Special Primes And Some Of Their Properties

Anantha Krishna B*[1], Mantha Sai Gopal†[2], and Sourangshu Ghosh‡[3]

[1]*Sri Sathya Sai Institute of Higher Learning*
[2]*Sri Sathya Sai Institute of Higher Learning*
[3]*Indian Institute of Technology Kharagpur*

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.The problem involves finding all the primes q, given a prime p such that $q \equiv 1(\mathrm{mod}p)$ and $2^{\frac{q-1}{p}} \equiv 1(\mathrm{mod}q)$. 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 that there exist infinitely many special primes for any given prime number.

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 $q \equiv 1(\mathrm{mod}p)$ and $2^{\frac{q-1}{p}} \equiv 1(\mathrm{mod}q)$.

Problem: Let p be a prime number. Find all q such that $q \equiv 1(\mathrm{mod}p)$ and $2^{\frac{q-1}{p}} \equiv 1(\mathrm{mod}q)$. [1]

2 Preliminaries

Before we study the properties of the special primes we need to discuss the elementary concepts in group theory such as cyclic groupsand Lagrange's theorem.

*Email address: ananthakrishnab2001@gmail.com
†Email address: sgptp99@gmail.com
‡Email address: sourangshug123@gmail.com ; Corresponding author

Definition 2.1. ***Cyclic Groups****: A cyclic group is a group that is generated by a single element. For any element g in any group G, one can get the other group elements by taking integer powers $\langle g\rangle = \{g^k | k \in \mathbb{Z}\}$.*

Theorem 2.1. ***Lagrange's theorem****: If G is a finite group of order n and H is a subgroup of G of order k, then k divides n and n/k is the number of distinct cosets of H in G. If H is a subgroup of a group G, then*

$$|G| = [G : H] \cdot |H| \,.|G| = [G : H] \cdot |H|$$

Lagrange's theorem can be further extended to state that if H is a subgroup of G and K is a subgroup of H, then

$$[G : K] = [G : H]\,[H : K].[G : K] = [G : H]\,[H : K].$$

The converse of Lagrange's theorem is not, in general, true [2] [3]. In this paper, we shall denote $U(n)$ as the set of numbers lesser than and prime to n.

3 Special primes and the group $U(n)$

Theorem 3.1. *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 $2^{\psi}(\mathrm{mod} q) = 1$

Also for any $k \in \mathbb{N}$ we have, $2^{k\psi}(\mathrm{mod} q) = 1$. 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 ψ is the order of element 2. Now, $2^{\frac{q-1}{p}}(\mathrm{\ mod\ } q) = (2^{\psi})^k(\mathrm{mod} q) = 1$. Hence q is a special prime □

Corollary 3.1. *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 above equation are finite □

Corollary 3.2. *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, given 2 is not a generator in the group $U(q)$*

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

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

only prime number satisfying the equation is 2 □

Corollary 3.3. *Let $p = 5$, all special primes q of p end with 1. Equivalently, $q \equiv 1(\mathrm{mod}10)$.*

Proof. By above theorem, we know that if q is a special prime of 5 then,

$$\frac{q-1}{5} = \psi \times k$$

for some natural number k. Thus we can rewrite the above equation as $q - 1 = 5\psi \times k$ Since q is odd prime, 2 divides $q - 1$. Thus either ψ or k must be even. Therefore, $q - 1 = 10\lambda$ or $q = 10\lambda + 1$ □

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. Clearly, 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.

Theorem 3.2. *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 □

The next question is - for what values of q, 2 is a generator in $U(q)$. Equivalently, it is to find all primes q such that 2 is a primitive root modulo q. Before that we need to state the Artin's conjecture on primitive roots.

Conjecture 3.1. *(Artin's conjecture) Let us assume that a is an integer not equal to -1 that is not a perfect square. Let us also write $a = a_0 b^2$ such that a_0 is square-free and $S(a)$ the set of prime numbers p such that a is a primitive root modulo p. Then the Artin's conjecture on primitive roots states:*

1. *The set $S(a)$ has a positive asymptotic density inside the set of primes and it is an infinite set.*
2. *Assuming that a is not a perfect power and that $a_0 \not\equiv 1(\mathrm{mod}4)$, this density is independent of a and equals Artin's constant C_{Artin}*

$$C_{Artin} = \prod_{p\, prime} \left(1 - \frac{1}{p(p-1)}\right) = 0.3739558136\ldots$$

For a not satisfying the above conditions, Gerard [5] proved similar conjectural product formulas for the density. In all the cases, the conjectural density is always a rational multiple of C_{Artin}. Assuming that the generalized Riemann hypothesis holds true, Hooley [6] proved a conditional proof for the conjecture. Brown showed that at least one of 2, 3, or 5 is a primitive root modulo infinitely many primes p [7]. He also proved that there are at most two primes for which Artin's conjecture fails.

Definition 3.1. *A number g is a primitive root modulo n, if for every integer a co-prime to n, there is some integer k for which $g^k \equiv a(modn)$.*

Trivially, g is a primitive root modulo n if and only if g is a generator of the multiplicative group of integers modulo n. The problem of finding the prime numbers q such that 2 is a generator in $U(q)$ is equivalent to finding all prime numbers q such that 2 is a primitive root $modq$. Thus if we assume that Artin's conjecture on primitive roots is true, then the set of primes p for which 2 is a primitive root has the density C_{Artin}.

Theorem 3.3. *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. This implies, $|2|$ 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 $U(2p+1)$. Thus $|2| = p$

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 3.4. *Given a prime p_0, all prime numbers q of the form $q \equiv 1(\text{mod } p_0)$ 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 $q \equiv 1(\text{mod}p_0)$ and $2^{\frac{q-1}{p}} \text{ mod } q = 1$. Consider all primes of the form $q \equiv 1(\text{ mod } p_0)$, 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 $\psi = {p_0}^{b_0} \times {p_1}^{b_1} \times ... \times {p_m}^{b_i}$ 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 $a_0 \leq b_0$ □

We shall next prove that there exist infinitely many special primes for any given prime p. Before that we state the Dirichlet's theorem on arithmetic progressions [9] which shall be used in it's proof.

Theorem 3.5. *(Dirichlet) For any two positive co-prime integers a and d, there are infinitely many primes of the form $a+nd$, where n is also a positive integer.*

The special case of $a = 1$ was proved by Euler by analyzing the splitting behavior of primes in cyclotomic extensions [10]. This theorem can be proved by showing that the value of the non-trivial character Dirichlet L-function at 1 is nonzero. This requires some calculus and analytic number theory [11]. An elementary proof was given by Selberg [12].

Theorem 3.6. *There exist infinitely many special primes for any given prime p.*

Proof. Let p be arbitrary prime number.To prove this theorem it is sufficient (by Theorem 1) to show that there exist infinitely many prime numbers q such that ψ (order of 2 in $U(q)$) divides $\frac{q-1}{p}$. Now we claim that there exist infinitely many primes q_i such that ψ is distinct in each $U(q_i)$. Say on the contrary there are only finite number of distinct values possible for ψ. This implies that there exist infinitely many prime numbers q_i such that $|2|$ is equal in each of the groups $U(q_i)$. This is however not possible, because, as $q_i \to \infty$, there exists N such that for all $n > N$, $q_n > 2^{\psi}$. This implies that $2^{\psi} mod q_n = 2^{\psi} \neq 1$. This is a contradiction and thus there exist infinitely many primes q_i such that ψ is distinct in each $U(q_i)$. Let this set be $Q = \{q_1, q_2, q_3, \dots\}$
By Theorem 4 we know that a prime number q is not a special prime of p if $a_0 \leq b_0$. Let us remove those prime numbers for which $a_0 \leq b_0$ from Q. If such primes are finite in number then we are done, since the remaining infinite primes are special primes for the given prime. However, if such primes are infinitely many then we must show that there are infinitely many primes in Q such that $a_0 \geq b_0$. Say on the contrary there are only finite number of primes such that $a_0 \geq b_0$.
Consider the polynomial $q(x) = p(kx) + 1$, where k is a natural number. Since $\gcd(p, 1) = 1$, by Dirichlet's theorem the polynomial $q(x)$ is a prime number for infinitely many values of x. This implies that the equation

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

has infinitely many prime number solutions q in the variable ψ. But we assumed that there are only finite number of primes such that $a_0 \geq b_0$. This implies that there exist only finite number of values of x which are the possible values for $|2|$ in $U(q)$, where x is a natural number and q is a prime number. This is a contradiction to the fact that there exist infinitely many distinct values for $|2|$ in $U(q)$, where q is a prime. Thus there exist infinitely many prime numbers that satisfy the condition $a_0 \geq b_0$ and by Theorem 4 all such primes are special primes of p. Thus any prime number p has infinitely many special primes. □

4 Quadratic forms and special primes

Definition 4.1 (Integral Binary Quadratic form)**.** *A quadratic homogeneous polynomial in two variables of the form,*

$$q(x, y) = ax^2 + bxy + cy^2$$

Let $S_2(x)$ denote the number of special primes less than or equal to x.

Theorem 4.1. $S_2(x) \approx \frac{x}{lnx^2}$

Proof. (Euler's criterion) Let q be an odd prime number and $\gcd(a, p) = 1$, then $a^{(\frac{p-1}{2})} \equiv 1(\bmod p)$ if and only if a is a quadratic residue of p. Let $a = 2$ then by above criterion q is a special prime of 2 if and only if $\left(\frac{2}{q}\right) = 1$. We know that $\left(\frac{2}{q}\right) = 1$ if and only if $q \equiv 1$ or $7(\bmod 8)$. Let $\pi_a(x)$ denote the function that counts the number of primes $\leq X$ in the progression $nk + a, n \in \mathbf{N}$
By Prime number theorem for arithmetic progressions [8] we have $\pi_a(x) \approx \frac{\pi(x)}{\phi(x)} \approx \frac{1}{\phi(x)} \frac{x}{lnx}$ if $(a, k) = 1$. Thus by taking $k = 8$ and $a = 1$ or 7 we get $S_2(x) = \pi_1(x) + \pi_7(x) \approx \frac{2}{\phi(8)} \frac{x}{lnx} \approx \frac{x}{lnx^2}$ □

Theorem 4.2. 2 *is a cubic residue modulo p if and only if* $2^{\frac{p-1}{3}} \equiv 1(\bmod p)$

Proof. (Euler's criterion) A number $a \not\equiv 0(\bmod p)$ is a power residue of degree n modulo a prime number p if and only if $a^{\frac{p-1}{\delta}} \equiv 1(\bmod p)$, where $\delta = \gcd(p - 1, n)$.
Let $n = 3$ and $a = 2$. Let $p \equiv 1(\bmod 3)$. Since, $2 \not\equiv 0(\bmod p)$. Thus by Euler's criterion 2 is a cubic residue modulo p if and only if $2^{\frac{p-1}{\delta}} \equiv 1(\bmod p)$ where, $\delta = \gcd(p - 1, 3)$. Clearly, $\delta = 3$ since $p - 1 \equiv 0(\bmod 3)$ □

Corollary 4.1. *A prime number q is of the form* $x^2 + 27y^2$ *if and only if q is a special prime of* 3*.*

Proof. Fermat proved that every prime $p \equiv 1(\bmod 3)$ can be written as $p = a^2 + 3b^2$ [13] [14]. Euler stated that if 2 is a cubic residue modulo q, then b is divisible by 3. Therefore a prime number q of the form $x^2 + 27y^2$ if and only if $q \equiv 1(\bmod 3)$ and 2 is a cubic residue modulo q. Thus by above theorem, it implies that q is a special prime of 3 if and only if q is of the form $x^2 + 27y^2$ □

Conjecture 4.1. *There exists an integer n for any prime p such that q is a special prime of p if and only if q is of the form* $x^2 + ny^2$

References

[1] George Balan (2011), Special Primes, Open Problem Garden,

[2] Gallian, J. A. "On the Converse of Lagrange's Theorem." Math. Mag. 66, 23, 1993.

[3] Gallian, J. A. Contemporary Abstract Algebra, 3rd ed. Lexington, MA: D. C. Heath, 1994.

[4] Hogan, G. T. "More on the Converse of Lagrange's Theorem." Math. Mag. 69, 375-376, 1996.

[5] Michon, Gerard P. (2006-06-15). "Artin's Constant". Numericana.

[6] Hooley, Christopher (1967). "On Artin's conjecture". J. Reine Angew. Math. 225: 209–220. doi:10.1515/crll.1967.225.209. MR 0207630.

[7] D. R. Heath-Brown (1986), Artin's Conjecture for Primitive Roots , The Quarterly Journal of Mathematics 37(1), 27-38, doi: 10.1093/qmath/37.1.27

[8] H. Daboussi (1989), On the prime number theorem for arithmetic progressions, Journal of Number Theory 31(3),243-254, doi: 10.1016/0022-314X(89)90071-1

[9] Dirichlet, P. G. L. (1837), "Beweis des Satzes, dass jede unbegrenzte arithmetische Progression, deren erstes Glied und Differenz ganze Zahlen ohne gemeinschaftlichen Factor sind, unendlich viele Primzahlen enthält", Abhandlungen der Königlichen Preußischen Akademie der Wissenschaften zu Berlin, 48: 45–71

[10] Neukirch, Jürgen (1999), Algebraic number theory. Translated from the 1992 German original and with a note by Norbert Schappacher, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], 322, Berlin: Springer-Verlag, ISBN 3-540-65399-6, MR 1697859, Zbl 0956.11021.

[11] Serre, Jean-Pierre (1973), A course in arithmetic, Graduate Texts in Mathematics, 7, New York; Heidelberg; Berlin: Springer-Verlag, ISBN 3-540-90040-3, Zbl 0256.12001.

[12] Selberg, Atle (1949), "An elementary proof of Dirichlet's theorem about primes in an arithmetic progression", Annals of Mathematics, 50 (2): 297–304, doi:10.2307/1969454, JSTOR 1969454, Zbl 0036.30603

[13] Gauss, Disquisitiones Arithmeticae, Art. 182

[14] Cox, David A. (1989), Primes of the form x^2+ny^2, New York: Wiley, ISBN 0-471-50654-0