Diophantine equation $\frac{q^n-1}{q-1} = y$ for four prime divisors of $y - 1$

Zdeněk Polický

Abstract. In this paper the special diophantine equation $\frac{q^n-1}{q-1} = y$ with integer coefficients is discussed and integer solutions are sought. This equation is solved completely just for four prime divisors of $y - 1$.

Keywords: diophantine equation, Fermat and Mersenne primes, Catalan conjecture

Classification: Primary 11D72; Secondary 11D45

1. Preliminaries

The theory of finite groups leads to some diophantine equations. There are some of them in which the variables are restricted to be prime. The techniques used vary from elementary properties of divisibility theory in integers leading to some more sophisticated results which can find applications in Galois theory. The diophantine equation $\frac{q^n-1}{q-1} = y$ which is solved in this paper is a special type of the equation

$$\frac{q^n - 1}{q - 1} = y^m \tag{1}$$

where q is a power of a prime, $y > 1$, $n > 2$, $m \geq 2$. This equation was studied in many articles. In his paper [12] W. Ljunggren found solutions of (1) for $m = 2$ and Ljunggren with T. Nagell found in [13] the only solutions

$$\frac{3^5 - 1}{3 - 1} = 11^2,\ \frac{7^4 - 1}{7 - 1} = 20^2,\ \frac{18^3 - 1}{18 - 1} = 7^3$$

if $3 \mid n$ or $4 \mid n$. French mathematicians Y. Bugeaud, M. Mignotte, and Y. Roy reached important progress in solving (1) in [5], [6] when q is a power of such prime p that $p \mid (y - 1)$ or when m is a prime and every prime divisor of q also divides $(y - 1)$.

Supported by the Grant Agency of the Czech Republic (Methods of Theory of Numbers, 201/04/381).

This work was motivated by the paper of Iranian mathematicians A. and B. Khosravi [9] who solved this diophantine equation for at most three prime divisors of $y-1$.

The main aim of this text is to develop their work and find solutions of $\frac{q^n-1}{q-1}=y$ for four prime divisors of $y-1$. Now we denote $y=a^\alpha b^\beta c^\gamma d^\delta+1$ where a,b,c,d are different primes and $\alpha,\beta,\gamma,\delta\geq 1$ are integers.
At first we mention some lemmas that we use in this paper.

Lemma 1.1. *Let p, q be distinct primes and $r,s>1$. Then the only solution of the equation $p^r-q^s=1$ is $3^2-2^3=1$.*

Lemma 1.2. *Let p, q be distinct primes and $r,s>1$. With the exception of the relation $239^2-2\times 13^4=-1$ a solution of the equation $p^r-2q^s=\pm 1$ exists only for exponents $r=s=2$.*

Remark 1.3. Lemma 1.1 is a special type of Catalan conjecture which was completely proved by P. Mihailescu (see Bilu [2]). The second lemma was proved by P. Crescenzo in [6].

The following lemma as well as Lemma 1.1 are due to E. Gerono (see Dickson [3, p. 744]).

Lemma 1.4. *If 2^m-1 is a power of a prime, hence $2^m-1=p^k$ where $k,m\in\mathbb{N}$ and p is a prime, then $k=1$ and m is prime. (Thus p is a Mersenne number.)*

The following propositions and Lemmas 1.5–1.9 are useful for the proof of the Main Theorem 2.1.

Lemma 1.5. *If $r>1$, $s\geq 1$ and $\frac{2^{r(4s+2)}-1}{2^r-1}$ has only three prime factors, then $r=3$, $s=1$.*

Proof (by A. Schinzel): By Bang's theorem generalized by Zsigmondy (see Dickson [3, pp. 385-386]) for every integer $n>1$, $n\neq 6$, 2^n-1 has a primitive prime factor, i.e. a prime factor that does not divide 2^m-1 for any $m<n$. Let $r=2^l m$, where m is odd and consider two cases, $m=1$ and $m>1$.

If $m=1$, then $\frac{2^{r(4s+2)}-1}{2^r-1}$ has prime factors belonging to exponents 2^{l+1} and $2^j(2s+1)$ $(0\leq j\leq l+1)$ except the exponent 6 if $2k+1=3$. Thus, we obtain $l+3>3$ prime factors if $2s+1>3$ and $l+2$ prime factors if $2s+1=3$, hence we have at least 4 prime factors, when $l=1$, $2s+1=3$. In the exceptional case $r=2,s=1$ the number $\frac{2^{12}-1}{2^2-1}=3\times 5\times 7\times 13$ has nevertheless 4 prime factors.

If $m>1$, then $\frac{2^{r(4s+2)}-1}{2^r-1}$ has prime factors belonging to exponents 2^{l+1}, $2^{l+1}m$, $2^{l+1}(2s+1)$, $2^l m(2s+1)$, $2^{l+1}m(2s+1)$ different from 6. Thus $\frac{2^{r(4s+2)}-1}{2^r-1}$ has at least 4 prime factors, unless $l=0$, $m=2s+1$, i.e. $r=3$, $s=1$. $\square$

Proposition 1.6. *Let p be a prime, $r \geq 4$. Then $r = 5$, $p = 5$ is the only solution of the equation*

$$2^{2r-5} - 2^{r-2} + 1 = p^2 \tag{2}$$

in integers.

Proof: Let us consider (2) in the form $2^{r-2}(2^{r-3} - 1) = (p-1)(p+1)$ and denote by K, L the greatest odd factors of $p+1$ and $p-1$ respectively. Since $(p-1, p+1) = 2$ we consider two subcases:

(i)

$$\begin{aligned} p - 1 &= 2^{r-3}L \\ p + 1 &= 2K. \end{aligned} \tag{$*$}$$

Then $K = 2^{r-4}L + 1$ and since $LK = 2^{r-3} - 1$, we have $2^{r-4}L^2 + L = 2^{r-3} - 1 \Rightarrow 2^{r-4} = \frac{L+1}{2-L^2}$ which implies that $L^2 < 2$, hence $L = 1$ and $K = 2^{r-3} - 1$. Then we deduce from $(*)$ that $2^{r-3} + 2 = 2(2^{r-3} - 1)$. Hence $r = 5$ and $p = 5$, as asserted.

(ii)

$$\begin{aligned} p - 1 &= 2K \\ p + 1 &= 2^{r-3}L. \end{aligned}$$

Then $K = 2^{r-4}L - 1$. The condition $LK = 2^{r-3} - 1$ implies that $2^{r-4}L^2 - L = 2^{r-3} - 1$ and consequently we have $2^{r-4} = \frac{L-1}{L^2-2}$. However, since we suppose that $r \geq 4$, we necessarily have $L \geq L^2 - 1$, a contradiction. $\square$

Lemma 1.7. *Let p, q be odd primes, $s \geq 1$. Then there does not exist a solution of the equation*

$$2p^{2s} - 2p^s + 1 - q^2 = 0 \tag{3}$$

in integers.

Proof: Let us consider (3) in the form $2p^s(p^s - 1) = (q-1)(q+1)$. Then we distinguish two possibilities according to p^s divides $q-1$ or p^s divides $q+1$.

At first, assume that $p^s \mid (q-1)$; then clearly $2p^s \mid (q-1)$ and we denote $q - 1 = 2p^s u$ where $u \in \mathbb{N}$. Then we get from (3) $2p^s(p^s - 1) = 2p^s u(q+1)$ and consequently $p^s - 1 = u(q+1)$. Hence $q+1 \leq p^s - 1 < 2p^s u = q-1$, a contradiction.

Now assume that $p^s \mid (q+1)$. By exactly the same arguments as above, we deduce that there exists a natural number u such that $q+1 = 2p^s u$. Since we consider (3) in the form $p^s - 1 = (q-1)u$, it follows that $q - 1 \leq p^s - 1$ and combining this inequality with another inequality $q+1 \geq 2p^s$ we get $2p^s \leq q+1 \leq p^s + 2$ and hence $p^s \leq 2$, a contradiction. $\square$

Proposition 1.8. *Let p, q be odd primes, $r > 2$, $s \geq 1$. Then there does not exist a solution of the equation*

$$2^{2r-3}p^{2s} - 2^{r-1}p^s + 1 - q^2 = 0 \tag{4}$$

in integers.

Proof: Assume that there exists a solution of (4) and denote $X = 2^{r-2}p^s$. Then we obtain from (4) the quadratic equation $2X^2 - 2X + 1 - q^2 = 0$. A solution exists only if the discriminant is the square of a natural number, $D = 4(2q^2 - 1)$, hence $2q^2 - 1 = s^2$, $s \in \mathbb{N}$ and if we write it as a congruence we have $s^2 \equiv -1 (\mathrm{mod}\, q)$. Since -1 is a quadratic residue $\mathrm{mod}\, q$ if and only if $q \equiv 1 (\mathrm{mod}\, 4)$, we denote $q = 1 + 4k$, $k \in \mathbb{N}$. Thus, immediately $2q^2 - 1 = 32k^2 + 16k + 1$ and it follows from (4) that $2q^2 - 1 = 2^r p^s (2^{r-2}p^s - 1) + 1$. Further, we get equation $16k(2k+1) = 2^r p^s (2^{r-2}p^s - 1)$. One can easily verify the statement for $r = 3$. The case $r = 2$ follows from Lemma 1.7. Hence assuming that $r \geq 4$ we have

$$k(2k+1) = 2^{r-4}p^s(2^{r-2}p^s - 1). \tag{5}$$

Since k and $2k+1$ are relatively prime then clearly $2^{r-4} \mid k$.

Now assume that $p \mid k$. Then $p^s \mid k$ and there would be such a number $Y \in \mathbb{N}$ that $k = 2^{r-4}p^s Y$. It follows immediately from (5) that $2^{r-4}p^s Y(2^{r-3}p^s Y + 1) = 2^{r-4}p^s(2^{r-2}p^s - 1)$ and consequently $Y(2^{r-3}p^s Y + 1) = 2^{r-2}p^s - 1$. Firstly, assume that $Y \geq 2$. Then we have $Y(2^{r-3}p^s Y + 1) \geq 2(2^{r-2}p^s + 1) > 2^{r-2}p^s - 1$ which leads to a contradiction. If $Y = 1$ then we get $2^{r-3}p^s + 1 = 2^{r-2}p^s - 1 \Rightarrow 2 = 2^{r-3}p^s$ which is a contradiction. Thus $p^s \mid (2k+1)$ and there would be such an odd natural number L that $p^s L = 2k + 1$.

Denote $M = 2^{r-3}$; then we get from (5) that $p^s L^2 - L = p^s 2M^2 - M$ and consequently $p^s(L^2 - 2M^2) = L - M$. Clearly $L^2 - 2M^2 \neq 0$ and we want to show that $L^2 - 2M^2 \neq \pm 1$. Firstly, assume that $L^2 - 2M^2 = -1$. Then $L^2 + 1 = 2M^2 = 2^{2r-5}$. Since $r \geq 4$ we have $4 \mid 2^{2r-5}$ and we get $L^2 + 1 \equiv 0 (\mathrm{mod}\, 4)$ which is impossible. Secondly, if $L^2 - 2M^2 = 1$ then $L^2 - 1 = 2^{2r-5}$ and consequently we have $(L-1)(L+1) = 2^{2r-5}$. Since $(L-1, L+1) = 2$, it follows that $L - 1 = 2$, $L + 1 = 4$ and $2\alpha - 5 = 3$, so that $\alpha = 4$ and consequently $p^s = 1$, a contradiction.

If $|L^2 - 2M^2| > 1$ then there exists such a prime h that $h \mid (L^2 - 2M^2)$ and also $h \mid (L - M)$. Thus h is odd and $h \mid (L^2 - M^2) - M^2$. Hence $h \mid M$, a contradiction. □

Proposition 1.9. *Let p, q be odd primes, $r > 2$, $t \geq 1$ and assume that $s(n-1)/2$ is odd where $n \geq 5$. If $q \mid (p^s + 1)$ then there does not exist a solution of the equation*

$$p^{s(n-1)/2} + 1 = 2^r q^t \tag{6}$$

in integers.

PROOF: Denote $p^{s(n-1)/2-s}-\ldots-p^s+1=A$ and $(n-1)/2=y$. Since we suppose that $q\,|\,(p^s+1)$, $p^{sm}\equiv 1(\operatorname{mod} q)$ holds for m even and $p^{sm}\equiv -1(\operatorname{mod} q)$ holds for m odd. Therefore $A\equiv y(\operatorname{mod} q)$ and since it follows from (6) that $q\,|\,A$ then clearly $q\,|\,y$ and consequently we have $y=qz$, $z\in\mathbb{N}$ and (6) in the form $p^{sqz}+1=2^rq^t$.

Now assume that $p^{sq^uw}+1=2^rq^t$, where $u,w\geq 3$ are odd. Then we have $p^{sq^uw}+1=(p^{sq^u}+1)(p^{sq^u(w-1)}-p^{sq^u(w-2)}+\ldots+1)=2^rq^t$. Denote $B=p^{sq^u(w-1)}-p^{sq^u(w-2)}+\ldots+1$. If $q\,|\,B$ then we observe by similar arguments as above that $q\,|\,w$, hence $w=qw'$, $w'\in\mathbb{N}$ and consequently we have such a natural number v that $p^{sq^v}+1=2^rq^t$.

Denote $C=p^{sq^{v-1}}$ and we want to show that q^2 does not divide p^s+1. Assume to the contrary that $q^2\,|\,(p^s+1)$. Then $C\equiv -1(\operatorname{mod} q^2)$ and consequently $C^q\equiv -1(\operatorname{mod} q^2)$ and it follows that $t\geq 2$. Since $p^s\equiv -1(\operatorname{mod} 2^r)$, we have $C\equiv -1(\operatorname{mod} 2^r)$ and we consider (6) as $C^q+1=(C+1)(C^{q-1}-C^{q-2}\ldots-C+1)=2^rq^t$. Since $t\geq 2$ and since $C\equiv -1(\operatorname{mod} q^2)$, we have $C^{q-1}-C^{q-2}\ldots-C+1\equiv q(\operatorname{mod} q^2)$ and consequently $C^{q-1}-C^{q-2}\ldots-C+1=q$. One knows that $C^x-C^{x-1}=C^{x-1}(C-1)\geq C(C-1)\geq 6$ for $x\geq 2$. Hence $C^{q-1}-C^{q-2}\ldots-C+1=q\geq 6\frac{q-1}{2}+1=3q-2>q$ which contradicts our assumption. It follows that q^2 does not divide p^s+1 and we obtain equation $p^s+1=2^rq$.

If now we denote $E=p^s$, then $E=2^rq-1$ and we have

$$E^q=\sum_{j=2}^{q}\binom{q}{j}(2^rq)^j(-1)^{q-j}+2^rq^2-1.$$

One can see that $\binom{q}{j}q^j\equiv 0(\operatorname{mod} q^3)$ holds for $2\leq j\leq q$. Then we have $E^q+1\equiv 2^rq^2(\operatorname{mod} 2^rq^3)$. If $v=1$ in $p^{sq^{v-1}}$ then we get $E^q+1=2^rq^2$. If $v>1$ then by using $p^{sq^v}+1=2^rq^t$ we get $(E^q)^{q^{v-1}}+1=(E^q+1)(E^{q^{v-1}-1}-E^{q^{v-1}-2}+\ldots+1)=2^rq^t$ and since $E^q+1\equiv 2^rq^2(\operatorname{mod} 2^rq^3)$, we have $E^q+1=2^rq^2$ for arbitrary natural number v.

Combining $E+1=2^rq$ with $(E+1)(E^{q-1}-E^{q-2}+\ldots+1)=2^rq^2$ we get $E^{q-1}-E^{q-2}+\ldots+1=q$. Since $E^z-E^{z-1}\geq 6$ for $x\geq 2$ by using similar arguments as above we have $q\geq 6\frac{q-1}{2}+1=3q-2\Rightarrow 1\geq q$ which is a contradiction. Hence the solution of (6) does not exist. $\square$

2. Main theorem

Theorem 2.1. *Let q be a power of a prime, b, c, d be primes, $n\geq 3$, odd and $\sharp\{p,\, p$ prime $\wedge\, p\,|\,(y-1)\}=4$. Then all solutions of the equation*

$$\frac{q^n-1}{q-1}=y \tag{7}$$

are listed in two following tables.

q	n	y	conditions
2	9	$2 \times 3 \times 5 \times 17 + 1$	
2^α	9	$2^\alpha \times (2^\alpha+1) \times (2^{2\alpha}+1) \times (2^{4\alpha}+1)+1$	$(2^\alpha+1)$, $(2^{2\alpha}+1)$, $(2^{4\alpha}+1)$ are Fermat primes
2^3	5	$2^3 \times 3^2 \times 5 \times 13 + 1$	
2^α	5	$2^\alpha \times (2^\alpha+1) \times (2^{2\alpha}+1) + 1$	$2^\alpha+1 = d$ is a Fermat prime and $2^{2\alpha}+1 = b^\beta c^\gamma$
2^α	3	$2^\alpha \times (2^\alpha+1)+1$	$2^\alpha + 1 = b^\beta c^\gamma d^\delta$
2	$2p+1$	$2 \times (2^p-1) \times (2^p+1)+1$	$2^p - 1 = d$ is a Mersenne prime and $2^p+1 = 3c$, p is a prime
2^α	$4k+3$, $k \geq 1$	$2^3 \times 3^3 \times 19 \times 73 + 1$	

Table 1: Solutions of the equation $(q^n-1)/(q-1) = y$ when $q = 2^\alpha$.

Proof: Let $y - 1 = A$. It follows from (7) that

$$\frac{q^n-1}{q-1} - 1 = \frac{q(q^{n-1}-1)}{q-1} = \frac{q(q^{(n-1)/2}-1)(q^{(n-1)/2}+1)}{q-1} = A.$$

Since $(q^{(n-1)/2}-1, q^{(n-1)/2}+1) \mid 2$ and since $(q-1) \mid (q^{(n-1)/2}-1)$, it follows that $(q^{(n-1)/2}+1) \mid A$. Since q is a power of a prime, denote $q = a^\alpha$, we consider three equations $a^{\alpha(n-1)/2}+1 = b^\beta$, $a^{\alpha(n-1)/2}+1 = b^\beta c^\gamma$, $a^{\alpha(n-1)/2}+1 = b^\beta c^\gamma d^\delta$. Clearly, one of the primes has to be even. Denote $a = 2$ and then we have $y = 2^\alpha b^\beta c^\gamma d^\delta + 1$. Now we distinguish two cases.

Case $q = 2^\alpha$

Since $(2^{\alpha(n-1)/2}-1, 2^{\alpha(n-1)/2}+1) = 1$, we consider three subcases:

2.1 $\quad 2^{\alpha(n-1)/2}+1 = d^\delta, \qquad \frac{2^{\alpha(n-1)/2}-1}{2^\alpha-1} = b^\beta c^\gamma.$

Clearly, $n \neq 3$. Using Lemma 1.1 we divide the equation on the left-hand side in 2.1 into three parts.

2.1.1 $\alpha(n-1)/2 = 1 \Rightarrow \alpha = 1$, $n = 3$ which is a contradiction.

2.1.2 $\alpha(n-1)/2 = 3$ and $d^\delta = 3^2$, since we have $\alpha = 1$, $n = 7 \Rightarrow b^\beta c^\gamma = 7$ which is contradiction.

q	n	y	conditions
b	5	$b\times 2(b+1)\times \frac{b^2+1}{2}+1$	$b=2^{\alpha-1}-1$ is a Mersenne prime and $b^2+1=2c^\gamma d^\delta$
b^β	3	$b^\beta\times 2\times \frac{b^\beta+1}{2}+1$	$b^\beta+1=2c^\gamma d^\delta$
b	5	$b\times 2^2\times \frac{b+1}{2}\times \frac{b^2+1}{2}+1$	$b+1=2c^\gamma$ and $b^2+1=2d$
b	9	$b\times 4(b+1)\times \frac{b^2+1}{2}\times \frac{b^4+1}{2}+1$	$2c=b^2+1$ and $2d=b^4+1$
b^2	5	$b^2\times 2^2\times \frac{b^2+1}{2}\times \frac{b^4+1}{2}+1$	$2c^2=b^2+1$ and $2d=b^4+1$
7	9	$7\times 2^5\times 5^2\times 1201+1$	
b^β	5	$b^\beta\times 2^2\times \frac{b^\beta+1}{2}\times \frac{b^{2\beta}+1}{2}+1$	$2c=b^\beta+1$ and $2d=b^{2\beta}+1$
b	5	$b\times 2(b+1)\times \frac{b^2+1}{2}+1$	$b+1=2^{\alpha-1}c^\gamma$ and $b^2+1=2d$
3	11	$3\times 2^2\times 11^2\times 61+1$	
b	$2k+1$, k is a prime	$b\times 2^\alpha\times c\times d+1$	$b=2^\alpha-1$ is a Mersenne prime and $b^{(n-1)/2-1}-\ldots-b+1=d$ and $b^{(n-1)/2-1}+\ldots+b+1=c$
b^β	3	$b^\beta\times\big(b^\beta+1\big)+1$	$b^\beta+1=2^\alpha c^\gamma d^\delta$

Table 2: Solutions of the equation $\frac{q^n-1}{q-1}=y$ when $q=b^\beta$, b odd.

2.1.3 $\delta=1$, since $2^{\alpha(n-1)/2}+1=d$ is a Fermat prime, we have $\alpha(n-1)/2=2^k$, $k\ge 1$ (If $k=0$ then the case $n=3$ is impossible.) Since $(2^{\alpha(n-1)/4}-1,2^{\alpha(n-1)/4}+1)=1$, we consider from the second equation in 2.1 $\frac{2^{\alpha(n-1)/4}-1}{2^\alpha-1}=b^\beta$, $2^{\alpha(n-1)/4}+1=c^\gamma$. Using Lemma 1.1 similarly as above we get three subcases of the last equation.

(a) $\alpha(n-1)/4=1\Rightarrow\alpha=1$, $n=5$ but then $b^\beta=1$ is a contradiction.

(b) $c^\gamma=3^2,\alpha(n-1)/4=3\Rightarrow\alpha=3$, $n=5$ then $b^\beta=1$ or $\alpha=1$, $n=13$ and $d=2^{\alpha(n-1)/2}+1=65$ is not a prime. In both cases we obtain a contradiction.

(c) $\gamma=1$, we have $2^{\alpha(n-1)/4}+1=c$, so c is a Fermat prime (d is a Fermat prime too) and $\frac{(2^{\alpha(n-1)/8}-1)(2^{\alpha(n-1)/8}+1)}{2^\alpha-1}=b^\beta$. Since $(2^{\alpha(n-1)/8}-1,2^{\alpha(n-1)/8}+1)=1$, we consider equations $\frac{2^{\alpha(n-1)/8}-1}{2^\alpha-1}=1$, hence $n=9$ and $2^{\alpha(n-1)/8}+1=b^\beta$. Thus solution of (7) is $[q=2,n=9,y=2\times 3\times 5\times 17+1]$ in case $\alpha=1$.

If $\alpha=3$, $b^\beta=3^2$ then $2^{\alpha(n-1)/4}+1=c=65$ which leads to a contradiction. If $\beta = 1$ then we can see that $b = 2^{\alpha} + 1$, $c = 2^{2\alpha} + 1$ and $2^{4\alpha} + 1$ are Fermat primes and the solution of (7) is $[q = 2^{\alpha}, n = 9, y = 2^{\alpha} \times (2^{\alpha} + 1) \times (2^{2\alpha} + 1) \times (2^{4\alpha} + 1) + 1]$.

2.2 $\quad 2^{\alpha(n-1)/2} + 1 = b^{\beta} c^{\gamma}, \qquad \frac{2^{\alpha(n-1)/2}-1}{2^{\alpha}-1} = d^{\delta}.$

2.2.1 $\alpha(n-1)/2$ is even.
Since $(2^{\alpha(n-1)/4} - 1, 2^{\alpha(n-1)/4} + 1) = 1$, we divide the equation on the right-hand side above by the only way: $\frac{2^{\alpha(n-1)/4}-1}{2^{\alpha}-1} = 1$ and $2^{\alpha(n-1)/4} + 1 = d^{\delta}$. Then $n = 5$ and we consider three possibilities:

(a) $\alpha = 1 \Rightarrow d^{\delta} = 3$ and $b^{\beta} c^{\gamma} = 5$ which is a contradiction.

(b) $\delta = 1$, then $d = 2^{\alpha} + 1$ is a Fermat prime and $2^{2\alpha} + 1 = b^{\beta} c^{\gamma}$ is a Fermat number. Therefore, solution of (7) is $[q = 2^{\alpha}, n = 9, y = 2^{\alpha} \times (2^{\alpha} + 1) \times (2^{\alpha} + 1) \times (2^{2\alpha} + 1) + 1]$.[1]

(c) $\alpha = 3$, $d^{\delta} = 3^2$, then we obtain a particular solution of [7] $[q = 2^3, n = 5, y = 2^3 \times 3^2 \times 5 \times 13 + 1]$.

2.2.2 $\alpha(n-1)/2$ is odd.
Since $2^{\alpha(n-1)/2} + 1 = (2+1)(2^{\alpha(n-1)/2-1} - \ldots - 2 + 1) = b^{\beta} c^{\gamma}$ one of the primes has to be three, denote $b = 3$.

(a) $\alpha \geq 3$, if we consider the equations above then we have $\frac{2^{\alpha}(n-1)-1}{2^{\alpha}-1} = b^{\beta} c^{\gamma} d^{\delta}$. According to Lemma 1.5 there exists the only solution of this equation $\alpha = 3$, $n = 7$ and consequently the solution of (7) is $[q = 2^3, n = 7, y = 2^3 \times 3^3 \times 19 \times 73 + 1]$.

(b) $\alpha = 1$ and $2^{(n-1)/2} - 1 = d^{\delta}$. Using Lemma 1.1 we have $\delta = 1$, d is a Mersenne prime and $(n-1)/2$ is also a prime. Let us denote $(n-1)/2 = p$ and $(2^{p-1} - 2^{p-2} + \ldots - 2 + 1) = K$. Then we get $2^p + 1 = (2+1)(2^{p-1} - 2^{p-2} + \ldots - 2 + 1) = 3^{\beta} c^{\gamma}$. If $\beta \geq 2 \Rightarrow 3 \mid K$ and since $2^{2m} \equiv 1 (\bmod 3)$, $-2^{2m+1} \equiv 1 (\bmod 3)$ for $m \in \mathbb{N}$ we have $K \equiv p \,(\bmod 3)$. Since $3 \mid K$, $3 \mid p$ and $b^{\beta} c^{\gamma} = 9$ which is a contradiction. If $\beta = 1$ then we have $2^p - 1 = d$, $2^p + 1 = 3c^{\gamma}$. According to [4] the equation $2^p + 1 = 3c^{\gamma}$ has no solution for $\gamma > 1$. Then the solution of (7) is $[q = 2, n = 2p + 1, y = 2 \times (2^p - 1) \times (2^p + 1) + 1]$ if $2^p - 1 = d$, $2^p + 1 = 3c$.

2.3 $\quad 2^{\alpha(n-1)/2} + 1 = b^{\beta} c^{\gamma} d^{\delta}, \qquad \frac{2^{\alpha(n-1)/2}-1}{2^{\alpha}-1} = 1.$

One can see that $n = 3$. The solutions for $\alpha \leq 50$ are listed in the following table.

---

[1] Until now we know the only couple of consecutive Fermat numbers F_4, F_5 satisfying conditions of the solution.

α	y	α	y
14	$2^{14} \times 5 \times 29 \times 113 + 1$	29	$2^{29} \times 3 \times 59 \times 3033169 + 1$
15	$2^{15} \times 3^2 \times 11 \times 331 + 1$	37	$2^{37} \times 3 \times 1777 \times 25781083 + 1$
21	$2^{21} \times 3^2 \times 43 \times 5419 + 1$	39	$2^{39} \times 3^2 \times 2731 \times 22366891 + 1$
22	$2^{22} \times 5 \times 397 \times 2113 + 1$	41	$2^{41} \times 3 \times 83 \times 8831418697 + 1$
24	$2^{24} \times 97 \times 257 \times 673 + 1$	44	$2^{44} \times 17 \times 353 \times 2931542417 + 1$
27	$2^{27} \times 3^4 \times 19 \times 87211 + 1$		

Table 3: Solutions of case 2.3 for $\alpha \leq 50$.

Case $q = b^\beta$, b-odd.

Since $(b^{\beta(n-1)/2} - 1, b^{\beta(n-1)/2} + 1) = 2$, we have nine subcases, four of them are leading immediately to a contradiction. Therefore we consider five types:

2.4 $\quad b^{\beta(n-1)/2} + 1 = 2c^\gamma d^\delta, \qquad \frac{b^{\beta(n-1)/2}-1}{b^\beta-1} = 2^{\alpha-1}.$

2.4.1 $\beta(n-1)/2$ is even.

By using $(b^{\beta(n-1)/4} - 1, b^{\beta(n-1)/4} + 1) = 2$ we consider two subcases of the equation on the right-hand side above:

(a) $\frac{b^{\beta(n-1)/4}-1}{b^\beta-1} = 2$, $b^{\beta(n-1)/4} + 1 = 2^{\alpha-2}$. Combining these two equations we get $2^{\alpha-2} = 2b^\beta$ which is a contradiction.

(b) $\frac{b^{\beta(n-1)/4}-1}{b^\beta-1} = 1 \Rightarrow n = 5$, $b^{\beta(n-1)/4} + 1 = 2^{\alpha-1}$, if we use Lemma 1.1 then we easily check that the solution of equation $b^\beta + 1 = 2^{\alpha-1}$ exists only for $\beta = 1$. Then $b = 2^{\alpha-1} - 1$ is a Mersenne prime and the solution of (7) is $[q = b, n = 5, y = b \times 2(b+1) \times \frac{b^2+1}{2} + 1]$ if $b^2 + 1 = 2c^\gamma d^\delta$.

2.4.2 $\beta(n-1)/2$ is odd.

Since $\frac{b^{\beta(n-1)/2}-1}{b^\beta-1} = \frac{(b^\beta-1)(b^{\beta(n-1)/2-\beta}+\ldots+1)}{b^\beta-1} = 2^{\alpha-1}$, we have $b^{\beta(n-1)/2-\beta} + \ldots + 1 = 2^{\alpha-1}$ and since $b^{\beta(n-1)/2-\beta} + \ldots + 1 \equiv 1 (\bmod 2)$, we easily check that $\alpha = 1$, $n = 3$. Then $b^\beta + 1 = 2c^\gamma d^\delta$ and the solution of (7) is $[q = b^\beta, n = 3, y = b^\beta \times 2 \times \frac{b^\beta+1}{2} + 1]$.

2.5 $\quad b^{\beta(n-1)/2} + 1 = 2d^\delta, \qquad \frac{b^{\beta(n-1)/2}-1}{b^\beta-1} = 2^{\alpha-1}c^\gamma.$

Using Lemma 1.2 we consider four subcases of the first equation in 2.5.

2.5.1 $\beta(n-1)/2 = 1 \Rightarrow \beta = 1$, $n = 3$ which is a contradiction.

2.5.2 $b^{\beta(n-1)/2} = 239^2$, $d^\delta = 13^4$, then $2^{\alpha-1}c^\gamma = \frac{239^2-1}{239-1} = 240 = 2^4 \times 15$ but 15 is not a prime.

2.5.3 $\delta = 1 \Rightarrow b^{\beta(n-1)/2}+1 = 2d$. If $\beta(n-1)/2$ is odd then we have $b^{\beta(n-1)/2}+1 = (b+1)(b^{\beta(n-1)/2-1} - \ldots + 1) = 2d$, however, $b^{\beta(n-1)/2} - \ldots + 1 \equiv 1 (\mathrm{mod}\, 2)$ and hence we have $b = 1$ which is impossible. Thus $\beta(n-1)/2$ is even and we consider four subcases of equation $\frac{(b^{\beta(n-1)/4}-1)(b^{\beta(n-1)/4}+1)}{b^{\beta}-1} = 2^{\alpha-1}c^{\gamma}$ since $(b^{\beta(n-1)/4} - 1, b^{\beta(n-1)/4} + 1) = 2$.

(a) $\frac{b^{\beta(n-1)/4}-1}{b^{\beta}-1} = c^{\gamma}$, $b^{\beta(n-1)/4}+1 = 2^{\alpha-1}$. It follows from Lemma 1.1 that the second equation has solution only if $\beta(n-1)/4 = 1$ and $b^{\beta(n-1)/4} = 3^2$ but in both cases we find a contradiction.

(b) $\frac{b^{\beta(n-1)/4}-1}{b^{\beta}-1} = 2c^{\gamma}$, $b^{\beta(n-1)/4} + 1 = 2^{\alpha-2}$. By the same arguments as in the previous point, we deduce a contradiction.

(c) $\frac{b^{\beta(n-1)/4}-1}{b^{\beta}-1} = 2^{\alpha-2}$, $b^{\beta(n-1)/4}+1 = 2c^{\gamma}$. Using Lemma 1.2 we consider following subcases of the second equation.

(c.1) $\beta(n-1)/4 = 1 \Rightarrow \beta = 1$, $n = 5$ and $2^{\alpha-2} = 1 \Rightarrow \alpha = 2$. Then the solution of (7) is $[q = b, n = 5, y = b \times 2^2 \times \frac{b+1}{2} \times \frac{b^2+1}{2} + 1]$ if we suppose that $b+1 = 2c^{\gamma}$ and $b^2+1 = 2d$.

(c.2) $\gamma = 1$, $\beta(n-1)/4$ is even otherwise $b^{\beta(n-1)/4} + 1 = (b+1)(b^{\beta(n-1)/4-1} - \ldots + 1) = 2c$ which is not possible. Since $(b^{\beta(n-1)/8} - 1, b^{\beta(n-1)/8} + 1) = 2$, one can verify according to Lemma 1.1 that the solution exists only for $b^{\beta(n-1)/8} + 1 = 2^{\alpha-2}$. Then $\frac{b^{\beta(n-1)/8}}{b-1} = 1 \Rightarrow n = 9$ and the equation $b^{\beta}+1 = 2^{\alpha-2}$ is solvable only for $\alpha-2 = 1$ or $\beta = 1$. The first case leads to a contradiction $b^{\beta} = 1$ and in the second case if we suppose that $b^2+1 = 2c$ and $b^4+1 = 2d$ then we get the solution of (7) in the form $[q = b, n = 9, y = b \times 4(b+1) \times \frac{b^2+1}{2} \times \frac{b^4+1}{2} + 1]$.

(c.3) $b^{\beta(n-1)/4} = 239^2$, $c^{\gamma} = 13^4$ but then $d = \frac{b^{\beta(n-1)/2}+1}{2} = \frac{239^4+1}{2} = 809 \times 1217 \times 1657$ which is a contradiction.

(c.4) $\beta(n-1)/4 = 2, \gamma = 2 \Rightarrow b^2 + 1 = 2c^2$ and $b^4 + 1 = 2d$. Firstly, we consider $\beta = 2, n = 5$, then $2^{\alpha-2} = 1 \Rightarrow \alpha = 2$ and the solution of (7) is $[q = b^2, n = 5, y = b^2 \times 2^2 \times \frac{b^2+1}{2} \times \frac{b^4+1}{2} + 1]$ if $b^2+1 = 2c^2$ and $b^4 + 1 = 2d$ holds.
Secondly, $\beta = 1$, $n = 9$ then $\frac{b^2-1}{b-1} = b + 1 = 2^{\alpha-2}$ $(\alpha \geq 4)$. Combining $b = 2^{\alpha-2} - 1$ with $b^2 + 1 = 2c^2$ yields $2^{2\alpha-5} - 2^{\alpha-2} + 1 = c^2$. It follows from Proposition 1.6 that the only solution of this equation is $\alpha = 5$ and $c = 5$. Then the solution of (7) is $[q = 7, n = 9, y = 7 \times 2^5 \times 5^2 \times 1201 + 1]$.

(d) $\frac{b^{\beta(n-1)/4}-1}{b^{\beta}-1} = 1 \Rightarrow n = 5$, $b^{\beta(n-1)/4} + 1 = 2^{\alpha-1}c^{\gamma}$.

(d.1) β is even.
Since $b^\beta+1 \equiv 2 \pmod 4$, we have $2^{\alpha-1}c^\gamma \equiv 2 \pmod 4$, hence $\alpha = 2$. Using Lemma 1.2 we consider four possibilities of $b^\beta+1 = 2c^\gamma$ but three of them were solved in case (c), therefore we find solution only if $\gamma = 1$. Then we have $b^\beta + 1 = 2c$, $b^{2\beta}+1 = 2d$ and the solution of (7) is $[q = b^\beta, n = 5, y = b^\beta \times 2^2 \times \frac{b^\beta+1}{2} \times \frac{b^{2\beta}+1}{2} + 1]$.

(d.2) β is odd.
Since $b^{2\beta}+1 = (b^2+1)(b^{2\beta-2} - b^{2\beta-4} + \ldots + 1) = 2d$ then clearly $b^2+1 = 2$ which is impossible. Hence, we consider the case $\beta = 1$. If $b^2+1 = 2d$ and $b+1 = 2^{\alpha-1}c^\gamma$ holds then the solution of (7) is $[q = b, n = 5, y = b \times 2(b+1) \times \frac{b^2+1}{2} + 1]$.

2.5.4 $\beta(n-1)/2 = 2, \delta = 2 \Rightarrow \beta = 1,\ n = 5$. Since $b+1 = 2^{\alpha-1}c^\gamma$ and since $b^2+1 = 2d^2$, we solve equation $2^{2\alpha-3}c^{2\gamma} - 2^{\alpha-1}c^\gamma + 1 - d^2 = 0$. However, according to Proposition 1.8 it follows that the solution does not exist in this case.

2.6 $\qquad b^{\beta(n-1)/2} + 1 = 2^\alpha c^\gamma d^\delta, \qquad \frac{b^{\beta(n-1)/2}-1}{b^\beta-1} = 1.$

In this case we found at least one solution for every odd prime number $b \le 20$.

2.7 $\qquad b^{\beta(n-1)/2} + 1 = 2^\alpha d^\delta, \qquad \frac{b^{\beta(n-1)/2}-1}{b^\beta-1} = c^\gamma.$

We easily check that $\beta(n-1)/2$ has to be odd and $n \neq 3$. Using Lemma 1.2 we observe that $\alpha \ge 2$. Now we consider two subcases:

2.7.1 d does not divide $(b^\beta+1)$.
Then we have $b^\beta = 2^\alpha - 1$. By Lemma 1.2 we have $\beta = 1$ and consequently b is a Mersenne prime. Now we consider from 2.7 two equations $b^{(n-1)/2-1} - \ldots - b + 1 = d^\delta$ and $b^{(n-1)/2-1} + \ldots + b + 1 = c^\gamma$. According to Ljunggren in [12] the second equation has the only solution $b = 3$, $n = 11$, $c^\gamma = 11^2$ for $\gamma > 1$. Then the solution of (7) is $[q = 3, n = 11, y = 3 \times 2^2 \times 11^2 \times 61 + 1]$. Now assume that $\gamma = 1$. Then we check that $(n-1)/2$ has to be a prime. Regarding [4] and since $d^\delta \equiv 1 \pmod b$ we may say that the solution of the equation $b^{(n-1)/2-1} - \ldots - b + 1 = d^\delta$ does not exist for $\delta > 1$. Then we find the solution of (7) in the form $[q = b, n = 2p+1, y = b \times 2^\alpha \times c \times d + 1]$ if we suppose that $b^{(n-1)/2-1} - \ldots - b + 1 = d$ and $b^{(n-1)/2-1} + \ldots + b + 1 = c$.

2.7.2 d divides $(b^\beta+1)$.
By Proposition 1.9 we see that there is no solution in this case.

2.8 $\qquad b^{\beta(n-1)/2} + 1 = 2^{\alpha-1} d^\delta, \qquad \frac{b^{\beta(n-1)/2}-1}{b^\beta-1} = 2c^\gamma.$

We check that $\beta(n-1)/2$ is even. Since $(b^{\beta(n-1)/4} - 1, b^{\beta(n-1)/4} + 1) = 2$, we consider $b^{\beta(n-1)/4} + 1 = 2c^\gamma, \frac{b^{\beta(n-1)/4}-1}{b^\beta-1} = 1$ from the second equation in 2.8. Then easily $n = 5$ and using Lemma 1.2 we solve four subcases of the equation above. But all these cases were already computed before in 2.5.

Acknowledgment. The author would like to thank Andrzej Schinzel and also the unknown referee for their careful reading of the text and their remarks.

References

[1] Bennett M., *Rational approximation to algebraic number of small height: The diophantine equation* $|ax^n - by^n| = 1$, J. Reine Angew. Math. **535** (2001), 1–49.

[2] Bilu Y.F., *Catalan's Conjecture*, Séminaire Bourbaki, 55ème année, 909, 2002.

[3] Bugeaud Y., *Linear forms in p-adic logarithms and the diophantine equation* $(x^n - 1)/(x - 1) = y^q$, Math. Proc. Cambridge Philos. Soc. **127** (1999), 373–381.

[4] Bugeaud Y., Mignotte M., *On the diophantine equation* $(x^n - 1)/(x - 1) = y^q$ *with negative* x, Proceedings of the Millennial Conference on Number Theory, Urbana-Champaign, IL, USA, 2002, pp. 145–151.

[5] Bugeaud Y., Mignotte M., Roy Y., Shorey T.N., *On the diophantine equation* $(x^n - 1)/(x - 1) = y^q$, Math. Proc. Cambridge Philos. Soc. **127** (1999), 353–372.

[6] Bugeaud Y., Mignotte M., Roy Y., *On the diophantine equation* $(x^n - 1)/(x - 1) = y^q$, Pacific J. Math. **193** (2000), 257–268.

[7] Crescenzo P., *A diophantine equation arises in the theory of finite groups*, Advances in Math. **17** (1975), 25–29.

[8] Dickson L.E., *History of the Theory of Numbers*, vol 2, AMS Chelsea, Providence, 1999.

[9] Khosravi A., Khosravi B., *On the diophantine equation* $(q^n - 1)/(q - 1) = y$, Comment. Math. Univ. Carolinae **44** (2003), no. 1, 1–7.

[10] Křížek M., Luca F., Somer L., *17 Lectures on Fermat Numbers: From Number Theory to Geometry*, Springer, New York, 2001.

[11] Ligh S., Neal L., *A note on Mersenne numbers*, Math. Mag. **47** (1974), 231–233.

[12] Ljunggren W., *Noen Setninger om ubestemte likninger av formen* $(x^n - 1)/(x - 1) = y^q$, Norsk. Mat. Tidsskr. **25** (1943), 17–20.

[13] Nagell T., *Note sur l'equation indéterminée* $(x^n - 1)/(x - 1) = y^q$, Norsk. Mat. Tidsskr. **2** (1920), 75–78.

[14] Polický Z., *Exercises of division theory leading to brand new results*, Proceedings of the International Conference The Mathematics Education into the 21st Century Project; Brno, Czech Republic, 2003, pp. 231–234.

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

[16] Saradha N., Shorey T.N., *The equation* $(x^n - 1)/(x - 1) = y^q$ *with x square*, Math. Proc. Cambridge Philos. Soc. **125** (1999), 1–19.

[17] Shorey T.N., *Exponential diophantine equation involving product of consecutive integers and related equations*, Bambah, R.P. et al., Number theory; Birkhäuser, Trends in Mathematics, Basel, 2000, pp. 463–495.

Department of Mathematics, Faculty of Science, Masaryk University, Janáčkovo nám. 2a, 662 95 Brno, Czech Republic

(*Received* January 27, 2004, *revised* February 16, 2005)