A RELATION BETWEEN TRIANGULAR NUMBERS AND PRIME NUMBERS

Rigoberto Flórez  
Division of Mathematics, Science and Engineering, University of South Carolina  
Sumter, Sumter, SC, U.S.A.  
florezr@uscsumter.edu

Leandro Junes  
Division of Mathematics, Science and Engineering, University of South Carolina  
Sumter, Sumter, SC, U.S.A.  
junesl@uscsumter.edu

Received: 3/26/11 , Revised: 5/30/11, Accepted: 8/4/11, Published: 8/8/11

Abstract  
We study a relation between factorials and their additive analog, the triangular numbers. We show that there is a positive integer k such that n! = 2^kT where T is a product of triangular numbers. We discuss the primality of T±1 and the primality of |T − p| where p is either the smallest prime greater than T or the greatest prime less than T.

1. Introduction

There is a natural relation between triangular numbers and factorials. Triangular numbers are the additive analogs of factorials. We show that there is a positive integer k such that n! = 2^kT where T is a product of triangular numbers. The number of factors of T depends on the parity of n.

There are many open questions about the relationship between prime numbers and factorials. For example, are there infinitely many primes of the form n! ± 1? Erdős [4] asked if there are infinitely many primes p for which p − k! is composite for each k such that 1 ≤ k! ≤ p. Fortune’s conjecture [5] asks whether the product of the first n consecutive prime numbers plus or minus one is a prime. Since T is a product of triangular numbers, it is natural to ask whether T ± 1 is a prime. It is also natural to ask whether |T − p| is a prime number, where p is either the smallest prime greater than T or the greatest prime less than T.

In this paper we prove that there are infinitely many cases for which T ± 1 is not a prime. We also give both numerical and theoretical evidence for the primality of
\[ |T - p| \text{ where } p \neq T \pm 1. \]

We now formally state the question. We denote by \( t_n \) the \( n^{th} \) triangular number where \( n \geq 0 \) with \( t_0 = 0 \) and \( t_n = t_{n-1} + n \). We define \( T(k) = \prod_{i=1}^{k} t_{2i-1} \) and \( T'(k) = t_3 \prod_{i=3}^{k} t_{2i} \) for \( k > 2 \) an integer. If there is no ambiguity, we use \( T \) to mean either \( T(k) \) or \( T'(k) \).

**Question 1.** If \( T \) is either \( T(k) \) or \( T'(k) \), and \( p \) is either the smallest prime greater than \( T + 1 \) or the greatest prime less than \( T - 1 \), then

(1) are there infinitely many primes of the form \( T \pm 1 \)?

(2) Is \( |T - p| \) a prime number?

2. Preliminaries

In this section we introduce some notation. Throughout the paper we use \( k \) to represent a positive integer. We prove that \( n! = 2^k \prod_{i=0}^{k-1} (t_k - t_i) \) if \( n = 2k \) and \( n! = 2^k \prod_{i=0}^{k-1} (t_k + t_i - t_i) \) if \( n = 2k + 1 \). Proposition 2, part (2) is in [2, 3]. Proposition 2, part (1) is a natural relation. Therefore, we believe that it is known, but unfortunately we have not found this property in the mathematics literature.

**Proposition 2.** If \( n \) is a positive integer, then

(1) \( n! = \begin{cases} 2^k T(k) & \text{if } n = 2k \\ 2^{k+1} T'(k) & \text{if } n = 2k + 1. \end{cases} \)

(2) \( T(k) = \prod_{i=0}^{k-1} (t_k - t_i). \)

(3) \( 2T'(k) = \prod_{i=0}^{k-1} (t_k + t_i - t_i). \)

**Proof.** We prove part (1) for \( n = 2k \), the other case is similar.

\[
2^k T(k) = 2^k \cdot t_1 \cdot t_3 \ldots t_{2k-1} \\
= 2^k \cdot \frac{1 \cdot 2 \cdot 3 \cdot 4 \cdots (2k-1) \cdot 2k}{2} \\
= (2k)! = n!.
\]

We now prove part (2). We suppose that \( n = 2k \). From part (1) we know that \( n! = 2^k T(k) \). So,

\[
2^k T(k) = 1 \cdot 2 \cdot 3 \cdot 4 \ldots k \cdot (k + 1) \ldots (2k - 3) \cdot (2k - 2) \cdot (2k - 1) \cdot 2k \\
= [1 \cdot 2k] \cdot [2 \cdot (2k - 1)] \cdot [3 \cdot (2k - 2)] \ldots [k \cdot (k + 1)] \\
= [k \cdot (k + 1)] \ldots [3 \cdot (2k - 2)] \cdot [2 \cdot (2k - 1)] \cdot [1 \cdot (2k)] \\
= \prod_{i=0}^{k-1} (k - i) \cdot (k + i + 1)
\]
\[ \begin{align*}
&= \prod_{i=0}^{k-1} (k^2 + k - i^2 - i) \\
&= \prod_{i=0}^{k-1} (k(k + 1) - i(i + 1)).
\end{align*} \]

Therefore,

\[ T(k) = \frac{1}{2^k} \prod_{i=0}^{k-1} (k(k + 1) - i(i + 1)) \]
\[ = \prod_{i=0}^{k-1} \left( \frac{k(k + 1)}{2} - \frac{i(i + 1)}{2} \right) \]
\[ = \prod_{i=0}^{k-1} (t_k - t_i). \]

We prove part (3). We suppose that \( n = 2k + 1 \). It is easy to see that
\[ 2T'(k) = \frac{T(k + 1)}{(k + 1)}. \]

Thus,
\[ 2T'(k) = \frac{T(k + 1)}{k + 1} = \frac{1}{k + 1} \prod_{i=0}^{k-1} (t_{k+1} - t_i) = \prod_{i=0}^{k-1} (t_{k+1} - t_i). \]

Notice that \( 2T'(k) = \prod_{i=1}^{k} t_{2i} \). Therefore, we can ask Question 1 replacing \( T'(k) \) by \( 2T'(k) \). Numerical calculations show that Question 1, part (2) is true for \( 2T'(k) \) with \( k \leq 1000 \). We have found that there are only 9 prime numbers of the form \( 2T'(k) - 1 \) for \( k \leq 1000 \) and 12 prime numbers of the form \( 2T'(k) + 1 \) for \( k \leq 1000 \).

Since \( t_k = \binom{k+1}{2} \), Proposition 2, part (1) can be restated as
\[ n! = 2^k \prod_{i=1}^{k} \left( \frac{2i}{2} \right) = 2^k \prod_{i=0}^{k-1} \left( \binom{k + 1}{2} - \binom{i + 1}{2} \right) \]
if \( n = 2k \)

and
\[ n! = 2^k \prod_{i=1}^{k} \left( \frac{2i + 1}{2} \right) = 2^k \prod_{i=0}^{k-1} \left( \binom{k + 2}{2} - \binom{i + 1}{2} \right) \]
if \( n = 2k + 1 \).

We use Theorem 3 to prove Propositions 6 and 7. These propositions give upper bounds for the number of primes in an interval.
Let $f$ be a real function and $g$ be a positive function. We use $f \ll g$ to mean that there is a constant $c > 0$ such that $|f(x)| \leq cg(x)$ for all $x$ in the domain of $f$. This is also denoted by $f = O(g)$. For the following two theorems $q$ is a prime. If $N$ is a positive even integer, we write $\pi_N(x)$ to denote the number of primes $b$ up to $x$ such that $N + b$ is also prime, and, we write $r(N)$ to denote the number of representations of $N$ as the sum of two primes.

Theorem 3. [6, Theorems 7.2 and 7.3] If $N$ is a positive even integer, then

\begin{align*}
(1) \quad \pi_N(x) &\ll \frac{x}{(\ln x)^2} \prod_{q \mid N} \left(1 + \frac{1}{q}\right). \\
(2) \quad r(N) &\ll \frac{N}{(\ln N)^2} \prod_{q \mid N} \left(1 + \frac{1}{q}\right).
\end{align*}

3. Evidences for Primality of $|T - p|

In this section we provide strong evidence that Question 1, part (2) is probably true. We use the prime number theorem to give a first approach for the validity of this question, and construct several examples that show that $|T - l|$ is a prime where $l$ is a prime number. We found that if $l$ is in a specific interval, then $|T - l|$ is a prime (we give a detailed description of this interval below.) We give an upper bound for the number of primes in this interval.

Propositions 4 and 6 give a theoretical support to believe that the facts shown in the following examples may be true in general. In Section 5 there are 2 tables that show some primes of the form $Q - T$ and $T - q$, where $Q$ is the smallest prime greater than $T$ and $q$ greatest prime less than $T$. We have observed that $Q$ is in the interval $(T, T + p^2)$ where $p$ is either the smallest prime greater than $2k$ if $T = T(k)$ or is the smallest prime greater than $2k + 1$ if $T = T'(k)$. From Table 4 we can verify that either $p \leq Q - T < p^2$ or $Q - T = 1$. From Table 1 we can verify that either $T - p^2 < q \leq T - p$ or $T - q = 1$. Using a computer program the authors verified that this fact is also true for all $k \leq 10^3$. Since every number in $(T + 1, T + p)$ is composite, we are going to analyze the behavior of $Q$ in $[T + p, T + p^2)$ and $Q = T + 1$. In Proposition 4 we show that if $T + p \leq Q < T + p^2$, then it proves Question 1, part (2).

We first give a heuristic argument to show that if $Q \neq T + 1$, then $T + p \leq Q < T + p^2$. It is known from prime number theorem that if $q$ is the next prime greater than a number $m + 1$, then $q$ is near $m + \ln m$. So, $Q$ is near $T + \ln T$. If $p$ is the next prime greater than $n$, then

$$
\ln(T) = \ln \left(\frac{n!}{2k}\right) \sim n \ln n - n - k \ln 2 + 1 < p^2.
$$
Therefore, if $Q \neq T + 1$ and $Q < T + \ln T$, then $T + p \leq Q < T + p^2$.

We now give some examples that show that there are several primes $l$ that satisfy $T + p \leq l < T + p^2$. Proposition 6 gives a general upper bound for the total number of primes of the form $T + b$ in $[T + p, T + p^2)$ where $b$ is a prime.

If $k = 3$, then $T(3) = 90$, $2k = 6$ and $p = 7$. So, $p^2 = 49$. These give rise to the interval $[T + p, T + p^2) = [97, 139]$. In this interval there are 9 primes. Thus, $Q - T(3)$ is prime where $Q$ is a prime with $97 \leq Q < 139$. Indeed, all possible outcomes for $Q - T(3)$ are: $97 - 90 = 7; 101 - 90 = 11; 103 - 90 = 13; 107 - 90 = 17; 109 - 90 = 19; 113 - 90 = 23; 127 - 90 = 37; 131 - 90 = 41; 137 - 90 = 47$. Note that 139 is a prime, but $139 - 90 = 49 = 7^2$.

For the next example we need $k > 3$. If we take $k = 4$, then $T'(4) = 11340, 2k + 1 = 9$ and $p = 11$. So, these give rise to the interval $[T + p, T + p^2) = [11351, 11461)$. For every prime $Q$ in $[11351, 11461)$, it holds that $Q - T'(4)$ is a prime. That is, $11351 - 11340 = 11; 11353 - 11340 = 13; 11359 - 11340 = 29; 11383 - 11340 = 43; 11393 - 11340 = 53; 11399 - 11340 = 59; 11411 - 11340 = 71; 11423 - 11340 = 83; 11437 - 11340 = 97; 11443 - 11340 = 103; 11447 - 11340 = 107$.

We have observed that $Q - T$ is also a prime for some primes $Q$ greater than $T + p^2$. That is, if there is no prime number between $T$ and $T + p^2$, this does not automatically mean that Question 1, part (2) will fail. For example, if $k = 5$, then $T(5) = 113400, 2k = 10$ and $p = 11 > 2k$. So, $p^2 = 121$. These give rise to the interval $[T + p, T + p^2) = [113411, 113521)$. The number $T(5) + 121 = 113400 + 121 = 113521 = 61 \cdot 1861$. We analyze the behavior of $Q - T(5)$, for consecutive primes $Q$ beyond $T(5) + 11^2$. The outcomes for $Q - T(5)$ are: $113537 - 113400 = 137; 113539 - 113400 = 139; 113557 - 113400 = 157; 113567 - 113400 = 167; 113591 - 113400 = 191$.

This example shows that if we take a prime $Q$ beyond $T + p^2$, then $Q - T$ is not automatically composite. Thus, even if there is no prime number between $T$ and $T + p^2$, we can expect that $Q - T$ may be a prime. Notice, if the next prime greater than $T$ is $Q = T + p^2$, then the question fails.

The following example shows that there are several primes $q$ such that $T(k) - q$ is either one or a prime with $T(k) - p^2 < q < T(k)$.

If $k = 3$, then $T(3) = 90$, $2k = 6$ and $p = 7$. So, $p^2 = 49$. These give rise to the interval $(T - p^2, T - p) = (41, 83)$. In this interval there are 10 primes $q$. All possible outcomes for $T(3) - q$ are: $90 - 83 = 7; 90 - 79 = 11; 90 - 73 = 17; 90 - 71 = 19; 90 - 67 = 23; 90 - 61 = 29; 90 - 59 = 31; 90 - 53 = 37; 90 - 47 = 43; 90 - 43 = 47$. In this example, 41 is prime, but $90 - 41 = 49 = 7^2$. Note that $T(3) - 1 = 89$ is prime. In Table 3 there are some $k$ values for which $T(k) - 1$ is prime.

We now give some notation needed for Propositions 4 and 6. We use $p_k$ to mean the smallest prime greater than $n$ when $n$ is either $2k$ if $T = T(k)$ or $2k + 1$ if $T = T'(k)$. The subscript $r$ takes a special role: $r - 1$ counts the number of primes less than or equal to $n$. 


Propositions 6 and 7 are a direct application of Theorem 3. We obtain an upper bound for the number of primes in the intervals \([T + p_r, T + p_r^2]\) and \((T - p_r^2, T + p_r]\). If there is a prime in the intervals \([T + p_r, T + p_r^2]\) then it gives a positive answer for Question 1, part (2). If Cramer’s Conjecture \([1]\) is true, then there is a prime in \([T + p_r, T + p_r^2]\).

**Proposition 4.** Let \(l\) be a prime and \(k > 3\).

1. If \(T + p_r \leq l < T + p_r^2\), then \(l - T\) is prime.
2. If \(T - p_r^2 < l \leq T - p_r\), then \(T - l\) is prime.

**Proof.** We prove part (1) for \(T = T(k)\), the other case and part (2) are similar. Suppose that \(T + p_r \leq l < T + p_r^2\). Since \(T(k) = \frac{(2k)!}{2^k}\), every prime \(t < 2k\) divides \(T(k)\). Thus, if \(t < 2k\) is a prime, then \(t\) does not divide \(l - T(k)\). We know that \(p_r \leq l - T(k) < p_r^2\). Since \(p_r^2\) is the smallest composite number that satisfies that \(T(k)\) and \(p_r^2\) are relatively prime, \(l - T\) is a prime number.

**Corollary 5.** If \(p\) is a prime and \(k > 3\), then

1. if \(p \in [T + p_r, T + p_r^2]\), then \(p\) has the form \(T + b\) where \(b\) is a prime.
2. if \(p \in (T - p_r^2, T - p_r]\), then \(p\) has the form \(T - b\) where \(b\) is a prime.

**Proof.** We prove part (1); part (2) is similar. Suppose that \(p \in [T + p_r, T + p_r^2]\), by Proposition 4, \(p - T\) is prime. Therefore, \(p = T + (p - T)\).

**Proposition 6.** The number of primes in \([T + p_r, T + p_r^2]\) is \(O((n + 1)r^2)\).

**Proof.** We prove the case \(n = 2k\), the other case is similar. By Corollary 5 the number of primes in \([T + p_r, T + p_r^2]\) is \(\pi_T(p_r^2)\) as in Theorem 3, part (1). Thus,

\[
\pi_T(p_r^2) \leq \frac{p_r^2}{(\ln p_r)^2} \prod_{p \mid T} \left(1 + \frac{1}{p}\right).
\]

\[
\pi_T(p_r^2) \leq \frac{p_r^2}{4(\ln p_r)^2} \prod_{t=1}^{n} \frac{t + 1}{t} = \left(\frac{p_r}{\ln p_r}\right)^2 \frac{n + 1}{4}.
\]

If \(r\) tends to infinity, then by the Prime Number Theorem \(r \sim \frac{p_r}{\ln p_r}\). This implies that \(\pi_T(p_r^2) = O(r^2(n + 1))\).

**Proposition 7.** The number of primes in \((T - p_r^2, T - p_r]\) is \(O\left(\frac{T}{\log T} (n + 1)\right)\).
Proof. Let \( S_T(p_r) \) be the number of primes of the form \( T - l \) where \( l < p_r^2 \) is prime. By Corollary 5 the number of primes in \( (T - p_r^2, T - p_r) \) is \( S_T(p_r) \). If \( T - l \) is a prime where \( l < p_r^2 \) is a prime, then \( T \) can be written as a sum of two primes. Indeed, \( T = (T - l) + l \). This and Theorem 3, part (2), imply that

\[
S_T(p_r) \leq r(T) \ll \frac{T}{\log^2 T} \prod_{q \mid T} \left( 1 + \frac{1}{q} \right) \leq \frac{T}{\log T} \prod_{t=1}^{n} \left( \frac{t+1}{t} \right) = \frac{T}{\log T} (n+1).
\]

This proves that \( S_T(p_r) \) is \( O \left( \frac{T}{(\log T)^2} (n+1) \right) \). \( \square \)

4. Primality of \( T \pm 1 \)

We are going to discuss whether a number of the form \( T \pm 1 \) is not a prime. From Tables 4 and 1 we observe that there are few primes of the form \( T \pm 1 \). For example, in our search we have found only 6 primes of the form \( T(k) - 1 \), for \( 2 \leq k \leq 2000 \) (see Table 2). Table 3 shows all \( k \) values for which \( T \pm 1 \) is prime, for \( k \leq 2000 \). Note that \( T(2000) \approx 1.59 \times 10^{12072} \).

Propositions 8, 9 and 10 prove that there are infinitely many \( k \) such that \( T \pm 1 \) is not a prime. These results give rise to another question. Are there infinitely many primes of the form \( T \pm 1 \)? We now formally state the propositions.

Proposition 8. If \( p > 7 \) is a prime number with \( p \) equal to either \( 2k + 1 \) or \( 2k + 3 \), then

1. \( p \equiv \pm 1 \) mod 8 if and only if \( p \) is a proper divisor of \( T(k) + 1 \).

2. \( p \equiv \pm 3 \) mod 8 if and only if \( p \) is a proper divisor of \( T(k) - 1 \).

Proof. We suppose that \( p \equiv \pm 1 \) mod 8 and prove that \( p \) divides \( T(k) + 1 \). If \( k = \frac{p-1}{2} \), then

\[
(2k)! = \left( 2 \cdot \frac{p-1}{2} \right)! = (p-1)!
\]

Therefore, by Wilson’s theorem \( (2k)! \equiv -1 \) mod \( p \). Since \( p \equiv \pm 1 \) mod 8, by the law of quadratic reciprocity 2 is a quadratic residue modulo \( p \). Therefore, by Euler’s criterion \( 2^k = 2^{\frac{p-1}{2}} \equiv 1 \) mod \( p \). This and Proposition 2 imply that

\[
T(k) = \frac{(2k)!}{2^k} = \frac{(p-1)!}{2^{\frac{p-1}{2}}} \equiv -1 \text{ mod } p.
\]

Thus, \( p \) divides \( T(k) + 1 \).
We suppose that \( p = T(k) + 1 \). That is,

\[
p = T(k) + 1 = \frac{(p - 1)!}{2^{\frac{p-1}{2}}} + 1.
\]

Therefore, \( (p - 1)! = (p - 1)2^{\frac{p-1}{2}} \). This implies that \( (p - 2)! = 2^{\frac{p-3}{2}} \). That is a contradiction. This proves that \( p \) is a proper divisor of \( T(k) + 1 \).

We now suppose that \( k = \frac{p - 3}{2} \). Since

\[
T(k) = \frac{(p - 3)!}{2^{\frac{p-3}{2}}} = \frac{(p - 3)!(-2)(1)}{2^{\frac{p-3}{2}}(2-1)(2)},
\]

\[
\frac{(p - 3)!}{2^{\frac{p-3}{2}}} \equiv \frac{(p - 3)!(p - 2)(p - 1)}{2^{\frac{p-3}{2}}} \equiv -1 \mod p.
\]

Thus, \( p \) divides \( T(k) + 1 \). If \( p = T(k) + 1 \), then

\[
p - 1 = \frac{(p - 3)!}{2^{\frac{p-3}{2}}}. \tag{1}
\]

Since \( p > 7 \), \( p - 3 = 2t \) for some \( t \geq 4 \). Thus,

\[
(p - 3)! = (2t)! = 2 \cdot 4 \cdots (2t) \cdot 1 \cdot 3 \cdots (2t - 1) = 2^t \cdot (1 \cdot 3 \cdots (2t - 1)).
\]

Therefore, \( (p - 3)!/2^t = t! \cdot (1 \cdot 3 \cdots (2t - 1)) \). This, (1) and \( p - 3 = 2t \) imply that \( 2(t + 1) = t! \cdot (1 \cdot 3 \cdots (2t - 1)) \). That is a contradiction, since \( 2(t + 1) < t! \) for \( t \geq 4 \). This proves that \( p \) is a proper divisor of \( T(k) + 1 \).

Conversely, we assume that \( p \) is a proper divisor of \( T(k) + 1 \) and prove that \( p \equiv \pm 1 \mod 8 \). We suppose that \( k = \frac{p - 1}{2} \). Since \( p \) is a proper divisor of \( T(k) + 1 \), \( T(k) \equiv -1 \mod p \). So, \( 2k! \equiv -2^k \mod p. \) Therefore, \( (p - 1)! \equiv -2^{\frac{p-1}{2}} \mod p. \) This and the Wilson’s theorem imply that \( 2^{\frac{p-1}{2}} \equiv 1 \mod p. \) By the law of quadratic reciprocity 2 is a quadratic residue modulo \( p. \) This implies that \( p \equiv \pm 1 \mod 8. \)

We now suppose that \( k = \frac{p - 3}{2} \). Since \( p \) divides \( T(k) + 1 \), \( T(k) \equiv -1 \mod p. \) So, \( (2k)! \equiv -2^k \mod p. \) Therefore, \( \left( 2^{(p - 3)/2} \right)! \equiv -2^{\frac{p-3}{2}} \mod p. \) Thus,

\[
(p - 3)!(p - 2)(p - 1) \equiv -2^{\frac{p-3}{2}}(-2)(-1) \mod p.
\]

This implies that

\[
(p - 1)! \equiv -2^{\frac{p-1}{2}}(2^{-1})(-2)(-1) \mod p.
\]

Since \( (p - 1)! \equiv -1 \mod p, \) \( 2^{\frac{p-1}{2}} \equiv 1 \mod p. \) This implies that \( p \equiv \pm 1 \mod 8. \)
Proof of part (2). We prove that \( p \) divides \( T(k) - 1 \). Suppose that \( p \equiv \pm 3 \text{ mod } 8 \). Wilson’s theorem and \( k = \frac{p-1}{2} \) imply that \( (2k)! \equiv -1 \text{ mod } p \). Since \( p \equiv \pm 3 \text{ mod } 8 \), by the quadratic reciprocity law, 2 is not a quadratic residue modulo \( p \). Therefore, by Euler’s criterion, \( 2^k = 2^{\frac{p-1}{2}} \equiv -1 \text{ mod } p \). This implies that \( T(k) \equiv 1 \text{ mod } p \).

So, \( p \) divides \( T(k) - 1 \). We suppose \( p = T(k) - 1 \). That is, \( p = \frac{(p-1)!}{2^{\frac{p-3}{2}}} - 1 \). So, 

\[
(p-1)! = (p+1)2^{\frac{p-3}{2}} \cdot \text{ That is a contradiction.}
\]

If \( k = \frac{p-3}{2} \), then

\[
T(k) = \frac{(p-3)!}{2^{\frac{p-3}{2}}} = \frac{(p-3)!}{2^{\frac{p-3}{2}}}(-1)^{\frac{p-3}{2}} \equiv 1 \text{ mod } p.
\]

So, the proof follows as above, proving that \( p \) is a proper divisor of \( T(k) - 1 \).

We prove that \( p \equiv \pm 3 \text{ mod } 8 \). Suppose that \( k = \frac{p-1}{2} \). Since \( p \) divides \( T(k) - 1 \), \( T(k) \equiv 1 \text{ mod } p \). So, \( (2k)! \equiv 2^k \text{ mod } p \). Therefore, \( (p-1)! \equiv 2^{\frac{p-3}{2}} \text{ mod } p \). This and Wilson’s theorem imply that \( 2^k \equiv -1 \text{ mod } p \). By the law of quadratic reciprocity, 2 is not a quadratic residue modulo \( p \). This implies that \( p \equiv \pm 3 \text{ mod } 8 \).

We now suppose that \( k = \frac{p-3}{2} \). Since \( p \) divides \( T(k) - 1 \), \( T(k) \equiv 1 \text{ mod } p \). So, \( (2k)! \equiv 2^k \text{ mod } p \). Therefore, \( \left(2^{\frac{(p-3)}{2}}\right)! = 2^{\frac{p-3}{2}} \equiv 1 \text{ mod } p \).

Thus, 

\[
(p-3)! (p-2) (p-1) \equiv 2^{\frac{p-3}{2}} (-2)(-1) \text{ mod } p.
\]

This implies that \( (p-1)! \equiv 2^{\frac{p-3}{2}} (2^{-1})(-2)(-1) \text{ mod } p \). This and Wilson’s theorem imply that \( 2^{\frac{p-3}{2}} \equiv -1 \text{ mod } p \). Thus, \( p \equiv \pm 3 \text{ mod } 8 \). \( \square \)

**Proposition 9.** If \( p > 3 \) is a prime number with \( p = 2k + 3 \), then

(1) \( p \equiv \pm 1 \text{ mod } 8 \) if and only if \( p \) is a proper divisor of \( T'(k) - 1 \).

(2) \( p \equiv \pm 3 \text{ mod } 8 \) if and only if \( p \) is a proper divisor of \( T'(k) + 1 \).

**Proof.** The proofs of parts (1) and (2) are similar to the proofs of Proposition 8, parts (1) and (2), respectively. \( \square \)

**Proposition 10.** Let \( p \) be a prime number such that \( p = 4k + 1 \). Then \( p \equiv 5 \text{ mod } 8 \) if and only if \( p \) is a proper divisor of either \( T'(k) + 1 \) or \( T'(k) - 1 \).

**Proof.** We first prove that \( \left(\frac{p-1}{2}\right)! \equiv -1 \text{ mod } p \). Obviously,

\[
(p-1)! = (1)(p-1)(2)(p-2) \ldots \left(\frac{p-1}{2}\right) \left( p - \frac{p-1}{2} \right).
\]
Therefore,
\[(p - 1)! \equiv (1)(-1)(2)(-2) \ldots \left(\frac{p - 1}{2}\right) \left(-\frac{p - 1}{2}\right) \mod p.\]

So,
\[(p - 1)! \equiv \left(\frac{p - 1}{2}\right)! \left(\frac{p - 1}{2}\right)!(-1)\frac{2}{2} \mod p.
\]

Since \(p = 4k + 1\), \((-1)^{k+1} = 1\). These and Wilson’s theorem imply that
\[
\left[\left(\frac{p - 1}{2}\right)!\right]^2 \equiv -1 \mod p. \tag{2}
\]

We now prove that \(p \equiv 5 \mod 8\) if and only if \(p\) is a proper divisor of either \(T(k) - 1\) or \(T(k) + 1\).

\((T(k))^2 \equiv 1 \mod p\) if and only if \(\left[\frac{2k}{2}\right]^2 \equiv 1 \mod p\) if and only if \(\left[\left(\frac{p - 1}{2}\right)!\right]^2 \equiv 1 \mod p.\)

This and (2), imply that
\[(T(k))^2 \equiv 1 \mod p\] if and only if \(2^{\frac{p-1}{2}} \equiv -1 \mod p\) if and only if \(p \equiv \pm 3 \mod 8.\)

Since \(p = 4k + 1\), \((T(k))^2 \equiv 1 \mod p\) if and only if \(p \equiv 5 \mod 8.\)

It is easy to see that if \(p\) is a divisor of either \(T(k) + 1\) or \(T(k) - 1\), then \(p\) is a proper divisor of either \(T(k) + 1\) or \(T(k) - 1\), respectively.

---

5. Tables

<table>
<thead>
<tr>
<th>(k)</th>
<th>(T(k) - q = \text{prime or 1})</th>
<th>(T'(k) - q = \text{prime or 1})</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>6 - 5 = 1</td>
<td>15 - 13 = 2</td>
</tr>
<tr>
<td>3</td>
<td>90 - 89 = 1</td>
<td>315 - 313 = 2</td>
</tr>
<tr>
<td>4</td>
<td>2520 - 2503 = 17</td>
<td>11340 - 11329 = 11</td>
</tr>
<tr>
<td>5</td>
<td>113400 - 113383 = 17</td>
<td>623700 - 623699 = 1</td>
</tr>
<tr>
<td>6</td>
<td>7484400 - 7484383 = 17</td>
<td>48648600 - 48648583 = 17</td>
</tr>
<tr>
<td>7</td>
<td>681080400 - 681080383 = 17</td>
<td>5108103000 - 5108102983 = 17</td>
</tr>
<tr>
<td>8</td>
<td>81729648000 - 81729647983 = 17</td>
<td>694702008000 - 694702007995 = 41</td>
</tr>
<tr>
<td>9</td>
<td>12504636144000 - 12504636143963 = 37</td>
<td>118794043368000 - 118794043367959 = 41</td>
</tr>
</tbody>
</table>

Table 1: Some primes of the form \(T - q\).
<table>
<thead>
<tr>
<th>k</th>
<th>Primes of the form $T(k) - 1$ for $1 &lt; k \leq 2000$</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>5</td>
</tr>
<tr>
<td>3</td>
<td>89</td>
</tr>
<tr>
<td>56</td>
<td>274017871895886614355245021851226872507509906980847975994484266521420</td>
</tr>
<tr>
<td></td>
<td>299245431500324669448454596593562846812310336529662113876355622264674</td>
</tr>
<tr>
<td></td>
<td>03999999999999999999999999999999999999</td>
</tr>
<tr>
<td>92</td>
<td>45001884356933882276227680596716006487089310681842539412541262048834</td>
</tr>
<tr>
<td></td>
<td>586837442952533537944205073472685159662546130153568890072873003795362</td>
</tr>
<tr>
<td></td>
<td>844451732581915058880113820207363358420852271846934410469478569624</td>
</tr>
<tr>
<td></td>
<td>63448505001949173095424216090269152543162087775133027616686079999999</td>
</tr>
<tr>
<td></td>
<td>99999999999999999999999999999999999999999999999999999999999999999999999</td>
</tr>
<tr>
<td>162</td>
<td>3915489045156717160513467872605008943291008048615998438632660593157</td>
</tr>
<tr>
<td></td>
<td>753938515286639595274480801803070927492211738171154934229102563766</td>
</tr>
<tr>
<td></td>
<td>29000032583951616619365288810637027813680446264582621040916668979828</td>
</tr>
<tr>
<td></td>
<td>58099991694315770272696168113862960117719779637815690306771585482508</td>
</tr>
<tr>
<td></td>
<td>107493783063031921640283161853810875428608665503789432862597460676</td>
</tr>
<tr>
<td></td>
<td>242327508423837879730051196922906972778986492294546611691256473129914</td>
</tr>
<tr>
<td></td>
<td>302664438196211535426598076748503430292272338133961040599560472739917</td>
</tr>
<tr>
<td></td>
<td>7450795107467206207869788258773512931544414565370969180904816639999</td>
</tr>
<tr>
<td></td>
<td>99999999999999999999999999999999999999999999999999999999999999999999999</td>
</tr>
<tr>
<td>170</td>
<td>34083526380004639832567760669297890375992796910781694237134220511694</td>
</tr>
<tr>
<td></td>
<td>59240722167451257352322669416194117314785261273499504784994820875427</td>
</tr>
<tr>
<td></td>
<td>864201761806754518975857807052407100550266675844455903421176972834</td>
</tr>
<tr>
<td></td>
<td>591260193200046550397020555465344872560673854426859683541035239901055</td>
</tr>
<tr>
<td></td>
<td>283433221132729908219748602654016681914173408384514905620110985521</td>
</tr>
<tr>
<td></td>
<td>966631215768575310684931422732355954952363718728820158624169776756</td>
</tr>
<tr>
<td></td>
<td>5345082565699216067256543121046992785044507318407554205409308573862</td>
</tr>
<tr>
<td></td>
<td>6945834092499747361419974907605708422218605584741173228268050943735</td>
</tr>
<tr>
<td></td>
<td>766736030844019883759359587830999999999999999999999999999999999999999999</td>
</tr>
</tbody>
</table>

Table 2: Some primes of the form $T(k) - 1$.

<table>
<thead>
<tr>
<th>Form</th>
<th>k values for which $T \pm 1$ is prime</th>
<th>Search limit</th>
</tr>
</thead>
<tbody>
<tr>
<td>$T(k) + 1$</td>
<td>2, 4, 6, 70, 146, 448, 978</td>
<td>2000</td>
</tr>
<tr>
<td>$T(k) - 1$</td>
<td>2, 3, 56, 92, 162, 170</td>
<td>2900</td>
</tr>
<tr>
<td>$T'(k) + 1$</td>
<td>7, 16, 18, 24, 38, 44, 194, 286, 382, 895</td>
<td>1000</td>
</tr>
<tr>
<td>$T'(k) - 1$</td>
<td>5, 12, 16, 24, 41, 46, 75, 337, 904, 2485</td>
<td>3200</td>
</tr>
</tbody>
</table>

Table 3: Some $k$ values for which $T \pm 1$ is prime.
\begin{table}
\begin{tabular}{|c|c|c|}
\hline
k & $Q - T(k)$ = prime or 1 & $Q - T'(k)$ = prime or 1 \\
\hline
2 & $7 - 6 = 1$ & $17 - 15 = 2$ \\
3 & $97 - 90 = 7$ & $317 - 315 = 2$ \\
4 & $2521 - 2520 = 1$ & $11351 - 11340 = 11$ \\
5 & $113417 - 113400 = 17$ & $623717 - 623700 = 17$ \\
6 & $7484401 - 7484400 = 1$ & $48648617 - 48648600 = 17$ \\
7 & $681080429 - 681080400 = 29$ & $5108103001 - 5108103000 = 1$ \\
8 & $81729648019 - 81729648000 = 19$ & $694702008041 - 694702008000 = 41$ \\
9 & $12504636144029 - 12504636144000 = 29$ & $118794043368047 - 118794043368000 = 47$ \\
\hline
\end{tabular}
\end{table}

Table 4: Some primes of the form $Q - T$.

Acknowledgment The authors are indebted to Florian Luca, for his comments that helped to improve the paper. We also thank A. Castaño for inspiring us to work on this problem.

References


