BULL. AUSTRAL. MATH. SOC. 11Y11, 11A51
VOL. 74 (2006) [419–441]

A GENERALISED LUCASIAN PRIMALITY TEST

ZHENXIANG ZHANG, WEIPING ZHOU AND XIANBEI LIU

We present a primality test for numbers of the form $M_{h,n} = h \cdot 2^n \pm 1$ (in particular with h divisible by 15), which generalises Berrizbeitia and Berry's test for such numbers with $h \not\equiv 0 \bmod 5$. With our generalised test, the primality of such a number $M_{h,n}$ can be proved by means of a Lucas sequence with a seed determined by h and π_q — primary irreducible divisor of a prime $q \equiv 1 \bmod 4$. We call the prime q a *judge* of the number $M_{h,n}$. We prescribe a sequence $\mathcal{S}$ of 48 primes $\equiv 1 \bmod 4$ in the interval $[13, 2593]$ such that, for all odd $h = 15t < 10^8$ and for all $n < 7.3 \cdot 10^{11}$, each number $M_{h,n}$ has a judge q in $\mathcal{S}$. Comparisons with Bosma's explicit primality criteria in "a well-defined finite sense" for the case $h = 3t < 10^5$ are given.

1. INTRODUCTION

Two classical results express that primality of $2^n \pm 1$ can be decided by a single modular exponentiation. Let $n \geqslant 2$, then as Pépin knew in 1877,

$$M = 2^n + 1 \text{ is prime} \iff 3^{(M-1)/2} \equiv -1 \bmod M. \tag{1.1}$$

On the other hand for $2^n - 1$, the formulation involves a Lucas sequence. The Lucas sequence with seed w_0 is the sequence $\{w_j\}$ defined from the given initial value w_0 by the recurrence:

$$w_{j+1} = w_j^2 - 2 \text{ for } j \geqslant 0. \tag{1.2}$$

Let $n \geqslant 3$, then as given by Lucas [8] and Lehmer [7],

$$M = 2^n - 1 \text{ is prime} \iff w_{n-2} \equiv 0 \bmod M, \tag{1.3}$$

where $\{w_j\}$ is the Lucas sequence with seed $w_0 = 4$.

The two tests (1.1) and (1.3) generalise to primality tests for integers of the forms

$$M_{h,n,+} = h \cdot 2^n + 1 \text{ and } M_{h,n,-} = h \cdot 2^n - 1 \tag{1.4}$$

Received 5th June, 2006
Research supported by the NSF of China Grant 10071001.

with h odd and $h < 2^n$ as follows. (All h in this paper are positive.) As Proth knew in 1878,

(1.5) $M = M_{h,n,+}$ is prime
$$\iff \text{there exists an integer } b \text{ such that } b^{(M-1)/2} \equiv -1 \bmod M.$$

Whereas for $M_{h,n,-}$, let $d \in \mathbb{Z}$ satisfy

$$\left(\frac{d}{M}\right) = -1, \tag{1.6}$$

where $(*/M)$ is the Jacobi symbol. Let $K = \mathbb{Q}(\sqrt{d})$, and let $\mathbb{Z}_K$ be the ring of integers of K. Let $\alpha \in \mathbb{Z}_K$ satisfy

$$\left(\frac{\alpha\overline{\alpha}}{M}\right) = -1, \tag{1.7}$$

where $\overline{\alpha}$ denotes the conjugate of α in K. Then [**10**]

$$M = M_{h,n,-} \text{ is prime} \iff (\alpha/\overline{\alpha})^{(M+1)/2} \equiv -1 \bmod M \iff w_{n-2} \equiv 0 \bmod M, \tag{1.8}$$

where $\{w_j\}$ is the Lucas sequence with seed

$$w_0 = (\alpha/\overline{\alpha})^h + (\overline{\alpha}/\alpha)^h = \mathrm{Tr}_{K/\mathbb{Q}}(\alpha/\overline{\alpha})^h. \tag{1.9}$$

Note that, given h, the seed w_0 in (1.9) is uniquely determined by the pair (d, α). For this reason, we call the pair (d, α) satisfying (1.6) and (1.7) (respectively, the integer b in (1.5)) a *judge* (of primality) of $M_{h,n,-}$ (respectively, of $M_{h,n,+}$) for short. In general, the judge depends on n as well as on h. However, it is certainly desirable to have it independent of n, if possible.

If $h \not\equiv 0 \bmod 3$, one may take $b = 3$ in (1.5) and

$$(d, \alpha) = (12, 2 + \sqrt{12}), \text{ hence } w_0 = (2 + \sqrt{3})^h + (2 - \sqrt{3})^h \tag{1.10}$$

in (1.8) for all n. More precisely, if

$$n \geqslant 2 \text{ and } 2^n > h \not\equiv 0 \bmod 3,$$

then [**2**, Theorem 3.1]

$$M = M_{h,n,+} \text{ is prime} \iff 3^{(M-1)/2} \equiv -1 \bmod M; \tag{1.11}$$

and [**11**, Theorem 4.16], [**2**, Theorem 3.2]

(1.12) $M = M_{h,n,-}$ is prime
$$\iff \left(\frac{2 + \sqrt{12}}{2 - \sqrt{12}}\right)^{(M+1)/2} \equiv -1 \bmod M \iff w_{n-2} \equiv 0 \bmod M,$$

where $\{w_j\}$ is the Lucas sequence with seed w_0 as given in (1.10).

The case $h \equiv 0 \bmod 3$ is studied in [**2, 10**]. In [**10, 11**] tables of seeds are given for $M_{h,n,-}$ for odd $h < 30$. In [**2**] for each $h \equiv 0 \bmod 3$, $h < 10^5$, but h not of the form $4^m - 1$, Bosma designed algorithms for determining finite sets of judges

$$\mathcal{B}_h = \{b_j\}, \quad \text{and} \quad \mathcal{D}_h = \{(d_j, \alpha_j)\} \tag{1.13}$$

such that, for any n, there is a judge of $M_{h,n,+}$ in $\mathcal{B}_h$; and a judge of $M_{h,n,-}$ in $\mathcal{D}_h$. On the other hand, for h of the form $4^m - 1$, he proves that there are no such finite sets (1.13) of judges.

Recently, Berrizbeitia and Berry [**1**] show that, a modification of the test (1.8) allows them, for $h \not\equiv 0 \bmod 5$, to test primality of $M_{h,n,-}$ and $M_{h,n,+}$ by means of a Lucas sequence with a seed independent of n. In particular when $h = 4^m - 1$, m odd, they have a single seed. More precisely, they prove the following Theorem 1, where they use notation

$$k^* = \left(\frac{-1}{k}\right) k \tag{1.14}$$

for any odd integer k. This notation allows them to treat the cases

$$M_{h,n} = h \cdot 2^n \pm 1 \tag{1.15}$$

simultaneously, where $M_{h,n}$ means either $M_{h,n,+}$ or $M_{h,n,-}$.

THEOREM 1. ([**1**, Theorem 3]) *Let $M = M_{h,n} = h \cdot 2^n \pm 1$ where $h < 2^{n-2} - 1$ is odd, $h \not\equiv 0 \bmod 5$, and $n \geqslant 4$. Let $\pi = -1 + 2i \in \mathbb{Z}[i]$, and let $\{w_j\}$ be the Lucas sequence with seed $w_0 = (\pi/\overline{\pi})^h + (\overline{\pi}/\pi)^h$. Then*

$$M \text{ is prime} \iff \begin{cases} w_{n-2} \equiv 0 \mod M, & \text{when } M^* \equiv \pm 2 \mod 5; \\ w_{n-3} \equiv 0 \mod M, & \text{when } M^* \equiv -1 \mod 5. \end{cases}$$

Berrizbeitia and Berry [**1**] did not say anything about the case $h \equiv 0 \bmod 5$. Of course, if $h \equiv 0 \mod 5$ but $h \not\equiv 0 \bmod 3$, tests (1.11) and (1.12) are still applicable. The remaining case is therefore $h \equiv 0 \bmod 15$, when it seems that one has to appeal Bosma's approach for determining finite sets (1.13) for the case $h \equiv 0 \bmod 3$.

In this paper, we go a little further to present a generalised test, which includes Berrizbeitia and Berry's test as a special case, and which can treat the cases (1.15) simultaneously as the Berrizbeitia and Berry test does. Moreover, our generalised test treats the case $h \equiv 0 \bmod 15$ more practically than using Bosma's approach for the case $h \equiv 0 \bmod 3$. We state our generalised test and main tasks of this paper in the following section.

2. The generalised test and main tasks

Let $D = \mathbb{Z}[i]$ be the ring of Gaussian integers, and by a prime we always mean a positive prime of $\mathbb{Z}$. Before stating our generalised test, we recall some basic facts concerning D and biquadratic residue characters. Details can be found in [**6**, Chapter 9], see also [**12**, Section 2].

It is well-known that D is a Euclidean domain. Let $\alpha, \beta, \pi \in D$. The norm of α, $N(\alpha) = \alpha\bar{\alpha} = 1$ if and only if α is a unit. The units of D are $\pm 1, \pm i$. The irreducibles of D are $\pm 1 \pm i$ with norm 2, primes $\equiv 3 \mod 4$ and their associates, and non-real elements with prime norms $\equiv 1 \mod 4$. A nonunit α is called primary if $\alpha \equiv 1$ or $3 + 2i \mod 4$. Among four associates of a nonunit α satisfying $(1+i) \nmid \alpha$ there is (only) one which is primary. A prime $q \equiv 1 \mod 4$ must be the norm of a unique primary irreducible π_q of D. If q is small, say $< 10^8$, then π_q is easily found by trial and error. There exist efficient algorithms for larger q, see [**4**, Algorithms 2.3.12 and 2.3.13]. If π is an irreducible with $N(\pi) \neq 2$, then there exists a unique integer $m, 0 \leqslant m \leqslant 3$, such that $\alpha^{(N(\pi)-1)/4} \equiv i^m \mod \pi$. The biquadratic residue character of α, for $\pi \nmid \alpha$, is defined and denoted by $(\alpha/\pi)_4 = i^m$, which is $1, -1, i$ or $-i$.

Now we are ready to state our generalised test in the following Theorem 2.

Theorem 2. *Let $M = M_{h,n} = h \cdot 2^n \pm 1$ where $h < 2^{n-2} - 1$ is odd and $n \geqslant 4$. Suppose that q is a prime $\equiv 1 \mod 4$ with primary irreducible $\pi = \pi_q = a + bi \in \mathbb{Z}[i]$ satisfying $N(\pi) = \pi\overline{\pi} = q$ and $(M^*/\pi)_4 \neq 1$. Let $\{w_k\}$ be the Lucas sequence with seed $w_0 = (\pi/\overline{\pi})^h + (\overline{\pi}/\pi)^h$. Then*

$$M \text{ is prime} \iff \begin{cases} w_{n-2} \equiv 0 \mod M, & \text{when } \left(\dfrac{M^*}{\pi}\right)_4 = \pm i; \\ w_{n-3} \equiv 0 \mod M, & \text{when } \left(\dfrac{M^*}{\pi}\right)_4 = -1. \end{cases}$$

Given h and n, let q be a prime $\equiv 1 \bmod 4$. If

$$\left(\frac{M^*_{h,n}}{\pi_q}\right)_4 \neq 1, \tag{2.1}$$

then by Theorem 2, the primality of $M_{h,n}$ can be proved by means of a Lucas sequence with seed w_0 depending only on π_q and h. On the other hand, if

$$\begin{cases} \left(\dfrac{M^*_{h,n}}{\pi_q}\right)_4 = 1, \\ 1 < \gcd(M_{h,n}, 2^{\operatorname{ord}_q(2)} - 1) < M_{h,n} \end{cases} \tag{2.2}$$

or

$$\begin{cases} \left(\dfrac{M^*_{h,n}}{\pi_q}\right)_4 = 1, \\ 1 < \gcd(M_{h,n}, 2^{\operatorname{ord}_q(2)} + 1) < M_{h,n} \end{cases} \tag{2.3}$$

https://doi.org/10.1017/S0004972700040478 Published online by Cambridge University Press

then $M_{h,n}$ is a composite, where $\mathrm{ord}_q(2)$ denotes the multiplicative order of 2 modulo q. Note that $M_{h,n}$ means either $M_{h,n,-}$ or $M_{h,n,+}$.

DEFINITION 2.1: If one of the three equations (2.1), (2.2) and (2.3) holds, we call the prime q a *bi-quadratic judge* of primality of the number $M_{h,n}$, or a *judge* of $M_{h,n}$ for short.

DEFINITION 2.2: Given an odd h, if there exists a common judge q of the numbers $M_{h,n}$ for all n, or in other words, the system

$$\text{(2.4)} \qquad \begin{cases} \left(\dfrac{M^*_{h,n}}{\pi_q}\right)_4 = 1, \\ \gcd(M_{h,n}, 2^{\mathrm{ord}_q(2)} - 1) = 1 = \gcd(M_{h,n}, 2^{\mathrm{ord}_q(2)} + 1) \end{cases}$$

has no solutions in n, we call the prime q a *minus flag* or *plus flag* of h according to that $M_{h,n}$ means $M_{h,n,-}$ or $M_{h,n,+}$. An odd h may have several minus or plus flags. We denote the smallest minus and plus flag of h by f_h^- and f_h^+ respectively.

Not every odd $h = 15t$ has minus and/or plus flags. For those odd $h = 15t$ having no minus and/or plus flags, one wonders whether it would be possible to solve the following problem.

PROBLEM 2.1. Given an odd $h = 15t$. Determine a finite set $\mathcal{W}_h^-$ (respectively $\mathcal{W}_h^+$) such that for any n, $M_{h,n,-}$ (respectively $M_{h,n,+}$) has a judge in $\mathcal{W}_h^-$ (respectively $\mathcal{W}_h^+$).

In Section 3 we prove Theorem 2, the proof uses biquadratic reciprocity as the proof of Berrizbeitia and Berry's Theorem 1 does. In Section 4, we tabulate 16 primes with the smallest being 13 and the largest being 2089, which are minus or plus flags of some odd $h = 15t < 10^8$. In Section 5 we prescribe a sequence $\mathcal{S}$ of 48 primes $\equiv 1 \bmod 4$ in the interval $[13, 2593]$ having the following properties: for all but a few odd $h = 15t < 10^8$, there exists a subset (subsequence)

$$\text{(2.5)} \qquad \mathcal{W}_h^- \text{ (respectively } \mathcal{W}_h^+) \subseteq \mathcal{S}$$

solving Problem 2.1; even if any subset of $\mathcal{S}$ does not solve Problem 2.1 for some odd $h = 15t$ (mainly h is of the form $4^{2m} - 1$), that is, none of the elements of $\mathcal{S}$ is a judge of $M_{h,n,-}$ (respectively $M_{h,n,+}$) for some n, then n would be very large. For this reason, we call $\mathcal{S}$ a *universal sequence of judges*. Brief conclusions are given in Section 6. Comparisons with Bosma's approach for the case $h \equiv 0 \bmod 3$ are given in relative sections, see Remarks 3.1, 4.1, 5.5 and 5.7.

3. PROOF OF THEOREM 2

To prove Theorem 2 we need two lemmas.

https://doi.org/10.1017/S0004972700040478 Published online by Cambridge University Press

LEMMA 3.1. ([1, Corollary 5]) *Let p be an odd prime and let $\pi \in \mathbb{Z}[i]$ be primary irreducible. Then*

$$\left(\frac{p^*}{\pi}\right)_4 \equiv (\pi/\overline{\pi})^{(p^*-1)/4} \mod p.$$

LEMMA 3.2. ([1, Lemma 7]) *Let p be an odd prime and let $\alpha \in \mathbb{Z}[i]$ be prime to p. Set $\gamma = \alpha/\overline{\alpha}$. Let $\{w_k\}$ be the Lucas sequence with seed $w_0 = \mathrm{Tr}(\gamma) = \alpha/\overline{\alpha} + \overline{\alpha}/\alpha$. Suppose that, for some j, $w_j \equiv 0 \mod p$. Then $p \equiv \pm 1 \mod 2^{j+2}$.*

PROOF: [Proof of Theorem 2] ($\Longrightarrow$) Suppose that M is a prime and $(M^*/\pi)_4 \neq 0, 1$. Then $(M^*/\pi)_4 = -1, \pm i$. By Lemma 3.1,

$$\left(\frac{M^*}{\pi}\right)_4 \equiv (\pi/\overline{\pi})^{(M^*-1)/4} \mod M.$$

If $(M^*/\pi)_4 = -1$, then $(\pi/\overline{\pi})^{(M^*-1)/4} \equiv -1 \mod M$. Thus

$$w_{n-2} = (\pi/\overline{\pi})^{h\cdot 2^{n-2}} + (\overline{\pi}/\pi)^{h\cdot 2^{n-2}} \equiv -2 \mod M.$$

Therefore $w_{n-3} \equiv 0 \mod M$ follows from the recurrence satisfied be the w_j.

If $(M^*/\pi)_4 = \pm i$, Then $(\pi/\overline{\pi})^{(M^*-1)/4} \equiv \pm i \mod M$. Thus

$$w_{n-2} = (\pi/\overline{\pi})^{h\cdot 2^{n-2}} + (\overline{\pi}/\pi)^{h\cdot 2^{n-2}} \equiv 0 \mod M.$$

($\Longleftarrow$) Let p be a prime divisor of M. Since $w_{n-3} \equiv 0 \mod M$ or $w_{n-2} \equiv 0 \mod M$, we have, by Lemma 3.2,

$$p \equiv \pm 1 \mod 2^{n-1} \text{ or } p \equiv \pm 1 \mod 2^n.$$

Then we have $p \geqslant 2^{n-1} - 1$ and $p^2 \geqslant 2^{2n-2} - 2^n + 1$. Since

$$M = h \cdot 2^n \pm 1 \leqslant h \cdot 2^n + 1$$

and $h < 2^{n-2} - 1$,

$$M < 2^{2n-2} - 2^n + 1 < p^2.$$

Thus $p > \sqrt{M}$. Therefore M is a prime. □

In our generalised test (Theorem 2) we need to check efficiently whether $(M^*_{h,n}/\pi)_4 \in \{1, -1\}$, hence we use the following Lemma 3.3 and its corollary.

LEMMA 3.3. [12, Lemma 2.5] *Let $\pi = u + vi$ be primary irreducible with prime $q = N(\pi) \equiv 1 \mod 4$ and $\alpha = c + di$. If $(\alpha/\pi)_4 \in \{1, -1\}$, then we have*

$$\left(\frac{\alpha}{\pi}\right)_4 \equiv (c - duv^{-1})^{(q-1)/4} \mod q.$$

NOTE. The condition " If $(\alpha/\pi)_4 \in \{1, -1\}$" was missed out in [12, Lemma 2.5] by the author with carelessness while typing. Fortunately, the misprint does not influence any results of [12]).

https://doi.org/10.1017/S0004972700040478 Published online by Cambridge University Press

COROLLARY 3.1. *Let $\pi = u + vi$ be primary irreducible with prime $q = \pi\overline{\pi}$ $= u^2 + v^2 \equiv 1 \mod 4$. If $(M^*_{h,n}/\pi)_4 \in \{1, -1\}$, then we have*

$$\left(\frac{M^*_{h,n,-}}{\pi}\right)_4 \equiv (-h_0 \cdot 2^{n_0} + 1)^{(q-1)/4} \mod q;$$
$$\left(\frac{M^*_{h,n,+}}{\pi}\right)_4 \equiv (h_0 \cdot 2^{n_0} + 1)^{(q-1)/4} \mod q,$$

where $h_0 = h \mod q$ and $n_0 = n \mod \operatorname{ord}_q(2)$.

EXAMPLE 3.1. Let $N_n = 85575 \cdot 2^n - 1$ with $n \geqslant 19$. Then

$$\left(\frac{N^*_n}{\pi_{13}}\right)_4 = 1 \Longleftrightarrow N_n^3 \equiv -1 \mod 13 \Longleftrightarrow n \equiv 1, 11 \mod 12;$$

and

$$\left(\frac{N^*_n}{\pi_{17}}\right)_4 = 1 \Longleftrightarrow N_n^4 \equiv 1 \mod 17 \Longleftrightarrow n \equiv 0, 2 \mod 8.$$

Since the system of congruences

$$\begin{cases} n \equiv 1, 11 \mod 12, \\ n \equiv 0, 2 \mod 8 \end{cases}$$

has no solutions, 13 is a judge of N_n for $n \equiv 0, 2, 3, 4, 5, 6, 7, 8, 9, 10 \mod 12$ and 17 is a judge of N_n for $n \equiv 1, 11 \bmod 12$. This means that $\mathcal{W}_h^- = \{13, 17\}$ solves Problem 2.1 for $h = 85575 = 15 \cdot 5705$. Let $\{w_k\}$ be the Lucas sequence with seed

$$w_0 = (\pi_{13}/\overline{\pi_{13}})^{85575} + (\overline{\pi_{13}}/\pi_{13})^{85575}$$

where $\pi_{13} = 3 + 2i$, and Let $\{w'_k\}$ be the Lucas sequence with seed

$$w'_0 = (\pi_{17}/\overline{\pi_{17}})^{85575} + (\overline{\pi_{17}}/\pi_{17})^{85575}$$

where $\pi_{17} = 1 + 4i$. Since

$$\left(\frac{N^*_n}{\pi_{13}}\right)_4 = \begin{cases} \pm i \Longleftrightarrow n \equiv 0, 3, 7, 8, 9, 10 \bmod 12, \\ -1 \Longleftrightarrow n \equiv 2, 5, 6 \bmod 12, \end{cases}$$

and

$$\left(\frac{N^*_n}{\pi_{17}}\right)_4 = \begin{cases} \pm i \Longleftrightarrow n \equiv 1, 5, 6, 7 \bmod 8, \\ -1 \Longleftrightarrow n \equiv 3, 4 \bmod 8, \end{cases}$$

we have by Theorem 2, N_n is prime $\Longleftrightarrow$

$$\begin{cases} w_{n-2} \equiv 0 \mod N_n, & \text{when } n \equiv 0, 3, 7, 8, 9, 10 \bmod 12; \\ w_{n-3} \equiv 0 \mod N_n, & \text{when } n \equiv 2, 5, 6 \bmod 12; \\ w'_{n-2} \equiv 0 \mod N_n, & \text{when } n \equiv 1, 13, 23 \bmod 24; \\ w'_{n-3} \equiv 0 \mod N_n, & \text{when } n \equiv 11 \bmod 24. \end{cases}$$

https://doi.org/10.1017/S0004972700040478 Published online by Cambridge University Press

Note that, the case $n \equiv 4 \bmod 12$ needs not be tested, since in this case N_n is a multiple of 13. In this way, we find that

N_n $(19 \leqslant n \leqslant 1750)$ is prime $\Longleftrightarrow$

$$n \in \{20, 24, 26, 30, 36, 42, 49, 55, 60, 7072, 79, 85, 90, 138, 175, 209, 230, 254, 309, 344, 373, 395, 406, 479, 725, 994, 1027, 1367, 1638, 1750\}.$$

REMARK 3.1. For testing primality of the numbers $85575 \cdot 2^n - 1$, Bosma [2, Supplement Table 6] used a modulus ('period') $r^- = 401148$, which is much larger than our modulus 24.

REMARK 3.2. If $(M^*/\pi)_4 = 0$ then either $M = q$ is a prime or M is a multiple of q. So, this trivial case is not mentioned in Theorem 2.

REMARK 3.3. If the prime q in Theorem 2 is 5, then $\pi = \pi_5 = -1 + 2i$. Since

$$\left(\frac{M^*}{\pi}\right)_4 = 1 \Longleftrightarrow h \equiv 0 \mod 5,$$

Theorem 2 includes Theorem 1 as a special case and $f_h^- = f_h^+ = 5$ for all odd $h \not\equiv 0 \bmod 5$, or in other words, the prime $5 = \pi\overline{\pi}$ is a judge of $M_{h,n}$ for all odd $h \not\equiv 0 \bmod 5$ and for any $n \geqslant 4$ with $h < 2^{n-2} - 1$.

4. FLAGS OF SOME ODD $h = 15t < 10^8$

Let

$$\mathcal{P} = \{\text{prime } p \equiv 1 \bmod 4 : \ 13 \leqslant p < 2600, \ \operatorname{ord}_p(2) < 350\}. \tag{4.1}$$

Then

$$\mathcal{P} = \{13, 17, 29, \ldots, 2441, 2593\}$$

with $\#\mathcal{P} = 83$.

In this section we determine the subset $\mathcal{F}$ of $\mathcal{P}$:

$$\mathcal{F} = \{q \in \mathcal{P} : q \text{ is a minus or plus flag of some odd } h = 15t < 10^8\} \tag{4.2}$$

For this purpose we need the following lemma, the validity of the lemma is obvious.

LEMMA 4.1. *Let prime q be a judge of $M_{h,n}$. If (2.1) or (2.2) holds, then q is a judge of $M_{h',n'}$ for all $n' \equiv n \bmod \operatorname{ord}_q(2)$ and for all odd $h' \equiv h \mod 2^{\operatorname{ord}_q(2)} - 1$. If (2.3) holds, then q is a judge of $M_{h',n'}$ for all $n' \equiv n \bmod 2\operatorname{ord}_q(2)$ and for all odd $h' \equiv h \bmod 2^{2\operatorname{ord}_q(2)} - 1$.*

A Pascal (Delphi) program based on Corollary 3.1 and Lemma 4.1 ran about five hours on a PC Pentium III/800 to get the set $\mathcal{F}$, which has 16 elements q tabulated in Table 1, where

$$count_q^- = \#\{\text{odd } h = 15t < 10^8 : f_h^- = q\},$$
$$count_q^+ = \#\{\text{odd } h = 15t < 10^8 : f_h^+ = q\},$$

https://doi.org/10.1017/S0004972700040478 Published online by Cambridge University Press

$h^-_{q,1}$ (respectively, $h^-_{q,count^-_q}$) is the smallest (respectively, largest) odd $h = 15t < 10^8$ with $f^-_h = q$, $h^+_{q,1}$ (respectively, $h^+_{q,count^+_q}$) is the smallest (respectively, largest) odd $h = 15t < 10^8$ with $f^+_h = q$.

Out of the 3333333 odd $h = 15t < 10^8$, there are $\sum count^-_q = 298217$ (about 8.9465%) having minus flags $\in \mathcal{P}$, and $\sum count^+_q = 298237$ (about 8.9471%) having plus flags $\in \mathcal{P}$.

Table 1: Flags q of some odd $h = 15t < 10^8$

q	$\mathrm{ord}_q(2)$	$count^-_q$	$h^-_{q,1}$	$h^-_{q,count^-_q}$	$count^+_q$	$h^+_{q,1}$	$h^+_{q,count^+_q}$
13	12	429	296445	99814005	429	97725	99976455
37	36	1	37618935	37618935	2	23920125	35856285
61	60	5	22464495	91298505	2	31243005	69729105
73	9	234749	435	99999915	234772	75	99999765
89	11	16648	915	99994785	16660	1425	99998865
97	48	10	5180865	98908755	12	6806145	93972315
109	36	2669	49485	99986685	2673	123465	99978525
241	24	6755	29775	99990405	6740	9315	99992625
257	16	11237	10845	99988575	11237	5805	99994485
337	21	25323	2115	99991725	25328	1545	99999555
433	72	54	184335	99835275	51	313095	97758825
601	25	5	9546795	90708885	5	45931785	98768385
673	48	14	6821445	96863265	18	11217825	94337745
1321	60	60	1196325	96400515	44	2701305	98938545
1801	25	42	2327775	95816385	46	220905	99560745
2089	29	216	106485	99854865	218	133335	99926535

EXAMPLE 4.1. Let $N_n = 296445 \cdot 2^n - 1$ with $n \geqslant 21$. Then

$$\left(\frac{N^*_n}{\pi_{13}}\right)_4 = 1 \Longleftrightarrow N^3_n \equiv -1 \mod 13 \Longleftrightarrow n \equiv 2, 4 \mod 12.$$

Note that $\mathrm{ord}_{13}(2) = 12$. We have

$$\begin{cases} \gcd(N_n, 2^{12} - 1) = 7 & \text{for } n \equiv 2 \bmod 12, \\ \gcd(N_n, 2^{12} + 1) = 17 & \text{for } n \equiv 4 \bmod 24, \\ \gcd(N_n, 2^{12} + 1) = 241 & \text{for } n \equiv 16 \bmod 24. \end{cases}$$

So, 13 is a minus flag of 296445 and thus $f^-_{296445} = 13$. Let $\{w_k\}$ be the Lucas sequence with seed

$$w_0 = (\pi/\overline{\pi})^{296445} + (\overline{\pi}/\pi)^{296445}$$

https://doi.org/10.1017/S0004972700040478 Published online by Cambridge University Press

where $\pi = \pi_{13} = 3 + 2i$. Since

$$\left(\frac{N_n^*}{\pi}\right)_4 = \begin{cases} \pm i \iff n \equiv 0, 1, 3, 6, 10, 11 \bmod 12, \\ -1 \iff n \equiv 5, 8, 9 \bmod 12, \end{cases}$$

we have by Theorem 2,

$$N_n \text{ is prime} \iff \begin{cases} w_{n-2} \equiv 0 \mod N_n, & \text{when } n \equiv 0, 1, 3, 6, 10, 11 \bmod 12; \\ w_{n-3} \equiv 0 \mod N_n, & \text{when } n \equiv 5, 8, 9 \bmod 12. \end{cases}$$

Note that, if $n \equiv 7 \bmod 12$, then $N_n \equiv 0 \bmod 13$. In this way, we find that

N_n $(21 \leqslant n \leqslant 1750)$ is prime $\iff$

$$n \in \{22, 34, 39, 73, 78, 165, 207, 333, 334, 423, 613, 798, 813, 819, 874\}.$$

EXAMPLE 4.2. Let $N_n = 97725 \cdot 2^n + 1$ with $n \geqslant 19$. Then

$$\left(\frac{N_n^*}{\pi_{13}}\right)_4 = 1 \iff N_n^3 \equiv 1 \mod 13 \iff n \equiv 1, 11 \mod 12.$$

We have

$$\begin{cases} \gcd(N_n, 2^{12} - 1) = 7 & \text{for } n \equiv 11 \bmod 12, \\ \gcd(N_n, 2^{12} + 1) = 241 & \text{for } n \equiv 1 \bmod 24, \\ \gcd(N_n, 2^{12} + 1) = 17 & \text{for } n \equiv 13 \bmod 24. \end{cases}$$

So, 13 is a plus flag of 97725 and thus $f_{97725}^+ = 13$. Let $\{w_k\}$ be the Lucas sequence with seed

$$w_0 = (\pi/\overline{\pi})^{97725} + (\overline{\pi}/\pi)^{97725}$$

where $\pi = \pi_{13} = 3 + 2i$. Since

$$\left(\frac{N_n^*}{\pi}\right)_4 = \begin{cases} \pm i \iff n \equiv 0, 3, 7, 8, 9, 10 \bmod 12, \\ -1 \iff n \equiv 2, 5, 6 \bmod 12, \end{cases}$$

we have by Theorem 2,

$$N_n \text{ is prime} \iff \begin{cases} w_{n-2} \equiv 0 \mod N_n, & \text{when } n \equiv 0, 3, 7, 8, 9, 10 \bmod 12; \\ w_{n-3} \equiv 0 \mod N_n, & \text{when } n \equiv 2, 5, 6 \bmod 12. \end{cases}$$

Note that, if $n \equiv 4 \bmod 12$, then $N_n \equiv 0 \bmod 13$. In this way, we find that

N_n $(19 \leqslant n \leqslant 1750)$ is prime $\iff$

$$n \in \{27, 63, 91, 147, 210, 282, 526, 750, 1051, 1134, 1260, 1476\}.$$

REMARK 4.1. Bosma [2] did not give examples of odd $h = 3t < 10^5$ having "flags" by his approach. We do not know whether there exist odd $h = 3t < 10^5$ having "flags" by Bosma's approach.

https://doi.org/10.1017/S0004972700040478 Published online by Cambridge University Press

5. A UNIVERSAL SEQUENCE OF JUDGES

Let

$$\mathcal{S} = \{q_1, q_2, \dots, q_s\} \tag{5.1}$$

be a finite sequence of different primes $q_j \equiv 1 \bmod 4$,

$$Q = \prod_{q \in \mathcal{S}} q, \quad \text{and let} \quad \mathcal{G}_Q = \mathbb{Z}_Q^* \tag{5.2}$$

be the multiplicative group of invertible elements modulo Q. Then

$$\#\mathcal{G}_Q = \prod_{q \in \mathcal{S}} (q-1).$$

Let $\mathcal{H}_Q = \langle 2 \rangle$ be the cyclic subgroup generated by 2 of $\mathcal{G}_Q$. It is clear that if the system of equations

$$\left(\frac{M^*_{15t,n}}{\pi_{q_1}}\right)_4 = \left(\frac{M^*_{15t,n}}{\pi_{q_2}}\right)_4 = \cdots = \left(\frac{M^*_{15t,n}}{\pi_{q_s}}\right)_4 = 1 \tag{5.3}$$

has solutions in n for a given odd $t = t_0$, then it has solutions in n for all odd $t \in t_0\mathcal{H}_Q$, or in other words, for all odd

$$t \equiv t_0 \cdot 2^m \bmod Q \text{ with } m \geqslant 0.$$

Thus we have proved the following lemma concerning the structure of the quotient group $\mathcal{G}_Q/\mathcal{H}_Q$.

LEMMA 5.1. *The quotient group*

$$\mathcal{G}_Q/\mathcal{H}_Q = \{\bar{t} : t \in \mathcal{G}_Q\} = \mathcal{U}_Q^- \cup \mathcal{V}_Q^- = \mathcal{U}_Q^+ \cup \mathcal{V}_Q^+, \tag{5.4}$$

where

$$\begin{cases} \mathcal{U}_Q^- = \{\bar{t} : \text{(5.3) has solutions in } n \text{ for } M_{15t,n,-}\}, \\ \mathcal{V}_Q^- = \{\bar{t} : \text{(5.3) has no solutions in } n \text{ for } M_{15t,n,-}\}, \end{cases} \tag{5.5}$$

and

$$\begin{cases} \mathcal{U}_Q^+ = \{\bar{t} : \text{(5.3) has solutions in } n \text{ for } M_{15t,n,+}\}, \\ \mathcal{V}_Q^+ = \{\bar{t} : \text{(5.3) has no solutions in } n \text{ for } M_{15t,n,+}\}. \end{cases} \tag{5.6}$$

Moreover, both maps

$$\mathcal{U}_Q^- \to \mathcal{U}_Q^+;\ \bar{t} \mapsto \overline{Q-t}$$

and

$$\mathcal{V}_Q^- \to \mathcal{V}_Q^+;\ \bar{t} \mapsto \overline{Q-t}$$

are bijective. Thus

$$\#\mathcal{U}_Q^- = \#\mathcal{U}_Q^+;\ \#\mathcal{V}_Q^- = \#\mathcal{V}_Q^+.$$

https://doi.org/10.1017/S0004972700040478 Published online by Cambridge University Press

Put

$$u = \#\mathcal{U}_Q^- = \#\mathcal{U}_Q^+ \text{ and } v = \#\mathcal{V}_Q^- = \#\mathcal{V}_Q^+. \tag{5.7}$$

Define

$$\tau_Q = \frac{v}{u+v}, \tag{5.8}$$

$$\mathcal{A}^-(h,\mathcal{S}) = \big\{n : 0 \leqslant n < 2L, (2.4) \text{ holds for all } q \in \mathcal{S} \text{ with } M_{h,n} = M_{h,n,-}\big\},$$

$$\mathcal{A}^+(h,\mathcal{S}) = \big\{n : 0 \leqslant n < 2L, (2.4) \text{ holds for all } q \in \mathcal{S} \text{ with } M_{h,n} = M_{h,n,+}\big\}, \tag{5.9}$$

where

$$L = \mathrm{Lcm}\big(\mathrm{ord}_{q_1}(2), \mathrm{ord}_{q_2}(2), \ldots, \mathrm{ord}_{q_s}(2)\big) = \#\mathcal{H}_Q. \tag{5.10}$$

If $\mathcal{A}^-(h,\mathcal{S}) \neq \emptyset$ or $\mathcal{A}^+(h,\mathcal{S}) \neq \emptyset$, define

$$\begin{aligned} g^-(h,\mathcal{S}) &= \min\big\{n > 0 : n \in \mathcal{A}^-(h,\mathcal{S})\big\}, \\ g^+(h,\mathcal{S}) &= \min\big\{n > 0 : n \in \mathcal{A}^+(h,\mathcal{S}), M_{h,n,+} \text{ is not a perfect square}\big\}. \end{aligned} \tag{5.11}$$

We call τ_Q the *impact factor* of Q or of $\mathcal{S}$. We hope that $\mathcal{S}$ has impact factor close to 1 and has as few elements as possible. If $\mathcal{A}^+(h,\mathcal{S}) \neq \emptyset$ (respectively, $\mathcal{A}^-(h,\mathcal{S}) \neq \emptyset$) for some odd $h = 15t$, we also hope that $g^+(h,\mathcal{S})$ (respectively $g^-(h,\mathcal{S})$) is rather large.

Let $\mathcal{P}$ be as defined by (4.1) and let

$$\mathcal{S}' = \big\{q \in \mathcal{P} : \exists\, p\,(\neq q) \in \mathcal{P} \text{ such that } \tau_{pq} > 0\big\}. \tag{5.12}$$

For determining the set $\mathcal{S}'$ we need a procedure described in §5.1 to find τ_{pq} for given $p, q \in \mathcal{P}$. We find that $\#\mathcal{S}' = 48$ and that $\tau_{13\cdot17} = 0.5 > \tau_{pq}$ for all $p, q \in \mathcal{P}$ with $\{p,q\} \neq \{13,17\}$. In §5.2, we sort the elements in the set $\mathcal{S}'$ to obtain a universal sequence (5.1) with $q_1 = 13$ and $q_2 = 17$, mainly based on the condition

$$\tau_{13\cdot17\cdot q_j} \geqslant \tau_{13\cdot17\cdot q_{j+1}} \text{ for } j \geqslant 3, \tag{5.13}$$

adjusted partially by τ_{pq} for some $p, q \in \mathcal{S}'$. In §5.3, we show how the universal sequence $\mathcal{S}$ works well for our generalised test.

REMARK 5.1. Note that, the definitions of $\mathcal{U}_Q^{-/+}$ and $\mathcal{V}_Q^{-/+}$ (see (5.5) and (5.6)) do not involve the gcd condition in (2.4). Since otherwise, the quotient group structure (5.4) would not be valid. But in practical implementation of our generalised test, the gcd checking makes things speed up. See Remark 5.2 below.

REMARK 5.2. It is clear that, if $\bar{t} \in \mathcal{V}_Q^-$, then $\mathcal{W}_{15t}^- = \mathcal{S}$ solves Problem 2.1. On the other hand, if $\bar{t} \in \mathcal{U}_Q^-$, then system (5.3) has solutions in n for this t. Suppose $n = n_0$ is one of the solutions. If there is some $q \in S$ such that (2.2) or (2.3) holds for $n = n_0$, then $M_{15t,n,-}$ is composite for all $n \equiv n_0 \bmod \mathrm{ord}_q(2)$ or for all $n \equiv n_0 \bmod 2\mathrm{ord}_q(2)$; otherwise if (2.4) holds for all $q \in \mathcal{S}$, then no subsets of $\mathcal{S}$ solve Problem 2.1 for $h = 15t$, $\bar{t} \in \mathcal{U}_Q^-$, thus for testing primality of $M_{15t,n_0,-}$, one should look for a judge outside the sequence $\mathcal{S}$. Corresponding words can be said for the case $M_{15t,n,+}$.

https://doi.org/10.1017/S0004972700040478 Published online by Cambridge University Press

EXAMPLE 5.1. Note that $\operatorname{ord}_{13}(2) = 12$, $\operatorname{ord}_{17}(2) = 8$ and $13 \cdot 17 = 221$. We have

$$\#\mathcal{G}_{221} = (13-1)\cdot(17-1) = 192,\ L = \#\mathcal{H}_{221} = \operatorname{Lcm}\big(\operatorname{ord}_{13}(2), \operatorname{ord}_{17}(2)\big) = 24,$$
$$\mathcal{U}_{221} = \{\overline{1}, \overline{5}, \overline{23}, \overline{55}\},\ \mathcal{V}_{221} = \{\overline{3}, \overline{9}, \overline{11}, \overline{25}\},\ \text{ and } \tau_{221} = \frac{4}{4+4} = 0.5.$$

If $\bar{t} \in \mathcal{V}_{221}$, then $\mathcal{W}_{15t}^{-} = \{13, 17\}$ solves Problem 2.1 for $h = 15t$. Since $3 \cdot 2^{15} \equiv 5705 \bmod 221$, $\overline{5705} = \overline{3} \in \mathcal{V}_{221}$, thus $\mathcal{W}_h^{-} = \{13, 17\}$ solves Problem 2.1 for $h = 15 \cdot 5705 = 85575$, see Example 3.1.

5.1. DETERMINING THE SET $\mathcal{S}'$

Given primes $p, q \equiv 1 \bmod 4$, let

$$m_0 = \#G_{pq} = (p-1)(q-1),\ m_1 = \operatorname{Lcm}\big(\operatorname{ord}_p(2), \operatorname{ord}_q(2)\big), \tag{5.14}$$
$$r = \#\{\text{prime } q' \equiv 1 \bmod 4 : 5 < q' < q,\ \#\mathcal{V}_{q'q} > 0\}, \tag{5.15}$$

and let p_0 be a prime $\equiv 1 \bmod 4$ with impact factor $\tau_{p_0q} \geqslant \tau_{q'q}$ for all $5 < q' < q$.

We use the following Procedure 5.1 to find τ_{pq} and use Procedure 5.2 to determine the set $\mathcal{S}'$.

Procedure 5.1. Finding τ_{pq};

{input primes $p, q \equiv 1 \bmod 4$ with $p \neq q$; }

{output u and v as defined by (5.7) with $Q = pq$, thus $\tau_{pq} = v/(u+v)$;}

{output also r, m_0, m_1 as defined by (5.14) and (5.15)}

Begin $m_0 \leftarrow (p-1)\cdot(q-1)$; $d \leftarrow \gcd\big(\operatorname{ord}_p(2), \operatorname{ord}_q(2)\big)$;

$m_1 \leftarrow \operatorname{Lcm}\big(\operatorname{ord}_p(2), \operatorname{ord}_q(2)\big)$;

For $t := 1$ **To** pq **Do**

If $(t \equiv 0 \bmod p)$ **Or** $(t \equiv 0 \bmod q)$ **Then** $T_t \leftarrow True$ **Else** $T_t \leftarrow False$;

$u \leftarrow 0$; $t \leftarrow 1$;

Repeat $h \leftarrow t \cdot 15$;

Using Corollary 3.1 to find solutions in n of $(M^*_{h,n,-}/\pi_p)_4 = 1$ by trial and error;

(Suppose k solutions $n = n_{11}, \ldots, n_{1k} \bmod \operatorname{ord}_p(2)$ are found)

Using Corollary 3.1 to find solutions in n of $(M^*_{h,n,-}/\pi_q)_4 = 1$ by trial and error;

(Suppose l solutions $n = n_{21}, \ldots, n_{2l} \bmod \operatorname{ord}_q(2)$ are found)

$j \leftarrow 0$; *morejudge* $\leftarrow False$;

repeat $j \leftarrow j + 1$; $i \leftarrow 0$;

Repeat $i \leftarrow i + 1$;

If $(n_{2j} - n_{1i}) \equiv 0 \bmod d$ **Then** *morejudge* $\leftarrow True$

Until *morejudge* or $(i = k)$

until *morejudge* or $(j = l)$;

If *morejudge* **Then**

begin $x \leftarrow t$; $u \leftarrow u + 1$; $T_x \leftarrow True$; $i \leftarrow 0$;

https://doi.org/10.1017/S0004972700040478 Published online by Cambridge University Press

repeat $x \leftarrow x + x$; **If** $x \geqslant pq$ **Then** $x \leftarrow x - pq$; $T_x \leftarrow True$; $i \leftarrow i + 1$
until $i = m_1$
end;
repeat $t \leftarrow t + 2$ **until** (not T_t) **Or** $(t = pq)$
Until $t = pq$;
$v \leftarrow 0$; $t \leftarrow 0$;
Repeat repeat $t \leftarrow t + 1$ **until** (not T_t) or $(t = pq)$;
If (t is odd) **And** (not T_t) **Then**
begin $x \leftarrow t$; $v \leftarrow v + 1$; $T_x \leftarrow True$; $i \leftarrow 0$;
repeat $x := x + x$; **If** $x \geqslant pq$ **Then** $x \leftarrow x - pq$; $T_x \leftarrow True$; $i \leftarrow i + 1$
until $i = m_1$
end
Until $t = pq$;
$\tau_{pq} \leftarrow v/(u + v)$
End;

Procedure 5.2. Determining the set $\mathcal{S}'$;
{Input the set $\mathcal{P} = \{p_1, \ldots, p_{83}\}$ as defined by (4.1); }
{Output the set $\mathcal{S}'$ as defined by (5.12)}

Begin Let $\mathcal{S}'$ be an empty set; $j \leftarrow 1$;
Repeat $j \leftarrow j + 1$; $q \leftarrow p_j$; $i \leftarrow 0$; $max\tau \leftarrow 0$; $r \leftarrow 0$;
repeat $i \leftarrow i + 1$; $p \leftarrow p_i$;
If $\tau_{pq} > 0$ **Then begin** $r \leftarrow r + 1$; $\mathcal{S}' \leftarrow \mathcal{S}' \cup \{p\}$ **end**;
If $\tau_{pq} > max\tau$ **Then begin** $max\tau \leftarrow \tau_{pq}$; $p_0 \leftarrow p$ **end**
until $i = j - 1$;
If $r > 0$ **Then**
begin $\mathcal{S}' \leftarrow \mathcal{S}' \cup \{q\}$;
output (q, r, p_0) and related values $(m_0, m_1, u, v, \tau_{qp_0})$
(which are found by Procedure 5.1 for finding τ_{qp_0})
end
Until $j = 83$
End.

The Pascal (Delphi) program ran about 3 hours on a PC Pentium III/800 to get 48 elements

https://doi.org/10.1017/S0004972700040478 Published online by Cambridge University Press

of the set $\mathcal{S}'$ with related values tabulated in Table 2. Thus

$$\begin{aligned}\mathcal{S}' =&\{\text{primes } q \text{ in the first column of Table 2}\}\\ &\cup\{\text{primes } p_0 \text{ in the third column of Table 2}\}\\ &\cup\{\text{primes } p \text{ in the last column of Table 2}\}\\ =&\{13,17,29,37,41,53,61,73,89,97,101,109,113,137,157,193,229,233,241,\\ &257,277,337,349,353,397,401,433,457,577,593,601,641,673,881,937,\\ &953,1013,1217,1249,1321,1429,1613,1657,1777,1801,2089,2113,2593\}.\end{aligned}$$

Note that all elements q of the set $\mathcal{F}$ (tabulated in Table 1) are contained in $\mathcal{S}'$.

REMARK 5.3. By (5.4), if $(u+v)\cdot m_1 \neq m_0$ in the outputs of Procedure 5.1, then there must be some errors in the programming.

5.2. DETERMINING THE SEQUENCE $\mathcal{S}$ Without much modification to Procedure 5.1, we have a procedure for computing $\tau_{13\cdot17\cdot q}$ for $q \in \mathcal{S}'\backslash\{13,17\}$. We sort elements of $\mathcal{S}'$ mainly based on (5.13), adjusted partially by τ_{pq} for some $p,q \in \mathcal{S}'$, to obtain the sequence $\mathcal{S}$ tabulated in Table 3 with related values:

$$\begin{aligned}\text{ord} = \text{ord}_q(2),\ m_0 = \#G_{13\cdot17\cdot q} = \phi(13\cdot17\cdot q) = 192(q-1),\\ m_1 = \text{Lcm}\big(\text{ord}_{13}(2),\text{ord}_{17}(2),\text{ord}_q(2)\big) = \text{Lcm}\big(24,\text{ord}_q(2)\big),\end{aligned}$$

u and v are defined by (5.7) with $Q = 13\cdot17\cdot q$, thus $\tau_Q = v/(u+v)$.

5.3. EFFECT OF THE UNIVERSAL SEQUENCE $\mathcal{S}$ Let

$$\mathcal{S}_j = \{q_1, q_2, \ldots, q_j\}$$

be sub-sequences of the first j elements of $\mathcal{S}$. Define

$$\begin{aligned}y_j^- = \#\big\{&\text{odd } h = 15t < 10^8 : j \text{ is the smallest subscript}\\ &\text{such that } \mathcal{W}_h^- = \mathcal{S}_j \text{ solves Problem 2.1}\big\},\end{aligned}$$

$$\begin{aligned}y_j^+ = \#\big\{&\text{odd } h = 15t < 10^8 : j \text{ is the smallest subscript}\\ &\text{such that } \mathcal{W}_h^+ = \mathcal{S}_j \text{ solves Problem 2.1}\big\},\end{aligned}$$

$$Y_j^- = \sum_{k=1}^{j} y_k^-, \quad \text{and} \quad Y_j^+ = \sum_{k=1}^{j} y_k^+.$$

Let $\mathcal{A}^-(h,\mathcal{S})$, $\mathcal{A}^+(h,\mathcal{S})$, $g^-(h,\mathcal{S})$ and $g^+(h,\mathcal{S})$ be as defined by (5.9) and (5.11) with

$$L = \text{Lcm}\big(\text{ord}_{q_1}(2),\text{ord}_{q_2}(2),\ldots,\text{ord}_{q_{48}}(2)\big) = 1034115765883200.$$

We use the following Procedure 5.3 to find, for each odd $h = 15t < 10^8$, the smallest j such that $\mathcal{W}_h = \mathcal{S}_j$ solves Problem 2.1 and use Procedure 5.4 to find values of functions y_j and Y_j, where $\mathcal{W}_h$ means either $\mathcal{W}_h^-$ or $\mathcal{W}_h^+$, y_j means either y_j^- or y_j^+, and Y_j means either Y_j^- or Y_j^+.

https://doi.org/10.1017/S0004972700040478 Published online by Cambridge University Press

Procedure 5.3. Finding the smallest j such that $\mathcal{W}_h = \mathcal{S}_j$ solves Problem 2.1;
{input odd $h = 15t < 10^8$ and the universal sequence $\mathcal{S} = \{q_1, \ldots, q_{48}\}$}
{output $1 \leqslant j \leqslant 48$ such that $\mathcal{W}_h = \mathcal{S}_j$ solves Problem 2.1}
{if $\mathcal{W}_h = \mathcal{S}_{48} = \mathcal{S}$ does not solve Problem 2.1, then output $g(h, S)$}
Begin $j \leftarrow 0$;
Repeat $j \leftarrow j + 1$; Using Corollary 3.1 and Lemma 4.1 to find solutions in n mod $2\text{ord}_q(2)$ of (2.4) for $q = q_j$;
If no solutions are found **Then**
begin output j and the message "$q = q_j$ is a minus (plus) flag of h"; exit **end**;
Using the Chinese Remainder Theorem to find common solutions in n of the system (2.4) for all $q \in \mathcal{S}_j$;
Saving all solutions mod $2\,\text{Lcm}\,\text{ord}_{q_1}, \ldots, \text{ord}_{q_j})$ in an array if they exist
Until $(j = 48)$ **Or** (no common solutions for all $q \in \mathcal{S}_j$ exist);
Output j;
If $\mathcal{W}_h = \mathcal{S}_{48} = \mathcal{S}$ does not solve Problem 2.1 **Then** output $g(h, S)$
End;

Procedure 5.4. Finding values of functions y_j and Y_j;
Begin $h \leftarrow 15$; **For** $k := 1$ **To** 48 Do **begin** $y_k \leftarrow 0$; $Y_k \leftarrow 0$ **end**;
Repeat Using Procedure 5.3 to find the smallest j such that $\mathcal{W}_h = \mathcal{S}_j$ solves Problem 2.1 or to find $g(h, S)$;
If the smallest j is found **Then**
begin $y_j \leftarrow y_j + 1$; **For** $k := j$ **To** 48 **Do** $Y_k \leftarrow Y_k + 1$ **end**;
$h \leftarrow h + 30$
Until $h > 10^8$;
For $k := 1$ **To** 48 Do output y_k and Y_k
End.

In Table 4 we tabulate y_j^-, y_j^+, Y_j^-, Y_j^+, $Y_j^-/Total$ and $Y_j^+/Total$ where

$$Total = \#\{\text{odd}\, h = 15t < 10^8\} = 3333333.$$

In Table 5 we tabulate all six odd $h = 15t$, all of them are of the form $h = 4^{2m} - 1$, such that $\mathcal{S}$ has no subsets $\mathcal{W}_h^-$ solving Problem 2.1. In Table 6 we tabulate all 52 odd $h = 15t$ such that $\mathcal{S}$ has no subsets $\mathcal{W}_h^+$ solving Problem 2.1, where $\#\mathcal{A}^+$ means $\#\mathcal{A}^+(h, \mathcal{S})$. From Tables 4-6, one may clearly see the effect of the universal sequence $\mathcal{S}$.

REMARK 5.4. Since six $h = 15t$ tabulated in Table 5 are all of the form $4^{2m} - 1$, it seems that Problem 2.1 has finite solutions $\mathcal{W}_h^-$ for all $h = 15t$ not of the form $4^{2m} - 1$.

https://doi.org/10.1017/S0004972700040478 Published online by Cambridge University Press

Table 2: Primes q and p with $\tau_{pq} > 0$

q	r	p_0	m_0	m_1	u	v	$v/(u+v)$	p other than p_0
17	1	13	192	24	4	4	0.50000	
37	1	13	432	36	9	3	0.25000	
41	2	17	640	40	11	5	0.31250	13
61	1	41	2400	60	38	2	0.05000	
73	2	13	864	36	20	4	0.16666	37
97	2	17	1536	48	27	5	0.15625	13
109	4	13	1296	36	29	7	0.19444	17,37,73
113	2	29	3136	28	97	15	0.13392	17
157	1	53	8112	52	155	1	0.00641	
193	2	17	3072	96	31	1	0.03125	97
241	6	13	2880	24	87	33	0.27500	17,73,97,109,193
257	8	17	4096	16	143	113	0.44140	13,41,97,109,113,193,241
337	5	73	24192	63	357	27	0.07031	13,29,113,241
353	3	17	5632	88	63	1	0.01562	89,257
397	4	89	34848	44	730	62	0.07828	17,257,353
433	6	73	31104	72	406	26	0.06018	17,37,109,241,257
457	3	17	7296	152	47	1	0.02083	229,257
577	3	17	9216	144	63	1	0.01562	241,257
601	1	101	60000	100	594	6	0.01000	
641	3	257	163840	64	2459	101	0.03945	17,97
673	7	17	10752	48	202	22	0.09821	13,97,109,193,241,257
881	2	89	77440	55	1317	91	0.06463	601
937	1	73	67392	117	567	9	0.01562	
953	1	137	129472	68	1887	17	0.00892	
1013	1	277	279312	92	3029	7	0.00230	
1217	2	17	19456	152	127	1	0.00781	257
1321	8	41	52800	60	851	29	0.03295	13,17,61,73,241,257,337
1429	4	13	17136	84	202	2	0.00980	29,113,337
1613	5	157	251472	52	4690	146	0.03019	17,53,257,1249
1657	2	277	457056	92	4956	12	0.00241	1013
1777	1	593	1051392	148	7103	1	0.00014	
1801	6	601	1080000	25	34352	8848	0.20481	41,101,401,881,1321
2089	2	233	484416	29	14035	2669	0.15978	349
2113	6	89	185856	44	3849	375	0.08877	17,257,353,397,881
2593	1	73	186624	81	2258	46	0.01996	

https://doi.org/10.1017/S0004972700040478 Published online by Cambridge University Press

Table 3: The Universal Sequence $\mathcal{S} = \{q_1, q_2, \cdots, q_{48}\}$

j	$q = q_j$	π_q	ord	m_0	m_1	u	v	$\frac{v}{u+v}$
1	13	$3+2i$	12					
2	17	$1+4i$	8					
3	241	$-15+4i$	24	46080	24	330	1590	0.82812
4	97	$9+4i$	48	18432	48	102	282	0.73437
5	257	$1+16i$	16	49152	48	286	738	0.72070
6	673	$-23+12i$	48	129024	48	765	1923	0.71540
7	37	$-1+6i$	36	6912	72	32	64	0.66666
8	109	$3+10i$	36	20736	72	98	190	0.65972
9	41	$5+4i$	20	7680	120	22	42	0.65625
10	73	$-3+8i$	9	13824	72	66	126	0.65625
11	433	$17+12i$	72	82944	72	419	733	0.63628
12	193	$-7+12i$	96	36864	96	146	238	0.61979
13	1321	$5+36i$	60	253440	120	916	1196	0.56628
14	61	$-5+6i$	60	11520	120	42	54	0.56250
15	577	$1+24i$	144	110592	144	337	431	0.56119
16	337	$9+16i$	21	64512	168	178	206	0.53645
17	1429	$23+30i$	84	274176	168	764	868	0.53186
18	113	$-7+8i$	28	21504	168	60	68	0.53125
19	397	$19+6i$	44	76032	264	136	152	0.52777
20	1249	$-15+32i$	156	239616	312	376	392	0.51041
21	353	$17+8i$	88	67584	264	126	130	0.50781
22	2113	$33+32i$	44	405504	264	762	774	0.50390
23	29	$-5+2i$	28	5376	168	16	16	0.50000
24	53	$7+2i$	52	9984	312	16	16	0.50000
25	101	$-1+10i$	100	19200	600	16	16	0.50000
26	157	$11+6i$	52	29952	312	48	48	0.50000
27	233	$13+8i$	29	44544	696	32	32	0.50000
28	277	$-9+14i$	92	52992	552	48	48	0.50000
29	349	$-5+18i$	348	66816	696	48	48	0.50000
30	401	$1+20i$	200	76800	600	64	64	0.50000
31	881	$25+16i$	55	168960	1320	64	64	0.50000
32	937	$-19+24i$	117	179712	936	96	96	0.50000
33	1013	$23+22i$	92	194304	552	176	176	0.50000
34	1657	$-19+36i$	92	317952	552	288	288	0.50000
35	2089	$45+8i$	29	400896	696	288	288	0.50000
36	89	$5+8i$	11	16896	264	32	32	0.50000
37	137	$-11+4i$	68	26112	408	32	32	0.50000
38	229	$15+2i$	76	43776	456	48	48	0.50000
39	457	$21+4i$	76	87552	456	94	98	0.51041
40	593	$-23+8i$	148	113664	888	64	64	0.50000
41	601	$5+24i$	25	115200	600	96	96	0.50000
42	641	$25+4i$	64	122880	192	308	332	0.51875
43	953	$13+28i$	68	182784	408	224	224	0.50000
44	1217	$-31+16i$	152	233472	456	254	258	0.50390
45	1613	$-13+38i$	52	309504	312	494	498	0.50201
46	1777	$-39+16i$	74	340992	888	192	192	0.50000
47	1801	$-35+24i$	25	345600	600	288	288	0.50000
48	2593	$17+48i$	81	497664	648	384	384	0.50000

https://doi.org/10.1017/S0004972700040478 Published online by Cambridge University Press

REMARK 5.5. It is easy to prove that, if $h = 15t$ is of the form $4^{2m} - 1$, then for any finite set of primes $\{q_j\}$, the system (5.3) has solutions in n. It seems that the gcd checking in (2.2) and (2.3) does not help much for h of this form. So, it seems that Problem 2.1 does not have a finite solution $\mathcal{W}_h$ for $h = 15t$ of the form $4^{2m} - 1$. Nevertheless, the determination of values of the functions $g(h, \mathcal{S})$ (see Tables 5 and 6) is a remediation of finite-solution-non-existing for $h = 15t$ of the form $4^{2m} - 1$. However, Bosma's approach for the case $h \equiv 0 \bmod 3$ did not provide such remediation.

REMARK 5.6. Out of the 52 odd $h = 15t$ tabulated in Table 6, there are 46 odd $h = 15t$ not of the form $4^{2m} - 1$. Although Problem 2.1 does not have solutions $\mathcal{W}_h^+ \subseteq \mathcal{S}$ for these 46 odd $h = 15t$, it seems that for all odd $h = 15t$ not of the form $4^{2m} - 1$, Problem 2.1 has finite solutions $\mathcal{W}_h^+$ with additional primes outside $\mathcal{S}$. For examples,

$$\begin{aligned} \mathcal{W}_{76245}^+ &= \{29, 37, 61, 73, 277, 1289, 1657\} \subset \mathcal{S} \cup \{1289\} \subset \mathcal{P}, \\ \mathcal{W}_{794155}^+ &= \{13, 29, 73, 281\} \subset \mathcal{S} \cup \{281\} \subset \mathcal{P}, \\ \mathcal{W}_{1259445}^+ &= \{13, 37, 97, 353, 7393\} \subset \mathcal{S} \cup \{7393\} \subset \mathcal{P} \cup \{7393\}, \\ &\dots \end{aligned}$$

solve Problem 2.1 for corresponding h.

REMARK 5.7. Note that, using (1.8) to test primality of $M_{h,n,-}$ for the case $h \equiv 0 \bmod 3$, one first finds $d \in \mathbb{Z}$ satisfying (1.6), then he finds an algebraic integer α in the quadratic extension $\mathbb{Q}(\sqrt{d})$ satisfying (1.7). Moreover, for determining finite judge set (1.13), Bosma needed the complete factorisations of all integers $2^u - 1$ for $2 \leqslant u \leqslant U = 250$. So, the judge (d, α) in Bosma's approach is not only "two-process finding", but also d may be as large as up to 106 decimal digits. In our generalised test, judges are "one-process finding", which are just some small primes $\equiv 1 \bmod 4$. Moreover we have the universal sequence $\mathcal{S}$ of judges for odd $h = 15t < 10^8$, but Bosma did not provide such a sequence of judges for odd $h = 3t < 10^5$.

REMARK 5.8. Now one may realise that the bound 2600 for p and the bound 350 for $\mathrm{ord}_p(2)$ in the set $\mathcal{P}$ defined by (4.1) are chosen after several trials for obtaining the effective universal sequence $\mathcal{S}$ of judges for odd $h = 15t < 10^8$. One may increase these bounds for $h > 10^8$.

REMARK 5.9. For determining the values of $g^+(h, S)$ defined by (5.11), one needs to check whether $M_{h,n,+}$ is a perfect square. This can be done by Newton's method (see [3, Section 1.7] and [4, Section 9.2.2]) or by Bosma [2, Proposition 4.2].

REMARK 5.10. We call $\mathcal{W}_h$ a minimal set of judges to solve Problem 2.1 for given odd h, if any proper subset of $\mathcal{W}_h$ does not solve Problem 2.1 but $\mathcal{W}_h$ itself solves Problem 2.1. Note that $\mathcal{W}_h$ means either $\mathcal{W}_h^-$ or $\mathcal{W}_h^+$. The subsequence $\mathcal{S}_j$ found by Procedure 5.3 is in general not a minimal set of judges to solve Problem 2.1 for given odd $h = 15t$. One may delete some elements of $\mathcal{S}_j$ to obtain a minimal set $\mathcal{W}_h$. For example, the subsequence $\mathcal{S}_j$ found by Procedure 5.3 for $h = 11897535 = 15 \cdot 793169$ is $\mathcal{W}_h^- = \mathcal{S}_{34}$. But both $\mathcal{W}_h^- = \{277, 1013, 1657\} \subset \mathcal{S}_{34}$ and $\mathcal{W}_h^- = \{229, 277, 457, 593, 1657, 1777\} \subset \mathcal{S}_{46}$ are minimal sets solving Problem 2.1 for $h = 11897535$. So, there may exist several minimal sets (with different cardinalities) of judges to solve Problem 2.1 for given odd h.

https://doi.org/10.1017/S0004972700040478 Published online by Cambridge University Press

Table 4: The functions y_j^-, y_j^+, Y_j^-, Y_j^+, $\frac{Y_j^-}{Total}$ and $\frac{Y_j^+}{Total}$

j	q_j	y_j^-	Y_j^-	$\frac{Y_j^-}{Total}$	y_j^+	Y_j^+	$\frac{Y_j^+}{Total}$
1	13	429	429	0.00012	429	429	0.00012
2	17	1554395	1554824	0.46644	1554395	1554824	0.46644
3	241	1049748	2604572	0.78137	1049752	2604576	0.78137
4	97	384445	2989017	0.89670	384927	2989503	0.89685
5	257	240217	3229234	0.96877	239660	3229163	0.96874
6	673	76507	3305741	0.99172	76503	3305666	0.99169
7	37	11892	3317633	0.99528	12124	3317790	0.99533
8	109	11098	3328731	0.99861	10966	3328756	0.99862
9	41	1823	3330554	0.99916	1776	3330532	0.99915
10	73	2013	3332567	0.99977	1985	3332517	0.99975
11	433	566	3333133	0.99993	497	3333014	0.99990
12	193	95	3333228	0.99996	122	3333136	0.99994
13	1321	60	3333288	0.99998	66	3333202	0.99996
14	61	19	3333307	0.99999	15	3333217	0.99996
15	577	8	3333315	0.99999	5	3333222	0.99996
16	337	0	3333315	0.99999	2	3333224	0.99996
17	1429	7	3333322	0.99999	11	3333235	0.99997
18	113	0	3333322	0.99999	2	3333237	0.99997
19	397	0	3333322	0.99999	1	3333238	0.99997
20	1249	0	3333322	0.99999	2	3333240	0.99997
21	353	1	3333323	0.99999	9	3333249	0.99997
22	2113	1	3333324	0.99999	2	3333251	0.99997
23	29	0	3333324	0.99999	1	3333252	0.99997
24	53	1	3333325	0.99999	5	3333257	0.99997
25	101	0	3333325	0.99999	2	3333259	0.99997
26	157	0	3333325	0.99999	5	3333264	0.99997
27	233	0	3333325	0.99999	0	3333264	0.99997
28	277	0	3333325	0.99999	0	3333264	0.99997
29	349	1	3333326	0.99999	2	3333266	0.99997
30	401	0	3333326	0.99999	1	3333267	0.99998
31	881	0	3333326	0.99999	2	3333269	0.99998
32	937	0	3333326	0.99999	3	3333272	0.99998
33	1013	0	3333326	0.99999	1	3333273	0.99998
34	1657	1	3333327	0.99999	4	3333277	0.99998
35	2089	0	3333327	0.99999	4	3333281	0.99998
36-48	89-2593	0	3333327	0.99999	0	3333281	0.99998

https://doi.org/10.1017/S0004972700040478 Published online by Cambridge University Press

Table 5: All odd $h = 15t < 10^8$ such that $\mathcal{S}$ does not have subsets $\mathcal{W}_h^-$ solving Problem 2.1

t	$h = 15t$	$\#\mathcal{A}^-(h,\mathcal{S})$	$g^-(h,\mathcal{S})$
1	15	128	18632716502396
17	255	32	44961555038392
273	4095	144	2374757985588
4369	65535	12	392017741315184
69905	1048575	96	18295167290380
1118481	16777215	24	124218110015

Table 6: All odd $h = 15t < 10^8$ such that $\mathcal{S}$ does not have subsets $\mathcal{W}_h^+$ solving Problem 2.1

t	$h = 15t$	$\#\mathcal{A}^+$	$g^+(h,\mathcal{S})$	t	$h = 15t$	$\#\mathcal{A}^+$	$g^+(h,\mathcal{S})$
1	15	384	3744810669600	1555421	23331315	240	9316358251204
17	255	80	32874965323200	1620409	24306135	16	208796029041605
273	4095	192	27949074753600	1624207	24363105	96	21416915519980
4369	65535	216	35892230774400	1689743	25346145	72	7934392065984
5083	76245	96	14312086588806	1693839	25407585	72	57450875882388
52941	794115	96	56017284523205	1694095	25411425	48	9322657343992
69905	1048575	128	13517853148800	1694111	25411665	24	101383898615996
83963	1259445	540	1245274430404	1737631	26064465	400	7826125507172
197743	2966145	96	13335179457604	2045407	30681105	20	118007204515176
224927	3373905	128	16007983991976	2053685	30805275	16	419236121304004
234481	3517215	16	157830069196805	2801779	42026685	16	172352627647209
298497	4477455	144	12966968851200	2941299	44119485	144	44977439707204
325039	4875585	30	24573582633588	3093983	46409745	432	4566842279980
346579	5198685	288	1048798951208	3159519	47392785	120	730694764784
546165	8192475	12	46581791256004	3163615	47454225	96	21738169252788
575631	8634465	24	148696384636776	3163871	47458065	60	5884015737592
733907	11008605	96	16897316436005	3163887	47458305	320	5388873890396
807823	12117345	8	225215774783996	3267165	49007475	450	1177930353605
1118481	16777215	16	37586686737600	3398759	50981385	16	27035706297606
1227083	18406245	128	5401061265604	3732271	55984065	72	31697034969604
1273503	19102545	288	7826125507180	4277607	64164105	144	13974537376804
1288007	19320105	72	31054527504007	4472013	67080195	144	6210905500804
1339039	20085585	32	24843622003184	5589327	83839905	32	47034504316772
1343135	20147025	40	87866045467188	5618313	84274695	240	14921556249606
1343391	20150865	96	45189691747192	6275577	94133655	60	3744810669604
1343407	20151105	144	1473987715196	6384911	95773665	16	97416702583176

6. Conclusions

We have presented a Lucasian primality test mainly for numbers of the form $M_{h,n} = h \cdot 2^n \pm 1$ with odd $h = 15t < 2^{n-2} - 1$, which generalises Berrizbeitia and Berry's test for such numbers with $h \not\equiv 0 \bmod 5$. With our generalised test, the primality of such a number $M_{h,n}$ can be proved by means of a Lucas sequence with a seed determined by h and π_q — primary irreducible divisor of a prime $q \equiv 1 \bmod 4$. We call the prime q a judge of the number $M_{h,n}$.

Given an odd h, if the numbers $M_{h,n,-} = h \cdot 2^n - 1$ (respectively, $M_{h,n,+} = h \cdot 2^n + 1$) share a common judge q for all n, we call the judge q a minus (respectively plus) flag of h. We found sixteen primes q which are minus or plus flags of some odd $h = 15t < 10^8$; 298217 (about 8.9465%) out of 3333333 odd $h = 15t < 10^8$ have minus flags, and 298237 (about 8.9471%) odd $h = 15t < 10^8$ have plus flags.

https://doi.org/10.1017/S0004972700040478 Published online by Cambridge University Press

We have also prescribed a sequence $\mathcal{S}$ of 48 primes $\equiv 1 \bmod 4$ in the interval $[13, 2593]$ including the sixteen flags, such that, for 3333327 out of the 3333333 odd $h = 15t < 10^8$ and for all n, each number $M_{h,n,-}$ has a judge q in the first 34 elements of $\mathcal{S}$. For the remaining six h (which are of the form $4^{2m} - 1$) and for all $n < 2.37 \cdot 10^{12}$, each number $M_{h,n,-}$ has a judge q in $\mathcal{S}$. Correspondent words can be said for the numbers $M_{h,n,+} = h \cdot 2^n + 1$. For 3333281 out of the 3333333 odd $h = 15t < 10^8$ and for all n, each number $M_{h,n,+}$ has a judge q in the first 35 elements of $\mathcal{S}$. For the remaining fifty two h and for all $n < 7.3 \cdot 10^{11}$, each number $M_{h,n,+}$ has a judge q in $\mathcal{S}$. The only limitation towards testing primality of numbers $M_{h,n}$ by our generalised test seems to be the difficulty of doing computation involving such numbers as large as

$$4095 \cdot 2^{2374757985588} - 1 \quad \text{or} \quad 47392785 \cdot 2^{730694764784} + 1,$$

much larger than the 43rd Mersenne prime (current largest known prime number)

$$2^{30402457} - 1 \ \text{(9152052 decimal digits)},$$

see http://www.mersenne.org, [**5**, A3], and [**9**, Chapter 5].

References

[1] P. Berrizbeitia and T.G. Berry, 'Biquadratic reciprocity and a Lucasian primality test', *Math. Comp.* **73** (2004), 1559–1564.

[2] W. Bosma, 'Explicit primality criteria for $h \cdot 2^n \pm 1$', *Math. Comp.* **61** (1993), 97–109.

[3] H. Cohen, *A course in computational algebraic number theory*, Graduate Texts in Mathmatics **138** (Springer–Verlag, Berlin, 1996).

[4] R. Crandall and C. Pomerance, *Prime numbers, a computational perspective* (Springer–Verlag, New York, 2005).

[5] R.K. Guy, *Unsolved problems in number theory* (Springer–Verlag, New York, 2004).

[6] K. Ireland and M. Rosen, *A classical introduction to modern number theory*, Graduate Texts in Mathematics **84** (Springer–Verlag, New York, 1990).

[7] D.H. Lehmer, 'On Lucas's test for the primality of Mersenne's number', *J. London Math. Soc.* **10** (1935), 162–165.

[8] E. Lucas, 'Théorie des fonctions numériques simplement périodiques, I. II', *Amer. J. Math.* **1** (1878), 184-239, 289-321.

[9] P. Ribenboim, *The little book of bigger primes* (Springer–Verlag, New York, 2004).

[10] H. Riesel, 'Lucasian criteria for the primality of $N = h \cdot 2^n - 1$', *Math. Comp.* **23** (1969), 869–875.

[11] H. Riesel, *Prime numbers and computer methods for factorization* (Birkhaűser, Boston, 1985).

[12] Z. Zhang, 'Finding strong pseudoprimes to several bases', *Math. Comp.* **70** (2001), 863–872.

Department of Mathematics
Anhui Normal University
Wuhu 241000
Anhui
Peoples Republic of China
e-mail: zhangzhx@mail.wh.ah.cn

Department of Applied Mathematics
Anhui University of Finance & Economics
Bengbu 233041
Anhui
Peoples Republic of China
e-mail: liuxianbei82@163.com

Department of Mathematics
Anqing Teachers College
Anqing 246011
Anhui
Peoples Republic of China
e-mail: pingzi212@163.com

https://doi.org/10.1017/S0004972700040478 Published online by Cambridge University Press