ACTA ARITHMETICA
169.4 (2015)

Primality test for numbers of the form $(2p)^{2^n} + 1$

by

Yingpu Deng and Dandan Huang (Beijing)

1. Introduction. Primality testing is an important problem in computational number theory. Although it was proved to be a **P** problem by Agrawal, Kayal and Saxena [AKS] in 2004, finding more efficient algorithms for specific families of numbers does make sense. In this paper we are concerned with the numbers of the form $a^{2^n} + 1$, with $n \geq 1$, $a \geq 2$, called *generalized Fermat numbers* by Ribenboim [RB]. Our main result is an efficient deterministic polynomial time algorithm for generalized Fermat numbers of the form $M = (2p)^{2^n} + 1$, with p an odd prime.

Let $a \geq 2$ be an integer. Prime numbers of the form $a^n \pm 1$, when a is fixed and $n \geq 1$ varies, have been studied for a long time. For $a^n - 1$, it is easy to see that it suffices to consider the case when $a = 2$ and $n = p$ is a prime. Numbers of the form $2^p - 1$ are called Mersenne numbers. For Mersenne numbers, Lucas [LU] and Lehmer [LE] gave the famous Lucas–Lehmer primality test, using the properties of Lucas sequences. Their test is as follows.

Lucas–Lehmer test. *Let $M_p = 2^p - 1$ be a Mersenne number, where p is an odd prime. Define $u_0 = 4$ and $u_k = u_{k-1}^2 - 2$ for $k \geq 1$. Then M_p is a prime if and only if $u_{p-2} \equiv 0 \pmod{M_p}$.*

For $a^n + 1$, it is clear that it suffices to consider the case when a is even and n is a power of 2, which are exactly the generalized Fermat numbers. When $a = 2$, the numbers of the form $2^{2^n} + 1$ are called *Fermat numbers*. For these, there is also a primality test due to Pépin (see [W2]):

Pépin test. *Let $F_n = 2^{2^n} + 1$ be the nth Fermat number, with $n > 0$. Then F_n is a prime if and only if $3^{(F_n - 1)/2} \equiv -1 \pmod{F_n}$.*

One can see that Pépin's test for $F_n = 2^{2^n} + 1$ is deterministic and efficient with complexity $\tilde{O}((\log_2 F_n)^2)$. There are no deterministic and efficient

2010 *Mathematics Subject Classification*: Primary 11A51; Secondary 11Y11.
Key words and phrases: primality test, generalized Fermat numbers, reciprocity law, computational complexity.

DOI: 10.4064/aa169-4-1

polynomial time algorithms for generalized Fermat numbers $M = (2p)^{2^n}+1$, where p is an odd prime. But there are some results on this subject. Tables of generalized Fermat prime numbers are available at [WW].

Now we recall some previous results about numbers $M = (2p)^{2^n} + 1$, where p is an odd prime, studied by Williams, Berrizbeitia, Berry and others. Williams [W1] obtained efficient primality tests for $p = 3, 5$ by using Lucas sequences. Additionally, these numbers are special types of numbers $A \cdot p^n \pm 1$ with A and p relatively prime. By using the cubic reciprocity law, Berrizbeitia and Berry [BB] gave an efficient deterministic primality test for numbers $A \cdot 3^n \pm 1$ such that $A < 3^n$ and A is coprime to 3, and a prime $q \equiv 1 \pmod 3$ is given such that $A \cdot 3^n \pm 1$ is not a cube modulo q. Afterwards, by using the quintic reciprocity law, Berrizbeitia, Odreman and Tena [BOT] presented an efficient deterministic primality test for numbers $A\cdot 5^n \pm \omega_n$, where $0 < A < 5^n$, $0 < \omega_n < 5^n/2$, $\omega_n^4 \equiv 1 \pmod{5^n}$, and a prime $q \equiv 1 \pmod 5$ is given such that $A \cdot 5^n \pm \omega_n$ is not a 5th power modulo q. Before long, by using properties of the power residue symbol, Berrizbeitia, Berry and Tena [BBT] extended the results in [BB] and [BOT] to numbers $G = A \cdot m^n \pm \omega_n$, where $m, n \geq 2$, $0 < A < m^n$, $0 < \omega_n < m^n/2$, $\omega_n^f \equiv 1 \pmod{m^n}$ with $f = \mathrm{ord}_m(G)$ and $\pi \in \mathbb{Z}[\zeta_m]$ is given such that the mth power residue symbol $\left(\frac{\pi}{G}\right)_m$ is a primitive mth root of 1.

Recently, Deng and Lv [DL] implemented the primality test related to [BBT] for numbers $H = A \cdot p^n + \omega_n$, where $0 < A, \omega_n < p^n$ and $\omega_n^{p-1} \equiv 1 \pmod{p^n}$. They give the form of the corresponding sequences and, by using the Eisenstein reciprocity law, give a primality test for numbers $H = A \cdot p^n + \omega_n$ such that $\pi \in \mathbb{Z}[\zeta_p]$ is given so that the pth power residue symbol $\left(\frac{\pi}{H}\right)_p$ is a primitive pth root of 1.

By directly applying the results of [DL] (or [BB, BBT, BOT]) to generalized Fermat numbers $M = (2p)^{2^n} + 1$, we find that the initial terms of their recurrence sequences depend on A (i.e., 2^{2^n} here), that is, depend on n. In this paper, we will give similar recurrence sequences to decide the primality of generalized Fermat numbers $M = (2p)^{2^n} + 1$, but the initial terms of our sequences are common for all $n \geq 1$ (i.e., independent of n). We mainly use a certain special $2p$th degree reciprocity law, and the original idea is inspired by [BBT, Proposition 4.1]. What is more, we will give a common $\pi \in \mathbb{Z}[\zeta_p]$ for numbers $M = (2p)^{2^n} + 1$ such that $\left(\frac{\pi}{M}\right)_{2p} \neq \pm 1$ for all $n \geq 1$, at least in the cases $p \leq 19$. Note that the $\pi \in \mathbb{Z}[\zeta_p]$ found by using the algorithm of [DL] (or [BB, BBT, BOT]) depends on n.

This paper is organized as follows. In Section 2 we give the definition of the power residue symbol, and prove a special $2p$th power reciprocity law that will be used in the proof of our main theorem. In Section 3 we state and prove our main result together with the analysis of the corresponding complexity. In Section 4, we give explicit primality tests for $M=(2p)^{2^n}+1$ with odd prime numbers $p\le 19$. In Section 5 we show the implementation and computational results for $p=3,5$.

2. Preliminaries. The material of this section may be found in [IR, Chapter 14].

For a positive integer m, let $\zeta_m=e^{2\pi\sqrt{-1}/m}$ be the complex primitive mth root of unity, and $D=\mathbb{Z}[\zeta_m]$ the ring of integers of the mth cyclotomic field $\mathbb{Q}(\zeta_m)$. Let $\mathfrak{p}$ be a prime ideal of D lying over a rational prime p with $\gcd(p,m)=1$. For every $\alpha\in D$, the mth *power residue symbol* $\left(\frac{\alpha}{\mathfrak{p}}\right)_m$ is defined by:

(1) If $\alpha\in\mathfrak{p}$, then $\left(\frac{\alpha}{\mathfrak{p}}\right)_m=0$.

(2) If $\alpha\notin\mathfrak{p}$, then $\left(\frac{\alpha}{\mathfrak{p}}\right)_m=\zeta_m^i$ with $i\in\mathbb{Z}$, where ζ_m^i is the unique mth root of unity in D such that

$$\alpha^{(N(\mathfrak{p})-1)/m}\equiv\zeta_m^i \pmod{\mathfrak{p}},$$

where $N(\mathfrak{p})$ is the absolute norm of the ideal $\mathfrak{p}$.

(3) If $\mathfrak{a}\subset D$ is an arbitrary ideal prime to m, and $\mathfrak{a}=\prod\mathfrak{p}_i^{n_i}$ is its factorization as a product of prime ideals, then

$$\left(\frac{\alpha}{\mathfrak{a}}\right)_m=\prod\left(\frac{\alpha}{\mathfrak{p}_i}\right)_m^{n_i}.$$

We set $\left(\frac{\alpha}{D}\right)_m=1$.

(4) If $\beta\in D$ and β is prime to m, define $\left(\frac{\alpha}{\beta}\right)_m=\left(\frac{\alpha}{\beta D}\right)_m$.

We will need the following proposition:

PROPOSITION 2.1 (see also [IR, Corollary 2, p. 218]). *Suppose $A,B\subset\mathbb{Z}[\zeta_m]$ are ideals prime to m, and $A=(\alpha)$ is principal with* $\gcd(N(A),N(B))=1$. *Then*

$$\left(\frac{N(B)}{\alpha}\right)_m=\left(\frac{\varepsilon(\alpha)}{B}\right)_m\left(\frac{\alpha}{N(B)}\right)_m$$

where $\varepsilon(\alpha)=\pm\zeta_m^i$ for some $i\in\mathbb{Z}$.

Applying Proposition 2.1, we now obtain a special $2p$th power reciprocity law, which is also a special case of Proposition 4.1 in [BOT].

PROPOSITION 2.2. *Let $M>1$ be a prime with $M\equiv 1 \pmod{4p^2}$, where p is an odd prime. Let $\pi\in\mathbb{Z}[\zeta_p]$ be coprime to $2pM$. Then*

$$\left(\frac{M}{\pi}\right)_{2p}=\left(\frac{\pi}{M}\right)_{2p}.$$

Proof. Let $\mathfrak{P}$ be a prime ideal of $\mathbb{Z}[\zeta_p]$ lying over M. Since $M \equiv 1 \pmod{2p}$, we have $N(\mathfrak{P}) = M$. By Proposition 2.1,

$$\left(\frac{N(\mathfrak{P})}{\pi}\right)_{2p} = \left(\frac{\varepsilon(\pi)}{\mathfrak{P}}\right)_{2p}\left(\frac{\pi}{N(\mathfrak{P})}\right)_{2p},$$

which implies

$$\left(\frac{M}{\pi}\right)_{2p} = \left(\frac{\varepsilon(\pi)}{\mathfrak{P}}\right)_{2p}\left(\frac{\pi}{M}\right)_{2p}.$$

And

$$\left(\frac{\varepsilon(\pi)}{\mathfrak{P}}\right)_{2p} \equiv \varepsilon(\pi)^{(M-1)/2p} \equiv (\pm\zeta_{2p}^i)^{(M-1)/2p} = 1 \pmod{\mathfrak{P}}$$

because $2p \mid \frac{M-1}{2p}$. Then $\left(\frac{\varepsilon(\pi)}{\mathfrak{P}}\right)_{2p} = 1$, and the proof is complete. ∎

3. The main result. Let $D = \mathbb{Z}[\zeta_p]$ be the ring of integers of $L = \mathbb{Q}(\zeta_p)$, where p is an odd prime. Let $K = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$ be the maximal real subfield of L. Clearly $[L : \mathbb{Q}] = p - 1$ and $[K : \mathbb{Q}] = (p-1)/2$.

First we give a recurrence expression for the minimal polynomial of $\zeta_p + \zeta_p^{-1}$ over $\mathbb{Q}$, denoted by $F(x)$. Clearly the degree of $F(x)$ is $(p-1)/2$. We define the polynomials $G_n(x)$ $(n \geq 0)$ by $G_0(x) = 1$, $G_1(x) = x$, and for $n \geq 2$ recursively by

$$G_n(x) = \begin{cases} G_{(n-1)/2}(x)G_{(n+1)/2}(x) - x & \text{if } n \text{ is odd,} \\ G_{n/2}(x)^2 - 2 & \text{if } n \text{ is even.} \end{cases} \tag{3.1}$$

We have $F(x) = \sum_{k=0}^{(p-1)/2} G_k(x)$. Indeed, $G_n(x + x^{-1}) = x^n + x^{-n}$ for all $n \geq 1$, and

$$F(\zeta_p + \zeta_p^{-1}) = 1 + \sum_{k=1}^{(p-1)/2} G_k(\zeta_p + \zeta_p^{-1}) = 1 + \sum_{k=1}^{(p-1)/2} (\zeta_p^k + \zeta_p^{-k}) = 0.$$

Suppose

$$F(x) = \sum_{j=0}^{(p-1)/2} (-1)^j a_j x^{(p-1)/2-j};$$

clearly $a_0 = 1$ and $a_j \in \mathbb{Z}$ for $1 \leq j \leq (p-1)/2$. Now $F(x)$ is easy to compute for fixed p. Also $F(x)$ is the minimal polynomial of $\zeta_p^l + \zeta_p^{-l}$ over $\mathbb{Q}$, where $l \not\equiv 0 \pmod{p}$.

Next we introduce the elementary symmetric polynomials of $(p-1)/2$ indeterminates $\{x_1, \ldots, x_{(p-1)/2}\}$:

$$S^{(j)}(x_1, \ldots, x_{(p-1)/2}) = \sum_{1 \leq i_1 < \cdots < i_j \leq (p-1)/2} x_{i_1} \cdots x_{i_j}, \qquad 1 \leq j \leq (p-1)/2.$$

Actually, $F(x)=\prod_{i=1}^{(p-1)/2}[x-(\zeta_p^{2i-1}+\zeta_p^{1-2i})]$, and thus

$$a_j = S^{(j)}(\zeta_p+\zeta_p^{-1},\zeta_p^3+\zeta_p^{-3},\ldots,\zeta_p^{p-2}+\zeta_p^{2-p}) \quad \text{for } 1\le j\le (p-1)/2.$$

Let $G=\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})\cong(\mathbb{Z}/p\mathbb{Z})^*$. For every integer c such that $\gcd(c,2p)=1$ denote by σ_c the element of G that sends ζ_p to ζ_p^c. We know that $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})=\{\sigma_{\pm(2i-1)}\mid 1\le i\le (p-1)/2\}$ and $\mathrm{Gal}(K/\mathbb{Q})=\{\sigma_{2i-1}|_K\mid 1\le i\le (p-1)/2\}$.

For τ in the group ring $\mathbb{Z}[G]$ and α in L with $\alpha\ne 0$, we often denote by α^τ the action of τ on α, that is,

$$\alpha^\tau := \prod_{\sigma\in G}\sigma(\alpha)^{k_\sigma} \quad \text{if} \quad \tau=\sum_{\sigma\in G}k_\sigma\sigma \text{ and } k_\sigma\in\mathbb{Z}.$$

If $\tau\in G$, we will write either α^τ or $\tau(\alpha)$. We also write $\sigma_1=1$ in $\mathbb{Z}[G]$.

Now we give some notation which will be used in the main theorem. Let $\pi\in D$ with $\pi\notin\mathbb{R}$. We denote

$$\alpha=(\pi/\bar\pi)^\gamma, \quad \text{where} \quad \gamma=\sum_{i=1}^{(p-1)/2}(2i-1)\sigma_{(2i-1)^{-1}}\in\mathbb{Z}[G],$$

the bar indicates complex conjugation, and $(2i-1)^{-1}$ is the number such that $(2i-1)\cdot(2i-1)^{-1}\equiv 1 \pmod{2p}$ and $1\le(2i-1)^{-1}<2p$. Obviously, $\alpha\overline{\alpha}=1$. We define $(p-1)/2$ sequences $\{T_k^{(j)}|_{k\ge 0}\},\ 1\le j\le (p-1)/2$, by

$$T_k^{(j)}=S^{(j)}(\alpha_1^{(k)},\ldots,\alpha_{(p-1)/2}^{(k)}),$$

where $\alpha_i^{(k)}=\sigma_{2i-1}(\alpha^{(2p)^k}+\bar\alpha^{(2p)^k}),\ i=1,\ldots,(p-1)/2$.

Note that $T_k^{(j)}\in\mathbb{Q}$. Indeed, $\beta:=\alpha^{(2p)^k}+\bar\alpha^{(2p)^k}\in K$. Let $C(x)$ be the characteristic polynomial of β over $\mathbb{Q}$. Then

$$C(x)=\prod_{i=1}^{(p-1)/2}(x-\alpha_i^{(k)}):=x^{(p-1)/2}+\sum_{j=1}^{(p-1)/2}c_jx^{(p-1)/2-j}\in\mathbb{Q}[x]$$

and $T_k^{(j)}=(-1)^jc_j\in\mathbb{Q}$. What is more, there are explicit recurrence relations from $T_k^{(j)}$ to $T_{k+1}^{(j)}$, $1\le j\le (p-1)/2$. We will give the details for the cases $p=3,5$ in Sections 4 and 5 respectively.

Our main theorem is a primality test for special generalized Fermat numbers $M=(2p)^{2^n}+1$ with p an odd prime:

THEOREM 3.1. *Let $T_k^{(j)}$ and a_j be as above. Let $M=(2p)^{2^n}+1$ with $n\ge 1$, p be an odd prime and $r=2^n$. Let $\pi\in\mathbb{Z}[\zeta_p]$ be coprime to $2pM$ such that $\pi\notin\mathbb{R}$ and $\left(\frac{M}{\pi}\right)_{2p}\ne\pm 1$. Suppose that if $x^{p-1}\equiv 1 \pmod{p^r}$ and $1<x<p^r$, then x does not divide M. Then M is prime if and only if one of the following holds:*

(i) $\left(\frac{M}{\pi}\right)_{2p} = \zeta_p^l$ *for some* $l \in \mathbb{Z}$ *with* $l \not\equiv 0 \pmod{p}$, *and* $T_{r-1}^{(j)} \equiv a_j \pmod{M}$ *for all* $1 \le j \le (p-1)/2$;

(ii) $\left(\frac{M}{\pi}\right)_{2p} = -\zeta_p^l$ *for some* $l \in \mathbb{Z}$ *with* $l \not\equiv 0 \pmod{p}$, *and* $T_{r-1}^{(j)} \equiv (-1)^j a_j \pmod{M}$ *for all* $1 \le j \le (p-1)/2$.

Proof. We first show necessity. Suppose M is a prime. Since π is prime to $2pM$, applying Proposition 2.2 we get $\left(\frac{M}{\pi}\right)_{2p} = \left(\frac{\pi}{M}\right)_{2p}$. Now $M \equiv 1 \pmod{2p}$ implies that the ideal MD can be factorized into a product of $p-1$ distinct prime ideals in D. We write

$$MD = (\mathfrak{p}\bar{\mathfrak{p}})^{\sum_{i=1}^{(p-1)/2} \sigma_{2i-1}},$$

thus

$$\begin{aligned}
\left(\frac{M}{\pi}\right)_{2p} &= \left(\frac{\pi}{M}\right)_{2p} = \prod_{i=1}^{(p-1)/2} \left(\frac{\pi}{(\mathfrak{p}\bar{\mathfrak{p}})^{\sigma_{2i-1}}}\right)_{2p} \\
&= \prod_{i=1}^{(p-1)/2} \left(\frac{(\pi/\bar{\pi})^{(2i-1)\sigma_{(2i-1)^{-1}}}}{\mathfrak{p}}\right)_{2p} = \left(\frac{(\pi/\bar{\pi})^{\sum_{k=1}^{(p-1)/2}(2i-1)\sigma_{(2i-1)^{-1}}}}{\mathfrak{p}}\right)_{2p} \\
&= \left(\frac{\alpha}{\mathfrak{p}}\right)_{2p} \equiv \alpha^{(M-1)/2p} \equiv \alpha^{(2p)^{r-1}} \pmod{\mathfrak{p}}.
\end{aligned}$$

Since $\mathfrak{p}$ is an arbitrary prime ideal lying over M, we have

$$\left(\frac{M}{\pi}\right)_{2p} \equiv \alpha^{(2p)^{r-1}} \pmod{M}.$$

Taking the complex conjugate of every term of the last congruence, we get

$$\alpha_1^{(r-1)} = \alpha^{(2p)^{r-1}} + \bar{\alpha}^{(2p)^{r-1}} \equiv \left(\frac{M}{\pi}\right)_{2p} + \left(\frac{M}{\pi}\right)_{2p}^{-1} \pmod{M}.$$

Also acting by the Galois group elements σ_{2i-1}, $1 \le i \le (p-1)/2$, on both sides of the last congruence, we obtain

$$\alpha_i^{(r-1)} = \sigma_{2i-1}(\alpha^{(2p)^{r-1}} + \bar{\alpha}^{(2p)^{r-1}}) \equiv \left(\frac{M}{\pi}\right)_{2p}^{2i-1} + \left(\frac{M}{\pi}\right)_{2p}^{1-2i} \pmod{M}$$

for all $1 \le i \le (p-1)/2$. Hence

$$\begin{aligned}
T_{r-1}^{(j)} &= S^{(j)}(\alpha_1^{(r-1)}, \dots, \alpha_{(p-1)/2}^{(r-1)}) \\
&\equiv S^{(j)}\left(\left(\frac{M}{\pi}\right)_{2p} + \left(\frac{M}{\pi}\right)_{2p}^{-1}, \dots, \left(\frac{M}{\pi}\right)_{2p}^{p-2} + \left(\frac{M}{\pi}\right)_{2p}^{2-p}\right) \pmod{M}
\end{aligned}$$

for $1 \le j \le (p-1)/2$.

(i) Suppose $\left(\frac{M}{\pi}\right)_{2p} = \zeta_p^l$ for some l with $l \not\equiv 0 \pmod{p}$. Using the polynomial $F(x)$, as shown before we get $a_j = S^{(j)}(\zeta_p + \zeta_p^{-1}, \zeta_p^3 + \zeta_p^{-3}, \dots,$

$\zeta_p^{p-2}+\zeta_p^{2-p})$ for $1\le j\le (p-1)/2$. Hence

$$T_{r-1}^{(j)} \equiv S^{(j)}(\zeta_p+\zeta_p^{-1},\zeta_p^3+\zeta_p^{-3},\dots,\zeta_p^{p-2}+\zeta_p^{2-p}) = a_j \pmod M$$

for all $j=1,\dots,(p-1)/2$.

(ii) Suppose $\left(\frac{M}{\pi}\right)_{2p} = -\zeta_p^l$ for some l with $l\not\equiv 0 \pmod p$. By the properties of elementary symmetric polynomials, we have

$$\begin{aligned}
T_{r-1}^{(j)} &\equiv S^{(j)}\left(\left(\frac{M}{\pi}\right)_{2p}+\left(\frac{M}{\pi}\right)_{2p}^{-1},\dots,\left(\frac{M}{\pi}\right)_{2p}^{p-2}+\left(\frac{M}{\pi}\right)_{2p}^{2-p}\right)\\
&= S^{(j)}(-\zeta_p-\zeta_p^{-1},-\zeta_p^3-\zeta_p^{-3},\dots,-\zeta_p^{p-2}-\zeta_p^{2-p})\\
&= (-1)^j S^{(j)}(\zeta_p+\zeta_p^{-1},\zeta_p^3+\zeta_p^{-3},\dots,\zeta_p^{p-2}+\zeta_p^{2-p})\\
&= (-1)^j a_j \pmod M
\end{aligned}$$

for all $j=1,\dots,(p-1)/2$. This completes the proof of necessity.

Next we turn to the proof of sufficiency. Suppose q is an arbitrary prime divisor of M. Let $\mathfrak{q}$ be a prime ideal in the ring of integers of K lying over q, and $\mathfrak{Q}$ be a prime ideal of D lying over $\mathfrak{q}$. We denote $\beta = \alpha^{(2p)^{r-1}}+\bar\alpha^{(2p)^{r-1}}\in K$ and $T_{r-1}^{(j)} = S^{(j)}(\beta,\sigma_3(\beta),\dots,\sigma_{p-2}(\beta))$ for $1\le j\le (p-1)/2$.

(i) Suppose $T_{r-1}^{(j)}\equiv a_j \pmod M$, that is,

$$S^{(j)}(\beta,\sigma_3(\beta),\dots,\sigma_{p-2}(\beta))\equiv a_j \pmod{\mathfrak{q}}.$$

Then

$$\begin{aligned}
0 &= (\beta-\beta)(\beta-\sigma_3(\beta))\cdots(\beta-\sigma_{p-2}(\beta))\\
&= \beta^{(p-1)/2}+\sum_{j=1}^{(p-1)/2}(-1)^j S^{(j)}(\beta,\sigma_3(\beta),\dots,\sigma_{p-2}(\beta))\beta^{(p-1)/2-j}\\
&\equiv \beta^{(p-1)/2}+\sum_{j=1}^{(p-1)/2}(-1)^j a_j\beta^{(p-1)/2-j} = F(\beta) \pmod{\mathfrak{q}}.
\end{aligned}$$

Since $F(x+x^{-1}) = \sum_{k=0}^{(p-1)/2} G_k(x+x^{-1}) = \sum_{k=0}^{(p-1)/2}(x^k+x^{-k})$, we get

$$\begin{aligned}
0 &\equiv F(\alpha^{(2p)^{r-1}}+\bar\alpha^{(2p)^{r-1}})\\
&= 1+\sum_{k=1}^{(p-1)/2}[(\alpha^{(2p)^{r-1}})^k+(\bar\alpha^{(2p)^{r-1}})^k] \pmod{\mathfrak{Q}}.
\end{aligned}$$

We multiply both sides of the above congruence by $\alpha^{(2p)^{r-1}\cdot(p-1)/2} = \bar\alpha^{-(2p)^{r-1}\cdot(p-1)/2}$ to get

$$\sum_{k=0}^{p-1}(\alpha^{(2p)^{r-1}})^k \equiv 0 \pmod{\mathfrak{Q}}.$$

Thus the image of $\alpha^{(2p)^{r-1}}$ has order p in the multiplicative group $(D/\mathfrak{Q})^*$, and the image of $\alpha^{2^{r-1}}$ has order p^r in $(D/\mathfrak{Q})^*$. Since the order of the group $(D/\mathfrak{Q})^*$ is $N(\mathfrak{Q})-1$ which divides $q^{p-1}-1$, we have $q^{p-1}\equiv 1 \pmod{p^r}$. By the assumption M is divisible by no solutions of the equation $x^{p-1}\equiv 1 \pmod{p^r}$ between 1 and p^r, that is, $q>p^r>\sqrt{(2p)^r+1}=\sqrt{M}$, so clearly M is prime.

(ii) If $T_{r-1}^{(j)}\equiv(-1)^j a_j \pmod{M}$, we have

$$S^{(j)}(\beta,\sigma_3(\beta),\dots,\sigma_{p-2}(\beta))\equiv(-1)^j a_j \pmod{\mathfrak{q}}$$

and

$$\begin{aligned}0&=\beta^{(p-1)/2}+\sum_{j=1}^{(p-1)/2}(-1)^j S^{(j)}(\beta,\sigma_3(\beta),\dots,\sigma_{p-2}(\beta))\beta^{(p-1)/2-j}\\ &\equiv\beta^{(p-1)/2}+\sum_{j=1}^{(p-1)/2}a_j\beta^{(p-1)/2-j}=(-1)^{(p-1)/2}F(-\beta) \pmod{\mathfrak{q}}.\end{aligned}$$

As in (i), we obtain

$$\begin{aligned}0&\equiv F(-\alpha^{(2p)^{r-1}}-\bar{\alpha}^{(2p)^{r-1}})\\ &=1+\sum_{k=1}^{(p-1)/2}[(-\alpha^{(2p)^{r-1}})^k+(-\bar{\alpha}^{(2p)^{r-1}})^k] \pmod{\mathfrak{Q}}\end{aligned}$$

and

$$\sum_{k=0}^{p-1}(-1)^{k-(p-1)/2}\alpha^{(2p)^{r-1}k}\equiv 0 \pmod{\mathfrak{Q}},$$

i.e.,

$$\sum_{k=0}^{p-1}(-1)^k(\alpha^{(2p)^{r-1}})^k\equiv 0 \pmod{\mathfrak{Q}}.$$

That is, the image of $\alpha^{(2p)^{r-1}}$ has order $2p$ in the multiplicative group $(D/\mathfrak{Q})^*$, and the image of α has order $(2p)^r$ in $(D/\mathfrak{Q})^*$. As in case (i), we get $q^{p-1}\equiv 1 \pmod{(2p)^r}$. Also using the assumption we obtain $q>p^r>\sqrt{(2p)^r+1}=\sqrt{M}$, hence M is prime. This completes the proof of sufficiency. ■

The assumptions of Theorem 3.1 are not difficult to check. First the congruence equation $x^{p-1}\equiv 1 \pmod{p^r}$ is easy to solve. Secondly, the existence of π is computable theoretically. One can see more details in [DL, Section 4]. Actually, in the next section for $M=(2p)^{2^n}+1$ with fixed odd prime $p\le 19$, we will find a common $\pi\in\mathbb{Z}[\zeta_p]$ for all $n\ge 1$ such that

$\left(\frac{\pi}{M}\right)_{2p} \neq \pm 1$. Having π independent of n is advantageous in the primality test.

The initial terms of the testing sequences in Theorem 3.1 are

$$T_0^{(j)} = S^{(j)}(\alpha_1^{(0)}, \ldots, \alpha_{(p-1)/2}^{(0)}), \quad 1 \le j \le (p-1)/2,$$

where $\alpha_i^{(0)} = \sigma_{2i-1}(\alpha + \bar{\alpha})$ for $i = 1, \ldots, (p-1)/2$. Since α is independent of n, the initial terms $T_0^{(j)}$, $1 \le j \le (p-1)/2$, are the same for all $M = (2p)^{2^n} + 1$, $n \in \mathbb{Z}^+$, with fixed odd prime p, at least for $p \le 19$. The recurrence sequences of [DL] have initial terms

$$\tilde{T}_0^{(j)} = S^{(j)}(\tilde{\alpha}_1^{(0)}, \ldots, \tilde{\alpha}_{(p-1)/2}^{(0)}), \quad 1 \le j \le (p-1)/2,$$

with $\tilde{\alpha}_i^{(0)} = \sigma_{2i-1}(\tilde{\alpha} + \bar{\tilde{\alpha}})$ for $i = 1, \ldots, (p-1)/2$, where $\tilde{\alpha} = \alpha^{2^{2^n}}$, which does depend on n.

Computational complexity. Since $T_k^{(j)} \in \mathbb{Q}$, all the computations of the sufficient and necessary conditions in Theorem 3.1 can be done in the residue class ring $\mathbb{Z}/M\mathbb{Z}$ once a specific π is given. There are $(p-1)/2$ recurrence relations for the testing sequences $\{T_k^{(j)}|_{k\ge 0}\}$, $1 \le j \le (p-1)/2$, from $T_k^{(j)}$ to $T_{k+1}^{(j)}$ with $1 \le j \le (p-1)/2$, which are polynomial relations in $(p-1)/2$ variables with all of their degrees at most $2p$. We will give the relevant details later for $p = 3, 5$. The elementary symmetric polynomials involved in the computation of initial terms can be obtained by pre-computation. Thus the running complexity of our primality test is $\tilde{O}(\frac{1}{2}(p-1)2^p \log_2 M + (r-1)\log_2(2p)\log_2 M) = \tilde{O}((p-1)2^p \log_2 M + (\log_2 M)^2)$ bit operations. This estimate of computational complexity is very crude. But still we can see that our primality test is efficient for fixed p.

4. Primality tests for $p \le 19$. We know from [WA, Chapter 11] that $\mathbb{Z}[\zeta_p]$ is a PID for $p \le 19$. In this section we will apply Theorem 3.1 to the cases $3 \le p \le 19$ with p prime. Firstly, we present $G_k(x)$, $0 \le k \le 9$, in Table 1.

Table 1. $G_k(x)$, $0 \le k \le 9$

k	$G_k(x)$	k	$G_k(x)$
0	1	5	$x^5 - 5x^3 + 5x$
1	x	6	$x^6 - 6x^4 + 9x^2 - 2$
2	$x^2 - 2$	7	$x^7 - 7x^5 + 14x^3 - 7x$
3	$x^3 - 3x$	8	$x^8 - 8x^6 + 20x^4 - 16x^2 + 2$
4	$x^4 - 4x^2 + 2$	9	$x^9 - 9x^7 + 27x^5 - 30x^3 + 9x$

We denote by $F_p(x),\ 3 \le p \le 19$ with p prime, the minimal polynomial of $\zeta_p + \zeta_p^{-1}$ over $\mathbb{Q}$. We list these $F_p(x)$ in Table 2.

Table 2. $F_p(x),\ 3 \le p \le 19$ and p prime

p	$F_p(x)$
3	$x+1$
5	x^2+x-1
7	x^3+x^2-2x-1
11	$x^5+x^4-4x^3-3x^2+3x+1$
13	$x^6+x^5-5x^4-4x^3+6x^2+3x-1$
17	$x^8+x^7-7x^6-6x^5+15x^4+10x^3-10x^2-4x+1$
19	$x^9+x^8-8x^7-7x^6+21x^5+15x^4-20x^3-10x^2+5x+1$

Next we give all π occurring in Theorem 3.1 for odd primes $p \le 19$ in Table 3. We will find that these π are suitable for the primality tests in the proof of the following propositions. Indeed, the fact that $\mathbb{Z}[\zeta_p]$ is a PID for $p \le 19$ is crucial during the process of specific computations with the help of Magma [BCP].

Table 3. Values of π in $\mathbb{Z}[\zeta_p]$

p	π	p	π
3	$2+3\zeta_3$	13	$1+\zeta_{13}^2+\zeta_{13}^5$
5	$1-\zeta_5-\zeta_5^3$	17	$1+\zeta_{17}^2+\zeta_{17}^9$
7	$1-\zeta_7+\zeta_7^4$	19	$-1-\zeta_{19}^2+\zeta_{19}^{15}$
11	$1+\zeta_{11}^7+\zeta_{11}^8$		

The primality tests for $M = (2p)^{2^n}+1$ with odd prime numbers $p \le 19$ are contained in the following propositions.

Proposition 4.1. *Let $M = 6^{2^n}+1$, $n \ge 1$ and $r = 2^n$. Let $\pi = 2+3\zeta_3 \in \mathbb{Z}[\zeta_3]$ and $\alpha = \pi/\bar{\pi}$. Define $T_0 = \alpha + \bar{\alpha}$ and $T_{k+1} = T_k^6 - 6T_k^4 + 9T_k^2 - 2$ for $k \ge 0$. Then M is prime if and only if $T_{r-1} \equiv -1 \pmod M$.*

Proof. Let $L = \mathbb{Q}(\zeta_3)$. Then $\mathrm{Norm}_{L/\mathbb{Q}}(\pi) = \pi\bar{\pi} = (2+3\zeta_3)(-1-3\zeta_3) = 7$. Since $M \equiv 2 \pmod 7$, we get $\left(\frac{M}{\pi}\right)_6 \equiv M^{(7-1)/6} = M \equiv 2 \equiv \zeta_3^2 \pmod \pi$, and so $\left(\frac{M}{\pi}\right)_6 = \zeta_3^2$. Let $T_k = \alpha^{6^k} + \bar{\alpha}^{6^k}$, $k \ge 0$. We can verify that T_k satisfies the recurrence relation in the assumption (or refer to Section 5 for the case $p = 5$). We have $F_3(x) = x+1$, that is, $a_1 = -1$. Applying the necessity part of Theorem 3.1 we deduce that if M is prime then $T_{r-1} \equiv -1 \pmod M$. This completes the proof of necessity.

By the proof of the sufficiency part of Theorem 3.1, if $T_{r-1} \equiv -1 \pmod M$, then 3^r divides q^2-1 for every prime divisor q of M, i.e.,

3^r divides only one of $q+1$ and $q-1$ because of $\gcd(q+1,q-1)=2$. Hence $q\ge 3^r-1>\sqrt{6^r+1}=\sqrt{M}$, and so M is prime. This completes the proof of sufficiency. ∎

PROPOSITION 4.2. *Let* $M=10^{2^n}+1$, $n\ge 1$ *and* $r=2^n$. *Let* $\pi=1-\zeta_5-\zeta_5^3\in\mathbb{Z}[\zeta_5]$ *and* $\alpha=(\pi/\bar\pi)^{1+3\sigma_{-3}}$. *Define* $T_k^{(1)}=\alpha_1^{(k)}+\alpha_2^{(k)}$, $T_k^{(2)}=\alpha_1^{(k)}\cdot\alpha_2^{(k)}$, $k\ge 0$, *where* $\alpha_1^{(k)}=\alpha^{10^k}+\bar\alpha^{10^k}$, $\alpha_2^{(k)}=\sigma_3(\alpha_1^{(k)})$. *Suppose that if* $x^4\equiv 1 \pmod{5^r}$ *and* $1<x<5^r$ *then* x *does not divide* M. *Then* M *is prime if and only if* $T_{r-1}^{(1)}\equiv 1\equiv -T_{r-1}^{(2)} \pmod M$.

Proof. Let $L=\mathbb{Q}(\zeta_5)$. Then $\mathrm{Norm}_{L/\mathbb{Q}}(\pi)=(\pi\bar\pi)^{1+\sigma_3}=11$. Since $M\equiv 2 \pmod{11}$, we get $\left(\frac{M}{\pi}\right)_{10}\equiv M^{(11-1)/10}=M\equiv 2\equiv -\zeta_5 \pmod{\pi}$, and so $\left(\frac{M}{\pi}\right)_{10}=-\zeta_5$. We notice that here $F_5(x)=x^2+x-1$, which implies $a_1=-1$ and $a_2=-1$. Thus all the assumptions of Theorem 3.1 are satisfied, giving the desired necessity and sufficiency. ∎

REMARK. (i) The explicit recurrence formula obtained for $M=6^{2^n}+1$ in Proposition 4.1 is similar to the ones of Williams [W1] and of Berrizbeitia and Berry [BB]. The degree of the recurrence formula in [BB] is lower than ours. However, the seed of their test is $Q_0=\alpha^{2^{2^n}}+\bar\alpha^{2^{2^n}}$, which depends on n while ours does not (due to $T_0=\alpha+\bar\alpha$ in Proposition 4.1). Anyway, these three primality tests for $M=6^{2^n}+1$ have the same computational complexity of $\tilde O((\log_2 M)^2)$.

(ii) In Proposition 4.2 we did not give the explicit recurrence relations for $M=10^{2^n}+1$ since they are a bit long. But we will state them in Section 5 by using the same method as in [BOT]. One can see that our recurrence sequences are similar to the ones in [BOT] and [W1]. All the three primality tests for $M=10^{2^n}+1$ have the same computational complexity of $\tilde O((\log_2 M)^2)$. For the same reason as in the previous remark the seeds of our test improve those of [BOT].

(iii) As to the recurrence sequences in the cases $7\le p\le 19$ with p prime, we will not give their explicit forms in this paper. We still have improved seeds compared to [DL] in all these cases.

Finally, we introduce the remaining five primality tests of the special generalized Fermat numbers $(2p)^{2^n}+1$ for $p\le 19$.

PROPOSITION 4.3. *Let* $M=14^{2^n}+1$, $n>1$ *and* $r=2^n$. *Let* $\pi=1-\zeta_7+\zeta_7^4\in\mathbb{Z}[\zeta_7]$ *and* $\alpha=(\pi/\bar\pi)^{1+3\sigma_5+5\sigma_3}$. *Define* $T_k^{(1)}=\alpha_1^{(k)}+\alpha_2^{(k)}+\alpha_3^{(k)}$, $T_k^{(2)}=S^{(2)}(\alpha_1^{(k)},\alpha_2^{(k)},\alpha_3^{(k)})$, $T_k^{(3)}=\alpha_1^{(k)}\alpha_2^{(k)}\alpha_3^{(k)}$, $k\ge 0$, *where* $\alpha_1^{(k)}=\alpha^{14^k}+\bar\alpha^{14^k}$, $\alpha_2^{(k)}=\sigma_3(\alpha_1^{(k)})$, $\alpha_3^{(k)}=\sigma_5(\alpha_1^{(k)})$. *Suppose that if* $x^6\equiv 1 \pmod{7^r}$ *and* $1<x<7^r$ *then* x *does not divide* M. *Then* M *is prime if and only if one of the following holds:*

(i) $M \equiv \pm 8 \pmod{29}$ *and* $T_{r-1}^{(1)} \equiv 1 \equiv -T_{r-1}^{(3)} \pmod{M}$, $T_{r-1}^{(2)} \equiv -2 \pmod{M}$;

(ii) $M \equiv -5 \pmod{29}$ *and* $T_{r-1}^{(1)} \equiv -1 \equiv -T_{r-1}^{(3)} \pmod{M}$, $T_{r-1}^{(2)} \equiv -2 \pmod{M}$.

Proof. Let $L = \mathbb{Q}(\zeta_7)$. Then $\mathrm{Norm}_{L/\mathbb{Q}}(\pi) = (\pi\bar{\pi})^{1+\sigma_3+\sigma_5} = 29$. Since $M \equiv \pm 8$ or $-5 \pmod{29}$, $n > 1$, we have $\left(\frac{M}{\pi}\right)_{14} \equiv M^{(29-1)/14} = M^2 \equiv 6$ or $-4 \equiv -\zeta_7^3$ or $\zeta_7 \pmod{\pi}$, and $\left(\frac{M}{\pi}\right)_{14} = -\zeta_7^3$ or $\zeta_7 \neq \pm 1$. Notice that $F_7(x) = x^3 + x^2 - 2x - 1$, which implies $a_1 = -1$, $a_2 = -2$, $a_3 = 1$. Thus all the assumptions of Theorem 3.1 are satisfied, giving the conclusion. ∎

Proposition 4.4. *Let* $M = 22^{2^n} + 1$, $n \geq 1$ *and* $r = 2^n$. *Let* $\pi = 1+\zeta_{11}^7+\zeta_{11}^8 \in \mathbb{Z}[\zeta_{11}]$ *and* $\alpha = (\pi/\bar{\pi})^\tau$, *where* $\tau = 1+3\sigma_{-7}+5\sigma_9+7\sigma_{-3}+9\sigma_5$. *Define* $T_k^{(j)} = S^{(j)}(\alpha_1^{(k)}, \ldots, \alpha_5^{(k)})$, $k \geq 0$, $1 \leq j \leq 5$, *where* $\alpha_1^{(k)} = \alpha^{22^k} + \bar{\alpha}^{22^k}$ *and* $\alpha_i^{(k)} = \sigma_{2i-1}(\alpha_1^{(k)})$, $2 \leq i \leq 5$. *Suppose that if* $x^{10} \equiv 1 \pmod{11^r}$ *and* $1 < x < 11^r$ *then* x *does not divide* M. *Then* M *is prime if and only if* $T_{r-1}^{(1)} \equiv -1 \equiv T_{r-1}^{(5)} \pmod{M}$, $T_{r-1}^{(2)} \equiv -4 \pmod{M}$ *and* $T_{r-1}^{(3)} \equiv 3 \equiv T_{r-1}^{(4)} \pmod{M}$.

Proof. Let $L = \mathbb{Q}(\zeta_{11})$. Then $\mathrm{Norm}_{L/\mathbb{Q}}(\pi) = (\pi\bar{\pi})^{\sum_{i=1}^5 \sigma_{2i-1}} = 23$. Since $M \equiv 2 \pmod{23}$, $n \geq 1$, we get $\left(\frac{M}{\pi}\right)_{22} \equiv M^{(23-1)/22} = M \equiv 2 \equiv \zeta_{11}^2 \pmod{\pi}$, and so $\left(\frac{M}{\pi}\right)_{22} = \zeta_{11}^2$. Also notice that $F_{11}(x) = x^5 + x^4 - 4x^3 - 3x^2+3x+1$, which implies $a_1 = -1$, $a_2 = -4$, $a_3 = 3$, $a_4 = 3$, $a_5 = -1$. Thus all the assumptions of Theorem 3.1 are satisfied, giving the conclusion. ∎

Proposition 4.5. *Let* $M = 26^{2^n}+1$, $n > 1$ *and* $r = 2^n$. *Let* $\pi = 1+\zeta_{13}^2+\zeta_{13}^5 \in \mathbb{Z}[\zeta_{13}]$ *and* $\alpha = (\pi/\bar{\pi})^\tau$, *where* $\tau = 1+3\sigma_9+5\sigma_{-5}+7\sigma_{-11}+9\sigma_3+11\sigma_{-7}$. *Define* $T_k^{(j)} = S^{(j)}(\alpha_1^{(k)}, \ldots, \alpha_6^{(k)})$, $k \geq 0$, $1 \leq j \leq 6$, *where* $\alpha_1^{(k)} = \alpha^{26^k} + \bar{\alpha}^{26^k}$ *and* $\alpha_i^{(k)} = \sigma_{2i-1}(\alpha_1^{(k)})$, $2 \leq i \leq 6$. *Suppose that if* $x^{12} \equiv 1 \pmod{13^r}$ *and* $1 < x < 13^r$ *then* x *does not divide* M. *Then* M *is prime if and only if one of the following holds:*

(i) $M \equiv 25, \pm 16, -6, 11, -24, -5, -10$ *or* $17 \pmod{53}$ *and, modulo* M, $T_{r-1}^{(1)} \equiv -1 \equiv T_{r-1}^{(6)}$, $T_{r-1}^{(2)} \equiv -5$, $T_{r-1}^{(3)} \equiv 4$, $T_{r-1}^{(4)} \equiv 6$ *and* $T_{r-1}^{(5)} \equiv -3$;

(ii) $M \equiv 14, -8$ *or* $-3 \pmod{53}$ *and, modulo* M, $T_{r-1}^{(1)} \equiv 1 \equiv -S_{r-1}^{(6)}$, $T_{r-1}^{(2)} \equiv -5$, $T_{r-1}^{(3)} \equiv -4$, $T_{r-1}^{(4)} \equiv 6$ *and* $T_{r-1}^{(5)} \equiv 3$.

Proof. Let $L = \mathbb{Q}(\zeta_{13})$. Then $\mathrm{Norm}_{L/\mathbb{Q}}(\pi) = (\pi\bar{\pi})^{\sum_{i=1}^6 \sigma_{2i-1}} = 53$. Since $M \equiv 25, \pm 16, -6, 11, -24, -5, -10, 17, 14, -8$ or $-3 \pmod{53}, n > 1$, we have $\left(\frac{M}{\pi}\right)_{26} \equiv M^{(53-1)/26} = M^2 \equiv -11, -9, -17, 15, -7, 25, -6, 24, -16, 11, 9 \equiv \zeta_{13}^3, \zeta_{13}^4, \zeta_{13}^5, \zeta_{13}^6, \zeta_{13}^7, \zeta_{13}^8, \zeta_{13}^9, \zeta_{13}^{10}, -\zeta_{13}^2, -\zeta_{13}^3, -\zeta_{13}^4 \pmod{\pi}$ respectively, and $\left(\frac{M}{\pi}\right)_{26} = \zeta_{13}^3, \zeta_{13}^4, \zeta_{13}^5, \zeta_{13}^6, \zeta_{13}^7, \zeta_{13}^8, \zeta_{13}^9, \zeta_{13}^{10}, -\zeta_{13}^2, -\zeta_{13}^3, -\zeta_{13}^4 \neq \pm 1$

respectively. Notice that $F_{13}(x) = x^6 + x^5 - 5x^4 - 4x^3 + 6x^2 + 3x - 1$, which implies $a_1 = -1$, $a_2 = -5$, $a_3 = 4$, $a_4 = 6$, $a_5 = -3$, $a_6 = -1$. Thus all the assumptions of Theorem 3.1 are satisfied, giving the conclusion. ∎

PROPOSITION 4.6. *Let* $M = 34^{2^n} + 1$, $n \ge 1$ *and* $r = 2^n$. *Let* $\pi = 1 + \zeta_{17}^2 + \zeta_{17}^9 \in \mathbb{Z}[\zeta_{17}]$, $\alpha = (\pi/\bar{\pi})^\tau$, *where* $\tau = 1 + 3\sigma_{-11} + 5\sigma_7 + 7\sigma_5 + 9\sigma_{-15} + 11\sigma_{-3} + 13\sigma_{-13} + 15\sigma_{-9}$. *Define* $T_k^{(j)} = S^{(j)}(\alpha_1^{(k)}, \dots, \alpha_8^{(k)})$, $k \ge 0$, $1 \le j \le 8$, *where* $\alpha_1^{(k)} = \alpha^{34^k} + \bar{\alpha}^{34^k}$ *and* $\alpha_i^{(k)} = \sigma_{2i-1}(\alpha_1^{(k)})$, $2 \le i \le 8$. *Suppose that if* $x^{16} \equiv 1 \pmod{17^r}$ *and* $1 < x < 17^r$ *then* x *does not divide* M. *Then* M *is prime if and only if one of the following holds:*

(i) $M \equiv -21$ *or* $15 \pmod{103}$ *and, modulo* M, $T_{r-1}^{(1)} \equiv -1 \equiv -T_{r-1}^{(8)}$, $T_{r-1}^{(2)} \equiv -7$, $T_{r-1}^{(3)} \equiv 6$, $T_{r-1}^{(4)} \equiv 15$, $T_{r-1}^{(5)} \equiv -10 \equiv T_{r-1}^{(6)}$ *and* $T_{r-1}^{(7)} \equiv 4$;
(ii) $M \equiv 35, 24, -2, -9, 10$ *or* $-30 \pmod{103}$ *and, modulo* M, $T_{r-1}^{(1)} \equiv 1 \equiv T_{r-1}^{(8)}$, $T_{r-1}^{(2)} \equiv -7$, $T_{r-1}^{(3)} \equiv -6$, $T_{r-1}^{(4)} \equiv 15$, $T_{r-1}^{(5)} \equiv 10 \equiv -T_{r-1}^{(6)}$ *and* $T_{r-1}^{(7)} \equiv -4$.

Proof. Let $L = \mathbb{Q}(\zeta_{17})$. Then $\mathrm{Norm}_{L/\mathbb{Q}}(\pi) = (\pi\bar{\pi})^{\sum_{i=1}^8 \sigma_{2i-1}} = 103$. Since $M \equiv -21, 15, 35, 24, -2, -9, 10$ or $-30 \pmod{103}$, $n \ge 1$, we get $\left(\frac{M}{\pi}\right)_{34} \equiv M^{(103-1)/34} = M^3 \equiv 9, -24, 27, 22, -8, -30, -14 \equiv \zeta_{17}^2, \zeta_{17}^7, -\zeta_{17}^3, -\zeta_{17}^4, -\zeta_{17}^6, -\zeta_{17}^{10}, -\zeta_{17}^{13} \pmod{\pi}$ respectively. Notice that $(-2)^3 \equiv (-9)^3 \equiv -8 \pmod{103}$, which leads to the combination of -2 and -9 in the second congruence. Thus $\left(\frac{M}{\pi}\right)_{34} = \zeta_{17}^2, \zeta_{17}^7, -\zeta_{17}^3, -\zeta_{17}^4, -\zeta_{17}^6, -\zeta_{17}^{10}, -\zeta_{17}^{13} \ne \pm 1$ respectively. Now $F_{17}(x) = x^8 + x^7 - 7x^6 - 6x^5 + 15x^4 + 10x^3 - 10x^2 - 4x + 1$ implies that $a_1 = -1$, $a_2 = -7$, $a_3 = 6$, $a_4 = 15$, $a_5 = -10$, $a_6 = -10$, $a_7 = 4$, $a_8 = 1$. Hence all the assumptions of Theorem 3.1 are satisfied, giving the conclusion. ∎

PROPOSITION 4.7. *Let* $M = 38^{2^n} + 1$, $n > 1$ *and* $r = 2^n$. *Let* $\pi = -1 - \zeta_{19}^2 + \zeta_{19}^{15} \in \mathbb{Z}[\zeta_{19}]$, $\alpha = (\pi/\bar{\pi})^\tau$, *where* $\tau = 1 + 3\sigma_{13} + 5\sigma_{-15} + 7\sigma_{11} + 9\sigma_{17} + 11\sigma_7 + 13\sigma_3 + 15\sigma_{-5} + 17\sigma_9$. *Define* $T_k^{(j)} = S^{(j)}(\alpha_1^{(k)}, \dots, \alpha_9^{(k)})$, $k \ge 0$, $1 \le j \le 9$, *where* $\alpha_1^{(k)} = \alpha^{38^k} + \bar{\alpha}^{38^k}$ *and* $\alpha_i^{(k)} = \sigma_{2i-1}(\alpha_1^{(k)})$, $2 \le i \le 9$. *Suppose that if* $x^{18} \equiv 1 \pmod{19^r}$ *and* $1 < x < 19^r$ *then* x *does not divide* M. *Then* M *is prime if and only if one of the following holds:*

(i) $M \equiv -48, -44, 15, -4, 56, -55, -45, -61, 26$ *or* $49 \pmod{229}$ *and, modulo* M, $T_{r-1}^{(1)} \equiv -1 \equiv T_{r-1}^{(9)}$, $T_{r-1}^{(2)} \equiv -8$, $T_{r-1}^{(3)} \equiv 7$, $T_{r-1}^{(4)} \equiv 21$, $T_{r-1}^{(5)} \equiv -15$, $T_{r-1}^{(6)} \equiv -20$, $T_{r-1}^{(7)} \equiv 10$ *and* $T_{r-1}^{(8)} \equiv 5$;
(ii) $M \equiv -98, 38, 92, -69, 112, -35, -77$ *or* $-32 \pmod{229}$ *and, modulo* M, $T_{r-1}^{(1)} \equiv 1 \equiv T_{r-1}^{(9)}$, $T_{r-1}^{(2)} \equiv -8$, $T_{r-1}^{(3)} \equiv -7$, $T_{r-1}^{(4)} \equiv 21$, $T_{r-1}^{(5)} \equiv 15$, $T_{r-1}^{(6)} \equiv -20$, $T_{r-1}^{(7)} \equiv -10$ *and* $T_{r-1}^{(8)} \equiv 5$.

Proof. Let $L=\mathbb{Q}(\zeta_{19})$. Then $\mathrm{Norm}_{L/\mathbb{Q}}(\pi)=(\pi\bar{\pi})^{\sum_{i=1}^{9}\sigma_{2i-1}}=229$. Since $M\equiv -48,-44,15,-4,56,-55,-45,-61,26,49,-98,38,92,-69,112,-35$, -77 or $-32 \pmod{229}$, $n>1$, we get $\left(\frac{M}{\pi}\right)_{38}\equiv M^{(229-1)/38}=M^6\equiv -4,16,-64,-26,42,-15,60,-68,43,4,\ -42,\ 15,-60,-44,-53,-17\equiv \zeta_{19}$, ζ_{19}^2, ζ_{19}^3, ζ_{19}^6, ζ_{19}^8, ζ_{19}^{10}, ζ_{19}^{11}, ζ_{19}^{16}, ζ_{19}^{17}, $-\zeta_{19}$, $-\zeta_{19}^8$, $-\zeta_{19}^{10}$, $-\zeta_{19}^{11}$, $-\zeta_{19}^{13}$, $-\zeta_{19}^{14}$, $-\zeta_{19}^{15} \pmod{\pi}$ respectively. Notice that $26^6\equiv 49^6\equiv 43 \pmod{229}$ and $38^6\equiv 92^6\equiv -42 \pmod{229}$, which leads to the combination of 26 and 49, 38 and 92 respectively in the second congruence. So $\left(\frac{M}{\pi}\right)_{38}=\zeta_{19}$, ζ_{19}^2, ζ_{19}^3, ζ_{19}^6, ζ_{19}^8, ζ_{19}^{10}, ζ_{19}^{11}, ζ_{19}^{16}, ζ_{19}^{17}, $-\zeta_{19}$, $-\zeta_{19}^8$, $-\zeta_{19}^{10}$, $-\zeta_{19}^{11}$, $-\zeta_{19}^{13}$, $-\zeta_{19}^{14}$, $-\zeta_{19}^{15}\neq\pm1$ respectively. Here $F_{19}(x)=x^9+x^8-8x^7-7x^6+21x^5+15x^4-20x^3-10x^2+5x+1$, that is, $a_1=-1$, $a_2=-8$, $a_3=7$, $a_4=21$, $a_5=-15$, $a_6=-20$, $a_7=10$, $a_8=5$, $a_9=-1$. Hence all the assumptions of Theorem 3.1 are satisfied, giving the conclusion. ∎

5. Implementation and computational results. In this section we will verify the correctness of the algorithms related to Propositions 4.1 and 4.2. We denote $G_n=6^{2^n}+1$ and $H_n=10^{2^n}+1$. First we make some preparations for the case $p=5$. When $k\ge 0$, the recurrence sequences $T_{k+1}^{(j)}$, $j=1,2$, involved in Proposition 4.2 can be obtained as follows.

By the definition of $\alpha_1^{(k)}$ and $\alpha_2^{(k)}$, we have

$$\begin{aligned}
\alpha_1^{(k+1)} &= (\alpha_1^{(k)})^{10}-10(\alpha_1^{(k)})^8+35(\alpha_1^{(k)})^6-50(\alpha_1^{(k)})^4+25(\alpha_1^{(k)})^2-2,\\
\alpha_2^{(k+1)} &= \sigma_3(\alpha_1^{(k+1)})\\
&= (\alpha_2^{(k)})^{10}-10(\alpha_2^{(k)})^8+35(\alpha_2^{(k)})^6-50(\alpha_2^{(k)})^4+25(\alpha_2^{(k)})^2-2.
\end{aligned}$$

From the expressions for $T_k^{(1)}$ and $T_k^{(2)}$ in Proposition 4.2, after some computations we get

$$\begin{aligned}
T_{k+1}^{(1)} &= (T_k^{(1)})^{10}-10(T_k^{(1)})^8T_k^{(2)}+35(T_k^{(1)})^6(T_k^{(2)})^2-50(T_k^{(1)})^4(T_k^{(2)})^3\\
&\quad+25(T_k^{(1)})^2(T_k^{(2)})^4-10(T_k^{(1)})^8+80(T_k^{(1)})^6T_k^{(2)}-200(T_k^{(1)})^4(T_k^{(2)})^2\\
&\quad+160(T_k^{(1)})^2(T_k^{(2)})^3-20(T_k^{(2)})^4+35(T_k^{(1)})^6-210(T_k^{(1)})^4T_k^{(2)}\\
&\quad+315(T_k^{(1)})^2(T_k^{(2)})^2-70(T_k^{(2)})^3-50(T_k^{(1)})^4+200(T_k^{(1)})^2T_k^{(2)}\\
&\quad-100(T_k^{(2)})^2-2(T_k^{(2)})^5+25(T_k^{(1)})^2-50T_k^{(2)}-4
\end{aligned}$$

and

$$\begin{aligned}
T_{k+1}^{(2)} &= (T_k^{(2)})^{10}+20(T_k^{(2)})^9-10(T_k^{(1)})^2(T_k^{(2)})^8+170(T_k^{(2)})^8\\
&\quad-140(T_k^{(1)})^2(T_k^{(2)})^7+800(T_k^{(2)})^7+35(T_k^{(1)})^4(T_k^{(2)})^6\\
&\quad-800(T_k^{(1)})^2(T_k^{(2)})^6+2275(T_k^{(2)})^6+300(T_k^{(1)})^4(T_k^{(2)})^5
\end{aligned}$$

$$
\begin{aligned}
&- 2400(T_k^{(1)})^2(T_k^{(2)})^5 + 4004(T_k^{(2)})^5 - 50(T_k^{(1)})^6(T_k^{(2)})^4\\
&+ 1000(T_k^{(1)})^4(T_k^{(2)})^4 - 4050(T_k^{(1)})^2(T_k^{(2)})^4 + 4290(T_k^{(2)})^4\\
&- 200(T_k^{(1)})^6(T_k^{(2)})^3 + 1600(T_k^{(1)})^4(T_k^{(2)})^3 - 3820(T_k^{(1)})^2(T_k^{(2)})^3\\
&+ 2640(T_k^{(1)})^3 + 25(T_k^{(1)})^8(T_k^{(2)})^2 - 320(T_k^{(1)})^6(T_k^{(2)})^2\\
&+ 1275(T_k^{(1)})^4(T_k^{(2)})^2 - 1880(T_k^{(1)})^2(T_k^{(2)})^2 + 825(T_k^{(2)})^2\\
&+ 20(T_k^{(1)})^8T_k^{(2)} - 160(T_k^{(1)})^6T_k^{(2)} + 420(T_k^{(1)})^4T_k^{(2)}\\
&- 400(T_k^{(1)})^2T_k^{(2)} - 2(T_k^{(1)})^{10} + 20(T_k^{(1)})^8 - 70(T_k^{(1)})^6\\
&+ 100(T_k^{(1)})^4 - 50(T_k^{(1)})^2 + 100T_k^{(2)} + 4.
\end{aligned}
$$

With the above two recurrence formulas, we can easily obtain an explicit primality test for H_n.

We implemented two algorithms related to the special generalized Fermat numbers G_n and H_n in Magma [BCP] respectively. Our program was run on a personal computer with Intel Core i5-3470 3.20GHz CPU and 4GB memory.

We verified the correctness of our program by comparing with the results in [RE] and with some known facts for generalized Fermat numbers [WW]. Since G_n and H_n grow very fast with n, when $n \geq 15$ our personal computer ran out of memory. If we deal with a better and more efficient representation of larger integers, we may test the primality of larger G_n or H_n. However, this is not the focus of this paper. Finally we verified the numbers G_n and H_n related to the cases $p = 3$ and $p = 5$ respectively in the range $1 \leq n < 15$ and found no mistakes (see Tables 4 and 5). Note that the assumption on the congruence equation $x^4 \equiv 1 \pmod{5^r}$ in Proposition 4.2 holds for H_n, $1 \leq n < 15$, by applying the corresponding algorithm of [DL].

Table 4. Primality of $G_n = 6^{2^n} + 1$ ($p = 3$)

n	G_n	Primality	Time (sec.)
1	37	yes	0.011
2	1297	yes	0.015
3 to 10	-	no	0.921
11	-	no	3.931
12	-	no	23.228
13	-	no	139.293
14	-	no	738.805

Table 5. Primality of $H_n = 10^{2^n} + 1$ ($p = 5$)

n	H_n	Primality	Time (sec.)
1	101	yes	0.015
2 to 10	-	no	7.909
11	-	no	37.004
12	-	no	204.579
13	-	no	1180.226
14	-	no	6576.924

Acknowledgements. This work was supported by the NNSF of China (grant no. 11471314), 973 Project (2011CB302401) and the National Center for Mathematics and Interdisciplinary Sciences, CAS.

References

[AKS] M. Agrawal, N. Kayal and N. Saxena, *PRIMES is in P*, Ann. of Math. 160 (2004), 781–793.

[BB] P. Berrizbeitia 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 (1999), 1923–1925.

[BBT] P. Berrizbeitia, T. G. Berry and J. Tena, *A generalization of Proth's theorem*, Acta Arith. 110 (2003), 107–115.

[BOT] P. Berrizbeitia, M. Odreman and J. Tena, *Primality test for numbers* M *with a large power of* 5 *dividing* $M^4 - 1$, Theoret. Computer Sci. 297 (2003), 25–36.

[BCP] W. Bosma, J. Cannon and C. Playoust, *The Magma algebra system I. The user language*, J. Symbolic Comput. 24 (1997), 235–265.

[DL] Y. Deng and C. Lv, *Primality test for numbers of the form* $Ap^n + w_n$, J. Discrete Algorithms 33 (2015), 81–92.

[IR] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, 2nd ed., Grad. Texts in Math. 84, Springer, New York, 1990.

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

[LU] E. Lucas, *Théorie des fonctions numériques simplement périodiques*, Amer. J. Math. 1 (1878), 184–240, 289–321.

[RB] P. Ribenboim, *The New Book of Prime Number Records*, Springer, New York, 1996.

[RE] H. Riesel, *Some factors of the numbers* $G_n = 6^{2^n} + 1$ *and* $H_n = 10^{2^n} + 1$, Math. Comp. 23 (1969), 413–415; Corrigenda, ibid. 24 (1970), 243.

[WA] L. C. Washington, *Introduction to Cyclotomic Fields*, 2nd ed., Grad. Texts in Math. 83, Springer, New York, 1997.

[W1] H. C. Williams, *A note on the primality of* $6^{2^n}+1$ *and* $10^{2^n}+1$, Fibonacci Quart. 26 (1988), 296–305.

[W2] H. C. Williams, *Édouard Lucas and Primality Testing*, Canad. Math. Soc. Ser. Monogr. Adv. Texts 22, Wiley, New York, 1998.
[WW] http://www.prothsearch.net/GFNfacs.html.

Yingpu Deng, Dandan Huang (corresponding author)
Key Laboratory of Mathematics Mechanization, NCMIS
Academy of Mathematics and Systems Science
Chinese Academy of Sciences
100190, Beijing, P.R. China
E-mail: dengyp@amss.ac.cn
hdd@amss.ac.cn

Received on 11.6.2014 (7837)