Journal of Integer Sequences, Vol. 13 (2010),
Article 10.9.5

On the Fermat Periods of Natural Numbers

Tom Müller
Forschungsstelle für interdisziplinäre Geisteswissenschaft
Institut für philosophische Bildung
Alanus-Hochschule für Kunst und Gesellschaft
Villestr. 3
53347 Alfter bei Bonn
Germany
and
Kueser Akademie für europäische Geistesgeschichte
Gestade 18
54470 Bernkastel-Kues
Germany
tom.mueller@alanus.edu

Abstract

Let $b > 1$ be a natural number and $n \in \mathbb{N}_0$. Then the numbers $F_{b,n} := b^{2^n} + 1$ form the sequence of generalized Fermat numbers in base b. It is well-known that for any natural number N, the congruential sequence $(F_{b,n} \pmod{N})$ is ultimately periodic. We give criteria to determine the length of this Fermat period and show that for any natural number L and any $b > 1$ the number of primes having a period length L to base b is infinite. From this we derive an approach to find large non-Proth elite and anti-elite primes, as well as a theorem linking the shape of the prime factors of a given composite number to the length of the latter number's Fermat period.

1 Introduction

Let N and $b > 1$ be natural numbers. For $n \in \mathbb{N}_0$ denote by $F_{b,n} := b^{2^n} + 1$ the terms of the sequence of generalized Fermat numbers in base b. The numbers $F_{b,n}$ obviously fulfill the recurrence relation

$$F_{b,n+1} = (F_{b,n} - 1)^2 + 1. \tag{1}$$

This immediately implies that the sequence $0 \leq f_n < N$ defined by $f_n \equiv F_{b,n} \pmod N$ is ultimately periodic. So, there exist two minimal natural numbers s and L such that $f_s = f_{s+kL}$ for all $k \in \mathbb{N}$. Then we call the terms $f_s, f_{s+1}, \ldots, f_{s+L-1}$ the *b-Fermat remainders* of N. Moreover, we say that the natural number N has a *b-Fermat period* of length L beginning with the Fermat number $F_{b,s}$. We shall denote the length of the b-Fermat period of the natural number N by $L_b(N)$ throughout this paper. Notice that, from another point of view, the Fermat remainders may be considered to be a special case of power generators. The statistical properties of the period lengths appearing in this standard method to generate pseudorandom numbers have been studied by several authors in the past years, e.g., by Kurlberg and Pomerance [8], who give new results together with a review of the present knowledge of this matter.

In his 1986 paper, Aigner [1] gave a complete characterization of s and L for prime numbers N in the case $b = 2$. That result was generalized for all bases $b > 1$ by the author and Reinhart [12].

The purpose of the present paper is to give a complete characterization of $L_b(N)$ for all bases $b > 1$ and all natural numbers N. To that respect, we show some multiplicative laws allowing us to compute $L_b(N)$ for composite N using the respective period lengths of its prime factors. This demands for a closer look to $L_b(p)$ for prime numbers p and selected bases b.

Moreover, we prove that for every $b > 1$ and every natural number l the set $\mathcal{F}_b(l)$ is infinite. Here, $\mathcal{F}_b(l) := \{p \in \mathbb{P} : L_b(p) = l\}$ denotes the set of all prime numbers with a b-Fermat period of length l. Finally, we present two possible applications of these theoretical approaches. First, the numbers considered in the infinity proof can be used to provide prime numbers with given period lengths. We examine several of these numbers in order to find large non-Proth elite and anti-elite prime numbers. Secondly, the multiplicative laws for $L_b(N)$ show that every composite number preserves a part of information on the periodical behavior of its prime factors. This could be – as we illustrate in one single example – used to develop or support methods of factorization.

2 The Fermat period of natural numbers

The theorem of Aigner can be generalized for every natural number N that is relatively prime to the given base $b > 1$.

Theorem 2.1. Let N and $b > 1$ be natural numbers with $\gcd(N, b) = 1$. Write the multiplicative order of b modulo N as $\operatorname{ord}_N(b) = 2^s \cdot t$ with $s \in \mathbb{N}_0$ and t an odd number. Then the b-Fermat period of N begins with the Fermat number $F_{b,s}$. The length $L_b(N)$ of the b-Fermat period equals the multiplicative order of 2 modulo t.

The proof of Theorem 2.1 works in total analogy to that of Theorem 2.6 in the paper of Müller and Reinhart [12].

Remark 1. If N is a prime number of the form $2^r \cdot h + 1$ with $r \in \mathbb{N}$ and h odd, it is obvious that the parameters of the multiplicative order of b modulo N, i.e., $2^s \cdot t$, fulfill $0 \leq s \leq r$ and $t|h$.

The question of the period length $L_b(N)$ remains open for the case $\gcd(N,b) > 1$ yet. It is resolved by the following results.

Lemma 2.2. *Let $b > 1$ and n be natural numbers. Then $L_b(2^n) = 1$.*

Proof. If b is even we immediately get $b^{2^m} + 1 \equiv 1 \pmod{2^n}$ for all m with $2^m > n$. It follows $L_b(2^n) = 1$.
For odd b we have $\gcd(b, 2^n) = 1$ such that the theorem of Euler guarantees

$$b^{2^{n-1}} + 1 \equiv b^{\phi(2^n)} + 1 \equiv 2 \pmod{2^n}, \tag{2}$$

and hence by recurrence relation (1) we have $F_{b,m} \equiv 2 \pmod{2^n}$ for all $m \geq n-1$. This again leads to $L_b(2^n) = 1$. □

Lemma 2.3. *Let p be an odd prime number. Let a and n be natural numbers. Then $L_{ap}(p^n) = 1$.*

Proof. We have $(ap)^{2^m} + 1 \equiv 1 \pmod{p^n}$ for all m with $2^m \geq n$. From this follows the claim. □

Lemma 2.4. *Let $b > 1$ and n be natural numbers. Write $n = am$ such that for every prime factor p of a we have $p|b$ and $\gcd(b,m) = 1$. Then $L_b(n) = L_b(m)$.*

Proof. The conditions of the lemma lead to the congruential system

$$\begin{cases} F_{b,k} \equiv 1 \pmod{a} \\ F_{b,k} \equiv \lambda_k \pmod{m} \end{cases}$$

for all indices k large enough. The Chinese remainder theorem states that then there exists an unique solution to this system of the form $F_{b,k} \equiv \Lambda_k \pmod{n}$.

Because of the periodicity we have $F_{b,k+L_b(m)} \equiv F_{b,k} \equiv \lambda_k \pmod{m}$ and hence $F_{b,k+L_b(m)} \equiv \Lambda_K \equiv F_{b,k} \pmod{n}$. This implies $L_b(m) \geq L_b(n)$.

Moreover, we get $F_{b,k+L_b(n)} \equiv F_{b,k} \pmod{n}$. Since $m|n$ we obtain from this latter congruence $F_{b,k+L_b(n)} \equiv F_{b,k} \pmod{m}$, i.e., $L_b(m) \leq L_b(n)$.

This proves the claim. □

Lemma 2.5. *Let $b > 1$ be a natural number. Let n and m be coprime natural numbers. Then $L_b(nm) = \operatorname{lcm}(L_b(n), L_b(m))$.*

Proof. First we study the case $\gcd(n,b) = \gcd(m,b) = 1$. Write $2^{s_n}t_n$ the multiplicative order of b modulo n and $2^{s_m}t_m$ the multiplicative order of b modulo m. Then by Theorem 2.1 we know that $L_b(n) = \operatorname{ord}_{t_n}(2)$ and $L_b(m) = \operatorname{ord}_{t_m}(2)$. Using a well-known result from elementary number theory, we get

$$\begin{aligned} \operatorname{ord}_{nm}(b) &= \operatorname{lcm}(\operatorname{ord}_n(b), \operatorname{ord}_m(b)) \\ &= \operatorname{lcm}(2^{s_n}t_n, 2^{s_m}t_m) \\ &= 2^s \operatorname{lcm}(t_n, t_m), \end{aligned}$$

where $s := \max\{s_n, s_m\}$. Moreover, it is well-known that $\mathrm{ord}_{\mathrm{lcm}(t_n,t_m)}(2) = \mathrm{lcm}(\mathrm{ord}_{t_n}(2), \mathrm{ord}_{t_m}(2))$. Again with Theorem 2.1 we then obtain

$$\begin{aligned} L_b(nm) &= \mathrm{ord}_{\mathrm{lcm}(t_n,t_m)}(2) \\ &= \mathrm{lcm}(\mathrm{ord}_{t_n}(2), \mathrm{ord}_{t_m}(2)) = \mathrm{lcm}(L_b(n), L_b(m)). \end{aligned}$$

Secondly we examine the case $\gcd(n, b), \gcd(m, b) \geq 1$. Write $n = a_n\nu$ and $m = a_m\mu$ such that for every prime factor p of a_n we have $p|b$ and $\gcd(b, \nu) = 1$ and such that for every prime factor q of a_m we have $q|b$ and $\gcd(b, \mu) = 1$. By Lemma 2.4 we know that $L_b(nm) = L_b(\nu\mu)$. Notice that $\gcd(\nu, \mu) = 1$. So, the first part of the present proof guarantees that $L_b(\nu\mu) = \mathrm{lcm}(L_b(\nu), L_b(\mu))$. Again with Lemma 2.4 this finally gives $L_b(nm) = \mathrm{lcm}(L_b(n), L_b(m))$. □

Using induction over the number of different prime factors of N, this latter result can be easily generalized.

Consequence 2.6. *Let $b > 1$ be a natural number. Let $N = \prod_{\nu=1}^{r} p_\nu^{\alpha_\nu}$ be the canonical prime factorization of the natural number $N > 1$. Then*

$$L_b(N) = \mathrm{lcm}(L_b(p_1^{\alpha_1}), L_b(p_2^{\alpha_2}), \ldots, L_b(p_r^{\alpha_r})).$$

Furthermore, if we define $L_b(1) := 1$, we obtain a complete characterization of $L_b(N)$ for every base $b > 1$ and every natural number N.

Remark 2.7. Let $n, m, b > 1$ be natural numbers with $\gcd(nm, b) = 1$. If the b-Fermat period of n, (resp., m) begins with the term F_{b,s_n} (resp., F_{b,s_m}) then the b-Fermat period of the number nm begins with the term $F_{b,\max\{s_n,s_m\}}$.

3 The infinity of the sets $\mathcal{F}_b(L)$

The following necessary condition for a prime number p to have a b-Fermat period of length L is known [12].

Theorem 3.1. *Let $p = 2^r \cdot h + 1$ be a prime number with a natural number $r \geq 1$ and h odd. Let $b > 1$ be a natural number. If p has a b-Fermat period of length $L > 1$ then p is a divisor of the number*

$$N_{b,r}^{(L)} := \sum_{n=0}^{2^L-2} (F_{b,r} - 1)^n. \tag{3}$$

We will use Theorem 2.1 and the latter result to show that for all natural numbers L and for every base $b > 1$ there are infinitely many prime numbers q having a b-Fermat period of length L. For $L = 1$ this claim is trivial since it is well-known that the odd parts of the Fermat numbers $F_{b,n}$ are pairwise coprime and for every odd prime divisor p of a given $F_{b,m}$ equation (1) implies $F_{b,n} \equiv 2 \pmod{p}$ for all $n > m$, i.e., we get $L = 1$ for infinitely many primes.

3.1 Factors of the numbers $N_{b,r}^{(L)}$

Notice that the condition in Theorem 3.1 is not sufficient for p to have a b-Fermat period of length $L > 1$. In fact, if $p = 2^r h + 1$ is a factor of $N_{b,r}^{(L)}$ then every positive divisor of L could be the length of the b-Fermat period of p too. In the proof of Theorem 3.1 one makes use of the fact that if L is the length of the period then $F_{b,r+L} \equiv F_{b,r} \pmod{p}$, i.e., there exists a natural number c with $c + 1 \equiv F_{b,r} \pmod{p}$ and $c^{2^L} \equiv c \pmod{p}$. From this follows (by excluding the cases $c \equiv 0$ and $c \equiv 1 \pmod{p}$ leading to period length 1) that p divides $N_{b,r}^{(L)}$. But for every natural number k we obtain, because of the definition of L, that $c^{2^{Lk}} \equiv c \pmod{p}$ and hence in total analogy to the previous argument that p is a divisor of $N_{b,r}^{(Lk)}$ as well.

The other way around, if $L > 1$ is the length of the b-Fermat period of $p = 2^r h + 1$ we have $p \mid N_{b,r}^{(L)}$, i.e., $c^{2^L} \equiv c \pmod{p}$. Like in Theorem 2.1 we write $2^s t$ the multiplicative order of b modulo p. This implies that there cannot be a natural number $m < L$ such that $p \mid N_{b,r}^{(m)}$ because otherwise we would get the relation $c^{2^m} \equiv c \pmod{p}$ contradicting the minimality of L. Suppose now that $p \mid N_{b,r}^{(L_1)}$ for some $L_1 > L$. Then we get the congruence $c^{2^{L(L_1-L)}-1} \equiv 1 \pmod{p}$. This is equivalent to the fact that the multiplicative order of c modulo p divides the difference of the exponents, i.e., the number $2^L(2^{L_1-L} - 1)$. As we have $c \equiv b^{2^r} \pmod{p}$, the multiplicative order of c modulo p equals t. Hence $2^{L_1-L} \equiv 1 \pmod{t}$, which implies that the multiplicative order of 2 modulo t, i.e., L, is a divisor of the exponent $L_1 - L$. So, we finally have $L_1 \equiv 0 \pmod{L}$. All this shows that the following theorem holds.

Theorem 3.2. *Let $b > 1$ be a natural number. Let $p = 2^r h + 1$ be a prime number dividing $N_{b,r}^{(K)}$ for a natural number K. Then the length L of the b-Fermat period of p is a divisor of K.*

In order to prove our main result we need the following factorization formula

$$N_{b,r+1}^{(L)} = N_{b,r}^{(L)} \left(N_{b,r}^{(L)} - 2 \sum_{n=0}^{2^{L-1}-2} (F_{b,r} - 1)^{2n+1} \right). \tag{4}$$

The truth of this can be seen as follows. Let $R \geq 0$ be an even number and let x be a natural number. Using the properties of geometric sums we get

$$\sum_{n=0}^{R} x^n \cdot \sum_{n=0}^{R} (-x)^n = \sum_{n=0}^{R} x^{2n}. \tag{5}$$

Notice that all three sums of this latter equation actually are odd numbers. Moreover, we see that

$$\sum_{n=0}^{R} x^n \quad = \quad 1 + (x + 1) \sum_{n=0}^{\frac{R}{2}-1} x^{2n+1} \tag{6}$$

and

$$\sum_{n=0}^{R} (-x)^n = \sum_{n=0}^{R} x^n - 2 \sum_{n=0}^{\frac{R}{2}-1} x^{2n+1}. \tag{7}$$

If we now define $x := b^{2^r} = (F_{b,r} - 1)$ and $R := 2^L - 2$ this leads to formula (4). Denote by d the greatest common divisor of the numbers $\sum_{n=0}^{R} x^n$ and $\sum_{n=0}^{R} (-x)^n$. Then d must be odd and we obtain by (7) that d is a divisor of $\sum_{n=0}^{\frac{R}{2}-1} x^{2n+1}$ as well. With (6) this leads to

$$0 \equiv \sum_{n=0}^{R} x^n \equiv 1 \pmod{d}, \tag{8}$$

which is possible if and only if $d = 1$. Hence the numbers $N_{b,r}^{(L)}$ and $Q_{b,r}^{(L)} := N_{b,r+1}^{(L)} / N_{b,r}^{(L)}$ are coprime for all r. Moreover, the sequence $Q_{b,n}^{(L)}$ $(n \in \mathbb{N}_0)$ consists of pairwisely coprime terms.

3.2 The main result

Lemma 3.3. *Let $b > 1$ be a natural number. Let L be a prime number. Then there are infinitely many prime numbers with a b-Fermat period of length L.*

Proof. Let L be a prime number. We already know that the terms of the sequence $Q_{b,r}^{(L)}$ are pairwisely coprime. This means that there are infinitely many prime numbers being factors of the numbers $N_{b,r}^{(L)}$ $(r \in \mathbb{N})$. Let p be such a prime number. By Theorem 3.2 we know that the length of the b-Fermat period of p is a divisor of L, i.e., 1 or L. The first case implies $x^2 \equiv x \pmod{p}$ for $x \equiv b^{2^r} \pmod{p}$. From this follows $x(x-1) \equiv 0 \pmod{p}$, i.e., either $x \equiv 0 \pmod{p}$ or $x \equiv 1 \pmod{p}$. Now, $x \equiv b^{2^r} \equiv 0 \pmod{p}$ implies $b \equiv 0 \pmod{p}$, which is only possible for the finite number of prime factors of b. From $x \equiv 1 \pmod{p}$ follows that $N_{b,r}^{(L)} \equiv 2^L - 1 \equiv 0 \pmod{p}$, i.e., p is an element of the finite set of all prime factors of the number $2^L - 1$. All in all, only a finite number of primes dividing one of the numbers $N_{b,r}^{(L)}$ have a b-Fermat period of length 1. Hence, all the remaining primes dividing the terms $N_{b,r}^{(L)}$ $(r \in \mathbb{N})$ must have a Fermat period of length L. $\square$

Theorem 3.4. *Let $b > 1$ and L be natural numbers. Then the set $\mathcal{F}_b(L)$ is infinite.*

Proof. For $L = 1$ we have $\mathcal{F}_b(1) = \{p \in \mathbb{P} : p | F_{b,r} \text{ for } r \in \mathbb{N}\}$. It is well-known that this latter set is infinite.
If L is a prime number this is the claim of Lemma 3.3. So let $L > 1$ be a composite number in the following. We again consider the numbers

$$N_{b,r}^{(L)} = \sum_{\nu=0}^{2^L-2} \left(b^{2^r}\right)^{\nu} \text{ and } Q_{b,r}^{(L)} = \sum_{\nu=0}^{2^L-2} \left(-b^{2^r}\right)^{\nu}$$

for $r \in \mathbb{N}$. In order to prove the claim of the theorem, we have to show that for all r large enough the numbers $Q_{b,r}^{(L)}$ have a prime divisor p not dividing any number $Q_{b,s}^{(d)} \neq Q_{b,r}^{(L)}$ with $s \leq r$ and $d | L$.
First, we consider the case $s < r$ and $d | L$. As seen above we then have $N_{b,s+1}^{(d)} | N_{b,r}^{(d)}$. Moreover, the properties of geometric sums tell us that the expression $\frac{x^{dk}-1}{x^d-1}$ is an natural number for

any base $x \in \mathbb{N}$. Hence, we obtain $N_{b,r}^{(d)} | N_{b,r}^{(L)}$ as well. Combining these observations, we get the fact that $N_{b,s+1}^{(d)} | N_{b,r}^{(L)}$. We already know that $N_{b,s+1}^{(d)} = N_{b,s}^{(d)} Q_{b,s}^{(d)}$. As $N_{b,r}^{(L)}$ and $Q_{b,r}^{(L)}$ are coprime, the numbers $Q_{b,s}^{(d)}$ and $Q_{b,r}^{(L)}$ must be coprime as well. So, in this case we find that no prime factor of $Q_{b,r}^{(L)}$ actually divides an term of the form $Q_{b,s}^{(d)}$ with $s < r$ and $d|L$.

The case $s = r$ and $d \neq L$ is still to study. We see that

$$Q_{b,r}^{(L)} = \frac{b^{(2^r)(2^L-1)} + 1}{b^{2^r} + 1}.$$

A well-known result of Carmichael [3] implies that for $1 < x \in \mathbb{N}$ and for all exponents n large enough the numbers of the form $x^n + 1$ do have a primitive divisor, i.e., a prime factor not dividing any number of the form $x^m + 1$ with $m < n$. Hence, for all r large enough the numbers $Q_{b,r}^{(L)}$ have a primitive factor not dividing a number of the form $Q_{b,r}^{(d)}$. This completes the proof. $\square$

Remark 3.5. The proof of Theorem 3.4 just given was proposed by the anonymous referee. Our original proof was much longer and used the following argument. We factorized the terms $N_{b,r}^{(L)}$ into the Form $M_r G_r R_r$, where G_r denotes the lowest common multiple of the numbers $N_{b,r}^{(d)}$ for all $d|L$ fulfilling $1 < d < L$. M_r is the product of all prime factors of $N_{b,r}^{(L)} G_r^{-1}$ having a b-Fermat period of length 1. For all r large enough M_r can be shown to be a constant. Moreover, it is possible to prove that R_r is not bound and that the greatest common divisor of G_r and R_r is also a constant for all r large enough. Finally, the terms R_n are pairwisely coprime such that for all r large enough there is a primitive divisor to R_r not dividing $M_r G_r$. Hence, this prime cannot have a period length inferior to L.

4 Consequences and application

4.1 Non-Proth elite and anti-elite primes

We will now have a closer look at the cases $L = 3$ and $L = 4$ for the base $b = 2$. As shown in Lemma 3.3, (resp., Theorem 3.4) there are infinitely many prime numbers with Fermat periods of length 3, (resp., 4). We get the following necessary and sufficient characterizations.

Corollary 4.1. *Let $b = 2$. Let $p = 2^r \cdot h + 1$ be a prime number with $r \geq 1$ and h odd. Then p has a 2-Fermat period of length $L = 3$ if and only if p is a divisor of the number*

$$N_{2,r}^{(3)} = \sum_{\nu=0}^{6} \left(2^{2^r}\right)^{\nu}. \tag{9}$$

Proof. As shown in the proof of Lemma 3.3 the number $N_{b,r}^{(L)}$ is divided only by finitely many primes with a period length 1 if L is a prime number. These primes are divisors of the number $2^L - 1$, (resp., the base b). Here we have $L = 3$, i.e., $2^3 - 1 = 7$, and $b = 2$. But these two prime numbers cannot divide $N_{2,r}^{(3)}$, since $N_{2,r}^{(3)}$ is an odd number and 7 has a 2-Fermat period of length 2. From this follows the claim. $\square$

Corollary 4.2. *Let $b = 2$. Let $p = 2^r \cdot h + 1$ be a prime number with $r > 1$ and h odd. Then p has a 2-Fermat period of length $L = 4$ if and only if p is a divisor of the number*

$$W_r := \frac{1}{5} \cdot \sum_{\nu=0}^{4} \left(2^{2^r \cdot 3}\right)^{\nu}. \tag{10}$$

If $r = 1$ the only prime numbers with a 2-Fermat period of length $L = 4$ are 11, 31, 151 and 331.

Proof. The case $r = 1$ is trivial. Consider now $r \geq 2$. We know that all the primes of the form $p = 2^r \cdot h + 1$ with a period length $L = 4$ divide the term

$$N_{2,r}^{(4)} = N_{2,r}^{(2)} \cdot \sum_{\nu=0}^{4} \left(2^{2^r \cdot 3}\right)^{\nu}.$$

All primes dividing $N_{2,r}^{(4)}$ and having a Fermat period of length 2 must also divide $N_{2,r}^{(2)}$. So the numbers we are looking for are all the prime divisors of the term

$$V_r := \sum_{\nu=0}^{4} \left(2^{2^r \cdot 3}\right)^{\nu}$$

not having a Fermat period of length 1 or 2. The first kind of primes again must be divisors of the numbers $b = 2$ or $2^L - 1 = 15$, i.e., 2, 3 or 5. The second kind of primes consists of common prime divisors of the numbers $N_{2,r}^{(2)}$ and V_r. Suppose p to be such a prime number. Then

$$\begin{aligned} 2^{2^r \cdot 3} &= 2^{2^r \cdot 3} + N_{2,r}^{(2)} - N_{2,r}^{(2)} \\ &= 2^{2^r} N_{2,r}^{(2)} - N_{2,r}^{(2)} + 1 \equiv 1 \pmod{p}. \end{aligned}$$

This leads to $0 \equiv V_r \equiv 5 \pmod{p}$ for all common prime divisors of $N_{2,r}^{(2)}$ and V_r. Therefore, only the primes 2, 3 and 5 have to be considered here. All three have a 2-Fermat period of length 1. As V_r is odd the first candidate is not a divisor, as well as 3 since $V_r \equiv 2 \pmod{3}$ for all natural numbers $r \geq 1$. An easy computation shows that $V_r \equiv 0 \pmod{5}$ and $V_r \equiv 5 \pmod{25}$ for all $r \geq 2$. Hence, the number $\frac{V_r}{5}$ is divided only by numbers having a period length $L = 4$. This proves the corollary. □

These two corollaries can be used to find prime numbers with 2-Fermat periods of the lengths 3 or 4, and furthermore to find elite or anti-elite primes. A b-*elite* prime number p is a prime number none of whose b-Fermat remainders is a quadratic residue modulo p. If all the b-Fermat remainders are quadratic residues modulo a prime number p then p is called a b-*anti-elite* prime [13]. If $b = 2$, we simply speak of elite or anti-elite primes. In the past years a number of papers on these two families of prime numbers have been published [1, 4, 5, 7, 10, 11, 15]. There have been two approaches to compute elites, resp., anti-elites. A first way consisted in checking all prime numbers of a given interval for eliteness, resp., anti-eliteness. As a result of such researches all 27 elite primes up to $2.5 \cdot 10^{12}$ are known [5], as well as all 84 anti-elite primes up to 10^{11} [11]. These prime numbers are summarized in sequence A102742, resp., sequence A128852 of Sloane's *On-Line Encyclopedia of Integer Sequences* [14]. Recently, Dennis R. Martin completed the search for elite and anti-elite primes up to 10^{14}. He found two new elite primes and 29 new anti-elite primes [9].

In a second approach only large primes of the easy-to-check Proth type $2^r \cdot h + 1$ with rather small $h < 2^r$ were examined in order to find large primes having relatively small Fermat periods, which then were checked for eliteness. That way, some 60 elite primes larger than $2.5 \cdot 10^{12}$ could be found, the largest of which have more than 300000 decimal digits [5]. No elite prime larger than 10^{12} and not being a Proth number was known until the year 2008. Using the Corollary 4.2 we can find one such prime with 35 decimal digits. Furthermore, a non-Proth anti-elite prime with 14 decimal digits can be found. For this we consider the prime factorization of the number W_5 which is given by

$$\begin{aligned} W_5 &= 11 \cdot 31 \cdot 41 \cdot 61 \cdot 151 \cdot 331 \cdot 1321 \cdot 23041 \cdot 61681 \cdot 414721 \cdot \\ &\quad 394783681 \cdot 4278255361 \cdot 4562284561 \cdot 46908728641 \\ &\quad \cdot 44479210368001 \cdot 14768784307009061644318236958041601. \end{aligned}$$

Let us have a look at the factors $p := 14768784307009061644318236958041601$ and $q := 44479210368001$. Notice that their primality can be established, e.g., by the well-known method of Brillhart, Lehmer and Selfridge [2]. We obtain

$$p = 2^9 \cdot 28845281849627073524059056558675 + 1$$

and

$$q = 2^{10} \cdot 43436728875 + 1.$$

A simple computation shows that p provides four Fermat remainders each being a quadratic non-residue modulo p, while all four Fermat remainders of q are quadratic residues modulo q, i.e., p is an elite and q an anti-elite prime number.

Investing more computational effort into the rather time-consuming factorization of the numbers W_r could probably lead to the discovery of even larger non-Proth elite or anti-elite primes.

Moreover, we find the non-Proth elite prime

$$p = 1475204679190128571777 = 2^7 \cdot 11525036556172879467 + 1$$

with period length $L = 6$ considering the prime factors of the integer number $\frac{N_{2,3}^{(6)}}{\mathrm{lcm}(N_{2,3}^{(2)}, N_{2,3}^{(3)})}$.

Remark 4.3. A fourth way of computing elite primes was recently proposed by "Eigenray" in a forum on the pages of UC Berkeley (compare the URL [6]; valid as of July 8, 2008). It is considered to search for elite primes among the factors of the values of the $5 \cdot 2^s$-th cyclotomic polynomial evaluated at 2. The following elite primes were found that way by the author of the forum entry:

$$\begin{aligned} s=7 &\ :\ p_1 = 3442404051886487041 && (11)\\ s=8 &\ :\ p_2 = 777164631747163559325665584128 1, && (12)\\ & p_3 = 2^{10}\cdot C99+1 && (13)\\ s=9 &\ :\ p_4 = 4645410716199911238955104861 6961 && (14)\\ s=10 &\ :\ p_5 = 3587745015951361 && (15)\end{aligned}$$

In line (13), the number

$$\begin{aligned} C99 \;=\; & 5123396952520626719145982679287262122419114 4511286\text{-}\\ & 8396608612454598970667762655058642306684254536535\end{aligned}$$

is an odd composite number with 99 decimal digits; p_3 is a prime with 102 decimal digits. The similar approach has lately also been discussed by Witno [15]. Notice that all the primes presented here are non-Proth elite primes with $L = 4$. This supports a conjecture about non-Proth elite primes proposed by Chaumont et al. [5].

4.2 Factors of composite numbers

A second application could lie in the field of factoring natural numbers. The following theorem connects the shape of a prime number p with the information on b-Fermat period lengths preserved in every composite number being a multiple of p.

Theorem 4.4. *Let N be an odd composite number. Then every prime factor p of N is of the form $p = 2^r \cdot k \cdot \delta + 1$ with $r \in \mathbb{N}$, k odd and δ a divisor of $2^{L_b(N)} - 1$ for any given natural number $b > 1$, i.e., δ is a divisor of the $L_b(N)$-th Mersenne number.*

Proof. If p is a divisor of N then $L_b(p)$ is a divisor of $L_b(N)$ as well. This can be seen by combining the above-mentioned Consequence 2.6 and Theorem 3.2. Now write $p = 2^r \cdot h + 1$ where r is a natural number and h is odd. Then we know by Aigner's theorem that there exists a divisor δ of h, i.e., $h = k \cdot \delta$ for some appropriate k, with $L_b(p) = \mathrm{ord}_\delta(2)$. Therefore, we get $p = 2^r k\delta + 1$ with $2^{L_b(p)} \equiv 1 \pmod{\delta}$. This completes the proof. $\square$

Example 4.5. Consider the 74-decimal-digit natural number

$$\begin{aligned} N \;:=\; & 96493407697763496186309154173906589877\text{-}\\ & 7249872213671366995479866732609413666 1.\end{aligned}$$

If one finds out that this number equals $N_{2,1}^{(7)}$ it is trivial to give the factorization $N = N_{2,0}^{(7)} \cdot Q_{2,0}^{(7)}$. If one is lacking this piece of information, the task of factoring the number N is not at all that easy.

As a reference, we use the standard integer factorization routine (`ifactor`) given in MAPLE 11. Optionally, this command can be used with an additional parameter allowing to run factorization algorithms based on D. Shanks' undocumented square-free factorization, Lenstra's elliptic curve method or on Pollard's Rho method. All these methods are not able to factorize N within 120 seconds on a PC powered by an AMD Sempron 2600 XP+ processor. Now, the MAPLE-implementation of Pollard's Rho method allows to add another parameter. If we know that one of the searched prime factors p is of the form $p \equiv 1 \pmod{\delta}$ we can run the command `ifactor(N,pollard,`δ`)` in order to increase the efficiency of the method.

A simple computation checking the congruences $F_{2,n} \pmod{N}$ for the indices $n \in \{1, 2, \ldots, 8\}$ shows that $L_2(N) = 7$. So, by Theorem 4.4 every prime factor p of N has to fulfill $p \equiv 1 \pmod{\delta}$ for some δ dividing $2^7 - 1 = 127$. As 127 is a prime and $\delta = 1$ only leads to a period length of 1, we obtain $\delta = 127$ here.

Running the command `ifactor(N,pollard,127)` gives the prime factorization $N = N_{2,0}^{(7)} \cdot Q_{2,0}^{(7)}$ in less than one hundredth of a second.

This one example may suffice here. Deeper insights in whether this approach might be worth of further considerations have to be brought to light by forthcoming studies. Maybe this is a first small step towards a "statistical" factorization approach.

5 Acknowledgements

The author wants to thank Dr. Markus Nieß from the Catholic University of Eichstätt-Ingolstadt for his help with the MAPLE-computations. Moreover, the author is grateful to the friendly referee who made very valuable suggestions to improve this paper.

References

[1] A. Aigner, Über Primzahlen, nach denen (fast) alle Fermatzahlen quadratische Nichtreste sind, *Monatsh. Math.* **101** (1986), 85–93.

[2] J. Brillhart, D. H. Lehmer, and J. L. Selfridge, New primality criteria and factorizations of $2^m \pm 1$, *Math. Comp.* **29** (1975), 620–647.

[3] R. D. Carmichael, On the numerical factors of the arithmetic forms $\alpha^n \pm \beta^n$, *Ann. of Math.* **15** (1913), 30–70.

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

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

[6] "Eigenray", Forum entry, available online at `http://www.ocf.berkeley.edu/~wwu/cgi-bin/yabb/YaBB.cgi?board=riddles_putnam;action=display;num=1204796915` (valid as of July 8, 2008).

[7] 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.

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

[9] D. R. Martin, Elite prime search and anti-elite prime search, published online: http://www.primenace.com/papers/math/ElitePrimes.htm and http://www.primenace.com/papers/math/Anti-ElitePrimes.htm (valid as of July 28, 2010).

[10] T. Müller, Searching for large elite primes, *Experiment. Math.* **15** (2006), 183–186.

[11] T. Müller, On anti-elite prime numbers, *J. Integer Seq.* **10** (2007), Article 07.9.4.

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

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

[14] N. J. A. Sloane, Online Encyclopedia of Integer Sequences (OEIS), available at http://www.research.att.com/~njas/sequences/.

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

2010 *Mathematics Subject Classification*: Primary 11A41; Secondary 11A51, 11N69, 11Y05.
Keywords: Generalized Fermat number; elite prime number; anti-elite prime number; Fermat period.

(Concerned with sequences A102742 and A128852.)

Received August 7 2010; revised version received October 11 2010; November 6 2010. Published in *Journal of Integer Sequences*, December 7 2010.

Return to Journal of Integer Sequences home page.