PRIMALITY TESTS FOR $2^p \pm 2^{(p+1)/2} + 1$
USING ELLIPTIC CURVES

YU TSUMURA

(Communicated by Ken Ono)

Abstract. Using the properties of elliptic curves, we propose primality tests for integers of the form $2^p \pm 2^{(p+1)/2} + 1$, where $p$ is a prime number.

1. Introduction

Let us define the notation used in this paper.

Definition 1.1. Let $G_k = 2^{2k+1} + 2^{k+1} + 1$ and $H_k = 2^{2k+1} - 2^{k+1} + 1$, where $k$ is assumed to be a positive integer.

Noting that $G_k \cdot H_k = 2^{2(2k+1)} + 1$, it is easy to see that $G_k$ or $H_k$ can be prime only when $2k+1$ is a prime. Since our primality tests depend on $k$, we use the notation $G_k$ and $H_k$ rather than $2^p \pm 2^{(p+1)/2} + 1$, where $p$ is a prime number.

In this paper, we study group structures of elliptic curves defined over finite fields of order $G_k$, and $H_k$ (if they are prime). The essential role is the action of an endomorphism $[1 + i]$ on the curves. After that we use the information of the group structure to give primality tests for $G_k$ and $H_k$.

The original work in this direction was done by Benedict H. Gross in [3] for Mersenne numbers and by Robert Denomme and Gordan Savin in [2] for Fermat numbers and integers of the form $3^{2^k} - 3^{2^{k-1}} + 1$ and $2^{2^k} - 2^{2^{k-1}} + 1$, where $k$ is a positive integer. Gross used the formula of the multiplication by 2 as a recursive formula, and Denomme and Gordan used the formula of the action of $[1 + i]$ on the curves. After that we use the information of the group structure to give primality tests for $G_k$ and $H_k$.

The work in this direction was done by Benedict H. Gross in [3] for Mersenne numbers and by Robert Denomme and Gordan Savin in [2] for Fermat numbers and integers of the form $3^{2^k} - 3^{2^{k-1}} + 1$ and $2^{2^k} - 2^{2^{k-1}} + 1$, where $k$ is a positive integer. Gross used the formula of the multiplication by 2 as a recursive formula, and Denomme and Gordan used the formula of the action of $[1 + i]$ on the curves. After that we use the information of the group structure to give primality tests for $G_k$ and $H_k$.

Gross used the formula of the multiplication by 2 as a recursive formula, and Denomme and Gordan used the formula of the action of $[1 + i]$ on the curves. After that we use the information of the group structure to give primality tests for $G_k$ and $H_k$.

In this paper, we further apply the idea to the numbers $G_k$ and $H_k$. It is easy to see that exactly one of $G_k$ and $H_k$ can be prime only when $2k+1$ is a prime. Since our primality tests depend on $k$, we use the notation $G_k$ and $H_k$ rather than $2^p \pm 2^{(p+1)/2} + 1$, where $p$ is a prime number.

In this paper, we study group structures of elliptic curves defined over finite fields of order $G_k$, and $H_k$ (if they are prime). The essential role is the action of an endomorphism $[1 + i]$ on the curves. After that we use the information of the group structure to give primality tests for $G_k$ and $H_k$.

The original work in this direction was done by Benedict H. Gross in [3] for Mersenne numbers and by Robert Denomme and Gordan Savin in [2] for Fermat numbers and integers of the form $3^{2^k} - 3^{2^{k-1}} + 1$ and $2^{2^k} - 2^{2^{k-1}} + 1$, where $k$ is a positive integer. Gross used the formula of the multiplication by 2 as a recursive formula, and Denomme and Gordan used the formula of the action of $[1 + i]$ as a recursive formula for Fermat numbers. In this paper, we further apply the idea to the numbers $G_k$ and $H_k$. It is easy to see that exactly one of $G_k$ and $H_k$ can be prime only when $2k+1$ is a prime. Since our primality tests depend on $k$, we use the notation $G_k$ and $H_k$ rather than $2^p \pm 2^{(p+1)/2} + 1$, where $p$ is a prime number.

There are fast primality tests for $p = G_k$ and $p = H_k$. For example, one could use Corollary 1 or Theorem 5 of [1]. These tests apply because $p - 1$ is divisible by a power of 2 near $\sqrt{p}$. These tests determine the primality of $p$ of these three special forms in polynomial time. Our new tests below also run in polynomial time and are the first such tests for $G_k$ and $H_k$ using elliptic curves.
2. Group structure

The next theorem allows us to determine the order of certain elliptic curve groups.

**Theorem 2.1.** Let \( p \equiv 1 \pmod{4} \) be an odd prime and let \( m \not\equiv 0 \pmod{p} \) be a fourth power mod \( p \). Let \( E \) be an elliptic curve defined by \( y^2 = x^3 - mx \). Let \( p = a^2 + b^2 \), where \( a, b \) are integers with \( b \) even and \( a + b \equiv 1 \pmod{4} \). Let \( E(p) \) be the elliptic curve \( E \) defined over \( \mathbb{F}_p \). Then we have \( \#E(p) = p + 1 - 2a = (a - 1)^2 + b^2 \).

**Proof.** See Theorem 4.23, page 115, in [5]. \( \square \)

From now on, we fix an elliptic curve \( E : y^2 = x^3 - mx \), where \( m \not\equiv 0 \pmod{p} \) is a fourth power mod a prime \( p \). We denote by \( E(p) \) the elliptic curve group \( E \) defined over the finite field \( \mathbb{F}_p \) when \( p \) is prime. Also let \( E(\overline{\mathbb{F}}_p) \) be the elliptic curve \( E \) defined over the algebraic closure \( \overline{\mathbb{F}}_p \) of \( \mathbb{F}_p \), and we denote by \( E[n] \) the elements in \( E(\overline{\mathbb{F}}_p) \) whose orders divide \( n \).

**Corollary 2.2.**

1. If \( G_k \) is prime, then \( \#E(G_k) = 2^{2k+1} \).
2. If \( H_k \) is prime, then \( \#E(H_k) = 2^{2k+1} \).

**Proof.** Let \( a = 2^k + 1 \) and \( b = 2^k \). Then we have \( G_k = a^2 + b^2 \) and \( a + b \equiv 1 \pmod{4} \). Hence we have \( \#E(G_k) = G_k + 1 - 2(2^k + 1) = 2^{2k+1} \) by Theorem 2.1.

Similarly, let \( a = -(2^k - 1) \) and \( b = 2^k \). Then we have \( H_k = a^2 + b^2 \) and \( a + b \equiv 1 \pmod{4} \). Hence \( \#E(H_k) = H_k + 1 + 2(2^k - 1) = 2^{2k+1} \). \( \square \)

The next lemma gives information on the group structures of \( E(p) \) and \( E[n] \).

**Lemma 2.3.** Let \( E \) be an elliptic curve over a finite field \( \mathbb{F}_p \). Then we have

\[
E(p) \cong \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2}
\]

for some positive integers \( n_1 \) and \( n_2 \) with \( n_1 \mid n_2 \). Also, if \( n \) is a positive integer which is not divisible by \( p \), then we have

\[
E[n] \cong \mathbb{Z}_n \oplus \mathbb{Z}_n.
\]

**Proof.** See Theorem 3.1 and Theorem 4.1 in [5]. \( \square \)

Let \( p \) denote either \( G_k \) or \( H_k \). Suppose \( p \) is prime. By Corollary 2.2 and Lemma 2.3, the group structure is \( E(p) \cong \mathbb{Z}_2^\alpha \oplus \mathbb{Z}_2^\beta \) with \( \alpha \leq \beta \) and \( \alpha + \beta = 2k + 1 \). Since \( m \) is a 4th power, all the roots of \( x^3 - mx \) are in \( \mathbb{F}_p \) and also in the subgroup \( E[2] \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2 \) by Lemma 2.3. Then \( \mathbb{Z}_2 \oplus \mathbb{Z}_2 \cong E[2] \subset E(p) \), hence \( E(p) \) is not cyclic. However, we can determine the group structure of \( E(p) \) precisely. First we need two lemmas.

**Lemma 2.4.** Let \( n \) be a positive integer which is not divisible by a prime \( p \). Let \( \phi \) be the Frobenius endomorphism on \( E(\overline{\mathbb{F}}_p) \) given by \( \phi(x, y) = (x^p, y^p) \). Then \( E[n] \subset E(p) \) if and only if \( \phi - 1 \) is divisible by \( n \) in \( \text{End}(E) \).

**Proof.** See Lemma 1 in [4]. \( \square \)

**Lemma 2.5.** If \( \#E(p) = p + 1 - A \), then the Frobenius endomorphism \( \phi \) satisfies \( \phi^2 - A\phi + p = 0 \) as an endomorphism of \( E \).

**Proof.** See Theorem 4.10, page 101, in [5]. \( \square \)
Theorem 2.6. Suppose $G_k$ is prime. Then we have

$$E(G_k) \cong \mathbb{Z}_{2k} \oplus \mathbb{Z}_{2^{k+1}}.$$ 

Proof. From Corollary 2.4 we know that $\#E(G_k) = 2^{2k+1} = G_k + 1 - 2(2^k + 1)$. Hence the Frobenius endomorphism $\phi$ satisfies $\phi^2 - 2(2^k + 1)\phi + G_k = 0$. Then we have $(\phi - 1)^2 - 2^{k+1}(\phi - 1) + 2^{2k+1} = 0$. Since $\text{End}(E) \cong \mathbb{Z}[i]$ (see chapter 10 in [5]), it is a unique factorization domain. Therefore, $\phi - 1 = 2^k(1 \pm i)$. Hence $2^k$ divides $\phi - 1$, and we have $E[2^k] \subset E(G_k)$ by Lemma 2.4. Since $\#E[2^k] = 2^k$ and $\#E(G_k) = 2^{2k+1}$, the group structure of $E(G_k)$ must be $E(G_k) \cong \mathbb{Z}_{2k} \oplus \mathbb{Z}_{2^{k+1}}$ by Lemma 2.3. $\Box$

Theorem 2.7. Suppose $H_k$ is prime. Then we have

$$E(H_k) \cong \mathbb{Z}_{2k} \oplus \mathbb{Z}_{2^{k+1}}.$$ 

Proof. Just note that the Frobenius endomorphism satisfies $\phi^2 + 2(2^k - 1)\phi + H_k = 0$. Hence $\phi - 1 = (-1 \pm i)2^k$. The rest of the proof is identical to that of Theorem 2.6. $\Box$

3. PRIMALITY TEST

Again let $p$ be either $G_k$ or $H_k$. As we noted in the proof of Theorem 2.6, $E$ has complex multiplication by $\mathbb{Z}[i]$. For a detailed explanation about complex multiplication, see chapter 10 in [5]. The action of $i$ on $(x, y) \in E$ is given by $[i] \cdot (x, y) = (-x, iy)$, where the $i$ in $(-x, iy)$ is a 4th root of unity in $\mathbb{F}_p$ (if $p$ is prime). This $i$ exists in $\mathbb{F}_p$ since $p \equiv 1 \pmod{4}$. Explicitly $i = 2^{k+1} + 1$ for $G_k$ and $i = 2^{k+1} - 1$ for $H_k$. Note that as an endomorphism, $i$ has degree 1 and hence it is an isomorphism. Now, let us denote $\eta = 1 + i$ in $\text{End}(E)$. This endomorphism is very important in this paper. Let us describe the action of $\eta$ on $(x, y)$ explicitly. Let $\eta \cdot (x, y) = (x', y')$. We have

$$\eta \cdot (x, y) = [1 + i] \cdot (x, y) = (x, y) + [i] \cdot (x, y) = (x, y) + (-x, iy),$$

and by the elliptic curve addition it is equal to

$$\left(\frac{(1 - i)y}{2x}, y'\right)$$

and

$$\left(\frac{x^2 - m}{2ix}, y'\right),$$

where $y' = \left(\frac{(1-i)y}{2x}\right)(x - x') - y$. Note that by equation (3.1), the $x$-coordinate $x'$ of $\eta \cdot (x, y)$ is a square and by equation (3.2), $x'$ can be computed without using $y$. Also note that $\eta$ has degree 2, hence $\#\ker(\eta) = 2$. Clearly, $(0, 0)$ is in the kernel, and so $\ker(\eta) = \{\infty, (0, 0)\}$, where $\infty$ is the identity of $E$.

Note that $\eta^2 = 2i$ and $\eta^2 = c^2i$, where $i$ is a positive integer and $\epsilon = \pm 1, \pm i$. Since $\epsilon = \pm 1, \pm i$ are isomorphisms, we do not care about these factors. We will use $\epsilon$ for $\pm 1, \pm i$ in this paper, but $\epsilon$ might have different values at each occurrence.
3.1. Primality test for $2^{2k+1}+2^{k+1}+1$.

**Theorem 3.1.** Let $k \geq 2$ be an integer and $m$ be a square integer. Let $P = (x,y) \in \mathbb{Z} \times \mathbb{Z}$ be a point satisfying $y^2 = x^3 - mx \mod G_k$. Also assume that we know beforehand that when $G_k$ is prime, $x$ is a quadratic non-residue mod $G_k$ and $m$ is a 4th power mod $G_k$. Let $x_0 = x$ and let $x_j = (x_{j-1}^2 - m)/(2x_{j-1}) \mod G_k$ with $i = 2^{k+1} + 1$ if $\gcd(x_{j-1}, G_k) = 1$ for $j \geq 1$ inductively mod $G_k$. Then $G_k$ with $k \geq 2$ is prime if and only if

$$\tag{3.3} \begin{cases} \gcd(x_{j-1}, G_k) = 1 & \text{for } j = 1, 2, \ldots, 2k - 1, \\ x_{2k-1} \in \{ \pm \sqrt{m}, 0 \}. \end{cases}$$

**Proof.** Suppose $G_k$ is prime. We consider the elliptic curve $E(G_k)$ and show that $\eta^{2k-1}P \in E[2] \setminus \{ \infty \}$. We have seen that $\phi - 1 = c\eta^{2k} = \epsilon\eta^{2k+1}$ in the proof of Theorem 2.6. Hence we have $E(G_k) = \text{Ker}(\phi - 1) = \text{Ker}(\eta^{2k+1})$. Since $\# \text{Ker}(\eta) = 2$ and $\# E(G_k) = 2^{2k+1}$, it is easy to see that $\text{Ker}(\eta^s) = \text{Im}(\eta^{2k+1-s})$, for $s = 0, 1, \ldots, 2k+1$. Taking $s = 2$, we see that $\eta^{2k-1}P \in E[2]$. Assume $\eta^{2k-1}P = \infty$. Then it follows that $P \in \text{Ker}(\eta^{2k-1}) = \text{Im}(\eta^2)$ (the case when $s = 2k - 1$). Since the $x$-coordinate $x$ of $P$ is square by hypothesis, $P$ is not in the image of $\eta$. Hence this is a contradiction. Therefore $\eta^{2k-1}P \neq \infty$.

We proved that $\eta^{2k-1}P \in E[2] \setminus \{ \infty \}$, and this is equivalent to condition (3.3) since $x_j$ is the $x$-coordinate of $\eta^j P$.

Conversely, suppose condition (3.3). Assume $G_k$ is composite and let $q$ be a prime divisor of $G_k$ such that $q \leq \sqrt{G_k}$. Then $P$ is a point on $E(q)$, and we have

$$\begin{cases} \gcd(x_{j-1}, q) = 1 & \text{for } j = 1, 2, \ldots, 2k - 1, \\ x_{2k-1} \in \{ \pm \sqrt{m}, 0 \}. \end{cases}$$

This implies that $\eta^{2k-1}P \in E(q)[2] \setminus \{ \infty \}$. Then $\eta^{2k-1}P$ is one of $(0, 0)$ or $(\pm \sqrt{m}, 0) \in E(q)$. If $\eta^{2k-1}P = (0, 0)$, then we have $2^{k-1}P = \eta^{2k-2}P \neq \infty$ and $2^2P = \eta^{2k}P = \infty$. Therefore $P$ has order $2^k$. If $\eta^{2k-1}P = (\sqrt{m}, 0)$, then let $P' = \eta P$. Then we have $\eta^{2k-1}P' = \eta(\sqrt{m}, 0) = (0, 0)$. This is the same situation as the case $\eta^{2k-1}P = (0, 0)$; hence $P'$ has order $2^k$. The case $\eta^{2k-1}P = (-\sqrt{m}, 0)$ is similar, and $\eta P$ has order $2^k$. We have seen in any case that there exists a point $(P$ or $\eta P)$ of order $2^k$. Let $R$ denote this point. Let us assume that $\{ R, iR \}$ is a basis for $E[2]$. Since $iR \in E(q)$ (note that $i$ is just an integer), we have $E[2^k] \subset E(q)$. Therefore we have

$$2^{2k} = \# E[2^k] \leq \# E(q) \leq (\sqrt{q} + 1)^2 \leq (G_k^{1/4} + 1)^2.$$ 

The second inequality follows from Hasse's inequality. However, this inequality does not hold for $k \geq 2$, and therefore $G_k$ is prime.

To complete the proof, we need to show that $\{ R, iR \}$ is a basis for $E[2^k]$. Suppose $uR + v(iR) = \infty$ for some integers $u, v$. Let $u = 2^u u'$ and let $v = 2^v v'$ with $u', v'$ odd. Since the order of $R$ is a power of 2, we have $\alpha = \beta$. Now $(u' + v'i)(2^\alpha R) = \infty \Rightarrow (u'^2 + v'^2)(2^{2^\alpha} R) = \infty \Rightarrow u'^2 + v'^2 \equiv 0 \pmod{2^{k-\alpha}}$. Since $u'^2 + v'^2 \equiv 2 \pmod{4}$, the above congruence holds only if $\alpha = k$ or $\alpha = k - 1$. If $\alpha = k$, then $u \equiv v \equiv 0 \pmod{2^k}$, and hence they are independent.
Next, let us consider the case \( \alpha = k - 1 \). Let \( R' = 2^{k-1}R \). Then \( R' \) has order 2. Hence \( R' \) is either \((0,0)\) or \((\pm\sqrt{m},0)\). However, we have \( \eta R' = \eta \cdot (\eta^{2k-2})R = \eta^{2k-1}R \)

\[
\eta^{2k-1}P \neq \infty \quad \text{if } R = P,
\]

\[
\eta \cdot \eta^{2k-1}P = \eta(1 \pm \sqrt{m},0) = (0,0) \neq \infty \quad \text{if } R = \eta P.
\]

Hence \( R' \neq (0,0) \). Therefore \( R' \) is either \((\sqrt{m},0)\) or \((-\sqrt{m},0)\). If \( R' = (\sqrt{m},0) \), then \( \infty = (u'+v')((\sqrt{m},0) = u'((\sqrt{m},0) + v'(-\sqrt{m},0) \) with odd \( u', v' \). Since \( \{(\sqrt{m},0),(-\sqrt{m},0)\} \) is a basis for \( E[2] \), they cannot be dependent with odd coefficients. The same thing happens when \( R' = (-\sqrt{m},0) \). Therefore, \( R \) and \( iR \) are independent. \( \square \)

To use Theorem 3.2, we need to find a point \( P \) on \( E \) satisfying the condition of the theorem. It is straightforward to check the following. Suppose \( G_k \) is prime.

- 3 is a quadratic non-residue mod \( G_k \) if and only if \( k \) is even.
- 5 is a quadratic non-residue mod \( G_k \) if and only if \( k \equiv 1 \pmod{4} \). Also if \( k \equiv 0, 3 \pmod{4} \), then \( G_k \) is divisible by 5.
- 7 is a quadratic non-residue mod \( G_k \) for all \( k \geq 1 \).

Using these facts, we can choose specific initial values depending on \( k \). Since \( G_k \) is composite when \( k \equiv 0, 3 \pmod{4} \) from the above fact, we only need to consider the cases when \( k \equiv 1 \pmod{4} \) and \( k \equiv 2 \pmod{4} \).

When \( k \equiv 2 \pmod{4} \), we take \( m = 21^2 \) and \( P = (3, 36i) \) satisfying \( y^2 = x^3 - 21^2x \mod G_k \), where \( i = 2^{k+1} + 1 \). (It is easy to see that \( i^2 \equiv -1 \pmod{G_k} \).) Note that when \( G_k \) is prime, we see that \( x = 3 \) is a quadratic non-residue mod \( G_k \) and \( m = 21^2 \) is a 4th power mod \( G_k \) since both 3 and 7 are quadratic non-residues mod \( G_k \) and hence 21 is a square mod \( G_k \). So \( P \) satisfies the condition of Theorem 3.1.

When \( k \equiv 1 \pmod{4} \) and \( k > 1 \), we can take \( m = 70^2 \) and \( P = (20, 300i) \) satisfying \( y^2 = x^3 - 70^2x \mod G_k \). Note that when \( G_k \) is prime, one sees that \( x = 20 = 2^2 \cdot 5 \) is a quadratic non-residue by the above fact and \( m = 70^2 \) is a 4th power since \( 70 = 2 \cdot 5 \cdot 7 \) is a quadratic residue mod \( G_k \) since 2 is a quadratic residue (because \( G_k \equiv 1 \pmod{8} \)) and 5 and 7 are quadratic non-residues from the above facts. Hence \( P \) satisfies the condition of Theorem 3.1.

3.1.1. The algorithm for \( G_k \). Then the algorithm to check the primality of \( G_k \) is as follows. Take a positive integer \( k \geq 2 \) such that \( 2k + 1 \) is a prime. Let \( x_0 = 3, m = 21^2 \) when \( k \equiv 2 \pmod{4} \) and \( x_0 = 20, m = 70^2 \) when \( k \equiv 1 \pmod{4} \). Then let \( i = 2^{k+1} + 1 \) and let \( x_j = (x_{j-1}^2 - m)/(2ix_{j-1}) \mod G_k \) if \( \gcd(x_{j-1}, G_k) = 1 \) for \( j \geq 1 \) inductively mod \( G_k \). If \( \gcd(x_{j-1}, G_k) > 1 \) for some \( j < 2k - 1 \), then \( G_k \) is composite and we terminate the algorithm. If we calculate \( x_{2k-1} \) and this is \( \pm\sqrt{m} \) or 0, then \( G_k \) is prime. Otherwise, \( G_k \) is composite.

3.2. Primality test for \( 2^{2k+1} - 2k + 1 + 1 \). Now let us discuss \( H_k = 2^{2k+1} - 2k + 1 + 1 \). By Theorem 2.2, we know that \( \phi - 1 = \eta^{2k+1} \). Therefore the proof of the next theorem is identical to that of Theorem 3.1.

**Theorem 3.2.** Let \( k \geq 2 \) be an integer and \( m \) be a square integer. Let \( P = (x, y) \in \mathbb{Z} \times \mathbb{Z} \) be a point satisfying \( y^2 = x^3 - mx \mod H_k \). Also assume that we know beforehand that when \( H_k \) is prime, \( x \) is a quadratic non-residue mod \( H_k \) and \( m \) is a 4th power mod \( H_k \). Let \( x_0 = x \) and let \( x_j = (x_{j-1}^2 - m)/(2ix_{j-1}) \) mod \( H_k \).
with \( i = 2^{k+1} - 1 \) if \( \gcd(x_{j-1}, H_k) = 1 \) for \( j \geq 1 \) inductively mod \( H_k \). Then \( H_k \) with \( k \geq 2 \) is prime if and only if

\[
(3.4) \quad \begin{cases} 
\gcd(x_{j-1}, H_k) = 1 & \text{for } j = 1, 2, \ldots, 2k - 1, \\
x_{2k-1} \in \{\pm \sqrt{m}, 0\}.
\end{cases}
\]

Again to use Theorem 3.2, we need to find a point \( P \) satisfying the condition of the theorem. The following is easy to check. Suppose \( x \equiv 2 \pmod{12} \) and \( k \equiv 3 \pmod{4} \). Hence when \( k \equiv 1, 2 \pmod{4} \), 5 divides \( H_k \).

- 3 is a quadratic non-residue mod \( H_k \) if and only if \( k \) is odd.
- 5 is a quadratic non-residue mod \( H_k \) if and only if \( k \equiv 3 \pmod{4} \). Also when \( k \equiv 1, 2 \pmod{4} \), 5 divides \( H_k \).
- When \( k \equiv 4 \pmod{12} \), 13 divides \( H_k \).

Hence when \( k \equiv 3 \pmod{4} \), we can take \( m = 30^2 \) and a point \((6, 72i)\), where \( i = 2^{k+1} - 1 \). The remaining cases are when \( k \equiv 0, 8 \pmod{12} \); otherwise 5 or 13 divides \( H_k \). However, it seems difficult to find a suitable small value. Instead, if we increase the modulus, we might find other points satisfying the conditions.

Once we have set an initial value, then the algorithm to check the primality of \( H_k \) is the same as the algorithm of Section 3.1 for \( G_k \). Simply replace the initial value and replace \( G_k \) by \( H_k \) and use \( i = 2^{k+1} - 1 \).

4. Examples

Let us see some examples of the algorithm of Section 3.1 for the primality tests of \( G_k \) and \( H_k \). We begin with \( G_k \), where \( k \equiv 2 \pmod{4} \). In this case, \( x_0 = 3, m = 21^2 \) and \( i = 2^{k+1} + 1 \). First take \( k = 2 \). Then \( 2k+1 = 5 \) is a prime. We calculate \( x_0 = 3 \) and \( x_j = (x_{j-1}^2 - 21^2)/(2ix_{j-1}) \) mod \( G_2 \) inductively for \( j \leq 2k - 1 = 3 \). Then we have \( \{x_j\}_{j=0}^{k=3} = \{3, 33, 16, -21\} \). Hence we have \( x_3 = -21 = -\sqrt{m} \) and conclude that \( G_2 = 41 \) is a prime.

Next, take \( k = 6 \equiv 2 \pmod{4} \). Then \( 2k + 1 = 13 \) is a prime. We calculate \( x_0 = 3 \) and \( x_j = (x_{j-1}^2 - 21^2)/(2ix_{j-1}) \) mod \( G_6 \) inductively for \( j \leq 2k - 1 = 11 \). Then we have \( \{x_j\}_{j=0}^{k=11} = \{3, 967, 7840, \ldots, 7840, 4999\} \). Hence \( x_{11} = 4999 \neq 0, \pm 21 \pmod{G_6} \), and we conclude that \( G_6 = 8321 = 53 \cdot 157 \) is not a prime.

Let us consider examples for \( H_k \), where \( k \equiv 3 \pmod{4} \). In this case, \( x_0 = 6, m = 30^2 \) and \( i = 2^{k+1} - 1 \). Take \( k = 3 \). Then \( 2k + 1 = 7 \) is a prime. Now we calculate \( x_0 = 6 \) and \( x_j = (x_{j-1}^2 - 30^2)/(2ix_{j-1}) \) mod \( H_3 \) inductively for \( j \leq 2k - 1 = 5 \). Then we have \( \{x_j\}_{j=0}^{k=5} = \{6, 63, 14, 22, 111, 30\} \). Hence \( x_5 = 30 = \sqrt{m} \), and we conclude that \( H_3 = 113 \) is a prime.

Finally, let \( k = 11 \equiv 3 \pmod{4} \). Then \( 2k + 1 = 23 \) is a prime. Then we calculate \( x_{21} = 999883 \neq 0, \pm 30 \pmod{H_{11}} \) and conclude that \( H_{11} = 8384513 \) is not a prime. Actually we have \( H_{11} = 8384513 = 277 \cdot 30269 \).

5. Fermat Numbers

The method we used here for \( G_k \) and \( H_k \) also applies to Fermat numbers \( 2^{2^k} + 1 \). Although the proof is slightly different, the result was already proved by Robert Denomme and Gordan Savin in [2]. Therefore we do not repeat it here.

Also Fermat numbers and \( G_k \) and \( H_k \) are the only numbers to which this method applies. This can be seen by considering the solution \( a, b \) with \( p = a^2 + b^2 \) of \( (a - 1)^2 + b^2 = 2^n \), where \( n \) is a positive integer. See Theorem [2,1]
As we noted in the introduction, Gross used the formula of the multiplication by 2 as a recursive formula, and Denomme and Gordan used the formula of the action of \([1 + i] \) as a recursive formula for Fermat numbers. It is not difficult to convert the primality test for Fermat numbers using the formula of the action of \([1 + i] \) to the primality test using the formula of multiplication by 2. For the proof of this fact as well as the proof of the primality test using the method in this paper, see the author’s note on the arXiv (arXiv:0912.2116v1).

Acknowledgments

The author would like to thank Professor Samuel Wagstaff for his corrections of English language errors in the paper. The author is also grateful to the referee for suggestions.

References


Department of Mathematics, Purdue University, 150 North University Street, West Lafayette, Indiana 47907-2067