Lecture 1

Training Camp

14 November 2020

Level 2

Lifting The Exponent Lemma (LTE)

حالة P عدد أولي فردي :

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

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

نسخة أخرى للجمع :

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*

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

حالة P=2 :

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

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

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

الإثبات : بالاستقراء الرياضي على $v_p(n)$.

Base Case: $v_p(n) = 0$

$$a^n - b^n = (a-b)(a^{n-1} + a^{n-2}b + \cdots + b^{n-1})$$

$$p \mid a-b \Rightarrow a \equiv b \pmod p$$

$$a^{n-1} + a^{n-2}b + \cdots + b^{n-1} \equiv b^{n-1} + b^{n-2}b + \cdots + b^{n-1}$$
$$\equiv n\, b^{n-1} \pmod p$$

لا يقبل القسمة على p

$$\Rightarrow p \nmid a^{n-1} + a^{n-2}b + \cdots + b^n$$

$$v_p(a^n - b^n) = v_p(a-b) \Rightarrow v_p(a^n - b^n) = v_p(a-b) + v_p(n)$$

Second Base Case:

$$v_p(n) = 1 \quad , \quad n = p\,\underline{n_1} \, , \quad p \nmid n_1$$

$$v_p(a^n - b^n) = v_p(a^{pn_1} - b^{pn_1})$$
$$= v_p((a^p)^{n_1} - (b^p)^{n_1})$$

نستطيع تطبيق Base Case 1 حيث أن $n = n_1$ ، $a := a^p$, $b := b^p$ ، لتطبيق Base Case

نحتاج إثبات أن $p \mid a^p - b^p$ ، ولكن هذا صحيح من فيرما.

$$v_p((a^p)^{n_1} - (b^p)^{n_1}) = v_p(a^p - b^p)$$

$$\Rightarrow \text{①} \; v_p(a^n - b^n) = \underline{v_p(a^p - b^p)} \overset{?}{=} v_p(a-b) + v_p(n)$$

$p \mid a-b \Rightarrow \underline{a-b = pk}, \; k \in \mathbb{Z}$

الآن ندرس $v_p(a^p - b^p)$ ،

نفرض أن $v_p(k) = \alpha$

$$a^p - b^p = (b+pk)^p - b^p$$

$$= b^p + b^{p-1}(pk)\binom{p}{1} + b^{p-2}(pk)^2\binom{p}{2} + \cdots + (pk)^p - b^p$$

$$= \underbrace{b^{p-1}\, \underset{1}{p}\, \underset{\alpha}{k}\, \underset{1}{\binom{p}{1}}}_{\alpha+2} + \underbrace{b^{p-2}(pk)^2\binom{p}{2}}_{\geq 2+2\alpha+1 > \alpha+2} + \cdots + \underbrace{(pk)^p}_{> \alpha+2}$$

$p \nmid k_1$

$k_2, k_3, \ldots, k_p \in \mathbb{Z}$

$$= p^{\alpha+2} k_1 + p^{\alpha+3} k_2 + p^{\alpha+3} k_3 + \cdots + p^{\alpha+3} k_p$$

$$= p^{\alpha+2}(\underbrace{k_1}_{\not\vdots\, p} + pN), \quad N = k_2 + k_3 + \cdots + k_p$$

$$v_p(a^p - b^p) = \alpha + 2 = v_p(k) + 2 = v_p\left(\frac{a-b}{p}\right) + 2$$

$$= v_p(a-b) - 1 + 2$$

$$= v_p(a-b) + 1 \qquad (2)$$

$$v_p(a^n - b^n) \overset{(1)}{=} v_p(a^p - b^p) = v_p(a-b) + 1 = v_p(a-b) + v_p(n)$$

$v_p(n) = 0, 1 \longrightarrow$ الفرضية صحيحة

نفترض أن الفرضية صحيحة لكل n تحقق $v_p(n) \in \{0, 1, \dots, k\}$

ونريد إثباتها لـ $v_p(n) = k+1$

$$n = p^{k+1} n_1$$

$$v_p(a^n - b^n) = v_p(a^{p^{k+1} n_1} - b^{p^{k+1} n_1})$$

$$= v_p\left(\left(a^{p^k}\right)^{pn_1} - \left(b^{p^k}\right)^{pn_1}\right)$$

بما أن $p \mid a^{p^k} - b^{p^k}$ من فيرما، و $v_p(pn_1) = 1$ من Base Case 2

$$= \underbrace{v_p(a^{p^k} - b^{p^k})}_{v_p(p^k) = k} + v_p(pn_1)$$

من فرضية الاستقراء

$$= v_p(a-b) + k + 1 = v_p(a-b) + v_p(n)$$

1. (Folklore) Fix $k \in \mathbb{N}$. Find all n such that $3^k \mid 2^n - 1$.

الحل الأول :

من الواضح أن n عدد زوجي لأن $3 \mid 2^n - 1$ ، أي أن $n = 2m$

$$3^k \mid 2^{2m} - 1 \Rightarrow 3^k \mid 4^m - 1 \iff k \leq v_3(4^m - 1)$$

$$\iff k \leq v_3(4-1) + v_3(m)$$

$$\iff k \leq 1 + v_3(m) \iff v_3(m) \geq k-1 \iff 3^{k-1} \mid m$$

أي أن $n = 2 \cdot 3^{k-1} l$ حيث أن $l \in \mathbb{Z}$

الحل الثاني :

lemma $\operatorname{ord}_{3^k} 2 = 2 \cdot 3^{k-1}$

تم إثباته خلال التدريب الالكتروني

$$3^k \mid 2^n - 1 \iff 2 \cdot 3^{k-1} \mid n \iff n = 2 \cdot 3^{k-1} l$$

2. (Iran 2008) Fix $a \in \mathbb{N}$. Suppose $4(a^n+1)$ is a perfect cube for all $n \in \mathbb{N}$. Prove that $a = 1$.

باعتبار $a^2+1 \pmod 4$ نلاحظ أن a^2+1 لا يمكن أن يكون قوة لـ 2

إذن $a^2+1 = 2^1 p_1^{3\alpha_1} p_2^{3\alpha_2} \cdots p_k^{3\alpha_k}$ ، ليكن $p = p_1$ أي p عدد فردي أولي إذا كان $a \neq 1$

$(k \geq 1)$

$$p \mid a^2+1 \quad , \quad \boxed{v_p(a^2+1) = 3\alpha_1} \quad *$$

$$a^{2p} = (a^2)^p \equiv a^2 \equiv -1 \pmod p \Longrightarrow \boxed{p \mid a^{2p}+1}$$

ولكن من معطى السؤال $4(a^{2p}+1)$ عبارة عن مكعب كامل

وبما أن $p \mid a^{2p}+1$ فإن $v_p(a^{2p}+1) = 3k$

$p \mid a^2+1$, p is odd

Using LTE : $v_p((a^2)^p + 1^p) = v_p(a^2+1) + v_p(p) \overset{*}{=} 3\alpha_1 + 1$

لا يقبل القسمة على 3 $\Leftarrow$ تناقض $\Leftarrow$ $\boxed{a=1}$ وهو حل.

3. (Ireland 1996) If $2^p + 3^p = a^n$ for some prime p, prove $n = 1$.

<u>Case 1</u> $p \neq 2$:

p is odd, $5 \mid 2+3$ so using LTE (version 2)

$$v_5(2^p + 3^p) = v_5(2+3) + v_5(p)$$

$$v_5(2^p + 3^p) = 1 + \underline{v_5(p)}$$

- If $p \neq 5$:

$$v_5(2^p + 3^p) = 1$$

$$\Rightarrow v_5(a^n) = 1$$

$$\Rightarrow n\, v_5(a) = 1 \Rightarrow \boxed{n=1}$$

- If $p = 5$:

$2^5 + 3^5$ is not a perfect power $\Rightarrow \boxed{n=1}$

<u>Case 2</u>: $p = 2$

$2^2 + 3^2 = 13$ is not a perfect power $\Rightarrow \boxed{n=1}$

4. (ISL 1991) Find the largest k such that $1991^k \mid 1990^{1991^{1992}} + 1992^{1991^{1990}}$.

5. (AIME 2018) Find the smallest n such that 3^n ends with 01 when written in base 143.

Example 3.3.1 (AoPS). *Let* $p > 2013$ *be a prime. Also, let* a *and* b *be positive integers such that* $p|(a+b)$ *but* $p^2 \nmid (a+b)$. *If* $p^2|(a^{2013}+b^{2013})$ *then find the number of positive integer* $n \leq 2013$ *such that* $p^n|(a^{2013}+b^{2013})$

Example 3.3.2 (AMM). *Let a, b, c be positive integers such that $c \mid a^c - b^c$. Prove that $c \mid \frac{a^c - b^c}{a - b}$.*

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