「Wolstenholmeの定理」とその周辺の面白い合同式

県立柏高等学校 西川 誠

1 Wolstenholmeの定理とその拡張の紹介

a を n と互いに素な整数とするとき，$\dfrac{b}{a} \equiv c \pmod{n}$ は，$b \equiv ac \pmod{n}$ が成り立つことで定義します。例えば $2 \times 3 = 6 \equiv 1 \pmod{5}$ なので，$\dfrac{1}{2} \equiv 3 \pmod{5}$ が成立します。もう 1 つ例をあげておくと，$2 \times 13 = 26 \equiv 1 \pmod{5^2}$ なので，$\dfrac{1}{2} \equiv 13 \pmod{5^2}$ です。

「Wolstenholme の定理」というのは，自然数の逆数の和に関する定理で，例えば

$\dfrac{1}{1} + \dfrac{1}{2} + \cdots + \dfrac{1}{6} = \dfrac{49}{20}$ なので，$\dfrac{1}{1} + \dfrac{1}{2} + \cdots + \dfrac{1}{6} \equiv 0 \pmod{7^2}$

となりますが，これを，一般化した次のような定理が,「Wolstenholme の定理」です。

定理①「Wolstenholme の定理」 P を 5 以上の素数とすれば,

$\dfrac{1}{1} + \dfrac{1}{2} + \dfrac{1}{3} + \cdots + \dfrac{1}{P-1} \equiv 0 \pmod{P^2}$ が成り立つ。

2010 年 1 月に北海道の島田一さんという方から,「Wolstenholme の定理」と「Faulhaber の定理」に関するお手紙をいただき，それが発端となっていろいろ実験してみることになりました。今回のレポートでは，その時に発見した「P^3 の定理」とその証明を，紹介したいと思います。また，定理 ① ∼ ④ は，島田一さんが使用されていた記号及び証明の方法を再整理したものですので，ここで感謝申し上げます。また，島田一さんから，プライム · ナンバーズ [?] という本に「Wolstenholme の定理」が紹介されているとのことで，調べてみると，次のような，拡張も書いてありました。

$P > 3$ のとき $\dfrac{1}{1^2} + \dfrac{1}{2^2} + \dfrac{1}{3^2} + \cdots + \dfrac{1}{(P-1)^2} \equiv 0 \pmod{P}$

$P > 5$ のとき $\dfrac{1}{1^3} + \dfrac{1}{2^3} + \dfrac{1}{3^3} + \cdots + \dfrac{1}{(P-1)^3} \equiv 0 \pmod{P^2}$

$P > 7$ のとき $\dfrac{1}{1^4} + \dfrac{1}{2^4} + \dfrac{1}{3^4} + \cdots + \dfrac{1}{(P-1)^4} \equiv 0 \pmod{P}$

実際に実験してみると，次のようになります。

$\dfrac{1}{1^2} + \dfrac{1}{2^2} + \cdots + \dfrac{1}{6^2} = \dfrac{7 \cdot 767}{3600}$　　$\dfrac{1}{1^3} + \dfrac{1}{2^3} + \cdots + \dfrac{1}{6^3} = \dfrac{49 \cdot 583}{24000}$

$\dfrac{1}{1^4} + \dfrac{1}{2^4} + \cdots + \dfrac{1}{6^4} = \dfrac{7 \cdot 2001623}{12960000}$ ←7で割れました。

この本に紹介されていた公式は，4 乗の和までですが，続けて実験してみると · · ·

$$\frac{1}{1^5}+\frac{1}{2^5}+\cdots+\frac{1}{6^5}=\frac{7\cdot 38390867}{259200000},\qquad \frac{1}{1^6}+\frac{1}{2^6}+\cdots+\frac{1}{6^6}=\frac{47464376609}{46656000000}$$
$$\frac{1}{1^7}+\frac{1}{2^7}+\cdots+\frac{1}{6^7}=\frac{343\cdot 19202222389}{933120000000}$$

(注)343 は，7 の 3 乗です。

最後の 7 乗の場合の和が 7 の 3 乗で割れるという現象が面白いので，$P=11$，13，17 などでもやってみると同じようになることが確認できました。$P=11$ のときには，11 乗のときの和が，分子が 11^3 で割れて，13，17 などでも 13 乗とか 17 乗のときが特別で，分子が 13^3 とか 17^3 で割れます。これって有名な公式なのでしょうか？どこかの本で見かけた方がいらっしゃいましたら御教示ください。

プライム・ナンバーズという本について一言 $\cdots$ この本では，

$$P>7\text{ のときに限り，}\quad \frac{1}{1^4}+\frac{1}{2^4}+\frac{1}{3^4}+\cdots+\frac{1}{(P-1)^4}\equiv 0\pmod P$$

が成立すると書いてありますが，実際は $P\geqq 7$ でも成立します。細かい所ですが，結構いいかげんな記述です。さらに，インターネットで検索してみると，この本をそのまま引用したのか「$P>7$ のときに限り」この等式が成り立つという同じ記述がありました。私自身も誤りとか，勘違いはあり得ますので，あまり偉そうなことは言えませんが，インターネットが普及してこういった間違いの連鎖が多くなってきているような気がします。

2 「Newton の恒等式」

これから証明等で使う記号及び公式等をまず準備しておきます。

$$(x-1)(x-2)(x-3)\cdots\{x-(P-1)\}=x^{P-1}-M_1x^{P-2}+M_2x^{P-3}-\cdots-M_{P-2}x+M_{P-1}$$

とおきます。つまり，展開したときの係数を M_j $(1\leqq j\leqq P-1)$ とおいています。ようするに

$$M_1=1+2+3+\cdots+(P-1),\quad M_2=1\cdot 2+1\cdot 3+\cdots+(P-2)(P-1),\cdots$$

一般的に $1,2,3,\cdots,(P-1)$ から異なる j 個を取ってきて積を作り，そういったものをすべて考えて和をとったものが，M_j です。つまり，解と係数の関係 (基本対称式) です。次に

$$N_1=1+2+3+\cdots+(P-1),\qquad N_2=1^2+2^2+3^2+\cdots+(P-1)^2,\cdots$$

一般的に $N_j=1^j+2^j+3^j+\cdots+(P-1)^j$ とおきます。

次に，これをすべて逆数で置き換えたものを，上にバーをつけて表示させることにします。

$$\overline{M}_1=\frac{1}{1}+\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{P-1},\ \overline{M}_2=\frac{1}{1\cdot 2}+\frac{1}{1\cdot 3}+\frac{1}{1\cdot 4}+\cdots+\frac{1}{(P-1)(P-2)}$$

のようになり

$$\overline{N}_1=\frac{1}{1}+\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{P-1},\ \overline{N}_2=\frac{1}{1^2}+\frac{1}{2^2}+\frac{1}{3^2}+\cdots+\frac{1}{(P-1)^2}$$

のようになる訳です。

ここで,「基本対称式」と「べき乗の和」に関する「Newton の恒等式」を紹介します。

$$\alpha^3+\beta^3+\gamma^3-3\alpha\beta\gamma=(\alpha+\beta+\gamma)\left(\alpha^2+\beta^2+\gamma^2-\beta\gamma-\gamma\alpha-\alpha\beta\right)$$

という公式がありますが，これは，$M_1=N_1$ に注意すると，

$$N_3-3M_3=M_1\left(N_2-M_2\right)=M_1N_2-M_2N_1$$

と表示できます。移項して整理すると，$3M_3=M_2N_1-M_1N_2+N_3$ となるのですが，こういった恒等式が「Newton の恒等式」と呼ばれているものです。(証明は，インターネット等ですぐ調べられます。) 最初から書くと

$$\begin{aligned}
&M_1=N_1\\
&2M_2=M_1N_1-N_2\\
&3M_3=M_2N_1-M_1N_2+N_3\\
&4M_4=M_3N_1-M_2N_2+M_1N_3-N_4\\
&5M_5=M_4N_1-M_3N_2+M_2N_3-M_1N_4+N_5
\end{aligned}$$

一般的には，$j\cdot M_j=M_{j-1}N_1-M_{j-2}N_2+\cdots\cdot+(-1)^{j-1}N_j$ となっています。
上にバーが付いた場合も同様に成り立ちます。

$$\overline{M}_1=\overline{N}_1\qquad 2\overline{M}_2=\overline{M}_1\overline{N}_1-\overline{N}_2\qquad 3\overline{M}_3=\overline{M}_2\overline{N}_1-\overline{M}_1\overline{N}_2+\overline{N}_3$$

となる訳です。

3 京都大学の入試問題

1995 年京都大学で次のような入試問題が出題されました。「入試数学 伝説の良問 100」(安田亨)[?] の中では，14 番に当たります。

自然数 n の関数 $f(n)$，$g(n)$ を $f(n)=n$ を 7 で割った余り，$g(n)=3f\left(\displaystyle\sum_{k=1}^{7}k^n\right)$ によって定める。
(1) すべての自然数 n に対して関数 $f\left(n^7\right)=f(n)$ が成り立つことを示せ。
(2) あなたの好きな自然数 n を 1 つ決めて $g(n)$ を求めよ。
その $g(n)$ の値を，この設問におけるあなたの得点とする。

$$\begin{aligned}
&1^1+2^1+3^1+4^1+5^1+6^1+7^1=28,\quad 1^2+2^2+3^2+4^2+5^2+6^2+7^2=140\\
&1^3+2^3+3^3+4^3+5^3+6^3+7^3=784,\quad 1^4+2^4+3^4+4^4+5^4+6^4+7^4=4676\\
&1^5+2^5+3^5+4^5+5^5+6^5+7^5=29008,\quad 1^6+2^6+3^6+4^6+5^6+6^6+7^6=184820
\end{aligned}$$

と計算してみると $g(1)\sim g(5)$ までは，7 で割り切れるので，0 になってしまうのですが，$\cdots\cdot$ $g(6)$ で初めて，$3\times6=18$ となり，やっと 18 点もらえるという，なかなか面白い問題です。普通は，1 から P までの和を取った場合，$(\mathrm{mod}\ P)$ で考えると 0 になってしまい，$(P-1)$ 乗が関係しているときだけは，特別に 0 にならないのです。このレポートでは，割り切れる方に

興味があるので，こちらの方も調べてみると，3 乗の和と 5 乗の和のときは，$784 = 49 \times 16$, $29008 = 49 \times 592$ と 49 でも割り切れます。

ちなみに $1^7+2^7+3^7+4^7+5^7+6^7+7^7 = 1200304 = 49\times 24496$ なので，7 乗の和のときも 49 で割り切れるので，3 以上の奇数の場合だったら，いつでも，49 で割り切れると予想されますが$\cdots$ 実はこれは，成立しません。$1^{13}+2^{13}+3^{13}+4^{13}+5^{13}+6^{13}+7^{13} = 113686341216 = 7\times 16240905888$ という例があり，これは，49 では割りきれません。ということで，べき乗の和を，もう少し詳しく調べてみましょう。

4 「Faulhaber の定理」と合同式

Faulhaber の定理とは，次のような定理です。

Faulhaber の定理

奇数のべき乗の和の場合は，$\left(\sum k \text{ の多項式}\right)$ となり，

偶数のべき乗の和の場合は，$(2n+1) \times \left(\sum k \text{ の多項式}\right)$ となる。

詳しい証明は，数学文化第 12 巻 [?] の拙文「べき乗和の不思議な世界 (高校生にもわかる Faulhaber の定理入門)」を見てください。今は，これを，$(\mathrm{mod}\ P)$ の計算に利用したいのです。

$\sum k = \dfrac{n\,(n+1)}{2}$ と $\sum k^3 = \left(\sum k\right)^2$ は，有名ですが，$\left(\sum k\right)^2$ の方の次数を上げて，$\left(\sum k\right)^m$ の差分を考えると $n^m\{(n+1)^m - (n-1)^m\} = 2m \times n^{2m-1} + (\ ) \times n^{2m-3} + \cdots$ のように奇数次数ばかり出てきます。これから次のような奇数べきの場合の関係式が求まります。

奇数べきの場合の関係式

$$\left(\sum k\right)^2 = \sum k^3$$
$$4\left(\sum k\right)^3 = 3\sum k^5 + \sum k^3$$
$$2\left(\sum k\right)^4 = \sum k^7 + \sum k^5$$
$$16\left(\sum k\right)^5 = 5\sum k^9 + 10\sum k^7 + \sum k^5$$
$$16\left(\sum k\right)^6 = 3\sum k^{11} + 10\sum k^9 + 3\sum k^7$$

一般的には，$2^{m-1}\left(\sum k\right)^m = {}_mC_1\sum k^{2m-1} + {}_mC_3\sum k^{2m-3} + \cdots$ となります。今から考えようとしているものは，素数 P に対して，1，2，$\cdots$，$P-1$ までの和，あるいは，それの何乗かの和です。P が 3 とか 5 で実験してみます。(末項は，P ではなく 1 つ前の $P-1$ の方が楽です。)

① $P=3$ のとき，
$1^1+2^1=3$，$1^2+2^2=5$，$1^3+2^3=9$，$1^4+2^4=17$，$1^5+2^5=33$

ここで，5 乗の和のときは，9 で割れないのは，$4\left(\sum k\right)^3 = 3\sum k^5 + \sum k^3$ の係数の 3 のせいです。

② $P=5$ のとき，
$1^1+2^1+3^1+4^1=10$，$1^2+2^2+3^2+4^2=30$，$1^3+2^3+3^3+4^3=100$，
$1^4+2^4+3^4+4^4=354$，$1^5+2^5+3^5+4^5=1300$，$1^6+2^6+3^6+4^6=4890$，
$1^7+2^7+3^7+4^7=18700$，$1^8+2^8+3^8+4^8=72354$，$1^9+2^9+3^9+4^9=282340$，

ここで，9 乗の和のときは，25 で割れないのは，$16\left(\sum k\right)^5 = 5\sum k^9 + 10\sum k^7 + \sum k^5$ の係数の 5 のせいです。

このように，例外的な場合を排除するために $(\mathrm{mod}\ P)$ とか $(\mathrm{mod}\ P^2)$ の場合は，$N_j = 1^j + 2^j + 3^j + \cdots + (P-1)^j$ において，$1 \leqq j \leqq P-2$ の範囲でしか考えないことにします。奇数べきの場合の関係式は，$2^{m-1}\left(\sum k\right)^m = {}_mC_1\sum k^{2m-1} + {}_mC_3\sum k^{2m-3} + \cdots$ となっていますから，$(\mathrm{mod}\ P)$ の場合に，$1 \leqq 2m-1 \leqq P-2$ なら，係数である ${}_mC_1$ などは，絶対に P を素因数に持つことはありません。これから，$(\mathrm{mod}\ P^2)$ で，$\sum k^3 \equiv 0$ が言えたら，$\sum k^5 \equiv 0$ が言えて，$\cdots$ というように，続けていけます。

偶数べきの場合は，奇数べきの場合を n で微分することができて，次のような関係式が求まります。

偶数数べきの場合の関係式

$$(2n+1)\left(\sum k\right) = 3\sum k^2$$

$$2\,(2n+1)\left(\sum k\right)^2 = 5\sum k^4 + \sum k^2$$

$$4\,(2n+1)\left(\sum k\right)^3 = 7\sum k^6 + 5\sum k^4$$

$$8\,(2n+1)\left(\sum k\right)^4 = 9\sum k^8 + 14\sum k^6 + \sum k^4$$

$$16\,(2n+1)\left(\sum k\right)^5 = 11\sum k^{10} + 30\sum k^8 + 7\sum k^6$$

今 $n = P-1$ で $(2n+1) = 2P-1$ ですから，$(2n+1)$ は，P で割り切れることはないので，普通は，$\sum k^{2m}$ などが P^2 で割り切れることは，期待できません。このことから，奇数の場合も含めて，まとめておくと，次のような補助定理 ① となります。

補助定理 ①

$1 \leqq j \leqq P-2$ ならば，$N_j = 1^j + 2^j + \cdots + (P-1)^j \equiv 0 \pmod{P}$ が成立し，
j が $3 \leqq j \leqq P-2$ の範囲にある奇数ならば，$N_j \equiv 0 \pmod{P^2}$ が成立します。

(参考) ベルヌーイ数の分子には，ときどき大きな素数がでてきます。
例えば，12 番目が $\dfrac{691}{2730}$ なので，次のような面白い例も発見しました。

$$P = 691 \text{ のとき } \sum k^{12} \equiv 61 \times P^2 \pmod{P^3} \quad \sum k^{13} \equiv 51 \times P^3 \pmod{P^4}$$

$\sum$ は，1 から 690 までの和です。(1 から 691 までの和でも同じ)

一般的にべき乗の和は，ベルヌーイ数を使って

$$S_m(n) = \sum_{k=1}^{n} k^m = \frac{1}{m+1} \times \sum_{j=0}^{m} {}_{m+1}C_j \cdot b_j \cdot n^{m+1-j}$$

と表示されるので，P は，3 以上の素数で，$P-2 \geqq m \geqq 3$，(b_m は，ベルヌーイ数です。) とすると，

$$\sum_{k=1}^{p} k^m \equiv \frac{m}{2} \times b_{m-1} \cdot P^2 + b_m \cdot P \pmod{P^3}$$

となっています。次に M_j に関して同様な合同式を作りたいと思います。

補助定理 ②

j が　$1 \leqq j \leqq P-2$ の範囲にあるならば，$M_j \equiv 0 \pmod{P}$ が成立し，
j が　$3 \leqq j \leqq P-2$ の範囲にある奇数ならば，$M_j \equiv 0 \pmod{P^2}$ が成立します。

(証明) 初等整数論で，よく知られた「Fermat の小定理」から，

$$(x-1)(x-2)(x-3)\cdots\{x-(P-1)\} \equiv x^{P-1}-1 \pmod{P}$$

となりますが，

$$(x-1)(x-2)(x-3)\cdots\{x-(P-1)\} = x^{P-1}-M_1x^{P-2}+M_2x^{P-3}-\cdots-M_{P-2}x+M_{P-1}$$

とおいていますから，補助定理 ② の前半は成立することがわかります。また，$M_{P-1} \equiv (P-1)! \equiv -1 \pmod{P}$ というのが「Wilson の定理」です。

補助定理 ② の後半は，補助定理 ① と ② の前半から，

$$3M_3 = M_2N_1 - M_1N_2 + N_3 \equiv 0 \pmod{P^2}$$
$$5M_5 = M_4N_1 - M_3N_2 + M_2N_3 - M_1N_4 + N_5 \equiv 0 \pmod{P^2}$$

のようになり，一般的には，$(P-2)M_j = M_{P-3}N_1 - M_{P-4}N_2 + \cdots + N_{P-2} \equiv 0 \pmod{P^2}$ となることから，わかります。　(証明完了)

次に M_j に関しても同様な合同式を作ります。

補助定理 ③

j が　$1 \leqq j \leqq P-2$ の範囲にあるならば，$\overline{M}_j \equiv 0 \pmod{P}$ が成立し，
j が　$1 \leqq j \leqq P-4$ の範囲にある奇数ならば，$\overline{M}_j \equiv 0 \pmod{P^2}$ が成立します。

(証明) アイデアは，$(P-1)!$ をかけて M_j の話に変換するということだけです。

$$(P-1)!\overline{M}_1 = (P-1)!\left[\frac{1}{1}+\frac{1}{2}+\frac{1}{3}\cdots+\frac{1}{P-1}\right] = M_{P-2} \equiv 0 \pmod{P^2}$$

となり，$M_1 \equiv 0 \pmod{P^2}$ が成立します。後は同様に

$(P-1)!\overline{M}_2 \equiv M_{P-3} \equiv 0 \pmod{P}$ ← $P-3$ は偶数です。
$(P-1)!\overline{M}_3 \equiv M_{P-4} \equiv 0 \pmod{P^2}$ ← $P-4$ は奇数なので，P^2 で割れます。
$(P-1)!\overline{M}_4 \equiv M_{P-5} \equiv 0 \pmod{P}$ ← $P-5$ は偶数です。
　　:
　　:
$(P-1)!\overline{M}_{P-4} \equiv M_3 \equiv 0 \pmod{P^2}$ ← P^2 で割れるのは，ここまでです。
$(P-1)!\overline{M}_{P-3} \equiv M_2 \equiv 0 \pmod{P}$
$(P-1)!\overline{M}_{P-2} \equiv M_1 \equiv 0 \pmod{P}$

となります。　(証明完了)

5 「Wolstenholmeの定理」の証明

定理 ①「Wolstenholme の定理」　P を 5 以上の素数とすれば

$$\frac{1}{1}+\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{P-1}\equiv 0 \pmod{P^2}$$ が成り立つ。

(証明) 補助定理 ③ から，$\overline{N}_1=\overline{M}_1\equiv 0 \pmod{P^2}$ が成立するので，明らかに成立します。
(証明完了)

定理 ②　P を 5 以上の素数とすれば

$$\frac{1}{1^2}+\frac{1}{2^2}+\frac{1}{3^2}+\cdots+\frac{1}{(P-1)^2}\equiv 0 \pmod{P}$$

(証明) 「Newton の恒等式」と補助定理 ③ から，$\overline{N}_2=\overline{M}_1\overline{N}_1-2\overline{M}_2\equiv 0 \pmod{P}$ が成立。
(証明完了)

定理 ③　P を 7 以上の素数とすれば，(これは，$P=3$ でも成立します。5 はだめ)

$$\frac{1}{1^3}+\frac{1}{2^3}+\frac{1}{3^3}+\cdots+\frac{1}{(P-1)^3}\equiv 0 \pmod{P^2}$$

(証明)「Newton の恒等式」と補助定理 ③ などから，
$\overline{N}_3=\overline{M}_1\overline{N}_2-\overline{M}_2\overline{N}_1+3\overline{M}_3\equiv 0 \pmod{P^2}$ となります。　(証明完了)
(参考)$P=3$ でも成立するのは，$\overline{N}_3=\overline{M}_1\overline{N}_2-\overline{M}_2\overline{N}_1+3\overline{M}_3$ の係数 3 があるからです。

定理 ④　P を 7 以上の素数とすれば，

$$\frac{1}{1^4}+\frac{1}{2^4}+\frac{1}{3^4}+\cdots+\frac{1}{(P-1)^4}\equiv 0 \pmod{P}$$

(証明)「Newton の恒等式」と補助定理 ③ などから，$\overline{N}_4=\overline{M}_1\overline{N}_3-\overline{M}_2\overline{N}_2+\overline{M}_3\overline{N}_1-4\overline{M}_4\equiv 0 \pmod{P}$ が成立。　(証明完了)

6 「P^3 の定理」の証明

P^3 の定理（P を 5 以上の素数とすれば,）

$$\frac{1}{1^P}+\frac{1}{2^P}+\frac{1}{3^P}+\cdots+\frac{1}{(P-1)^{P-1}}\equiv 0 \pmod{P^3}$$

(証明の概略) まず $P=5$ のとき簡単に実験してみます。
$\frac{1}{2}\equiv 3 \pmod 5$ を見つけたら，$\frac{1}{2}\equiv 3+y\times 5 \pmod{5^2}$ とでもおいて解くことにより，
$\frac{1}{2}\equiv 3+2\times 5 \pmod{5^2}$ という解が作れます。

さらに続けて $\frac{1}{2} \equiv 3 + 2 \times 5 + 2 \times 5^2 \pmod{5^3}$ となります。他の分数も同様に

$$\frac{1}{3} \equiv 2 + 3 \times 5 + 1 \times 5^2 \pmod{5^3} \qquad \frac{1}{4} \equiv 4 + 3 \times 5 + 3 \times 5^2 \pmod{5^3}$$

となります。この後 $\frac{1}{2^5} \equiv \left(3 + 2 \times 5 + 2 \times 5^2\right)^5 \pmod{5^3}$ のようになる訳ですが，一般的に $\left(x + y \times 5 + z \times 5^2\right)^5 \equiv x^5 + x^4 \cdot y \times 5^2 \pmod{5^3}$[1]これから，$\pmod{5^3}$ で考えるなら最後の z は，不用であることもわかります。以上のことから，

$$\begin{aligned}
&\frac{1}{1^5} + \frac{1}{2^5} + \frac{1}{3^5} + \frac{1}{4^5} \\
&\equiv \left(1^5 + 1^4 \cdot 0 \times 5^2\right) + \left(3^5 + 3^4 \cdot 2 \times 5^2\right) + \left(2^5 + 2^4 \cdot 3 \times 5^2\right) + \left(4^5 + 4^4 \cdot 3 \times 5^2\right) \\
&\equiv \left(1^5 + 2^5 + 3^5 + 4^5\right) + \left(1^4 \cdot 0 + 3^4 \cdot 2 + 2^4 \cdot 3 + 4^4 \cdot 3\right) \times 5^2 \\
&\equiv \left(52 \times 5^2\right) + \left(3^4 \cdot 2 + 2^4 \cdot 3 + 4^4 \cdot 3\right) \times 5^2 \pmod{5^3}
\end{aligned}$$

ここで，$3^4 \equiv 1$，$2^4 \equiv 1$，$4^4 \equiv 1 \pmod 5$ に注意すると，

$$(52) + \left(3^4 \cdot 2 + 2^4 \cdot 3 + 4^4 \cdot 3\right) \equiv 2 + 2 + 3 + 3 \equiv 0 \pmod 5$$

となるので，$\pmod{5^3}$ で

$$\left(52 \times 5^2\right) + \left(3^4 \cdot 2 + 2^4 \cdot 3 + 4^4 \cdot 3\right) \times 5^2 \equiv 0$$

となります。(ここまでが $P = 5$ のときの実験です。)

今，これを 5 以上の素数 P に対して実行できればよい訳です。1 から $P - 1$ までの自然数 k に対して x，y を先ほどやったように設定します。つまり x，y は，k の関数で，次の式を満たすものとします。

$$\frac{1}{k^P} \equiv (x + y \times P)^P \equiv x^P + x^{P-1} \cdot y \times P^2 \pmod{P^3}$$

ここで 1 から $P - 1$ までの和を取る訳ですが，$x^{P-1} \equiv 1 \pmod P$ に注意してまず，$\sum y \equiv \frac{-(P-1)}{2} \pmod P$ となることを示します。

x は，1 から $P - 1$ までをちゃんと 1 回ずつ変化してくれますが，y は，変則的なので困ります。しかし，もともと y は，次の合同式が成り立つように設定したものでした。

$$\frac{1}{k} \equiv x + y \times P \pmod{P^2}$$

ここで，1 から $P-1$ までの和を取れば，左辺は,「Wolstenholme の定理」から 0 になり，$\sum x \equiv \frac{(P-1)\,P}{2}$ なので，$0 \equiv \frac{(P-1)\,P}{2} + \sum y \times P \pmod{P^2}$ となり，全部を P で約すと，$\pmod{P^2}$ の P も 1 つ約せます。

[1]展開して少し計算するとわかります

$$0 \equiv \frac{(P-1)}{2} + \sum y \pmod{P}$$

つまり，$\sum y \equiv \frac{-(P-1)}{2} \pmod{P}$ となりました。

次に $\sum x^P \equiv P^2 \times \frac{(P-1)}{2} \pmod{P^3}$ を示します。$\pmod{P^3}$ で考えて

$$\begin{aligned}
(P-1)^P &\equiv P^2 \times 1^{P-1} - 1^P \\
(P-2)^P &\equiv P^2 \times 2^{P-1} - 2^P \\
&\vdots \\
&\vdots \\
\{P-(P-1)\}^P &\equiv P^2 \times (P-1)^{P-1} - (P-1)^P \text{ で,}
\end{aligned}$$

$x^{P-1} \equiv 1 \pmod{P}$ から $\sum x^{P-1} \equiv (P-1) \pmod{P}$ に注意して，これらを辺ごとに加えると

$$\sum x^P \equiv P^2 \times (P-1) - \sum x^P \pmod{P^3}$$

つまり $\sum x^P \equiv P^2 \times \frac{(P-1)}{2} \pmod{P^3}$ が示せました。 (証明完了)

これで，証明ができていると思いますが，何か間違い等がありましたら，御教示ください。

最後に「Wolstenholme の定理」に関することで，$P = 16843, 2124679$ のとき $\overline{N}_1 \equiv 0 \pmod{P^3}$ となりますが，こういった素数を「Wolstenholme の素数」というのだそうで，今の所この 2 つだけ発見されているようです。

参考文献

[1] David Wells,「プライムナンバーズ」，オライリージャパン，2008 年

[2] 安田亨,「入試数学 伝説の良問 100」，講談社ブルーバックス，2003 年

[3] 日本数学協会,「数学文化第 12 巻」，日本評論社，2009 年