Some Theorems on P-adic Order and Their Applications

Cuneyd Ozturk[1] and Kursat Rasim Mestav[1]

[1]Ankara Science High School

01.2011

1 Introduction

Using the auxiliary function called p-adic order is useful working with exponential Diophantine equations. One can prove the theorems in the main section of this article (also known as Lifting the Exponent Lemmas) using p-adic order which is a powerful tool to construct simple proofs for many theorems. Here we had several simple proofs for known theorems in number theory. The most impressive result of this work is we proposed a generalized version of Zsigmondy's Theorem by relaxing the condition $k < m$ when $m \not| k$.

We also applied it to prove a bunch of well-known theorems relating to primitive roots, proved Euler Theorem and proved some special cases of famous Preda-Mihalescu Theorem and Fermat's Last Theorem. We also shared some Mathematics Olympiad problems for the students interested in the math competitions.

2 Main Theorems

Definition 1: For a given prime number p, the ***p*-adic order** of a number n is the highest exponent a such that $p^a|n$. It is commonly abbreviated $V_p(n)$.

$$V_p(n) = a \Leftrightarrow p^a \| n \Leftrightarrow p^a | n, p^{a+1} \not| n.$$

Theorem 2: Let p is an odd prime number, x and y are integers such that $p|x-y$ and $p \not| x, y$. Then for all positive number n,

$$V_p(x^n - y^n) = V_p(x-y) + V_p(n).$$

Theorem 3: Let p is an odd prime number, x and y are integers such that $p|x+y$ and $p \not| x, y$. Then for all positive number n,

$$V_p(x^n + y^n) = V_p(x+y) + V_p(n).$$

Theorem 4: For x and y are odd integers n is positive integer;
(i) if n is odd

$$V_2(x^n - y^n) = V_2(x-y).$$

(ii) if n if even

$$V_2(x^n - y^n) = V_2(\frac{x^2 - y^2}{2}) + V_2(n).$$

3 Applications

3.1 Zsigmondy's Theorem

We extended the Zsigmondy's Theorem by replacing the condition $k < m$ with $m \not| k$.

Theorem 5: ***Extended Zsigmondy's Theorem*****(part I)** $x > y \geq 1$ are coprime integers and $m, k > 1$ positive integers then $x^m - y^m$ has at least one prime divisor such that $k < m$ and it doesn't divide $x^k - y^k$ with the exception is $x + y = 2^\alpha$.

Theorem 6: ***Extended Zsigmondy's Theorem (part II):*** $x > y \geq 1$ are coprime integers and $m, k > 1$ positive integers then $x^m + y^m$ has a prime divisor such that $k < m$ and it doesn't divide $x^k + y^k$ with the exception is $x = 2$,$y = 1$ and $m = 3$.

3.2 Euler's Theorem

Euler's theorem: If n and a are coprime positive integers, then $a^{\varphi(n)} \equiv 1 (mod n)$ where $\varphi(n)$ is Euler's totient function.

3.3 Theorems on the Primitive Roots

Theorem 7: If g is a primitive root modulo p ($p > 2$), g or $g+p$ must be primitive root modulo p^2.

Theorem 8: If g is a primitive root modulo p^k ($p > 2$) ($k \geq 2$), g is also primitive root modulo (p^l for all $l \leq k$.

Theorem 9: If g is a primitive root modulo $(mod p^k)$ ($p > 2$) ($k \geq 2$), g is also primitive root modulo $(mod p^l)$ for all $l \geq k$.

Theorem 10: If $g \equiv -1 (mod 3)$ and $g \equiv -1 (mod 9)$, g is a primitive root modulo 3^a. (a>0).

Theorem 11: If $n \geq 3$ is a integer there isn't exist a primitive root in $(mod 2^n)$.

3.4 Small Cases of the Big Theorems

The theorems below are some of the most challenges theorems to prove in number theory. We proved them only for some special cases.

Theorem 12 (A special case of Fermat's Last Theorem): For $n > 2$, x, y and z are positive integers $x^n + y^n = z^n$ has no solution. We proved this theorem for the condition, x or y is a prime number.

Theorem 13(A special case of Preda-Mihailescu Theorem): x, a, y, b are positive integers and $x, a, y, b > 1$ so only solution for $x^a - y^b = 1$ is $(x, a, y, b) = (3, 2, 2, 3)$. We proved this theorem for the condition, y is a prime number.

4 Exercise Math Olympiad Problems

The solution to the problems below is simple using the main theorems. They are collected for the students interested in math olympiads contest.

Question 1: (IMO 1991 Shortlist) What is the largest power of 1991 which divides $1990^{1991^{1992}} + 1992^{1991^{1990}}$.

Question 2: (IMO 1997 Shortlist) Let b, m, n be positive integers such that $b > 1$ and $m \neq n$ Prove that if $b^m - 1$ and $b^n - 1$ have the same prime divisors, then $b + 1$, is a power of 2.

Question 3: (Balkan M.O. 1993) Let p be a prime and $m \geq 2$ be an integer. Prove that the equation $\frac{x^p + y^p}{2} = \left(\frac{x+y}{2}\right)^m$ has a positive integer solution $(x, y) \neq (1, 1)$ if and only if $m = p$.

Question 4: (IMO 1989 Shortlist) Let m be a positive odd integer, $(m \geq 2)$ Find the smallest positive integer n such that $2^{1989} | m^n - 1$.

Question 5: (Romania Team Selection Test 2009) $a, n \geq 2$ are integers such that there exist an integer k satisfying that $n | (a-1)^k$. Show that $n | a^{n-1} + a^{n-2} + ... + 1$.

Question 6: (IMO-99) Find all the pairs of positive integers (x, p) such that p is a prime, $x \leq 2p$ and $x^{p-1} | (p-1)^x + 1$.

Question 7: (Russia 1996) Let x, y, p, n, k be natural numbers such that $x^n + y^n = p^k$. Prove that if $n > 1$ is an odd number and p an odd prime, then n is a power of p.

Question 8: (Italy Team Selection Test 1999) Prove that for any prime number p the equation $2^p + 3^p = a^n$ has no solution (a, n) in integers greater than 1.

Question 9: (IMO 2000) Does there exist a positive integer n such that n has exactly 2000 prime divisors and n divides $2^n + 1$?

Generalizing the question we also proved the following theorem.

Theorem 14: For all a, b and t positive integers such that $a + b$ has at least one odd divisor there exist infinitely many positive integer n such that $n | a^n + b^n$ and n has exactly t different prime divisor.

5 Appendix A - Preperation for Proofs

Lemma 15. If p is a prime and m, n are integers, then $V_p(mn) = V_p(m) + V_p(n)$.

Proof of Lemma 15: Let's define α and β such that $V_p(m) = \alpha$ and $V_p(n) = \beta$. There exist integers k and l such that $p^\alpha k = m$, $p^\beta l = n$, $p \nmid k$ and $p \nmid l$. Hence $mn = p^{\alpha+\beta}kl$ and

$$p^{\alpha+\beta} \| mn \Leftrightarrow V_p(mn) = \alpha + \beta.$$

Lemma 16. Let p is a prime number, m and n are integers such that $V_p(m) \neq V_p(n)$, then $V_p(m+n) = \min\left\{V_p(m), V_p(n)\right\}$.

Proof of Lemma 16: Let's define u and v such that $p^u \| m$, $p^v \| n$. Then there exist integers k and l such that $m = p^u l$, $n = p^v k$, $p \nmid k$ and $p \nmid l$. Without loss of generality we can say $u > v$. So $m + n = p^v(p^{u-v}l) + k)$. Since $u - v \geq 1$ $(p^{u-v}l) + k \equiv k \not\equiv 0(mod p)$. Then $p^v \| m+n$ and $V_p(m+n) = v = \min\left\{V_p(m), V_p(n)\right\}$.

Lemma 17. Let p is a prime number, x, y and u are integers such that $u \geq 0$, $p \nmid u$, $p \nmid x$, $p \nmid y$ and $p|x-y$, then $V_p(x^u - y^u) = V_p(x-y)$.

Proof of Lemma 17: $(x^u - y^u) = (x-y)(x^{u-1} + ... + y^{u-1})$. We can say $V_p(x^u - y^u) = V_p(x-y) + V_p(x^{u-1} + ... + y^{u-1})$from Lemma 15. Let's find the residue of $(x^{u-1} + ... + y^{u-1})$on $(mod p)$. $p|x-y$is equivalent to $x \equiv y(mod p)$. So $(x^{u-1} + ... + y^{u-1}) \equiv u.x^{u-1}(mod p)$ Because of $p \nmid u$ and$p \nmid x$,$(x^{u-1} + ... + y^{u-1}) \not\equiv 0(mod p)$. Hence $V_p(x^{u-1} + ... + y^{u-1}) = 0$and $V_p(x^u - y^u) = V_p(x-y)$.

Lemma 18. Let p is a prime number, x and y are integers, u is a positive odd integer such that $p \nmid u, p|x+y, p \nmid x$ and $p \nmid y$, then $V_p(x^u + y^u) = V_p(x+y)$.

Proof of Lemma 18: $(x^u + y^u) = (x+y)(x^{u-1} - x^{u-2}y + ... + y^{u-1})$. We can say $V_p(x^u + y^u) = V_p(x+y) + V_p(x^{u-1} - x^{u-2}y + ... + y^{u-1})$ from Lemma 15. Let's find the residue of $(x^{u-1} - x^{u-2}y + ... + y^{u-1})$on (mod p). $p|x+y$is equivalent to $x \equiv -y(mod p)$. So $(x^{u-1} - x^{u-2}y + ... + y^{u-1}) \equiv u.x^{u-1} \not\equiv 0(mod p)$ Because of $p \nmid u$ and$p \nmid x$,$p \nmid (x^{u-1} - x^{u-2}y + ... + y^{u-1})$. Hence $V_p(x^{u-1} - x^{u-2}y + ... + y^{u-1}) = 0$ and $V_p(x^u + y^u) = V_p(x+y)$

Lemma 19. Let p is a prime, i is a positive integer and $0 < i < p$, then $p \| C(p,i)$.

Proof of Lemma 19: $C(p,i) = \frac{p!}{i!(p-i)!}$. We know $p \nmid i!$, $p \nmid (p-i)!$ and $p \| p!$ because $0 < i < p$. So $p \| C(p,i)$.

Lemma 20. p is a prime number a and b are integers such that $p \nmid a$,$p \nmid b$ and $p|a-b$, then $V_p(a^p - b^p) = V_p(a-b) + V_p(p)$.

Proof of Lemma 20: Let's define k such that $p^k \| a-b$. We can find an integer

t such that $a-b=p^k t$ and$p \nmid t$. So $a=p^k t+b$,

$$(a^p-b^p)=(p^k t+b)^p-b^p=\sum_{i=1}^{p}(p^k t)^i b^{p-i}C(p,i).$$

For all i which is in the interval $1\leq i\leq p-1$, $p\|C(p,i)$ from Lemma 19. Hence $p^{ki+1}\left\|(p^k t)^i b^{p-i}C(p,i)\right.$ In other words $V_p((p^k t)^i b^{p-i}C(p,i))=ki+1$. Therefore $V_p\left(\sum_{i=1}^{p}(p^k t)^i b^{p-i}C(p,i)\right)=k+1$ and

$$V_p(a^p-b^p)=V_p\left(\sum_{i=1}^{p}(p^k t)^i b^{p-i}C(p,i)\right)=k+1=V_p(p^k t)+1=V_p(a-b)+V_p(p).$$

Lemma 21 Let a and b are integers and $p\neq 2$ is a prime number such that $p \nmid a$, $p \nmid b$ and $p|a+b$, then $V_p(a^p+b^p)=V_p(a+b)+V_p(p)$.

Proof of Lemma 21: If we define $c=-b$ and use Lemma 20 we get the equation $V_p(a^p-(-c)^p)=V_p(a-(-c))+V_p(p)$. As p is odd it is equivalent to

$$V_p(a^p+c^p)=V_p(a+c)+V_p(p).$$

Lemma 19 Let a is an integer, p is a prime m and n are positive integers such that $a^m\equiv 1(mod p)$, $a^n\equiv 1(mod p)$. Then $a^{(m,n)}\equiv 1(mod p)$.

Proof of Lemma 19: Let $d=(m,n)$ From Euclidean Algorithm there exist x and y such that $mx+ny=d$. So

$$a^{mx+ny}\equiv a^{mx}a^{ny}\equiv 1(mod p).$$

6 Appendix B - Proofs of the Theorems

Proof of Theorem 2: Let's define a such that $p^a \| n$. We can find an integer k such that $n = p^a.k$ and $p \nmid k$. Let define u and v such that $x^{p^a} = u$, $y^{p^a} = v$
$V_p(x^n - y^n) = V_p(u^k - v^k) = V_p(u - v) = V_p(x^{p^a} - y^{p^a})$ from Lemma 17
From Lemma 20 following equations are true,

$$V_p(x^{p^a} - y^{p^a}) = V_p(x^{p^{a-1}} - y^{p^{a-1}}) + V_p(p).$$

$$V_p(x^{p^{a-1}} - y^{p^{a-1}}) = V_p(x^{p^{a-2}} - y^{p^{a-2}}) + V_p(p).$$

$$\vdots$$

$$V_p(x^p - y^p) = V_p(x - y) + V_p(p).$$

If we sum these equations we get

$$V_p(x^n - y^n) = V_p(x^{p^a} - y^{p^a}) = V_p(x - y) + a.V_p(p) = V_p(x - y) + a = V_p(x - y) + V_p(n).$$

Proof of Theorem 3: Let's define a such that $p^a \| n$. We can find an integer k such that $n = p^a.k \text{and} p \nmid k$. Let define u and v such that $x^{p^a} = u$, $y^{p^a} = v$. $V_p(x^n + y^n) = V_p(u^k + v^k) = V_p(u + v) = V_p(x^{p^a} + y^{p^a})$ from Lemma 18. From Lemma 21. following equations are true,

$$V_p(x^{p^a} + y^{p^a}) = V_p(x^{p^{a-1}} + y^{p^{a-1}}) + V_p(p).$$

$$V_p(x^{p^{a-1}} + y^{p^{a-1}}) = V_p(x^{p^{a-2}} + y^{p^{a-2}}) + V_p(p).$$

$$\vdots$$

$$V_p(x^p + y^p) = V_p(x + y) + V_p(p).$$

If we sum these equations we get

$$V_p(x^n + y^n) = V_p(x^{p^a} + y^{p^a}) = V_p(x + y) + a.V_p(p) = V_p(x + y) + a = V_p(x + y) + V_p(n).$$

Proof of Theorem 4: Let's look at the cases;
i) if n is odd;
$V_2(x^n - y^n) = V_2(x - y) + V_2(\sum_{i=0}^{n-1} x^i y^{n-i-1})$ from Lemma 15. From both x and y are odd $x \equiv y (mod 2)$. $\sum_{i=0}^{n-1} x^i y^{n-i-1} \equiv n.x^{n-1} \not\equiv 0 (mod 2)$ and $V_2(n) = 0$ So $\sum_{i=0}^{n-1} x^i y^{n-i-1} \equiv n.x^{n-1} \not\equiv 0 (mod 2)$. ii) if n is even;
We show that case with using induction. For $V_2(n) = 1$ we can define positive integer m such that$m = \frac{n}{2}$, $2 \nmid m$. $V_2(x^{2m} - y^{2m}) = V_2(x^2 - y^2)$...(Lemma 17.).

$V_2(x^2-y^2) = V_2(\frac{x^2-y^2}{2}) + V_2 \ldots$ from Lemma 15. For $V_2(n) = q$ we suppose it is true that

$$V_2(x^n - y^n) = V_2(\frac{x^2-y^2}{2}) + V_2(n)$$

$V_2(x^{2^q} - y^{2^q}) = V_2(\frac{x^2-y^2}{2}) + q \ldots (*)$ from Lemma 17. For $V_2(n) = q+1$ following equation is true from Lemma 15. $V_2(x^n - y^n) = V_2(x^{2^{q+1}} - y^{2^{q+1}}) = V_2(x^{2^q} - y^{2^q}) + V_2(x^{2^q} + y^{2^q})$. $V_2(x^{2^q} - y^{2^q}) = V_2(\frac{x^2-y^2}{2}) + q$ is true. $x^{2^q} \equiv 1(mod 4)$ and $y^{2^q} \equiv 1(mod 4)$ are true from x and y are odd. So, $x^{2^q} + y^{2^q} \equiv 2(mod 4)$ and $V_2(x^{2^q} + y^{2^q}) = 1$. Then $V_2(x^{2^{q+1}} - y^{2^{q+1}}) = V_2(x^{2^q} - y^{2^q}) + V_2(x^{2^q} + y^{2^q}) = V_2(x^{2^q} - y^{2^q}) + 1$. $V_2(x^{2^{q+1}} - y^{2^{q+1}}) = V_2(x^{2^q} - y^{2^q}) + 1 = V_2(\frac{x^2-y^2}{2}) + V_2(2^{q+1})$ is true. So it is true for $q+1$ too. From induction it is true for all even integers n.

Proof of Theorem 5: Let's assume that the greatest common divisor of m and k is d. We can find a, b, n and l positive integers satisfying that $x^d = a$, $y^d = b$, $\frac{m}{d} = n$ and $\frac{k}{d} = l$. In this case, n and l are coprime integers. Because x and y are coprime integers, a and b are coprime integers, too. Now we should prove that there is at least one prime divisor which divides $a^n - b^n$ but does not divide $a^l - b^l$. Our condition was $m \nmid k$ .Then n cannot be equal one. Because if n is equal to one, m must divide k. However it contradicts with our initial conditions. Then we can assume that n is bigger than 1. Let us assume towards a contradiction that there is not such prime for some integers n and l. Then we can easily say that every prime divisor of $a^n - b^n$ divides also $a^l - b^l$ for some integers n and l. Let's rewrite $a^n - b^n$ as ${p_1}^{\alpha_1}.{p_2}^{\alpha_2}...{p_s}^{\alpha_s}$ where $p_i \neq p_j$ and p_i is prime for $i \neq j$. Therefore for all p_i prime numbers such that $\alpha > 1$ p_i must divide $a^l - b^l$. Then the following ones are also true $\left(\frac{a}{b}\right)^n \equiv 1(mod p_i)$ and $\left(\frac{a}{b}\right)^l \equiv 1(mod p_i)$. Therefore from Lemma 19 it is obvious to see that $\left(\frac{a}{b}\right) \equiv 1(mod p_i)$ .In other words $p_i | a-b$. Therefore every prime of $a^n - b^n$ divides also $a-b$. Because $(a-b)|(a^n-b^n)$ all prime divisors of a^n-b^n and $a-b$ are same. Now let's investigate our problem in three cases.

i) if $n = 2^k$

We want to reach a contradiction . In other words we want to show that there exists at least one prime number such that divides $a^n - b^n$ however does not divide $a-b$ if we define $u = a^{2^{k-1}}$ and $v = b^{2^{k-1}} (k \geq 1)$. It is enough to show that there exists at least one prime divisor of $u^2 - v^2$ which does not divide $u-v$. Due to the fact that, $a-b$ divides $u-v$. Since $u+v|u^2-v^2$ if we show that there exists at least one prime divisor of $u+v$ which does not divide $u-v$, we solved this case. According to our first assumption all prime divisors of $u+v$ divide also $u-v$. If p is one of the prime divisors of $u+v$.

$$p|u+v \Rightarrow p|u-v.$$

Then $p|2u$ and $p|2v$. On the other hand greatest common divisor of x and y is 1. Thus p should be equal to 2. Then it is clear to claim that $u+v$ has no odd prime

divisor. Which means $u+v=2^{\beta}$. Let's rewrite this equation as $a^{2^{k-1}}+b^{2^{k-1}}=2^{\beta}$. Firstly, let's investigate this equation for $k>1$. Then if $\beta=1$ it is obvious to see that $a$and $b$is 1. On the other side we defined $x^d=a$ and$y^d=b$. Furthermore, x was bigger than 1. So a cannot be equal to zero. Then we should investigate this case for $\beta>1$. As we know that greatest common divisor of a and $b$is 1 . Thus it is obvious to see that a and $b$are odd integers. Afterwards, if we investigate the sum of $a^{2^{k-1}}+b^{2^{k-1}}$ in $mod4$, we can reach a contradiction. Since a and $b$are odd integers , their residues in $mod4$ are equal to 1. Therefore the sum of $a^{2^{k-1}}+b^{2^{k-1}}$ in $mod4$ is equal to 2. However, $\beta>1$ and it causes a contradiction. Therefore we proved Zsigmondy's Theorem(part I) in this case.

ii)if n has at least one odd prime divisor which does not divide $a-b$. Let's assume that p is one of these primes. We want to reach a contradiction. In other words we want to show that there exists at least one prime number such that divides a^n-b^n however does not divide $a-b$. If we show that a^p-b^phas at least one prime divisor which does not divide$a-b$, we reach the contradiction as we know a^p-b^p divides a^n-b^n. For a prime number q satisfying $q^a\|a-b$ From Theorem 2; $V_q(a^p-b^p)=V_q(a-b)+V_q(p)=V_q(a-b)$ Therefore$q^a\|a^p-b^p$ Hence it is obvious to see that either there exist some prime divisors of a^p-b^p which does not divide $a-b$ or $a^p-b^p=a-b$. According to our first assumption $a^p-b^p=a-b$. Since $a\neq b$, $a^{p-1}+...+b^{p-1}=1$. Because $a>1$ and $b\geq 1$ there is no solution. Therefore we get contradiction. We showed that there exist some prime divisors of a^p-b^pwhich does not divide$a-b$. Hence we proved Zsigmondy's Theorem(part I) in this case.

iii) if n has at least one odd prime divisor and all odd prime divisors of n divide $a-b$. Let's one of the odd prime divisors of n be p. As we know that $p|a-b$. Again, if we showed that there exists at least one prime divisor ofa^p-b^pwhich does not divide $a-b$,we get contradiction and we prove Zsigmondy's Theorem(part I) in this case. If $p^{\beta}\|a-b$ From Theorem 2; $V_p(a^p-b^p)=V_p(a-b)+V_p(p)=V_p(a-b)+1$ Therefore $p^{\beta+1}\|a^p-b^p$ For all q primes such that $q\neq p$and $q^a\|a-b$ Again by Theorem 2; $V_q(a^p-b^p)=V_q(a-b)+V_q(p)=V_q(a-b)$ Therefore$q^a\|a^p-b^p$ Unless there exists at least one prime divisorsa^p-b^p which does not divide $a-b$ a^p-b^pshould be equal to$p(a-b)$. In this case since $a\neq b$; $a^{p-1}+...+b^{p-1}=p$ Since $a>1, b\geq 1$ the equation has no solution in integers. Therefore we get a contradiction. Thus we proved Zsigmondy's Theorem (part I) in this case.

***Proof of Theorem 6*:** Let's assume that greatest common divisor of m and k is d. We can take a, b,n and l positive integers satisfying that $x^d=a$, $y^d=b$, $\frac{m}{d}=n$ and $\frac{k}{d}=l$. In this case, n and l are coprime integers. Because x and $y$are coprime integers, a and b are coprime integers, too. Now we should prove that there is at least one prime divisor which divides a^n+b^nbut does not divide a^l+b^l. Our condition was $m\nmid k$ .Then n cannot be equal one. Because if n is equal to one, m must divide k. However it contradicts with our initial conditions. Then we can assume that n is bigger than 1. Let us assume towards a contradiction that there is not such prime for some integers n and l. Then we can easily

say that every prime divisor of $a^n + b^n$divides also $a^l + b^l$ for some integers n and l. Let's rewrite $a^n - b^n$ as ${p_1}^{\alpha_1}.{p_2}^{\alpha_2}...{p_s}^{\alpha_s}$ where $p_i \neq p_j$ and p_i is prime for $i \neq j$. Therefore for all p_i prime numbers such that $\alpha > 1$ p_i must divide $a^l + b^l$. Then the following ones are also true $\left(\frac{a}{b}\right)^n \equiv -1(mod p_i)$ and $\left(\frac{a}{b}\right)^l \equiv -1(mod p_i)$. Therefore it is obvious to see that ;$\left(\frac{a}{b}\right)^{2n} \equiv 1(mod p_i)$ and $\left(\frac{a}{b}\right)^{2l} \equiv 1(mod p_i)$ Thus from Lemma 19 ; $\left(\frac{a}{b}\right)^2 \equiv 1(mod p_i) \Rightarrow \left(\frac{a}{b} - 1\right)\left(\frac{a}{b} + 1\right) \equiv 1(mod p_i)$ If $\left(\frac{a}{b}\right)$is equal to 1 in$(mod p_i)$, $\left(\frac{a}{b}\right)^n$ is also equal to 1 in$(mod p_i)$ However it is a contradiction since $\left(\frac{a}{b}\right)^n \equiv -1(mod p_i)$ Then it can be claimed that $\left(\frac{a}{b}\right) \equiv -1(mod p_i)$ Which means$p_i|a + b$, therefore according to our assumption; Every prime divisor of$a^n + b^n$ also divide$a + b$. Now let's investigate our problem in three cases;

i) if $n = 2^k$ for every prime p such that $p|a^n + b^n$, $p|a + b$ is also true. Since $a \equiv -b(mod p)$ and $n$is even $a^n \equiv b^n(mod p)$. We also know that $a^n \equiv -b^n(mod p)$ Therefore $p|2a^n$ and $p|2b^n$. On the other side$a$ and b are coprime integers. Hence $p|2$. In other words $p = 2$ Which means $a^n + b^n$ has no odd prime divisor Therefore $a^n + b^n = 2^\alpha$ For $\alpha > 1$ If we investigate residue of $a^n + b^n$ in $(mod 4)$. Since n is even the residue cannot be equal to zero. However $2^\alpha$is equal to zero in $(mod 4)$. Which means we get contradiction! Therefore α should be smaller than 2. However as we know that $a > 1$and $b \geq 1$ Therefore there is no solution for this case. In other words we get contradiction! We proved Zsigmondy's Theorem(part II) in this case.

ii) if n has at least one odd prime divisor which does not divide $a + b$. Let's assume that $p$is one of these primes. We want to reach a contradiction. In other words we want to show that there exists at least one prime number such that divides $a^n + b^n$ however does not divide $a + b$. If we show that $a^p + b^p$has at least one prime divisor which does not divide$a - b$, we reach the contradiction . Because as we know $a^p + b^p$divides $a^n + b^n$. For a prime number q satisfying $q^a \| a + b$. From Theorem 3,

$$V_q(a^p + b^p) = V_q(a + b) + V_q(p) = V_q(a + b)$$

Therefore$q^a \| a^p + b^p$ Hence it is obvious to see that either there exist some prime divisors of $a^p + b^p$ which does not divide $a + b$ or $a^p + b^p = a + b$ According to our assumption; $a^p + b^p = a + b$. On the other side since $a^p > a$ and $b^p \geq b$ there is no solution. This means we get contradiction! Therefore We proved Zsigmondy's Theorem(part II) in this case.

iii) if n has at least one odd prime divisor and all odd prime divisors of n divide $a + b$. Let's one of the odd prime divisors of n be p. As we know that $p|a + b$. Again, if we showed that there exists at least one prime divisor of$a^p + b^p$which does not divide $a + b$ we get contradiction and we prove Zsigmondy's Theorem(part I) in this case. If $p^\beta \| a + b$ From Theorem 3; $V_p(a^p + b^p) = V_p(a + b) + V_p(p) = V_p(a + b) + 1$ Therefore $p^{\beta+1} \| a^p + b^p$ For all q primes such that $q \neq p$and $q^a \| a + b$ Again by Theorem 3; $V_q(a^p + b^p) = V_q(a + b) + V_q(p) = V_q(a + b)$ Therefore$q^a \| a^p + b^p$ According to our assumption $a^p + b^p$ has no other prime

divisor than $a+b$ has. Therefore $a^p + b^p = p(a+b)$ This case give us a trivial solution. Therefore the only solution is that $x = 2$,$y = 1$ and $m = 3$.

Proof of Euler's Theorem: For an integer n, let odd prime divisors of n bep_1,...,p_k and $n = 2^u {p_1}^{a_1}...{p_k}^{a_k}$. First let's show that it is true for odd primes From the Little Fermat's Theorem $a^{p-1} \equiv 1(mod p)$is true. Because $\varphi(p^{a_i}) = p^{a_i-1}(p-1)$ we want to show that $p^{a_i}|a^{(p-1)p^{a_i-1}} - 1$ for all integers $a_i > 0$ $V_p(a^{(p-1).p^{a_i-1}} - 1) = V_p(a^{p-1} - 1) + V_p(p^{a_i-1}) \geq a_i$ from Theorem 2. and (*) So $p^{a_i}|a^{(p-1)p^{a_i-1}} - 1$ and we proved Euler's theorem for odd primes. Then let's prove for$p = 2$. We want to show that $a^{\varphi(2^u)} \equiv 1(mod 2^u)$ because $\varphi(2^u) = 2^{u-1}$. $V_2(a^{2^{u-1}} - 1) = V_2(a^2-1)+V_2(2^{u-1})-1$ is true from Theorem 3. For all odd integers a $V_2(a^2-1) = V_2((a-1)(a+1)) \geq 3$is true from (mod 4) $V_2(a^{2^{u-1}}-1) > u \Leftrightarrow 2^u|a^{2^{u-1}}-1$ so proof is finished.

Proof of Theorem 7: Let define $g$is the primitive root in $(mod p)$So the smallest number d which satisfies $g^d \equiv 1(mod p)$is $d = p-1$. Let's take the smallest number m which satisfies $g^m \equiv 1(mod p^2)$. It also satisfies $g^m \equiv 1(mod p)$ So $p-1|m$ We can find a positive integer l such that $m = (p-1).l$. From Theorem 2 $V_p(g^m - 1) = V_p(g^{(p-1)l} - 1) = V_p(g^{p-1} - 1) + V_p(l)$ and from $g^m \equiv 1(mod p^2)$. $V_p(g^{p-1} - 1) + V_p(l) \geq 2$ is true. If $p \| g^{p-1} - 1$, p should divide l and $p(p-1)|m$. So from Euler's Theorem. $g^m \equiv 1(mod p^2)$is satisfy. From we choose m smallest $m$must be equal to$p(p-1)$. Then g is primitive root in $(mod p^2)$. If $p^2|g^{p-1}-1$ We will show that $p \| (g+p)^{p-1}-1$. $(g+p)^{p-1}-1 \equiv g^{p-1}-1+(p-1)pg^{p-2} \equiv (p-1)pg^{p-2} \equiv -pg^{p-2} \equiv 0(mod p^2)$ Because g and p are coprime. From$p \| (g+p)^{p-1} - 1$ $g+p$is primitive root in $(mod p^2)$.

Proof of Theorem 8: Because $g$is the primitive root in $(mod p^k)$the smallest $d$which satisfies $g^d \equiv 1(mod p^k)$is $\varphi(p^k) = (p-1)p^{k-1}$. Let define a as the smallest integer n which satisfies $g^n \equiv 1(mod p^{k-1})$. $V_p(g^{ap} - 1) = V_p(g^a - 1) + V_p(p) \geq k$ is true From Theorem 2. So $g^{ap} \equiv 1(mod p^k)$and $p^k|g^{ap}-1$. We know$\varphi(p^k)|a.p$because $g$is the primitive root in $(mod p^k)$. So $\varphi(p^{k-1})|a$ and we know $g^{\varphi(p^{k-1})} \equiv 1(mod p^{k-1})$ from Euler's Theorem. Hence we showed that $a = \varphi(p^{k-1})$ and $g$is also the primitive root in $(mod p^{k-1})$. From induction principle if $g$is a primitive root in $(mod p^k)(k \geq 2)$, $g$is also primitive root in $(mod p^l)$ for all $l \leq k$.

Proof of Theorem 9: If $g$is the primitive root in $(mod p^k)$the smallest $d$which satisfies $g^d \equiv 1(mod p^k)$is $\varphi(p^k) = p^{k-1}(p-1)$ Let define $a$as the smallest integer n which satisfies $g^n \equiv 1(mod p^l) l \geq k$. From $g^a \equiv 1(mod p^l)$ $g^a \equiv 1(mod p^k)$is also true. So $p^{k-1}(p-1)|a$. We can find an integer t such that $a = p^{k-1}(p-1).t$. $(g^{p-1})^{p^{k-1}t} \equiv 1(mod p^l)$. $V_p((g^{p-1})^{p^{k-1}t} - 1) = V_p(p^{k-1}.t) + V_p(g^{p-1} - 1)$ is true from Theorem 2. g is a primitive root in $(mod p^2)$ from Theorem 8. So $V_p(g^{p-1}-1) = 1$ is true and $p|g^{p-1} - 1$... (Fermat's Little Theorem) is also true, so $p \| g^{p-1} - 1$ is must be true. From $V_p((g^{p-1})^{p^{k-1}.t-1}) = V_p(p^{k-1}.t) + V_p(g^{p-1}-1) \geq l$, $1 + V_p(p^{k-1}.t)$ So $p^{l-1}|p^{k-1}.t \Rightarrow p^{l-k}|t \Rightarrow p^{l-1}(p-1)|a$from $p^{l-1}(p-1) = \varphi(p^l)$, $g$is also primitive

root in $(mod p^l)$.

Proof of Theorem 10: Let's define $d$as the smallest number satisfying $g^d \equiv 1(mod 3^a)$. We want to show that $d = \varphi(3^a)$. We know $g^d \equiv 1(mod 3)$ and $g \equiv -1(mod 3)$, so d is even. We can choose an integer $m$such that $d = 2m$. So $g^{2m} \equiv 1(mod 3^a)$. $V_3(g^{2m}-1) = V_3(g^2-1) + V_3(m)$ is true from Theorem 2. We know $g \equiv -1(mod 3)$ and $g \equiv 8(mod 9)$ so $3\|g^2-1$ and $V_3(g^2-1) = 1$. We know $V_3(g^{2m}-1) \geq a \Leftrightarrow V_3(g^2-1) + V_3(m) \geq a \Leftrightarrow V_3(m) \geq a-1$.
So $3^{a-1}|d$ and d is even. Therefore g is a primitive root in $(mod 3^a)$ because $2.3^{a-1} = \varphi(3^a)$ and $d = \varphi(3^a)$ is satisfying conditions.

Proof of Theorem 11: Showing that for all odd integer x, $x^{2^{n-2}} \equiv 1(mod 2^n)$ is enough for proof. So $2|\frac{x^2-1}{2}$. $V_2(x^{2^{n-2}}-1) = V_2(\frac{x^2-1}{2}) + V_2(2^{n-2})$ is true from Theorem 3. We want to show that$V_2(x^{2^{n-2}}-1) = V_2(\frac{x^2-1}{2}) + V_2(2^{n-2}) \geq n$. From we know $8|x^2-1$, $V_2(\frac{x^2-1}{2}) \geq 2.V_2(2^{n-2}) = n-2$, so $V_2(x^{2^{n-2}}-1) = V_2(\frac{x^2-1}{2}) + V_2(2^{n-2}) \geq n$.

Proof of Theorem 12: Without loss of generality let's suppose that y is prime.
a)If y is odd prime, from $z-x|z^n-x^n = y^n$ we can find an integer $m$such that$z-x = y^m$. i)If $m > 0$, $y|z-x$. Then from Theorem 2 $V_y(z^n-x^n) = n = V_y(z-x) + V_y(n)$ so $V_y(n) = n-m$ we can find an integer t such that $n = y^{n-m}.t$and $t \nmid y$. There is also true that $V_y(z^{y^{n-m}}-x^{y^{n-m}}) = V_y(z-x) + V_y(y^{n-m}) = n$ from this we can say $y^n|z^{y^{n-m}}-x^{y^{n-m}}$. So $z^{y^{n-m}}-x^{y^{n-m}}|z^n-x^n = y^n$ is true. From $y^n|z^{y^{n-m}}-x^{y^{n-m}}andz^{y^{n-m}}-x^{y^{n-m}}|y^n$ it must be$z^{y^{n-m}}-x^{y^{n-m}} = y^n = z^n-x^n$ and $n = y^{n-m}$ So $(z-x).n = z^n-x^n$ which is a trivial case and only solution is (1,1) but in that case y must be 0. ii)If $m = 0$ let's take a prime divisor$q$of n. $z^q-x^q|z^n-x^n$ and $(z^q-x^q) > z-x = 1$. So $y|z^q-x^q$. Let's define the integer t as $n = q.t$; From theorem 2 $V_y(z^{q.t}-x^{q.t}) = V_y(z^q-x^q) + V_y(t) = q.t$is true. And let's define$k$such that $V_y(z^q-x^q) = k$. So$y^{qt-k}|t$. From$z^q-x^q|y^n$, it must be true that $z^q-x^q = y^k$. Let's define s such that $t = y^{qt-k}.s$. From $y^n|z^{q.y^{qt-k}}-x^{q.y^{qt-k}}$and $z^{q.y^{qt-k}}-x^{q.y^{qt-k}}|z^{q^t}-x^t = y^n$, $z^{q.y^{qt-k}}-x^{q.y^{qt-k}} = z^{q^t}-x^{q^t}$. So $t = y^{qt-k}$ Then $t(z^q-x^q) = z^{q^t}-x^{q^t}$ and it is trivial case which has no solution.
b) If y=2, $z^n-x^n = 2^n$, x and z have same parity because $z-x$ is even. i) If both of them are even; Let's define z=2u and x=2v. So $u^n-v^n = (u-v)(u^{n-1}+...+v^{n-1}) = 1$ it is a trivial case which has no solution. ii) If both of them are odd from Theorem 3. $V_2(z^n-x^n) = V_2(z^2-x^2) + V_2(n) - 1 = n$if we say $V_2(z^2-x^2) = s$it will be that $V_2(n) = n+1-s$. We define k such that $k = n+1-s$; We can find an integer r such that $n = 2^k r$. From $2^n|z^{2^k}-x^{2^k}$ and $z^{2^k}-x^{2^k}|z^n-x^n = 2^n$, $n = 2^k$. So our equation becomes $z^{2^k}-x^{2^k} = 2^{2^k}$ From $z^{2^{k-1}}+x^{2^{k-1}}|z^{2^k}-x^{2^k}$it is true that $z^{2^{k-1}}+x^{2^{k-1}} = 2^w$ $(k > 1)$. In this case there aren't any solution because of $(mod 4)$.

Proof of Theorem 13: $x^a-1 = y^b$. Firstly let's consider the case $y = 2$. If a has an odd prime divisor; Let's assume that one of these prime divisors is q. From

Lemma 17. $V_2(x^a-1)=V_2(x^{\frac{a}{q}}-1^{\frac{a}{q}})$, $a=qt, \Rightarrow (x^a-1)=(x^t-1)(1+...+x^{t(q-1)})$. Since $1+...+x^{t(q-1)}$is an odd integer; $1+...+x^{t(q-1)}=1$ which means if $t\geq 1 \Rightarrow$ Contradiction! If $t=0 \Rightarrow a=0 \Rightarrow$ Contradiction! (Since$a>1$) Therefore a cannot have any odd prime divisors, which means$a=2^k$. $x^{2^k}-1=2^b(x^{2^{k-1}}-1)(x^{2^{k-1}}+1)=2^b \Rightarrow x^{2^{k-1}}-1=2^m, x^{2^{k-1}}+1=2^n$ If $k>1 \Rightarrow x^{2^{k-1}}+1\equiv 2(mod 4)$ which means $n=1 \Rightarrow x=1$ contradiction! (Since $x>1$) Then k should be equal to $1 \Rightarrow (x-1)(x+1)=2^b$ $x-1=2^c, x+1=2^d \Rightarrow 2^d-2^c=2$ $2^d>2 \Rightarrow d>1$. In this case 2^c should be even $\Rightarrow c\geq 1 \Rightarrow 2^{d-1}=2^{c-1}+1$. If $d-1=0$ $\Rightarrow 2^{c-1}=0$ Contradiction! If $d-1>0 \Rightarrow 2|2^{d-1} \Rightarrow 2^{c-1}$should be odd. In other words $c=1$. Therefore $d=2 \Rightarrow b=3$. In this case $x=3, a=2$ Therefore the solution is that $(3,2,2,3)$ Now let's consider the another case $y>2$ If $y|x-1$ $\Rightarrow (x-1)(x^{a-1}+...+1)=y^b$ $x-1=y^c, x^{a-1}+...+1=y^d$. From Theorem 2 $V_p(x^a-1)=V_p(x-1)+V_p(a)=c+d \Rightarrow y^d \| a$ $x^{a-1}<y^d$. (Since $x^{a-1}+...+1=y^d$) Since $x^{y^d-1}\leq x^{a-1}<y^d \Rightarrow x^{y^d-1}<y^d$ Let's denote y^d as u ($u\geq 1$) Since $x^{u-1}<u$,$x>1 \Rightarrow 2^{u-1}\leq x^{u-1}<u$ Which means $2^{u-1}<u$.However it is not true. Claim: $2^{u-1}\geq u$when $u\geq 1$ Let's prove our claim. Our claim is when $u=1$ Let's assume that our claim is true for u Which means $2^{u-1}\geq u$. $2^{u-1}.2\geq 2u\geq u+1$ Therefore we proved our claim by induction. Hence we get contradiction. In other words when $y\neq 2 \Rightarrow y \nmid x-1$ $x-1=y^c \Rightarrow c=0 \Rightarrow x=2 2^a-1=y^b$. If b is even $\Rightarrow y^b\equiv 1(mod 4)$. In other words $2^a=2(mod 4) \Rightarrow a\leq 1$ Contradiction! Since $a>1$.
If b is odd $\Rightarrow y^b+1=(y+1)(\sum_{i=0}^{b-1} y^i(-1)^i)=2^a(\sum_{i=0}^{b-1} y^i(-1)^i)=2^k\equiv b\equiv 1(mod 2) \Rightarrow$ $k=0$ $y^b+1=y+1 \Rightarrow b=1$ Again contradiction! Since $b>1$ Therefore the only solution is $(3,2,2,3)$.

Proof of Theorem 14: We know $a+b$ has at least one odd divisor. Let's assume this prime divisor is p and define sequence $A_k=a^{p^k}+b^{p^k}$ for $k=1,2,...$ and sequence q_k such that$q_k|\left(\frac{a^{p^{k+1}}+b^{p^{k+1}}}{p\left(a^{p^k}+b^{p^k}\right)}\right)$. From Theorem 3. $V_2\left(a^{p^k}+b^{p^k}\right)=V_2\left(a^{p^{k+1}}+b^{p^{k+1}}\right)$. So there isn't any q_k equal to 2. From theorem 3 $V_p(a^{p^{k+1}}+b^{p^{k+1}})=V_p(a^{p^k}+b^{p^k})+V_p(p)$. So $p \nmid \left(\frac{a^{p^{k+1}}+b^{p^{k+1}}}{p\left(a^{p^k}+b^{p^k}\right)}\right)$, and there is not any $q_k$is equal to p. Also the sequence q_k have not two terms such that $q_m=q_n$and $m\neq n$. Let assume towards a contradiction and suppose $m<n$without loss of generality. Then $q_m|\frac{a^{p^{m+1}}+b^{p^{m+1}}}{p}|\frac{a^{p^n}+b^{p^n}}{p}$ is true and $q_n|\left(\frac{a^{p^{n+1}}+b^{p^{n+1}}}{p\left(a^{p^n}+b^{p^n}\right)}\right)$. From$q_m=q_n$,$q_m$must divide the gcd of $\frac{a^{p^n}+b^{p^n}}{p}$and $\frac{a^{p^{n+1}}+b^{p^{n+1}}}{p\left(a^{p^n}+b^{p^n}\right)}$. From $q_m|a^{p^n}+b^{p^n}$ and Theorem 3. $V_{q_m}(a^{p^{n+1}}+b^{p^{n+1}})=V_{q_m}(a^{p^n}+b^{p^n})+V_{q_m}(p)$ We know $V_{q_m}(p)=0$. So,

$$V_{q_m}(a^{p^{n+1}}+b^{p^{n+1}})=V_{q_m}(a^{p^n}+b^{p^n}) \Leftrightarrow V_{q_m}\left(\frac{a^{p^{n+1}}+b^{p^{n+1}}}{a^{p^n}+b^{p^n}}\right)=0.$$

Hence, there must be gcd of $\frac{a^{p^n}+b^{p^n}}{p}$ and $\frac{a^{p^{n+1}}+b^{p^{n+1}}}{p\left(a^{p^n}+b^{p^n}\right)}$ is 1 Contradiction! Hence we can find different primes for every $k = 1,...,t-1$ in the sequence q_k. Let's show that the number $n = p^t q_1 q_2 ... q_{t-1}$ is satisfies the conditions for positive numbers $q_1, q_2, ..., q_{t-1}$. For $k = 1, 2, ..., t-1$, from $q_k \left| \left(\frac{a^{p^{k+1}}+b^{p^{k+1}}}{p\left(a^{p^k}+b^{p^k}\right)} \right) \right.$ is true $q_k | a^{p^t}+b^{p^t}$ is also true. So $q_k | a^n + b^n$ is true. From $p|a+b$ and Theorem 3 $V_p(a^n + b^n) = V_p(a+b) + V_p(n)$. From $V_p(n) = t-1$ and $V_p(a+b) \geq 1$; $V_p(a^n + b^n) \geq t$. $p^t | a^n + b^n$. So we can say n is the number satisfies the conditions.