Abstract

In this paper, we present the definition, some properties and solve a problem on special primes. These properties help in providing us with better understanding of the problem posed related to special primes on the open problem garden website [1]. The problem involves finding all the primes $q$, given a prime $p$ such that $q \equiv 1 \pmod{p}$ and $2^{\frac{q-1}{p}} \equiv 1 \pmod{q}$. We prove that a prime number $q$ is a special prime of $p$ if and only if order of 2 in $U(q)$ divides $\frac{q-1}{p}$. Also we prove that a prime number $q$ is not a special prime for any prime number if 2 is a generator of the group $U(q)$ and some other properties.

Keywords: special primes, properties

1. Introduction

Since there is more than one definition for a special prime, we define explicitly what we mean by a special prime, and this definition is used throughout our discussion.

Let $p$ be any natural prime then the definition of a special prime is given by the following.

**Definition:** A prime number $q$ is a special prime of $p$, if $q \equiv 1 \pmod{p}$ and $2^{\frac{q-1}{p}} \equiv 1 \pmod{q}$.

**Problem:** Let $p$ be a prime number. Find all $q$ such that $q \equiv 1 \pmod{p}$ and $2^{\frac{q-1}{p}} \equiv 1 \pmod{q}$. 

Preprint submitted to The College Mathematics Journal November 13, 2020
2. Preliminaries

First we need some facts from number theory. The number of elements in $U(n)$ is commonly denoted by $\phi(n)$, the Euler phi-function. When $p$ is prime $\phi(p) = p - 1$ because every number less than $p$ is relatively prime to $p$. Also the reader is assumed to have the knowledge of elementary concepts in group theory such as cyclic groups, unitary group and Lagrange’s theorem.

**Theorem 1.** A prime number $q$ is a special prime of $p$ if and only if $|2|$ in $U(q)$ divides $\frac{q-1}{p}$.

*Proof.* If $q$ is a special prime of $p$, consider the group $U(q)$ the order of the group is given by $\phi(q)$. Since $q$ is a prime $\phi(q) = q - 1$ observe that 2 belongs to the group $U(q)$ and let $|2| = \psi$

By the definition of the order of a group and since 1 is the identity element of the group $U(q)$, we have $2^\psi \mod q = 1$

Also for any $k \in \mathbb{N}$ we have, $2^{k\psi} \mod q = 1$. Thus $\frac{q-1}{p} = k\psi$ for some $k \in \mathbb{N}$

$\Rightarrow |2| = \psi$ divides $\frac{q-1}{p}$

Conversely, if $|2|$ in the group $U(q)$, (where $q$ is a prime) divides $\frac{q-1}{p}$, then

$$\frac{q-1}{p} = \psi \times k$$

for some natural number $k$ and $\psi$ is the order of element 2

Now, $2^{\frac{q-1}{p}} \mod q = (2^\psi)^k \mod q = 1$ Hence $q$ is a special prime. $\square$

**Corollary 1.** Given any prime number $q$, is a special prime for only finite number of primes.

*Proof.* Let $q$ be a prime and consider the group $U(q)$

Let $|2| = \psi$, then by the above theorem for $q$ to be special prime of $p$, $p$ must satisfy the following equation

$$\frac{q-1}{p} = \psi \times k$$

for some natural number $k$ The number of primes satisfying this equation are finite. $\square$
Corollary 2. A prime number $q$ of the form $2^n + 1$ for some natural number $n$, is a special prime only for the prime number 2.

Proof. Consider the group $U(q) = U(2^n + 1)$ then the order of the group is $\phi(2^n + 1) = 2^n$

By the above theorem $q$ is a special prime of primes - $p$ that satisfy the equation

$$\frac{q - 1}{p} = k\psi$$

given the hypothesis of the theorem the above equation now becomes

$$\frac{2^n}{p} = k\psi$$

The only prime number satisfying the equation is 2.

By now it must be clear that a prime number $q$ being a special prime or not depends on the prime number we choose. For example, 17 is a special prime of 2 but is not a special prime for any other prime number. Though we do not prove this fact, there is no prime number which is a special prime for every prime number. Also there are prime numbers which are not special primes for any natural prime number. The following theorem reveals the nature of such primes.

Theorem 2. If 2 is a generator of the group $U(q)$, then $q$ is not a special prime for any prime number $p$.

Proof. Let $q$ be the given prime and consider the group $U(q)$

we know from previous theorem that $q$ is a special prime of $p$ if and only if it satisfies the equation

$$\frac{q - 1}{p} = k\psi$$

Since 2 is a generator of the group $U(q)$ , $|2| = q - 1$

The above equation now becomes

$$\frac{q - 1}{p} = k(q - 1)$$

which has no natural prime solutions.

3
The next question is - for what values of \(q\), 2 is a generator in \(U(q)\). Though we do not know the exact form of \(q\) that satisfies the above condition, we shall find the density of such primes over a finite range on \(\mathbb{N}\).

Let \(P(< 2 >= U(q))\) denote the probability that 2 is a generator in \(U(q)\).

**Theorem 3.** Let \(X\) be a natural number, then the probability that 2 is a generator in \(U(q)\), where \(q\) is a random natural number on \([1, X]\) satisfies,

\[
\frac{2}{(q - 1)\ln(X)} \leq P(< 2 >= U(q)) \leq 1
\]

**Proof.** By the Prime Number Theorem, we know that the density of primes on \([1, X]\) is \(\frac{1}{\ln(X)}\). Suppose that the random natural number picked (say \(q\)) is an odd prime, implies that the unitary group \(U(q)\) is a cyclic group. Any generator of \(U(q)\) where \(q\) is a prime has order \(q - 1\). The number of elements of order \(q - 1\) is given by \(\phi(q - 1)\). Thus,

\[
P(< 2 >= U(q)) = \frac{1}{\phi(q - 1)}
\]

we have,

\[
\phi(q - 1) \leq \frac{q - 1}{2}
\]

This implies,

\[
P(< 2 >= U(q)) \geq \frac{2}{q - 1}
\]

But we obtained this inequality on the assumption that \(q\) is a prime. If we were to remove that restriction we simply have to divide the right hand side of the inequality by \(\ln(X)\). Therefore we obtain

\[
\frac{2}{(q - 1)\ln(X)} \leq P(< 2 >= U(q)) \leq 1
\]

\(\square\)

**Theorem 4.** Let \(q\) be a prime number of the form \(2p + 1\), where \(p\) is a prime number such that 2 is not a generator of the group \(U(q)\) then \(q\) is a special prime of 2.
Proof. Let \( q \) be a prime of the form \( 2p + 1 \), consider the group \( U(q) \)

Order of the group is \( \phi(2p + 1) = 2p \) we know that \( 2 \) belongs to \( U(q) \)

By Lagrange’s theorem, we know that order of a group element must divide
order of the group.

\[ \Rightarrow |2| \text{ must divide } |U(q)| = 2p \]

given the above information, the possible orders for \( 2 \) are \( 2, p \) and \( 2p \).

The case when \( |2| = 2p \) is not possible because, if \( |2| = 2p \) then \( 2 \) is a
generator of \( U(q) \) which is a contradiction.

Similarly, for any prime number \( p \), \( |2| \neq 2 \) in the group \( U(2p + 1) \)

\[ \Rightarrow |2| = p \]

From Theorem 1, for a prime to be special prime it must satisfy the following

equation

\[ \frac{q - 1}{x} = k\psi \]

Since \( \psi = p \), the above equation now becomes

\[ \frac{2p}{x} = pk \]

clearly, the only solution to the above equation is \( 2 \)

Now, using Theorem 1 and Theorem 2 we will prove the final theorem which
is a solution to the problem discussed in the introduction.

**Theorem 5.** Given a prime \( p_0 \), all prime numbers \( q \) of the form \( q \equiv 1(mod p_0) \)
are special primes of \( p_0 \), except if \( a_0 \leq b_0 \), where \( a_0 \) and \( b_0 \) are the powers of \( p_0 \)
in the prime decomposition of \( q - 1 \) and order of \( 2 \) in \( U(q) \) respectively.

Proof. For a prime number \( q \) to be special prime number of \( p_0 \) it must satisfy
the following conditions \( q \equiv 1(mod p_0) \) and \( 2^{\frac{q-1}{p_0}} mod q = 1 \)

Consider all primes of the form \( q \equiv 1(mod p_0) \), now we investigate which
primes \( q \) satisfy the following condition for a given \( p_0 \)

\[ \frac{q - 1}{p_0} = \psi \times k \]
Let prime decomposition of \( q - 1 = p_0^{a_0} \times p_1^{a_1} \times ... \times p_n^{a_n} \) and the prime decomposition of \( \psi = p_0^{b_0} \times p_1^{b_1} \times ... \times p_m^{b_m} \). The above equation now becomes,

\[
\frac{1}{p_0} \prod_{i=0}^{n} p_i^{a_i} = k \prod_{j=0}^{m} p_j^{b_j}
\]

we will handle the possible values of \( b_0 \) in cases:

Case 1 : If \( b_0 = 0 \), then clearly \( q \) is a special prime of \( p_0 \)

Case 2 : Similarly, if \( b_0 \geq 1 \) and \( a_0 \leq b_0 \) then the above equation becomes,

\[
\frac{1}{x} \prod_{i=1}^{n} p_i^{a_i} = k \times p_0^{b_0 - a_0} \prod_{j=1}^{m} p_j^{b_j}
\]

clearly, \( x = p_0 \) does not satisfy the equation.

Case 3 : If \( b_0 \leq a_0 \) then \( q \) is a special prime of \( p_0 \). Since, \( p_0 \) is a solution to the equation

\[
\frac{q - 1}{x} = \psi \times k
\]

In conclusion, a prime number \( q \) such that \( q \equiv 1 \mod p_0 \) is not a special prime of given \( p_0 \) if \( a_0 \leq b_0 \)

\[
\square
\]

References

URL http://www.openproblemgarden.org/op/special_primes