Journal of Mathematics Research; Vol. 10, No. 3; June 2018
ISSN 1916-9795 E-ISSN 1916-9809
Published by Canadian Center of Science and Education

Brief Summary on Frequently-used Properties about Divisibility of Two's Power Plus-minus One

Jianhui LI[1,2]

[1] Department of Computer Science, Guangdong Neusoft Institue, PRC

[2] State Key Laboratory of Mathematical Engineering and Advanced Computing, China

Correspondence: Jianhui LI, Department of Computer Science, Guangdong Neusoft Institue, Foshan City, Guangdong Province, PRC, 528200.

Received: February 24, 2018 Accepted: March 15, 2018 Online Published: March 27, 2018

doi:10.5539/jmr.v10n3p53 URL: https://doi.org/10.5539/jmr.v10n3p53

Abstract

The article collects the most frequently-used properties of two's power plus-minus one, and classifies them into seven sorts in accordance with the criterion of divisibility, indivisiblity, the calculation of the great common divisor and other traits. Each property is marked with its concrete provenance so that it is a useful reference and convenient for researcher to refer. Some new useful identities are also proved in the paper.

Keywords: Divisibility, number theory, discrete mathematics, mathematical competition

1. Introduction

Two's power plus-minus one, whose mathematical expression is $2^k \pm 1$ with k being a positive integer, frequently occurs in either $2^k + 1$ or $2^k - 1$ in many occasions, such as in number theory (Rosen, 2011 & PANs, 2013), in computer science (Graham R L,1994) and in mathematical competition (Liu P J,2010). Looking into current publications, one can see that, most problems related with $2^k \pm 1$ with k are around their divisibility. A recent research project came across a problem to estimate the smallest order of 2 to an odd prime p. Since this problem needs to know divisibility of $2^k \pm 1$, I had to look through literatures in hand and tried to find something available for solving the problem. Then I found the materials were scattered in many books and articles. After careful classification, I collected the most frequently-used contents and presents them in this article so as to be a reference to other researchers.

2. Symbols and Notations

In this whole paper, numbers are integers by default unless especial comments. Symbol $a|b$ means integer b is divisible by integer a, symbol $a \nmid b$ means b is not divisible by a, and symbol $a^k \| b$ means $a^k | b$ but $a^{k+1} \nmid b$ with integer $k \geq 1$. Formula $a \equiv b (\mathrm{mod} m)$ means a is congruent to b modulo m and it is equivalent to $m|(a-b)$. Symbol (a, b) denotes the greatest common divisor (GCD) between integers a and b. Symbol $A \Leftrightarrow B$ means A is equivalent to B or B holds if and only if A holds. Symbol $A \Longrightarrow B$ means A can derive out B or B is obtained from A. For convenience, use symbol **T** to express the word 'Theorem'. For example, '**T**1' means 'Theorem 1'.

3. Collected Theorems

Relations are classified by divisibility, indivisibility, GCD and the other sort, as listed below.

3.1 Divisible Relations

T1: **Fermat's Little Theorem**[Rosen.2011.p217]. For arbitrary odd prime p, it holds

$$2^{p-1} - 1 \equiv 0 (\mathrm{mod} p)$$

In general, if p is an arbitrary prime and a is an integer with $(p, a) = 1$, then

$$a^{p-1} - 1 \equiv 0 (\mathrm{mod} p)$$

T2: **Euler's Theorem**[Rosen.2011.235]. For arbitrary positive odd integer m, it holds

$$2^{\phi(m)} - 1 \equiv 0 (\mathrm{mod} m)$$

where $\phi(m)$ is the Euler's totient.

In general, if m is a positive integer and a is an integer with $(a, m) = 1$, then

$$a^{\phi(m)} - 1 \equiv 0 (\mathrm{mod} m)$$

T3: [LIU.2008.(v1).p50]. For positive integers m and n,

$$(2^m + 1)|(2^n + 1) \Rightarrow m|n$$

In general, if m ,n and a are arbitrary positive integers with $a > 1$,then

$$(a^m + 1)|(a^n + 1) \Rightarrow m|n$$

if m , n , a and b are positive integers with $(a, b) = 1$,then

$$(a^m + b^m)|(a^n + b^n) \Rightarrow m|n$$

T4: [PAN.2013.p24].Let m and n be positive integers with $m < n$; then

$$(2^m - 1)|(2^n - 1) \Leftrightarrow m|n$$

T5: [LIU.2008.(v1).p69 & PAN.2013.p19]. Let α be an odd integer with $\alpha > 1$; then among the numbers $2^1 - 1, 2^2 - 1, ..., 2^{\alpha-1} - 1$, there exists at least one divisible by α .

3.2 Indivisible Relations

T6: [PAN.2013.p24, LIU.2008.(v1).p57]. For positive integers m and n with $m > 2$, it holds

$$(2^m - 1) \nmid (2^n + 1)$$

T7: [LIU.2008.(v2.1).p11]. Suppose α and β are two primes with $\alpha < \beta$; then for arbitrary integer m, it holds

$$\alpha\beta \nmid m^{\beta-\alpha} + 1$$

Particularly,

$$\alpha\beta \nmid 2^{\beta-\alpha} + 1$$

T8: [Graham.1994.p148, LIU.2008.(v2.1).p86]. For arbitrary integer $n > 1$, it holds

$$n \nmid 2^n - 1$$

T9: [LIU.2008.(v2.1).p11] For positive integers m and n with $n > 1$ and $2 \nmid m$, it holds

$$n \nmid m^{n-1} + 1$$

Particularly,

$$n \nmid (2l)^{n-1} + 1$$

where l is a positive integer.

T10: [LIU.2008.(v2.1).p102&p141]. Suppose d and n are positive integers with $3 \leq d \leq 2^{n+1}$; then

$$d \nmid 2^{2n} + 1$$

In general, suppose a, d and n are positive integers with $3 \leq d \leq 2^{n+1}$; then

$$d \nmid a^{2n} + 1$$

3.3 GCD Relations

T11: [Rosen.2011.p107, PAN.2013.p46 & LIU.2008(v1).p142]. Let m and n be positive integers; then

$$(2^m - 1, 2^n - 1) = 2^{(m,n)} - 1$$

In general, arbitrary integers $a > b$ with $(a, b) = 1$ yields

$$(a^m - b^m, a^n - b^n) = a^{(m,n)} - b^{(m,n)}$$

and thus

$$(a^m - 1, a^n - 1) = a^{(m,n)} - 1$$

and it yields

$$(a^m - 1)|(a^n - 1) \Leftrightarrow m|n$$

T12: [LIU.2008.(v1).p134]. Let k and n be positive integers; then

$$(2^{2k-1} - 1, 2^n + 1) = 1$$

T13: [LIU.2008.(v1).p162]. Let m and n be positive integers such that $\alpha||m$ and $\beta||n$ with α and β being nonnegative integers; then

$$(2^m - 1, 2^n + 1) = \begin{cases} 1, \alpha \leq \beta \\ 2^{(m,n)} + 1, \alpha > \beta \end{cases}$$

T14: [LIU.2008.(v1).p142]. Let m and n be positive integers ; then

$$(2^m + 1, 2^n + 1)|(2^{(m,n)} + 1)$$

3.4 Associate Relations

T15: [PAN.2013.p19]. Let α be odd number with $\alpha > 2$; suppose d is the smallest positive integer x that satisfies $\alpha|(2^x - 1)$; then positive integer h satisfies $\alpha|(2^h - 1)$ if and only if $d|h$.

T16: [LIU.2008.(v2.1).p86] Let p be an odd prime; suppose a is the smallest positive integer x that satisfies $2^x - 1 \equiv 0(\mathrm{mod}p)$ and b is the smallest positive integer y that satisfies $2^y + 1 \equiv 0(\mathrm{mod}p)$; then $a = 2b$. Arbitrary positive integer n that satisfies $2^n + 1 \equiv (\mathrm{mod}p)$ must hold $n = kb$ with k being a positive odd integer.

T17: [PAN.2013.p239]. Suppose p is a prime and h is the smallest positive integer such that $2^h - 1 \equiv 0(\mathrm{mod}p)$; then

$$2|h \Rightarrow 2^{\frac{h}{2}} + 1 \equiv 0(\mathrm{mod}p)$$

3.5 The Mersenne Number & Fermat Number

T18: [Rosen.2011.p258]. If $2^m - 1$ is a prime number, then m is also a prime.

T19: [PAN.2013.p14]. If $2^m + 1$ is a prime number, then m is the form of 2^n with n being a positive integer.

T20: [Rosen.2011.p130]. Let m and n be distinct nonnegative integers; then the two Fermat numbers $F_m = 2^{2^m} + 1$ and $F_n = 2^{2^n} + 1$ satisfy

$$(2^{2^m} + 1, 2^{2^n} + 1) = 1$$

T21: [PAN.2013.p14 & Rosen.2011.p130]. Suppose $m \geq 0$; let $F_m = 2^{2^m} + 1$; then

$$2^{2^{m+1}} - 1 = F_0 \cdot F_1 \cdot \cdots \cdot F_m + 2$$

3.6 Miscellaneous Relations

T22: [LIU.2008.(v1)p61].For arbitrary positive integer n, it holds

$$2^{3n} + 1 = (2^n + 1)(2^{2n} - 2^n + 1)$$

and thus

$$3|(2^{2n} - 2^n + 1)$$

T23: [SHAN.2011.p111]. For arbitrary positive odd numbers m and n, it holds

$$(2^m + 1, 2^n + 1) = 3$$

which also says $3|(2^{2k-1} + 1)$ with arbitrary positive integer k.

T24: [WANG.2017]. For arbitrary integer $\alpha \geq 1$, it holds

$$2^{2\alpha-1} + 1 \equiv 0(\mathrm{mod}3)$$

and

$$2^{2\alpha-2} - 1 \equiv 0(\mathrm{mod}3)$$

And for arbitrary integer $\alpha \geq 1$, it holds

$$2^{2\alpha-1} - 1 \not\equiv 0(\mathrm{mod}3)$$

and

$$2^{2\alpha-2}+1 \not\equiv 0(\mathrm{mod}3)$$

3.7 Related Relations

T25: [LIU.2008.(v1)p162].Arbitrary positive integers n, a and b yield

$$(n, a^n-b^n)=(n, \frac{a^n-b^n}{a-b})$$

T26: [LIU.2008.(v2.1).p91] Let a,b be positive integers and p be an odd prime; then

(1) if $p^l||(a^c-1)$ for positive integers l and c, then $p^{l+1}||(a^{pc}-1)$;

(2) if $p^l||(a^c-1)$ for positive integers l and c, then $p^l||(a^{ce}-1)$ for integer e with $(p,e)=1$;

(3) if $p^l||(a^c-1)$ for positive integers l and c, then $p^{l+k}||(a^{p^k c}-1)$;

(4) if $p^k||(a^b-1)$ for positive integers k and b, then $p^k||b(a^d-1)$ with $d=(b,p-1)$.

T27: [LIU.2008.(v2.1).p8] Let a,b be positive integers and $p>3$ be an odd prime; then

$$ab^p-ba^p \equiv 0(\mathrm{mod}\, p)$$

Particularly,

$$2^p a-2a^p \equiv 0(\mathrm{mod}\, p)$$

T28: [LIU.2008.(v2.1).p189]. If positive integer b is divisible by a^n with a and n being positive integers, then

$$a^{n+1}|((a+1)^b-1)$$

T29: [LIU.2008.(v2.1).p184]. Let p be an odd prime; then

$$\sum_{j=0}^{p}\binom{p}{j}\binom{p+j}{j} \equiv 2^p+1(\mathrm{mod}\, p^2)$$

where $\binom{p}{j}$ is the binomial coefficients such that $\binom{p}{j}=\frac{p!}{j!(p-j)!}$ with $p\geq j\geq 0$.

T30: [LIU.2008.(v2.1).p143].Let p and q be prime numbers with $p+q>6$, then

$$pq \nmid 2^p+2^q$$

T31: [LIU.2008.(v1).p258].Let n and k be positive numbers, then

$$(n^2+n+1)|(n^{3k+2}+n^{3k+1}+1)$$

T32: [LIU 2008.(v1).p139].Let a and b be positive integers with $(a,b)=1$ and p be an odd prime number; then

$$(a+b, \frac{a^p+b^p}{a+b}) = \begin{cases} 1 \\ p \end{cases}$$

T33: Let a and b be positive integers with $(a,b)=1$ and p be an odd prime number; then

$$(a-b, \frac{a^p-b^p}{a-b}) = \begin{cases} 1 \\ p \end{cases}$$

Proof. Let $a-b=t$; then

$$\frac{a^p-b^p}{a-b}=\frac{(t+b)^p-b^p}{t}=\frac{\sum_{i=0}^{p}\binom{p}{i}t^i b^{p-i}-b^p}{t}=\sum_{i=1}^{p}\binom{p}{i}t^{i-1}b^{p-i}$$

Hence

$$(a-b, \frac{a^p-b^p}{a-b})=(t, \sum_{i=1}^{p}\binom{p}{i}t^{i-1}b^{p-i})=(t, pb^{p-1})$$

Note that $(a, b) = 1$ yields $(a + b, b) = 1$; thus

$$(a - b, \frac{a^p - b^p}{a - b}) = (t, p)$$

Since p is a prime number, it knows either $(p, t) = p$ or $(p.t) = 1$.

□

T34:Let a and b be positive integers with $(a, b) = 1$, m be a positive integer and n be an odd integer; then

$$(a - b, \frac{a^m - b^m}{a - b}) = (a - b, m)$$

$$(a + b, \frac{a^n + b^n}{a + b}) = (a + b, n)$$

Proof. The proof of the first one can refer to that of **T**33. Here only prove the second one.Let $a - b = t$; then $a = t - b$ and

$$\frac{a^n + b^n}{a + b} = \frac{(t - b)^n + b^n}{t} = \frac{\sum_{i=0}^{n} \binom{n}{i} t^{n-i}(-b)^i + b^n}{t} = \sum_{i=0}^{n-1} \binom{n}{i} t^{n-i-1}(-b)^i$$

Hence

$$(a + b, \frac{a^n + b^n}{a + b}) = (t, \sum_{i=0}^{n-1} \binom{n}{i} t^{n-i-1}(-b)^i) = (t, \binom{n}{n-1} b^{n-1}) = (t, nb^{n-1})$$

Since $(a, b) = 1$ it holds $(a + b, b) = 1$; thus $(a + b, nb^{n-1}) = (a + b, n)$.

□

T35:Let p be an odd prime number and m be a positive integer; then

$$(p, 2^{m(p-1)} + 2^{(m-1)(p-1)} + ... + 2^{p-1} + 1) = \begin{cases} 1, p \nmid m + 1 \\ p, p|m + 1 \end{cases}$$

or equivalently,

$$(p, \frac{2^{(m+1)(p-1)} - 1}{2^{p-1} - 1}) = \begin{cases} 1, p \nmid m + 1 \\ p, p|m + 1 \end{cases}$$

Proof. Since p is an odd prime number, it holds by Fermats little theorem

$$2^{p-1} - 1 \equiv 0 (\mathrm{mod}\, p)$$

and it holds for arbitrary positive integer k

$$2^{k(p-1)} - 1 \equiv 0 (\mathrm{mod}\, p)$$

Then it yields

$$\begin{aligned}
&(p, 2^{m(p-1)} + 2^{(m-1)(p-1)} + ... + 2^{(p-1)} + 1) \\
&= (p, 2^{m(p-1)} + 2^{(m-1)(p-1)} + ... + 2^{2(p-1)} + 2 + 2^{(p-1)} - 1) \\
&= (p, 2^{m(p-1)} + 2^{(m-1)(p-1)} + ... + 2^{2(p-1)} + 2) \\
&= (p, 2^{m(p-1)} + 2^{(m-1)(p-1)} + ... + 2^{3(p-1)} + 3 + 2^{2(p-1)} - 1) \\
&= (p, 2^{m(p-1)} + 2^{(m-1)(p-1)} + ... + 2^{3(p-1)} + 3) \\
&= ... \\
&= (p, 2^{m(p-1)} + m) \\
&= (p, m + 1 + 2^{m(p-1)} - 1) \\
&= (p, m + 1)
\end{aligned}$$

Since p is prime, it knows either $(p, m+1) = 1$ or $(p, m+1) = p$ holds. Since $2^{m(p-1)} + 2^{(m-1)(p-1)} + ... + 2^{p-1} + 1 = \frac{2^{(m+1)(p-1)} - 1}{2^{p-1} - 1}$, it knows

$$(p, \frac{2^{(m+1)(p-1)} - 1}{2^{p-1} - 1}) = \begin{cases} 1, p \nmid m + 1 \\ p, p|m + 1 \end{cases}$$

□

4. Conclusions and Future Work

Each researcher of science and technology has experienced searching bibliographies in library, or through the Internet or somewhere else. It is really a boring and time-consuming thing when he or she has to face a pile of books, magazines, and even manuscripts because he/she has to look for and record the required contents first and then analyze the gathered materials to select what is needed. It is believed that, the bibliographies prepared process will take almost half the time of writing a paper or report. Therefore, collecting and classifying the former achievements in accordance with professional background are surely necessary and helpful for researchers. This is the purpose of this article. Hope it can benefit as wishes.

Acknowledgements

The research work is supported by the State Key Laboratory of Mathematical Engineering and Advanced Computing under Open Project Program No.2017A01. The author sincerely presents thanks to her.

References

Graham, R. L., Knuth, D. E., & Patashnik, O.(1994). *Concrete Mathematics: A Foundation for Computer Science* (2nd ed). MA: Addison-Wesley, ISBN 0-201-55802-5.

LIU, P. J. (2010). *The Collection of Difficult problems of Elementary Number Theory*, Harbin:Press of Harbin University.

PAN, C. D., & Pan, C. B. (2013). *Elementary Number Theory* (3rd Edition), Beijing:Press of Peking University.

Rosen, K. H. (2011). *Elementary Number Theory and Its Applications* (6th ed). New York: Addison-Wesley.

SHAN, Z. (2011). *The Knowledge and Question of Elementary Number Theory*, Harbin:Harbin Institute of Technology Press.

WANG, X. (2017). Two More Symmetric Properties of Odd Numbers, *IOSR Journal of Mathematics*, 13(3 Ver. II), 37-40. https://doi.org/10.9790/5728-1303023740