Characterization of the integers of the form $\frac{z^n - y^n}{z - y}$ that are divisible by some perfect nth powers.

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

January 1, 2019

Abstract

In this work, we show a sufficient and necessary condition for an integer of the form $\frac{z^n - y^n}{z - y}$ to be divisible by some perfect nth power p^n, where p is an odd prime. We also show how to construct such integers. A link between the main result and Fermat's last theorem is discussed. Other related ideas, examples and applications are provided.

AMS Subj. Class.:11A07 ; 11D41

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

1 Introduction

The motivation behind the current work is Fermat last theorem itself. The author tried to come up with a complete proof of this theorem in the following way. Given that y and z are relatively prime integers and n is an odd prime such that $z - y$ and n are relatively prime, The ideas was that the famous theorem can be easily proved if we arrive to show that an integer of the form $\frac{z^n - y^n}{z - y}$, cannot be, in any case, divisible by an nth power p^n of a prime integer p. In contrast to what we had expected, we found that almost for every odd prime integer p, there is a freedom to

construct infinitely many pairwise relatively prime integers of the form $\frac{z^n - y^n}{z - y}$, each of which is divisible by p^n. The main tool of our analysis in this work, is the concept of primitive root modulo integer. Given a positive integer m, we say that r is a primitive root modulo m if r is an integer relatively prime to m and the smallest integer a such that $r^a \equiv 1 \pmod{m}$ is $\phi(m)$, where ϕ is the Euler totient function. Only elementary ideas about this concept are used in our analysis. For the readers who may need a review of some elementary facts about primitive roots modulo integers, we refer to some textbooks such as [1], [3], [4], [5], [6] and [9]. Throughout the paper, we use the following notation.

1. The Euler totient function is denoted by ϕ. For every positive integer n, $\phi(n)$ is the number of positive integers strictly less than n and relatively prime to it.

2. The greatest common divisor of two integers a and b is denoted $\gcd(a, b)$.

2 Main result

We start this section by stating, as a lemma, an idea about primitive roots modulo integers.

Lemma 2.1. *Let p be and odd prime and let n be a positive integer with $n \geq 2$. If the integer r is a primitive root modulo p^n, then r is also a primitive root modulo $p^{n-1}, p^{n-2}, \ldots, p$.*

Proof. First, recall that for every perfect nth power p^n, $n = 1, 2, \ldots$, of some odd prime integer p, there is a primitive root modulo p^n [4, Theorem 8.14]. Let t be an integer relatively prime to p. Hence t is relatively prime to p^n for $n = 2, 3, \ldots$ Suppose that t is not a primitive root modulo p^n. Then there exists a positive integer k strictly less than $\phi(p^n) = (p-1)p^{n-1}$ such that $t^k \equiv 1 \pmod{p^n}$. Let's show that t is not a primitive root modulo p^{n+1}. If $t^k \equiv 1 \pmod{p^{n+1}}$, then, obviously, t is not a primitive root modulo p^{n+1}. Suppose that $t^k \not\equiv 1 \pmod{p^{n+1}}$. Then

$$\begin{aligned} t^{kp} - 1 &= (t^k - 1)\sum_{j=0}^{p-1} t^{jk} \\ &= (t^k - 1)\sum_{j=0}^{p-1} (t^{jk} - 1 + 1) \qquad (1) \\ &= (t^k - 1)\Big(\sum_{j=1}^{p-1} (t^{jk} - 1) \; + \; p\Big). \end{aligned}$$

By our assumption, p^n divides $t^k - 1$. Hence, p^n divides $t^{jk} - 1$ for $j = 1, 2, \ldots,$ and p divides $\sum_{k=1}^{p-1}(t^{jk} - 1) + p$. Combining these two facts with the last line of (1), we have that $t^{kp} \equiv 1 \pmod{p^{n+1}}$. Since $kp < (p-1)p^n = \phi(p^{n+1})$, the integer t cannot be a primitive root modulo p^{n+1}. This is equivalent to saying that if t is a primitive root modulo p^{n+1}, then t is a primitive root modulo p^n. Using induction, we conclude that t is also a primitive root modulo p^j for $j = n-1, n-2, \ldots 1$. □

Corollary 2.2. Let r be a positive integer and let p be an odd prime integer. Then r is a primitive root modulo p^2 if and only if r is a primitive root modulo p^n for $n = 1, 2, \ldots$.

Proof. It is known that if r is a primitive root modulo p^2, then r is also a primitive root modulo p^n for $n = 1, 2, \ldots$ For more information, you can look, for example, at [4, Theorem 8.9]. The converse is implied by Lemma 2.1. □

Using group theory language, we state Corollary 2.2 as follows.

Corollary 2.3. An element r is a generator of the multiplicative group of integers modulo p^2 if and only if it is a generator of the multiplicative group of integers modulo p^n for $n = 3, 4, \ldots$

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

Lemma 2.4. *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 $gcd\Big(z - y\,,\ \dfrac{z^n - y^n}{z - y}\Big) = n$.

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

3. n^2 does not divides $\dfrac{z^n - y^n}{z - y}$.

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

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

Since y and z are relatively prime, then y^{n-1} and $(z-y)$ are relatively prime. Hence, Formula (2) implies that

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

and

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

Moreover, (2) can be rewritten as

$$\frac{z^n - y^n}{z-y} = (z-y)^{n-1} + \Big\{\sum_{i=1}^{n-1}\binom{n}{i}(z-y)^{(i-1)}\,y^{(n-i)}\Big\}. \tag{3}$$

Since n is a prime integer, we have

$$\text{gcd}\Big(n, \binom{n}{i}\Big) = n \quad \text{for} \quad i = 1, 2, \ldots n-1. \tag{4}$$

From (3) and (4) , we get

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

It follows from (5) 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 (2) and (4), we can see easily that, in this case,

$$\frac{z^n - y^n}{z - y} \equiv n y^{(n-1)} \pmod{n^2}. \tag{6}$$

If n^2 divides $\dfrac{z^n - y^n}{z - y}$, then (6) 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 2.5. The first two assertions of Lemma 2.4 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 $\dfrac{5^2 - 3^2}{5 - 3} = 8$.

Next, we state and prove the main theorem.

Theorem 2.6. *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. Let n be an odd prime integer. Then p^n divides $\dfrac{z^n - y^n}{z - y}$ if and only if*

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

where c is any integer that satisfies:

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

Proof. Recall that since r is a primitive root modulo p^2, then r is also a primitive root modulo p^n for $n = 3, 4, \ldots$ Suppose that n divides $p - 1$ and

$$z \equiv y\, r^{cp^{n-1}} \pmod{p^n}, \tag{7}$$

for some integer c such that $0 < c < p - 1$ and $p - 1$ divides nc. Formula (7) implies that $z^n \equiv y^n\, r^{ncp^{n-1}} \pmod{p^n}$. Since $p - 1$ divides nc, it follows that $\phi(p^n) = (p - 1)p^{n-1}$ divides ncp^{n-1} and therefore

$$z^n \equiv y^n \pmod{p^n}. \tag{8}$$

Also, Formula (7) implies that $z \equiv y\, r^{cp^{n-1}} \pmod{p}$, which is equivalent to $z \equiv y\, r^c\, r^{c(p^{n-1}-1)} \pmod{p}$. Since $\phi(p) = p - 1$ divides $c(p^{n-1} - 1)$, it

follows that $z \equiv y\, r^c \pmod{p}$. By Lemma 2.1, r is a primitive root modulo p and since $0 < c < p-1$, we have that $r^c \not\equiv 1 \pmod{p}$. Hence

$$z \not\equiv y \pmod{p}. \tag{9}$$

It follows from (8) and (9) that $\dfrac{z^n - y^n}{z-y}$ is divisible by p^n.
Conversely, we treat two different cases.

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

   $$z^n \equiv y^n \pmod{p^n}. \tag{10}$$

   Since z and y are relatively prime and r is a primitive root modulo p^n, there exists an integer k such that $0 < k < (p-1)p^{n-1}$ and

   $$z \equiv y\, r^k \pmod{p^n}. \tag{11}$$

   This implies

   $$z^n \equiv y^n r^{nk} \pmod{p^n}. \tag{12}$$

   From (10) and (12) we have $y^n(1 - r^{nk}) \equiv 0 \pmod{p^n}$, which leads to $(1 - r^{nk}) \equiv 0 \pmod{p^n}$ since y and p are relatively prime. Therefore,

   $$\phi(p^n) = (p-1)p^{n-1} \text{ divides } nk. \tag{13}$$

   By the third assertion of Lemma 2.4, n^2 does not divide $\dfrac{z^n - y^n}{z-y}$; and since p^n divides $\dfrac{z^n - y^n}{z-y}$, it follows that

   $$p \neq n. \tag{14}$$

   We obtain from (13) and (14) that p^{n-1} divides k and since $0 < k < (p-1)p^{n-1}$, there exists an integer c such that $0 < c < p-1$ and

   $$k = cp^{n-1}. \tag{15}$$

   From (15) and (13), we have that $(p-1)p^{n-1}$ divides ncp^{n-1}. Thus,

   $$(p-1) \text{ divides } nc. \tag{16}$$

   Since $0 < c < p-1$ and n is a prime integer, Expression (16) implies that

   $$n \text{ divides } p-1, \tag{17}$$

   We complete the proof of Case1 by taking (15) into (11) to obtain

   $$z \equiv y\, r^{cp^{n-1}} \pmod{p^n}. \tag{18}$$

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

$$\frac{z^n - y^n}{z - y} = q^{n-1} \ \frac{z'^n - y'^n}{z' - y'}. \tag{19}$$

   Therefore, if p^n divides $\dfrac{z^n - y^n}{z - y}$ with p and y are relatively prime, then we have, by Case1, that n divides $p - 1$ and $z' \equiv y' r^{cp^{n-1}} \pmod{p^n}$, so that $z \equiv y r^{cp^{n-1}} \pmod{p^n}$, where c is an integer such that $0 < c < p - 1$ and $p - 1$ divides nc.

□

Corollary 2.7. Let y and z be two distinct nonnegative integers. Let p be an odd prime integer relatively prime to y and let n be an odd prime integer. If $p < 2n + 1$ then p^n does not divide $\dfrac{z^n - y^n}{z - y}$.

Proof. Follows from Theorem 2.6, which requires that n has to be an odd prime integer dividing the even integer $p - 1$, so that $p - 1 \geq 2n$. □

Corollary 2.8. Let y and z be two distinct nonnegative integers. Let p be an odd prime integer relatively prime to y and having the form $p = 2^k + 1$ for some positive integer k. Let n be an odd prime integer. Then p^n does not divide $\dfrac{z^n - y^n}{z - y}$.

Proof. Follows, immediately, from Theorem 2.6 since there is no odd prime integer n that divides $p - 1 = 2^k$. □

Follows an idea that can be seen from the proof of Theorem 2.6 and may be of some independent interest.

Corollary 2.9. The system of congruence equations

$$\begin{aligned}
z &\equiv y\, r^{c} && \pmod{p} \\
z &\equiv y\, r^{cp} && \pmod{p^2} \\
z &\equiv y\, r^{cp^2} && \pmod{p^3} \\
&\vdots \\
z &\equiv y\, r^{cp^{n-1}} && \pmod{p^n}.
\end{aligned}$$

is dependent, has rank 1 and it is equivalent to the last equation in it,

$$z \equiv y\, r^{cp^{n-1}} \pmod{p^n}. \tag{20}$$

Proof. Clearly, the congruence equation (20) implies

$$z \equiv y\, r^{cp^{n-1}} \pmod{p^t}, \text{ for } t = 1, 2, \ldots, n-1. \tag{21}$$

Observe that

$$\begin{array}{rcl} p^{n-1} & = & p^{n-1} - p^{t-1} + p^{t-1} \\ & = & p^{t-1}(p^{n-t} - 1) + p^{t-1} \\ & = & (p-1)p^{t-1}(\sum_{j=0}^{j=n-t-1} p^j) + p^{t-1} \\ & = & \phi(p^t)\,(\sum_{j=0}^{j=n-t-1} p^j) + p^{t-1}. \end{array} \tag{22}$$

By (21) and (22), we have $z \equiv y\, r^{cp^{t-1}} \pmod{p^t}$ for $t = 1, 2, \ldots, n-1$. □

As a completion of Theorem 2.6, we show that integers of the form $\dfrac{z^n - y^n}{z - y}$ are not divisible by 2^n, given that z and y are not both even and n is an odd prime integer.

Remark 2.10. If y and z are two distinct nonnegative integers not both even and n is an odd prime integer, then 2^n does not divide $\dfrac{z^n - y^n}{z - y}$. To understand this, It suffices to show that $\dfrac{z^n - y^n}{z - y}$ is an odd integer. In fact, 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, so that 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 2.4, $\gcd\Big(\dfrac{z^n - y^n}{z - y}, z - y\Big) = 1$ or n.

3 Some applications of Theorem 2.6

3.1 Constructions of an integer $\dfrac{z^n - y^n}{z - y}$ divisible by p^n

Theorem 2.6, beside being a characteristic theorem, it is also a constructive theorem. In other word, for a given odd prime integer p with $p \geq 7$, Theorem 2.6 allows to construct the set ξ_p of all integers of the form $\dfrac{z^n - y^n}{z - y}$ that are divisible by p^n,

$$\begin{array}{rcl} \xi_p & = & \Big\{\dfrac{z^n - y^n}{z - y} \;\Big|\; \gcd(y, p) = 1\ ,\ n \text{ divides } p-1\ , \\ & & \qquad z \equiv y\, r^{cp^{n-1}} \pmod{p^n} \text{ and } p-1 \text{ divides } nc\Big\}. \end{array} \tag{23}$$

If y is also fixed to be any integer relatively prime to p, then we can construct the set

$$\xi_{p,y} = \Big\{ \frac{z^n - y^n}{z-y} \;\Big|\; n \text{ divides } p-1\,,\; z \equiv y\, r^{cp^{n-1}} \,(mod\, p^n),\;\; \text{and}\;\; p-1 \text{ divides } nc. \Big\} \tag{24}$$

Example 3.1. Take $p = 7, r = 3, n = 3, c = 2$ and $y = 1$. We have that $n = 3$ divides $p - 1 = 6$ and $nc = 6$ divides $p - 1 = 6$. Construct the integer $z = r^{cp^{n-1}} = 3^{98}$. Then, by theorem 2.6,

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

Of course, this is a huge number. But Theorem 2.6 ensures that we can find other positive numbers that are less than and equivalent to z modulo p^n. By the use of a calculator, we find easily that $3^{98} \equiv 324 \;\; (mod\; 7^3)$. Indeed,

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

3.2 Proving a general fact about primitive roots modulo p^n

Beside its constructive aspect, the most interesting application of Theorem 2.6 that we have obtained in this paper, is the following.

Corollary 3.2. Let p be an odd prime integer and let r be a primitive root modulo p^2. Suppose that n is an odd prime integer such n divides $p - 1$ and let c be an integer such that $0 < c < p - 1$ and $p - 1$ divides nc. Then

$$\sum_{k=0}^{n-1} r^{kcp^{n-1}} \equiv 0 \;\;\; (mod\;\; p^n). \tag{25}$$

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

$$z = y r^{cp^{n-1}}. \tag{26}$$

By Theorem 2.6, we have $\dfrac{z^n - y^n}{z - y} \equiv 0 \;\;\; (mod\;\; p^n)$, which is equivalent to

$$\sum_{k=0}^{n-1} z^k\, y^{n-k-1} \equiv 0 \;\;\; (mod\;\; p^n). \tag{27}$$

Taking (26) into (27), we obtain

$$y^{n-1} \sum_{k=0}^{n-1} r^{kcp^{n-1}} \equiv 0 \pmod{p^n}. \tag{28}$$

Since y and p are relatively prime, it follows from (28) that

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

□

Example 3.3. As in Example 3.1, we take $p = 7, r = 3, n = 3$ and $c = 2$. Then

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

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 nonnegative integers x, y and z satisfy*

$$x^n + y^n + z^n = 0.$$

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.

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, is a perfect nth power; not necessary equal to p^n but maybe equal to $(p_1 p_2)^n$ or $(p_1 p_2 p_3)^n$ and so on ..., for

some prime integers $p_1, p_2, \ldots$ By going back to Formula (23) and looking at how large is the set ξ_p and the degrees of freedom that we have to construct such set by acting on different parameters p, y, n and c, one may think, naively, that some elements of ξ_p are perfect nth powers. Finding such elements could be done by a constructive proof or by a well-written algorithm.

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.