Amir Khosravi; Behrooz Khosravi
On the Diophantine equation $\frac{q^n-1}{q-1} = y$

Commentationes Mathematicae Universitatis Carolinae, Vol. 44 (2003), No. 1, 1--7

Persistent URL: http://dml.cz/dmlcz/119363

Terms of use:
© Charles University in Prague, Faculty of Mathematics and Physics, 2003

Institute of Mathematics of the Academy of Sciences of the Czech Republic provides access to
digitized documents strictly for personal use. Each copy of any part of this document must
contain these Terms of use.

This paper has been digitized, optimized for electronic delivery and stamped
with digital signature within the project DML-CZ: The Czech Digital
Mathematics Library http://project.dml.cz
On the Diophantine equation \( \frac{q^n - 1}{q - 1} = y \)

AMIR KHOSRAVI, BEHROOZ KHOSRAVI

Abstract. There exist many results about the Diophantine equation \((q^n - 1)/(q - 1) = y^m\), where \(m \geq 2\) and \(n \geq 3\). In this paper, we suppose that \(m = 1\), \(n\) is an odd integer and \(q\) a power of a prime number. Also let \(y\) be an integer such that the number of prime divisors of \(y - 1\) is less than or equal to 3. Then we solve completely the Diophantine equation \((q^n - 1)/(q - 1) = y\) for infinitely many values of \(y\). This result finds frequent applications in the theory of finite groups.

Keywords: higher order Diophantine equation, exponential Diophantine equation

Classification: 11D61, 11D41

The theory of finite groups leads to some Diophantine equations in which the variables are restricted to be prime or a power of a prime number.

There exist many results about the Diophantine equation

\[ (*) \quad \frac{q^n - 1}{q - 1} = y^m \text{ in integers } q > 1, \ y > 1, \ n > 2, \ m \geq 2. \]

A long standing conjecture claims that the Diophantine equation \((*)\) has finitely many solutions, and, may be, only those given by

\[ \frac{3^5 - 1}{3 - 1} = 11^2, \quad \frac{7^4 - 1}{7 - 1} = 20^2, \quad \text{and} \quad \frac{18^3 - 1}{18 - 1} = 7^3. \]

Among the known results, let us mention that Ljunggren [14] solved \((*)\) completely when \(m = 2\) and Ljunggren [14] and Nagell [16] when \(3|n\) and \(4|n\): they proved that in these cases there is no solution, except the previous ones.
Also Equation (\textit{*}) is completely solved when \( q \) is square (there is no solution in this case [17], [5], [1]); when \( q \) is a power of any integer in the interval \{2, \cdots , 10\} (the only two solutions are listed above [4]); when \( q \) is a power of a prime number, say \( p \), and \( p\mid y - 1 \) [4]; or when \( m \) is a prime number and every prime divisor of \( q \) also divides \( y - 1 \) [6].

For more information and in particular for finiteness type results under some extra hypothesis, we refer the reader to Shorey & Tijdeman [19], [20] and to the survey of Shorey [18].

If \( k \) is an integer, then \( \pi(k) \) is the set of prime divisors of \( k \). Y. Bugeaud and M. Mignotte in [4] solved the Equation (\textit{*}) when \( m \geq 2 \) and \( q \) be a power of a prime number, say \( p \), and \( p\mid y - 1 \). Hence in this paper we consider Equation (\textit{*}) when \( m = 1 \) and \( q \) be a power of a prime number, say \( p \). Obviously \( p\mid y - 1 \). Also we let \( 2 \nmid n \) and \( |\pi(y - 1)| \leq 3 \). Then we solve completely the Diophantine equation \( \frac{q^n - 1}{q - 1} = y \). This result finds frequent applications in the theory of finite groups.

\textbf{Lemma A ([4], [8]).} With the exceptions of the relations \((239)^2 - 2(13)^4 = -1 \) and \( 3^5 - 2(11)^2 = 1 \), every solution of \[ p_1^r - 2p_2^s = \pm 1; \quad p_1, p_2 \text{ primes}; \quad r, s > 1, \] has exponents \( r = s = 2 \); i.e., it comes from a unit \( p_1 - p_2, 2^{1/2} \) of the quadratic field \( \mathbb{Q}(2^{1/2}) \) for which the coefficients \( p_1, p_2 \) are prime.

\textbf{Remark.} Although it is proved that (with two exceptions) the above equation becomes \( p_1^2 - 2p_2^2 = \pm 1 \), we do not know whether or not there are infinitely many prime pairs \( p_1, p_2 \) that satisfy this equation.

\textbf{Lemma B ([8]).} The only solution of the equation \( p_1^r - p_2^s = 1 \), where \( p_1, p_2 \) are prime numbers and \( r, s > 1 \), is \( 3^2 - 2^3 = 1 \).

\textbf{Remark ([11]).} If \( n > 1 \) and \( a^n - 1 \) is prime, then \( a = 2 \) and \( n \) is prime, but the converse is not true. Prime numbers of the form \( 2^n - 1 \) are called \textit{Mersenne primes}.

Also if \( a \geq 2 \) and \( a^n + 1 \) is prime, then \( a \) is even and \( n = 2^k \), but the converse is not true. Prime numbers of the form \( 2^n + 1 \) are called \textit{Fermat primes}.

\textbf{Main Theorem.} Let \( q \) be a power of a prime number, \( |\pi(y - 1)| \leq 3 \) and \( n \geq 3 \) an odd integer. Then the solutions of the Diophantine equation

\[ \frac{q^n - 1}{q - 1} = y, \]

are listed in table (I):
On the Diophantine equation $\frac{q^n - 1}{q - 1} = y$

<table>
<thead>
<tr>
<th>$q$</th>
<th>$n$</th>
<th>$y$</th>
<th>conditions</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>3</td>
<td>7</td>
<td>$p$ is a Fermat prime</td>
</tr>
<tr>
<td>8</td>
<td>3</td>
<td>73</td>
<td></td>
</tr>
<tr>
<td>$p - 1$</td>
<td>3</td>
<td>$p^2 - p + 1$</td>
<td>$p$ is a prime number</td>
</tr>
<tr>
<td>$p$</td>
<td>3</td>
<td>$p^2 + p + 1$</td>
<td>$p$ is a Mersenne prime</td>
</tr>
<tr>
<td>2</td>
<td>7</td>
<td>127</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>5</td>
<td>31</td>
<td></td>
</tr>
<tr>
<td>$2^\alpha$</td>
<td>5</td>
<td>$\frac{2^{2\alpha} - 1}{2^\alpha - 1}$</td>
<td>$2^{\alpha} + 1$ and $2^{2\alpha} + 1$ are Fermat primes, $\alpha \geq 1$</td>
</tr>
<tr>
<td>$p$</td>
<td>3</td>
<td>$p^2 + p + 1$</td>
<td>$p$ is a prime number</td>
</tr>
<tr>
<td>$2p - 1$</td>
<td>3</td>
<td>$4p^2 - 2p + 1$</td>
<td>$2p - 1$ is a prime number</td>
</tr>
<tr>
<td>3</td>
<td>5</td>
<td>121</td>
<td></td>
</tr>
<tr>
<td>$239^2$</td>
<td>3</td>
<td>3262865763</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>5</td>
<td>2801</td>
<td></td>
</tr>
<tr>
<td>$p^2$</td>
<td>3</td>
<td>$p^4 + p^2 + 1$</td>
<td>$p^4 + 1 = p^2$ where $p$ is a prime number</td>
</tr>
<tr>
<td>$b$</td>
<td>5</td>
<td>$\frac{b^n - 1}{b - 1}$</td>
<td>$b = 2^{\alpha} - 1$ and $p = 2^{2\alpha} - 2^{\alpha - 1} + 1$ are prime</td>
</tr>
</tbody>
</table>

**Proof:** Let $(q, n, y)$ be a solution of (1). Let $y = A + 1$, where $|\pi(A)| \leq 3$. Then

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

Also $(q^{n-1}/2 - 1, q^{n-1}/2 + 1)|2, q - 1|q^{n-1}/2 - 1$ and hence $q^{n-1}/2 + 1|A$.

If $|\pi(A)| = 1$ then $n = 2$, since $(q, \frac{2^{n-1} - 1}{2^n - 1}) = 1$, which is a contradiction.

If $|\pi(A)| = 2$ then $y = x^\alpha p^\beta + 1$, where $p, x$ are prime numbers and $\alpha, \beta$ are positive integers. Now we have $q(q^{n-1} - 1)/(q - 1) = x^\alpha p^\beta$. Therefore $q = x^\alpha$ or $q = p^\beta$. Let $q = x^\alpha$ then $q^{n-1}/2 + 1 = p^\beta$, for some $\beta \leq \beta$. Therefore $p = 2$ or $x = 2$, and hence $y = 2^{\alpha} p^\beta + 1$. Now we consider two cases:

**Case 1. $q = 2^\alpha$**

Then $q^{n-1}/2 + 1 = p^\beta$ and $\frac{q^{n-1}/2 - 1}{q - 1} = 1$, since $(q^{n-1}/2 - 1, q^{n-1}/2 + 1) = 1$.

Hence $n = 3, 2^{\alpha} + 1 = p^\beta$. If $\alpha = 1$ then $p^\beta = 3$, and hence $(2, 3, 7)$ is a solution of (1). If $\alpha, \beta > 1$ then $\alpha = 3, p^\beta = 3^2$ by Lemma B. Hence $(8, 3, 73)$ is a solution of (1), too. If $\beta = 1$ then $p = 2^{\alpha} + 1$. Since $p$ is a prime number, $\alpha = 2^t$. Hence if $p = 2^{2t} + 1, t \geq 1$, is a prime number, then $(p - 1, 3, p^2 - p + 1)$ is a solution of (1). Special cases are $(4, 3, 21), (16, 3, 273), (256, 3, 65793)$. 

Case 2. \( q = p^\beta \)

Obviously if \( n \neq 3 \) then \( \frac{q^{(n-1)/2} - 1}{q - 1} > 2 \). Therefore \( \frac{q^{(n-1)/2} - 1}{q - 1} = 1 \) and \( q^{(n-1)/2} + 1 = 2^\alpha \) which implies that \( n = 3, p^\beta + 1 = 2^\alpha \). By using Lemma B, \( \beta = 1, p = 2^\alpha - 1 \), and hence \( \alpha \) is a prime number. Therefore if \( p = 2^\alpha - 1 \) is a prime number, then \( (p, 3, p^2 + p + 1) \) is a solution of (1). Special cases are \( (3, 3, 13), (7, 3, 57) \).

If \( |\pi(A)| = 3 \), then \( y = a^\alpha b^\beta p^\lambda + 1 \), where \( \alpha, \beta \) and \( \lambda \) are positive integers. Similar to the case \( |\pi(A)| = 2 \), we have \( y = 2^\alpha b^\beta p^\lambda + 1 \), and \( q = 2^\alpha \) or \( q = b^\beta \) or \( q = p^\lambda \), where \( \alpha, \beta \) and \( \lambda \) are positive integers.

Step 1. \( q = 2^\alpha \)

Then

\[
2^{\alpha(n-1)/2} + 1 = p^\lambda \quad \text{and} \quad \frac{2^{\alpha(n-1)/2} - 1}{2^\alpha - 1} = b^\beta.
\]

Obviously \( n \neq 3 \), since \( \beta \neq 0 \). Now we consider 3 cases:

(1.1) If \( \alpha(n-1)/2 = 1 \) then \( \beta = 0 \), which is a contradiction.
(1.2) If \( \alpha(n-1)/2 > 1, \lambda > 1 \) then \( \alpha(n-1)/2 = 3 \) and \( p^\lambda = 3^2 \), by Lemma B.

Then \( n = 7 \) and \( \alpha = 1 \), since \( n \neq 3 \). Hence \((2, 7, 127)\) is a solution of (1).
(1.3) If \( \lambda = 1 \) then \( p = 2^{\alpha(n-1)/2} + 1 \). Hence \( \alpha(n-1)/2 = 2^t > 1 \), since \( p \) is a prime number. Therefore

\[
b^\beta = \frac{2^{\alpha(n-1)/2} - 1}{2^\alpha - 1} = \frac{(2^{\alpha(n-1)/4} - 1)(2^{\alpha(n-1)/4} + 1)}{2^\alpha - 1}
\]

and since \( (2^{\alpha(n-1)/4} - 1, 2^{\alpha(n-1)/4} + 1) = 1 \) we have \( n = 5 \), and \( p = 2^{2^\alpha} + 1 \). Hence \( b^\beta = 2^\alpha + 1 \). Now we consider 3 subcases:

(1.3.1) If \( \alpha = 1 \) then \( b^\beta = 3, p = 5 \) and \( y = 31 \). Hence \((2, 5, 31)\) is a solution of (1).
(1.3.2) If \( \alpha > 1, \beta > 1 \) then \( b^\beta = 3^2 \) and \( \alpha = 3 \) by Lemma B. But then \( p = 65 \) which is not a prime number, a contradiction.
(1.3.3) If \( \beta = 1 \) then \( b = 2^\alpha + 1 \) and \( p = 2^{2^\alpha} + 1 \). Hence \((2^\alpha, 5, 2^{4\alpha} + 2^{3\alpha} + 2^{2\alpha} + 2^\alpha + 1)\) is a solution of (1), where \( 2^\alpha + 1 \) and \( 2^{2\alpha} + 1 \) are prime numbers.

Step 2. \( q = b^\beta \)

Then \( (q^{(n-1)/2} - 1, q^{(n-1)/2} + 1) = 2 \), and \( n \neq 3 \). Similar to the last step we have 3 subcases:

(2.1) If

\[
\frac{b^{\beta(n-1)/2} - 1}{b^\beta - 1} = 2p^\lambda, \quad b^{\beta(n-1)/2} + 1 = 2^\alpha - 1,
\]
then $\beta(n-1)/2 = 1$, by Lemma B, which is a contradiction since $n > 3$.

(2.2) If

$$\frac{b^{\beta(n-1)/2} - 1}{b^\beta - 1} = p^\lambda, \quad b^{\beta(n-1)/2} + 1 = 2^\alpha,$$

then similarly to (2.1), we have $n = 3$ which is a contradiction.

(2.3) If

$$\frac{b^{\beta(n-1)/2} - 1}{b^\beta - 1} = 2^{\alpha-1}, \quad b^{\beta(n-1)/2} + 1 = 2p^\lambda,$$

then by using Lemma A we consider 4 cases:

(2.3.1) If $\beta(n-1)/2 = 1$ then $n = 3$, $\beta = 1$ and $q = b$. Then $\alpha = 1$, $b + 1 = 2p^\lambda$. Hence if $(b, p, \lambda)$ is a solution of the Diophantine equation $b + 1 = 2p^\lambda$, then $(b, 3, b^2 + b + 1)$ is a solution of (1).

(2.3.2) If $\lambda = 1$ then $b^{\beta(n-1)/2} + 1 = 2p$. Let $m = \frac{n-1}{2}$. Hence $q^m - 1 = 2^{\alpha-1}(q - 1)$ and $q^m + 1 = 2p$.

If $m$ is odd and $m > 1$ then $2p = q^m + 1 = (q + 1)(q^{m-1} - \cdots + 1)$, which is a contradiction, since $p$ is a prime number. Therefore $m = 1$, $\alpha = 1$ and hence $y = 2b^\beta p + 1$, $2p = b^\beta + 1$. Hence if $p$ is a prime number and $2p - 1$ is a power of a prime number then $(2p - 1, 3, 4p^2 - 2p + 1)$ is a solution of (1).

If $m$ is even then let $m = 2k$. Now we have $(q^k - 1)(q^k + 1) = 2^{\alpha-1}(q - 1)$. Therefore $k = 1$, $n = 5$ and $q + 1 = 2^{\alpha-1}$. Hence $b^\beta + 1 = 2^{\alpha-1}$. By using Lemma B, $\beta = 1$ and hence $b = 2^{\alpha-1} - 1$. Now if $b = 2^{\alpha-1} - 1$ and $p = 2^{2\alpha-3} - 2^{\alpha-1} + 1$ are prime numbers, then $(b, 5, b^4 + b^3 + b^2 + b + 1)$ is a solution of (1). But we guess that the only possible case is $(3, 5, 121).

(2.3.3) If $p^\lambda = 13^4$ and $b^{\beta(n-1)/2} = 239^2$ then $\beta(n-1)/2 = 2$.

If $\beta = 2$, $n = 3$ then $\alpha = 1$ and $y = 3262865763$.

If $\beta = 1$, $n = 5$ then $\frac{239^2 - 1}{239 - 1} = 240$ which is not a power of 2, which is a contradiction. Hence $(239^2, 3, 3262865763)$ is a solution of (1).

(2.3.4) If $\lambda = 2$ and $\beta(n-1)/2 = 2$ then we have two subcases:

(2.3.4.1) If $\beta = 1$, $n = 5$ then $b^2 + 1 = 2p^2$ and $b + 1 = 2^{\alpha-1}$. Hence $p^2 = 2^{2\alpha-3} - 2^{\alpha-1} + 1$ which implies that $(p-1)(p+1) = 2^{\alpha-1}(2^{\alpha-2} - 1)$. Therefore $p - 1 = 2^{\alpha-2}$ and $p + 1 = 2(2^{\alpha-2} - 1)$. Hence $\alpha = 4$, $p = 5$, $b = 7$ and $y = 2801$. Therefore $(7, 5, 2801)$ is a solution of (1).

(2.3.4.2) If $\beta = 2$ and $n = 3$ then $b^2 + 1 = 2p^2$. Hence if $b$ and $p$ are odd prime numbers such that $b^2 + 1 = 2p^2$ then $(b^2, 3, b^4 + b^2 + 1)$ is a solution of (1).

(2.4) If

$$\frac{b^{\beta(n-1)/2} - 1}{b^\beta - 1} = 2^\alpha, \quad b^{\beta(n-1)/2} + 1 = p^\lambda,$$
then we get a contradiction since \( b \) and \( p \) are odd numbers.

Now the proof of the main theorem is completed. \( \square \)

**Remark.** Sometimes in the theory of finite groups we need the solutions of (1), where \( y \) is prime.

**References**


241, Golnaz Street, Golbahar Street, Daneshjou Blvd., Velenjak, Tehran 19847, Iran

Faculty of Mathematical Sciences and Computer Engineering, University for Teacher Education, 599 Taleghani Ave., Tehran 15614, Iran

E-mail: khosraobbb@yahoo.com

(Received June 1, 2002, revised November 18, 2002)