Lecture 3

Training Camp

16 November 2020

Level 2

Lifting The Exponent Lemma (LTE)

Theorem 3.3.1. *For p being an odd prime relatively prime to integers a and b with $p \mid a - b$ then*

$$v_p\left(a^n - b^n\right) = v_p\left(a - b\right) + v_p\left(n\right).$$

Corollary 3.3.1. *For p being an odd prime relatively prime to a and b with $p \mid a + b$ and n is a **odd** positive integer than*

$$v_p\left(a^n + b^n\right) = v_p\left(a + b\right) + v_p\left(n\right)$$

Theorem 3.3.2. *If $p = 2$ and n is even, and*

- $4 \mid x - y$ *then* $v_2(x^n - y^n) = v_2(x - y) + v_2(n)$
- $4 \mid x + y$ *then* $v_2(x^n - y^n) = v_2(x + y) + v_2(n)$

Example 3.3.3 (IMO 1999). *Find all pairs of positive integers (x,p) such that p is prime, $x \leq 2p$, and $x^{p-1} \mid (p-1)^x + 1$.*

من الواضح أن $x=1$ عبارة حل ، إذن $(x,p) = (1,p)$ حل.

① $p \neq 2$ بما أن $(p-1)^x + 1$ مقدار فردي ، فإن x فردي

$$v_p(x^{p-1}) = (p-1)\, v_p(x) \quad ①$$

$$v_p\left((p-1)^x + 1\right) \geq v_p(x^{p-1}) \quad ②$$

بما أن $p \mid (p-1)+1$ و x فردي فمن LTE

$$v_p\left((p-1)^x + 1\right) = v_p(p) + v_p(x)$$
$$= v_p(x) + 1 \quad ③$$

من ① و ② و ③

$$v_p(x) + 1 \geq (p-1)\, v_p(x)$$

Example 3.3.3 (IMO 1999). *Find all pairs of positive integers (x,p) such that p is prime, $x \leq 2p$, and $x^{p-1} \mid (p-1)^x + 1$.*

$\Rightarrow \quad 1 \geq (p-2)\,(v_p(x))$

Case 1 : $v_p(x) = 1$, $p = 3$

$p \mid x$, $x \leq 2p$ $\Rightarrow$ $3 \mid x$, $x \leq 6$

$\Rightarrow$ $x = 3, 6$

$(x,p) = (3,3)$ $\Leftarrow$ $x = 3$ بالتجريب

Case 2 : $v_p(x) = 0$

ليكن q أصغر قاسم أولي لـ x

$(p-1)^x \equiv -1 \pmod q \Rightarrow (p-1)^{2x} \equiv 1 \pmod q$

$\operatorname{ord}_q(p-1) \mid 2x$, $\operatorname{ord}_q(p-1) \mid q-1$

Example 3.3.3 (IMO 1999). *Find all pairs of positive integers (x,p) such that p is prime, $x \leq 2p$, and $x^{p-1} \mid (p-1)^x + 1$.*

$ord_q(p-1) \mid \gcd(2x, q-1)$

ولكن $\gcd(x, q-1) = 1$ (لأن q هو أصغر قاسم أولي)

$ord_q(p-1) \mid 2 \Rightarrow (p-1)^2 \equiv 1 \pmod q$

$\Rightarrow (p-2)p \equiv 0 \pmod q$

وبما أن $p \nmid x$ فإن $q \neq p$ ، أي أن $p-2 \equiv 0 \pmod q$

$\Rightarrow p \equiv 2 \pmod q$

$\Rightarrow (p-1)^x + 1 \equiv 1+1 \equiv 2 \pmod q$

$\Rightarrow 0 \equiv 2 \pmod q \Rightarrow q = 2$ وهذا تناقض

Example 3.3.3 (IMO 1999). *Find all pairs of positive integers* (x, p) *such that* p *is prime,* $x \leq 2p$, *and* $x^{p-1} \mid (p-1)^x + 1$.

(2) $p = 2$

$$x \mid 1+1 \Rightarrow x \mid 2 \Rightarrow (x, p) = (2, 2)$$

مجموعة الحل:

$$(x, p) = (2, 2), (3, 3), (1, p)$$

$\forall$ p عدد أولي

Example 3.3.3 (IMO 1999). *Find all pairs of positive integers (x, p) such that p is prime, $x \leq 2p$, and $x^{p-1} \mid (p-1)^x + 1$.*

محاولة :

Case 1 $p \mid x$, $p \neq 2$

$v_p(x) = 1$ ($x \leq 2p$ ، و)

$v_p(x^{p-1}) = p-1$

$v_p\left((p-1)^x + 1\right) = v_p(p) + v_p(x)$

$= 2$

$v_p\left((p-1)^x + 1\right) \geq (p-1)\, v_p(x)$ $\Rightarrow$ $3 \geq p$

$2 \geq (p-1)\,1$ $\Rightarrow$ $p = x = 3$

Case 2 $p \nmid x$

$x = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$

$v_{p_1}\left((p-1)^x + 1\right) = v_{p_1}$

Theorem 3.3.2. *If $p = 2$ and n is even, and* x, y are odd integers

- $4 \mid x - y$ *then* $v_2(x^n - y^n) = v_2(x - y) + v_2(n)$
- $4 \mid x + y$ *then* $v_2(x^n - y^n) = v_2(x + y) + v_2(n)$

أثبتنا سابقاً أن:

$$v_p(x^n - y^n) = v_p(x - y) \cdot \gcd(n, p) = 1 \quad n = 2^m n'$$

* كما

$$v_2(x^n - y^n) = v_2\left((x^{2^m})^{n_1} - (y^{2^m})^{n_1}\right) = v_2\left(x^{2^m} - y^{2^m}\right)$$

$$x^{2^m} - y^{2^m} = \left(x^{2^{m-1}} + y^{2^{m-1}}\right)\left(x^{2^{m-1}} - y^{2^{m-1}}\right)$$

$$= \left(x^{2^{m-1}} + y^{2^{m-1}}\right)\left(x^{2^{m-2}} + y^{2^{m-2}}\right) \cdots (x+y)(x-y)$$

Case1 $4 \mid x - y$

$$x \equiv y \equiv \pm 1 \pmod 4$$

$$\Rightarrow \quad x^{2^i} + y^{2^i} \equiv 2 \pmod 4 \quad \forall\, i \geq 0 \Rightarrow v_2\left(x^{2^i} + y^{2^i}\right) = 1$$

$$\Rightarrow v_2\left(x^{2^m} - y^{2^m}\right) = \sum_{i=0}^{m-1} v_2\left(x^{2^i} + y^{2^i}\right) + v_2(x - y) = m + v_2(x - y)$$

$$= v_2(n) + v_2(x - y)$$

Theorem 3.3.2. *If $p = 2$ and n is even, and*

- $4 \mid x - y$ *then* $v_2(x^n - y^n) = v_2(x - y) + v_2(n)$
- $4 \mid x + y$ *then* $v_2(x^n - y^n) = v_2(x + y) + v_2(n)$

Case 2: $4 \mid x+y$

$$x^2 \equiv y^2 \equiv 1 \pmod 4 \Rightarrow x^{2^i} + y^{2^i} \equiv 2 \pmod 4 \quad \forall\ i \geq 1$$

$$\Rightarrow v_2(x^{2^i} + y^{2^i}) = 1$$

$$\Rightarrow v_2(x^{2^m} - y^{2^m}) = \sum_{i=1}^{m-1} v_2(x^{2^i} + y^{2^i}) + v_2(x+y) + v_2(x-y)$$

$$= (m-1) + v_2(x+y) + 1$$

$$= v_2(x+y) + m$$

$$v_2(x^n - y^n) = v_2(x-y) + v_2(x+y) + v_2(n) - 1$$

Example 3.3.4 (Bulgaria). *For some positive integers n, the number $3^n - 2^n$ is a perfect power of a prime. Prove that n is a prime.*

$3^n - 2^n = p^\alpha$, $\alpha \geq 1$ ليكن p عدد أولي يحقق أن

لنفرض أن $n = p_1 p_2 \cdots p_k$ حيث أن $p_1 \leq p_2 \leq \cdots \leq p_k$

و $k \geq 2$. إذن لدينا

$$3^{p_i} - 2^{p_i} \mid 3^n - 2^n \quad \forall \; i \in \{1, 2, \ldots, k\}$$

$$p \mid 3^{p_i} - 2^{p_i} \quad , \quad p \neq 2, 3$$

$$3^{p_i} \equiv 2^{p_i} \pmod p \Rightarrow 3^{p_i} (2^{-1})^{p_i} \equiv 2^{p_i} (2^{-1})^{p_i} \pmod p$$
$$\equiv 1 \pmod p$$

$$\Rightarrow (3 \cdot 2^{-1})^{p_i} \equiv 1 \pmod p \quad , \quad z \equiv 3 \cdot 2^{-1} \pmod p$$

$$z^{p_i} \equiv 1 \pmod p \Rightarrow \operatorname{ord}_p z \mid p_i \quad \forall \; i \in \{1, \ldots, k\}$$

Example 3.3.4 (Bulgaria). *For some positive integers n, the number $3^n - 2^n$ is a perfect power of a prime. Prove that n is a prime.*

$$\text{ord}_p 2 \mid p_i \quad \forall \quad i \in \{1, \dots, k\}$$

$$\text{ord}_p 2 \mid \gcd(p_1, p_2, \dots, p_k)$$

Case 1) $\gcd(p_1, p_2, \dots, p_k) = 1$

$$\text{ord}_p 2 \mid 1 \Rightarrow 2^1 \equiv 1 \pmod p$$

$$\Rightarrow 3 \cdot 2^{-1} \equiv 1 \pmod p$$

$$\Rightarrow 3 \equiv 2 \pmod p$$

وهنا تناقض

Example 3.3.4 (Bulgaria). *For some positive integers n, the number $3^n - 2^n$ is a perfect power of a prime. Prove that n is a prime.*

Case 2) $p_1 = p_2 = \cdots = p_k = q$

$n = q^k$, $\quad ord_p 2 \mid q = \gcd(p_1, p_2, \ldots, p_k)$

$ord_p 2 \neq 1 \Rightarrow ord_p 2 = q$, $\quad q \mid p-1 \Rightarrow p \neq q$ *

$(3\,2^{-1})^q \equiv 1 \pmod p \Rightarrow 3^q \equiv 2^q \pmod p$

$\Rightarrow p \mid 3^q - 2^q$ **

$3^n - 2^n = 3^{q^k} - 2^{q^k} = p^\alpha$

بما أن $p \mid 3^q - 2^q$ ، فإن

$\alpha = v_p\left((3^q)^{q^{k-1}} - (2^q)^{q^{k-1}}\right) = v_p(3^q - 2^q) + v_p(q^{k-1})$

بما أن $p \neq q$ فإن $v_p(q^{k-1}) = 0$

$\alpha = v_p(3^q - 2^q)$

Example 3.3.4 (Bulgaria). *For some positive integers n, the number $3^n - 2^n$ is a perfect power of a prime. Prove that n is a prime.*

$$\alpha = \nu_p(3^q - 2^q) \Rightarrow p^\alpha \mid 3^q - 2^q$$

بما ان $3^q - 2^q$ قوة لـ p فان

$$\Rightarrow 3^q - 2^q = p^\alpha$$

$$\Rightarrow 3^q - 2^q = 3^n - 2^n$$

$$3^n - 3^q = 2^n - 2^q$$

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

وبما ان $n - q > 0$ فان

$3^q > 2^q$ و $3^{n-q} - 1 > 2^{n-q} - 1$

$$\Rightarrow 3^q(3^{n-q} - 1) > 2^q(2^{n-q} - 1)$$

وهذا تناقض ، اذن $k = 1$ و p عدد اولي .

Example 3.3.5 (IMO 1990)**.** *Find all natural n such that $\frac{2^n+1}{n^2}$ is an integer.*

Problem 7 (Russia 1996)**.** Find all positive integers n for which there exist positive integers x, y and k such that $\gcd(x, y) = 1, k > 1$ and $3^n = x^k + y^k$.

Problem 8 (Russia 1996)**.** Let x, y, p, n, k be positive integers such that n is odd and p is an odd prime. Prove that if $x^n + y^n = p^k$, then n is a power of p.

More Number Theory Problems ☺

Let $\mathcal{F}$ be a set of subsets of the set $\{1, 2, \ldots, n\}$ such that

(1) if A is an element of $\mathcal{F}$, then A contains exactly three elements;

(2) if A and B are two distinct elements in $\mathcal{F}$, A and B share at most one common element.

Let $f(n)$ denote the maximum number of elements in $\mathcal{F}$. Prove that

$$\frac{(n-1)(n-2)}{6} \leq f(n) \leq \frac{(n-1)n}{6}.$$

Determine all positive integers k such that

$$\frac{\tau(n^2)}{\tau(n)} = k,$$

for some n.

Let n be a positive integer greater than two. Prove that the Fermat number f_n has a prime divisor greater than $2^{n+2}(n+1)$.