8. Tìm tất cả các số nguyên dương n sao cho tồn tại đa thức P(x) hệ số nguyên thỏa mãn : Với mọi số nguyên dương k, khi chia các số $P^k(0),P^k(1),\ldots,P^k(n-1)$ cho n, ta thu được đúng $\left\lceil \frac{n}{2^k} \right\rceil$ số dư phân biệt.

Step 1): Nếu là lũy thừa của 2 thì P(x)=2x thỏa, easy.
Nếu n là số nguyên tố ta sẽ vẽ đồ thị rồi nội suy Lagrange cái một. Đầu tiên cho nối đỉnh 0 vào chính nó, ta phải nối 1 đỉnh vào chính nó do đặc điểm của đồ thị x->P(x) này. Đặt $a_k=\left\lceil \frac{n}{2^k} \right\rceil$. Ở lượt thứ k thỏa mãn $a_{k-1}>1$ ta sẽ xét các số $a_k,a_k+1,\ldots,a_{k-1}-1$. Ta nối a_{k-1}-i với a_k-i, với mọi $i=1,2,\ldots,a_{k-1}-a_k$. Để ý $2a_k-a_{k-1}\in\{0;1\}$ và đỉnh 0 luôn đc nối với chính nó nên dễ dàng quy nạp là $\{P^k(x) \pmod n | x=0,1,2,\ldots\}=\{0;1;\ldots;a_k-1\}$ với mọi k thỏa $a_{k-1}>1$. Nếu $a_{k-1}=2$ thì $a_k=1$ thì cũng dễ thấy là $\{P^k(x) \pmod n | x=0,1,2,\ldots\}=\{0\}$
Vậy n nguyên tố hoặc lũy thừa 2 thỏa mãn ycbt.
Nhận xét: Với dãy a_k giảm bất kì và n nguyên tố, điều kiện cần và đủ để tồn tại đồ thị là $a_{k-1}-a_k \geq a_{k-2}-a_{k-1}$

Step 2): Ta sẽ loại đi trường hợp lũy thừa số nguyên tố lẻ. Xét n là lũy thừa của p. Ta xét mọi thứ theo (mod n). Ở đây hễ a=b tức là a=b(mod n)
Bổ đề gần như hiển nhiên nhưng CỰC KỲ quan trọng:
Bổ đề: Cho số nguyên tố p, số nguyên ko âm r<p thỏa mãn p | P'(r), khi này với mọi số
nguyên dương n là lũy thừa của p, ta có:
$|\{P(kp+r) \pmod n | k=0,1,\ldots,n/p\}| \leq \frac{n}{p^2}$
Ban đầu, xét $P'(0),P'(1),\ldots,P'(p-1)$, nếu tất cả chúng đều chia hết cho p, thì theo bổ đề ta có $|\{P(i) \pmod n | i=0,1,\ldots,n-1\}| \leq \frac{n}{p}$, tạch
Nên bây h ta xét: Tồn tại số nguyên n để P'(n) khác 0 (mod p)
Gọi c là 1 số m tốt nếu $P'(c), P'(P(c)),\ldots,P'(P^{m+1}(c))$ ko chia hết cho p
Xét $Z_m=\{kp+m \pmod n | k=0,1,2,\ldots\}$. Với tập hợp S, đặt $P^m(S)=\{P^m(x) \pmod n | x\in S\}$
Ý tưởng chính để đánh giá: nếu c là số m tốt thì tồn tại số a sao cho thì $P^{m+1}(Z_c)=Z_a$ nếu ko thì $|P^{m+1}(Z_c)| \leq \frac{n}{p^2}$. Việc $P^{m+1}(Z_c)$ giảm đột ngột xuống $\frac{n}{p^2}$ sẽ thích hợp để đánh giá.
Đặt $S_i=\{P^i(j) | j=0,1,2,\ldots.\}$. Ý tưởng là ta sẽ chọn thời điểm mà $|S_{i+1}|<\frac{1}{2}|S_i|$
Gọi i là số nguyên LỚN NHẤT sao cho tồn tại số i tốt và **thử xét i>0**. Ý tưởng ở đây là xét số c thỏa mãn c là số i tốt và khi này $P^{i+1}(Z_c)=Z_a$ và $X_1=S_{i+1}\backslash Z_a$ khi này $S_{i+2}=P(Z_a)\cup P(X_1)$. Khi này $S_{i+2} \leq \frac{n}{p^2}+|X_1|$ và $S_{i+1}=\frac{n}{p}+|X_1|$. Ta sẽ chọn thời điểm i này vì ở tập S_{i+2} tất cả mọi thứ $(P^{i+2}(Z_c))$ đều $\leq \frac{n}{p^2}$ trong khi ở S_{i+1} vẫn còn $\geq \frac{n}{p}$.
Bắt tay vào thực hiện ý tưởng:

Khi i>0: Ta muốn chặn $|X_1|<\frac{(p-2)n}{p^2}$. Để ý khi này ta sẽ thử xét 2 con a,b thuộc X_1 thỏa mãn $P(a)=P(b) \pmod p$ khi này rất có thể $P^{i+1}(Z_a)$ và $P^{i+1}(Z_b)$ cùng thuộc 1 tập nào đó có kích thước $\leq \frac{n}{p^2}$.

Bây giờ xét con x thỏa mãn $P(x)=x \pmod p$, con này hơi hi hữu. Ta có $P'(x)=0 \pmod p$. Điều khiến ta để ý là $P^m(Z_x)\subset P^{m-1}(Z_x)$ và $|P^m(Z_x)|<|P^{m-1}(Z_x)|$ nên sẽ thuận tiện đánh giá. Để ý 1 con y thỏa mãn $P(y)=x \pmod p$ và y khác x (mod p), để ý là y khác c (mod p) do y ko là số i tốt, khi này $P(Z_y)\subset Z_x$ và $P^3(Z_y)\subset P^2(Z_x)$ và $P^3(Z_x)\subset P^2(Z_x)$. Vì i>0 nên $P^{i+2}(Z_y)$ và $P^{i+2}(Z_x)$ đều $\subset P^2(Z_x)$ nên $|P(X_1)|\leq |P^{i+2}(Z_y)\cup P^{i+2}(Z_x)|+(p-3)\frac{n}{p^2}<(p-2)\frac{n}{p^2}$. Ta có $S_{i+2}\leq \frac{n}{p^2}+|P(X_1)|$ còn $S_{i+1}\geq \frac{n}{p}+|P(X_1)|$ (đúng vậy ta sẽ xét $P(X_1)$ thay vì X_1). Khi này ko khó thấy $|S_{i+2}|<\frac{1}{2}|S_{i+1}|$

Nhận xét khi i>0: Khi bạn nhận ra rằng bạn đã ra 90% bài toán nhưng đánh giá ngu 1 bước là thay vì xét $S_{i+2}\leq \frac{n}{p^2}+|X_1|$ thì bạn có thể xét $S_{i+1}\geq \frac{n}{p}+|P(X_1)|$ vì ra thẳng là $|P(X_1)|<(p-2)\frac{n}{p^2}$ luôn rồi, còn đánh giá $|X_1|$ làm mình mất 5 tiếng cuộc đời mà ko xử lí đc dấu đẳng thức. Để ý là nếu xét X_1 thì bị vướng cái là $|P^{i+1}(Z_y)\cup P^{i+1}(Z_x)|\leq |P(Z_x)|$ nó chỉ $\leq \frac{n}{p^2}$ chứ ko có $<\frac{n}{p^2}$ và khó xử lí dấu =.

Khi i=0: Vậy th hi hữu là i=0. Khi này xét $n_1,n_2,\dots,n_c$ là những số 0 tốt và đôi 1 ko = nhau (mod p), khi này tồn tại $m_1,m_2,\dots,m_d$ đôi 1 ko = nhau (mod p) để $A_1=P(Z_{n_1})\cup P(Z_{n_2})\cup\dots\cup P(Z_{n_c})=Z_{m_1}\cup Z_{m_2}\cup\dots\cup Z_{m_d}$ và xét $X_1=S_1\setminus A_1$. Để ý là $|X_1|\leq (p-c)\frac{n}{p^2}$. Nếu d≥2 thì $X_1=\frac{dn}{p}+A_1$ và $S_2=P(S_1)\cup P(A_1)\leq \frac{dn}{p^2}+A_1$ khi này nếu d≥2 thì $|S_2|<\frac{1}{2}|S_1|$. Nếu d=1, khi này $S_1\leq \frac{n}{p}+\frac{(p-1)n}{p^2}<\frac{n}{2}$ nếu p>3.

Nếu p=3. WLOG $P(2)=2 \pmod 3$ và $P'(0)$ ko chia hết cho 3. Nếu $P(0)=P(1)=2 \pmod 3$ thì $S_1\subset Z_2$, tạch. Trong P(0), P(1) phải có 1 số $=2 \pmod 3$, WLOG là P(1), cái còn lại tương tự, khi này phải có $P(0)=1 \pmod 3$. Nếu $P'(1)$ ko chia hết cho 3 thì Z_1 và $Z_2\subset S_1$ nên $|S_1|\geq \frac{2n}{3}$, tạch. Nên 3 | $P'(1)$, khi này $P(Z_1)\subset Z_2$ và $P^2(Z_1)\subset P(Z_2)$ mặt khác $P^2(Z_2)\subset P(Z_2)$ và $P^2(Z_0)\subset P(Z_1)$. Nên $S_2\leq |P^2(Z_1)\cup P^2(Z_2)|+P^2(Z_0)\leq \frac{2n}{9}$, tạch.

Tóm lại mọi lũy thừa của số nguyên tố lẻ và ko phải số nguyên tố đều ko thỏa.

Step 3): Ta sẽ loại khi n ko phải lũy thừa số nguyên tố. Giả sử $n={p_1}^{a_1}{p_2}^{a_2}\dots{p_k}^{a_k}$. Đặt $S_{(i;j)}=\{P^j(k) \pmod{{p_i}^{a_i}} \mid k=0,1,2,\dots\}$ và đặt $b_{(i;j)}=|S_{(i;j)}|$ và để ý là $S_{(i;j+1)}\subset S_{(i;j)}$ với mọi i,j nên nếu $b_{(i;j+1)}=b_{(i;j)}$ thì $b_{(i,k)}=b_{(i;j)}$ với mọi k≥j+1. Ban đầu, phải có ít nhất 2 số i thỏa mãn $b_{(i;1)}>1$ do $b_{(1;1)}b_{(2;1)}\dots b_{(k;1)}=\left\lceil\frac{n}{2}\right\rceil$. Để ý là với mọi m đủ lớn thì $b_{(i;m)}=1$ với mọi i. Từ đó sẽ tồn tại thời điểm j thỏa mãn, có 2 con số a,b thỏa $b_{(a;j)}$ và $b_{(b;j)}>1$ và $b_{(a;j+1)}=1$. Khi này ta thấy $b_{(b;j+1)}<b_{(b;j)}$ và dễ thấy $b_{(1;j)}b_{(2;j)}\dots b_{(k;j)}>2b_{(1;j+1)}b_{(2;j+1)}\dots b_{(k;j+1)}$, toang.

Tóm lại n ko phải lũy thừa số nguyên tố thì ko thỏa ycbt.