mod pでみた累乗数

高校1年1組24番　関 典史

1　はじめに

この記事では、与えられた自然数m, n, 整数aに対して$x^n \equiv a \pmod{m}$を満たす整数xが存在するか、与えられた素数p, 自然数n, l, 整数aに対して$x_1^n + \cdots + x_l^n \equiv a \pmod{p}$を満たす整数$x_1, \cdots, x_l$が存在するか、について考えたいと思います。

2　準備

必要な定義・定理をいくつか書いておきます。

定義 2.1 (合同式)
$a, b, m \in \mathbb{Z}$について、$a - b$がmで割り切れるとき

$$a \equiv b \pmod{m}$$

と書き、aとbはmを法として合同であるという。

定義 2.2 (オーダー)
素数p, 自然数nに対して、$p^k \mid n$ ($a \mid b$で、bがaで割り切れることを表す) となるような非負整数kの最大値を$ord_p n$と表す。

つまり、$ord_p n$はnがpで何回割れるかを表します。

定義 2.3 (n冪剰余, 非剰余)
p : 素数,$n \in \mathbb{N}(n \geq 2), a \in \mathbb{Z}$とする。
$x^n \equiv a \pmod{p}$を満たすxが存在するときaをpのn冪剰余といい、存在しないときaをpのn冪非剰余という。
$n = 2$のときは、平方剰余, 平方非剰余という。

定理 2.4 (中国剰余定理)
$m_1, m_2, \cdots, m_j \in \mathbb{N}$ はどの二つも互いに素であるとする。
このとき、任意の $a_1, a_2, \cdots, a_j \in \mathbb{Z}$ に対して、

$$x \equiv a_1 \pmod{m_1}$$

$$x \equiv a_2 \pmod{m_2}$$

$$\cdots$$

$$x \equiv a_j \pmod{m_j}$$

を満たす x が $m_1 m_2 \cdots m_j$ を法としてただ一つ存在する。

証明略
この定理の証明はそれほど難しくないのでやってみてください。

定理 2.5 (フェルマーの小定理)
p が素数のとき、任意の $a \in \mathbb{Z}$ に対して

$$a^p \equiv a \pmod{p}$$

が成り立つ。

証明
$a \equiv 0 \pmod{p}$ のときは明らか。
$a \not\equiv 0 \pmod{p}$ のときについて示す。
$p-1$ 個の数 $a, 2a, 3a, \cdots, (p-1)a$ の中の異なる 2 数 ai, aj について $ai \equiv aj \pmod{p}$ が成り立つと仮定すると、$ai \equiv aj \pmod{p} \Leftrightarrow a(i-j) \equiv 0 \pmod{p}$ で、$a \not\equiv 0 \pmod{p}$ より $i - j \equiv 0 \pmod{p}$ であるが、これは $i \neq j, 1 \leq i, j \leq p-1$ に矛盾。
よって、$a, 2a, 3a, \cdots, (p-1)a$ を $\bmod p$ でみると $1, 2, 3, \cdots, p-1$ の並べ替えになっているので、

$$\begin{aligned} a \cdot 2a \cdot 3a \cdots (p-1)a &\equiv 1 \cdot 2 \cdot 3 \cdots (p-1) \pmod{p} \\ \Leftrightarrow 1 \cdot 2 \cdot 3 \cdots (p-1)a^{p-1} &\equiv 1 \cdot 2 \cdot 3 \cdots (p-1) \pmod{p} \end{aligned}$$

$1 \cdot 2 \cdot 3 \cdots (p-1) \not\equiv 0 \pmod{p}$ より

$$a^{p-1} \equiv 1 \pmod{p}$$

よって示された。

証明終

定理 2.6 (原始根の存在)
p が素数であるとき、$r^n \equiv 1 \pmod{p} \Leftrightarrow p-1 \mid n$ となるような r が存在する。このような r を p の原始根という。
また、p : 奇素数,$k \in \mathbb{N}$ であるとき、$r^n \equiv 1 \pmod{p^k} \Leftrightarrow p^{k-1}(p-1) \mid n$ となるような r が存在する。このような r を p^k の原始根という。

証明略
素数 p の原始根を r とすると、$r, r^2, \cdots, r^{p-1}$ は $\bmod p$ でみたとき $1, 2, \cdots, p-1$ の並べ替えになっていて、奇素数の冪 p^k の原始根を r とすると、$r, r^2, \cdots, r^{p^{k-1}(p-1)}$ は $\bmod p^k$ でみたとき $1, 2, \cdots, p^k-1$ のうち p の倍数でないものの並び替えになっています。
これで準備は終わりです。

3 $x^n \equiv a \pmod{m}$

このセクションでは、与えられた自然数 $m, n (m, n \geq 2)$, 整数 a に対して、$x^n \equiv a \pmod{m}$ を満たす x が存在するかどうかを判定することを考えます。

3.1 法が素数の冪であるときへの帰着

定理 3.1
m の素因数分解を $m = p_1^{k_1} p_2^{k_2} \cdots p_j^{k_j}$ とすると $x^n \equiv a \pmod{m}$ が解を持つための必要十分条件は、$1 \leq i \leq j$ なる任意の $i \in \mathbb{N}$ について $x^n \equiv a \pmod{p_i^{k_i}}$ が解を持つことである。

証明
$(\Rightarrow) p_i^{k_i} \mid m$ より明らか。
$(\Leftarrow)$ 各 i に対して $x^n \equiv a \pmod{p_i^{k_i}}$ の解の一つを x_i とする。
中国剰余定理より $x \equiv x_1 \pmod{p_1^{k_1}}, \cdots, x \equiv x_j \pmod{p_j^{k_j}}$ を満たす x が存在し、そのような x は $x^n \equiv a \pmod{m}$ を満たす。

証明終

この定理により、法が素数の冪であるときについてのみ考えればよいことが分かります。

3.2　法が素数の冪であるとき

与えられた素数 p, 自然数 $n(\geq 2), k$, 整数 a に対して $x^n \equiv a \pmod{p^k}$ を満たす x が存在するかどうかを判定することを考えていきましょう。
$p \nmid a$ のときと $p \mid a$ のときに場合分けします。

3.2.1　$p \nmid a$ の場合

まず、$k = 1$ のときは次が成り立ちます。

定理 3.2
$(n, p-1) = m$ ((s,t) は s と t の最大公約数を表す) とすると

$$x^n \equiv a \pmod{p} \text{ が解を持つ} \Leftrightarrow a^{\frac{p-1}{m}} \equiv 1 \pmod{p}$$

が成り立つ。

証明
r を p の原始根とし、$a \equiv r^i \pmod{p}$ とおくと

$$\begin{aligned} x^n \equiv a \pmod{p} \text{ が解を持つ} &\Leftrightarrow (r^j)^n \equiv r^i \pmod{p} \text{ なる } j \text{ が存在する} \\ &\Leftrightarrow nj \equiv i \pmod{p-1} \text{ なる } j \text{ が存在する} \\ &\Leftrightarrow i \text{ が } (n, p-1) = m \text{ で割り切れる} \\ &\Leftrightarrow r^{i \cdot \frac{p-1}{m}} \equiv 1 \pmod{p} \\ &\Leftrightarrow a^{\frac{p-1}{m}} \equiv 1 \pmod{p} \end{aligned}$$

よって示された。

証明終

次に、一般の $k \in \mathbb{N}$ について考えます。$p \nmid n$ のときと $p \mid n$ のときに場合分けします。
$(1) p \nmid n$ のとき

定理 3.3
$x^n \equiv a \pmod{p}$ が解を持つならば、任意の $k \in \mathbb{N}$ に対して、

$$x^n \equiv a \pmod{p^k} \text{ かつ } x^n \not\equiv a \pmod{p^{k+1}}$$

を満たす x が存在する。

証明

まず、任意の $k \in \mathbb{N}$ に対して $x^n \equiv a \pmod{p^k}$ が解を持つことを k に関する数学的帰納法で示す。

(1)$k = 1$ のとき

仮定より明らか。

(2)$k = t$ のとき解を持つと仮定する。

$x^n \equiv a \pmod{p^t}$ の解の一つを x_t とし、$x_t^n - a = bp^t$ $(b \in \mathbb{Z})$ とおく。

$l \in \mathbb{Z}$ に対して、

$$\begin{aligned}(x_t + lp^t)^n - a &= x_t^n - a + nx_t^{n-1}lp^t + \binom{n}{2}x_t^{n-2}l^2p^{2t} + \cdots + l^np^{nt} \\ &= bp^t + nx_t^{n-1}lp^t + \binom{n}{2}x_t^{n-2}l^2p^{2t} + \cdots + l^np^{nt} \\ &\equiv p^t(b + nx_t^{n-1}l) \pmod{p^{t+1}}\end{aligned}$$

よって、$b + nx_t^{n-1}l \equiv 0 \pmod{p}$ となるような $l \in \mathbb{Z}$ をとることができれば、$x_t + lp^t$ は $x^n \equiv a \pmod{p^{t+1}}$ の解となる。

$x_t^n \equiv a \pmod{p}, p \nmid a$ より $x_t \not\equiv 0 \pmod{p}$

これと $p \nmid n$ より $nx_t^{n-1} \not\equiv 0 \pmod{p}$ なので、$b + nx_t^{n-1}l \equiv 0 \pmod{p}$ となるような $l \in \mathbb{Z}$ は存在する。

よって $k = t + 1$ のときも解を持つ。

(1), (2) より、任意の $k \in \mathbb{N}$ について $x^n \equiv a \pmod{p^k}$ は解を持つ。

$x^n \equiv a \pmod{p^k}$ の解の一つを x_k とおくと $x_k + p^k$ も解となっている。

$x_k, x_k + p^k$ がどちらも $x^n \equiv a \pmod{p^{k+1}}$ を満たすと仮定すると、$x_k^n \equiv (x_k + p^k)^n \pmod{p^{k+1}}$ が成り立ち、

$$\begin{aligned}(x_k + p^k)^n &= x_k^n + nx_k^{n-1}p^k + \binom{n}{2}x_k^{n-2}p^{2k} + \cdots + p^{nk} \\ &\equiv x_k^n + nx_k^{n-1}p^k \pmod{p^{k+1}}\end{aligned}$$

より $nx_k^{n-1}p^k \equiv 0 \pmod{p^{k+1}}$ であるが、$x_k^n \equiv a \pmod{p^k}, p \nmid a$ より x_k は p で割り切れず、また仮定より n も p で割り切れないので矛盾。

よって、$x_k, x_k + p^k$ の少なくともどちらか一方は $x^n \not\equiv a \pmod{p^{k+1}}$ を満たすので定理は示された。

証明終

$p \nmid a, p \nmid n$ のときは、$x^n \equiv a \pmod{p}$ が解を持つならば、任意の k に対して $x^n \equiv a \pmod{p^k}$ は解を持ち、それだけでなく任意の k に対して $ord_p(x^n - a) = k$ も解を持

つということが分かったわけです。
$p \nmid a, p \nmid n$ のときは、定理 3.2, 3.3 を用いて $x^n \equiv a \pmod{p^k}$ が解を持つかどうかを判定できます。
(2)$p \mid n$ のとき
まずは補題を一つ示します。

補題 3.4
p : 素数,$m \in \mathbb{N}$ とするとき、$k = 1, 2, \cdots, p^m$ について

$$ord_p \binom{p^m}{k} = m - ord_p k$$

が成り立つ。

証明
$\binom{p^m}{k} = \dfrac{p^m(p^m-1)\cdots(p^m-k+1)}{1\cdot 2\cdots k}$ より

$$ord_p \binom{p^m}{k} = ord_p p^m(p^m-1)\cdots(p^m-k+1) - ord_p 1\cdot 2\cdots k$$

(1)k が p の倍数でないとき
$1, 2, \cdots, k$ の中の p の倍数を $p, 2p, \cdots, lp$ とすると、$lp < k < (l+1)p$ より、$p^m, p^m - 1, \cdots, p^m - k + 1$ の中の p の倍数は $p^m, p^m - p, \cdots, p^m - lp$ である。
よって

$$\begin{aligned} ord_p \binom{p^m}{k} &= \sum_{i=0}^{l} ord_p(p^m - ip) - \sum_{i=1}^{l} ord_p ip \\ &= ord_p p^m + \sum_{i=1}^{l} ord_p(p^m - ip) - \sum_{i=1}^{l} ord_p ip \\ &= m + \sum_{i=1}^{l} (ord_p(p^m - ip) - ord_p ip) \end{aligned}$$

$ord_p ip = n_i$ とすると、$ip = a_i p^{n_i} (a_i \in \mathbb{N}, p \nmid a_i)$ とおける。
また、$ip < k \leq p^m$ より $n_i < m$
よって、$p^m - ip = p^{n_i}(p^{m-n_i} - a_i)$ となり、$p \nmid a_i$ より $p \nmid (p^{m-n_i} - a_i)$ なので、$ord_p(p^m - ip) = n_i = ord_p ip$
したがって $ord_p \binom{p^m}{k} = m$
(2)k が p の倍数であるとき
$1, 2, \cdots, k$ の中の p の倍数を $p, 2p, \cdots, lp$ とすると、$lp = k$ より、$p^m, p^m - 1, \cdots, p^m -$

$k+1$ の中の p の倍数は $p^m, p^m-p, \cdots, p^m-(l-1)p$ である。
よって

$$\begin{aligned} ord_p\binom{p^m}{k} &= \sum_{i=0}^{l-1} ord_p(p^m-ip) - \sum_{i=1}^{l} ord_p ip \\ &= ord_p p^m - ord_p lp + \sum_{i=1}^{l-1} ord_p(p^m-ip) - \sum_{i=1}^{l-1} ord_p ip \\ &= m - ord_p k + \sum_{i=1}^{l-1}(ord_p(p^m-ip) - ord_p ip) \end{aligned}$$

(1) と同様にして、$i=1,2,\cdots,l-1$ に対して $ord_p(p^m-ip) = ord_p ip$
したがって $ord_p\binom{p^m}{k} = m - ord_p k$
(1), (2) より示された。

証明終

では、まず $n=p^m$ のときを考えます。p が奇素数であるときと 2 であるときとで少し違います。
p が奇素数であるとき、次が成り立ちます。

定理 3.5
p を奇素数とする。
$(A) x^{p^m} \equiv a \pmod{p^{m+1}}$ が解を持つ $\Leftrightarrow a^{p-1} \equiv 1 \pmod{p^{m+1}}$
$(B) x^{p^m} \equiv a \pmod{p^{m+1}}$ が解を持つならば、$m+1$ 以上の任意の $k \in \mathbb{N}$ に対して、

$$x^{p^m} \equiv a \pmod{p^k} \text{ かつ } x^{p^m} \not\equiv a \pmod{p^{k+1}}$$

を満たす x が存在する。

証明
(A) r を p^{m+1} の原始根とし、$a \equiv r^i \pmod{p^{m+1}}$ とおくと

$$\begin{aligned} x^{p^m} \equiv a \pmod{p^{m+1}} \text{ が解を持つ} &\Leftrightarrow (r^j)^{p^m} \equiv r^i \pmod{p^{m+1}} \text{ なる } j \text{ が存在する} \\ &\Leftrightarrow p^m j \equiv i \pmod{p^m(p-1)} \text{ なる } j \text{ が存在する} \\ &\Leftrightarrow i \text{ が } (p^m, p^m(p-1)) = p^m \text{ で割り切れる} \\ &\Leftrightarrow r^{i(p-1)} \equiv 1 \pmod{p^{m+1}} \\ &\Leftrightarrow a^{p-1} \equiv 1 \pmod{p^{m+1}} \end{aligned}$$

よって示された。
(B) まず、$m+1$ 以上の任意の $k \in \mathbb{N}$ に対して $x^{p^m} \equiv a \pmod{p^k}$ が解を持つことを

k に関する数学的帰納法で示す。
$(1)k = m+1$ のとき
仮定より明らか。
$(2)k = t(t \geq m+1)$ のとき解を持つと仮定する。
$x^{p^m} \equiv a \pmod{p^t}$ の解の一つを x_t とし、$x_t^{p^m} - a = bp^t$ $(b \in \mathbb{Z})$ とおく。
$l \in \mathbb{Z}$ に対して

$$\begin{aligned}(x_t + lp^{t-m})^{p^m} - a &= \sum_{i=0}^{p^m} \binom{p^m}{i} x_t^{p^m - i} l^i p^{i(t-m)} - a \\ &= x_t^{p^m} - a + p^m x_t^{p^m - 1} l p^{t-m} + \sum_{i=2}^{p^m} \binom{p^m}{i} x_t^{p^m - i} l^i p^{i(t-m)} \\ &= p^t(b + x_t^{p^m - 1} l) + \sum_{i=2}^{p^m} \binom{p^m}{i} x_t^{p^m - i} l^i p^{i(t-m)}\end{aligned}$$

補題 3.4 より $ord_p \binom{p^m}{i} = m - ord_p i$ なので、

$$\begin{aligned}ord_p \binom{p^m}{i} x_t^{p^m - i} l^i p^{i(t-m)} &\geq ord_p \binom{p^m}{i} p^{i(t-m)} \\ &= m - ord_p i + i(t-m) \\ &\geq t + (i-1)(t-m) - ord_p i \\ &\geq t + i - 1 - ord_p i\end{aligned}$$

$i \geq 2$ のとき
$ord_p i = 0$ ならば、$i - ord_p i = i \geq 2$
$ord_p i = \alpha \geq 1$ ならば、$p \geq 3$ より $i - ord_p i \geq p^\alpha - \alpha \geq 2$
よって、$i = 2, 3, \cdots p^m$ に対して

$$\begin{aligned}ord_p \binom{p^m}{i} x_t^{p^m - i} l^i p^{i(t-m)} &\geq t + i - 1 - ord_p i \\ &\geq t + 1\end{aligned}$$

となるので、$(x_t + lp^{t-m})^{p^m} - a \equiv p^t(b + x_t^{p^m - 1} l) \pmod{p^{t+1}}$ である。
したがって、$b + x_t^{p^m - 1} l \equiv 0 \pmod{p}$ となるように $l \in \mathbb{Z}$ をとることができれば、$x_t + lp^{t-m}$ は $x^{p^m} \equiv a \pmod{p^{t+1}}$ の解となる。
$x_t^{p^m} \equiv a \pmod{p^t}, p \nmid a$ より $x_t \not\equiv 0 \pmod{p}$ なので、$x_t^{p^m - 1} \not\equiv 0 \pmod{p}$ であるから、$b + x_t^{p^m - 1} l \equiv 0 \pmod{p}$ となるような $l \in \mathbb{Z}$ は存在する。
よって、$k = t+1$ のときも解を持つ。
$(1), (2)$ より、$m+1$ 以上の任意の $k \in \mathbb{N}$ に対して $x^{p^m} \equiv a \pmod{p^k}$ は解を持つ。

$x^{p^m} \equiv a \pmod{p^k}$ の一つの解を x_k とすると $x_k + p^{k-m}$ も解となっている。
$x_k, x_k + p^{k-m}$ がどちらも $x^{p^m} \equiv a \pmod{p^{k+1}}$ を満たすと仮定すると、$x_k^{p^m} \equiv (x_k + p^{k-m})^{p^m} \pmod{p^{k+1}}$ が成り立ち、$(x_k + p^{k-m})^{p^m} \equiv x_k^{p^m} + x_k^{p^m-1}p^k \pmod{p^{k+1}}$ より $x_k^{p^m-1}p^k \equiv 0 \pmod{p^{k+1}}$ であるが、$x_k^{p^m} \equiv a \pmod{p^k}, p \nmid a$ より x_k は p では割り切れないので矛盾。
よって、$x_k, x_k + p^{k-m}$ の少なくともどちらか一方は $x^{p^m} \not\equiv a \pmod{p^{k+1}}$ を満たすので定理は示された。

証明終

$x^{p^m} \equiv a \pmod{p^{m+1}}$ が解を持つならば、$m+1$ 以上の任意の $k \in \mathbb{N}$ に対して $x^{p^m} \equiv a \pmod{p^k}$ が解を持つことが分かりました。
では、$x^{p^m} \equiv a \pmod{p^m}$ は解を持つが $x^{p^m} \equiv a \pmod{p^{m+1}}$ は解を持たないような a は存在するか、という疑問が生まれますが、これは次に示すように存在します。

定理 3.6
$x^{p^m} \equiv a \pmod{p^m}$ は解を持つが $x^{p^m} \equiv a \pmod{p^{m+1}}$ は解を持たないような a が存在する。

証明
$a = 1 + p^m$ とする。
$x = 1$ は明らかに $x^{p^m} \equiv a \pmod{p^m}$ の解である。
また、

$$\begin{aligned} a^{p-1} &= (1+p^m)^{p-1} \\ &= 1 + (p-1)p^m + \binom{p-1}{2}p^{2m} + \cdots + p^{(p-1)m} \\ &\equiv 1 + (p-1)p^m \pmod{p^{m+1}} \\ &\not\equiv 1 \pmod{p^{m+1}} \end{aligned}$$

となるので、定理 3.5(A) より $x^{p^m} \equiv a \pmod{p^{m+1}}$ は解を持たない。
よって定理は示された。

証明終

次に $p = 2$ すなわち $n = 2^m$ のときを考えます。

定理 3.7
$(A) x^{2^m} \equiv a \pmod{2^{m+2}}$ が解を持つ $\Leftrightarrow a \equiv 1 \pmod{2^{m+2}}$
$(B) x^{2^m} \equiv a \pmod{2^{m+2}}$ が解を持つならば、$m+2$ 以上の任意の $k \in \mathbb{N}$ に対して、

$$x^{2^m} \equiv a \pmod{2^k} \text{ かつ } x^{2^m} \not\equiv a \pmod{2^{k+1}}$$

を満たす x が存在する。

証明

$(A)(\Rightarrow)2 \nmid a$ すなわち a は奇数なので、x は奇数。

よって、$x = 1 + 2y$ $(y \in \mathbb{Z})$ とおけて、

$$\begin{aligned} x^{2^m} &= (1+2y)^{2^m} \\ &= 1 + 2^m \cdot 2y + \binom{2^m}{2} 4y^2 + \sum_{i=3}^{2^m} \binom{2^m}{i} 2^i y^i \\ &= 1 + 2^{m+1} y + 2^{m+1}(2^m - 1)y^2 + \sum_{i=3}^{2^m} \binom{2^m}{i} 2^i y^i \\ &= 1 + 2^{m+1}(y + (2^m - 1)y^2) + \sum_{i=3}^{2^m} \binom{2^m}{i} 2^i y^i \end{aligned}$$

となる。

補題 3.4 より $ord_2 \binom{2^m}{i} = m - ord_2 i$ なので、

$$\begin{aligned} ord_2 \binom{2^m}{i} 2^i y^i &\geq ord_2 \binom{2^m}{i} 2^i \\ &= m - ord_2 i + i \end{aligned}$$

$i \geq 3$ のとき

$ord_2 i = 0, 1$ ならば $i - ord_2 i \geq i - 1 \geq 2$

$ord_2 i = \alpha \geq 2$ ならば $i - ord_2 i \geq 2^\alpha - \alpha \geq 2$

よって、$i = 3, \cdots, 2^m$ に対して

$$\begin{aligned} ord_2 \binom{2^m}{i} 2^i y^i &\geq m - ord_2 i + i \\ &\geq m + 2 \end{aligned}$$

となるので、$x^{2^m} \equiv 1 + 2^{m+1}(y + (2^m - 1)y^2) \pmod{2^{m+2}}$ である。

$y + (2^m - 1)y^2 = y + y^2 + (2^m - 2)y^2 = y(1+y) + (2^m - 2)y^2 \equiv 0 \pmod 2$ より

$y + (2^m - 1)y^2$ は偶数なので、$x^{2^m} \equiv 1 \pmod{2^{m+2}}$

よって、$x^{2^m} \equiv a \pmod{2^{m+2}}$ が解を持つならば $a \equiv 1 \pmod{2^{m+2}}$ である。

$(\Leftarrow) a \equiv 1 \pmod{2^{m+2}}$ であるとき、$x = 1$ は明らかに $x^{2^m} \equiv a \pmod{2^{m+2}}$ の解となる。

(B) 定理 3.5(B) の証明と同じ方針でできるので省略。

証明終

定理 3.6 の証明と同様にして、$x^{2^m} \equiv a \pmod{2^{m+1}}$ は解を持つが $x^{2^m} \equiv a \pmod{2^{m+2}}$ は解を持たないような a が存在することが示せます。

定理 3.8
$x^{2^m} \equiv a \pmod{2^{m+1}}$ は解を持つが $x^{2^m} \equiv a \pmod{2^{m+2}}$ は解を持たないような a が存在する。

証明
$a = 1 + 2^{m+1}$ とすればよい。

証明終

$n = p^m$ の場合は、定理 3.5, 3.7 を用いて $x^n \equiv a \pmod{p^k}$ が解を持つかどうかを判定できます。
$p \mid n$ のとき、$n = n_0 p^m (n_0, m \in \mathbb{N}, p \nmid n_0)$ と表せて、$x^n \equiv a \pmod{p^k} \Leftrightarrow (x^{n_0})^{p^m} \equiv a \pmod{p^k}$ となるので、n が p の冪の場合と $p \nmid n$ の場合を組み合わせて判定することができます。
これで $p \nmid a$ の場合は終わりです。

3.2.2 $p \mid a$ の場合

$p \mid a$ のとき、$a = bp^m (b \in \mathbb{Z}, m \in \mathbb{N}, p \nmid b)$ と表せます。
$k \leq m$ のとき、$bp^m \equiv 0 \pmod{p^k}$ より $x^n \equiv bp^m \pmod{p^k} \Leftrightarrow x^n \equiv 0 \pmod{p^k}$ となり、これは明らかに解を持ちます。
では $k \geq m+1$ のときを考えましょう。次が成り立ちます。

定理 3.9
$k \geq m+1, p \nmid b$ のとき

$x^n \equiv bp^m \pmod{p^k}$ が解を持つ $\Leftrightarrow n \mid m$ でかつ $y^n \equiv b \pmod{p^{k-m}}$ が解を持つ

が成り立つ。

証明
$(\Rightarrow) x^n \equiv bp^m \pmod{p^k}$ が成り立つとすると、$ord_p(x^n - bp^m) \geq k$ である。
$ord_p x^n = l$ とし、$x^n = cp^l (c \in \mathbb{Z}, p \nmid c)$ とおく。
$l > m$ であるとすると、$ord_p(x^n - bp^m) = ord_p(cp^l - bp^m) = ord_p p^m (cp^{l-m} - b) = m < k$ となり矛盾。
$l < m$ であるとすると、$ord_p(x^n - bp^m) = ord_p(cp^l - bp^m) = ord_p p^l (c - bp^{m-l}) = l < m < k$ となり矛盾。

よって、$l = m$ である。
$m = l = ord_p x^n = n \cdot ord_p x$ より $n \mid m$
$n \cdot ord_p x = m$ より $ord_p x = \dfrac{m}{n}$ なので $x = yp^{\frac{m}{n}} (y \in \mathbb{Z}, p \nmid y)$ とおけて、$x^n \equiv bp^m \pmod{p^k}$ より $y^n p^m \equiv bp^m \pmod{p^k}$
よって $y^n \equiv b \pmod{p^{k-m}}$ である。
$(\Leftarrow)$ $n \mid m$ を満たすような n と $y^n \equiv b \pmod{p^{k-m}}$ を満たすような y に対して $x = yp^{\frac{m}{n}}$ とおくと、$x^n \equiv bp^m \pmod{p^k}$ を満たす。
よって示された。

証明終

ちなみに、$y^n \equiv b \pmod{p^{k-m}}$ かつ $y^n \not\equiv b \pmod{p^{k-m+1}}$ を満たすような y が存在するときは、そのような y をとって $x = yp^{\frac{m}{n}}$ とおくと、$x^n \equiv bp^m \pmod{p^k}$ かつ $x^n \not\equiv bp^m \pmod{p^{k+1}}$ を満たします。
この定理を用いて $x^n \equiv bp^m \pmod{p^k}$ が解を持つかを判定できます。
これで $x^n \equiv a \pmod{p^k}$ については終わりです。

以上のことを用いて、与えられた自然数 $m, n (m, n \geq 2)$, 整数 a に対して $x^n \equiv a \pmod{m}$ を満たす x が存在するかどうかを判定することができます。

4 $x_1^n + \cdots + x_l^n \equiv a \pmod{p}$

まずは補題を一つ示します。これは定理 3.2 から容易に得られます。

補題 4.1
p : 素数,$n \in \mathbb{N} (n \geq 2)$ とし、$(n, p-1) = m$ とする。
r を p の原始根とするとき、$r, r^2, \cdots r^{p-1}$ のうち $r^m, r^{2m}, \cdots r^{\frac{p-1}{m} \cdot m}$ が n 冪剰余、それ以外が非剰余であり、$0, 1, 2, \cdots, p-1$ のうち n 冪剰余であるものは $\dfrac{p-1}{m} + 1$ 個, 非剰余であるものは $\dfrac{(m-1)(p-1)}{m}$ 個である。

証明
定理 3.2 より、$r^i (i = 1, 2, \cdots, p-1)$ が n 冪剰余であるための必要十分条件は i が m で割り切れることであるので、補題の前半部分は成り立つ。
$1, 2, \cdots, p-1$ を mod p でみると $r, r^2, \cdots, r^{p-1}$ の並べ替えであるということと前半部分より、$1, 2, \cdots, p-1$ のうち n 冪剰余であるものは $\dfrac{p-1}{m}$ 個, 非剰余であるものは $\dfrac{(m-1)(p-1)}{m}$ 個で、0 は明らかに n 冪剰余なので、後半部分は成り立つ。

証明終

では $x_1^n + \cdots + x_l^n \equiv a \pmod{p}$ について考えていきましょう。
$n = 2$ のときは次が成り立ちます。

定理 4.2
p を素数とするとき、任意の $a \in \mathbb{Z}$ に対して、

$$x_1^2 + x_2^2 \equiv a \pmod{p}$$

を満たす x_1, x_2 が存在する。

証明
補題 4.1 より、$0, 1, 2, \cdots, p-1$ のうち平方剰余であるものは $\dfrac{p+1}{2}$ 個, 非剰余であるものは $\dfrac{p-1}{2}$ 個である。
$0, 1, 2, \cdots, p-1$ のうち平方剰余であるものを $b_1, b_2, \cdots b_{\frac{p+1}{2}}$ とおく。
$a - b_1, a - b_2, \cdots, a - b_{\frac{p+1}{2}}$ がすべて平方非剰余であると仮定すると、$a - b_1, a - b_2, \cdots, a - b_{\frac{p+1}{2}}$ のうちのどの 2 数も p を法として合同でないことから、$0, 1, 2, \cdots, p-1$ のうち平方非剰余であるものが $\dfrac{p+1}{2}$ 個以上あることになり、矛盾。
よって、$a - b_1, a - b_2, \cdots, a - b_{\frac{p+1}{2}}$ のうちの少なくとも一つは平方剰余である。
$a - b_i$ が平方剰余であるとすると、$x_1^2 \equiv b_i \pmod{p}$ なる x_1 と $x_2^2 \equiv a - b_i \pmod{p}$ なる x_2 が存在する。
この x_1, x_2 に対して、$x_1^2 + x_2^2 \equiv a \pmod{p}$ が成り立つ。

証明終

この定理を一般化した次の定理が成り立ちます。

定理 4.3
p : 素数,$n \in \mathbb{N}$ とし、$(n, p-1) = m$ とする。
このとき、任意の $a \in \mathbb{Z}$ に対して、

$$x_1^n + \cdots + x_m^n \equiv a \pmod{p}$$

を満たす $x_1, \cdots, x_m$ が存在する。

証明
r を p の原始根とする。
補題 4.1 より $0, r^m, r^{2m}, \cdots$ は n 冪剰余であるので、任意の a に対して、

$$r^{mj_i} + r^{mj_2} + \cdots + r^{mj_h} \equiv a \pmod{p}$$

となるような $h \leq m, j_1, j_2, \cdots, j_h \in \mathbb{N}$ がとれることを示せばよい。
$k = 0, 1, \cdots, m-1$ に対して

$$A_k = \left\{ a \in \mathbb{Z} \mid \text{ある } i \in \mathbb{N} \text{ が存在して } a \equiv r^{mi+k} \pmod{p} \text{ となる} \right\}$$

とおく。
$r, r^2, \cdots, r^{p-1}$ は mod p でみると $1, 2, \cdots, p-1$ の並べ替えなので、すべての $a \in \mathbb{Z}$ が $A_0, \cdots, A_{m-1}$ のいずれかに属し、また $r^s \equiv 1 \pmod{p} \Leftrightarrow p-1 \mid s$ より $A_0, \cdots, A_{m-1}$ のうちのどの 2 つの共通部分も空集合である。
「$1 \leq d \leq m$ なる任意の $d \in \mathbb{N}$ に対して、ある異なる d 個の集合 $A_{k_1}, \cdots, A_{k_d}$ が存在して、$A_{k_1}, \cdots, A_{k_d}$ のすべての要素 a について

$$r^{mj_1} + \cdots + r^{mj_h} \equiv a \pmod{p}$$

となるような $h \leq d, j_1, \cdots, j_h \in \mathbb{N}$ がとれる (つまり d 個以下の n 冪剰余の和で a を表せる)」$\cdots$ ☆ ことを d に関する数学的帰納法で示す。
$(1) d = 1$ のとき
A_0 のすべての要素 a について $r^{mj_1} \equiv a \pmod{p}$ $(j_1 \in \mathbb{N})$ と表せるので成り立つ。
$(2) d = t$ $(t = 1, 2, \cdots, m-1)$ のとき成り立つと仮定する。
$A_{k_1}, \cdots, A_{k_t}$ のすべての要素 a について、t 個以下の n 冪剰余の和で a を表せるとする。
$A_{k_1}, \cdots, A_{k_t}$ のいずれにも属さない $a \in A_k$ について $r^{mj_1} + \cdots + r^{mj_h} \equiv a \pmod{p}$ $(h \leq t)$ と表せるとすると、任意の $j \in \mathbb{N}$ に対して

$$r^{m(j_1+j)} + \cdots + r^{m(j_h+j)} \equiv ar^{mj} \pmod{p}$$

であるので、A_k のすべての要素 a について $r^{mj_1} + \cdots + r^{mj_h} \equiv a \pmod{p}$ $(h \leq t)$ と表せる。
よって $t+1$ 個の集合 $A_{k_1}, \cdots, A_{k_t}, A_k$ をとると、$d = t+1$ のときも成り立つ。
以下、t 個以下の n 冪剰余の和で表せるような a はすべて $A_{k_1}, \cdots, A_{k_t}$ のいずれかに属するとして考える。
$1 + r^{mj_1} + \cdots + r^{mj_t} \equiv a \pmod{p}$ と表せる a であって、$A_{k_1}, \cdots, A_{k_t}$ のいずれにも属さないようなものが存在することを背理法で示す。
$1 + r^{mj_1} + \cdots + r^{mj_t} \equiv a \pmod{p}$ と表せる a はすべて $A_{k_1}, \cdots, A_{k_t}$ のいずれかに属すると仮定する。
$A_{k_1}, \cdots, A_{k_t}$ のいずれかに属する a を任意にとり、$r^{mj_1} + \cdots + r^{mj_h} \equiv a \pmod{p}$ となるような $h \leq t, j_1, \cdots j_h \in \mathbb{N}$ をとる。
$h = t$ のとき、背理法の仮定より $a+1$ は $A_{k_1}, \cdots, A_{k_t}$ のいずれかに属する。
$h < t$ のとき、$a+1$ が $A_{k_1}, \cdots, A_{k_t}$ のいずれにも属さないとすると、

$$\begin{aligned} r^m + r^{m(j_1+1)} + \cdots + r^{m(j_h+1)} &= r^m(r^{mj_1} + \cdots + r^{mj_h}) \\ &\equiv r^m(a+1) \pmod{p} \end{aligned}$$

より、$A_{k_1},\cdots,A_{k_t}$ のいずれにも属さない $r^m(a+1)$ が t 個以下の n 冪剰余の和で表せることになり矛盾するので、$a+1$ は $A_{k_1},\cdots,A_{k_t}$ のいずれかに属する。
よって、$A_{k_1},\cdots,A_{k_t}$ のすべての要素 a について、$a+1$ も $A_{k_1},\cdots,A_{k_t}$ のいずれかに属するので、$1,2,\cdots,p-1$ がすべて $A_{k_1},\cdots,A_{k_t}$ のいずれかに属することになり、矛盾する。
したがって、$1+r^{mj_1}+\cdots+r^{mj_t}\equiv a \pmod p$ と表せる a であって、$A_{k_1},\cdots,A_{k_t}$ のいずれにも属さないようなものが存在する。
そのような a をとり、$a\in A_k$ とすると、任意の $j\in\mathbb{N}$ について

$$\begin{aligned} r^{mj}+r^{m(j_1+j)}+\cdots+r^{m(j_t+j)} &= r^{mj}(1+r^{mj_1}+\cdots+r^{mj_t}) \\ &\equiv ar^{mj} \pmod p \end{aligned}$$

なので、A_k のすべての要素 a について $r^{mj_1}+\cdots+r^{mj_{t+1}}\equiv a \pmod p$ と表せる。
よって、$t+1$ 個の集合 $A_{k_1},\cdots,A_{k_t},A_k$ をとると、$d=t+1$ のときも成り立つ。
(1), (2) より、☆が示された。
☆を $d=m$ のときについて適用することにより定理は示された。

証明終

これで、どんな整数も mod p において $(n,p-1)$ 個の n 冪剰余の和として表せるという綺麗な事実が分かりました。

5 最後に

4 で、どんな整数も mod p において $(n,p-1)$ 個の n 冪剰余の和として表せるということを示しましたが、この $(n,p-1)$ 個というのは必ずしも最小の個数であるとは限りません。例えば $p=13,n=3$ とすると、$(n,p-1)=3$ ですが、実際には mod13 においてすべての整数を 2 個の 3 次剰余の和で表すことができます (一度やってみてください)。この最小個数を求める問題は今後の課題です。この問題について何か分かった方、もしくは質問・感想がある方は、是非 n_seki@wc4.so-net.ne.jp までメール下さい。

なお、この記事を TEX で打つのに
pLATEX 2ε for WINDOWS Another Manual（乙部厳己, 江口庄英 著 SOFTBANK 社）
を参考にしました。
また、整数論の参考文献としては以下のようなものがあります。
初等整数論講義（高木貞治 著 共立出版）

数論入門 I,II（G.H.Hardy,E.M.Wright 著　シュプリンガー・フェアラーク東京）
この記事を読んで整数論に興味を持たれた方は是非読んでみてください。

今回この記事を書いて、質の高い記事を書くのはやはり難しいということを痛感しました。来年は今年より少しでもいいものを書けるよう努力しようと思います。そして最後に、協力してくれた部員のみんなに感謝です。

最後まで読んでいただき、本当にありがとうございました！