ON THE BASIC CHARACTER OF RESIDUE CLASSES

P. HILTON, J. HOOPER AND J. PEDERSEN

Abstract

Let \( t, b \) be mutually prime positive integers. We say that the residue class \( t \mod b \) is basic if there exists \( n \) such that \( t^n \equiv -1 \mod b \); otherwise \( t \) is not basic. In this paper we relate the basic character of \( t \mod b \) to the quadratic character of \( t \) modulo the prime factors of \( b \). If all prime factors \( p \) of \( b \) satisfy \( p \equiv 3 \mod 4 \), then \( t \) is basic \( \mod b \) if \( t \) is a quadratic non-residue \( \mod p \) for all such \( p \); and \( t \) is not basic \( \mod b \) if \( t \) is a quadratic residue \( \mod p \) for all such \( p \). If, for all prime factors \( p \) of \( b, p \equiv 1 \mod 4 \) and \( t \) is a quadratic non-residue \( \mod p \), the situation is more complicated. We define \( d(p) \) to be the highest power of 2 dividing \( (p-1) \) and postulate that \( d(p) \) takes the same value for all prime factors \( p \) of \( b \). Then \( t \) is basic \( \mod b \). We also give an algorithm for enumerating the (prime) numbers \( p \) lying in a given residue class \( \mod 4t \) and satisfying \( d(p) = d \). In an appendix we briefly discuss the case when \( b \) is even.

0. Introduction

In a series of papers [1, through 4], culminating in the monograph [5], Hilton and Pedersen developed an algorithm – in fact, two algorithms, one being the reverse of the other – for calculating the quasi-order of \( t \mod b \), where \( t, b \) are mutually prime positive integers, and determining whether \( t \) is basic \( \mod b \). Here the quasi-order of \( t \mod b \) is the smallest positive integer \( k \) such that \( t^k \equiv \pm 1 \mod b \); and \( t \) is said to be basic if, in fact, \( t^k \equiv -1 \mod b \). Thus \( t \) is basic if and only if the order of \( t \mod b \) is twice the quasi-order of \( t \mod b \) (in the contrary case the quasi-order and the order coincide). Froemke and Grossman carried the number-theoretical investigation considerably further in [6] and drew attention to the importance, where \( b \) is prime, of the quadratic character of \( t \mod b \) in their arguments.

Our object in this paper is to relate the basic character of \( t \mod b \) to the quadratic character of \( t \) modulo the prime factors of \( b \). We assume \( b \) odd, but add a few remarks in an appendix on the case when \( b \) is even.

Given a pair \( (t, p) \) where \( p \) is an odd prime not dividing \( t \), we distinguish 4 possibilities as follows: \( t \) may or may not be a quadratic residue \( \mod p \), and we may have \( p \equiv 1 \mod 4 \) or \( p \equiv 3 \mod 4 \). We restrict attention, in our
discussion of the basic character of $t \mod b$, to the situation in which all prime factors $p$ of $b$ place $(t, p)$ in the same class. If $t$ is a quadratic residue $\mod p$ and $p \equiv 1 \mod 4$, we are unable to draw any general conclusion about the basic character of $t \mod p$. Thus, for example, $7^7 \equiv 1 \mod 29$, $7^7 \equiv -1 \mod 113$, and $7$ is a quadratic residue modulo 29 or 113. If all prime factors $p$ of $b$ satisfy $p \equiv 3 \mod 4$, it is easy to draw general conclusions about the basic character of $t \mod b$; our results are given in Section 2.

The most interesting case for our purposes is that in which $t$ is not a quadratic residue $\mod p$ and $p \equiv 1 \mod 4$, for all prime factors $p$ of $b$. It then becomes important to be able to calculate the function $d(p)$, where $d(p) = d$ if $p = 1 + 2^d\ell$, with $\ell$ odd. Thus $d$ is a positive integer and, in fact, $d \geq 2$ in the case we are discussing. Since the quadratic character of $t \mod p$ depends only on the residue class of $p \mod 4t$, we give an algorithm for enumerating those primes $p$, as functions of $s$ and $d$, such that

\begin{equation}
(0.1) \quad d(p) = d, \quad p \equiv s \mod 4t, \quad 1 \leq s \leq 4t - 3.
\end{equation}

If the prime factors $p$ of $b$ are confined to those satisfying (0.1) for fixed $s$, $d$, then, as we show in Section 3, $t$ is basic $\mod b$.

In Section 1 we announce some elementary results which are used in proving our main theorems.

Throughout the paper we use the symbol $\varepsilon$ for a number which is $+1$ or $-1$.

1. Some preliminary lemmas

The first result extends to the quasi-order a familiar result on order.

Lemma 1.1. Let the quasi-order of $t \mod b$ be $n$ and let $t^m \equiv \varepsilon \mod b$. Then $n|m$.

Proof: Let $m = qn + r$, $0 \leq r < n$, and $t^n \equiv \eta \mod b$, $\eta = \pm 1$. Then $t^r = t^m(t^n)^{-q} \equiv \varepsilon\eta^q = \pm 1 \mod b$, so that $r = 0$.

We now restrict $b$ by the condition $b \geq 3$, so that the basic character of $t \mod b$ comes into question.

Lemma 1.2. The residue $t \mod b$ is basic if and only if $t^m \equiv -1 \mod b$ for some exponent $m$.

Proof: The necessity of the condition is obvious. Suppose then that $t^m \equiv -1 \mod b$ and that the quasi-order of $t \mod b$ is $n$. Then $n | m$, by Lemma 1.1. Thus, if $t^n \equiv 1 \mod b$, it follows that $t^m \equiv 1 \mod b$. This contradiction shows that $t^n \equiv -1 \mod b$, so that the residue $t \mod b$ is basic. $\blacksquare$
Lemma 1.3. The residue \( t \mod b \) is non-basic if \( t^m \equiv 1 \mod b \) for some odd exponent \( m \).

Proof: Let the quasi-order of \( t \mod b \) be \( n \) with \( t^n \equiv \epsilon \mod b \). Then \( n \mid m \), so that \( m = nq \). Since \( m \) is odd, \( q \) is odd. Thus \( t^m \equiv \epsilon^n = \epsilon \mod b \), so \( \epsilon = 1 \) and the residue \( t \mod b \) is non-basic. ■

Our next result is of a different kind.

Proposition 1.4. Let \( x \equiv y \mod m \). Then \( x^{m^k-1} \equiv y^{m^k-1} \mod m^k, k \geq 1 \).

Proof: We argue by induction on \( k \), the case \( k = 1 \) being trivial. If we assume \( x^{m^k-1} \equiv y^{m^k-1} \mod m^k \) for a certain \( k \geq 1 \), then

\[
    x^{m^{k+1}} = y^{m^{k+1}} + \lambda m^k,
\]

so that

\[
    x^{m^k} = (y^{m^{k-1}} + \lambda m^{k-1})^m
    = y^{m^k} + \lambda m^{k+1} y^{m^{k-1}(m-1)} + \binom{m}{2} \lambda^2 m^{2k} y^{m^{k-1}(m-2)} + \ldots
    \equiv y^{m^k} \mod m^{k+1}.
\]

This establishes the inductive step, and hence the proposition. ■

We have the immediate consequence:

Lemma 1.5. Let \( c \equiv \epsilon \mod m \), where \( m \) odd. Then \( c^{m^k-1} \equiv \epsilon \mod m^k, k \geq 1 \).

Proof: We have only to note that \( c^{m^k-1} = \epsilon \) if \( m \) is odd. ■

2. The main results

We recall the following key results on quadratic reciprocity.

Theorem 2.1 (Euler). Let \( p \) be an odd prime. Then

(i) \( t^{\frac{p-1}{2}} \equiv 1 \mod p \) if and only if \( t \) is a quadratic residue \( \mod p \);
(ii) \( t^{\frac{p-1}{2}} \equiv -1 \mod p \) if and only if \( t \) is not a quadratic residue \( \mod p \).

Theorem 2.2 (Gauss). Let \( p \) be an odd prime. Then the quadratic character of \( t \mod p \) depends only on the residue class of \( p \mod 4t \) and is the same for two odd primes \( p \) and \( q \) such that \( p \equiv -q \mod 4t \).
Thus, given \( t \) and \( p \), we distinguish 4 classes into which the pair \((t, p)\) may fall:

- I \( p \equiv 1 \mod 4, t^{\frac{p-1}{2}} \equiv 1 \mod p; \)
- II \( p \equiv 1 \mod 4, t^{\frac{p-1}{2}} \equiv -1 \mod p; \)
- III \( p \equiv 3 \mod 4, t^{\frac{p-1}{2}} \equiv 1 \mod p; \)
- IV \( p \equiv 3 \mod 4, t^{\frac{p-1}{2}} \equiv -1 \mod p; \)

We will say nothing further about residues \( t \mod b \) if \( b \) admits a factor \( p \) such that \((t, p)\) is in class I. We will henceforth, until otherwise stated, assume that \( b \) is odd.

**Theorem 2.3.** Suppose that the prime factors \( p \) of \( b \) are all such that \((t, p)\) is in Class III. Then the residue \( t \) is not basic \( \mod b \).

**Proof:** Let \( b = \prod_{i=1}^{N} p_i^{k_i}, \) \( k_i \geq 1. \) Then \( \frac{b-1}{2} \) is odd and \( t^{\frac{p_i-1}{2}} \equiv 1 \mod p_i. \)

By Lemma 1.5, \( t^{(\frac{p_i-1}{2})p_i^{k_i}-1} \equiv 1 \mod p_i^{k_i}. \) Set \( m = \prod_{i=1}^{N} (\frac{p_i-1}{2})p_i^{k_i}-1. \) Then \( m \) is odd, and

\[ t^m \equiv 1 \mod p_i^{k_i}. \]

It follows that \( t^m \equiv 1 \mod b, \) so that, by Lemma 1.3, the residue \( t \) is not basic \( \mod b. \)

**Theorem 2.4.** Suppose that the prime factors \( p \) of \( b \) are all such that \((t, p)\) is in Class IV. Then the residue \( t \) is basic \( \mod b. \)

**Proof:** We argue as for Theorem 2.3, except that now

\[ t^{(\frac{p_i-1}{2})p_i^{k_i}-1} \equiv -1 \mod p_i^{k_i}, \]

\[ t^m \equiv -1 \mod p_i^{k_i}, \]

\[ t^m \equiv -1 \mod b, \]

with \( m \) odd. We apply Lemma 1.2 to obtain the result.

**Example 2.1.** Let \( t = 7. \) Then, by Theorem 2.2, we must consider primes \( p \mod 28. \) We easily find

\[
\begin{align*}
p &\equiv 1 \text{ or } 27 \mod 28 : 7^{\frac{27-1}{2}} \equiv 1 \mod p \\
p &\equiv 3 \text{ or } 25 \mod 28 : 7^{\frac{25-1}{2}} \equiv 1 \mod p \\
p &\equiv 5 \text{ or } 23 \mod 28 : 7^{\frac{23-1}{2}} \equiv -1 \mod p \\
p &\equiv 9 \text{ or } 19 \mod 28 : 7^{\frac{19-1}{2}} \equiv 1 \mod p \\
p &\equiv 11 \text{ or } 17 \mod 28 : 7^{\frac{17-1}{2}} \equiv -1 \mod p \\
p &\equiv 13 \text{ or } 15 \mod 28 : 7^{\frac{15-1}{2}} \equiv -1 \mod p
\end{align*}
\]
Thus

\[(7, p)\text{ is in Class I if } p \equiv 1, 9, 25 \text{ mod } 28;\]
\[(7, p)\text{ is in Class II if } p \equiv 5, 13, 17 \text{ mod } 28;\]
\[(7, p)\text{ is in Class III if } p \equiv 3, 19, 27 \text{ mod } 28;\]
\[(7, p)\text{ is in Class IV if } p \equiv 11, 15, 23 \text{ mod } 28.\]

We conclude that 7 is not basic mod \(b\) if \(b\) is a product of primes \(p\) such that \(p \equiv 3, 19\) or 27 mod 28; and 7 is basic mod \(b\) if \(b\) is a product of primes \(p\) such that \(p \equiv 11, 15\) or 23 mod 28.

As we have said, no inference can be drawn if \(b\) is a product of primes \(p\) such that \(p \equiv 1, 9\) or 25 mod 28. Indeed, the fact that \((7, p)\) is then in Class I is a special case of the following phenomenon, which we describe here for the sake of completeness.

**Proposition 2.5.** Let \(p\) be an odd prime such that \(p = k^2 + 4l\). Then any factor of \(l\) is a quadratic residue mod \(p\).

**Proof:** It suffices to prove this for prime factors \(q\) of \(l\). Now if \(q = 2\), then \(p \equiv 1 \text{ mod } 8\), so 2 is a quadratic residue mod \(p\). If \(q\) is odd, then \(p\) is a quadratic residue mod \(q\) and \(\frac{p-1}{2}\) is even, so that, by quadratic reciprocity, \(q\) is a quadratic residue mod \(p\). \(\square\)

Note that it follows, by Theorem 2.1, that \(7^{\frac{p-1}{2}} \equiv 1 \text{ mod } p\) if \(p \equiv 1, 9\) or 25 mod 28.

We will devote the next section to a discussion of the Class II. At this point, we are content to remark

**Theorem 2.6.** Suppose that \(b = p^k\), where \((t, p)\) is in Class II. Then the residue \(t\) is basic mod \(b\).

**Proof:** \(t^{(p-1)/2}p^{k-1} \equiv -1 \text{ mod } p^k\). Apply Lemma 1.2. \(\square\)

In the next section we generalize this obvious conclusion.

### 3. The class II situation

We define a function \(d\) from positive integers \(\geq 2\) to non-negative integers by

\[(3.1) \quad d(n) = d \leftrightarrow 2^d \mid (n-1), \ 2^{d+1} x(n-1).\]

Notice that, for an odd prime \(p\), \(d(p) \geq 1\) and that \(d(p) \geq 2\) if \((t, p)\) is in Class II. Let \(d\) be a fixed integer \(\geq 2\); we then have the following theorem, generalizing Theorem 2.6.
in this way, splitting the inequality \( d(p) \geq d \) into the two possibilities \( d(p) = d \) or \( d(p) \geq d + 1 \). We demonstrate this tree in Figure 1.

\[
1 + 2^N b, \quad N \geq M \\
\quad \quad \quad d \geq M
\]

- if \( N = M \) stops, \( d = M \)
- if \( N > M \) goes on, \( d \geq M + 1 \)

General Case

Figure 1

\[
5, \quad d \geq 2
\]

\[
5, \quad d = 2 \\
33, \quad d \geq 3
\]

\[
33, \quad d \geq 4 \\
145, \quad d = 4
\]

\[
33, \quad d = 5 \\
257, \quad d \geq 6
\]

\[
257, \quad d \geq 7 \\
705, \quad d = 6
\]

\[ p \equiv 5 \mod 28 \]

Special Case

Figure 1

The tree provides the conceptual basis for the proof (see Theorem 3.2) that the primes \( p \) satisfying the congruence \( p \equiv 2^d c + 1 \mod 2^{d+1} u \) constitute the totality of the primes \( p \) satisfying \( p \equiv s \mod 4t \) and \( d(p) = d \). For we may argue by induction on \( d \) that there is only one residue class \( \mod 2^{d+1} u \) containing such primes. We assume \( n \geq m + 2 \) and we rewrite (3.4) as

\[
2^d c(d) \equiv 2^u v \mod u,
\]
to emphasize the dependence of \( c \) on \( d \); recall \( d \geq m+2 \). We start the induction (and the tree) by rewriting \( p \equiv s \mod 4t \), using (3.11), as

\[(3.12) \quad p \equiv 1 + 2^{m+2}c(m+2) \mod 2^{m+2}u.\]

Then (3.12) branches into the two congruences

\[(3.13) \begin{cases} p \equiv 1 + 2^{m+2}c(m+2) \mod 2^{m+3}u, \\ p \equiv 1 + 2^{m+2}c(m+2) + 2^{m+2}u \mod 2^{m+3}u, \end{cases}\]

the sign being chosen so that the right-hand side is in the range \((0, 2^{m+3}u)\). The first possibility in (3.13) yields \( d(p) = m+2 \) (recall that \( c(d) \) is always odd) and the second yields \( d(p) \geq m+3 \), since \( u \) is also odd. Thus our assertion holds in the initial case \( d = m+2 \).

Now assume inductively that, for \( d(p) \geq d \), we require

\[(3.14) \quad p \equiv 1 + 2^d c(d) \mod 2^d u,\]

for some \( d \geq m+2 \). Then, as above, we find that, for \( d(p) = d \), we require

\[(3.15) \quad p \equiv 1 + 2^d c(d) \mod 2^{d+1} u;\]

while, for \( d(p) \geq d + 1 \), we require

\[(3.16) \quad p \equiv 1 + 2^d c(d) + 2^d u \mod 2^{d+1} u.\]

This shows the uniqueness of the residue class \( \mod 2^{d+1} u \) of \( p \), given \( d(p) = d \). But it also shows that, if \( c(d+1) \) is to be odd, to satisfy the inequality \( 1 \leq c(d+1) \leq 2u - 1 \), and to render \( p \equiv 1 + 2^{d+1} c(d+1) \mod 2^{d+1} u \) equivalent to (3.16), then \( c(d+1) \) is determined by

\[(3.17) \quad c(d+1) = \begin{cases} \frac{1}{2}(c(d) + u) & \text{if } \frac{1}{2}(c(d) + u) \text{ is odd} \\ \frac{1}{2}(c(d) - u) & \text{if } \frac{1}{2}(c(d) - u) \text{ is odd and positive} \\ \frac{1}{2}(c(d) + 3u) & \text{if } \frac{1}{2}(c(d) - u) \text{ is odd and negative} \end{cases}\]

Thus, in any case, \( 2c(d+1) \equiv c(d) \mod u \), so that, if \( 2^d c(d) \equiv 2^n u \mod u \), then \( 2^{d+1} c(d+1) \equiv 2^n u \mod u \). This establishes the inductive step and also gives us a recurrence relation (3.17) for determining \( c(d) \). Of course, this recurrence relation is deducible from

\[(3.18) \quad 2c(d+1) \equiv c(d) \mod u,\]

which also shows why the period of \( c(d) \) is the order of \( 2 \mod u \).

We emphasize that (3.17), together with the initial congruence \( c(m+2) \equiv 2^{n-m-2} u \mod u \), gives a practical algorithm for determining the values \( c(d) \)
recall that \( c(d) \) is odd with \( 1 \leq c(d) \leq 2u - 1 \). We then apply Theorem 3.2 to determine the primes \( p \) in a given residue class mod \( 4t \) and satisfying \( d(p) = d \).

Example 3.2. Let \( t = 11, s = 5 \), so that \( p \equiv 5 \mod 44 \). Thus

\[
\begin{align*}
    s &= 5, \quad u = 11, \quad m = 0 \\
    t &= 11, \quad v = 1, \quad n = 2
\end{align*}
\]

To calculate \( c(d) \) we start the induction with \( c(2) \equiv 1 \mod 11 \), so \( c(2) = 1 \). Now \( l \), the order of \( 2 \mod 11 \), is 10, so the period of \( c(d) \) is 10, and (3.17) yields the table

<table>
<thead>
<tr>
<th>( d )</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>11</th>
</tr>
</thead>
<tbody>
<tr>
<td>( c )</td>
<td>1</td>
<td>17</td>
<td>3</td>
<td>7</td>
<td>9</td>
<td>21</td>
<td>5</td>
<td>19</td>
<td>16</td>
<td>13</td>
</tr>
</tbody>
</table>

The tree diagram is shown in Figure 2.

\[
\begin{align*}
    d = 2, \quad d \geq 2 \\
    d = 4, \quad d \geq 4 \\
    d = 5, \quad d \geq 5
\end{align*}
\]

Notice that not only does \( c(d) \) repeat from \( d = 12 \) onwards, but that the whole tree pattern repeats.
We introduce the equivalence relation $t \sim t'$ in the set of positive integers, defined by

(4.1) \[ t \sim t' \iff t/t' \text{ is the square of a rational number.} \]

It is then plain that $t$ is a quadratic residue mod $p$ if and only if $t'$ is a quadratic residue mod $p$ (where $t \sim t'$ and $t, t'$ are both prime to $p$). This shows that the class, in the sense of Section 2, to which $(t, p)$ belongs depends only on the equivalence class of $t$. Thus our conclusions embodied in Theorems 2.3, 2.4, 2.6 and 3.1 apply to entire equivalence classes of integers $t$. Moreover, it follows that, insofar as we only exploit these results, we may assume that $t$ is square-free. This has the important effect that, in applying the techniques of Section 3 to provide an explicit description of those primes $p$ such that $(t, p)$ is in class II and $d(p) = d$, we may, in practice, confine attention to $m = 0$ or $1$. Of course, the formal analysis for $t = 12$, say, is different from that for $t = 3$, but the conclusions are coextensive—and the same!

Indeed, so far as the methods of this paper are concerned, we may really confine ourselves to the case that $t$ is itself a prime. For it is trivial to derive the quadratic character of $t$ from the quadratic characters of its prime factors; and our deductions are exclusively based on the quadratic character of $t$ modulo the prime factors of $b$. Notice that we are far from saying that the basic character of $t$ mod $b$ can be deduced from that of the prime factors of $t$—just as we do not claim that, in general, the basic character of $t$ mod $b$ depends only on the equivalence class of $t$ under the equivalence relation (4.1). For example, 4 is basic mod 17 but 1 is not. It remains to make a remark if $b$ is even. We do not attempt a careful analysis of this case, but we point out the following

**Proposition 4.1.** Let $t, b$ be mutually prime odd numbers. Then the basic character of $t$ mod $b$ coincides with the basic character of $t$ mod $2b$.

**Proof:** Let the quasi-order of $t$ mod $b$ be $n$, and let $t^n \equiv e \mod b$. Since $t^n - e$ is even, it follows that $t^n \equiv e \mod 2b$. It next follows that $n$ is the quasi-order of $t$ mod $2b$; for the quasi-order of $t$ mod $2b$ is seen to be neither less than nor greater than the quasi-order of $t$ mod $b$. This proves the proposition. ■

Finally, we analyse the basic character of $t$ mod $2^n$, $n \geq 2$; of course, $t$ is then odd.

**Theorem 4.2.** Let $d(t) = q \geq 2$. Then the quasi-order of $t$ mod $2^n$ is

\[
\begin{align*}
1 & \quad \text{if } n \leq q \\
2^{n-q} & \quad \text{if } n > q.
\end{align*}
\]
Moreover, \( t \) is not basic mod \( 2^n \).

**Proof.** We have \( t = 1 + c2^q \), with \( c \) odd. The conclusion is obvious if \( n \leq q \). Let \( n > q \). Now since
\[
(t^{2^{r-1}} - 1)(t^{2^{r-1}} + 1) = t^{2^r} - 1, \quad r \geq 1
\]
it follows by an easy inductive argument on \( r \) that
(4.2) \[ d(t^{2^r}) = q + r, \quad r \geq 0; \]
plainly
(4.3) \[ t^{2^r} + 1 \equiv 2 \mod 4, \quad r \geq 0. \]
Thus
\[ t^{2^{n-q}} \equiv 1 \mod 2^n, \]
while
\[ t^{2^{n-q}-1} \not\equiv \pm 1 \mod 2^n, \]
establishing the theorem. \( \blacksquare \)

We can also handle the case \( q = 1 \). Thus let us suppose \( d(t) = 1 \), so that
\[ t = 1 + 2c, \quad \text{with } c \text{ odd}. \]
We write
(4.4) \[ t = -1 + 2^q'c', \quad \text{with } c' \text{ odd}; \]
notice that \( q' \geq 2 \).

**Theorem 4.3.** If \( t \) is given by (4.4), with \( q' \geq 2 \), then
(i) if \( n \leq q' \), the quasi-order of \( t \) mod \( 2^n \) is 1 and \( t \) is basic;
(ii) if \( n > q' \), the quasi-order of \( t \) mod \( 2^n \) is \( 2^{n-q'} \) and \( t \) is not basic.

**Proof:** (i) is obvious. Thus we suppose \( n > q' \). As before, we exploit the identity
\[
(t^{2^{r'-1}} - 1)(t^{2^{r'-1}} + 1) = t^{2^{r'}} - 1,
\]
but now only for \( r \geq 2 \). For we deduce from (4.4) that \( t^2 = 1 + 2^{q'+1}c'' \), with \( c'' \) odd.
Thus
\[ d(t^{2^r}) = q' + r, \quad r \geq 1, \]
and
\[ t^{2^r} + 1 \equiv 2 \mod 4, \quad r \geq 1. \]
This shows that
\[ t^{2^{n-q'}} \equiv 1 \mod 2^n, \]
\[ t^{2^{n-q'}-1} \not\equiv \pm 1 \mod 2^n, \]
establishing the theorem.
References


P. Hilton: Department of Mathematical Sciences
SUNY Binghamton
Binghamton, New York 13901 USA

J. Hooper: Department of Mathematics
University of Utah
Salt Lake City, Utah 84112 USA

J. Pedersen: Department of Mathematics
University of Santa Clara
Santa Clara, California 95053 USA

Rebut el 12 de Setembre de 1988