Journal of Integer Sequences, Vol. 20 (2017),
Article 17.2.7

On the Exponents of Non-Trivial Divisors of Odd Numbers and a Generalization of Proth's Primality Theorem

Tom Müller
Institut für Cusanus-Forschung
University and Theological Faculty of Trier
Domfreihof 3
54290 Trier
Germany
mueller2887@t-online.de

Abstract

We present a family of integer sequences characterizing the behavior of the quotients σ/s for a given odd natural number H, where $N = H \cdot 2^\sigma + 1$ is a composite number and $h \cdot 2^s + 1$ ($h \geq 1$ odd, $s, \sigma \in \mathbb{N}$) is a non-trivial divisor of N. As an application we prove a generalization of the primality theorem of Proth.

1 Introduction

For every odd natural number $N > 1$ there exists an unique pair (H, σ) with H an odd natural number, $\sigma \in \mathbb{N}$ and $N = H \cdot 2^\sigma + 1$. In this parametric notation, we call H the *multiplier* of N and σ the *exponent* of N. Here and subsequently, the notation $A \cdot 2^\alpha + 1$ always means that A is the multiplier and α the exponent of the represented odd natural number. For a given natural number $N > 1$ we let $\mathcal{D}(N)$ denote the set of the non-trivial divisors of N, i.e., the set of all natural numbers d fulfilling $1 < d < N$ and $d|N$. Obviously, N is a prime number if and only if $\mathcal{D}(N) = \emptyset$.

The aim of this paper is to introduce and study a family of integer sequences characterizing the behavior of the quotient $\frac{\sigma}{s}$ for a given H, where $N = H \cdot 2^\sigma + 1$ is a composite number and $h \cdot 2^s + 1 \in \mathcal{D}(N)$. These sequences can be used to give a generalization of the well-known primality theorem of Proth.

If the exponent s is large compared to σ, then there must exist a rather small real number $m > 0$ with $m \geq \frac{\sigma}{s}$. All the values of σ fulfilling this inequality for a given odd natural number H are elements of the following set:

$$S_m(H) := \left\{\sigma \in \mathbb{N} \,|\, \exists d = h \cdot 2^s + 1 \in \mathcal{D}(H \cdot 2^\sigma + 1) : m \geq \frac{\sigma}{s}\right\}. \tag{1}$$

With this we define the integer sequence

$$\sigma_m(H) := \sup\left(S_m(H)\right).$$

As usual, we adopt the conventions that $\sup(\emptyset) = 0$ and $\sup(A) = \infty$ if $|A| = |\mathbb{N}|$. The aforementioned definitions immediately imply $S_k(H) \subset S_l(H)$ and hence $\sigma_k(H) \leq \sigma_l(H)$ if $k < l$.

2 The σ_m-sequences

2.1 Diophantine equations

Definition (1) leads to a general Diophantine equation, which allows to determine the elements of $S_m(H)$ for a given $m \geq 1$. Suppose $N = H \cdot 2^\sigma + 1 = AB$ to be composite with two non-trivial divisors $A = h \cdot 2^r + 1$ and $B = k \cdot 2^s + 1$. Without loss of generality we can denote A and B such that $1 \leq r \leq s$. It follows that

$$AB = 2^r\left(2^s hk + 2^{s-r}k + h\right) + 1 = 2^\sigma H + 1 = N.$$

This is equivalent to the Diophantine equation

$$2^s hk + 2^{s-r}k + h = 2^{\sigma-r}H. \tag{2}$$

Note that $r \leq s \in \mathbb{N}$ and that h and k are odd natural numbers. To reflect the condition $m \geq \frac{\sigma}{s}$ of the definition we may include a supplementary parameter n in order to write $\lfloor ms \rfloor - n = \sigma$. In general, n can take any integer value between 0 and $\lfloor ms \rfloor - 1$. For practical purposes it is useful to demand for further restrictions, which render the computations more comfortable.

If $m = 1$ then we get $r = \sigma < s$. Therefore, (2) turns into

$$2^s hk + 2^{s-r}k + h = H. \tag{3}$$

It is easy to see that for $H \in \{1, 3\}$ equation (3) has no solution (under the abovementioned assumptions). Hence $\sigma_1(1) = \sigma_1(3) = 0$. For $H > 3$ the estimate $\sigma < s \leq \log_2(H)$ obviously holds. This gives $\sigma_1(H) \leq \lfloor \log_2(H) \rfloor - 1$ for all $H \geq 3$. In fact, this estimate is best possible in the sense that there are infinitely many values of H for which we actually have $\sigma_1(H) = \lfloor \log_2(H) \rfloor - 1$. We will establish this in subsection 2.3.

It is immediate that by explicitly giving a solution (r, s, h, k, H) of (3), we get the lower bound $\sigma_1(H) \geq r$.

Example 1. Because $8 \cdot \frac{10^n-1}{9} + 2 \cdot \frac{10^n-1}{9} + 1 = \frac{10^{n+1}-1}{9}$, we have $\sigma_1\left(\frac{10^{n+1}-1}{9}\right) \geq 2$ for all natural numbers n.

Remark 2. Since $\sigma_1(H) < \infty$ for every odd natural number H it is obvious that $\sigma_m(H) < \infty$ for every $0 < m < 1$. Because of $S_m(H) \subset S_1(H)$, the value of $\sigma_m(H)$ can thus explicitly be calculated by examining the elements of $S_1(H)$.

Note that for $m > 1$ we already get $r = s < \sigma$ in the Diophantine equation (2). Therefore, the Diophantine equation to consider concerning $\sigma_2(H)$ reads

$$2^s hk + h + k = 2^{\sigma-s} \cdot H \tag{4}$$

with the supplementary condition $2s \geq \sigma$, i.e., $s \geq \sigma - s$. For computational reasons we will deal with another Diophantine equation in this context:

$$2^s hk + h + k = 2^{s-n} \cdot H \tag{5}$$

with $h \leq k$ odd and $0 \leq n < s$. Note that (5) follows from (4) by setting $2s = \sigma + n$. The solutions (n, s, h, k, H) of (5) yield the elements $\sigma = 2s - n \in S_2(H) \setminus S_1(H)$. Some simple but very useful results can be derived from this Diophantine equation. First, (5) implies $2^n hk < H$, showing that $\sigma_2(H) < \infty$ for every odd H. In subsection 2.4 we will give a best possible upper bound of the values of $\sigma_2(H)$. Again, by explicitly giving a solution (n, s, h, k, H) of (5), we get the lower bound $\sigma_2(H) \geq 2s - n$.

Example 3. Since $4(8 \cdot 10^w - 1) + 8 \cdot 10^w = 4(10^{w+1} - 1)$, we see that $\sigma_2(10^{w+1} - 1) \geq 4$ for all natural numbers w.

For $m = 3$ there is also a condition for existence, limiting the value of n in the Diophantine equation

$$2^s hk + h + k = 2^{2s-n} \cdot H, \tag{6}$$

where $h \leq k$ are odd natural numbers and $0 \leq n < s$. Note that (n, s, h, k, H) is a solution of equation (6) if and only if the corresponding $\sigma = 3s - n$ is an element of $S_3(H) \setminus S_2(H)$.

Now consider such a solution (n, s, h, k, H). By equation (6) we get $h + k \equiv 0 \pmod{2^s}$, i.e., $h + k = 2^s \cdot d$ for an appropriate natural number d. Moreover, there exists a natural number a with $a + n = s$, i.e., $2s - n = s + a$. Then $hk = 2^a H - d \leq 2^a H - 1$. This implies $h + k \leq hk + 1 \leq 2^a H \leq 2^s H$ and hence $2^s = \frac{h+k}{2^a H - hk} \leq 2^a H$. Finally, he have $2^n = 2^{s-a} \leq H$, yielding $n \leq \log_2(H)$.

Remark 4. This condition of existence already implies that $\sigma_m(H) < \infty$ for every odd H and $m \in (2, 3)$. To see this, suppose $\sigma \in S_m(H) \setminus S_2(H) \subset S_3(H) \setminus S_2(H)$ for a $m \in (2, 3)$. This means that the corresponding s leads to a solution in (6) and hence fulfils the inequality $s \leq \frac{\sigma + \log_2(H)}{3}$. Consequently, σ satisfies $\frac{\sigma}{m} \leq \frac{\sigma + \log_2(H)}{3}$ which is equivalent to

$$\sigma \leq \frac{m \log_2(H)}{3 - m}. \tag{7}$$

Since $\sigma_2(H) < \infty$, we can conclude with inequality (7) that $\sigma_m(H)$ is finite as well.

2.2 Some elementary primality results

Proposition 5. *Let m be a natural number and $H \geq 1$ be an odd number such that $\sigma_m(H) = 0$. Then $N := H \cdot 2^m + 1$ is a prime number.*

Proof. The number $N = H \cdot 2^m + 1$ is either prime or it has a non-trivial divisor of the form $h \cdot 2^r + 1$ with $r \geq 1 = \frac{\sigma}{m}$. The latter case would imply $\sigma_m(H) \geq m > 0$. $\square$

Corollary 6. *Let $H \geq 1$ be an odd number. Let l be a nonnegative integer number and m be a natural number with $\sigma_m(H) = l < m$. Then $N := H \cdot 2^\sigma + 1$ is a prime number for every $\sigma \in [l+1, m] \cap \mathbb{N}$.*

Proof. For $m = 1$ this is exactly the claim of Proposition 5. For $m > 1$ we know that $r = s < \sigma$ if there are non-trivial divisors $A := h \cdot 2^r + 1$ and $B := k \cdot 2^s + 1$ of N such that $AB = N$. But this leads to $m > s \geq 1 \geq \frac{\sigma}{m}$ and hence $\sigma_m(H) \geq \sigma > l$. $\square$

Corollary 7. *Let H be an odd natural number and let $m \geq 1$ be a real number. If the natural number $\sigma \leq m$ is not an element of $S_m(H)$ then $N = H \cdot 2^\sigma + 1$ is a prime number.*

Proof. Let $N = H \cdot 2^\sigma + 1 = AB$ be a composite number with $\sigma \leq m$. As usual, write $A = h \cdot 2^r + 1$ and $B = k \cdot 2^s + 1$ with $r \leq s$. Now suppose that σ is not an element of $S_m(H)$. Then we have $s < \frac{\sigma}{m} \leq 1$, contradicting the condition $1 \leq s$. $\square$

2.3 Special values of σ_1

Theorem 8. *Let l and $m \geq l+1$ be natural numbers. Then $\sigma_1(2^m + 2^l + 1) \geq m - l$.*

Proof. Under the conditions of the theorem, $(r, s, h, k, H) = (m - l, m, 1, 1, 2^m + 2^l + 1)$ is a solution of (3). $\square$

Theorem 9. *Let $m \geq 2$ be a natural number. Then $\sigma_1(2^m + 3) = m - 1$.*

Proof. For every $H > 1$ we know that $\sigma_1(H) \leq \lfloor \log_2(H) \rfloor - 1$. Therefore, $\sigma_1(2^m + 3) \leq m - 1$ for all $m \geq 2$. The claim follows with Theorem 8. $\square$

On the one hand, Theorem 9 shows that for every $H = 2^m + 3$ $(m \geq 2)$ the best possible value $\sigma_1(H) = \lfloor \log_2(H) \rfloor - 1$ is actually reached. On the other hand, we can conclude that the arithmetical function $\sigma_1 : \mathbb{N} \setminus 2\mathbb{N} \to \mathbb{N}_0$ is surjective.

Theorem 10. *Let $m \geq 3$ be a natural number. Then $\sigma_1(2^m + 5) = m - 2$.*

Proof. Theorem 8 gives $\sigma_1(2^m + 5) \geq m - 2$ for all $m \geq 3$. Moreover, $\sigma_1(2^m + 5) \leq \lfloor \log_2(H) \rfloor - 1 = m - 1$ for all $m \geq 3$. Suppose that there were a solution of (3) yielding $\sigma = m - 1$. This solution would have to be of the form $2^m hk + 2k + h = 2^m + 5$, since $s \leq \log_2(H)$. But for $h = k = 1$ we have $2^m + 2 + 1 < 2^m + 5$, whereas for $\max\{h, k\} > 1$ there is $2^m + 5 < 2^m hk + 2k + h$. Thus, such a solution does not exist. $\square$

Remark 11. The sequence $(a(n))_{n \geq 0}$ with $a(n) = \sigma_1(2n + 1)$ is sequence A272894 of the OEIS.

2.4 Special values of σ_2

Theorem 12. *Let m be a natural number and let H be an odd natural number with $H < 2^m$. Then $\sigma_2(H) \leq 2m - 1$.*

Proof. We already know that $\sigma_1(H) \leq \log_2(H) < m$, so we do not have to consider the solutions of (3) here. Given the Diophantine equation (5), we see that $h + k \equiv 0 \pmod{2^{s-n}}$, i.e., there is a natural number d with $h + k = d \cdot 2^{s-n}$. This implies $2^n hk = H - d \leq 2^m - 2$ or

$$hk \leq \frac{2^m - 2}{2^n}. \tag{8}$$

First, if $n = 0$ then (8) gives

$$h + k \leq hk + 1 \leq 2^m - 1 < 2^m.$$

Consequently, a transformation of the Diophantine equation (5) leads to

$$2^s = \frac{h + k}{H - hk} < 2^m,$$

since $H - hk$ is a natural number. So, here we have $s < m$, i.e., $s \leq m - 1$ and hence $\sigma \leq 2m - 2$.

Secondly, for $n \geq 1$, again with (8), we get

$$h + k \leq hk + 1 \leq 2^{m-n} + 1 - \frac{1}{2^{n-1}}.$$

This means that the even natural number $h + k$ always fulfils $h + k \leq 2^{m-n}$. In the present case, the Diophantine equation (5) can be changed into

$$2^{s-n} = \frac{h + k}{H - 2^n hk} \leq 2^{m-n}$$

with a natural denominator $H - 2^n hk$, giving the estimations $s \leq m$ and $\sigma \leq 2m - n$. The maximal value of the latter expression obviously is $2m - 1$. Therefore, $\sigma_2(H) \leq 2m - 1$ for every $H < 2^m$. □

Moreover, the arguments H leading to maximal values of $\sigma_2(H)$ can be specified.

Theorem 13. *Let $m \geq 2$ be a natural number and let H be an odd natural number with $H < 2^m$. Then $\sigma_2(H) = 2m - 1$ if and only if $H = 2^m - 1$.*

Proof.
(1) If $H = 2^m - 1$ with $m \geq 2$ then the Diophantine equation (5) has the solution $(n, s, h, k) = (1, m, 1, 2^{m-1} - 1)$ and consequently $\sigma_2(H) = 2m - 1$.

(2) Suppose that $\sigma_2(H) = 2m - 1$ for a $H < 2^m$. The Diophantine equation $h + k = hk + 1$ (under the assumption that $1 \leq h \leq k$) implies $h = 1$. So, if $3 \leq h \leq k$, then we have

$h+k<hk$. Note that $h+k=hk$ is impossible for every odd k. Applying (8) we can assert that

$$h+k<hk\le\frac{2^m-2}{2^n}<2^{m-n}$$

for $3\le h\le k$ and $H<2^m$. Hence $2^{s-n}<2^{m-n}$. This leads to $s\le m-1$ and $\sigma\le 2m-2-n\le 2m-2$.

It follows that $\sigma=2m-1$ requires $h=1$, $n=1$ and $s=m$. Then (5) can be rewritten as

$$2^m k+k+1=2^{m-1}H,$$

or

$$k+1=2^{m-1}(H-2k). \tag{9}$$

As seen above, we have $k+1=k+h\le 2^{m-n}=2^{m-1}$ and hence $H-2k=1$, or

$$k=\frac{H-1}{2}. \tag{10}$$

Substituting (10) in (9) yields $H=2^m-1$. $\square$

Remark 14. Combining the Theorems 12 and 13 yields the inequality $\sigma_2(H)\le 2\log_2(H)$ for every odd natural number H.

Some other subsequences can be given in parametric form.

Theorem 15. *Let $m\ge 3$ be a natural number and let H be an odd natural number with $H<2^m$. Then $\sigma_2(H)=2m-2$ if and only if $H=2^m-3$.*

Proof.
(1) For $H=2^m-3$ with $m\ge 3$ there is the solution

$$(n,s,h,k)=(2,m,1,2^{m-2}-1)$$

to the Diophantine equation (5), i.e., $\sigma=2m-2$. Theorem 13 states that $\sigma_2(2^m-3)\ne 2m-1$, which is why $\sigma_2(2^m-3)=2m-2$.

(2) Suppose that for a $H<2^m$ we have $\sigma_2(H)=2m-2$. The only pairs (n,s) leading to $\sigma=2s-n=2m-2$ are $(0,m-1)$ or $(2,m)$. Moreover, we know that $3\le h\le k$ implies $s<m$. Therefore, the second pair requires $h=1$ and transforms (5) into $2^mk+k+1=2^{m-2}H$ or

$$k+1=2^{m-2}(H-4k). \tag{11}$$

Because $k+1\le 2^{m-2}$, we get $H-4k=1$, i.e., $k=\frac{H-1}{4}$. Substituting k in (11) yields $H=2^m-3$.

Let us now turn our attention to the pair $(0,m-1)$. Suppose that there is a solution to the Diophantine equation $2^{m-1}hk+h+k=2^{m-1}H$ with $H<2^m$. A simple transformation gives $h+k=2^{m-1}(H-hk)$, yielding $H-hk=2$ since $h+k\le 2^m$ and $H-hk$ even. So, $h=2^m-k$ and $h=\frac{H-2}{k}$. Combining these two equalities gives $k^2-2^mk+H-2=0$, or

$$H=-k^2+2^mk+2.$$

Note that the inequality $-k^2+2^mk<2^m-2$ is fulfilled for no $1\le k<2^m$. This can be verified, e.g., by basic analytic considerations of the polynomial function $f(x)=-x^2+2^mx-2^m$. Consequently, we obtain $H>2^m$. This contradiction proves the theorem. $\square$

Theorem 16. *Let $m>3$ be a natural number. Then $\sigma_2(2^m+1)=2m-2$.*

Proof. Note that for all $m>3$ there is $\sigma_1(2^m+1)\le\lfloor\log_2(2^m+1)\rfloor-1=m-1\le 2m-2$. Consider the equality $2^{m-1}(2^m-1)+2^m=2^{m-1}(2^m+1)$ showing that $(n,s,h,k)=(0,m-1,1,2^m-1)$ is a solution of the Diophantine equation (5). Therefore, we have $\sigma_2(2^m+1)\ge 2m-2>\sigma_1(2^m+1)$. According to the Theorems 12, 13 and 15, the only larger value that $\sigma_2(2^m+1)$ could equal to for $m\ge 3$ is $2m-1$. The latter value requires $(n,s)\in\{(1,m),(3,m+1)\}$. The first of these pairs gives $2^mhk+h+k=2^{m-1}(2^m+1)$ or

$$h+k=2^{m-1}(2^m+1-2hk)\le 2^m.$$

Since $2^m+1-2hk$ is odd, this implies $2^m+1-2hk=1$ which is impossible for odd h and k when $m>3$. The second pair yields $2^{m+1}hk+h+k=2^{m-2}(2^m+1)$ or

$$h+k=2^{m-2}(2^m+1-8hk)\le 2^{m-2}.$$

This gives $2^m+1-8hk=1$, an equality that also cannot hold for odd h and k when $m>3$. Hence, $\sigma_2(2^m+1)=2m-2$ for all $m>3$. $\square$

Theorem 17. *Let $m\ge 3$ be a natural number. Then $\sigma_2(2^m+3)=2m-4$.*

Proof. Note that for all $m\ge 3$ there is $\sigma_1(2^m+3)\le\lfloor\log_2(2^m+3)\rfloor-1=m-1\le 2m-4$. Consider the equality $2^{m-2}(2^m-1)+2^m=2^{m-2}(2^m+3)$. Thus $(n,s,h,k)=(0,m-2,1,2^m-1)$ is a solution of the Diophantine equation (5) for all $m\ge 3$ and hence $\sigma_2(2^m+3)\ge 2m-4\ge\sigma_1(2^m+3)$. Because $2^m+3<2^{m+1}-3$ for all $m\ge 3$, we know by the Theorems 12, 13 and 15 that $\sigma_2(2^m+3)<2(m+1)-2=2m$. Therefore, other potential values for $\sigma_2(2^m+3)$ are $2m-3, 2m-2$ or $2m-1$.

To obtain $\sigma=2m-3$ we need $(n,s)\in\{(1,m-1),(3,m),(5,m+1)\}$.

The first pair gives $2^{m-1}hk+h+k=2^{m-2}(2^m+3)$ or

$$h+k=2^{m-2}(2^m+3-2hk). \tag{12}$$

Since $h+k\le 2^m$, the odd natural number $2^m+3-2hk$ can take the values 1 or 3.

(a) $2^m+3-2hk=1$ is equivalent to $h=\frac{2^{m-1}+1}{k}$. Substituting h in (12) gives $k^2-2^{m-2}k+2^{m-1}+1=0$. The latter quadratic equation has integer solutions k only if $\Delta=2^{2m-2}-4(2^{m-1}+1)=4(2^{2m-4}-2^{m-1}-1)$ is a perfect square. It is easy to see that Δ is a perfect square if and only if $\frac{\Delta}{4}$ is one as well. But for $m \geq 3$ we have $\frac{\Delta}{4} \equiv 3 \pmod 4$, which is impossible for a perfect square.

(b) $2^m + 3 - 2hk = 3$ is equivalent to $h = \frac{2^{m-1}}{k}$ which is impossible for odd h and k.

The pair $(3, m)$ yields $2^m hk + h + k = 2^{m-3}(2^m + 3)$ or

$$h + k = 2^{m-3}(2^m + 3 - 8hk).$$

Here, we have $h + k \leq 2^{m-2}$ and so, the odd natural number $2^m + 3 - 8hk$ can only take the value 1. This gives $h = \frac{2^{m-1}+1}{4k}$ which is impossible.

With the pair $(5, m+1)$ we get $2^{m+1}hk + h + k = 2^{m-4}(2^m + 3)$ or

$$h + k = 2^{m-4}(2^m + 3 - 32hk).$$

Here, we have $h + k \leq 2^{m-4}$ and hence $2^m + 3 - 32hk = 1$ or $h = \frac{2^{m-1}+1}{16k}$ which again is impossible. We can conclude that $\sigma_2(2^m + 3) \neq 2m - 3$.

The case $\sigma = 2m-2$ requires $(n, s) \in \{(0, m-1), (2, m), (4, m+1)\}$, while for $\sigma = 2m-1$ there ought to be $(n, s) \in \{(1, m), (3, m+1)\}$. In total analogy to the case $\sigma = 2m - 3$, one can establish that none of these five pairs leads to a solution of the Diophantine equation (5). The details of these computations are left to the reader. Consequently, $\sigma_2(2^m + 3) = 2m - 4$ for all $m \geq 3$. □

Remark 18.

(1) We know that $\sigma_2(1) = 0$. Moreover, the Theorems 17 and 13 state that for every natural number $N \geq 2$ there exists an odd number H with $\sigma_2(H) = N$. A question arising from these observations is, whether the sequence σ_2 is surjective on $\mathbb{N}_0$? The answer is "yes", since a straightforward computation yields $\sigma_2(27) = 1$.

(2) The sequence $(a(n))_{n \geq 0}$ with $a(n) = \sigma_2(2n + 1)$ is sequence A272895 of the OEIS.

2.5 Some further observations about σ_3

The Diophantine equation (6) is equivalent to

$$h + k = 2^s(2^{s-n}H - hk). \tag{13}$$

From the observations made at the end of subsection 2.1 we know that $h + k \leq 2^s \cdot H$. So, there is an odd natural number $\alpha \leq H$ with $2^{s-n}H - hk = \alpha$, i.e., $h = \frac{2^{s-n}H - \alpha}{k}$. Substituting h in (13) gives

$$k^2 - 2^s\alpha k + 2^{s-n}H - \alpha = 0. \tag{14}$$

The latter quadratic equation in the variable k is solvable in integers if and only if the number $\tau := 2^{2s-2}\alpha^2 + \alpha - 2^{s-n}H$ is a perfect square.

We study two different cases. First, if $\alpha \equiv 3 \pmod 4$ then we have to consider the following subcases. If $s - n = 1$ then τ has the form $2^{2n}\alpha^2 + \alpha - 2H$. So, for $n = 0$

we get $\tau = \alpha^2 + \alpha - 2H \equiv 2 \pmod 4$, which cannot be a perfect square. In the case $n \geq 1$ this yields $\tau \equiv 1 \pmod 4$ and hence a potential perfect square leading to a solution of (14) of the form $k = 2^n\alpha \pm \sqrt{2^n\alpha^2 + \alpha - 2H}$. The corresponding value of σ would be $\sigma = 3(n+1) - n = 2n + 3$. Note, that the condition $1 \leq n \leq \log_2(H)$ has to be fulfilled, which is why only a finite number of solutions of the latter form can exist. If $s - n \geq 2$ then $\tau \equiv 3 \pmod 4$ and hence τ never is a perfect square.

Secondly, let $\alpha \equiv 1 \pmod 4$. Again consider the case $s - n = 1$, i.e., $\tau = 2^{2n}\alpha^2 + \alpha - 2H$. For $n = 0$ we get $\tau \equiv 0 \pmod 4$ and therefore the potential solution $k = \alpha \pm \sqrt{\alpha^2 + \alpha - 2H}$ with a corresponding $\sigma = 3$. If $n \geq 1$ then $\tau \equiv 3 \pmod 4$ cannot be a perfect square. The case $s - n \geq 2$ always gives $\tau \equiv 1 \pmod p$ and hence potential solutions of the form $k = 2^{s-1}\alpha \pm \sqrt{2^{2s-2}\alpha^2 + \alpha - 2^{s-n}H}$ with corresponding $\sigma = 3s - n$.

Note that the latter subcase is the only one that could possibly lead to an infinity of solutions. More precisely, we can have $\sigma_3(H) = \infty$ only if $\tau = 2^{2s-2}\alpha^2 + \alpha - 2^{s-n}H$ is a perfect square for an infinity of tuples (s, n, α) fulfilling $0 \leq n < s - 1$, $n \leq \log_2(H)$ and $1 \leq \alpha \leq H$ with $\alpha \equiv 1 \pmod 4$.

Proposition 19. *Let H be an odd natural number. Then*
1) $\sigma = 3 \in S_3(H) \setminus S_2(H)$ if $k = \alpha \pm \sqrt{\alpha^2 + \alpha - 2H}$ and $h = \frac{2^{s-n}H-\alpha}{k}$ are odd natural numbers for a given $\alpha \equiv 1 \pmod 4$ with $\alpha \leq H$.
2) $\sigma = 3s - n \in S_3(H) \setminus S_2(H)$ if $k = 2^{s-1}\alpha \pm \sqrt{2^{2s-2}\alpha^2 + \alpha - 2^{s-n}H}$ and $h = \frac{2^{s-n}H-\alpha}{k}$ are odd natural numbers for $0 \leq n < s - 1$, $n \leq \log_2(H)$ and $1 \leq \alpha \leq H$ with $\alpha \equiv 1 \pmod 4$.
3) $\sigma = 2n + 3 \in S_3(H) \setminus S_2(H)$ if $k = 2^n\alpha \pm \sqrt{2^n\alpha^2 + \alpha - 2H}$ and $h = \frac{2^{s-n}H-\alpha}{k}$ are odd natural numbers for $1 \leq n \leq \log_2(H)$ and $\alpha \leq H$ with $\alpha \equiv 3 \pmod 4$.
These three cases give all possible elements of the set $S_3(H) \setminus S_2(H)$.

Example 20.
(1) For a given odd natural number t the tuples $(s, 0, t^2)$ yield the perfect squares $2^{2s-2}t^4 + t^2 - 2^st^3 = (2^{s-1}t^2 - t)^2$ for all $s \in \mathbb{N}$, leading to $k = 2^st^2 - t$ and $h = t$. This means that $\sigma_3(t^3) = \infty$ for every odd natural number t.
(2) It is easy to verify that the expressions $2^{2s-2} + 1 - 2^{s-n} \cdot 3$ are never perfect squares for $n \in \{0, 1\}$ and $s \geq n + 2$. Thus, we obtain $\sigma_3(3) < \infty$. A straightforward computation actually yields $\sigma_3(3) = \sigma_2(3) = 3$.

3 Primality testing and generalized Fermat numbers

In 1877, Pépin [21] showed that for $n > 1$ the Fermat number $F_n = 2^{2^n} + 1$ is prime if and only if $5^{\frac{F_n-1}{2}} \equiv -1 \pmod{F_n}$. The so-called Pépin test has since been a popular method to check Fermat numbers for primality. A structural equivalence of Pépin's test for Fermat numbers and the Lucas-Lehmer test for Mersenne numbers has been brought to light recently [11].

Some further results were inspired by Pépin's theorem. First, Proth [22] found the following generalization: Let $N = H \cdot 2^\sigma + 1$ be an odd number with $2^\sigma > H$. Let b be a quadratic nonresidue modulo N. Then N is a prime number if and only if $b^{\frac{N-1}{2}} \equiv -1$ (mod

N). So called Proth primes, i.e., numbers that can be shown being prime using Proth's theorem, play an important role in finding factors of Fermat numbers.

Another question, arising from an observation by Lucas [16, p. 313], was brought up by Aigner [1] in 1986: Are there other prime numbers suitable to be used as bases in Pépin's test? Aigner identified the basic property of any suitable prime number p to be that almost all Fermat numbers are quadratic nonresidues modulo p. He found 14 such primes less than $35 \cdot 10^6$ and, because of their rareness, called them *elite* prime numbers. In recent years, elite primes have been the subject of a number of research papers [5, 6, 14, 15, 17, 18, 19, 23, 24].

In this context, Reinhart and the author [18, 20] studied some fundamental properties of the behavior of the so called Fermat periods of natural numbers. For a natural number b consider the generalized Fermat numbers $F_{b,n} = b^{2^n} + 1$. Because of the recurrence relation $F_{b,n+1} = (F_{b,n} - 1)^2 + 1$ it is obvious that the congruence $F_{b,n} \pmod N$ becomes periodic for every natural number N, i.e., there exist minimal nonnegative integer numbers s and $L \geq 1$ such that $F_{b,s} \equiv F_{b,s+Lk} \pmod N$ for all natural numbers k. We call the parameter $s =: s_b(N)$ the *start index* and $L =: L_b(N)$ the *period length* of the b-Fermat period of N. Some applications of generalized Fermat numbers have been studied [4, 7, 9, 12]. For a survey on Fermat numbers we refer the reader to the book of Křížek, Luca, and Somer [13]. Some generalizations of Proth's theorem dealing with other parametric forms of $N = Ka^n + b$ have been discussed by several authors [2, 8, 10]. In this section, we give another generalization of Proth's primality theorem lowering the requirements that the base b has to fulfil.

Theorem 21. *Let H be an odd natural number and let $m \geq 1$ be a real number such that $\sigma_m(H) < \infty$. Let $N = H \cdot 2^\sigma + 1$ be an odd natural number with $\sigma > \sigma_m(H)$. Then N is a prime number if and only if there are two natural numbers b and k with $\gcd(N, b) = 1$, $k \geq \frac{\sigma}{m}$ and $b^{2^{k-1}H} \equiv -1 \pmod N$.*

Remark 22.
(1) Taking into account the inequality $\sigma_1(H) \leq \log_2(H)$, Proth's theorem follows from Theorem 21 when we use $m = 1$.

(2) In many cases, the condition $\sigma > \sigma_m(H)$ is actually weaker than that demanded by Proth. E.g., $\sigma_1(3) = 0$, $\sigma_2(165) = 0$, $\sigma_2(27) = \sigma_2(45) = \sigma_2(267) = 1$, $\sigma_2(H) = 2$ for $H \in \{11, 51, 85, 195, 201, 231, \ldots\}$, $\sigma_2(H) = 3$ for $H \in \{21, 37, 55, 87, 93, 123, 153, 181, 243, 245, \ldots\}$, etc.

(3) Proth's theorem needs the base b to be a quadratic nonresidue modulo N. In our result this requirement falls aside for $m > 1$. E.g., because of $\sigma_2(1) = 0$, the first four Fermat Numbers $F_n := 2^{2^n} + 1$ ($n \in \{0, 1, 2, 3\}$) can be proved being prime numbers using Theorem 21 with $b = 2$, $k := n + 1 \geq 2^{n-1}$ and $2^{2^{k-1}} \equiv -1 \pmod{F_n}$. Unfortunately, for all $n \geq 4$ the base $b = 2$ is not suitable anymore and $b = 3$, i.e., Pépin's Test, has to be applied for larger Fermat Numbers.

The proof of Theorem 21 is based on elementary properties of b-Fermat periods and thus points out another application of generalized Fermat numbers.

3.1 Fermat periods

Using the parametric form $N = H \cdot 2^\sigma + 1$ allows a characterization of the start index and the length of the Fermat periods of N [20].

Theorem 23. *Let $N = H \cdot 2^\sigma + 1$ and b be natural numbers with $\gcd(N, b) = 1$. We let $t \cdot 2^s$ (t odd) denote the multiplicative order of b modulo N. Then we have $s_b(N) = s$ and $L_b(N) = \mathrm{ord}_t(2)$. If N is a prime number, then $s \le \sigma$ and t divides H.*

A result linking the period length of a composite N to the period lengths of coprime factors is also known [20].

Theorem 24. *Let A and B be two coprime natural numbers and $b \in \mathbb{N}$. Then $L_b(AB) = \mathrm{lcm}(L_b(A), L_b(B))$.*

A similar result can be shown for the start indices of composite numbers.

Proposition 25. *Let A, B and b be natural numbers with $\gcd(A, B) = \gcd(AB, b) = 1$. Then $s_b(AB) = \max\{s_b(A), s_b(B)\}$.*

Proof. It is well-known that for natural numbers A, B and b with $\gcd(A, B) = \gcd(AB, b) = 1$ we have $\mathrm{ord}_{AB}(b) = \mathrm{lcm}(\mathrm{ord}_A(b), \mathrm{ord}_B(b))$. With Theorem 23 this implies $s_b(AB) = \max\{s_b(A), s_b(B)\}$. □

The following proposition settles the problem of the start indices of non-squarefree numbers.

Proposition 26. *Let p be an odd prime number. Let m and b be natural numbers with $\gcd(p, b) = 1$. Then $s_b(p^m) = s_b(p)$.*

Proof. We let α denote the multiplicative order of b modulo p, i.e., $b^\alpha = pk + 1$ for a suitable $k \in \mathbb{Z}$. This leads to

$$\begin{aligned} b^{\alpha p^{m-1}} &= (pk+1)^{p^{m-1}} \\ &= \sum_{\nu=0}^{p^{m-1}} \binom{p^{m-1}}{\nu} p^\nu k^\nu \\ &\equiv 1 \pmod{p^m}. \end{aligned}$$

It follows that the multiplicative order of b modulo p^m is a divisor of αp^{m-1}. Now suppose that there is a $\beta < \alpha$ fulfilling $b^{\beta p^{m-1}} \equiv 1 \pmod{p^m}$. Then Fermat's little theorem implies $b^\beta \equiv 1 \pmod{p}$, contradicting the fact that α is the multiplicative order of b modulo p.

So, the multiplicative order of b modulo p^m has to be of the form αp^d with $d \in \{0, 1, \ldots, m-1\}$. By writing $p = h \cdot 2^r + 1$, Theorem 23 states that $\alpha = 2^s t$ with $s \le r$, t a divisor of h and $s_b(p) = s$. Again with Theorem 23, this time applied to p^m, we obtain the start index $s_b(p^m) = s$ since $\mathrm{ord}_{p^m}(b) = 2^s t p^d$ and tp^d is odd. □

Corollary 27. *Let $N = \prod_{\nu=1}^{n} p_\nu^{\alpha_\nu}$ be the canonical prime factorization of an odd natural number N. Then $s_b(N) = \max_{1 \le \nu \le n}\{s_b(p_\nu)\}$ for every base $b \in \mathbb{N}$ with $\gcd(N, b) = 1$.*

Proof. By induction over the number of prime factors, Proposition 25 can be generalized to $s_b(N) = \max_{1 \le k \le n}\{s_b(p_k^{\alpha_k})\}$. With Proposition 26 we then get $s_b(N) = \max_{1 \le k \le n}\{s_b(p_k)\}$. □

Remark 28. All the results formulated so far for Fermat numbers remain correct if we consider power sequences instead. So, for practical use, it does not matter whether we investigate the congruential behavior of the numbers $F_{b,n}$ or that of the numbers b^{2^n}.

3.2 A primality theorem using Fermat periods

Theorem 29. *Let H be an odd natural number and let $m \ge 1$ be a real number such that $\sigma_m(H) < \infty$. Let $N = H \cdot 2^\sigma + 1$ be an odd natural number with $\sigma > \sigma_m(H)$. Then N is a prime number if and only if there is a natural number b with $\gcd(N, b) = 1$ and $s_b(N) \ge \frac{\sigma}{m}$.*

Proof.
(1) Suppose $N = H \cdot 2^\sigma + 1$ to be a prime number. Then there exists a primitive root b modulo N, i.e., $\gcd(N, b) = 1$ and $\mathrm{ord}_N(b) = 2^\sigma \cdot H$. With Theorem 23, this implies $s_b(N) = \sigma \ge \frac{\sigma}{m}$.

(2) Let b be a natural number with $\gcd(N, b) = 1$ and $s_b(N) \ge \frac{\sigma}{m}$. Suppose that $N = H \cdot 2^\sigma + 1 = AB$ is a composite number with the two factors $A = h \cdot 2^r + 1$ and $B = k \cdot 2^s + 1$. Note that by definition there is $1 < A, B$. Therefore, the numbers A and B represent every possible combination of two nontrivial divisors of N that multiply to N.

Since $\sigma > \sigma_m(H)$, we know that $r = s < \frac{\sigma}{m}$. It follows that every prime factor $p = q \cdot 2^w + 1$ of N must fulfil $w < \frac{\sigma}{m}$. Corollary 27 then implies $s_b(N) < \frac{\sigma}{m}$ for every base b with $\gcd(N, b) = 1$. This contradiction proves the theorem. □

3.3 Proof of Theorem 21

(1) Let N be a prime number. Then there is a primitive root b modulo N fulfilling $\gcd(N, b) = 1$ and, by Euler's criterion, $b^{2^{\sigma-1}H} \equiv -1 \pmod{N}$.

(2) Let b and k be natural numbers with $\gcd(N, b) = 1$, $k \ge \frac{\sigma}{m}$ and

$$b^{2^{k-1}H} \equiv -1 \pmod{N}.$$

Therefore, $2^k H$ is a multiple of the multiplicative order of b modulo N, while $2^{k-1}H$ is not. Hence, there must be a divisor d of H such that $\mathrm{ord}_N(b) = 2^k d$. Theorem 23 now gives $s_b(N) = k \ge \frac{\sigma}{m}$. Since $\sigma > \sigma_m(H)$, we can apply Theorem 29 and we immediately obtain the primality of N. □

4 Discussion and open problems

(1) Are there more elegant criteria than those of Proposition 19 to decide whether $\sigma_3(H) < \infty$? Are the multipliers $H = t^3$ the only values giving $\sigma_3(H) = \infty$?

(2) Are there conditions of existence for values $m > 3$ allowing to evaluate $\sigma_m(H)$?

(3) Another open problem is the question how to efficiently find a suitable base b in order to use Theorem 21 for primality testing. The following heuristic argument suggests that it might suffice to try $b = 2$ for $m \geq 2$, $H \geq 3$ with $\sigma_m(H) < \infty$ and large σ. We know that for every prime number $p = H \cdot 2^\sigma + 1$ that is not a divisor of $2^H - 1$, there exists a generalized Fermat number of the form $(2^H)^{2^{k-1}} + 1$ being a multiple of p. In such a case, the difference $\sigma - k := t$ indicates that 2^H is a 2^t-power residue but not a 2^{t+1}-power residue modulo p [3]. Now suppose that $k < \frac{\sigma}{m}$. This would imply $t > \frac{(m-1)\sigma}{m}$ and thus 2^H would have to be at least a $2^{\lfloor\frac{(m-1)\sigma}{m}\rfloor+1}$-power residue modulo p. The probability that this is true actually equals $2^{-\lfloor\frac{(m-1)\sigma}{m}\rfloor-1}$. Therefore, for large values of σ it is quite improbable that our test fails with $b = 2$.

Evidently, if $N = H \cdot 2^\sigma + 1$ (not being a divisor of $2^H - 1$) does not divide a generalized Fermat number of the form $(2^H)^{2^k} + 1$ for $1 \leq k \leq \sigma - 1$, then N is composite. Therefore, under the assumption that $b = 2$ is suitable, an algorithm based on Theorem 21 leads to a primality or compositeness statement for a given $N = H \cdot 2^\sigma + 1$ with large σ after at most $\sigma - 1$ squaring and congruence operations and hence runs in $O(\log(N))$.

(4) Perhaps it is useful to consider restrictions of the sequences σ_m for $m \geq 3$ in order to get finite subsequences that allow us to use Theorem 21 for selected exponents σ even though $\sigma_m(H) = \infty$.

References

[1] A. Aigner, Über Primzahlen, nach denen (fast) alle Fermatschen Zahlen quadratische Nichtreste sind, *Monatsh. Math.* **101** (1986), 85–94.

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

[3] A. Björn and H. Riesel, Factors of generalized Fermat numbers, *Math. Comp.* **67** (1998), 441–446.

[4] C. K. Caldwell and T. Komatsu, Powers of Sierpinski numbers base B, *Integers* **10** (2010), A36, 423–436.

[5] A. Chaumont and T. Müller, All elite primes up to 250 billion, *J. Integer Sequences* **9** (2006), Article 06.3.8.

[6] A. Chaumont, J. Leicht, T. Müller, and A. Reinhart, The continuing search for large elite primes, *Int. J. Number Theory* **5** (2009), 209–218.

[7] J. B. Cosgrave and K. Dilcher, A role for generalized Fermat numbers, *Math. Comp.*, to appear.

[8] J. M. Grau, A. M. Oller-Marcén, and S. Sadornil, A primality test for Kp^n+1 numbers, *Math. Comp.* **84** (2015), 505–512.

[9] T. A. Gulliver, Self-reciprocal polynomials and generalized Fermat numbers, *IEEE Trans. Inform. Theory* **38** (1992), 1149–1154.

[10] A. Guthmann, *A generalization of Proth's theorem.* Preprint No. 216, Universität Kaiserslautern, Fachbereich Mathematik, 1992.

[11] J. H. Jaroma, Equivalence of Pepin's and the Lucas-Lehmer tests, *Eur. J. Pure Appl. Math.* **2** (2009), 352–360.

[12] P. Kurlberg and C. Pomerance, On the periods of the linear congruential and power generators, *Acta Arith.* **119** (2005), 149–169.

[13] M. Křížek, F. Luca, and L. Somer, *17 Lectures on Fermat Numbers. From Number Theory to Geometry*, Springer, 2001.

[14] M. Křížek, F. Luca, and L. Somer, On the convergence of series of reciprocals of primes related to the Fermat numbers, *J. Number Theory* **97** (2002), 95–112.

[15] M. Křížek, F. Luca, I. E. Shparlinski, and L. Somer, On the complexity of testing elite primes, *J. Integer Sequences* **14** (2011), Article 11.1.2.

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

[17] T. Müller, Searching for large elite primes, *Exp. Math.* **15** (2005), 183–186.

[18] T. Müller and A. Reinhart, On generalized elite primes, *J. Integer Sequences* **11** (2008), Article 08.3.1.

[19] T. Müller, A generalization of a theorem by Křížek, Luca and Somer on elite primes, *Analysis (Munich)* **28** (2008), 375–382.

[20] T. Müller, On the Fermat periods of natural numbers, *J. Integer Sequences* **13** (2010), Article 10.9.5.

[21] T. Pépin, Sur la formule $2^{2^n}+1$, *C. R. Acad. Sci. Paris* **85** (1877), 329–331.

[22] F. Proth, Théorèmes sur les nombres premiers, *C. R. Acad. Sci. Paris* **87** (1878), 926.

[23] A. Witno, On elite primes of period four, *Int. J. Number Theory* **6** (2010), 667–671.

[24] A. Witno, Primes modulo which almost all Fermat numbers are primitive roots, *Note Mat.* **30** (2010), 133–140.

2010 *Mathematics Subject Classification*: Primary 11A41; Secondary 11A51, 11B83, 11D61, 11D72, 11Y11.
Keywords: exponent, non-trivial divisor, composite number, primality test, prime number, Diophantine equation, generalized Fermat number, Fermat period.

(Concerned with sequences A000125, A102742, A128852, A272894, and A272895.)

Received May 12 2016; revised version received December 1 2016. Published in *Journal of Integer Sequences*, December 27 2016.

Return to Journal of Integer Sequences home page.