素数に関する考察

5年B組　山名　大二郎
指導教員　川口　慎二

１．要約

サイエンス研究会数学班5年生は素数について学習している。今回は、ウィルソンの定理を素数判定としてより簡単に計算できるよう研究した。また、フェルマーの小定理の別証明を試みたので、その研究過程を記す。

キーワード　　素数、合同式

２．研究の背景と目的

私は、素数の分布に関する公式が見つかっていない数字に興味をもち、素数に関する様々な定理について調べ、考察をしたので、それを本稿にまとめることにする。

３．研究内容

３－１．ウィルソンの定理の応用

定理１（ウィルソンの定理）

p を素数とするとき、次が成り立つ：

$$(p-1)!\equiv -1 \quad (\mathrm{mod}\quad p)$$

（証明）

$p=2$ のとき、

$(2-1)!\equiv -1$ （mod 2)より成立。

以下、$p\geqq 3$ とする。m を $1\leqq m\leqq p-1$ である整数として、

$$m,\ 2m,\ 3m,\ \cdots,\ (p-1)m$$

について考える。これらに含まれる2数 $am,\ bm\quad (a>b)$ において、$am\equiv bm$ $(\mathrm{mod}\quad p)$ と仮定すると、$(a-b)m\equiv 0$ $(\mathrm{mod}\quad p)$ となるが、$1\leqq a-b<p$ であり、かつ p と m は互いに素なので、これは矛盾する。よって、$m,\ 2m,\ 3m,\ \cdots,\ (p-1)m$ を p で割った余りはすべて異なる。したがって、$mn\equiv 1$ となる n が1から $p-1$ の間にただ1つ存在する。

$m=n$ のとき、

$$m^2\equiv 1,\ (m-1)(m+1)\equiv 0 \quad (\mathrm{mod}\quad p)$$

合同式の性質より、$m-1\equiv 0$ または $m+1\equiv 0$ $(\mathrm{mod}\quad p)$.

よって、$m\neq 1,\ p-1$ のとき $m\neq n$ となる。また、$2\leqq m\leqq p-2$ の範囲で $n=1,\ p-1$ のときそれぞれ、$mn=m,\ mp-m$ となり、どちらも p で割った余りが1にならない。よって $2,\ 3,\ \cdots,\ p-2$ の中で積が1になる $m,\ n$ の組が $\dfrac{p-3}{2}$ 個できるので、

$(p-1)!\equiv 1^{\frac{p-3}{2}}\cdot 1\cdot(p-1)\equiv -1$ （mod　p）

となる。 (Q. E. D.)

定理２

整数$m\geqq 2$について、$(m-1)!\equiv -1$

（mod　m）ならば、mは素数である。

（証明）

$(m-1)!\equiv -1$ （mod　m）より、

$$(m-1)!+1=mk \quad \cdots①$$

を満たす整数kが存在する。mが合成数だと仮定すると、$m=nl$　$(n, l\geqq 2)$と表すことができる。①より、$(m-1)!+1=nlk$.

よって、

$$1=nlk-(m-1)!$$

$$=nlk-(m-1)(m-2)\cdots(n+1)n(n-1)\cdots 2\cdot 1$$

$$=n\{lk-(m-1)(m-2)\cdots(n+1)(n-1)\cdots 2\cdot 1\}$$

より、1はmの倍数となり、矛盾する。したがって、mは素数である。 (Q. E. D.)

ウィルソンの定理を素数判定法としてより簡易にさせることができた。以下、pを素数、nを自然数とする。

命題１

$n\neq p, p^2$のとき、$\left\lfloor\frac{n}{2}\right\rfloor!\equiv 0$ （mod　n）

（証明）

条件より、$n=ab$（a, bは自然数で$a>b>1$)と表せる。このとき、

$$\frac{n}{2}\geqq a>b\geqq 2.$$

$a=\frac{n}{2}$，　$b=2$のとき、$\left\lfloor\frac{n}{2}\right\rfloor=a>b>1$.

$\frac{n}{2}>a$，　$b\geq 3$のとき、$\left\lfloor\frac{n}{2}\right\rfloor>\frac{n}{2}-1\geqq a$.

よって、$\left\lfloor\frac{n}{2}\right\rfloor>a>b>1$．したがって、

$$\left\lfloor\frac{n}{2}\right\rfloor!=\left\lfloor\frac{n}{2}\right\rfloor\left(\left\lfloor\frac{n}{2}\right\rfloor-1\right)\cdots a\cdots b\cdots 2\cdot 1\equiv 0$$

（mod　n）

である。 (Q.E.D.)

命題２

$(2p)!\equiv 0$ （mod　p^2）

（証明）

$$(2p)!=2p(2p-1)\cdots p(p-1)\cdots 2\cdot 1$$

$$=p^2\{2(2p-1)\cdots(p+1)(p-1)\cdots 2\cdot 1\}$$
$$\equiv 0 \pmod{p^2}$$

(Q. E. D.)

命題３

$n\neq p$かつ$n>9$のとき、

$$\left\lfloor\frac{n}{2}\right\rfloor!\equiv 0 \text{ （mod　} n\text{）}$$

（証明）

命題１より$n\neq p, p^2$のとき成り立つ。

$p \geqq 3$ のとき、

$$\left\lfloor \frac{p^2}{2} \right\rfloor ! = \frac{p^2-1}{2} \cdot \frac{p^2-3}{2} \cdots (2p+1)2p(2p-1) \cdots (p+1)p(p-1) \cdots 2 \cdot 1$$

となれば p^2 でわりきれる。

$\frac{p^2-1}{2} \geqq 2p$ となる p の範囲は、

$\frac{p^2-1}{2} - 2p \geqq 0$ より、

$$\frac{1}{2}\left(p-2+\sqrt{5}\right)\left(p-2-\sqrt{5}\right) \geqq 0$$

から、$p \geqq 5$ なので、$p > 3$.

したがって、$p^2 > 9$ のとき

$\left\lfloor \frac{p^2}{2} \right\rfloor ! \equiv 0 \pmod{p^2}$ である。 (Q.E.D.)

定理２より、$n \neq 2$ であり、$\left(\frac{n-1}{2}\right)!$ が n で割り切れないとき、n は素数となる。

３－２．フェルマーの小定理の別証明

定理３（フェルマーの小定理）

p を素数とするとき、任意の整数 a について、G.C.D.$(p,a)=1$ ならば、$a^{p-1} \equiv 1 \pmod{p}$ が成り立つ。

（証明）

定理１の証明より、p と a が互いに素なとき、$a, 2a, 3a, \cdots, (p-1)a$ を p で割った余りはすべて異なるので、

$$a \cdot 2a \cdot 3a \cdots (p-1)a \equiv (p-1)! \pmod{p}$$

となる。$(p-1)!$ と p は互いに素なので、両辺を $(p-1)!$ で割って、$a^{p-1} \equiv 1 \pmod{p}$ とわかる。 (Q.E.D.)

１つ目の別証明は、すべての a において $a^{p-1} \equiv 1$ が成り立つことを数学的帰納法で示す。

（定理３の別証明）

$a = bp + c$（b, c は整数で、$1 \leqq c \leqq p-1$）とおく。このとき、

$$(bp+c)^{p-1} \equiv c^{p-1} \pmod{p}.$$

$c = 1$ のとき、$1^{p-1} \equiv 1$ より成り立つ。また、$c = p-1$ のとき、c と p は互いに素のため p は奇数となるので、

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

が成り立つ。以下、$2 \leqq c \leqq p-2$ とする。

$c = 2$ のとき、二項定理より

$$2^{p-1} = (1+1)^{p-1}$$

$$= 1^{p-1} + {}_{p-1}C_1 + \cdots + {}_{p-1}C_{p-2} + 1^{p-1}.$$

いま、

$${}_{p-1}C_m = \frac{(p-1)(p-2)\cdots\{p-(m-1)\}(p-m)}{1 \cdot 2 \cdots (m-1)m}$$

$$\equiv \frac{(-1)\cdot(-2)\cdots\{-(m-1)\}(-m)}{1\cdot 2\cdots(m-1)m}$$

$\equiv(-1)^m \pmod{p}$なので、

$$2^{p-1}\equiv 1^{p-1}-1+1-\cdots+1-1+1^{p-1}\equiv 1.$$

よって、成り立つ。

$c=k$ のとき、$k^{p-1}\equiv 1 \pmod{p}$が成り立つと仮定する。二項定理より、

$$(k+1)^{p-1}=k^{p-1}+{}_{p-1}C_1k^{p-2}+{}_{p-1}C_2k^{p-3}$$
$$+\cdots+{}_{p-1}C_{p-3}k^2+{}_{p-1}C_{p-2}k+1$$

であり、${}_{p-1}C_m\equiv(-1)^m \pmod{p}$より、

$$(k+1)^{p-1}=k^{p-1}-k^{p-2}+k^{p-3}-\cdots+k^2-k+1$$
$$=\left(k^{p-1}+k^{p-3}+\cdots+k^4+k^2\right)$$
$$-\left(k^{p-2}+k^{p-4}+\cdots+k^3+k\right)+1$$
$$=\sum_{i=1}^{\frac{p-1}{2}}k^{2i}-\frac{1}{k}\sum_{i=1}^{\frac{p-1}{2}}k^{2i}+1$$
$$=\frac{k^2(k-1)\left(k^{p-1}-1\right)}{k(k-1)(k+1)}+1.$$

$k\neq 0,1$より

$$(k+1)^{p-1}=\frac{k\left(k^{p-1}-1\right)}{k+1}+1.$$

さらに、$k+1\neq 0$，$k^{p-1}-1\equiv 0$より、

$\frac{k\left(k^{p-1}-1\right)}{k+1}\equiv 0$．ゆえに、$(k+1)^{p-1}\equiv 1 \pmod{p}$.

したがって、数学的帰納法より

$a^{p-1}\equiv 1 \pmod{p}$が示された。(Q.E.D.)

2つ目の別証明の方針は、

$$a^{p-1}-1\equiv(a+1)(a+2)\cdots(a+p-1) \pmod{p}$$

を示すことである。しかし、証明を試みたができなかったため、その途中過程をここでは記すことにする。

<u>命題４</u>

$(a+1)(a+2)\cdots(a+p-1)$の項a^{p-n}の係数は、

$$\sum_{k_{n-1}=1}^{p-n+1}\left(k_{n-1}\sum_{k_{n-2}=k_{n-1}+1}^{p-n+2}\left(k_{n-2}\cdots\sum_{k_2=k_3+1}^{p-2}\left(k_2\sum_{k_1=k_2+1}^{p-1}k_1\right)\cdots\right)\right)$$

と表せる。

（証明）

a^{p-n}の係数は、

$$1\Big(2\big(3\cdots\cdots\big((p-n-3)$$
$$\times\Big[(p-n-2)\big\{(p-n-1)+\cdots+(p-1)\big\}$$
$$+(p-n-1)\big\{(p-n)+\cdots+(p-1)\big\}$$
$$+\cdots+(p-2)(p-1)\Big]$$
$$+(p-n-2)\Big[(p-n-1)\big\{(p-n)+\cdots+(p-1)\big\}$$

$$+(p-2)(p-1)\Big]+\cdots+(p-3)(p-2)(p-1)\Big)$$

$$+\cdots+(n+1)\cdots\cdots(p-1)$$

$$=\sum_{k_{n-1}=1}^{p-n+1}\left(k_{n-1}\sum_{k_{n-2}=k_{n-1}+1}^{p-n+2}\left(k_{n-2}\cdots\sum_{k_2=k_3+1}^{p-2}\left(k_2\sum_{k_1=k_2+1}^{p-1}k_1\right)\cdots\right)\right)$$

となる。 (Q. E. D.)

$(a+1)(a+2)\cdots(a+p-1)$ の定数項を p で割った余りは、ウィルソンの定理(定理１)より、$(p-1)!\equiv -1 \pmod{p}$ なので、－1であることがわかる。

命題５

$(a+1)(a+2)\cdots\cdots(a+p-1)$ の項 a の係数は p で割り切れる。

（証明）

a の係数は

$$\sum_{1\leqq k_1<k_2<\cdots<k_{p-2}\leqq p-1}k_1k_2\cdots k_{p-2}$$

$$=\frac{(p-1)!}{1}+\frac{(p-1)!}{2}+\cdots+\frac{(p-1)!}{p-1}.$$

いま、整数 k が $k\leqq\frac{p-1}{2}$ であるとき、

$$\frac{(p-1)!}{p-k}=\frac{1}{-k}\{1\cdot 2\cdots k\cdots(p-k-1)(-k)$$

$$\times(p-k+1)\cdots(p-1)\}$$

$$\equiv\frac{(p-1)!}{-k} \pmod{p}$$ なので、

$$\frac{(p-1)!}{1}+\frac{(p-1)!}{2}+\cdots+\frac{(p-1)!}{p-1}\equiv 0$$

$\pmod{p}$ となる。 (Q.E.D.)

命題６

$(a+1)(a+2)\cdots(a+p-1)$ の項 a^{p-2} の係数は p で割り切れる。

（証明）

a^{p-2} の係数は、$p>2$ より、

$$\sum_{k=1}^{p-1}k=\frac{1}{2}(p-1)p\equiv 0 \pmod{p}$$

となる。 (Q. E. D.)

命題７

$(a+1)(a+2)\cdots(a+p-1)$ の項 a^{p-3} の係数は p で割り切れる。

（証明）

$p>3$ より、

$$-\sum_{k_2=1}^{p-2}\left(k_2\sum_{k_1=1}^{k_2}k_1\right)$$

$$=-\frac{1}{2^3}(p-2)(p-1)p(p+1)$$

$$+\frac{1}{3}(p-2)(p-1)p$$

$$\equiv 0 \pmod{p}.$$ (Q. E. D.)

命題８

$(a+1)(a+2)\cdots(a+p-1)$ の a^{p-4} の係数は p で割り切れる。

（証明）

$p>4$ より

$$\sum_{k_3=1}^{p-3} k_3 \sum_{k_2=1}^{k_3} k_2 \sum_{k_1=1}^{k_2} k_1$$

$$= \frac{1}{2^4\cdot 3}(p-3)(p-2)\cdots(p+2) - \frac{1}{2\cdot 3}(p-3)(p-2)\cdots(p+1) + \frac{1}{2^2}(p-3)(p-2)\cdots p$$

$\equiv 0 \pmod{p}$. (Q. E. D.)

a^{p-n} の係数を

$$a_{n-1}^{(1)}(p-n+1)(p-n+2)\cdots(p+n-2)$$

$$+a_{n-2}^{(2)}(p-n+1)(p-n+2)\cdots(p+n-3)$$

$$+\cdots+a_1^{(n-1)}(p-n+1)(p-n+2)\cdots p$$

としたとき、$\left\{a_n^{(1)}\right\}$ は $\frac{1}{2}, -\frac{1}{2\cdot 4}, \frac{1}{2\cdot 4\cdot 6}, \cdots$,

$\left\{a_n^{(2)}\right\}$ は $\frac{1}{3}, -\left(\frac{1}{3}+\frac{1}{2}\right)\cdot\frac{1}{5}$,

$\left\{\left(\frac{1}{3}+\frac{1}{2}\right)\cdot\frac{1}{5}+\frac{1}{2\cdot 4}\right\}\frac{1}{7}, \cdots$, $\left\{a_n^{(3)}\right\}$ は

$\frac{1}{4}, -\left(\frac{1}{4}+\frac{1}{3}+\frac{1}{2}\right)\cdot\frac{1}{6}$,

$\left\{\left(\frac{1}{4}+\frac{1}{3}+\frac{1}{2}\right)\cdot\frac{1}{6}+\left(\frac{1}{3}+\frac{1}{2}\right)\cdot\frac{1}{5}+\frac{1}{2\cdot 4}\right\}\cdot\frac{1}{8}, \cdots$

となり、

$$a_{n+1}^{(1)} = -a_n^{(1)}\cdot\frac{1}{2n+2}$$

$$a_{n+1}^{(2)} = -\left(a_n^{(2)}+\frac{1}{2^n n!}\right)\cdot\frac{1}{2n+3}$$

$$a_{n+1}^{(3)} = -\left(a_n^{(3)}+\frac{1}{3\cdot 2^{n-1}(n-1)!}+\frac{1}{2^n\cdot n!}\right)\cdot\frac{1}{2n+4}$$

となることが予想できる。このとき、一般項は

$$a_n^{(1)} = (-1)^{n+1}\cdot\frac{1}{2^n\cdot n!}$$

$$a_n^{(2)} = (-1)^{n+1}\cdot\frac{1}{3\cdot 2^{n-1}(n-1)!}$$

$$a_n^{(3)} = (-1)^{n+1}\cdot\frac{4n+5}{9\cdot 2^{n+1}(n-1)!}$$

となる。証明は、数学的帰納法を使って容易にできる。

４．今後の課題

フェルマーの別証明においては、

$a_n^{(1)}, a_n^{(2)}, a_n^{(3)}$ のすべての一般項の分母に

2^n と $n!$ が含まれているので、それを指針に証明をしていきたい。また、オイラーの定理についても考察をしていきたい。

５．参考文献

[1] 「初等整数パーフェクト・マスター」，鈴木晋一，日本評論社

[2] https://mathtrain.jp/

６．謝辞

今回の研究にあたり、ご指導くださった顧問の川口先生ありがとうございました。また、サイエンス研究会の方々にもご協力いただきました。ありがとうございました。