PRIMES p HAVING AT MOST ONE DIVISOR OF $p-1$ OF A SPECIFIED MULTIPLICATIVE ORDER

Peter Fletcher
Christiansburg, Virginia

Camron Withrow
Department of Mathematics, Virginia Tech, Blacksburg, Virginia
cwithrow@vt.edu

Received: 1/30/19, Accepted: 10/25/19, Published: 11/4/19

Abstract

For a prime p, let $L(p)$ denote the least common-multiple of the multiplicative orders in $(\mathbb{Z}/p\mathbb{Z})^\times$ of the divisors of $p-1$. We investigate those primes p with the property that there is exactly one divisor of $p-1$ of order $L(p)$. This condition is closely related to two other properties: there is exactly one divisor of $p-1$ that is a primitive root; the restriction of multiplicative order to the set of divisors of $p-1$ is a permutation on this set. Indeed, through 10^{12} we have found no prime that distinguishes some two of these properties. If p is a prime with the putatively strongest of these three properties and p is not 5, then $p-1$ is square free. Our proof of this proposition relies on a property of primes for which there is a divisor of $p-1$ of order three. Finally we look at primes p for which no divisor of $p-1$ has order $L(p)$ and for which $p-1$ is square free. These primes have interesting properties, but we have only empirical evidence for the two most intriguing possibilities that for these primes $L(p) = p-1$ and that for these primes the order of any divisor of $p-1$ other than 1 and $p-1$ is a multiple of the largest prime divisor of $p-1$.

1. Introduction

Throughout p denotes a prime greater than 3, $(\mathbb{Z}/p\mathbb{Z})^\times$ denotes the group of units of the field $\mathbb{Z}/p\mathbb{Z}$, and for $x \in \mathbb{Z}/p\mathbb{Z}$, $\widehat{\mathfrak{o}}(x)$ is the multiplicative order of x.

Let D_{p-1} denote the lattice of divisors of $p-1$; if the prime p is understood, we will often omit it from the notation, writing D for D_{p-1}. For $d \in D$, d^* denotes $(p-1)/d$, the complement of d. We investigate the function $\mathfrak{o}$ on D defined by

$$\mathfrak{o}(d) = \widehat{\mathfrak{o}}([d]),$$

where $[d] \in \mathbb{Z}/p\mathbb{Z}$ is the image of d under the canonical quotient $\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$. We denote the odd part of $\mathfrak{o}(d)$ by $\overline{\mathfrak{o}}(d)$, and the join of the elements

$$\{\mathfrak{o}(d) : d \in D\}$$

by $L(p)$. (Note, $L(p)$ is the least common-multiple of the set $\{\mathfrak{o}(d) : d \in D\}$.) We sometimes use terminology relating to $\mathbb{Z}/p\mathbb{Z}$ for elements of D, for example we may say $d \in D$ is a *primitive root* provided $[d] \in \mathbb{Z}/p\mathbb{Z}$ is a primitive root.

We first consider which primes have the property that $\mathfrak{o} : D \to D$ is a permutation. The first five primes have this property, but the property is more restrictive than this auspicious beginning makes it appear. We are also concerned with a related question, which we conjecture is the same question in disguise: for which primes is there exactly one divisor of $p-1$ that is a primitive root? These questions lead naturally to the consideration of primes for which there is a divisor of $p-1$ of order 3, in part for the reason one might think, that there can be only one such divisor of $p-1$, but also because if d is the divisor of $p-1$ with $\mathfrak{o}(d) = 3$, then $d^* = d + 1$. The existence of such a divisor of $p-1$ is one of two characterizations we give of primes p for which some divisor of $p-1$ has order 3. The other characterization, that there is a positive integer L such that $L^2 = 4p - 3$, makes it easy to hunt for these primes.

In Section 4, we consider primes p for which there is exactly one divisor of $p-1$ whose order is $p-1$. All safe primes, that is primes of the form $2a + 1$ where a is also prime, have this property, and through 10^{12} all primes p with this property are either safe primes or primes of the form $p = 2ab+1$, where a and b are odd primes. Our main theorem gives several characterizations of such primes (see Corollary 2; we have omitted some of the characterizations which will be motivated later in the paper.)

Theorem 1. *Let $p = 2ab + 1$ where a and b are primes. Then the following statements are equivalent:*

1. $\mathfrak{o} : D_{p-1} \to D_{p-1}$ *is a permutation;*
2. *there is exactly one divisor of $p-1$ whose order is $L(p)$;*
3. *more than half the divisors of $p-1$ are orders of divisors of $p-1$ and the complement of the order of any $d \in D_{p-1}$ is the order of a divisor of $p-1$.*

We do not know if there exists a prime p for which there are more than three prime divisors of $p-1$, and for which there is exactly one divisor d of $p-1$ with $\mathfrak{o}(d) = p-1$. It seems natural to ask if there is always at least one divisor d of $p-1$ with $\mathfrak{o}(d) = p-1$, but there are primes, such as 439, for which there is a prime divisor of $p-1$ that does not divide the order of any divisor of $p-1$. For this reason, we ask instead if there is always a divisor of $p-1$ whose order is $L(p)$. The answer to this question is also no, the smallest example, among the primes p for which $p-1$ is square free, being 77,869,111. We have observed several interrelated properties that hold for all the nearly three thousand primes p for which $p-1$ is square free and for which no divisor of $p-1$ has order $L(p)$. Some of the results given in Section 5 hint at the possibility that the observed properties persist for all such primes. The most intriguing of these properties is that the largest prime divisor of $p-1$ divides the order of every divisor of $p-1$ other than $\mathfrak{o}(1)=1$ and $\mathfrak{o}(p-1)=2$.

2. Preliminary Results

We make frequent use of the following facts about multiplicative order. For all $a, b \in \mathbb{Z}/p\mathbb{Z}$:

1. $\widehat{\mathfrak{o}}(ab) \mid \widehat{\mathfrak{o}}(a)\widehat{\mathfrak{o}}(b)$;
2. if $d \mid \widehat{\mathfrak{o}}(a)$ and $d \nmid \widehat{\mathfrak{o}}(b)$, then $d \mid \widehat{\mathfrak{o}}(ab)$;
3. for any positive integer n,
$$\widehat{\mathfrak{o}}(a^n) = \widehat{\mathfrak{o}}(a)/\gcd(n, \widehat{\mathfrak{o}}(a));$$
4. for each $x \in (\mathbb{Z}/p\mathbb{Z})^\times$, $\widehat{\mathfrak{o}}(x)$ divides $p-1$.

Proposition 1. *Let p be a prime and $d \in D$.*

1. *If $2 \mid\mid \mathfrak{o}(d)$, then $\mathfrak{o}(d^*) = \mathfrak{o}(d)/2$.*
2. *If $4 \mid \mathfrak{o}(d)$, then $\mathfrak{o}(d) = \mathfrak{o}(d^*)$.*
3. *If $2 \nmid \mathfrak{o}(d)$, then $\mathfrak{o}(d^*) = 2\mathfrak{o}(d)$.*

Proof. (1) Suppose that $\mathfrak{o}(d) = 2x$, where x is odd. Then

$$d^x \equiv p-1 \equiv dd^* \pmod p \quad \text{and} \quad d^{x-1} \equiv d^* \pmod p.$$

Thus

$$\begin{aligned}\mathfrak{o}(d^*) = \mathfrak{o}(d^{x-1}) &= (2x)/\gcd(2x, x-1) \\ &= (2x)/2 = x = \mathfrak{o}(d)/2.\end{aligned}$$

(2) Since for any positive integer x, the integers $2x-1$ and $4x$ are coprime, the proof follows as in (1).

(3) Suppose $\mathfrak{o}(d) = x$ where x is odd. Since

$$2 = \mathfrak{o}(p-1) = \mathfrak{o}(dd^*) \quad \text{and} \quad \mathfrak{o}(dd^*) \mid \mathfrak{o}(d)\mathfrak{o}(d^*),$$

$\mathfrak{o}(d^*) = 2y$ for some number y. It follows from (2) that y is odd. By (1), $\mathfrak{o}(d) = \mathfrak{o}(d^{**}) = y$. But $\mathfrak{o}(d) = x$. Thus $\mathfrak{o}(d^*) = 2x = 2\mathfrak{o}(d)$. □

Proposition 2. *The prime $p = 5$ is the only prime $p \equiv 1 \pmod 4$ for which there is exactly one divisor of $p-1$ that is a primitive root.*

Proof. Suppose that $p \equiv 1 \pmod 4$ and suppose that there is only one divisor d of $p-1$ such that $\mathfrak{o}(d) = p-1$. By Proposition 1(2), $\mathfrak{o}(d^*) = p-1$ and so $d^* = d$. Therefore

$$2 = \mathfrak{o}(p-1) = \mathfrak{o}(dd^*) = \mathfrak{o}(d^2) = (p-1)/2$$

and $p = 5$. $\square$

Definition. A prime $p = 2a+1$, where a is also prime, is called a *safe prime*. (The prime a is called a Sophie Germain prime.)

Proposition 3. *For any safe prime p, multiplicative order is a permutation of the set D_{p-1}.*

Proof. We have already noted that the proposition holds for $p = 5$. Let $p = 2a+1$ where a is an odd prime. Clearly $\mathfrak{o}(1) = 1$; $\mathfrak{o}(2a) = 2$ and both $\mathfrak{o}(a)$ and $\mathfrak{o}(2)$ belong to $\{a, 2a\}$. By Proposition 1, $\mathfrak{o}(2)$ and $\mathfrak{o}(a)$ have opposite parity. $\square$

It is a well-known unsolved problem whether or not there are infinitely many Sophie Germain primes (see [3, Section 1] and [4, Section 5.5.5].) Consequently, it seems likely that it is a difficult problem to decide if there are infinitely many primes for which there is exactly one divisor of $p-1$ that is a primitive root.

We look briefly at primes of the form $2ab+1$, where a and b are two odd primes. In some sense these primes are as close to safe primes as we can get.

Suppose $\mathfrak{o}(a) = a$ and $\mathfrak{o}(b) = b$. Then $\mathfrak{o}(ab) = ab$, $\mathfrak{o}(2) = 2ab$, $\mathfrak{o}(2b) = 2a$ and $\mathfrak{o}(2a) = 2b$, so that $\mathfrak{o} : D \to D$ is a permutation. The trouble is that we have been unable to find such a prime.

Question 1. Is there a prime of the form $2ab+1$, with two odd primes a and b, such that $\mathfrak{o}(a) = a$ and $\mathfrak{o}(b) = b$?

The same sort of argument as the one given above shows that if $\mathfrak{o}(a) = b$ and $\mathfrak{o}(b) = a$, then $\mathfrak{o} : D \to D$ is a permutation. We have found just one such prime, namely $112643 = 2(17)(3313) + 1$.

3. Primes for Which There is a Divisor d Such That $d^* = d + 1$

Proposition 4. *Let p be prime. There is at most one $d \in D_{p-1}$ such that $d^* = d+1$.*

Proof. Let d and e be divisors of $p-1$ such that $d^* = d+1$ and $e^* = e+1$. Then

$$p - 1 = d^2 + d = e^2 + e.$$

If $d \neq e$,

$$d + e \leq (p-1)/2 + (p-1)/3$$

and so $d + e + 1 < p$. Since $(d-e)(d+e+1) = 0$, we have $d = e$. □

Proposition 5. *Let p be a prime greater than 3. The following statements are equivalent:*

1. *there is $d \in D$ with $\mathfrak{o}(d) = 3$;*
2. *there is $d \in D$ such that $d^* = d + 1$ and $\mathfrak{o}(d) = 3$;*
3. *there is $d \in D$ such that $d^* = d + 1$;*
4. *$4p - 3$ is a square.*

Proof. (1) $\Rightarrow$ (2). Let d be a divisor of $p - 1$ such that $\mathfrak{o}(d) = 3$. Then $p \mid d^3 - 1 = (d-1)(d^2 + d + 1)$ and $d \neq 1$. Therefore p divides both $d(d+1) + 1$ and $d(d^*) + 1$. Hence $p \mid d^* - (d+1)$. As $0 \leq d^* - (d+1) < p$, $d^* = d + 1$.

(2) $\Rightarrow$ (3) is evident.

(3) $\Rightarrow$ (1). Let d be a divisor of $p-1$ such that $d^* = d+1$. Then $p = dd^* + 1 = d^2 + d + 1$ and so $p \mid (d-1)(d^2+d+1) = d^3 - 1$. Since $p > 3$, $d \neq 1$. Thus $\mathfrak{o}(d) = 3$.

(4) $\Leftrightarrow$ (3). Suppose there is a divisor d of $p - 1$ such that $d^* = d + 1$. Then $4p = 4(dd^* + 1) = 4(d^2 + d + 1) = (2d + 1)^2 + 3$. Now suppose that L is a positive integer such that $4p = L^2 + 3$. The equation $x^2 + x + 1 = p$ has roots $r_1 = -1/2 + L/2$ and $r_2 = -1/2 - L/2$. Set $d = r_1$ and note that $|r_2| = d + 1$. Since $d|r_2| = |r_1 r_2| = p - 1$, $d^* = d + 1$. □

Consider a prime of the form $6a + 1$ (where a is also prime) that has a divisor d of $p-1$ such that $d^* = d+1$. There are only 8 divisors of $p-1$, and we know that there is exactly one divisor of $p - 1$ for each of 1,2,3, and 6. So for such a prime there is a good chance that $\mathfrak{o} : D \to D$ is a permutation. The good news is that this is true for all primes of this form. Alas, there are only two such primes, 31 with $d = 5$ and 43 with $d = 6$.

Proposition 6. *The primes 31 and 43 are the only primes of the form $6a + 1$, where a is a prime greater than 3, for which there exists a divisor d of $p - 1$ such that $d^* = d + 1$.*

Proof. Let $p = 6a + 1$, where $a > 3$ and a is prime, and suppose there is a divisor d of $p - 1$ such that $d^* = d + 1$. Because $6 \in \{d, d^*\}$, either $d = 5$ and $d^* = 6$ or $d = 6$ and $d^* = 7$. □

Proposition 7. *Let p be a prime greater than 5 for which $\mathfrak{o} : D \to D$ is a permutation. Then $p - 1$ is square free.*

Proof. The proof is by contradiction. Suppose d^2 is a divisor of $p-1$ such that $1 < d < d^2 \leq p-1$. Because $\mathfrak{o}(d^2) = \mathfrak{o}(d)/\gcd(\mathfrak{o}(d), 2)$, $\mathfrak{o}(d)$ is even, say $\mathfrak{o}(d) = 2K$. By Proposition 2, K is odd. Therefore by Proposition 1(1), $\mathfrak{o}(d^*) = K = \mathfrak{o}(d^2)$, and $d^3 = p-1$. It follows that $2 = \mathfrak{o}(d^3) = 2K/\gcd(3, 2K)$, and so $K = 3$. Because $\mathfrak{o}(d^2) = 3$, it follows from Proposition 5 that $d = (d^2)^* = d^2+1$, a contradiction. □

Remark. The previous proposition shows: if $\mathfrak{o} : D \to D$ is a permutation (and $p > 5$), then D is a Boolean lattice.

We make no use of the last proposition in this section, other than to motivate the following question.

Question 2. Suppose that $p = 6ab+1$ where a and b are two primes greater than 3. If there is a divisor d of $p-1$ such that $d^* = d+1$, is it true that 3 is a primitive root?

Example 1. Let $p = 71023$. Then $p - 1 = (6)(7)(19)(89) = (266)(267)$, but $\mathfrak{o}(3) = (p-1)/7$.

Proposition 8. *Let p be a prime of the form $p = 6ab + 1$, where a and b are two primes greater than 3, for which there is a divisor d of $p - 1$ such that $d^* = d + 1$. Then 3 is a divisor of $p - 1$ and $\mathfrak{o}(3)$ is a multiple of 6.*

Proof. Since $p = 6ab+1$, 3 is a divisor of $p-1$. By the law of quadratic reciprocity, $\mathfrak{o}(3)$ is even, because $\left(\frac{p}{3}\right) = \left(\frac{1}{3}\right) = 1$ and since $p \equiv 3 \pmod 4$, $\left(\frac{3}{p}\right) = -1$. Because $p \equiv 1 \pmod 3$, there are uniquely determined positive integers L and M such that $4p = L^2+27M^2$ (see [1] and [2, Proposition 8.3.2],) and by a result of Jacobi, $3 \mid \mathfrak{o}(3)$ if, and only if, M is not a multiple of 3. There are two cases:

1. $d \equiv 0 \pmod 3$. Set $M = d/3$. Then $4p-27M^2 = 4d^2+4d+4-3d^2 = (d^*+1)^2$. Thus $L = d^* + 1$.
2. $d \equiv 2 \pmod 3$. Set $M = d^*/3$. Then $4p - 27M^2 = 4d^2 + 4d + 4 - 3(d^*)^2 = (d-1)^2$. Thus $L = d - 1$.

In either case, $M \mid p-1$ and since $9 \nmid p-1$, $3 \nmid M$. □

4. A Generalization of Safe Primes

For the remainder of the paper, p always denotes a prime greater than 3 for which $p-1$ is square free.

Proposition 9. *Let p be a prime and let q be an odd prime divisor of $L(p)$. Then there are at least two prime divisors of $p-1$ whose orders are divisible by q.*

Proof. Because $q \mid L(p)$, there is a divisor d of $p-1$ such that

$$q \mid \mathfrak{o}(d) \mid \prod\{\mathfrak{o}(x) : x \text{ is a prime and } x \mid d\}.$$

Thus there is a prime divisor x of d such that $q \mid \mathfrak{o}(x)$. By Proposition 1, $q \mid \mathfrak{o}(d^*)$ and so there is a prime y such that $y \mid d^*$ and $q \mid \mathfrak{o}(y)$. As $p-1$ is square free, $x \neq y$. $\square$

Definition. A prime p has the *two-prime property* provided that for each odd prime divisor q of $p-1$ there are at most two divisors $d, e \in D$ such that d, e are prime, and $q \mid \mathfrak{o}(d)$ and $q \mid \mathfrak{o}(e)$.

Evidently all safe primes have the two-prime property: this is true vacuuously for the safe prime 5 and true trivially for all other safe primes.

We adopt the following notation, which the authors refer to as "wedge" (short for "the wedge product of.") Let $a, b \in D$. Then

$$\bar{\mathfrak{o}}(a) \nabla \bar{\mathfrak{o}}(b) := \prod\{d \in D : d \text{ is a prime and } d \mid \bar{\mathfrak{o}}(a) \text{ XOR } d \mid \bar{\mathfrak{o}}(b)\}.$$

Note that for $a, b \in D$

$$\bar{\mathfrak{o}}(a) \nabla \bar{\mathfrak{o}}(b) \mid \bar{\mathfrak{o}}(ab) \mid \bar{\mathfrak{o}}(a)\bar{\mathfrak{o}}(b).$$

Proposition 10. *Let p have the two-prime property and let d and e be coprime divisors of $p-1$. Then*

$$\bar{\mathfrak{o}}(d) \nabla \bar{\mathfrak{o}}(e) = \bar{\mathfrak{o}}(de).$$

Proof. It suffices to show that $\bar{\mathfrak{o}}(de) \mid \bar{\mathfrak{o}}(d) \nabla \bar{\mathfrak{o}}(e)$. Let u be an odd prime divisor of $\bar{\mathfrak{o}}(de)$. Then $u \mid \bar{\mathfrak{o}}(d)$ or $u \mid \bar{\mathfrak{o}}(e)$. Suppose that u divides both $\bar{\mathfrak{o}}(d)$ and $u \mid \bar{\mathfrak{o}}(e)$ and let r and s be the two prime divisors of $p-1$ whose orders are divisible by u. Then $rs \mid de$ and so $u \nmid \mathfrak{o}(de)$. Thus $u \mid \bar{\mathfrak{o}}(d) \nabla \bar{\mathfrak{o}}(e)$. $\square$

Definition. A prime p is *order multiplicative* provided that whenever a and b are coprime divisors of $p-1$, $\bar{\mathfrak{o}}(a) \nabla \bar{\mathfrak{o}}(b) = \bar{\mathfrak{o}}(ab)$.

Lemma 1. *Suppose that p is order multiplicative and let a and b be coprime divisors of $p-1$ such that $ab \neq 1$ and such that $\bar{\mathfrak{o}}(a) = \bar{\mathfrak{o}}(b)$. Then $b = a^*$.*

Proof. $\bar{\mathfrak{o}}(ab) = \bar{\mathfrak{o}}(a) \nabla \bar{\mathfrak{o}}(b) = 1$. Since $ab \neq 1$, $ab = p-1$. $\square$

Lemma 2. *Suppose that p is order multiplicative, let a and b be divisors of $p-1$ such that $\bar{\mathfrak{o}}(a) = \bar{\mathfrak{o}}(b)$, and let $x = \gcd(a, b)$. Then $\bar{\mathfrak{o}}(a/x) = \bar{\mathfrak{o}}(b/x)$.*

Proof. $\bar{\mathfrak{o}}(a/x) \nabla \bar{\mathfrak{o}}(x) = \bar{\mathfrak{o}}(a) = \bar{\mathfrak{o}}(b) = \bar{\mathfrak{o}}(b/x) \nabla \bar{\mathfrak{o}}(x)$. Let q be a prime that divides $\bar{\mathfrak{o}}(a/x)$. There are two cases:

1. $q \mid \bar{\mathfrak{o}}(x)$. Then $q \nmid \bar{\mathfrak{o}}(b/x) \nabla \bar{\mathfrak{o}}(x)$ and so $q \mid \bar{\mathfrak{o}}(b/x)$.
2. $q \nmid \bar{\mathfrak{o}}(x)$. Then $q \mid \bar{\mathfrak{o}}(b/x) \nabla \bar{\mathfrak{o}}(x)$ and so $q \mid \bar{\mathfrak{o}}(b/x)$.

Thus $\bar{\mathfrak{o}}(a/x) \mid \bar{\mathfrak{o}}(b/x)$ and by symmetry $\bar{\mathfrak{o}}(b/x) = \bar{\mathfrak{o}}(a/x)$. □

Proposition 11. *Suppose that p is order multiplicative. Then multiplicative order is a permutation of the divisors of $p-1$.*

Proof. Let a and b be divisors of $p-1$. It suffices to show that if $\bar{\mathfrak{o}}(a) = \bar{\mathfrak{o}}(b)$, then $a = b$ or $a = b^*$. For it follows that if $\mathfrak{o}(a) = \mathfrak{o}(b)$, either $a = b$ or $a = b^*$ and $a \neq b^*$ because, by Proposition 1, b and b^* have different orders. To this purpose, suppose that $\bar{\mathfrak{o}}(a) = \bar{\mathfrak{o}}(b)$ and $a \neq b$. Let $x = \gcd(a, b)$. By Lemma 2, $\bar{\mathfrak{o}}(a/x) = \bar{\mathfrak{o}}(b/x)$. By Lemma 1, if $ab/x^2 \neq 1$, $b/x = (a/x)^*$. Since $a \neq b$, $ab/x^2 \neq 1$. Thus $(b/x) = (a/x)^*$ and $x = 1$. Thus $b = a^*$. □

Corollary 1. *Let p be a prime such that $L(p) \neq p-1$. Then there is an odd prime divisor of $p-1$ that divides $\mathfrak{o}(d)$ for at least three prime divisors $d \in D_{p-1}$.*

We make the conjecture, which we have confimed for primes less than 10^{11}, that when p is a prime for which $L(p) \neq p-1$, the largest prime divisor of $p-1$ always divides $\mathfrak{o}(d)$ for at least three prime divisors $d \in D_{p-1}$.

Example 2. Let $p = 71$. Then $L(p) = p-1$, $\mathfrak{o}(2) = 35$, $\mathfrak{o}(5) = 5$, and $\mathfrak{o}(7) = 70$. Thus the largest prime divisor of 70, namely 7, divides $\mathfrak{o}(d)$ for only two prime divisors d of $p-1$, whereas 5 divides $\mathfrak{o}(d)$ for every divisor d of $p-1$ other than 1 and $p-1$.

Corollary 2. *Let $p = 2ab+1$ where a and b are prime. Then the following statements are equivalent:*

1. *the prime p has the two-prime property;*
2. *the prime p is order multiplicative;*
3. *$\mathfrak{o} : D \to D$ is a permutation;*
4. *there is exactly one divisor d of $p-1$ such that $\mathfrak{o}(d) = L(p)$;*
5. *for each $d \in D$, there is a divisor $e \in D$ such that $\mathfrak{o}(e) = \mathfrak{o}(d)^*$, and more than half of the elements of D are in the image of $\mathfrak{o}$.*

Proof. We have seen that (1) $\Rightarrow$ (2) $\Rightarrow$ (3) and it follows immediately from Proposition 9 that (3) $\Rightarrow$ (1). Clearly (3) implies both (4) and (5).

Suppose that (4) holds. Note that for each $d \in D \setminus \{1, p-1\}$, $\mathfrak{o}(d)$ is a multiple of a or b. Therefore $L(p) = p-1$. Also every divisor of $p-1$ other than 1 and $p-1$ is either prime or the complement of a prime, and exactly one $d \in D$ such that d is prime, and $\mathfrak{o}(d)$ is a multiple of ab. Moreover, by Proposition 9, both a and b divide $\mathfrak{o}(d)$ for at least two prime divisors d of $p-1$. By the pigeonhole property, p satisfies the two-prime property.

Suppose that (5) holds and suppose that there is a divisor d of $p-1$ not in the image of $\mathfrak{o}$. If d is odd, $d, d^*, 2d$, and $(2d)^*$ are four divisors of $p-1$ that are not in the image of $\mathfrak{o}$, and if d is even, $d, d^*, d/2$, and $(d/2)^*$ are four divisors of $p-1$ that are in the image of $\mathfrak{o}$. In either case, the condition that more than half the divisors of $p-1$ are in the image of $\mathfrak{o}$ cannot hold. □

Through 10^{12}, we have found only three primes, p, other than the safe primes for which there is exactly one divisor d of $p-1$ such that $\mathfrak{o}(d) = L(p)$. They are $p = 31, p = 43$, and $p = 112643$, and all these primes are of the form $p = 2ab + 1$, where a and b are prime. Thus the reappearance of 31 and 43 from Section 3 is explained by condition (3) of the previous corollary.

5. Primes p for Which No Divisor has $\mathfrak{o}(d) = L(p)$

As we mentioned in the introduction, $p = 77869111$ is the least prime for which there is no divisor d of $p-1$ such that $\mathfrak{o}(d) = L(p)$. We have found 2989 such primes less than 10^{12}.

Definitions. A nonempty subset of D that is closed under complementation and coprime multiplication is called a *complete set*.

Note that if C is a complete set of divisors of $p-1$, then $\{1, p-1\} \subset C$. If A and B are complete sets of divisors of $p-1$ and $A \cap B = \{1, p-1\}$, we say that A and B are *almost disjoint*.

Lemma 3. *Let $C \subset D$ be a complete set that contains a prime divisor q of $p-1$ and suppose that C is the almost disjoint union of two complete sets A and B. Then $A = C$ or $B = C$.*

Proof. It suffices to show that $A = \{1, p-1\}$ or $B = \{1, p-1\}$. The proof is by contradiction. Suppose without loss of generality that $q \in A \setminus \{1, p-1\}$ and that there exists $b \in B \setminus \{1, p-1\}$. Either $\gcd(q, b) = 1$ or $\gcd(q, b^*) = 1$ and since both b and b^* belong to B we assume without loss of generality that $\gcd(q, b) = 1$. Then $q^*/b = (qb)^* \in C$ and $q^*/b \notin B$, lest q^* belongs to B. Thus $q^*/b \in A$ and $b^* = q(q^*/b) \in A$, a contradiction. □

Proposition 12. *Let p be a prime for which there is no $d \in D$ such that $\mathfrak{o}(d) = L(p)$ and suppose that $p-1$ has four or fewer prime divisors. Then $L(p) = p-1$.*

Proof. We consider only the case that $p-1$ has exactly four prime divisors, say $p - 1 = 2abc$. The proof is by contradiction. Suppose that $L(p) < p-1$. Then without loss of generality we may assume that $L(p) = 2ab$. Let $A = \{d \in D : a \nmid \mathfrak{o}(d)\}$ and $B = \{d \in D : b \nmid \mathfrak{o}(d)\}$. Then A and B are almost disjoint complete sets and $A \cup B = D$. By Lemma 3, $A = D$ or $B = D$, which contradicts the assumption that $ab \mid L(p)$. □

Definition. A prime divisor of $p-1$ is *dense* provided it divides $\mathfrak{o}(d)$ for every $d \in D \setminus \{1, p-1\}$. We denote the set of prime divisors of $p-1$ that are not dense by $S(p)$.

Proposition 13. *Let p be a prime for which $L(p) = p-1$ and for which there is no divisor d of $p-1$ such that $\mathfrak{o}(d) = p-1$. Then $S(p)$ has at least four members. If $S(p)$ has exactly four members, then for each odd prime $x \in S(p)$, $x^* = \mathfrak{o}(d)$ for some $d \in D$.*

Proof. It is clear that $S(p)$ has at least three members. For if $S(p) = \{2\}$ and $d \in D \setminus \{1, p-1\}$, either d or d^* is a primitive root, and if $S(p) = \{2, s\}$ there is a divisor d of $p-1$ such that $s \mid \mathfrak{o}(d)$ and either d or d^* is a primitive root. Let $2, a, b$ be three members of $S(p)$. By Proposition 9 there are prime divisors, r and s, of $p-1$ such that $a \mid \mathfrak{o}(r)$ and $b \mid \mathfrak{o}(s)$. Then ab divides at least one of $\mathfrak{o}(r), \mathfrak{o}(s)$ and $\mathfrak{o}(rs)$, and so there is a fourth member of $S(p)$.

Now suppose that $S(p) = \{2, r, s, t\}$ and let x be one of r, s, t. By the argument just given there is a divisor d of $p-1$ such that $(rst/x) \mid \mathfrak{o}(d)$ and so $x^* = \mathfrak{o}(d)$ or $x^* = \mathfrak{o}(d^*)$. □

Corollary 3. *Let p be a prime for which $L(p) = p-1$ and for which there is no divisor $d \in D$ such that d is a primitive root, and let x be the least odd prime divisor of $p-1$. If $x \in S(p)$ and $S(p)$ has exactly four members, then x^* is the largest divisor in the image of $\mathfrak{o}$.*

Examples. The following are examples of primes p for which $L(p) = p-1$ and for which there is no divisor d of $p-1$ with $\mathfrak{o}(d) = p-1$:

1. $p = 77869111 = 2 \cdot 3 \cdot 5 \cdot 11 \cdot 235967 + 1$. The only dense divisor of $p-1$ is 235967. By the corollary, 3^* is the largest divisor in the image of $\mathfrak{o}$.

2. $p = 7624557571 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 31 \cdot 1171207 + 1$. The only dense divisor of $p-1$ of $p-1$ is 1171207. For this prime $3^*, 5^*, 7^*$ are in the image of $\mathfrak{o}$ but 31^* is not.

3. $p = 694081875103 = 2 \cdot 3 \cdot 7 \cdot 11 \cdot 41 \cdot 59 \cdot 621059 + 1$ has three dense divisors of $p-1$, namely 41, 59 and 621059.

4. $p = 398975049691 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 17 \cdot 111757717 + 1$. The only dense divisor of $p-1$ is 111757717 and x^* is in the image of $\mathfrak{o}$ for each odd member x of $S(p)$.

We have found that if p is a prime less than 10^{12} and p has no divisor d of $p-1$ such that $\mathfrak{o}(d) = L(p)$, then p has the following properties:

1. $L(p) = p - 1$;
2. the largest prime divisor of $p-1$ is dense;
3. if $x \in S(p)$ and y is a dense prime divisor of $p-1$, then $x < y$ (cf. Example 2 of Section 4);
4. the largest divisor in the image of $\mathfrak{o}$ is x^*, where x is the least odd prime divisor of $p-1$;
5. there is an odd member x of $S(p)$ for which x^* in the image of $\mathfrak{o}$;
6. $3 \mid p-1$ or $5 \mid p-1$.

It is noteworthy that through 3×10^{11} properties 1,2, and 6 also hold for primes $p \equiv 3 \pmod 4$ for which $p-1$ is not square free. There is not much point in considering primes $p \equiv 1 \pmod 4$. The prime $q = 3541$ illustrates what goes wrong: although there are two divisors d of $p-1$ such that $\mathfrak{o}(d) = L(q)/2$, there is no divisor e of $p-1$ with the property $\mathfrak{o}(e) = L(q)$.

Examples. The following are examples of primes $p \equiv 3 \pmod 4$ for which $p-1$ is not square free, and there is no divisor d of $p-1$ with $\mathfrak{o}(d) = L(p)$.

1. $p = 3815197471 = 2{\cdot}3^3{\cdot}5{\cdot}7{\cdot}2018623{+}1$ has dense prime divisors 3 and 2018623. Hence p does not satisfy property 3. Since $S(p) = \{2, 5, 7\}$, Proposition 13 does not extend to primes for which $p-1$ is not square free.
2. $p = 26499741031 = 2 \cdot 3^3 \cdot 5 \cdot 7 \cdot 14021027 + 1$. The largest divisor in the image of $\mathfrak{o}$ is $\mathfrak{o}(6) = 5^*$. Thus p does not satisfy property 4.
3. $p = 336932887411 = 2 \cdot 3^3 \cdot 5 \cdot 7 \cdot 178271369 + 1$ has no odd prime divisor x for which x^* is in the image of $\mathfrak{o}$.
4. $p = 819267931 = 2 \cdot 3^3 \cdot 5 \cdot 13 \cdot 700229 + 1$ is the least prime for which $p \equiv 3$ mod 4, $p-1$ is not square free, and no divisor d of $p-1$ such that $\mathfrak{o}(d) = L(p)$.

References

[1] K. Williams, On Euler's criterion for cubic nonresidues, *Proc. Amer. Math. Soc.* **49** (1975), 277-283.

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

[3] P. Leonetti, A characterization of Sophie Germain primes, *Int. J. Number Theory* **14** (2018), 653-660.

[4] V. Shoup, *A Computational Introduction to Number Theory and Algebra*, Cambridge University Press, Cambridge, 2009.