Problems on Order of an Element 2

11 June, 2020

Let $a > 1$ and n be given positive integers. If p is an odd prime divisor of $a^{2^n} + 1$, prove that $p - 1$ is divisible by 2^{n+1}.

حل فاطمة

$$p \mid a^{2^n} + 1 \Rightarrow 2^{n+1} \mid p-1$$

$\mathrm{ord}_{p^*}(a) = s$

$$\Rightarrow a^{2^n} \equiv -1 \pmod p$$

$$\Rightarrow a^{2^{n+1}} \equiv 1 \pmod p$$

$$\Rightarrow s \mid 2^{n+1}$$

$$s \in \{1, 2, 4, \dots, 2^n, 2^{n+1}\}$$

$$s \nmid 2^n$$

$$\Rightarrow s = 2^{n+1}$$

$$\Rightarrow s \mid \phi(p) \Rightarrow 2^{n+1} \mid p-1$$

(Classical). *Let n be an integer with $n \geq 2$. Prove that n doesn't divide $2^n - 1$.*

Q5.6

$n \nmid 2^n - 1$

Let by contradiction

$n \mid 2^n - 1 \Rightarrow 2^n \equiv 1 [n]$ let $ord_n(2) = d_1 \Rightarrow \underline{d_1 \mid n}$

$2^{d_1} \equiv 1 [n] \overset{d_1 \mid n}{\Rightarrow} 2^{d_1} \equiv 1 [d_1]$

let $ord_{d_1}(2) = d_2 \Rightarrow d_2 \mid d_1$

$\Rightarrow 2^{d_2} \equiv 1 [d_2]$ ---- $\Rightarrow \underline{2^{d_t} \equiv 1 [d_t]}$ ⊛ we will need to stop in 2

cases:

① $\underline{ord_{d_t}(2) = d_t}$, $ord_{d_t}(2^k) \mid \phi(d_t)$

$\cdot \underline{d_t > \phi(d_t)} \geq ord_{d_t}(2^k) = d_t \Rightarrow \leftarrow$

$\Rightarrow \underline{d_1 > d_2 > \cdots > d_t}$

② $d_t \in \mathbb{P}$ $\Leftarrow$ بما أن d_t آخر حد ممكن بالمتسلسلة

$\Rightarrow 2^{d_t - 1} \equiv 1 [d_t]$ ⊛⊛ $\rightarrow$ من فيرما

$2^{gcd(d_t, d_t - 1)} \equiv 1 [d_t] \Rightarrow 2^1 \equiv 1 [d_t] \Rightarrow \underline{d_t \mid 1} \Rightarrow \leftarrow$

من ⊛ ⊛⊛

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

حل إياد

لماذا $d_t > e(d_t)$ ؟ $d_t \geq 2$

* عدد الأعداد الأولية نسبياً مع d_t والأقل من أو تساوي d_t على الأكثر d_t.

$e(d_t) = d_t(1 - \frac{1}{p_1}) \cdots (1 - \frac{1}{p_k})$ *

$< d_t$

(Classical). *Let n be an integer with $n \geq 2$. Prove that n doesn't divide $2^n - 1$.*

2

$n \Rightarrow odd$

p هو أصغر عدد أولي يقسم n ~~فكذلك~~ p

لنفرض أن $n \mid 2^n - 1$

$\therefore p \mid 2^n - 1$

$2^n \equiv 1 \quad [p]$

ومن فيرما

$2^{p-1} \equiv 1 \quad [p]$

$\therefore p \mid 2^{p-1} - 1$ و $p \mid 2^n - 1$

$\therefore p \mid 2^a - 1 \quad \gcd(n, p-1) = a$

[تم إثباته بسؤال سابق]

وبما أن p هو أصغر عدد أولي يقسم n ، إذاً $\gcd(n, p-1) = 1$

$d = 1$

$p \mid 2 - 1 \Rightarrow p \mid 1 \Rightarrow p = 1$

وهذا مستحيل

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

حل ثاني

$n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$

$p_1 < p_2 < \cdots < p_k$

$p_1 - 1 = q_1^{\beta_1} \cdots q_m^{\beta_m}$

$\Rightarrow q_i < p_1 - 1 < p_1 < \cdots < p_k$

$\Rightarrow \gcd(n, p_1 - 1) = 1$

Let a and b be relatively prime integers. Prove that any odd divisor of $a^{2^n} + b^{2^n}$ is of the form $2^{n+1}m + 1$.

(a) let p prime s.t. $p \mid a^{2^n} + b^{2^n}$ (1), p odd

$\Rightarrow p \mid a^{2^{n+1}} - b^{2^{n+1}}$ (2) $= (a^{2^n} + b^{2^n})(a^{2^n} - b^{2^n})$

let b^{-1} be the inverse of b mod p

$\Rightarrow p \mid (a b^{-1})^{2^{n+1}} - 1$

let $ab^{-1} = c \Rightarrow p \mid c^{2^{n+1}} - 1$ (2), $p \mid c^{2^n} + 1$ (1)

$\text{ord}_p(c) \mid 2^{n+1}$, $\text{ord}_p(c) \nmid 2^n$

$\text{ord}_p(c) \mid p-1$

$\Rightarrow \text{ord}_p(c) \mid \gcd(p-1, 2^{n+1}) = 2^k$

if $k \le n \Rightarrow p \mid c^{2^n} - 1 \Rightarrow p \mid 2$ ↯

$\Rightarrow k = n+1 \Rightarrow 2^{n+1} \mid p-1 \Rightarrow p = 2^{n+1} \cdot m + 1$

حل مهدي

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

$\Rightarrow a^{2^{n+1}} \cdot b^{-2^{n+1}} \equiv b^{2^{n+1}} (b^{-1})^{2^{n+1}}$

$\Rightarrow (a b^{-1})^{2^{n+1}} \equiv 1 \; [p]$

$\Rightarrow c^{2^{n+1}} \equiv 1 \; [p]$

$\Rightarrow$ أي قاسم فردي يطابق

$d = \prod p_i^{\alpha_i} \equiv 1 \pmod{2^{n+1}}$

$\Rightarrow d = 2^{n+1} m' + 1$

(Bulgaria 1996). *Find all pairs of prime p, q such that* $pq \mid (5^p - 2^p)(5^q - 2^q)$.

حل علي

$pq \mid (5^p - 2^p)(5^q - 2^q)$ (1)

if $p = 3$

$\Rightarrow 3q \mid 117 (5^q - 2^q)$

$q \mid 39 (5^q - 2^q)$

$\Rightarrow \boxed{q = 3, 13}$

and if $q = 3$

$\Rightarrow p = 3, 13$

$p, q \neq 3$

(if $p = 5$

$5^p - 2^p \equiv -2 \ [p]$

$(p, 5^p - 2^p) = 1$)

$5^p - 2^p \equiv 5 - 2 \equiv 3 \ [p]$

$(p, 5^p - 2^p) = 1$

$\Rightarrow p \mid (5^q - 2^q)$

$\Rightarrow 5^q \equiv 2^q \ [p]$

$\Rightarrow 5^q \equiv 2^q \ [p]$

بما أن $\gcd(p, 2) = 1$

$(5 \cdot 2^{-1})^q \equiv 1 \ [p]$

$\text{ord}_p (5 \cdot 2^{-1}) = h$

$h \mid q$

if $h = 1$

$2^{-1} = 5^{-1}$

$\Rightarrow \Leftarrow$

$h = q$

$\Rightarrow q \mid p - 1$

by the same steps $p \mid q - 1$

$\Rightarrow \Leftarrow$

$(3,3), (3,13), (13,3)$

$5^q - 2^q \equiv 5 - 2 \pmod q$

* الأسس الأولية توحي باستخدام الأوردر.

+ الأسس التي تكون على الصيغة p^n.

(USA TST 2003). *Find all ordered prime triples* (p, q, r) *such that* $p \mid q^r + 1$, $q \mid r^p + 1$, *and* $r \mid p^q + 1$.

أولي

$p \mid q^r + 1$

يوصي بالـ order

فكرة الحل

$q^r \equiv -1 \pmod{p}$

$q^{2r} \equiv 1 \pmod{p}$ $\Rightarrow$ $\mathrm{ord}_p(q) \mid 2r \Rightarrow$ الاحتمالات الممكنة

$\mathrm{ord}_p(q) \mid p-1$ $+$

$p \mid q^r + 1$ $+$

(USA TST 2003). *Find all ordered prime triples* (p, q, r) *such that* $p \mid q^r + 1$, $q \mid r^p + 1$, *and* $r \mid p^q + 1$.

Case 1: $p, q, r \neq 2$

$\Rightarrow \underline{p \nmid q^r - 1}$

$$\begin{cases} q^{2r} \equiv 1 \pmod{p} \\ r^{2p} \equiv 1 \pmod{q} \\ p^{2q} \equiv 1 \pmod{r} \end{cases} \Rightarrow \begin{cases} \operatorname{ord}_p(q) \mid 2r \Rightarrow \operatorname{ord}_p(q) \in \{1, 2, \cancel{r}, 2r\} \\ \operatorname{ord}_p(q) \mid p-1 \\ \operatorname{ord}_q(r) \mid 2p \Rightarrow \operatorname{ord}_q(r) \in \{1, 2, \cancel{p}, 2p\} \\ \operatorname{ord}_q(r) \mid q-1 \\ \operatorname{ord}_r(p) \mid 2q \Rightarrow \operatorname{ord}_r(p) \in \{1, 2, \cancel{q}, 2q\} \\ \operatorname{ord}_r(p) \mid r-1 \end{cases}$$

(USA TST 2003). *Find all ordered prime triples* (p, q, r) *such that* $p \mid q^r + 1$, $q \mid r^p + 1$, *and* $r \mid p^q + 1$.

Assume that $\operatorname{ord}_p(q), \operatorname{ord}_q(r), \operatorname{ord}_r(p) \in \{1, 2\}$

case 1: $\operatorname{ord}_p(q) = 1 \Rightarrow q \equiv 1 \pmod{p}$

case 2: $\operatorname{ord}_p(q) = 2 \Rightarrow q^2 \equiv 1 \pmod{p} \Rightarrow q \equiv -1 \pmod{p}$

$$\Rightarrow \begin{cases} q \equiv \pm 1 \pmod{p} \\ r \equiv \pm 1 \pmod{q} \\ p \equiv \pm 1 \pmod{r} \end{cases} \Rightarrow \begin{cases} p \mid q \pm 1 \\ q \mid r \pm 1 \\ r \mid p \pm 1 \end{cases} \Rightarrow \begin{cases} q \pm 1 \geq 2p \\ r \pm 1 \geq 2q \\ p \pm 1 \geq 2r \end{cases}$$

$\{q \pm 1, r \pm 1, p \pm 1\}$ are even

وهذا النظام من المتباينات مستحيل

(USA TST 2003). *Find all ordered prime triples* (p, q, r) *such that* $p \mid q^r + 1$, $q \mid r^p + 1$, *and* $r \mid p^q + 1$.

$\Rightarrow$ WLOG $\operatorname{ord}_p(q) = 2r$

$\Rightarrow$ $2r \mid p-1 \Rightarrow r \mid p-1$

$r \mid p^q + 1 \Rightarrow r \mid 1^q + 1 = 2 \Rightarrow r = 2$

تناقض

<u>Case 2</u>: $p=2$ or $q=2$ or $r=2$

WLOG assume that $p=2$

$\Rightarrow$ $p \mid q^r + 1 \Rightarrow q \equiv 1 \pmod 2 \Rightarrow q$ odd

$r \mid 2^q + 1 \Rightarrow r$ odd

$\rightarrow q \mid r^2 + 1 \Rightarrow q \mid r^4 - 1$

$\rightarrow r \mid 2^q + 1 \Rightarrow r \mid 2^{2q} - 1$

$$\Rightarrow \begin{cases} \operatorname{ord}_q(r) \in \{1, 4\} \mid q-1 \\ \operatorname{ord}_r(2) \in \{1, 2, \cancel{4}, 2q\} \mid r-1 \end{cases}$$

(USA TST 2003). *Find all ordered prime triples* (p, q, r) *such that* $p \mid q^r + 1$, $q \mid r^p + 1$, *and* $r \mid p^q + 1$.

- If $\mathrm{ord}_r(2) = 1 \Rightarrow 2^1 \equiv 1 \pmod r \Rightarrow r = 1 \Rightarrow \Leftarrow !$
- If $\mathrm{ord}_r(2) = 2 \Rightarrow 2^2 \equiv 1 \pmod r \Rightarrow r = 3$

$q \mid 3^4 - 1 = 80 \Rightarrow q = 5$ (q odd)

$\Rightarrow (p, q, r) = (2, 5, 3)$.

- If $\mathrm{ord}_r(2) = 2q \Rightarrow 2q \mid r-1 \Rightarrow q \mid r-1$

$r \equiv 1 \pmod q$

ولكن $q \mid r^p + 1 \Leftarrow q \mid 1^p + 1 \Leftarrow q \mid 2 \Leftarrow q = 2$

but q is odd $\Rightarrow \Leftarrow$

Prove that for $n > 1$ we have $n \nmid 2^{n-1} + 1$.

Assume that $n \mid 2^{n-1}+1$

- Let p be a prime, $p \mid n$

$$\Rightarrow \begin{cases} p \mid 2^{p-1} - 1 & * \\ p \mid 2^{n-1} + 1 \Rightarrow p \mid 2^{2(n-1)} - 1 & ** \end{cases}$$

$$\Rightarrow \left\{ p \mid 2^{\gcd(p-1,\, 2(n-1))} - 1 \right.$$

$$\mathrm{ord}_p(2) = s \Rightarrow \begin{cases} s \mid p-1 \\ s \mid 2(n-1) \\ s \nmid (n-1) \end{cases}$$

Prove that for $n > 1$ we have $n \nmid 2^{n-1} + 1$.

$$\begin{cases} s \mid 2(n-1) \\ s \nmid (n-1) \end{cases} \Rightarrow \quad 2(n-1) = s\,k, \quad k \text{ odd}$$

$$v_2(s) = v_2(2(n-1)) \quad (1)$$
$$= v_2(n-1) + 1$$

$$s \mid p-1 \Rightarrow v_2(s) \leq v_2(p-1) \overset{(1)}{\Longrightarrow} v_2(2(n-1)) \leq v_2(p-1) \quad (3)$$

$$\Rightarrow v_2(n-1)+1 \leq v_2(p-1)$$

$$\begin{cases} n \mid 2^{n-1}+1 \\ p \nmid 2 \end{cases} \Rightarrow \quad n-1 = 2^{v_2(n-1)}\, m$$

$$\overset{(2)}{\Rightarrow} p-1 \equiv 0 \pmod{2^{v_2(n-1)+1}}$$

$$\Rightarrow p \equiv 1 \pmod{2^{v_2(n-1)+1}} \longrightarrow p \mid n \quad \text{تناقض}$$

$$\Rightarrow \prod p_i^{\alpha_i} \equiv 1 \pmod{2^{v_2(n-1)+1}} \Rightarrow n \equiv 1 \pmod{2^{v_2(n-1)+1}}$$

Prove that for $n > 1$ we have $n \nmid 2^{n-1} + 1$.

$$2^{v_2(n-1)+1} \mid n-1, \quad n = 2^{v_2(n-1)} m + 1$$

$$\Rightarrow \quad 2^{v_2(n-1)+1} \mid 2^{v_2(n-1)} \cdot m, \quad m \text{ odd}$$

$$\Rightarrow \Leftarrow !!$$

Summary

① القوة الأولية توحي باستخدام الـ order

② القوة التي تأتي على الصيغة p^α ، $2p$ ، pq ———

③ في المقادير مثل

$a^n \equiv -1 \pmod p$ نستنتج $p \mid a^n+1$

$a^{2n} \equiv 1 \pmod p \Rightarrow \operatorname{ord}_p a \mid 2n$

if $p \neq 2 \Rightarrow \operatorname{ord}_p a \nmid n$

④ في عبارات مثل $x \mid 2y$ ، $x \nmid y$ نستنتج أن $v_2(x) = v_2(2y)$

Summary

$* \; v_2(\mathrm{ord}_p a) = v_2(2n)$ ⇐ باستخدام ④ و ③

$** \; v_2(\mathrm{ord}_p a) \leq v_2(p-1)$ ⇐ $\mathrm{ord}_p a \mid p-1$ بمعرفة أن

من $*$ و $**$:

$$v_2(2n) \leq v_2(p-1)$$

$$v_2(n) + 1 \leq v_2(p-1)$$

(China 2009) Find all pairs of primes p, q such that

$$pq \mid 5^p + 5^q$$

* توصي باستخدام الأوردر : ① الأعداد أولية
② الأسس أولية.

<u>Case 1</u>: $p=5$ or $q=5$

WLOG $p=5$.

$\Rightarrow \quad 5q \mid 5^5 + 5^q \Rightarrow q \mid 5^4 + 5^{q-1}$

- If $q=5 \Rightarrow 5 \mid 5^4 + 5^4$ ✓ $\Rightarrow (5,5)$
- If $q \neq 5 \Rightarrow q \mid 5^4 + \underbrace{1}_{\text{من فيرما}} \Rightarrow q \in \{2, 313\}$

$(5,2), (5,313)$

(China 2009) Find all pairs of primes p, q such that

$$pq \mid 5^p + 5^q$$

Case 2: $p, q \neq 5$

$p \mid 5^p + 5^q \Rightarrow p \mid 5 + 5^q \Rightarrow p \mid 1 + 5^{q-1}$

$q \mid 5^p + 5^q \Rightarrow q \mid 5 + 5^p \Rightarrow q \mid 1 + 5^{p-1}$

نفس ما ورد في الـ summary

$$\Rightarrow \begin{cases} 5^{q-1} \equiv -1 \pmod{p} \\ 5^{p-1} \equiv -1 \pmod{q} \end{cases}$$

(China 2009) Find all pairs of primes p, q such that

$$pq \mid 5^p + 5^q$$

- If $p=2$ or $q=2$

  WLOG $p=2$:

  $5 \equiv -1 \pmod{q} \Rightarrow q \mid 6 \Rightarrow q = 2, 3$

  $(2,2) \rightarrow \times$ $\qquad$ $\underline{\underline{(2,3)}}$

- If $p, q \neq 2$

$5^{2(q-1)} \equiv 1 \pmod{p}$

$5^{2(p-1)} \equiv 1 \pmod{q}$

$s_p = \mathrm{ord}_p(5)$, $s_q = \mathrm{ord}_q 5$

$\underline{s_p \mid 2(q-1)}$, $\underline{s_p \nmid q-1}$

$s_q \mid 2(p-1)$, $s_q \nmid p-1$

(China 2009) Find all pairs of primes p, q such that

$$pq \mid 5^p + 5^q$$

$$* \begin{cases} v_2(S_p) = v_2(2(q-1)) = v_2(q-1)+1 \\ v_2(S_q) = v_2(p-1)+1 \end{cases}$$

من الـ summary :

$$5^{p-1} \equiv 1 \pmod{p} \Rightarrow S_p \mid p-1 \Rightarrow v_2(S_p) \leq v_2(p-1)$$

$$5^{q-1} \equiv 1 \pmod{q} \Rightarrow S_q \mid q-1 \Rightarrow v_2(S_q) \leq v_2(q-1)$$

$**$

من $*$ و $*$:

$$v_2(q-1)+1 \leq v_2(p-1)$$

$$v_2(p-1)+1 \leq v_2(q-1)$$

$\Rightarrow$ تناقض

(China 2009) Find all pairs of primes p, q such that

$$pq \mid 5^p + 5^q$$

مجموعة الحل هي :

$(2,3), (3,2), (5,2), (2,5), (5,313), (3,313), (5,5)$

Let q be fixed prime number. Show that there exists infinitely many primes of the form $qm + 1$

Calculate $ord_{3^n}(2)$ *for any* $n \in \mathbb{N}$.