On the prime decomposition of integers of the form $\dfrac{z^n - y^n}{z - y}$

Rachid Marsli
Preparatory Math Department
King Fahd University of Petroleum and Minerals
Dhahran, 31261
Kingdom of Saudi Arabia
rmarsliz@kfupm.edu.sa

June 4, 2019

Abstract

In this work, the author shows a sufficient and necessary condition for an integer of the form $\frac{z^n - y^n}{z - y}$ to be divisible by some perfect mth power p^m, where p is an odd prime and m is a positive integer. A constructive method of this type of integers is explained with details and examples. Links between the main result and known ideas such as Fermat's last theorem, Goormaghtigh conjecture and Mersenne numbers are discussed. Other related ideas, examples and applications are provided.

AMS Subj. Class.:11A07 ; 11D41

Keywords: primitive root modulo integer; prime integer, perfect nth power; Fermat's last theorem, Goormaghtigh conjucture.

1 Introduction

Contrary to our expectations, while we were trying to prove Fermat's last theorem by showing that if y and z are relatively prime and n and p are odd prime integers, then p^n does not divide $\frac{z^n - y^n}{z - y}$, we found that for almost every p we can construct infinitely many integers of the form $\frac{z^n - y^n}{z - y}$ each of which is divisible by p^n.

Not only that, but no matter how large is the positive integer m, we can always construct integers of the form $\frac{z^n - y^n}{z - y}$ that are divisible by p^m. The main tool of our analysis in this work, is the concept of primitive root modulo integer. Given a positive integer p, we say that r is a primitive root modulo p if r is an integer relatively prime to p and the smallest integer a such that $r^a \equiv 1 \pmod{p}$ is $\phi(p)$, where ϕ denotes the well-known Euler function. A positive integer possesses a primitive root if and only if $n = 2, 4, p^t$ or $2p^t$, where p is an odd prime and t is a positive integer [4, Theorem 8.14]. Another important fact about primitive roots is given by the following theorem which we state as a lemma for its use in the proof of the main result.

Lemma 1.1. *[4, Theorem 8.9] Let p be an odd prime, then p^k has a primitive root for all positive integer k. Moreover, if r is a primitive root modulo p^2, then r is a primitive root modulo p^k, for all positive integer k.*

Note that there are some rare cases where a primitive root modulo p is not a primitive root modulo p^2. As an example, the prime integer $p = 487$ has a primitive root $r = 10$ which is not a primitive root modulo 487^2 [4, Section 8.3]. More elementary ideas about primitive roots modulo integers can be found in number theory textbooks such as [1], [3], [4], [5], [6] and [9]. Throughout the paper, the greatest common divisor of two integers a and b is denoted (a, b).

2 Main result

The following lemma is needed in the proof of the main result and contains some ideas that are well-known to mathematicians working on Fermat's last theorem. Nevertheless, we prefer to provide a proof because we couldn't find a reference where all the three assertions of the lemma are proved together.

Lemma 2.1. *Let y and z be two relatively prime integers with $z \neq y$ and let n be an odd prime integer.*

1. If n divides $z - y$, then $\left(z - y\ ,\ \frac{z^n - y^n}{z - y}\right) = n$.

2. If n does not divides $z - y$, then n, $(z - y)$ and $\frac{z^n - y^n}{z - y}$ are pairwise relatively prime.

3. n^2 does not divide $\frac{z^n - y^n}{z - y}$.

Proof. We have

$$z^n = (z - y + y)^n = \sum_{i=2}^{n} \binom{n}{i} (z - y)^i \, y^{(n-i)} + n(z - y)y^{(n-1)} + y^n,$$

from which,

$$\begin{aligned} z^n - y^n &= (z-y)\Big[\sum_{i=2}^{n} \binom{n}{i} (z-y)^{(i-1)}\, y^{(n-i)} + ny^{(n-1)}\Big] \\ &= (z-y)\Big[(z-y)\Big\{\sum_{i=2}^{n} \binom{n}{i} (z-y)^{(i-2)}\, y^{(n-i)}\Big\} + ny^{(n-1)}\Big], \end{aligned}$$

so that

$$\frac{z^n - y^n}{z-y} = (z-y)\Big\{\sum_{i=2}^{n} \binom{n}{i} (z-y)^{(i-2)}\, y^{(n-i)}\Big\} + ny^{(n-1)}. \tag{1}$$

Since y and z are relatively prime, the power y^{n-1} and $(z-y)$ are relatively prime. Hence, Formula (1) implies that

$$\Big(z-y\ ,\ \frac{z^n-y^n}{z-y}\Big) =\ n,\ \ \text{if } n \text{ divides } z-y,$$

and

$$\Big(z-y\ ,\ \frac{z^n-y^n}{z-y}\Big) =\ 1,\ \ \text{if } n \text{ is relatively prime to } z-y.$$

Moreover, (1) can be rewritten as

$$\frac{z^n - y^n}{z-y} = (z-y)^{n-1} + \Big\{\sum_{i=1}^{n-1} \binom{n}{i} (z-y)^{(i-1)}\, y^{(n-i)}\Big\}. \tag{2}$$

Since n is a prime integer, we have

$$\Big(n, \binom{n}{i}\Big) = n \quad \text{for} \quad i = 1, 2, \dots n-1. \tag{3}$$

From (2) and (3) , we get

$$\frac{z^n - y^n}{z-y} \equiv (z-y)^{n-1}\ \ (mod\, n). \tag{4}$$

It follows from (4) that if n is relatively prime to $z-y$, then n and $\dfrac{z^n-y^n}{z-y}$ are relatively prime. This is to prove the second assertion. The third assertion of the lemma follows directly from the second one if n does not divide $z-y$. Otherwise, suppose that n divides $z-y$. Then from (1) and (3), we can see easily that, in this case,

$$\frac{z^n-y^n}{z-y} \equiv ny^{(n-1)} \ \ (mod \ \ n^2). \tag{5}$$

If n^2 divides $\frac{z^n-y^n}{z-y}$, then (5) implies that n divides y, so that also, n divides z since it divides $z-y$. This is in contradiction with our assumptions that y and z are relatively prime. □

Remark 2.2. The first two assertions of Lemma 2.1 apply to the case where $n=2$, but the third one does not. For example, if we take $z=5, y=3$ and $n=2$, then 2^2 divides $\frac{5^2-3^2}{5-3}=8$.

Next we state and prove the main result.

Theorem 2.3. *Let y and z be two distinct nonnegative integers and let n be an odd prime integer. Let p be an odd prime integer that is different than n and relatively prime to y. Let r be a primitive root modulo p^2 and let m be a positive integer. Then p^m divides $\frac{z^n-y^n}{z-y}$ if and only if*

$$n \ \ divides \ \ p-1 \quad and \quad z \equiv y\, r^{cp^{m-1}} \ \ (mod \ \ p^m),$$

where c is any integer that satisfies:

1. $0<c<p-1$.
2. $p-1$ *divides* nc.

Proof. First recall that, by Lemma 1.1, r is also a primitive root modulo p^m for $m=1$ as well as for $m=3,4,\ldots$ Suppose that n divides $p-1$ and

$$z \equiv y\, r^{cp^{m-1}} \ \ (mod \ \ p^m), \tag{6}$$

for some integer c such that $0<c<p-1$ and $p-1$ divides nc. Formula (6) implies that $z^n \equiv y^n\, r^{ncp^{m-1}} \ \ (mod \ \ p^m)$. Since $p-1$ divides nc, it follows that $\phi(p^m)$, which is equal to $(p-1)p^{m-1}$, divides ncp^{m-1} and therefore

$$z^n \equiv y^n \ \ (mod \ \ p^m). \tag{7}$$

Also, Formula (6) implies that $z \equiv y\, r^{cp^{m-1}} \ \ (mod \ \ p)$, which is equivalent to $z \equiv y\, r^c\, r^{c(p^{m-1}-1)} \ \ (mod \ \ p)$. Since $\phi(p)$, which is equal to $p-1$, divides

$c(p^{m-1}-1)$, it follows that $z \ \equiv \ y\, r^c \quad (mod \ \ p)$. By Lemma 1.1, r is a primitive root modulo p and since $0 < c < p-1$, we have that $r^c \not\equiv 1 \quad (mod \ \ p)$. Hence

$$z \not\equiv y \quad (mod \ \ p). \tag{8}$$

It follows from (7) and (8) that $\dfrac{z^n - y^n}{z-y}$ is divisible by p^m.
Conversely, we have two different cases.

1. Case1: z and y are relatively prime.
   Suppose that p^m divides $\dfrac{z^n - y^n}{z-y}$. Then p^m divides $z^n - y^n$ or equivalently,

   $$z^n \ \equiv \ y^n \quad (mod \ \ p^m). \tag{9}$$

   Since p is different than n and divides $\dfrac{z^n - y^n}{z-y}$, Lemma 2.1 implies that p does not divides $z-y$. Hence, there exists an integer k such that

   $$0 < k < (p-1)p^{m-1} \tag{10}$$

   and

   $$z \ \equiv \ y\, r^k \quad (mod \ \ p^m). \tag{11}$$

   This implies

   $$z^n \ \equiv \ y^n r^{nk} \quad (mod \ \ p^m). \tag{12}$$

   From (9) and (12) we have $y^n(1-r^{nk}) \ \equiv \ 0 \ (mod \ \ p^m)$, which leads to $(1-r^{nk}) \equiv 0 \ (mod \ \ p^m)$ since y and p are relatively prime. Therefore,

   $$\phi(p^m), \ \ \text{which is equal to} \ \ (p-1)p^{m-1}, \ \ \text{divides} \ \ nk. \tag{13}$$

   Since $p \neq n$, the above expression implies that p^{m-1} divides k and because $0 < k < (p-1)p^{m-1}$, there exists an integer c such that $0 < c < p-1$ and

   $$k = cp^{m-1}. \tag{14}$$

   From (14) and (13), we have that $(p-1)p^{m-1}$ divides ncp^{m-1}. Thus,

   $$(p-1) \ \ \text{divides} \ \ nc. \tag{15}$$

   Since $0 < c < p-1$ and n is a prime integer, Formula (15) implies that

   $$n \ \ \text{divides} \ p-1, \tag{16}$$

   We complete the proof of this case by taking (14) into (11) to obtain

   $$z \ \equiv \ y\, r^{cp^{m-1}} \quad (mod \ \ p^m). \tag{17}$$

2. Case2: $(z, y) = q > 1$.
   Let y' and z' be such that $y = qy'$ and $z = qz'$. Then $(z', y') = 1$ and

$$\frac{z^n - y^n}{z - y} = q^{n-1} \ \frac{z'^n - y'^n}{z' - y'}. \tag{18}$$

   If p^m divides $\dfrac{z^n - y^n}{z - y}$ with p and y being relatively prime, then p^m divides $\dfrac{z'^n - y'^n}{z' - y'}$. It follows, by Case1, that n divides $p-1$ and $z' \equiv y' r^{cp^{m-1}} \pmod{p^m}$, so that $z \equiv y r^{cp^{m-1}} \pmod{p^m}$, where c is an integer such that $0 < c < p-1$ and $p-1$ divides nc.

□

Remark 2.4. The integer c is even and different than $\dfrac{p-1}{2}$. If c_1 satisfies $n\, c_1 = p-1$, then the integer c takes all the values $c_1, c_2 = 2\, c_1, c_3 = 3\, c_1, \ldots, c_{n-1} = (n-1)c_1$. That makes a total of $(n-1)$ values. Notice also that if $z = y r^{c_i P^{m-1}}$ for some index $i \in \{1, 2, \ldots, n-1\}$, then, by analogy between z and y, we have $y = z r^{c_j P^{m-1}}$ for some integer $j \in \{1, 2, \ldots, n-1\}$ such that $c_i + c_j = p - 1$. Moreover, $c_i \neq c_j$ for if they were equal, then we would have $c = \dfrac{p-1}{2}$, which is impossible as is already mentioned.

Remark 2.5. Note that, in the statement of Theorem 2.3, the condition $p \neq n$ needs to be stated for the case $m = 1$ only. If $m \geq 2$ and p^m divides $\dfrac{z^n - y^n}{z - y}$, then the third assertion of Lemma 2.1 ensures that $p \neq n$.

Remark 2.6. Observe that n divides $\dfrac{p-1}{2}$ in Theorem 2.3. Therefore, if $p < 2n + 1$, then p^m does not divide $\dfrac{z^n - y^n}{z - y}$.

Remark 2.7. If an odd prime q divides $\dfrac{z^n - y^n}{z - y}$ but n does not divide $q - 1$, then by Theorem 2.3 and Lemma 2.1, t is equal to n and divides $z - y$.

Example 2.8. Goormaghtigh conjecture states that the Diophantine equation

$$\frac{x^{n_1} - 1}{x - 1} = \frac{y^{n_2} - 1}{y - 1}, \quad x > y > 1 \ \text{ and } \ n, m > 2,$$

is satisfied for only two trivial cases:

$$\frac{5^3 - 1}{5 - 1} = \frac{2^5 - 1}{2 - 1} = 31$$

and

$$\frac{90^3 - 1}{90 - 1} = \frac{2^{13} - 1}{2 - 1} = 8191.$$

The condition imposed by Theorem 2.3 that n divides $p - 1$ is satisfied in both cases. In the first case, we have $n_1 = 3$ divides $p - 1 = 30 = (2)(3)(5)$. In the second case, $p = 8191$ is a prime number and each of $n_1 = 3$ and $n_2 = 13$ divides $p - 1 = 8190 = (3^2)(7)(13)$.

Example 2.9. A Mersenne number is an integer of the form $2^n - 1$.Therefore, it is of the form $\frac{z^n - y^n}{z - y}$. It is well-known that if a prime p divides $2^n - 1$, where n is an odd prime, then n divides $p - 1$. This fact is in accordance with Theorem 2.3. It means that for every odd prime integer n, there is another prime integer p strictly larger than n. As it is known, This idea implies the infinitude of prime integers.

Two particular cases of Theorem 2.3 are $m = 1$ and $m = n$. we state the second one as a corollary because of its connection with Fermat's last theorem.

Corollary 2.10. Let y and z be two distinct nonnegative integers. Let p be an odd prime integer relatively prime to y and let r be a primitive root modulo p^2. and let n be an odd prime integer. Then p^n divides $\frac{z^n - y^n}{z - y}$ if and only if

$$n \text{ divides } p - 1 \quad \text{and} \quad z \equiv y\, r^{cp^{n-1}} \quad (mod\ p^n),$$

where c is any integer that satisfies:

1. $0 < c < p - 1$.
2. $p - 1$ divides nc.

Corollary 2.11. Let y and z be two distinct nonnegative integers and let n be an odd prime integer. Let p be an odd prime integer different than n, relatively prime to y and having the form $p = 2^k + 1$ for some positive integer k. Then p does not divide $\frac{z^n - y^n}{z - y}$.

Proof. Follows, immediately, from Theorem 2.3 since there is no odd prime integer n that divides $p - 1 = 2^k$. □

As a completion of Theorem 2.3, we show that integers of the form $\frac{z^n - y^n}{z - y}$ are not divisible by 2, given that z and y are not both even and n is an odd prime integer.

Theorem 2.12. *Let y and z be two distinct nonnegative integers not both even and let n be an odd prime integer. Then 2 does not divide $\dfrac{z^n - y^n}{z - y}$.*

Proof. It suffices to show that $\dfrac{z^n - y^n}{z - y}$ is an odd integer. If one of y and z is odd and the other is even, then both $(z^n - y^n)$ and $(z - y)$ are odd integers. Hence, their quotient $\dfrac{z^n - y^n}{z - y}$ is also odd. If each of y and z is odd, then $(z - y)$ is even. Hence, $\dfrac{z^n - y^n}{z - y}$ has to be an odd integer since, by Lemma 2.1, $\Big(\dfrac{z^n - y^n}{z - y}, z - y\Big) = 1$ or n. □

3 Some applications of Theorem 2.3

3.1 Construction of integers having the form $\dfrac{z^n - y^n}{z - y}$ and divisible by p^m

Theorem 2.3, beside being a characteristic theorem, it is also a constructive theorem. In other words, if $y, p, n, m,$ are as in theorem 2.3, $c_1 = \dfrac{p-1}{n}$ and r, is a primitive root modulo p^2, then we can construct the set $\xi(y, p, n, m, c_1)$ of all integers of the form $\dfrac{z^n - y^n}{z - y}$ that are divisible by p^m,

$$\xi(y, p, n, m, c_1) = \Big\{\frac{z^n - y^n}{z - y} \;\Big|\; z \equiv r^{c_1\, p^{m-1}} \;(mod\;\, p^m)\Big\}. \tag{19}$$

As we have explained in Remark 2.4, the integer c_1 can be replaced by $c_i = i\, c_1$ for $i = 1, 2, \ldots, n-1$, so that we can construct sets of the form:

$$\xi(y, p, n, m, c_i) = \Big\{\frac{z^n - y^n}{z - y} \;\Big|\; z \equiv r^{i\, c\, p^{m-1}} \;(mod\;\, p^m)\Big\}, \quad i = 1, 2, \ldots, n-1. \tag{20}$$

The union, over i, of the above sets is

$$\xi(y, p, n, m) = \bigcup_{i=1}^{n-1} \xi(y, p, n, m, c_i). \tag{21}$$

Let $\xi(p, n, m)$ be the set of all integers of the form $\dfrac{z^n - y^n}{z - y}$ that are divisible by p^m, y relatively prime to p, Then $\xi(p, n, m)$ is obtained by taking the union of the sets of the form $\xi(y, p, n, m)$ over all possible values of y.

$$\xi(p, n, m) = \bigcup_{\substack{y \in \mathbb{N} \\ p \nmid y}} \xi(y, p, n, m) = \bigcup_{\substack{y \in \mathbb{N} \\ p \nmid y}} \bigcup_{i=1}^{n-1} \xi(y, p, n, m, c_i). \tag{22}$$

Remark 3.1. Unless $p = 3$, there are many primitive roots that are incongruent modulo p^2. However, we do not consider r to be a parameter in the construction of $\xi(p, n, m)$ since this set remains invariant if we replace r by another primitive root modulo p^2. This can be easily verified.

Suppose that $\dfrac{z^n - y^n}{z - y} \in \xi(y, p, n, m, c = c_2)$. Then

$$z \equiv y\, r^{c_2\, p^{m-1}} \quad (mod\ \ p^m).$$

Since $c_2 = 2\, c_1$, the above congruence equation can be rewritten as

$$z \equiv \left(y\, r^{c_1\, p^{m-1}}\right) r^{c_1\, p^{m-1}} \quad (mod\ \ p^m).$$

Letting $y' = y\, r^{c_1\, p^{m-1}}$, we obtain

$$z \equiv y'\, r^{c_1\, p^{m-1}} \quad (mod\ \ p^m),$$

so that $\dfrac{z^n - y'^n}{z - y'} \in \xi(y', p, n, m, c_1)$. The above reasoning shows that

$$\bigcup_{\substack{y \in \mathbb{N} \\ p \nmid y}} \bigcup_{i=1}^{n-1} \xi(y, p, n, m, c_i) = \bigcup_{\substack{y \in \mathbb{N} \\ p \nmid y}} \xi(y, p, n, m, c_1). \tag{23}$$

Therefore, we have the following corollary.

Corollary 3.2. Let p be an odd prime integer for which there exists an other odd prime integer n such that $p - 1 = n\, c$ for some positive integer c. Let r be a primitive root modulo p^2. Then

$$\xi(p, n, m) = \bigcup_{\substack{y \in \mathbb{N} \\ p \nmid y}} \left\{ \frac{z^n - y^n}{z - y} \;\middle|\; z \equiv r^{c\, p^{m-1}} \quad (mod\ \ p^m) \right\} \tag{24}$$

is the set of all integers of the form $\dfrac{z^n - y^n}{z - y}$ that are divisible by p^m, where p does not divide y and m is a positive integer.

Remark 3.3. Notice that no matter how the integer m is large, we can construct infinitely many integers of the form $\dfrac{z^n - y^n}{z - y}$ divisible by p^m. Notice also that

$$\xi(p,n,m) \subseteq \xi(p,n,m'), \quad \text{for } 1 \le m' < m.$$

Example 3.4. Let's construct an integer of the form $\dfrac{z^3 - y^3}{z - y}$ that is divisible by 7^3. Take $p = 7, r = 3, n = 3, c = 2$ and $y = 1$. We have that $n = 3$ divides $p - 1 = 6$ and $nc = 6 = p - 1$. Construct the integer $z = r^{cp^{n-1}} = 3^{98}$. Then, by Theorem 2.3,

$$7^3 = 343 \text{ divides } \frac{(3^{98})^3 - 1}{3^{98} - 1}.$$

Of course, this is a huge number. But Theorem 2.3 ensures that we can use positive numbers that are less than and equivalent to z modulo p^n. By the use of a calculator, we find easily that $3^{98} \equiv 324 \pmod{7^3}$. Indeed,

$$\frac{324^3 - 1}{324 - 1} = 105301 = (307)(7^3).$$

Now, let's ask a question:
Is it true that, for an odd prime integer n, there are infinitely many odd prime integers p such that n divides $p - 1$?
Consider the set

$$\xi(y = 1, p, n, m = 1) = \Big\{ \frac{z^n - 1}{z - 1} \mid z \equiv r^c \pmod{p} \Big\}.$$

and let E be the set of all odd prime integers p such that p divides some element from $\xi(y = 1, p, n, m = 1)$. Since, by Theorem 2.3, n divides $p - 1$ for every element $p \in E$, an affirmative answer of the above question can be obtained if we prove that there are infinitely many element in E. This seems to be true because every two element of $\xi(y = 1, p, n, m = 1)$ have, more likely, different prime decomposition.

3.2 Proving a general fact about the congruence modulo p^m

Beside its constructive aspect, Theorem 2.3 has other applications such as the following.

Corollary 3.5. Let p be an odd prime integer for which there exist another prime integer n such that n divides $p - 1$. Let r be a primitive root modulo p^2. Let c be an integer such that $0 < c < p-1$ and $p-1$ divides nc. Then, for every positive integer m, we have

$$\sum_{k=0}^{n-1} r^{kcp^{m-1}} \equiv 0 \pmod{p^m}. \tag{25}$$

In particular, for $m = 1$, we have

$$\sum_{k=0}^{n-1} r^{kc} \equiv 0 \pmod{p}. \tag{26}$$

Proof. We choose an integer y relatively prime to p, and we construct the integer

$$z = yr^{cp^{m-1}}. \tag{27}$$

By Theorem 2.3, we have $\dfrac{z^n - y^n}{z-y} \equiv 0 \pmod{p^m}$, which is equivalent to

$$\sum_{k=0}^{n-1} z^k \, y^{n-k-1} \equiv 0 \pmod{p^m}. \tag{28}$$

Taking (27) into (28), we obtain

$$y^{n-1} \sum_{k=0}^{n-1} r^{kcp^{m-1}} \equiv 0 \pmod{p^m}. \tag{29}$$

Since y and p are relatively prime, it follows from (29) that

$$\sum_{k=0}^{n-1} r^{kcp^{m-1}} \equiv 0 \pmod{p^m}. \tag{30}$$

□

Remark 3.6. It is well-known that if r is primitive root mod p, then

$$\sum_{k=0}^{p-1} r^k \equiv 0 \pmod{p}. \tag{31}$$

To see this, recall that $r^1, r^2, \ldots, ..., r^{n-1}$ form a complete residue set modulo p. A question that arises is: do we have similar formula for an integer t that is not a primitive root modulo p? The above corollary gives a partial answer to this question by the mean of Formula (26) which can be considered as an extension of Formula

(31). In fact, if $t = r^c$, then t is not a primitive root modulo p since $0 < c < p-1$ and $\big(c, p-1\big) \neq 1$. Then Formula (26) becomes

$$\sum_{k=0}^{n-1} t^k \equiv 0 \quad (mod\ \ p). \tag{32}$$

Note that $n < \dfrac{p}{2}$. That is, the number of summands in (32) is less than half of that in (31).

Example 3.7. As in Example 3.4, we take $p = 7, r = 3, n = 3$ and $c = 2$. If we let $m = n = 3$, then we have

$$\begin{array}{rcl} \sum_{k=0}^{n-1} r^{kcp^{n-1}} & = & \sum_{k=0}^{2} 3^{98k} \\ & = & 1 + 3^{98} + 3^{196} \\ & \equiv & 1 + 324 + 324^2 \quad (mod\ \ 7^3) \\ & \equiv & 1 + 324 + (-19)^2 \quad (mod\ \ 343) \\ & \equiv & 1 + 324 + 361 \quad (mod\ \ 343) \\ & \equiv & 0 \quad (mod\ \ 7^3) \end{array}$$

By the same reasoning, if $m = 1$, then

$$\sum_{k=0}^{2} 3^{kc} = 3^0 + 3^2 + 3^4 = 91 \equiv 0 \quad mod\ \ 7.$$

An other primitive root of 7 is the integer 5. For $m = 1$, we have

$$\sum_{k=0}^{2} 5^{kc} = 5^0 + 5^2 + 5^4 = 651 \equiv 0 \quad mod\ \ 7.$$

3.3 Case where the mth power of a composite integer divides $\dfrac{z^n - y^n}{z - y}$

Let $p_1, p_2, \ldots, p_k$ be k distinct prime integers each of which is different than n and relatively prime to y. Suppose that the product $\displaystyle\prod_{i=1}^{k} p_i^{m_i}$ divides $\dfrac{z^n - y^n}{z - y}$, where $m_1, m_2, \ldots, m_k$ are k positive integers. According to Theorem 2.3, this hold if and only if n divides $p_i - 1$ for $i = 1, 2, \ldots, k$ and

$$\begin{aligned}
&z \equiv y\, r_1^{c_1 p_1^{m_1 - 1}} \quad (mod\ \ p_1^{m_1})\\
&z \equiv y\, r_2^{c_2 p_2^{m_2 - 1}} \quad (mod\ \ p_2^{m_2})\\
&\ldots\\
&z \equiv y\, r_k^{c_k p_k^{m_k - 1}} \quad (mod\ \ p_k^{m_k}),
\end{aligned}$$

where, for $i = 1, 2, \ldots, k$, r_i is a primitive root modulo p_i, the integer c_i satisfies $0 < c_i < p_i - 1$ and $p_i - 1$ divides nc_i. By the Chinese remainder theorem, the above system of congruence equations holds if and only if

$$\begin{aligned}
z \quad &\equiv \quad \sum_{i=1}^{k} \left(y\, r_i^{c_i p_i^{m_i - 1}}\right) \left(M_i\, q_i\right) \quad (mod\ \ p_1^{m_1}\, p_2^{m_2} \ldots p_k^{m_k})\\
&\equiv \quad y \sum_{i=1}^{k} M_i\, q_i\, r_i^{c_i p_i^{m_i - 1}} \quad (mod\ \ p_1^{m_1}\, p_2^{m_2} \ldots p_k^{m_k}), \qquad (33)
\end{aligned}$$

where $M_i = \dfrac{\prod_{j=1}^{k} p_j^{m_j}}{p_i^{m_i}}$ and q_i is any integer that satisfies $M_i q_i \equiv 1 \quad (mod\ \ p_i^{m_i})$. The following corollary summarize the above result.

Corollary 3.8. Let y and z be two relatively prime integers and let n be an odd prime integer. Let $p_1, p_2, \ldots, p_k$ be k distinct odd prime integers, each of which is different than n. and let $r_1, r_2, \ldots, r_k$ be, respectively, primitive root modulo $p_1^2, p_2^2, \ldots, p_k^2$. Let $m_1, m_2, \ldots, m_k$ be k positive integers. Then the product $\prod_{i=1}^{k} p_i^{m_i}$ divides $\dfrac{z^n - y^n}{z - y}$ if and only if

$$n \quad \text{divides} \quad p_i - 1, \quad \text{for} \quad i = 1, 2, \ldots, k, \qquad (34)$$

and

$$z \equiv y \sum_{i=1}^{k} M_i\, q_i\, r_i^{c_i p_i^{m_i - 1}} \quad (mod\ \ p_1^{m_1}\, p_2^{m_2} \ldots p_k^{m_k}), \qquad (35)$$

where

1. $M_i = \dfrac{\prod_{j=1}^{k} p_j^{m_j}}{p_i^{m_i}}$,

2. q_i is any integer that satisfies $M_i q_i \equiv 1 \quad (mod\ \ p_i^{m_i})$,

3. c_i is an integer such that $0 < c_i < p_i - 1$ and $p_i - 1$ divides nc_i.

4 Connection with Fermat's last theorem

Fermat's last theorem [8] states:

Theorem 4.1. *For every positive integer n with $n \geq 3$, no positive integers x, y and z satisfy*

$$z^n = x^n + y^n.$$

This theorem, which has been proved around 1995 [8], implies the following fact.

Corollary 4.2. Let z and y be two relatively prime integers, and let n be an odd prime integer. Then $z - y$ is a perfect nth power if and only if $\dfrac{z^n - y^n}{z - y}$ is not a perfect nth power. In particular, if $z - y = 1$, then $\dfrac{z^n - y^n}{z - y}$ is not an nth perfect power.

We have proved in this work, that $\dfrac{z^n - y^n}{z - y}$ can be multiple of some perfect nth power p^n. But we don't know if $\dfrac{z^n - y^n}{z - y}$, itself, can be a perfect nth power having the form $(p_1 p_2 \dots)^n$ for not necessary distinct prime integers $p_1, p_2, \dots$ By going back to Formula (24) and looking at how large is the set $\xi(p, n, m)$ and the degree of freedom that we have to construct such set by acting on different parameters p and n, one may believe that there is chance for some elements of $\xi(p, n, m)$ to be perfect nth powers. For instance, consider the number $a = \dfrac{16^3 - 5^3}{16 - 5}$ which is equal to 19^2. Of course, the integer a is not a perfect nth power since $n = 3$. But it is well a perfect power. Moreover, it is a perfect power of a prime integer. Since such number a exists and it is remarkably small, we believe that nothing impede the existence of a perfect nth power of the form $\dfrac{z^n - y^n}{z - y}$. However, it may turn out that the smallest of these numbers is tremendously large and therefore difficult to reach with a computer. Perhaps, a constructive proof, is the best way to find such integers if they exist.

For mathematicians seeking a proof of Fermat's last theorem by the mean of classical methods, we have a little result that may be of some use and which is consequence of Theorem 2.3.

Theorem 4.3. *Suppose that there are pairwise relatively prime positive integers x, y, z such that $z^n = x^n + y^n$, where n is an odd prime integer. If p is an odd prime integer such that $p \neq n$ and p divides $\dfrac{x^n y^n z^n}{(z-x)(z-y)(x+y)}$, then n divides $p-1$.*

Proof. p divides one of $\dfrac{x^n}{z-x}$, $\dfrac{y^n}{z-y}$ and $\dfrac{z^n}{x+y}$. Then, by Theorem 2.3, n divides $p-1$. □

5 Conclusion

We believe that a lot can be done about the integers of the form $\dfrac{z^n - y^n}{z-y}$. A better understanding of this type of integers may lead to a more accessible proof of Fermat's last theorem as well as to the solutions of other Diophantine equations. For instance, an observations made on some few integers of the form $\dfrac{z^n - y^n}{z-y}$ gives us the impression that there may be always some prime integer p divisor of $\dfrac{z^n - y^n}{z-y}$ that is greater than each of $|z|$ and $|y|$. We strongly believe that this observation holds for all integers of the form $\dfrac{z^n - y^n}{z-y}$. Therefore we state it as a conjecture.

Conjecture 5.1. *Let z and y be two relatively prime positive integers with $z > y$ and let n be an odd prime integer. There is a prime integer p divisor of $\dfrac{z^n - y^n}{z-y}$ such that $p > z$.*

If it happens that this conjecture is true, then Fermat's last theorem will be an immediate consequence of it.

y	z	$\frac{z^3-y^3}{z-y}$	prime decomp	$p,\ p>z$		y	z	$\frac{z^5-y^5}{z-y}$	prime decomp	$p,\ p>z$
5	6	91	$7*13$	13		7	8	15961	$11*1451$	1451
5	7	109	prime	109		7	9	21121	prime	21121
5	8	129	$3*43$	43		7	10	27731	$11*2521$	2521
5	9	151	prime	151		7	11	36061	prime	36061
5	11	201	$3*67$	67		7	12	46405	$5*9281$	9281
5	12	229	prime	229		7	13	59081	$11*41*131$	$131, 41$
5	13	259	$7*37$	37		7	15	92821	prime	92821
5	14	291	$3*97$	97		7	16	114641	prime	114641
5	16	361	$19*19$	19		7	17	140305	$5*11*2551$	2551
5	17	399	$3*7*19$	19		7	18	170251	$61*2791$	2791
5	18	439	prime	439		7	19	204941	$11*31*601$	$601, 31$
5	19	481	$13*37$	37		7	20	244861	prime	244861
5	21	571	prime	571		7	22	342455	$5*68491$	68491
5	22	619	prime	619		7	23	401221	$71*5651$	$71, 5651$
5	23	669	$3*223$	223		7	24	467401	$11x42491$	42491
5	24	721	$7*103$	103		7	25	541601	$31x17471$	$31, 17471$
5	26	831	$3*277$	277		7	26	624451	prime	624451
5	27	889	$7*127$	127		7	27	716605	$5*251*571$	$251, 571$
5	28	949	$13*73$	73		7	29	931561	$41*22721$	$41, 22721$
5	29	1011	$3*337$	337		7	30	1055791	$11*41*2341$	$41, 2341$
5	31	1141	$7*163$	163		7	31	1192181	prime	1192181

Table1: The prime decomposition of some small numbers of the forms $\frac{z^n-y^n}{z-y}$.
Each one of them has a prime divisor that is larger than z.

Acknowledgements

The author would like to thank Abdullah Laaradji from King Fahd University of Minerals and Petroleum for his very useful comments and suggestions.

References

[1] David M. Burton, Elementary Number Theory, Allyn and Bacon, Inc., Boston, 1980.

[2] C. F. Gauss, Disquisitiones Arithmeticae, English translation, Yale University Press, New Haven, 1986.

[3] R. Kumanduri and C. Romero, Number Theory With Computer Applications, Prentice Hall, New Jersey, 1998.

[4] K. H. Rosen, Elementary number theory and its applications, Addison-Wesley, Massachusetts, 1984.

[5] I. Niven, H. S. Zuckerman, and H. L. Montgomery, An Introduction to the Theory of Numbers, 5th Ed., John Wiley and Sons, New York, 1991.

[6] O. Ore, Number Theory and Its History, Dover Publications, Inc.,New York, 1988.

[7] P. Ribenboim, Fermat's Last Theorem for Amateurs, Springer-Verlag, New York, 1999.

[8] R. Taylor and A. Wiles, Ring-theoretic properties of certain Hecke algebras, Annals of Math., 141(1995), 553-572.

[9] Underwood Dudley, Elementary Number Theory, W. H. Freeman and Company, San Fransisco, 1969.