DEPARTMENT OF MATHEMATICS
UNIVERSITY OF NIJMEGEN
The Netherlands

Cubic reciprocity and explicit primality tests for $h \cdot 3^k \pm 1$

Wieb Bosma

Report No. 05.15 (2005)

DEPARTMENT OF MATHEMATICS
UNIVERSITY OF NIJMEGEN
Toernooiveld
6525 ED Nijmegen
The Netherlands

Cubic reciprocity and explicit primality tests for $h \cdot 3^k \pm 1$

Wieb Bosma

Abstract

As a direct generalization of the Lucas-Lehmer test for the Mersenne numbers $2^k - 1$, explicit primality tests for numbers of the form $N = h \cdot 3^k \pm 1$ are derived, for fixed h, and all k with $3^k > h$. The result is that N is prime if and only if $w_{k-1} \equiv \pm 1 \bmod N$, where w is given by the recursion $w_j = w_{j-1}(w_{j-1}^2 - 3)$; the main difference with the original Lucas-Lehmer test is that the starting value w_0 of this recursion may depend on k, (as is the case in tests for $h \cdot 2^k \pm 1$). For $h \neq 27^m \pm 1$ it is usually easy to determine a finite covering prescribing a starting value depending only on the residue class of k modulo some auxiliary integer. We show how this can be done using cubic reciprocity and give some examples, drawing from the cases $h \leq 10^5$, which were all computed explicitly for this paper.

1 Introduction

This paper was written with the intention of serving several purposes, besides marking the birthday of Hugh Williams. One of these purposes was to show that results from [4] for numbers of the form $h \cdot 2^k \pm 1$ could easily be adapted to $h \cdot 3^k \pm 1$. Assuming only the cubic reciprocity law (replacing quadratic reciprocity) it was intended to give an entirely elementary exposition from a computational point of view, leading up to a generalization of the famous Lucas-Lehmer test, but avoiding the language of 'Lucas functions'. Cubic reciprocity is far less known than quadratic reciprocity, but just as easy to implement and use in practice. From the description given it should be easy for an interested reader to write programs (similar to the ones I wrote using MAGMA) for finding the explicit primality tests and for executing them. There is an emphasis on finding finite covers, especially single-element covers, as Hugh Williams mentioned his interest in them to me long ago, and as he wrote about them in several places, see for example [8]. Finally, some results and curiosities from computational experiments I conducted were included.

Only when putting together the list of references after writing most of this paper, I became aware of the existence of [3]. In that paper, Berrizbeitia and Berry formulated the primality tests for $h \cdot 3^k \pm 1$ analogous to the Lucas-Lehmer test for the first time (it is essentially Corollary 4.4 below). Their proofs are along lines very similar to mine; their use of the trace function leads to a formulation that is better than my

original one (where I used the difference rather than the sum of two conjugates), and so I decided to change my exposition slightly accordingly. The formulation of Corollary 4.2 and Corollary 4.4 should therefore be attributed to them.

The main idea of the primality criteria in this paper can be explained as follows; the precise formulation is found in Theorems 2.1 and 2.3 in the next section. This idea is that when $N = h \cdot 3^k \pm 1$ and 3^k exceeds h, showing the existence of an element α of multiplicative order 3^k in certain finite ring of cardinality N or N^2 equivalent to showing that a this ring is a field and that N is prime. To prove that α has the right order it is shown that the $\alpha^{(N\pm1)/3}$ is a primitive third root of unity ζ_3.

The tasks that remain from then on are to show that the test can be performed simply in $\mathbf{Z}[\zeta_3]/N$, that taking the required power of an element can be done by a simple recursion modulo N, and to furnish the element α. The result will best imitate the classical Lucas-Lehmer test, which says that

$$2^k - 1 \quad \text{is prime} \qquad \Longleftrightarrow \qquad e_{k-2} \equiv 0 \bmod (2^k - 1),$$

where $e_0 = -4$ and $e_{j+1} = e_j^2 - 2$, when we explicitly write down the element α. However, the α to be taken may depend on the exponent k; the analogy is complete if a single α (which means a single starting value for the recursion) can be used for every k. That happens when a single-element cover is found.

Most results from [4] carry over to the present paper in a straightforward manner. There are a few differences though. The main difference has to do with the primality criterion we mentioned; for $N = h \cdot 2^k + 1$ (with $2^k > \sqrt{N}$) one looks for an element for which the power $(N-1)/2$ is a primitive second root of unity, i.e., equals -1. The entire primality test can then be carried out in $(\mathbf{Z}/N\mathbf{Z})^*$. Already for $N = h \cdot 2^k - 1$ we need to work in a quadratic extension ring in order to find an element for which the power $(N+1)/2$ is -1. In the present case, for $h \cdot 3^k \pm 1$, it is best to ensure that the third roots of unity are present, by starting in $\mathbf{Z}[\zeta_3]$. Then both tests can take place in a finite quotient of this ring, without the need to make further extensions.

Notation and Preliminaries

Thus, the primality tests in this paper are essentially performed in the ring of integers $\mathbf{Z}[\zeta_3]$ of the cyclotomic field $\mathbf{Q}(\zeta_3)$. Elements α of the field will be represented as $a + b \cdot \zeta_3$, with $a, b \in \mathbf{Q}$, the non-trivial automorphism sending ζ_3 to $\zeta_3^2 = -1 - \zeta_3$ by $\bar{}$ and the norm and trace are then given by $\operatorname{Nm} \alpha = \alpha \cdot \bar{\alpha} = a^2 - ab + b^2$ and $\operatorname{Tr} \alpha = \alpha + \bar{\alpha} = 2a - b$. Occasionally we will use that $\mathbf{Q}(\zeta_3)$ is isomorphic to the quadratic field $\mathbf{Q}(\sqrt{-3})$, and we write $\zeta_3 = (-1 + \sqrt{-3})/2$.

It is well-known that $\mathbf{Z}[\zeta_3]$ is a unique factorization domain, in which there are three types of prime: the inert rational primes $q \equiv 2 \bmod 3$ of norm q^2, the primes π of prime norm $p = \pi \cdot \bar{\pi} \equiv 1 \bmod 3$, and the prime $1 - \zeta_3$, which lies over 3 as $3 = -\zeta_3^2 \cdot (1 - \zeta_3)^2$.

The units of $\mathbf{Z}[\zeta_3]$ are the sixth roots of unity $\pm\zeta_3^i$, for $i = 0, 1, 2$.

The cubic character introduced in Section 3 is analogous to the well-known Jacobi symbol, for which we will here use the notation $\left(\frac{a}{m}\right)_2$. The Euler criterion mentioned

in the following proof states that for primes p and every a not divisible by p always $\left(\frac{a}{p}\right)_2 \equiv a^{(p-1)/2} \bmod p$.

Theorem 1.1 *Let $\alpha, \pi \in \mathbf{Z}[\zeta_3]$, with π prime of norm $\neq 3$. Then:*

(i) $\alpha^{\pi} \equiv \bar{\alpha} \bmod \pi$, *if* $\pi \in \mathbf{Z}$, *so* $\pi \equiv 2 \bmod 3$;

(ii) $\alpha^{\mathrm{Nm}\,\pi} \equiv \alpha \bmod \pi$;

(iii) there is a unique $i \in \{0, 1, 2\}$ *such that* $\alpha^{\frac{\mathrm{Nm}\,\pi - 1}{3}} \equiv \zeta_3^i \bmod \pi$ *if* $\alpha \not\equiv 0 \bmod \pi$.

Proof If $\pi = q \equiv 2 \bmod 3$ is a prime in $\mathbf{Z}$ with $q > 2$, then Fermat's little theorem implies that $a^q \equiv a \bmod q$ for every a. Write $\alpha = (x + y \cdot \sqrt{-3})/z$ with $z \in \{1, 2\}$ and use that every binomial coefficient $\binom{q}{i}$ is divisible by q, as well as Euler's criterion, to see that

$$\alpha^q = \left(\frac{x + y\sqrt{-3}}{z}\right)^q \equiv \frac{x + (-3)^{\frac{q-1}{2}} y\sqrt{-3}}{z} \equiv \bar{\alpha} \bmod q,$$

as -3 is a quadratic non-residue for primes $q \equiv 2 \bmod 3$.

The second result follows from this if $\pi = q \equiv 2 \bmod 3$, and in any case holds since $\mathbf{Z}[\zeta_3]/\pi$ is a finite field of $\mathrm{Nm}\,\pi$ elements with multiplicative group of order $\mathrm{Nm}\,\pi - 1$.

The third results must then hold because $\alpha^{(\mathrm{Nm}\,\pi - 1)/3} \bmod \pi$ must equal one of the three solutions to $x^3 - 1 = 0$ in this field.

2 Primality criteria

The primality criteria in $\mathbf{Z}[\zeta_3]$ we use are formulated in the Theorems 2.1 and 2.3.

Theorem 2.1 *Let $\nu \in \mathbf{Z}[\zeta_3]$ with $N = \mathrm{Nm}\,\nu$. If $N > 1$ is odd and $3^k > \sqrt{N}$, where $k \geq 1$ is such that $3^k \mid N - 1$, then:*

$$\nu \text{ is prime} \quad \Longleftrightarrow \quad \exists\, \alpha \in \mathbf{Z}[\zeta_3] :\ \alpha^{\frac{N-1}{3}} \equiv \zeta_3 \bmod \nu. \tag{1}$$

Proof First note that by hypothesis $N = \mathrm{Nm}\,\nu \equiv 1 \bmod 3$.

If ν is prime then the ring $\mathbf{Z}[\zeta_3]/\nu$ is a field of N elements. Its multiplicative group is cyclic of order $N - 1$, so for any non-cube $\gamma \bmod \nu$ (for example, any generator of the group), the power $(N-1)/3$ will be a primitive third root of unity, so either $\alpha = \gamma$ or $\alpha = \gamma^2$ will have the desired property.

For the converse, let α have the property stated and let $\pi \in \mathbf{Z}[\zeta_3]$ be any prime divisor of ν. Then $\alpha^{(N-1)/3} \equiv \zeta_3 \not\equiv 1 \bmod \pi$, as $\zeta_3 - 1$ is a prime of norm 3 which does not divide N. So the multiplicative order of α in $(\mathbf{Z}[\zeta_3]/\pi)^*$ is divisible by the largest power 3^k dividing $N - 1$. The order $\mathrm{Nm}\,\pi - 1$ of the group $(\mathbf{Z}[\zeta_3]/\pi)^*$ is then divisible by 3^k.

If $\pi = q$ is a prime in $\mathbf{Z}$ that is 2 mod 3 then $\mathrm{Nm}\,\pi = q^2$ divides $\mathrm{Nm}\,\nu = N$. Now $3^k \mid q^2 - 1$ but 3 does not divide $q - 1$, so $3^k \mid q + 1$ and hence $q + 1 \geq 3^k$. As N is

odd, so is q, and this inequality must be strict, so $q \geq 3^k > \sqrt{N}$, contradicting that q^2 divides N.

Therefore any prime π dividing ν has $\mathrm{Nm}\,\pi = p$, a prime in $\mathbf{Z}$ dividing N, with $3^k \mid p-1$. Then $p-1 \geq 3^k > \sqrt{N}$, so $p > \sqrt{N}$. But then every prime p dividing N exceeds $\sqrt{N}$, so N is prime and so is ν.

Corollary 2.2 *If $N > 1$ is odd and $3^k \mid N-1$, with $k \geq 1$ and $3^k > \sqrt{N}$, then:*

$$N \text{ is prime in } \mathbf{Z} \quad \Longleftrightarrow \quad \exists\, \alpha \in \mathbf{Z}[\zeta_3] :\ \alpha^{\frac{N-1}{3}} \equiv \zeta_3 \bmod N. \tag{2}$$

Proof If N is prime then $N = \nu \cdot \bar{\nu}$ since $N \equiv 1 \bmod 3$; by Theorem 2.1 there are elements α_1 and α_2 in $\mathbf{Z}[\zeta_3]$ with $\alpha_1^{(N-1)/3} \equiv \zeta_3 \bmod \nu$ and $\alpha_2^{(N-1)/3} \equiv \zeta_3 \bmod \bar{\nu}$. But ν and $\bar{\nu}$ are coprime in $\mathbf{Z}[\zeta_3]$, and by the Chinese remainder theorem there exists $\alpha \in \mathbf{Z}[\zeta_3]$ such that $\alpha \equiv \alpha_1 \bmod \nu$ and $\alpha \equiv \alpha_2 \bmod \bar{\nu}$; this implies that $\alpha^{(N-1)/3} \equiv \zeta_3 \bmod \nu \cdot \bar{\nu}$ as desired.

For the converse we argue as in the proof of the theorem: for a prime $q \equiv 2 \bmod 3$ dividing N the existence of α implies that $q+1$ is divisible by 3^k. As q is odd this implies that it exceeds $\sqrt{N}$. If $p \equiv 1 \bmod 3$ is a prime divisor of N then the existence of α forces $p-1$ to be divisible by 3^k, and so p exceeds $\sqrt{N}$. Thus every prime divisor of N exceeds $\sqrt{N}$, and N must be prime itself.

Theorem 2.3 *If $N > 1$ is odd and $3^k \mid N+1$, with $k \geq 1$ and $3^k > \sqrt{N}$, then:*

$$N \text{ is prime} \quad \Longleftrightarrow \quad \exists\, \alpha \in \mathbf{Z}[\zeta_3] :\ \alpha^{\frac{N+1}{3}} \equiv \zeta_3 \bmod N. \tag{3}$$

Proof Note that by hypothesis $N \equiv 2 \bmod 3$, and so N is prime in $\mathbf{Z}$ if and only if N is prime in $\mathbf{Z}[\zeta_3]$.

If N is prime, then $\mathbf{Z}[\zeta_3]/N$ is a field of N^2 elements. Hence any $\eta \in \mathbf{Z}[\zeta_3]$ with $\eta \not\equiv 0 \bmod N$ will satisfy $\eta^{N^2-1} \equiv 1 \bmod N$ by Theorem 1.1(ii) and if η is a non-cube modulo N we get $\eta^{(N^2-1)/3} \not\equiv 1 \bmod N$, so it must be a primitive third root of unity. Taking α congruent to $\eta^{N-1} \bmod N$ or its square will give the result.

For the converse, let π be a prime element of $\mathbf{Z}[\zeta_3]$ dividing N and let α satisfy $\alpha^{\frac{N+1}{3}} \equiv \zeta_3 \bmod \pi$. Note that π cannot be the prime over 3 as $N \equiv 2 \bmod 3$. Then the largest power 3^k dividing $N+1$ also divides the order of $\alpha \bmod \pi$, hence the order of $(\mathbf{Z}[\zeta_3]/\pi)^*$. If $\pi \notin \mathbf{Z}$ then $\bar{\pi}$ also divides N and $\mathrm{Nm}\,\pi = \mathrm{Nm}\,\bar{\pi} = p$, an odd prime; in this case $p-1$ is divisible by, and hence exceeds, $3^k > \sqrt{N}$.

If $\pi = q \equiv 2 \bmod 3$ is a prime in $\mathbf{Z}$ dividing N, then $3^k \mid q+1$, so $q+1 \geq 3^k > \sqrt{N}$. Since N is odd, so is q, and $q+1 > 3^k$ hence q exceeds $\sqrt{N}$.

Now all prime divisors of N exceed $\sqrt{N}$, so N must be prime.

Remark 2.4 The above results provide a primality criterion for all odd integers $N > 1$ for which either $N-1$ or $N+1$ has a factor of the form 3^k exceeding $\sqrt{N}$.

The requirement $3^k > \sqrt{N}$ can be slightly relaxed by considering the divisibility properties more carefully than by just deriving inequalities. This was done by Williams in Lemma 1 of [9], and used also in in [3]. They essentially need $3^k > h/8$.

The non-explicit part of the criteria lies in the choice of α. To prove that N is prime using Corollary 2.2 or Theorem 2.3 one would have to exhibit an element α with the desired property. To prove compositeness using them directly one would even have to show that no α has this property.

In practice both problems can be solved quite easily using probabilistic methods. For primes, one third of random choices for α will be non-cubes and hence lead to a primality proof. For composite integers random choices for α will usually quickly yield a non-zero example for which $\alpha^{\mathrm{Nm}\,\nu-1} \not\equiv 1 \bmod \nu$, violating the generalization of Fermat's little theorem. However, for pseudoprimes this may fail; one could overcome this by using a stronger test analogous to the Miller-Rabin test. Or one could simply subject N to the original Miller-Rabin test.

The alternative we consider here is to make the criteria implied by the theorems explicit by prescribing a single α to be tested for a given ν or N.

We formulate a first version of the problem that arises.

Problem 2.5 *Given an odd integer $N > 1$ with $N-1$ or $N+1$ divisible by 3^k for some $k \geq 1$ with $3^k > \sqrt{N}$, determine an element $\alpha \in \mathbf{Z}[\zeta_3]$ with the property that*

$$N \quad \textit{is prime} \quad \Longleftrightarrow \quad \alpha^{\frac{N\pm 1}{3}} \equiv \zeta_3 \bmod N. \tag{4}$$

Instead of solving the problem by constructing α for a single N, we consider *families of integers* of the form $\mathcal{N}_h^+ = \{h \cdot 3^k + 1\}$ and $\mathcal{N}_h^- = \{h \cdot 3^k - 1\}$, for fixed h, with k running, such that $3^k > \sqrt{N}$, to satisfy the requirements of the theorems above. For obvious reasons we will insist that h is even and not divisible by 3. By *constructing an explicit primality test* we will now mean writing $\mathcal{N}_h^+$ (or $\mathcal{N}_h^-$) as a finite union of subsets consisting of $N = h \cdot 3^k + 1$ with k in a fixed residue class modulo an auxiliary integer m, and exhibiting an element α that works for every N in such a subset. We also say that we construct a *finite cover* by doing this.

The reformulated problem reads as follows.

Problem 2.6 *Given an even, positive integer h not divisible by 3, find a finite set $\mathcal{S}_h^+ = \{(m, r, \alpha)_j : j = 1, \ldots, t\}$ of tuples (m, r, α) consisting of an integer m with $m \geq 2$, a representative r for a residue class in $\mathbf{Z}/m\mathbf{Z}$, and an element $\alpha \in \mathbf{Q}(\zeta_3)$, such that for all integers $N \in \mathcal{N}_h^+$ there exists a tuple $(m, r, \alpha) \in \mathcal{S}_h^+$ for which $k \equiv r \bmod m$ and*

$$N = h \cdot 3^k + 1 \quad \textit{is prime} \quad \Longleftrightarrow \quad \alpha^{\frac{N-1}{3}} \equiv \zeta_3 \bmod N. \tag{5}$$

Similarly, find $\mathcal{S}_h^- = \{(m, r, \alpha)_j : j = 1, \ldots, t\}$ such that for all integers $N \in \mathcal{N}_h^-$ there exists a tuple $(m, r, \alpha) \in \mathcal{S}_h^-$ for which $k \equiv r \bmod m$ and

$$N = h \cdot 3^k - 1 \quad \textit{is prime} \quad \Longleftrightarrow \quad \alpha^{\frac{N+1}{3}} \equiv \zeta_3 \bmod N. \tag{6}$$

We have deliberately allowed $\alpha \in \mathbf{Q}(\zeta_3)$; its denominator ought to be coprime to every N for which it is employed. We will use cubic reciprocity to solve this problem.

3 Cubic reciprocity

The cubic character $\left(\frac{\alpha}{\pi}\right)_3$ indicates for an element α of $\mathbf{Z}[\zeta_3]$ whether or not it is a cube modulo π, provided $\pi \in \mathbf{Z}[\zeta_3]$ is a prime element. This fact, together with an efficient method of establishing the character using cubic reciprocity provides a means to solve our problem of finding α efficiently in most cases.

We review the main properties of the cubic character here; for some proofs we refer the reader to [7] and [2].

Definition 3.1 For prime $\pi \in \mathbf{Z}[\zeta_3]$ with $n = \mathrm{Nm}\,\pi \neq 3$, we let $\left(\frac{\alpha}{\pi}\right)_3$ be the element of $\{0, 1, \zeta_3, \zeta_3^2\} \subset \mathbf{Z}[\zeta_3]$ defined as follows, If π divides α then the value is 0, in in all other cases it is the element ζ_3^i satisfying $\alpha^{\frac{n-1}{3}} \equiv \zeta_3^i \bmod \pi$. This is well-defined by Theorem 1.1(iii).

Lemma 3.2 *For every $\alpha \in \mathbf{Z}[\zeta_3]$ and every prime $\pi \in \mathbf{Z}[\zeta_3]$ of norm $n \neq 3$:*

$$\alpha^{\frac{n-1}{3}} \not\equiv 1 \bmod \pi \quad \Longleftrightarrow \quad \forall\, x \not\equiv 0 \bmod \pi :\ x^3 \not\equiv \alpha \bmod \pi \quad \Longleftrightarrow \quad \left(\frac{\alpha}{\pi}\right)_3 \neq 1.$$

Proof All three statements express that α is either 0 mod π or not equivalent to the cube of an element modulo π.

Next one defines the cubic symbol for arbitrary 'denominator' by multiplicativity (in the second argument).

Definitions 3.3 For $\alpha, \beta \in \mathbf{Z}[\zeta_3]$ with $\mathrm{Nm}\,\beta$ not divisible by 3 we define

$$\left(\frac{\alpha}{\beta}\right)_3 = \left(\frac{\alpha}{\pi_1}\right)_3 \cdot \left(\frac{\alpha}{\pi_2}\right)_3 \cdots \left(\frac{\alpha}{\pi_k}\right)_3,$$

where $\pi_i \in \mathbf{Z}[\zeta_3]$ is prime and $\beta = \pi_1 \cdot \pi_2 \cdots \pi_k$.

Other important properties of the cubic residue symbol, including its multiplicativity (in the first argument), are summarized in the following theorem.

Theorem 3.4 *For every α, β in $\mathbf{Z}[\zeta_3]$ the following hold for prime $\pi \in \mathbf{Z}[\zeta_3]$ of norm unequal to 3, and hence for every π of norm not divisible by 3:*

$$\left(\frac{\alpha\beta}{\pi}\right)_3 = \left(\frac{\alpha}{\pi}\right)_3 \left(\frac{\beta}{\pi}\right)_3$$

and

$$\alpha \equiv \beta \bmod \pi \quad \Rightarrow \quad \left(\frac{\alpha}{\pi}\right)_3 = \left(\frac{\beta}{\pi}\right)_3.$$

Proof For prime π both statements follow directly from Definition 3.1; for composite π they then follow from Definition 3.3.

The following is an easy consequence of the definitions that will turn out to be useful for us.

Lemma 3.5 *For any prime element $\pi \in \mathbf{Z}[\zeta_3]$ of norm unequal to 3, and hence for any element of $\mathbf{Z}[\zeta_3]$ of norm not divisible by 3:*

$$\left(\frac{\bar{\alpha}}{\bar{\pi}}\right)_3 = \overline{\left(\frac{\alpha}{\pi}\right)_3}.$$

In particular, for any $m \in \mathbf{Z}$ of norm not divisible by 3:

$$\left(\frac{\bar{\alpha}}{m}\right)_3 = \overline{\left(\frac{\alpha}{m}\right)_3}.$$

Proof Let $n = \mathrm{Nm}\,\pi = \mathrm{Nm}\,\bar{\pi} \neq 3$. Note that by conjugating

$$\alpha^{\frac{n-1}{3}} \equiv \left(\frac{\alpha}{\pi}\right)_3 \bmod \pi$$

we obtain

$$\bar{\alpha}^{\frac{n-1}{3}} \equiv \overline{\left(\frac{\alpha}{\pi}\right)_3} \bmod \bar{\pi},$$

and the first result follows. The second is an immediate consequence.

Definition 3.6 An element $\alpha \in \mathbf{Z}[\zeta_3]$ is *primary* if and only if $\alpha \equiv 2 \bmod 3$.

Lemma 3.7 *The primary prime elements of $\mathbf{Z}[\zeta_3]$ are precisely the positive rational primes $q \equiv 2 \bmod 3$ and the elements $\pi = a + b\cdot\zeta_3$ with $a \equiv 2 \bmod 3$ and $b \equiv 0 \bmod 3$ for which $\mathrm{Nm}\,\pi = a^2 - ab + b^2 = p \equiv 1 \bmod 3$ prime.*

Proof An element $\beta = a + b \cdot \zeta_3 \in \mathbf{Z}[\zeta_3]$ is primary if and only if $a \equiv 2 \bmod 3$ and $b \equiv 0 \bmod 3$. The result follows from the classification of primes in $\mathbf{Z}[\zeta_3]$.

Corollary 3.8 *Let $\beta \in \mathbf{Z}[\zeta_3]$ of norm not divisible by 3. Among the associates of β exactly one is primary, and if β is primary it can be written uniquely (up to order) as a product of primary prime elements and a power of the primary unit -1.*

Proof The first assertion follows from simple inspection of the six associates $\pm\zeta_3^i \cdot \beta$ of β. The second follows by writing β as a product of primary primes and units.

We can now formulate analogues of the law of quadratic reciprocity and the supplementary law for the quadratic character.

Theorem 3.9 [Cubic Reciprocity Law] *Let $\alpha, \beta \in \mathbf{Z}[\zeta_3]$ be primary elements of norm not divisible by 3. Then:*

$$\left(\frac{\alpha}{\beta}\right)_3 = \left(\frac{\beta}{\alpha}\right)_3.$$

Proof Here we refer the reader to [7], Chapter 9, and to [2], Chapter 8 for the proof when both α and β are primary primes. The general statement then follows from Theorem 3.4.

Theorem 3.10 [Supplementary Law] *Let $\beta \in \mathbf{Z}[\zeta_3]$ be a primary prime element, $\beta = (3m-1) + b \cdot \zeta_3$, with $b \equiv 0 \bmod 3$. Then:*

$$\left(\frac{1-\zeta_3}{\beta}\right)_3 = \zeta_3^{2m}.$$

Proof See [2], Theorem 8.1.9.

Finally, the following takes care of the units.

Lemma 3.11 *Let $\pi \in \mathbf{Z}[\zeta_3]$ be a prime element of norm unequal to 3. Then*

$$\left(\frac{-1}{\pi}\right)_3 = \left(\frac{1}{\pi}\right)_3 = 1 \quad \textit{and} \quad \left(\frac{\zeta_3}{\pi}\right)_3 = \begin{cases} 1 & \textit{if} \quad \mathrm{Nm}\,\pi \equiv 1 \bmod 9, \\ \zeta_3 & \textit{if} \quad \mathrm{Nm}\,\pi \equiv 4 \bmod 9, \\ \zeta_3^2 & \textit{if} \quad \mathrm{Nm}\,\pi \equiv 7 \bmod 9. \end{cases}$$

Proof Direct from the definition and evaluation of $\zeta_3^{(\mathrm{Nm}\,\pi-1)/3} \bmod \pi$.

Just as Jacobi symbols can be computed efficiently using just quadratic reciprocity and the ability to divide by 2, the above results enable us to compute the cubic character without a general factorization algorithm in $\mathbf{Z}[\zeta_3]$, as long as we are able to divide by the prime over 3, that is, to take out any factors $1-\zeta_3$.

Algorithm 3.12 *Computing the cubic residue symbol*

in: *Elements α, $\beta \neq 0$ of $\mathbf{Z}[\zeta_3]$ such that β is not divisible by $1-\zeta_3$.*

out: *The value of $\left(\frac{\alpha}{\beta}\right)_3 \in \{0, 1, \zeta_3, \zeta_3^2\}$.*

0. *If $\alpha = 0$ return 0; if β is a unit, then return 1. In all other cases replace β by its unique primary conjugate, initialize $r = 1$ and repeat the following steps:*

1. *Replace α by an element α' of norm less than β in the congruence class $\alpha \bmod \beta$. If $\alpha' = 0$ then return the value 0.*

2. *Find a unit $u \in \mathbf{Z}[\zeta_3]$ and an integer $e \geq 0$ such that $\alpha' = u \cdot (1-\zeta_3)^e \cdot \alpha''$ with α'' primary, and multiply r by the following value (using 3.10 and 3.11):*

$$\left(\frac{u}{\beta}\right)_3 \cdot \left(\frac{1-\zeta_3}{\beta}\right)_3^e.$$

3. *If $\alpha'' = -1$ then return r, otherwise go back to step* **1.** *with α replaced by β and β by α''.*

Termination of this Algorithm in finitely many steps is guaranteed because the norm of α decreases with every time we execute Step 1 (except possibly the first time). Correctness is based on the fact that $\mathbf{Z}[\zeta_3]$ is Euclidean with respect to the norm, on cubic reciprocity, the supplementary law and the result on units above.

4 Explicit primality tests

It may seem that we now have all the ingredients for explicit primality tests. This is certainly the case if $N \equiv 2 \bmod 3$; as we will see below, any cubic non-residue for N can be used to apply Theorem 2.3. If $N \equiv 1 \bmod 3$ there is still a problem: to apply Theorem 2.1 directly we would like to have a cubic non-residue modulo ν, where $N = \mathrm{Nm}\,\nu$. However, computing ν from N may be a cumbersome task (which may not be solvable if N is not prime) that we would like to avoid when possible. However, a cubic non-residue modulo N may well be a residue modulo ν. Conjugates come to the rescue here.

Theorem 4.1 *Suppose that $N > 1$ is odd and that $3^k \mid N^2 - 1$, with $3^k > \sqrt{N}$. If $\alpha \in \mathbf{Z}[\zeta_3]$ satisfies*

$$\left(\frac{\alpha}{N}\right)_3 = \zeta_3$$

then

$$N \text{ is prime in } \mathbf{Z} \iff \begin{cases} \left(\frac{\alpha}{\bar{\alpha}}\right)^{\frac{N-1}{3}} \equiv \zeta_3 \bmod N & \text{if} \quad 3^k | N-1, \\ \left(\frac{\bar{\alpha}}{\alpha}\right)^{\frac{N+1}{3}} \equiv \zeta_3 \bmod N & \text{if} \quad 3^k | N+1. \end{cases} \tag{7}$$

Proof Note that the hypotheses imply that α and $\bar{\alpha}$ are coprime to N.

The implication from right to left follows immediately from Corollary 2.2 and Theorem 2.3, as we can find elements in $\mathbf{Z}[\zeta_3]$ congruent to $\alpha \cdot \bar{\alpha}^{-1}$ and $\bar{\alpha} \cdot \alpha^{-1}$ modulo N.

So suppose for the converse that N is prime, and $\left(\frac{\alpha}{N}\right)_3 = \zeta_3$. Then either $3^k \mid N-1$ or $3^k \mid N+1$ holds. In the former case $N \equiv 1 \bmod 3$ and $N = \nu \cdot \bar{\nu}$, while

$$\left(\frac{\alpha}{\nu}\right)_3 \left(\frac{\alpha}{\bar{\nu}}\right)_3 = \left(\frac{\alpha}{N}\right)_3 = \zeta_3.$$

This leaves three possibilities:

$$\left(\frac{\alpha}{\nu}\right)_3 = \zeta_3, \left(\frac{\alpha}{\bar{\nu}}\right)_3 = 1, \text{ or } \left(\frac{\alpha}{\nu}\right)_3 = 1, \left(\frac{\alpha}{\bar{\nu}}\right)_3 = \zeta_3, \text{ or } \left(\frac{\alpha}{\nu}\right)_3 = \left(\frac{\alpha}{\bar{\nu}}\right)_3 = \zeta_3^2.$$

Now use that by Lemma 3.5

$$\left(\frac{\bar{\alpha}}{\nu}\right)_3 = \overline{\left(\frac{\alpha}{\bar{\nu}}\right)_3},$$

to obtain in all three cases

$$\left(\frac{\alpha}{\nu}\right)_3 \cdot \left(\frac{\bar{\alpha}}{\nu}\right)_3^{-1} \equiv \zeta_3 \bmod \nu.$$

Theorem 2.1 now implies that ν, and hence N, is prime.

If $N \equiv 2 \bmod 3$ is an inert prime in $\mathbf{Z}[\zeta_3]$ of norm N^2, then

$$\left(\frac{\alpha}{N}\right)_3 \equiv \alpha^{\frac{N^2-1}{3}} \equiv \left(\alpha^{N-1}\right)^{\frac{N+1}{3}} \equiv \left(\bar{\alpha} \cdot \alpha^{-1}\right)^{\frac{N+1}{3}} \equiv \zeta_3^2 \cdot \zeta_3^{-1} \bmod N,$$

by Theorem 1.1(i), and since here

$$\left(\frac{\bar\alpha}{N}\right)_3 \equiv \overline{\left(\frac{\alpha}{N}\right)_3} \equiv \zeta^2 \bmod N$$

by Lemma 3.5.

This completes the proof.

Corollary 4.2 *Suppose that $N > 1$ is odd and $3^k \mid N \pm 1$, with $3^k > \sqrt{N}$. If $\alpha \in \mathbf{Z}[\zeta_3]$ satisfies*

$$\left(\frac{\alpha}{N}\right)_3 = \zeta_3$$

then

$$N \text{ is prime in } \mathbf{Z} \quad \Longleftrightarrow \quad \mathrm{Tr}\left(\frac{\alpha}{\bar\alpha}\right)^{\frac{N\pm1}{6}} \equiv \pm 1 \bmod N$$

(where the sign in $N \pm 1$ is chosen in such a way that $N \pm 1$ is divisible by 3).

Proof If N is prime then Theorem 4.1 implies immediately that the trace of $(\alpha/\bar\alpha)^{(N\pm1)/3}$ equals the sum of ζ_3 and its conjugate, which equals -1, modulo N. Only $\pm\zeta_6$ are square root of ζ_3, and the result follows easily.

For the converse, let p be a prime divisor of N in $\mathbf{Z}$. The trace of $(\alpha/\bar\alpha)^{(N\pm1)/6}$ is $\equiv \pm 1$ by hypothesis. Suppose that $u + v \cdot \zeta_3$ is any element of $\mathbf{Q}(\zeta_3)$ of norm 1, for which the trace is $\equiv \pm 1 \bmod p$. Then $u^2 + v^2 - uv = 1$ and $2u - v \equiv \pm 1 \bmod p$. But the only solutions to these equations are

$$u \equiv 0, v \equiv \pm 1 \bmod p, \quad \text{or} \quad u \equiv v \equiv \pm 1 \bmod p$$

when $p > 3$, that is, $u + v\zeta_3 \equiv \pm\zeta_3$ or $\pm\zeta_3^2 \bmod p$. It follows that

$$\frac{\alpha}{\bar\alpha}^{\frac{N\pm1}{3}} \equiv \zeta_3 \ \text{ or } \ \zeta_3^2 \bmod p,$$

so 3^k divides the order of $\alpha \cdot \bar\alpha^{-1}$ modulo p, and the result follows by the usual argument.

The only remaining ingredient now tells us how to compute the trace of a large power of an element modulo N by a simple recursion modulo N.

Lemma 4.3 *Let $\gamma \in \mathbf{Q}(\zeta_3)$ with $\mathrm{Nm}\gamma = 1$. If, for $j \geq 0$,*

$$w_j = \gamma^{3^j} + \gamma^{-3^j},$$

then $w_0 = \mathrm{Tr}\,\gamma \in \mathbf{Q}$ and for $j \geq 0$:

$$w_{j+1} = w_j(w_j^2 - 3) \in \mathbf{Q}.$$

Proof Note that

$$w_j^3 = (\gamma^{3^j} + \gamma^{-3^j})^3 = (\gamma^{3^{j+1}} + \gamma^{-3^{j+1}}) + 3(\gamma^{3^j} + \gamma^{-3^j}) = w_{j+1} + 3w_j.$$

Since $1 = \mathrm{Nm}\gamma = \gamma\bar\gamma$ we see that $\bar\gamma = \gamma^{-1}$, so $\mathrm{Tr}\,\gamma = \gamma + \gamma^{-1} = w_0 \in \mathbf{Q}$; from the recursion we obtain that $w_j \in \mathbf{Q}$.

Corollary 4.4 *Let $N = h \cdot 3^k \pm 1$ with $h > 1$ even and $3^k > h$, and let $\alpha \in \mathbf{Z}[\zeta_3]$ be such that*

$$\left(\frac{\alpha}{N}\right)_3 \in \{\zeta_3, \zeta_3^2\}.$$

Then:

$$N \text{ is a prime number} \quad \Longleftrightarrow \quad w_{k-1} \equiv \pm 1 \bmod N,$$

where

$$w_0 = \mathrm{Tr}\left(\frac{\alpha}{\bar{\alpha}}\right)^{\frac{h}{2}} \quad \text{and} \quad w_j = w_{j-1}(w_{j-1}^2 - 3), \quad \text{for } j \geq 1.$$

Proof Immediate by the previous Corollary.

Remarks 4.5 The computation of w_0 can also be done recursively in $\mathbf{Q}$, using for example that

$$v_i v_j = v_{i+j} - v_{i-j}, \quad \text{for} \quad i \geq j \geq 0,$$

when $v_i = \mathrm{Tr}\left(\frac{\alpha}{\bar{\alpha}}\right)^i$. The single rational number w_0 will be used for all exponents k in a residue class modulo an auxiliary number m. However, if h becomes bigger it may be more convenient to compute w_0 modulo N for each k, since the rational number may become rather large.

The use of $(N \pm 1)/6$ in Corollary 4.2 rather than $(N \pm 1)/3$, and consequently of $h/2$ in Corollary 4.4 rather than h leads only to a minor improvement over the equivalent test

$$N \text{ is prime} \quad \Longleftrightarrow \quad w_{k-1} \equiv -1 \bmod N,$$

where $w_0 = \mathrm{Tr}\left(\frac{\alpha}{\bar{\alpha}}\right)^h$ and $w_j = w_{j-1}(w_{j-1}^2 - 3)$. However it suggests that we could have used the sextic residue symbol symbol rather than the cubic symbol: indeed $\mathbf{Z}[\zeta_3]$ contains the sixth roots of unity.

5 Finding covers

To make the main test from the previous section, Corollary 4.4, entirely explicit, we will attempt to solve the following problem.

Problem 5.1 *Given an even, positive integer h not divisible by 3, find a finite set $\mathcal{S}_h^+ = \{(m, r, \alpha)_j : j = 1, \ldots, t\}$ of tuples (m, r, α) consisting of an integer m with $m \geq 2$, a representative r for a residue class in $\mathbf{Z}/m\mathbf{Z}$, and an element $\alpha \in \mathbf{Q}(\zeta_3)$, such that for all integers k with $3^k > h$ there exists a tuple $(m, r, \alpha) \in \mathcal{S}_h^+$ for which $k \equiv r \bmod m$ and*

$$\left(\frac{\alpha}{h \cdot 3^k + 1}\right)_3 \neq 1. \tag{8}$$

Similarly, for the set $\mathcal{S}_h^-$, we require

$$\left(\frac{\alpha}{h \cdot 3^k - 1}\right)_3 \neq 1. \tag{9}$$

Remark 5.2 It will be clear that any α with residue symbol ζ_3 or ζ_3^2 will be useful in the primality test of Corollary 4.4. If we would use only such elements, we would only need to consider prime elements $\pi \in \mathbf{Z}[\zeta_3]$ not in $\mathbf{Z}$ (by Lemma 3.5). However, rational primes $\equiv 2 \bmod 3$ will be useful as divisors, elements for which the cubic symbol becomes zero! See also the examples below.

Before we consider an algorithm to construct covers, we give a negative result, showing that such covers do not always exist.

Proposition 5.3 *Finite covers do not exist for $\mathcal{N}_h^+$ when $h = 27^m - 1$, with $m \geq 1$, and they do not exist for $\mathcal{N}_h^-$ when $h = 27^m - 1$, with $m \geq 1$, and $h = 27^m + 1$, with $m \geq 0$.*

Proof Suppose that C is some finite cover of elements from $\mathbf{Z}[\zeta_3]$; let P be the finite set of primes in $\mathbf{Z}$ consisting of the primes $q \in \mathbf{Z}$ dividing some $c \in C$ and the primes $p = \operatorname{Nm}\pi$, for $\pi \in \mathbf{Z}[\zeta_3] \setminus \mathbf{Z}$, for which π divides some $c \in C$. Choosing k to be a multiple of all multiplicative orders $o_p(3)$ of 3 modulo p in P it is easy to see that all elements in C are cubic residues modulo $(27^m - 1) \cdot 3^k + 1$.

This shows that no finite cover for $\mathcal{N}_h^+$ exists when $h = 27^m - 1$.

The same argument shows that no finite cover for $\mathcal{N}_h^-$ can exist when $h = 27^m + 1$.

Choosing k simultaneously congruent to $-3m$ modulo every order $o_p(3)$ we find a that every prime is cubic residue modulo $(27^m - 1) \cdot 3^k - 1$. That proves $\mathcal{N}_h^+$ has no finite cover when $h = 27^m - 1$.

Remark 5.4 This results is an immediate analogue of a results in [4]. The argument given was later generalized by Williams in [11]; see also [8].

Here is a very simple but effective way to find a cover for given h.

Algorithm 5.5 *Finding a cover*

in: *Element h of $\mathbf{Z}$ such that h is even and not divisible by 3*

out: *A finite cover $\mathcal{S}_h^+$ for $\mathcal{N}_h^+$, or the empty set*

0. *Find a sequence P of odd primes p_i as well as a corresponding sequence O consisting of the multiplicative orders o_i of 3 modulo p_i for each of the p_i. Moreover, let Π be a sequence of primes π_i in $\mathbf{Z}[\zeta_3]$ such that $\operatorname{Nm}\pi_i = p_i$ if $p_i \equiv 1 \bmod 3$ and $\pi_i = p_i$ if $p_i \equiv 2 \bmod 3$. For P one could use the complete factorization for $3^e - 1$ for $1 \leq e \leq 50$, for example.*

Initialize $k = 0$ and $M = \{1\}$ and repeat the following three steps.

1. *Increment k and find the subset Π_k of primes π in Π with $\left(\frac{\pi}{h \cdot 3^k + 1}\right)_3 \neq 1$ as well as the corresponding sequence O_k of multiplicative orders for 3 modulo $\pi \in \Pi_k$. If Π_k is empty, then no cover is found and the empty set returned.*

2. *Replace M by the set of least common multiples* $\operatorname{lcm}(m, o)$ *of elements m of M with elements o of O_k. [The elements of the new M are the moduli m with the property that we have found cubic non-residues for exponents in residue classes j modulo m with $1 \leq j \leq k$.]*

3. *If $k \notin M$ then go back to step* **1**. *Otherwise, return the finite cover $\mathcal{S}_h^+$ consisting of triples (m_j, j, π_j) for $1 \leq j \leq k$, with m_j a divisor of k and π_j an element of Π_j found in step* **1** *with the order of* 3 *modulo π_j equal to m_j and $\left(\frac{\pi_j}{h \cdot 3^k+1}\right)_3 \neq 1$.*

Remarks 5.6 Several tricks (most of them also described in [4]) can be used to enhance the performance of the algorithm, We indicate a few.

The algorithm was used to compute covers for a large collection of values for h. Once a cover is found for a particular value of h it will be useful for certain residue classes of h with respect to some auxiliary modulus. Computing these residue classes makes it possible to re-use the cover quickly.

For hard cases (see also Section 6) it is often possible to predict which primes will have to appear and hence a factor that will appear in the auxiliary modulus m, by looking at values for which $h \cdot 3^k \pm 1$ is a cube.

It is often not necessary to factor large values of $3^e - 1$ to use a large modulus: known factors for all proper divisors of e can be used.

Example 5.7 To explain the idea behind the algorithm we construct $\mathcal{S}_{14}^-$.

For step **0** of the algorithm we generate the prime factorization of $3^e - 1$ for $e \leq 50$. In the table below we give a relevant excerpt, in which the third and fourth columns list the primitive prime factors that are 2 and 1 mod 3 respectively, for each e. In the fifth column we give one of the conjugates in $\mathbf{Z}[\zeta_3]$ of the primes that are 1 mod 3. We only listed the primitive primes, that is, those that do not appear for a smaller e. This also means that e is the order of 3 modulo the primes in the row for e.

In step **1** we find the primes that give a non-zero cubic residue symbol with $h \cdot 3^k - 1 = 41$; it turns out that the first few are $3\zeta_1$, of order $e = 3$, $36\zeta + 29$ of order $e = 7$, 41 of order 8, $27\zeta - 1$ of order $e = 9$ and $9\zeta + 8$ of order 12. This means that we can use these elements for k with $k \equiv 1 \bmod 3$, $1 \bmod 7$, $1 \bmod 8$, $1 \bmod 9$ and $1 \bmod 12$ respectively.

The set M in step **2** will therefore contain $3, 7, 8, 9, 12$ and their multiples (in fact we will only store $3, 7, 8$ of these, and remember that all multiples of elements should be included as well).

Since $k = 1$ is not contained in M, we return in step **3** to step **1** and repeat the search for cubic non-residues with $14 \cdot 3^2 - 1 = 125$. Of course we will only find that $q = 5$ works! And as the order e of 3 modulo 5 is 4, it will work for any k with $k \equiv 2 \bmod 4$.

The set M will then be updated to consist of common multiples of 4 and the integers previously found, so multiples of $8, 12, 28$ and so on.

For $k = 3$ the elements of order $3, 7, 9, 12$ we found before work again, and M contains multiples of $12, 28, 40$ and so on. This means, then, that we can deal with $k = 1, 2, 3$ using only prime divisors of $3^{12} - 1$, or only prime divisors of $3^{28} - 1$, and so on.

We know from what we saw for $k = 1$ that $3\zeta - 1$ will also work for $k = 4, 7, 10$. The algorithm simply repeats step **1** for $k = 4$, without using this knowledge. The smallest entries of M remain $12, 28, 40$ after this round for $k = 4$.

e	$3^e - 1$	q	p	π
1	2	2		
2	8			
3	26		13	$3\zeta - 1$
4	80	5		
5	242	11		
6	728		7	$-3\zeta - 1$
7	2186		1093	$36\zeta + 29$
8	6560	41		
9	19682		757	$27\zeta - 1$
10	59048		61	$9\zeta + 5$
11	177146	$23, 3851$		
12	531440		73	$9\zeta + 8$
13	1594322		797161	$351\zeta - 664$
14	4782968		547	$-27\zeta - 13$
15	14348906		4561	$-75\zeta - 19$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
24	282429536480		6481	$81\zeta + 80$

When looking at $k = 5$, no divisors of 12 yield useful primes, and the set M will contain $24, 28, 36, 40$ as smallest elements after this. From then on we find for every k with $6 \leq k \leq 24$ a prime element π for which the order e of 3 mod π divides 24 that furnishes a non-cubic residue. Hence, when we get to $k = 24$, we finally arrive at the situation where k is contained in M, and we are essentially finished. The only remaining task, when we want to produce the test explicitly, is to recover all elements and the residue classes for which they work; we now know where to look and just consider the prime divisors of $3^{24} - 1$ again (or we could have kept track somehow along the line).

The cover we find is summarized as follows.

$$\mathcal{S}_{14}^{-} = \{(3, \{0, 1\}, 3\zeta - 1), (4, 2, 5), (12, \{8, 11\}, 9\zeta + 8), (1, 8, 41), (24, \{5, 11\}, 81\zeta + 80)\}$$

This means that $3\zeta - 1$ works for $0, 1$ mod 3, and 5 works for 2 mod 4, etc.

6 Computational results

In this Section we list some of the results and curiosities found while computing covers for all h up to 10^5 using MAGMA, cf. [5]. We used factors of $3^e - 1$ for e up to 340.

Example 6.1 The first example concerns a cover $\mathcal{S}_2^{+}$ for the smallest case $h = 2$.

Since

$$\left(\frac{2\cdot 3^k+1}{3\zeta_3-1}\right)_3 = \begin{cases} \zeta_3^2 & \text{if} \quad k\equiv 0 \bmod 3, \\ \zeta_3 & \text{if} \quad k\equiv 1,2 \bmod 3, \end{cases}$$

the cover can be summarized by

$$\mathcal{S}_2^+ = \{(3,\{0,1,2\},3\zeta_3-1)\},$$

to emphasize that a *single element* can be used for all k. We say that *a single-element cover* exists when this happens.

Example 6.2 In this example we give a finite cover $\mathcal{S}_{98}^+$: we contend that the following set of tuples forms a finite cover for $h=98$. Here we use the same convention as in the previous example to denote that an element can be used for several residue classes.

$$\mathcal{S}_{98}^+ = \{(3,1,3\zeta_3-1),(4,1,5),(12,\{0,3,8,11\},9\zeta_3+8),(24,\{2,6,14,18\},81\zeta_3+80)\}$$

This is a four-element cover. It is easy to see that all residue classes modulo 24 are indeed covered by these cases, and it is also easily verified that the cubic symbols involved are not 1. Note that the element 5 works for $k\equiv 1 \bmod 4$ since $98\cdot 3^k+1$ is divisible by 5 in this case.

The first table below lists the values of e used for the 33334 cases for h even and not divisible by 3 below 10^5; the first line does so for $h\cdot 3^k+1$, the second for $h\cdot 3^k-1$. The entry 6594 in the + line in the column with $m=6$ means, for example, that for 6594 values of h less than 10^5 we found a cover using prime divisors of 3^6-1. These divisors are 7 and 13, and it means that $-3\zeta_3-1$ and $3\zeta_3-1$ provided a cover in these cases.

The first column in the table (with $m=0$) is used to indicate the exceptional cases when no finite cover exists: this happens for $h=2,27\pm 1,729\pm 1,19683\pm 1$ in $h\cdot 3^k-1$ and for $h=26,728,19682$ in $h\cdot 3^k+1$ (compare Proposition 5.3).

Note that a table like this is very sensitive to the order in which one looks for covers. Very often several (small) covers exist and the one found first depends on the order in which covers already found for other h are searched for re-use, for example.

m	0	3	6	7	9	10	12	13	14	15	16	18	≥ 19
+	3	15385	6594	245	133	53	1634	6	284	52	0	6630	2315
−	7	15385	6595	214	144	47	1546	6	242	46	1	7008	2093

For $h\cdot 3^k-1$ we used m exceeding 100 only six times, the largest being $m=176$ for $h=26110$ and $m=318$ for $h=15124$. For $h\cdot 3^k+1$ it happened five times that m exceeded 100; the largest cases occurred for $h=17822$ ($m=162$) and $h=40346$ ($m=246$).

The second table lists the sizes of the covers generated.

#	0	1	2	3	4	5
+	3	15649	15847	1766	65	4
−	7	15612	16107	1540	61	7

We did not adapt our algorithm to look systematically for small covers first, so the table does not imply that single-element covers will only exist in roughly half the cases. Since this question was raised before by Williams we look into it a little more closely.

Once an element $\alpha \in \mathbf{Z}[\zeta_3]$ provides a single-element cover, it will do so for certain residue classes of h modulo $\mathrm{Nm}\,\alpha$. Very few elements however, do provide single element covers.

Examples 6.3 The prime element $3\zeta_3 - 1$ lying over 13 provides a single-element cover of $\mathcal{S}_h^+$ for half the non-zero residue classes of h modulo 13 (as does its conjugate $-3\zeta_3 - 4$), namely when $h \equiv 1, 2, 3, 5, 6, 9 \bmod 13$; these fill two cosets of the subgroup generated by 3 in $(\mathbf{Z}/13\mathbf{Z})^*$. Similarly, for a single coset of h (consisting of 9 elements) modulo 757 the element $27\zeta_3 - 1$ gives a single-element cover, and 11 cosets of size 7 give 77 residue classes modulo 1093 covered by the single element $36\zeta_3 + 29$ or its conjugate. A single coset of size 15 of residue classes for h modulo 4561 is covered by $-75\zeta_3 - 19$. There are no other cases of elements of norm less than 10000 that provide single-element covers. This clearly gives a lower bound for the fraction of h for which a single element cover exists.

As there are exactly 15385 integers h below 10^5 in the residue classes 1, 2, 3, 5, 6, 9 mod 13, the single element $3\zeta_3 - 1$ is responsible the first entry in the first table, as well as the majority of the 15649 single-element covers in the + case.

In 245 more cases we used the single-element cover $36\zeta_3 + 29$ in 6 cases the element $351\zeta - 664$ of norm 797161 ($e = 13$) and in 13 cases the element $-75\zeta - 19$ of norm 4561.

The corresponding numbers for − are 214, 6, 6, and in one case we used the element $168\zeta - 505$ of norm 86716 (a divisor of $3^{21} - 1$).

Example 6.4 Our standard algorithm not always finds these single-element covers (first). For example, when $h = 62$, our algorithm produces the two-element cover

$$\mathcal{S}_{62}^+ = \{(6, \{0, 1, 3, 4, 5\}, -3\zeta_3 - 1), (3, 2, 3\zeta_3 - 1)\}$$

whereas the single-element cover

$$\mathcal{S}_{62}^+ = \{(7, \{0, \ldots, 6\}, 36\zeta_3 + 29)\}$$

also works. In this case, Corollary 4.4 reads as follows: for $k \geq 4$

$$N = 62 \cdot 3^k + 1 \text{ is prime} \quad \Longleftrightarrow \quad w_{k-1} \equiv \pm 1 \bmod N,$$

where $w_j = w_{j-1}(w_{j-1}^2 - 3)$ and w_0 equals

$$\frac{1802735979234295773020016465809702988876663383390446444230256347985656038624690524286426617380 2}{1574798601491537183123369748283101884240139220354321372755447549738595342523318111694928819815 7}$$

Example 6.5 Another interesting example is $h = 4$. Our algorithm finds a two-element cover

$$\mathcal{S}_4^+ = \{(6, \{0, 2, 3, 5\}, -3\zeta_3 - 1), (3, \{1\}, 3\zeta_3 - 1)\}.$$

However, when $k \equiv 1 \bmod 3$ then $4 \cdot 3^k + 1$ is divisible by 13 and hence only prime for $k = 1$. But that means that there remain only 4 interesting residue classes for k modulo 6 to be tested. In fact, for $k \equiv 5 \bmod 6$ we always get divisibility by 7, and only three cases remain. Thus:

$$4 \cdot 3^k + 1 \text{ is prime} \quad \Longleftrightarrow \quad k = 1, \text{ or } k \equiv 0, 2, 3 \bmod 6 \text{ and } w_{k-1} \equiv \pm 1 \bmod N,$$

where $w_j = w_{j-1}(w_{j-1}^2 - 3)$ and $w_0 = \frac{71}{49}$.

It is an easy consequence of Lemma 3.11 that if a prime π gives a single-element cover for $h \cdot 3^k + 1$ when $h \equiv r \bmod m$, then π also provides a single-element cover for $h \cdot 3^k - 1$ when $h \equiv -r \bmod m$. In particular, $-1 + \zeta_3$ forms a single-element cover for $\mathcal{S}_h^-$ when when $h \equiv 4, 7, 8, 10, 11, 12 \bmod 13$.

We constructed finite covers $\mathcal{S}_h^+$ and $\mathcal{S}_h^-$ for all $h \leq 10^5$ (except for the cases $27^m \pm 1$ mentioned in 5.3 of course). We also executed the explicit primality tests in these cases to find all primes with $k \leq 1000$. Some statistics will appear on my web page; here I mention just another curiosity. The smallest prime in the family $\mathcal{H}_{302}^-$ occurs at $k = 2091$, giving the 1001 digit prime $302 \cdot 3^{2091} - 1$. This made us wonder about the existence of analogues to the numbers that have the names of Riesel, Sierpinski and Selfridge attached to them (see for example [1], or Problem **B21** in [6] and the references therein). These are numbers $h \cdot 2^k \pm 1$ that are composite for all $k \geq 1$, and for which there exists a finite cover of prime divisors. By slightly adapting our algorithm we could simply search for covers consisting solely of elements giving cubic symbol equal to zero. We found no examples for $h \leq 10^7$, using all primes appearing in the factorization of $3^e - 1$ for $e \leq 300$. A similar search among $h \cdot 2^k \pm 1$ quickly generates the known examples below 10^6, $h = 78557, 271129, 271577, 322523, 327739, 482719, 575041, 603713$, for $h \cdot 2^k + 1$ and $h = 509203, 762701, 777149, 790841, 992077$, for $h \cdot 2^k - 1$.

References

[1] Baillie, Robert, and G. V. Cormack, H. C. Williams, *The problem of Sierpinski concerning* $k \cdot 2^n + 1$, Math. Comp. **37** (1981), 229–231, corrigendum: **39** (1982), 308.

[2] Berndt, Bruce C., Ronald J. Evans and Kenneth S. Williams, *Gauss and Jacobi Sums*, Canad. Math. Soc. series of monographs and advanced texts **21**, John Wiley & Sons, New York, 1997.

[3] Berrizbeitia, Pedro, and T. G. Berry, *Cubic reciprocity and generalized Lucas-Lehmer tests for primality of* $A \cdot 3^n \pm 1$, Proc. Amer. Math. Soc. **127**-7 (1999), 1923–1925.

[4] Bosma, Wieb, *Explicit primality criteria for* $h \cdot 2^k \pm 1$, Math. Comp. **61**-203 (1993), 97–109.

[5] Bosma, Wieb, John Cannon, and Catherine Playoust, *The Magma Algebra System I: The User Language*, J. Symbolic Comp. **24** (1997), 235–265.

[6] Guy, Richard K., *Unsolved problems in number theory*, Unsolved problems in intuitive mathematics **1**, Springer, New York 1994 (second edition).

[7] Ireland, Kenneth, and Michael Rosen, *A classical introduction to modern number theory*, Graduate texts in mathematics **84**, Springer, New York, 1982.

[8] Stein, Andreas, and H. C. Williams, *Explicit primality criteria for* $(p-1)p^n - 1$, Math. Comp. **69**-232, 1721–1734.

[9] Williams, H. C. *The primality of* $N = 2A3^n - 1$, Canad. Math. Bull. **15**-4, (1972), 585–589.

[10] Williams, H. C. *A class of primality tests for trinomials which includes the Lucas-Lehmer test*, Pacific J. Math. **98**-2, (1982), 477–494.

[11] Williams, Hugh C. *Édouard Lucas and primality testing*, Canad. Math. Soc. series of monographs and advanced texts **22**, John Wiley & Sons, New York, 1998.