lim_{m\to\infty} \frac{\sum_{k\le m}\left(\pi\left(\frac{2^{k+t}+5}{2^t+1}\right) - \pi\left(\frac{2^{k+t-1}+5}{2^{t-1}+1}\right)\right)}{\pi\left(\frac{2^{m+t}+5}{2^t+1}\right)}\\ &= \lim_{m\to\infty} \frac{\sum_{k\le m}\left(\pi\left(\frac{2^{k+t}}{2^t+1}\right) - \pi\left(\frac{2^{k+t}}{2^t+2}\right)\right)}{\pi\left(\frac{2^{m+t}}{2^t+1}\right)}\\ &= \lim_{m\to\infty} \frac{\sum_{k\le m}\pi\left(\frac{2^{k+t}}{(2^t+1)(2^t+2)}\right)}{\pi\left(\frac{2^{m+t}}{2^t+1}\right)} = \frac{1}{2^{t-1}+1}\lim_{m\to\infty}\frac{\sum_{k\le m}\pi(2^{k+t-1})}{\pi(2^{m+t})}.\end{aligned}$$

Since by the Bertrand postulate $\pi(2^{m+t+1}) > \pi(2^{m+t})$, the classical Stolz theorem and the prime number theorem yield

$$\lim_{m\to\infty}\frac{\sum_{k\le m}\pi(2^{k+t-1})}{\pi(2^{m+t})} = \lim_{m\to\infty}\frac{\pi(2^{m+t-1})}{\pi(2^{m+t}) - \pi(2^{m+t-1})} = 1.$$

Thus the second formula of Theorem 3 follows.

Analogously,

$$\liminf_{n\to\infty} \frac{|\{q\in P,\ q\le n : |C_2^! \cap C_q^!| = 2t\}|}{\pi(n)}$$
$$= \lim_{m\to\infty} \frac{\sum_{k\le m-1}\left(\pi\left(\frac{2^{k+t}+5}{2^t+1}\right) - \pi\left(\frac{2^{k+t-1}+5}{2^{t-1}+1}\right)\right)}{\pi\left(\frac{2^{m-1+t}+5}{2^{t-1}+1}\right)}$$
$$= \lim_{m\to\infty} \frac{\sum_{k\le m-1}\pi\left(\frac{2^{k+t}}{(2^t+1)(2^t+2)}\right)}{\pi\left(\frac{2^{m+t-1}}{2^{t-1}+1}\right)}$$
$$= \frac{1}{2^t+1}\lim_{m\to\infty}\frac{\sum_{k\le m-1}\pi(2^{k+t-1})}{\pi(2^{m+t-1})} = \frac{1}{2^t+1}. \ \blacksquare$$

6. Some corollaries. Since the function $(x-5)/(2^k-x)$ increases for any fixed $k\ge 4$, from (44) we obtain the following result.

COROLLARY 5. *If q is a prime ≥ 7, then in the estimate*

$$|C_2^! \cap C_q^!| \le 2(1+\lfloor \log_2(q-5)\rfloor) \tag{79}$$

we have equality if and only if q is a Mersenne prime.

Further, from (79) and Proposition 2 we have:

COROLLARY 6. *If $7\le q<2^k$, then*

$$2 \le |C_2^! \cap C_q^!| \le 2k. \tag{80}$$

Moreover, the upper bound in (80) *is attained if and only if q is a Mersenne prime.*

COROLLARY 7. *If $q\ge 7$ and $n\in C_2^!\cap C_q^!$, then $n\le \frac{1}{2}(q+1)^2+3$. Equality holds for Mersenne primes ≥ 31.*

Proof. From the proof of Theorem 2 it follows that

$$S_q := \max\{n : n\in C_2^!\cap C_q^!\} \tag{81}$$
$$= \begin{cases} 19, & q=3,\\ 131, & q=5,\\ 5q-1, & q=(2^{4k+1}+3)/5,\ k\ge 1,\\ 2q+1, & q=2^{2^{k-1}}+1,\ k\ge 3,\\ 2q-3, & q=2^k+3,\ k\ge 3,\\ 2^{k+\lfloor \log_2 \frac{q-5}{2^k-q}\rfloor}+3, & 2^{k-1}+5\le q\le 2^k-1,\\ & k\ge 4,\ q\ne (2^{k+2}+3)/5. \end{cases}$$

Therefore, for $q\ge 31$ the maximal value of S_q is attained at a Mersenne prime $q = 2^k - 1, k \geq 5$. Thus, for $q \geq 31$,

$$S_q \leq (q+1)2^{\lfloor \log_2(q-5) \rfloor} + 3 = (q+1)\,\frac{q+1}{2} + 3 = \frac{1}{2}\,(q+1)^2 + 3,$$

and this estimate, according to (81), is true for $q \geq 7$. ∎

Corollary 8. *For $q = 7$ and all non-Fermat primes $q \geq 13$, $q \in (2^{k-1}, 2^k)$, $k \geq 4$, that do not have the forms $2^n + 3$, $(2^n + 3)/5$ $(n > 3)$ and for which*

$$\left\lfloor \log_2 \frac{q-1}{2^k - q} \right\rfloor \nmid k \tag{82}$$

we have

$$|C_2^! \cap C_q^!| = 2\max\{\alpha \in \mathbb{N} : \exists m,\ \lfloor 2^m/q \rfloor = 2^{\alpha-1}\}. \tag{83}$$

Proof. From the equality $\lfloor 2^m/q \rfloor = 2^{\alpha-1}$, we find

$$2^{m-\alpha} \leq \frac{2^m}{2^{\alpha-1}+1} < q < 2^{m-\alpha+1}. \tag{84}$$

So, $m - \alpha + 1 = k$. Therefore, by (84),

$$2^{m-\alpha+1} - \frac{2^m}{2^{\alpha-1}+1} > 2^k - q,$$

whence $2^k/(2^k - q) > 2^{\alpha-1} + 1$, $2^{\alpha-1} < q/(2^k - q)$. Thus,

$$\max \alpha = 1 + \left\lfloor \log_2 \frac{q}{2^k - q} \right\rfloor.$$

By Theorem 2 it is left to prove that

$$\left\lfloor \log_2 \frac{q}{2^k - q} \right\rfloor = \left\lfloor \log_2 \frac{q-5}{2^k - q} \right\rfloor. \tag{85}$$

If (85) is not true, then there exists $\beta \in \mathbb{N}$ so that

$$\frac{q-5}{2^k - q} < 2^\beta \leq \frac{q}{2^k - q},$$

so that

$$2^{k+\beta} \leq q(2^\beta + 1) < 2^{k+\beta} + 5. \tag{86}$$

But if $q(2^\beta + 1) = 2^{k+\beta} + 3$, then by Lemma 7, q has the form $(2^n + 3)/5$, contrary to assumption. Thus by (86),

$$q(2^\beta + 1) = 2^{k+\beta} + 1,$$

whence $\beta \,|\, k$ and $\beta = \left\lfloor \log_2 \frac{q-1}{2^k - q} \right\rfloor$. The latter contradicts (82). In addition notice that formula (83) is also true for $q = 7$. ∎

Corollary 9. *For every $t \geq 1$ the set of primes*

$$\{q \in P : |C_2^! \cap C_q^!| = 2t\}$$

is infinite. Moreover, every arithmetic progression $a, a+d, a+2d, \dots$ with $(a,d)=1$ contains infinitely many primes of this type for every fixed t.

Proof. If, for a fixed t, $x_k = (2^{k+t-1}+5)/(2^{t-1}+1)$, then the interval (78) contains only primes under consideration and has length asymptotically equal to $x_k/(2^t+1)$ $(k\to\infty)$. Consequently, as is well known [10], it contains asymptotically $x_k/\varphi(d)(2^t+1)\log x_k$ primes belonging to the above arithmetic progression. ∎

7. Proof of Theorem 4. In the theory of the existence of primes in short intervals the best result known to date is due to Baker, Harman and Pintz [2]. They showed for sufficiently large x the existence of a prime in the interval $(x, x+x^{0.525})$ and, moreover, obtained the estimate

$$\pi(x+x^{0.525})-\pi(x) > 0.09\,\frac{x^{0.525}}{\log x}. \tag{87}$$

According to Theorem 2 the interval (78) contains only primes $q\in(2^{k-1}+3, 2^k-1)$, $k\ge 4$, for which $|C_2^! \cap C_q^!| = 2t$ if $q\ne (2^{k+2}+3)/5$.

We shall show that for each $t\in[1, 0.475k-1]$ $(k\ge 5)$ the interval (78) contains an interval of type $[x, x+x^{0.525}]$. Indeed, we have

$$\begin{aligned}\frac{2^{k+t}+5}{2^t+1} &= \frac{2^{k+t-1}+5}{2^{t-1}+1}+\frac{2^{k+t-1}-5\cdot 2^{t-1}}{(2^{t-1}+1)(2^t+1)}\\ &> \frac{2^{k+t-1}+5}{2^{t-1}+1}+2^{k-t-1} \ge \frac{2^{k+t-1}+5}{2^{t-1}+1}+2^{0.525k}\\ &= \frac{2^{k+t-1}+5}{2^{t-1}+1}+\left(\frac{2^{k+t-1}+2^k}{2^{t-1}+1}\right)^{0.525}\\ &\ge \frac{2^{k+t-1}+5}{2^{t-1}+1}+\left(\frac{2^{k+t-1}+5}{2^{t-1}+1}\right)^{0.525}.\end{aligned}$$

By (87) for sufficiently large k the number of primes for which $|C_2^! \cap C_q^!| = 2t$ with $t\in[1, 0.475k-1]$ is not less than

$$0.09\left(\frac{2^{k+t-1}+5}{2^{t-1}+1}\right)^{0.525}\Big/\ln\frac{2^{k+t-1}+2^k}{2^{t-1}+1}\ge\frac{0.09}{\log 2}\cdot\frac{2^{0.525(k-1)}}{k}. \ ∎$$

Remark 6. Notice that if H. Cramer's 1937 conjecture ([8, A2])

$$\limsup_{n\to\infty}\frac{p_{n+1}-p_n}{(\ln p_n)^2}=1,$$

where p_n is the nth prime, is true, then in Theorem 4(i) for large enough k the number $|C_2^! \cap C_q^!|$ assumes all even values in the interval $[2, \lfloor(1-\varepsilon)k\rfloor]$.

8. Proof of Theorem 5. Notice that from Theorem 2 it follows that

$$q(1) = 37, \quad q(2) = 13, \quad q(3) = 5,$$
$$q(4) = 29, \quad q(5) = 31, \quad \dots .$$

Let $t \geq 5$. For $k \geq t$ consider the number

$$\varrho = \varrho(k,t) = \min\{j \geq 2^{k-t} : 3 \leq 2^k - j \in P\}. \tag{88}$$

It is evident that

$$2^{k-t} \leq \varrho, \quad \text{i.e.} \quad k - t \leq \lfloor \log_2 \varrho \rfloor. \tag{89}$$

LEMMA 10. *If*

$$q = 2^k - \varrho \in P, \tag{90}$$

then in (89) *equality holds if and only if*

$$|C_2^! \cap C_q^!| = 2t, \qquad t \geq 5. \tag{91}$$

Proof. It is evident that $q > 2^{k-1}$ and $\varrho < 2^{k-1}$. Let (91) be valid. Then by Theorem 2 for the prime q of (90) we have

$$\begin{aligned} t &= 1 + \left\lfloor \log_2 \frac{q-5}{2^k - q} \right\rfloor = 1 + \left\lfloor \log_2 \frac{2^k - \varrho - 5}{\varrho} \right\rfloor \\ &\leq 1 + \lfloor \log_2 (2^k - \varrho - 5) \rfloor - \lfloor \log_2 \varrho \rfloor \leq 1 + k - 1 - \lfloor \log_2 \varrho \rfloor \\ &= k - \lfloor \log_2 \varrho \rfloor, \end{aligned}$$

i.e. $k - t \geq \lfloor \log_2 \varrho \rfloor$. Therefore, in (89) we have equality.

Conversely, let

$$k - t = \lfloor \log_2 \varrho \rfloor. \tag{92}$$

Then by Theorem 2 and (90) we have

$$\begin{aligned} |C_2^! \cap C_q^!| &= 2\left(1 + \left\lfloor \log_2 \frac{q-5}{2^k - q} \right\rfloor\right) = 2\left(1 + \left\lfloor \log_2 \frac{2^k - \varrho - 5}{\varrho} \right\rfloor\right) \\ &\leq 2(1 + \lfloor \log_2 (2^{t + \lfloor \log_2 \varrho \rfloor} - \varrho - 5) \rfloor - \lfloor \log_2 \varrho \rfloor) \\ &= 2(1 + t + \lfloor \log_2 \varrho \rfloor - 1 - \lfloor \log_2 \varrho \rfloor) = 2t. \end{aligned}$$

On the other hand,

$$\begin{aligned} |C_2^! \cap C_q^!| &= 2\left(1 + \left\lfloor \log_2 \frac{2^k - \varrho - 5}{\varrho} \right\rfloor\right) \\ &\geq 2(1 + \lfloor \lfloor \log_2 (2^k - \varrho - 5) \rfloor - \log_2 \varrho \rfloor) \\ &= 2(1 + \lfloor \log_2 (2^k - \varrho - 5) \rfloor - \lfloor \log_2 \varrho \rfloor) \\ &= 2(1 + k - 1 - k + t) = 2t. \end{aligned}$$

So, $|C_2^! \cap C_q^!| = 2t$. ∎

Corollary 10. *Let*

$$k_0(t) = \min\{k \ge t : k - t = \lfloor \log_2 \varrho(t,k) \rfloor\}. \tag{93}$$

Then

$$q(t) = 2^{k_0(t)} - \varrho. \tag{94}$$

Now we complete the proof of Theorem 5. Put $x = 2^k - 2^{0.525k}$. Then

$$x + x^{0.525} = 2^k - 2^{0.525k} + 2^{0.525k}\left(1 - \frac{1}{2^{0.475k}}\right)^{0.525} = 2^k - \frac{0.525}{2^{0.475k}} - \cdots < 2^k.$$

So by (88)–(89), taking into account the above result of Baker, Harman and Pintz, for sufficiently large k, say $k \ge k_1$, we have

$$2^{k-t} \le \varrho \le 2^{\max(0.525k,\, k-t)}.$$

Therefore, the condition $k - t = \lfloor \log_2 \varrho(t,k) \rfloor$ in (93) is satisfied at least for $k \ge \max(t/0.475, k_1)$. Consequently, for large enough t, namely $t \ge 0.475k_1$, we have $k_0 \le \lceil 40t/19 \rceil$. By (94) we conclude that $q(t) \le 2^{\lceil 40t/19 \rceil}$. ∎

Remark 7. According to Cramer's above-mentioned conjecture the interval $(x, x + x^{\varepsilon})$ must contain a prime for sufficiently large x, namely $x \ge x_{\varepsilon}$. In this case in the same way one can prove that for $t \ge (1-\varepsilon)x_{\varepsilon}$ we have $q(t) = 2^{\lceil t/(1-\varepsilon) \rceil}$.

9. Numerical results. 1) Theorem 2 and Proposition 3 give a possibility to fill the following tables, except for the cases $3 \le p < q \le 47$ for which $(q-1)/(p-1)$ is a power of 2.

Table 1. The cardinality of $C_p^! \cap C_q^!$ for $2 \le p < q \le 47$

$q \setminus p$	2	3	5	7	11	13	17	19	23	29	31	37	41	43
3	7													
5	7	?												
7	6	8	9											
11	3	4	9	22										
13	4	3	11	?	23									
17	4	?	?	13	23	22								
19	3	2	10	16	38	25	42							
23	4	0	7	28	28	53	29	37						
29	8	3	16	13	15	24	48	39	40					
31	10	6	25	11	18	21	61	46	39	90				
37	2	3	8	14	36	22	36	?	52	50	63			
41	2	3	5	21	?	36	27	42	73	53	52	96		
43	2	3	5	21	26	39	25	33	109	57	55	81	147	
47	4	3	10	32	19	69	26	29	79	68	63	64	93	120

Notice that for the exceptional cases the count up to 10^8 shows that

$$|C^!_3 \cap C^!_5| \geq 25, \quad |C^!_3 \cap C^!_{17}| \geq 10, \quad |C^!_5 \cap C^!_{17}| \geq 23, \quad |C^!_7 \cap C^!_{13}| \geq 66,$$
$$|C^!_{11} \cap C^!_{41}| \geq 76, \quad |C^!_{19} \cap C^!_{37}| \geq 175.$$

Table 2. The maximal elements $M_{p,q}$ of the sets $C^!_p \cap C^!_q$, $2 \leq p < q \leq 47$

$q \setminus p$	2	3	5	7	11	13	17	19	23	29	31	37	41	43
3	19													
5	131	2												
7	34	20	20											
11	19	20	24	98										
13	35	20	38	?	54									
17	35	?	?	50	50	38								
19	35	20	39	55	170	56	152							
23	67	–	39	202	98	390	68	94						
29	259	71	260	55	54	116	144	86	68					
31	575	518	524	55	92	64	278	154	92	260				
37	67	71	74	104	332	110	152	?	184	86	154			
41	67	71	74	202	?	204	84	170	368	122	92	332		
43	67	71	74	202	175	207	84	94	730	128	128	184	696	
47	131	71	134	1550	98	1550	140	94	390	234	140	110	204	386

Notice that for the exceptional cases the count until 10^8 shows that

$$M_{3,5} \geq 524306, \quad M_{3,17} \geq 262160, \quad M_{5,17} \geq 262164,$$
$$M_{7,13} \geq 25165860, \quad M_{11,41} \geq 20503, \quad M_{19,37} \geq 18874439.$$

Further, notice that Proposition 4 gives a qualitative explanation of the variation of the numbers $M_{p,q}$, in particular, near the "resonance points" (p, q), for which $(q-1)/(p-1)$ is a power of 2.

2) The list of primes $\leq 10^8$ for which formula (83) of Corollary 8 is not true contains only 25 primes. They are:

$$3, 5, 11, 13, 17, 19, 43, 67, 103, 131, 241, 257, 683, 2731, 4099, 32771, 43691,$$
$$61681, 65537, 65539, 174763, 262147, 2796203, 6710887, 15790321.$$

3) *Evaluation of the function $q(t)$.* Notice that formulas (88), (93), (94) give a simple algorithm for finding the values of $q(t)$. It follows from Theorem 5 that the running time of this algorithm is $O(t)$ with the implicit constant in $O(\ldots)$ not exceeding $40/19$.

Example. Let $t = 6$. If $k = 6$, then $\varrho = 64 - 61 = 3$, but $6 \neq 6 - \lfloor \log_2 3 \rfloor$; if $k = 7$, then $\varrho = 128 - 113 = 15$, but $6 \neq 7 - \lfloor \log_2 15 \rfloor$; if $k = 8$, then

$\varrho = 256 - 251 = 5$ and $6 = 8 - \lfloor \log_2 5 \rfloor$. Therefore, by (93), (94), $k_0 = 8$, $\varrho = 5$, and $q(6) = 2^8 - 5 = 251$.

Table 3. Values of $q(t)$

t	1	2	3	4	5	6	7	8	9	10
$q(t)$	2^6-27	2^4-3	2^3-3	2^5-3	2^5-1	2^8-5	2^7-1	2^9-3	$2^{10}-3$	$2^{12}-5$

t	11	12	13	14	15	16	17	18	19
$q(t)$	$2^{12}-3$	$2^{16}-17$	$2^{13}-1$	$2^{17}-9$	$2^{18}-11$	$2^{18}-5$	$2^{17}-1$	$2^{20}-5$	$2^{19}-1$

t	20	21	22	23	24	25	26	27	28
$q(t)$	$2^{23}-15$	$2^{22}-3$	$2^{26}-27$	$2^{24}-3$	$2^{26}-3$	$2^{30}-35$	$2^{31}-61$	$2^{31}-19$	$2^{29}-3$

4) *On numbers n for which $e_p(n)$ and $e_q(n)$ are powers of an odd prime ν.* The following two tables are based on a natural generalization of Proposition 3. Let $\nu \geq 2$ be a prime. For a prime p define $C^!_{\nu,p} = \{n \in \mathbb{N} : \exists \alpha \in \mathbb{Z}_+,\ e_p(n) = \nu^\alpha\}$. One can prove, similarly to Proposition 3, the following generalization.

Proposition 15. *If $p < q$ are primes so that $(q-1)/(p-1)$ is not a power of ν, then the set $C^!_{\nu,p} \cap C^!_{\nu,q}$ is finite. Moreover, if $n \in C^!_{\nu,p} \cap C^!_{\nu,q}$, then*

$$n \in \left[q, 2\left(1 + \frac{\log 2}{2\log q - 1}\right)q^2 - 1\right).$$

Notice that if $\nu \geq 3$ and $p = 2$ then $(q-1)/(p-1)$ is never a power of ν and thus *all* sets $C^!_{\nu,2} \cap C^!_{\nu,q}$ are finite. In addition consider the case $p = 2, q = \nu$.

Proposition 16. *For $\nu \geq 5$ we have $|C^!_{\nu,2} \cap C^!_{\nu,\nu}| = 0$ or 2.*

Proof. Let $n \in C^!_{\nu,2} \cap C^!_{\nu,\nu}$. By Proposition 16 for $q = \nu \geq 5$ we have

$$n \leq 2\left(1 + \frac{\log 2}{2\log 5 - 1}\right)\nu^2 - 1 = 2.62\ldots\nu^2 - 1.$$

Therefore, $e_\nu(n) = 1$ or ν. Notice now that $n \notin [2\nu, \nu^2 - 1]$ (else $2 \leq e_\nu(n) \leq \nu - 1$) and $n \notin [\nu^2, 2.62\ldots\nu^2 - 1]$ (else $e_\nu(n) \geq \nu + 1$). Thus, $n \leq 2\nu - 1$ and $e_\nu(n) = 1$. Further, $n \geq \nu \geq 5$, therefore $e_2(n) \geq 3$, and consequently $e_2(n) \geq \nu$. Moreover, $e_2(n) < n \leq 2\nu - 1$. Thus, $e_2(n) = \nu$, and if n is even, also $n + 1 \in C^!_{\nu,2} \cap C^!_{\nu,\nu}$. Since $e_2(n-2) \leq \nu - 1$ and $e_2(n+2) \geq \nu + 1$, we have $|C^!_{\nu,2} \cap C^!_{\nu,\nu}| = 2$ or 0. ∎

In addition, notice that if an even $n \in C^!_{\nu,2} \cap C^!_{\nu,\nu}$ is given then by Lemmas 3, 4 using the facts that $n \leq 2\nu - 2, e_2(n) = \nu$ we have

$$\begin{aligned} \nu + 1 \leq n = e_2(n) + \sigma_2(n) &\leq \nu + \log_2(n+1) \\ &\leq \nu + \log_2(2\nu - 1) < \nu + 1 + \log_2 \nu. \end{aligned}$$

Thus, if for some even $n \in [\nu+1, \nu+1+\log_2 \nu)$ we have $e_2(n-2) \le \nu - 1$ and $e_2(n) \ge \nu + 1$, then

$$C^!_{\nu,2} \cap C^!_{\nu,\nu} = \emptyset.$$

According to Proposition 16 we have a partition of the set of all primes ≥ 5 into two subsets. In Table 4 we provide the value of $|C^!_{\nu,2} \cap C^!_{\nu,\nu}|$ for $\nu < 200$.

Table 4. The numbers $\lambda_\nu = |C^!_{\nu,2} \cap C^!_{\nu,\nu}|$, $5 \le \nu \le 199$

ν	5	7	11	13	17	19	23	29	31	37	41	43	47	53	59	61	67
λ_ν	0	2	2	0	0	2	2	0	2	0	2	0	2	2	0	0	2

ν	71	73	79	83	89	97	101	103	107	109	113	127	131	137
λ_ν	2	2	2	0	2	2	2	0	2	0	2	2	2	2

ν	139	149	151	157	163	167	173	179	181	191	193	197	199
λ_ν	0	2	0	0	0	0	2	0	2	2	2	2	0

Table 5. The cardinality of $C^!_{3,p} \cap C^!_{3,q}$ for $2 \le p < q \le 61$

$q \setminus p$	2	3	5	7	11	13	17	19	23	29	31	37	41	43	47	53	59
3	3																
5	1	1															
7	0	?	3														
11	0	1	9	4													
13	0	3	?	6	14												
17	0	9	3	16	6	10											
19	0	2	1	?	8	7	26										
23	2	1	5	5	11	10	11	22									
29	0	1	6	2	33	13	12	10	22								
31	0	3	10	6	?	20	14	12	15	61							
37	0	3	?	7	7	?	17	18	14	26	38						
41	0	3	4	7	3	18	28	19	18	17	22	59					
43	2	6	2	11	1	10	34	20	20	15	19	50	97				
47	2	6	0	14	0	5	58	36	23	18	16	34	58	77			
53	2	12	0	21	7	0	26	76	28	24	22	21	34	46	70		
59	2	1	3	4	11	1	9	30	46	29	28	22	23	27	46	82	
61	2	0	5	2	11	5	7	22	58	29	30	24	21	25	38	74	156

Notice that for the exceptional cases for which $(q-1)/(p-1)$ is a power of 3, the count up to 10^8 shows that

$$|C^!_{3,3} \cap C^!_{3,7}| \geq 8, \quad |C^!_{3,5} \cap C^!_{3,13}| \geq 18, \quad |C^!_{3,3} \cap C^!_{3,19}| \geq 7, \quad |C^!_{3,7} \cap C^!_{3,19}| \geq 29,$$
$$|C^!_{3,11} \cap C^!_{3,31}| \geq 65, \quad |C^!_{3,5} \cap C^!_{3,37}| \geq 17, \quad |C^!_{3,13} \cap C^!_{3,37}| \geq 75.$$

Remark 8. One can prove, similarly to Proposition 4, the following generalization that gives a qualitative explanation of the variation of the maximal elements $M_{\nu,p,q}$ of the sets $C^!_{\nu,p} \cap C^!_{\nu,q}$.

Proposition 17. *If ν is an odd prime and $p < q$ are primes so that $(q-1)/(p-1)$ is not a power of ν, then for $n \in C^!_{\nu,p} \cap C^!_{\nu,q}$ we have*

$$\frac{n}{\log(n+1)} \leq \max(a_\nu(p,q), b_\nu(p,q)),$$

where

$$a_\nu(p,q) = \frac{p-1}{\log p}\,(1 - \nu^{-\{\log_\nu \frac{q-1}{p-1}\}})^{-1},$$
$$b_\nu(p,q) = \frac{q-1}{\log q}\,(1 - \nu^{\{\log_\nu \frac{q-1}{p-1}\}^{-1}})^{-1}.$$

10. Open problems

1. Is $C^!_p$ infinite for $p \geq 3$?

Due to the fact that C_p is of density close to 1 by Theorem 1, we expect the answer to be in the affirmative.

2. Is the set $C^!_p \cap C^!_q$ finite for primes $3 \leq p < q$ with $(q-1)/(p-1)$ a power of 2?

3. Does the diophantine equation $\sigma_p(n) = \sigma_q(n)$, where $p \neq q$ are fixed primes, have infinitely many solutions?

4. Is the set of primes q for which $|C^!_2 \cap C^!_q| = 3$ infinite?

Notice that by Theorem 2 this question is equivalent to the question about the infinity of primes of the form $2^n + 3$.

5. Is the set of primes q for which $|C^!_2 \cap C^!_q| = 5$ infinite?

By Theorem 2, this question is equivalent to the question about the infinity of primes of the form $(2^n + 3)/5$.

6. Is the set of primes q for which $|C^!_2 \cap C^!_q| \neq 2\max\{\alpha \in \mathbb{N} : \exists m,\ \lfloor 2^m/q \rfloor = 2^{\alpha-1}\}$, infinite?

The question arises in view of Corollary 8.

7. Find a generalization of Theorem 2 to the set $C^!_{\nu,\nu} \cap C^!_{\nu,q}$, $\nu < q$ (see Sections 7, 4).

Remark 9. Together with Proposition 15, one can obtain a generalization of Proposition 5: if $p < q$ are primes so that $(q-1)/(p-1)$ is a power of ν (≥ 3), then $n \in C^!_{\nu,p} \cap C^!_{\nu,q}$ if $n \in C^!_{\nu,p}$ and $\sigma_p(n) = \sigma_q(n)$ (and for $n \geq q^2$, only if).

Moreover, if we call the primes of the form $1+(\nu-1)\nu^k$ ν-*Fermat primes*, then for $n \geq 2\nu$, $p=\nu$ and a ν-Fermat prime q (cf. Proposition 5(ii)) we have: $n \in C^!_{\nu,\nu} \cap C^!_{\nu,q}$ if and only if $n \in C^!_{\nu,\nu}$ and $\sigma_\nu(n)=\sigma_q(n)$. Moreover, as in Proposition 1 one can prove that for $n \geq \nu^3-\nu^2+\nu$ we have: $n \in C^!_{\nu,\nu}$ if and only if n has the form $(\nu-1)\nu^\alpha+\nu+i$, $\alpha \geq 2$, $i=0,1,\ldots,\nu-1$. Taking into account that $[2\nu,\nu^3-\nu^2+\nu) \cap C^!_{\nu,\nu}=\emptyset$, we conclude that if $n \geq 2\nu$ and q is a ν-Fermat prime, then there is a bijection between $C^!_{\nu,\nu} \cap C^!_{\nu,q}$ and the set of solutions of the diophantine equation

$$\sum_{j=1}^{2\nu-1} q^{x_j}=(\nu-1)\nu^\alpha+2\nu-1, \qquad \nu \geq 2,$$

in integers $\alpha \geq 2$, $0 \leq x_1 \leq \cdots \leq x_{2\nu-1}$ (cf. Proposition 6).

8. Is the set $\{p \in P : |C^!_{p,2} \cap C^!_{p,p}|=t\}$ infinite a) for $t=0$; b) for $t=2$?

Remark 10. Notice that this question for $t=2$ is equivalent to the question of infinitude of primes of the form $p=e_2(n)$, $n \in \mathbb{N}$. E.g., for the Mersenne primes $p=2^k-1, k \geq 3$, we have $e_2(p+1)=p$. Thus, in this case $|C^!_{p,2} \cap C^!_{p,p}|=2$. On the other hand, for the Fermat primes $p=2^k+1$, $k \geq 2$, we have $e_2(p+1)=p-1$ and $e_2(p+3)=p+1+\delta_{p,5}$. Thus, for each Fermat prime $p \geq 5$ the set $C^!_{p,2} \cap C^!_{p,p}$ is empty.

Analogously, one can show that for a prime p of the form $p=2^k+2^l-1$, $2 \leq l \leq k-1$, we have $e_2(p+3)=p$. Thus, $|C^!_{p,2} \cap C^!_{p,p}|=2$. On the other hand, for a prime p of the form $p=2^k-l$, $3 \leq l \leq k$, we have $e_2(p+l-2)<p$, $e_2(p+l)>p$. Therefore, $C^!_{p,2} \cap C^!_{p,p}=\emptyset$, etc.

Acknowledgments. The author would like to express his deep gratitude to Professor Daniel Berend (Department of Mathematics and of Computer Science, Ben-Gurion University), without the fruitful conversations with whom this article most likely would not have been written. The author also wishes to thank Professor Simon Litsyn (Department of Electrical Engineering Systems, Tel-Aviv University) and Professor Andrzej Schinzel (IMPAN, Warsaw) for some important advice.

References

[1] L. J. Alex, *On the diophantine equation* $1+2^a=3^b5^c+2^d3^e5^f$, Math. Comp. 44 (1985), 267–278.

[2] R. C. Baker, G. Harman and J. Pintz, *The difference between consecutive primes, II*, Proc. London Math. Soc. (3) 83 (2001), 532–562.

[3] D. Berend, *Parity of exponents in the factorization of* $n!$, J. Number Theory 64 (1997), 13–19.

[4] K. Chandrasekharan, *Introduction to Analytic Number Theory*, Springer, Berlin, 1968.

[5] Y.-G. Chen, *On the parity of exponents in the standard factorization of* $n!$, J. Number Theory 100 (2003), 326–331.
[6] Y.-G. Chen and Y.-C. Zhu, *On the prime power factorisation of* $n!$, ibid. 82 (2000), 1–11.
[7] P. Erdős and R. L. Graham, *Old and New Problems and Results in Combinatorial Number Theory*, Enseign. Math., Univ. de Genève, Genève, 1980.
[8] R. K. Guy, *Unsolved Problems in Number Theory*, Springer, New York, 1981.
[9] F. Luca and P. Stanica, *On the prime power factorization of* $n!$, J. Number Theory 102 (2003), 298–305.
[10] K. Prachar, *Primzahlverteilung*, Springer, 1957.
[11] J. C. Puchta und J. Spilker, *Altes und Neues zur Quersumme*, Math. Semesterber. 49 (2002), 209–226.
[12] B. Rosser, *Explicit bounds for some functions of prime numbers*, Amer. J. Math. 63 (1941), 211–232.
[13] J. W. Sander, *On the parity of exponents in the prime factorization of factorials*, J. Number Theory 90 (2001), 316–328.
[14] V. S. Shevelev, *Multiplicative functions in the Fermi–Dirac arithmetic*, Izv. Vyssh. Uchebn. Zaved. Sev.-Kavk. Reg. Estestv. Nauki 1996, no. 4, 28–43 (in Russian).
[15] W. Sierpiński, *Elementary Theory of Numbers*, North-Holland and PWN–Polish Sci. Publ., 1988.
[16] E. Trost, *Primzahlen*, Birkhäuser, 1953.
[17] A. Walfisz, *Weylsche Exponentialsummen in der neueren Zahlentheorie*, Deutsch. Verlag Wiss., Berlin, 1963.

Department of Mathematics
Ben-Gurion University of the Negev
Beer-Sheva 84105, Israel
E-mail: shevelev@bgu.ac.il

Received on 12.8.2005
and in revised form on 9.10.2006 (5052)