初等整数論入門から マスターデーモンの解法まで

FoxQ(@foxq_stm)

2019/10/26

自己紹介

FoxQ(@foxq_stm)

①元物理系ポスドクの鬱病患者(療養しながら数学中)

②整数論を軸に数学を基礎から勉強中

③相転移と臨界現象はライフワーク

④ゲーム、音楽(ヨルシカ、ボカロ等)が趣味

⑤ブログでtwitterの数学の問題を解いたり、プログラムを書いたりしている

⑥詳しくは、twitterのプロフィールとツイフィール参照してください

参考文献

はじめての数論（原著第3版）

この講演で証明等省略したところの詳細は、この本に書いてあります。ただし、マスターデーモンの解法は除く。

初等整数論は自然数を調べる学問

$$\mathbb{N} = \{1,2,3,\cdots\}$$

自然数に0は含まないものとする。

基本事項の復習(高校数学)

除算と倍数の定義

自然数a, bについて割り算ができる[1](q, rは0以上の整数)

$$a = qb + r \quad (0 \leq r < b)$$

特に、$r = 0$のとき

$$b|a$$

と書き「bはaを割り切る」または「aはbの倍数、bはaの約数」という。

bがaを割り切らないとき、

$$b \nmid a$$

と書く。

[1]以後、断りがない限り、文字記号は自然数を表すものとする。

最大公約数の定義

自然数a, bを共に割り切る自然数の内最大のものを最大公約数といい、

$$\gcd(a, b)$$

で表す。

特に、$\gcd(a, b) = 1$のとき、aとbは互いに素という。

例:

$$\gcd(13,7) = 1$$

$$\gcd(24,36) = 12$$

ユークリッドの互除法

最大公約数を求めるにはユークリッドの互除法というアルゴリズムを用いる。

例えば、gcd(132,36)を計算するには、

$$132 = 3 \times \boxed{36} + \boxed{24}$$

$$36 = 1 \times \boxed{24} + \boxed{12}$$

$$\boxed{24} = 2 \times \boxed{12} + \mathbf{0}$$

よって、

$$\gcd(132,36) = 12$$

1次方程式と最大公約数

自然数$a, b,$ cに対して、

$$ax + by = c$$

を満たす整数x, yを求める。$g = \gcd(a, b)$とおくと、

$$g \nmid c$$

のとき解なし、

$g|c$のとき、

$$ax + by = g$$

の解は**ユークリッドの互除法**で解(x, y)を見つけられるので

$$a\left(\frac{xc}{g}\right) + b\left(\frac{yc}{g}\right) = g\left(\frac{c}{g}\right) = c$$

とすれば解が見つかる。

素数p

ある自然数$p(\neq 1)$が素数であるとは、
pの正の約数が1とpの2個だけ

素数の整除性定理(補助定理)

素数の特徴①

$$p|ab\text{ならば}p|a\text{または}p|b$$

証明:

$p|$aならば主張は成立する。$p \nmid a$とすると、$\gcd(p,a)=1$となるので、

$$px+ay=1$$

を満たす自然数x,yが存在する。両辺にbをかけると

$$pbx+(ab)y=b$$

左辺は仮定より、pで割れるので

$$p|b$$

素数の整除性定理

素数pが自然数の積$a_1 a_2 \cdots a_r$を割るものとする。このとき、

素数pは因数$a_1, a_2, \cdots, a_r$の内少なくとも１つを割る。

(数学的帰納法より、$a_1(a_2 \cdots a_r)$と分解すれば、証明は明らかなので省く。)

素因数分解と算術の基本定理(1)

算術の基本定理:全ての整数$n \geq 2$は素数の積

$$n = p_1 p_2 \cdots p_r$$

に1通りに分解できる。

主張１:整数nは素数の積に表すことができる。

主張２:そのような分解は(並べ方の違いを除いては)1通りである。

素因数分解と算術の基本定理(2)

主張１:整数nは素数の積に表すことができる

証明:帰納法を使う。$n = 2$のとき、明らかに成立。

$n \leq N$で主張が正しいと仮定する。$N + 1$をチェックする。

(i)$N + 1$が素数の場合→ok

(ii)$N + 1$が合成数の場合、$2 \leq n_1, n_2 \leq N$が存在して、

$$N + 1 = n_1 n_2$$

と表せる。仮定より、n_1, n_2は素数の積に表せるので、$N + 1$も素数の積に表せる。

素因数分解と算術の基本定理(3)

主張２:素因数分解は(並べ方の違いを除いては)1通りである。

証明：主張１より、nが2通りの素数の積で表せたと仮定すると、

$$n = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$$

$p_1 | n$より、$p_1 | q_1 q_2 \cdots q_s$、素数の整除性定理より順序を適当に入れ替えて

$$p_1 | q_1 \Rightarrow p_1 = q_1$$

よって、両辺をp_1で割って、

$$p_2 \cdots p_r = q_2 \cdots q_s$$

この操作をp_iまたはq_iがなくなるまで続ける。もし、左辺が1で右辺が1でないならば矛盾。よって、$r = s$。

$$p_1 = q_1, p_2 = q_2, \cdots, p_r = q_r$$

となり素因数分解の一意性が示された。

マスターデーモンを倒す武器
(初等整数論入門の入門)

4つの武器

①合同式
②フェルマーの小定理
③位数の整除性定理
④オイラーの公式

合同式(1)

aがmを法としてbと合同であるとは、mが$a-b$を割り切る時を言い、

$$a \equiv b \ (mod\ m)$$

と表す。合同でないとき、

$$a \not\equiv b \ (mod\ m)$$

と表す。

例:

$$7 \equiv 2 \ (mod\ 5)$$

$$8 \not\equiv 4 \ (mod\ 6)$$

合同式(2)

$$a_1 \equiv b_1 \,(mod\, m), \qquad a_2 \equiv b_2 \,(mod\, m)$$

が成り立つならば、

$$a_1 \pm a_2 \equiv b_1 \pm b_2 \,(mod\, m)$$

$$a_1 a_2 \equiv b_1 b_2 \,(mod\, m)$$

も成り立つ。また、$\gcd(c, m) = 1$のとき、

$$ac \equiv bc \,(mod\, m) \Rightarrow a \equiv b \,(mod\, m)$$

も成り立つ。

合同式(3)（寄り道）

$3\ (mod\ 4)$の素数定理：4を法として3に合同な素数は無数に存在する。

証明:

4を法として3に合同な素数のリスト

$$3, p_1, p_2, \cdots, p_r$$

が与えられたとする。次の数Aを考える。

$$A = 4p_1p_2 \cdots p_r + 3$$

Aを素因数分解して、新しい素数のリストを得る。

$$A = q_1q_2 \cdots q_s$$

$A \equiv 3\ (mod\ 4)$であるが、もし、$q_1, q_2, \cdots, q_s$が全て4を法として1に合同であるとすると、$A \equiv 1(mod\ 4)$となり、矛盾。よって、新しい素数$q_i \equiv 3(mod\ 4)$が得られる。

フェルマーの小定理(1)

素数pに対して、$a \not\equiv 0 \ (mod\ p)$とする。このとき、

$$a^{p-1} \equiv 1 \ (mod\ p)$$

が成り立つ。

例と応用例:

$$6^{22} \equiv 1 \ (mod\ 23)$$

$$2^{35} = 2^{6 \cdot 5+5} = (2^6)^5 2^5 \equiv 1^5 2^5 \equiv 32 \equiv 4 \ (mod\ 7)$$

フェルマーの小定理(2)

補助定理:法をpとした自然数の列($a \not\equiv 0 \Leftrightarrow p$は$a$を割らない。)

$$a, 2a, 3a, \cdots, (p-1)a \ (mod\ p)$$

を考える。これは順序を除いて

$$1,2, \cdots, , p-1 \ (mod\ p)$$

に一致する。

フェルマーの小定理(3)

補助定理の証明:

$$ja \equiv ka \ (mod\ p)$$

が成り立ったとすると、定義より$p|(j-k)a$、pはaを割らないと仮定しているので、整除性定理より

$$p|(j-k)$$

$1 \leq j,k \leq p-1$より、

$$|j-k| < p-1$$

従って、

$$j-k=0 \Leftrightarrow j=k$$

よって、

$$a, 2a, \cdots, (p-1)a \ (mod\ p)$$

は全て相異なる。よって、$a, 2a, \cdots, (p-1)a \ (mod\ p)$と$1,2, \cdots, , p-1 \ (mod\ p)$は順所を除いて一致する。

フェルマーの小定理(4)

補助定理より、

$$a \cdot (2a) \cdots \big((p-1)a\big) \equiv 1 \cdot 2 \cdots (p-1)\ (mod\ p)$$

$$a^{p-1}(p-1)! \equiv (p-1)!\ (mod\ p)$$

ここで、$\gcd\big((p-1)!, p\big) = 1$より、

$$a^{p-1} \equiv 1\ (mod\ p)$$

が得られた。

位数

定義:

素数pに対して$e \geq 1$で、

$$a^e \equiv 1 \ (mod\ p)$$

となる最小のべき指数を**pを法としたaの位数**という。

例:

$$1^1 \equiv 1 \ (mod\ 7)$$
$$2^3 \equiv 1 \ (mod\ 7)$$
$$3^6 \equiv 1 \ (mod\ 7)$$
$$4^3 \equiv 1 \ (mod\ 7)$$

$e = p - 1$とは限らないことに注意！

位数の整除性定理(1)

$a \not\equiv 0 \ (mod\ p)$とし、

$$a^n \equiv 1 \ (mod\ p)$$

とする。このとき、**pを法としたaの位数e**について

$$e|n(e\text{は}n\text{の約数})$$

が成り立つ。

位数の整除性定理(2)

証明:

nをeで割った商をq、余りをrとすると、

$$n = eq + r\ (0 \leq r < e)$$

$$1 \equiv a^n = a^{eq+r} = (a^e)^q a^r \equiv a^r$$

を得る。ここで、$r \neq 0$とすると、位数eの最小性に反する。よって、$r = 0$。

$$n = eq \Leftrightarrow e|n$$

が言えた。

オイラーの公式(1)

オイラーのφ関数:

$\varphi(m)$=1とmの間で、mと互いに素な自然数の個数

$$= \#\{a: 1 \leq a \leq m, \gcd(a, m) = 1\}$$

オイラーの公式:

$\gcd(a, m) = 1$のとき、

$$a^{\varphi(m)} \equiv 1 \ (mod\ m)$$

が成り立つ。

オイラーの公式(2)

$$1 \leq b_1 < b_2 < \cdots < b_{\varphi(m)} < m$$

を1からmの間にあるmと互いに素な$\varphi(m)$個の数とする。このとき、

補助定理:

$\gcd(a, m) = 1$のとき、数のリスト、

$$b_1 a, b_2 a, \cdots, b_{\varphi(m)} a \ (mod\ m)$$

と数のリスト、

$$b_1, b_2, \cdots, b_{\varphi(m)} \ (mod\ m)$$

は順序を除いて一致する。

オイラーの公式(3)

補助定理の証明:

$$b_j a \equiv b_k a \ (mod\ m)$$

が成り立ったとすると、$m|(b_j - b_k)a$。aとmは互いに素なので

$$m|(b_j - b_k)$$

$1 \leq b_j, b_k \leq m-1$より、

$$|b_j - b_k| \leq m-1$$

絶対値がmより小さくて、mで割れる数は0しかないので、

$$b_j - b_k = 0 \Leftrightarrow b_j = b_k$$

よって、

$$b_1 a, b_2 a, \cdots, b_{\varphi(m)} a \ (mod\ m)$$

は全て相異なる。よって、数のリスト$b_1 a, b_2 a, \cdots, b_{\varphi(m)} a \ (mod\ m)$と数のリスト$b_1, b_2, \cdots, b_{\varphi(m)}$は順所を除いて一致する。

オイラーの公式(4)

補助定理より、

$$(b_1 a)(b_2 a)\cdots\left(b_{\varphi(m)} a\right) \equiv b_1 b_2 \cdots b_{\varphi(m)} \ (mod\ m)$$

$$\left(b_1 b_2 \cdots b_{\varphi(m)}\right) a^{\varphi(m)} \equiv b_1 b_2 \cdots b_{\varphi(m)} \ (mod\ m)$$

ここで、b_jはmと互いに素であったので、

$$a^{\varphi(m)} \equiv 1 \ (mod\ m)$$

が成り立つ。

φ関数の計算

素数pに対して、

$$\varphi(p^k) = p^k - p^{k-1}$$

証明:

1とp^kの間で、pと互いに素でない数、即ち、pの倍数は

$$p, 2p, 3p, \cdots, (p^{k-1} - 1)p, p^k$$

なので、これらの個数はp^{k-1}個である。よって、成り立つ。

また、証明は省くが、$\gcd(m, n) = 1$のとき、

$$\varphi(mn) = \varphi(m)\varphi(n)$$

が言えるので、nの素因数分解が与えられれば、$\varphi(n)$は計算できる。

マスターデーモン

1990年IMO中国大会第3問

2以上の整数nで

$$\frac{2^n+1}{n^2}$$

が整数となるようなものを全て求めよ。言い換えれば、

$$n^2|2^n+1$$

を満たす2以上の自然数を求めよ。

解答の方針

①nを素因数分解して、最小の素因数に着目する。

$$n = p^k N$$

Nは1またはpより大きな素数の積

②pを絞り込む。$(p = 3)$

一旦、2を一般の自然数rに置き換えておくと、後々楽。

$$n^2 | r^n + 1$$

③pの指数kを絞り込む。$(k = 1)$

④$N = 1$を証明する。

結論として、$n = 3$のみが解であることをしめす。

①nの素因数分解

nが偶数だとすると、2^n+1は奇数なので素因数2を持たない。従って、

$$n \nmid 2^n+1$$

となり、nは偶数ではない。つまり、nは奇数の素因数の積のみからなる。

nの最小の奇数の素因数をpとすると、

$$n = p^k N$$

と表せる。

Nは1またはpより大きな素数の積

②pを絞り込む(1)

問題を一般化して、自然数rに対して

$$n^2 | r^n + 1$$

とすると、

nの最小の素因数pは

$r + 1$の素因数のいずれかに一致する

②pを絞り込む(2)

$$n^2|r^n+1 \Leftrightarrow p^2N^2|r^n+1 \Rightarrow p|r^n+1$$

となる。$r \equiv 0\ (mod\ p)$とすると、

$$0^n+1 \equiv 1 \equiv 0\ (mod\ p)$$

となり矛盾。$r \not\equiv 0\ (mod\ p)$なので、フェルマーの小定理より、

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

$$r^p = r \Longrightarrow r^{p^k} = (r^p)^{p^{k-1}} = \cdots = r$$

また、フェルマーの小定理より

$$r^n+1 \equiv 0\ (mod\ p)$$

$$\Leftrightarrow r^{p^kN} \equiv -1\ (mod\ p)$$

$$\Leftrightarrow r^N \equiv -1\ (mod\ p)$$

$$\Rightarrow r^{2N} \equiv 1\ (mod\ p)$$

②pを絞り込む(3)

pを法としたrの位数をeとすると、位数の整除性定理より、

$$e|p-1, e|2N$$

なので、

$$e\text{は}\gcd(p-1,2N)\text{の約数}$$

である。Nは1またはpより大きな素因数の積だったので、

$$\gcd(p-1,2N)=2$$
$$\Rightarrow e=1,2$$
$$\Leftrightarrow r\equiv 1\ (mod\ p)\text{または}r^2\equiv 1\ (mod\ p)$$

ここで、

$$r^2\equiv 1\ (mod\ p)\Leftrightarrow (r-1)(r+1)\equiv 0\ \Leftrightarrow r\equiv 1\text{または}r\equiv -1\ (mod\ p)$$

なので、

$$r\equiv 1\ (mod\ p)\text{または}r\equiv -1\ (mod\ p)$$

②pを絞り込む(4)

$r \equiv 1$のとき、

$$r^n + 1 \equiv 1 + 1 \equiv 2 \equiv 0 \ (mod\ p)$$

より矛盾。よって、

$$r \equiv -1 \ (mod\ p)$$
$$r + 1 \equiv 0 \ (mod\ p)$$

以上より、$r + 1$の素因数分解を

$$r + 1 = p_1 p_2 \cdots p_r$$

とすると、

$$p | p_1 p_2 \cdots p_r$$

より、pは$r + 1$の素因数のいずれかに一致する。

②pを絞り込む(5)

元の問題に戻って、$r = 2$とすると、

$$r + 1 = 3$$

なので、

$$p = 3$$
$$n = 3^k N(k \geq 1)$$

が言えた。

③pの指数kを絞り込む(1)

まず、観察から、

$$2^3+1=9=3\times3$$
$$2^9+1=513=3\times3\times3\times19$$
$$2^{15}+1=3\times\frac{2^3+1}{3}\times\frac{2^{15}+1}{2^3+1}=3\times3\times？$$
$$2^{27}+1=2^{3^3}+1=3\times\frac{2^3+1}{3}\times\frac{2^9+1}{2^3+1}\times\frac{2^{27}+1}{2^9+1}$$
$$=3\times3\times3\times19\times？(=3\times？)$$

$n=3^kN$のとき、2^n+1は素因数3を$k+1$個持ちそうだ。

そして、**3を1つずつ含む適当な因数分解**が存在しそうだ。

③pの指数kを絞り込む(2)

そこで、次の因数分解を考える。

$$2^n+1=(2+1)\left(\frac{2^3+1}{2+1}\right)\left(\frac{2^{3^2}+1}{2^3+1}\right)\cdots\left(\frac{2^{3^k}+1}{2^{3^{k-1}}+1}\right)\left(\frac{2^{3^k N}+1}{2^{3^k}+1}\right)$$

隣り合う分母分子は互いにキャンセルしあっている。簡単のため奇数mと自然数rに対して、自然数$f_m(x)$を

$$f_m(r)=\frac{r^m+1}{r+1}=1-r+r^2-\cdots+r^{m-1}$$

と定義すると、

$$2^n+1=3f_3(2)f_3(2^3)\cdots f_3\left(2^{3^{k-1}}\right)f_N\left(2^{3^k}\right)$$

$f_3(2),f_3(2^3),\cdots f_3\left(2^{3^{k-1}}\right),f_N\left(2^{3^k}\right)$がそれぞれ3で何回割れるか調べる。

③pの指数kを絞り込む(3)

フェルマーの小定理より、自然数$l = 0,1,2,\cdots,k-1$に対して

$$f_3\left(2^{3^l}\right) \equiv f_3(2) \equiv 1 - 2 + 2^2 \equiv 3 \equiv 0\ (mod\ 3)$$

より、$f_3\left(2^{3^l}\right)$は3で少なくとも１回割れる。次に、法を$9 = 3^2$とすると、オイラーの公式より、$\varphi(9) = 3^2 - 3$より

$$2^{3^2-3} \equiv 1 \Longrightarrow 2^{3^2} = 2^3$$

$$2^{3^l} \equiv \left(2^{3^2}\right)^{3^{l-2}} \equiv (2^3)^{3^{l-2}} \equiv 2^{3^{l-1}} \equiv \cdots \equiv 2^3\ (l \geq 2)$$

が成り立つので、$l \geq 1$に対して、

$$f_3(2) \equiv 1 - 2 + 4 \equiv 3 \not\equiv 0\ (mod\ 3^2)$$

$$f_3\left(2^{3^l}\right) \equiv f_3(2^3) \equiv 1 - 2^3 + 2^{2\cdot 3} \equiv 1 - (-1) + (-1)^2 \equiv 3 \not\equiv 0\ (mod\ 3^2)$$

より、$f_3\left(2^{3^l}\right)(l = 0,1,\cdots,k-1)$は$3^2$では割れない。よって、$f_3\left(2^{3^l}\right)(l = 0,1,\cdots,k-1)$は3でちょうど1回だけ割れる。

③pの指数kを絞り込む(3)

同様にして、フェルマーの小定理より、

$$\begin{aligned} f_N\left(2^{3^k}\right) &\equiv f_N(2) \equiv 1-2+2^2-\cdots+2^{N-1} \ (mod\ 3) \\ &\equiv 1-(-1)+(-1)^2-\cdots+(-1)^{N-1} \ (mod\ 3) \\ &\equiv N \ (mod\ 3) \end{aligned}$$

ここで、Nは1または3より大きな素因数の積であったので、

$$f_N\left(2^{3^k}\right) \equiv N \not\equiv 0 (mod\ 3)$$

となり、$f_N\left(2^{3^k}\right)$は、3で割り切れない。

③pの指数kを絞り込む(4)

$$2^n+1=3f_3(2)f_3(2^3)\cdots f_3\left(2^{3^{k-1}}\right)f_N\left(2^{3^k}\right)$$

3でちょうど1回だけ割れる。

3で割れない。

2^n+1は3でちょうど$k+1$回だけ割れる。$n^2|2^n+1$であったので、

$$n^2=3^{2k}N^2$$

より、$n^2|2^n+1$となるためには、指数を比較して

$$2k\leq k+1\Leftrightarrow k\leq 1\Leftrightarrow k=1$$

④$N = 1$を証明する(1)

$$2^n + 1 = 2^{3N} + 1 = 8^N + 1$$

$r = 8$として、題意の式は、

$$9N^2 | r^N + 1 \Rightarrow N^2 | r^N + 1$$

となる。よって、$N = 1$またはNの最小の素因数は

$$r + 1 = 8 + 1 = 9 = 3^2$$

の素因数でなければならない。ところが、Nの素因数は3よりも大きくなければいけないので、Nは3より大きな素因数を持たない。よって、$N = 1$。

以上より、求める解は、

$$n = 3$$

のみであることがわかった。

初等整数論入門

①ピタゴラス数とフェルマーの最終定理
②法pでの平方数
③素数と平方和とガウス素数

ピタゴラス数とフェルマーの最終定理

ピタゴラス数とフェルマーの最終定理(1)

フェルマーの最終定理：

3以上の自然数nについて、

$$x^n + y^n = z^n$$

となる自然数の組は存在しない。(Andrew Wiles, 1995)

$n = 2$では、

$$x^2 + y^2 = z^2$$

を満たす自然数の組は無数に存在する(ピタゴラス数)。

ピタゴラス数(1)

$$x^2 + y^2 = z^2$$

もしピタゴラス数(x, y, z)があれば、ある自然数dをかけることで(dx, dy, dz)もピタゴラス数になる。そこで、3つ組が共通因子を持たない場合、即ち、(x, y, z)がいずれも互いに素な場合を考える(既約ピタゴラス数という)。

①x, yいずれか一方は偶数でもう一方は奇数である。

共に偶数とすると、zも偶数となり共通因子2を持つので矛盾。

共に奇数とすると、法を4として

$$x^2 \equiv y^2 \equiv 1 \ (mod\ 4)$$

このとき、zは偶数なので、

$$x^2 + y^2 \equiv 1 + 1 \equiv 2 \equiv z^2 \equiv 0 \ (mod\ 4)$$

となり矛盾。よって、題意は成り立つ。以後、yを偶数とする。

ピタゴラス数(2)

$$x^2 = z^2 - y^2 = (z - y)(z + y)$$

②$z - y$と$z + y$は共通因数を持たない。

dを$z - y$と$z + y$の共通因数とすると、

$$d|z - y, \quad d|z + y$$
$$(z + y) + (z - y) = 2z, (z + y) - (z - y) = 2y$$
$$\Rightarrow d|2z\ d|2y$$

仮定よりz, yは共通因数を持たないので、dは1または2。ところが、dは奇数$x^2 = (z - y)(z + y)$を割り切るので、$d = 1$。

ピタゴラス数(3)

共通因数を持たない積$(z-y)(z+y)$が平方数になるためには、$z-y, z+y$が共に平方数でなければならない。よって、共通因数を持たない奇数$s > t \geq 1$によって、

$$z+y=s^2, z-y=t^2$$

と表すことができ、これをy, zについて解くと、

$$z=\frac{s^2+t^2}{2}, y=\frac{s^2-t^2}{2}$$

となり、このとき、

$$x=\sqrt{(z-y)(z+y)}=st$$

となる。

ピタゴラス数(4)
(ピタゴラス数を表すもう１つの方法)

$$x = st, y = \frac{s^2 - t^2}{2}, z = \frac{s^2 + t^2}{2}$$

において、$s = u + v, t = u - v$と変数変換すると、

$$x = u^2 - v^2$$
$$y = 2uv$$
$$z = u^2 + v^2$$

という別の表示を得る。ここでは、u, vは奇数、偶数どちらでもよいが互いに素でなければならない。

ピタゴラス数とフェルマーの最終定理(2)

今回は、フェルマーの最終定理で$n = 4$の場合を示す。

$$x^4 + y^4 = z^4$$

(x, y, z)は共通因数を持たないとして一般性を失わない(持てばそれで割ればよい。)。改めて、

$$x^4 + y^4 = z^2$$

と書き直す。

ピタゴラス数とフェルマーの最終定理(3)

$$x^4 + y^4 = z^2$$

からより小さな解

$$X^4 + Y^4 = u^2$$

を得ることができれば、この操作は無限に繰り返すことができる。ところが最初の正の整数から無限に減少していく数のリストを作ることはできないので矛盾。よって、$n = 4$のときのフェルマーの最終定理の解は存在しない。

以下、このことを示す。

ピタゴラス数とフェルマーの最終定理(4)

$$x^4 + y^4 = z^2$$

と置き直す。(x^2, y^2, z)は既約ピタゴラス数なので、

$$x^2 = st, y^2 = \frac{s^2 - t^2}{2}, z = \frac{s^2 + t^2}{2}$$

を満たす奇数s, tが存在する。積stは奇数かつ平方数なので、

$$st \equiv 1 \ (mod\ 4)$$

これを満たすs, tは4を法として共に1に等しいか共に3に等しいかのいずれか。よって、

$$s \equiv t \ (mod\ \ 4)$$

従って、$s - t$は4の倍数。

ピタゴラス数とフェルマーの最終定理(5)

$$y^2 = \frac{s^2 - t^2}{2} \Leftrightarrow 2y^2 = (s-t)(s+t)$$

s, tは互いに素な奇数なので、$s-t, s+t$の共通因数は2。$s-t$は4の倍数なので、$s+t$は奇数の2倍でなければならない。$(s-t)(s+t)$は平方数の2倍なので、互いに素な整数u, vにより、

$$s+t = 2u^2, s-t = 4v^2$$
$$\Leftrightarrow s = u^2 + 2v^2, t = u^2 - 2v^2$$

$x^2 = st$に代入して、

$$x^2 = u^4 - 4v^4 \Leftrightarrow x^2 + 4v^4 = u^4$$

ピタゴラス数とフェルマーの最終定理(6)

$$x^2 + 4v^4 = u^4$$

は既約ピタゴラス数なので、互いに素な奇数S, Tによって、

$$x = ST, 2v^2 = \frac{S^2 - T^2}{2}, u^2 = \frac{S^2 + T^2}{2}$$

と表される。

$$4v^2 = (S - T)(S + T)$$

$S - T, S + T$の最大公約数は2で、それらの積は平方数なので、ある自然数X, Yが存在して、

$$S + T = 2X^2, S - T = 2Y^2$$
$$\Leftrightarrow S = X^2 + Y^2, T = X^2 - Y^2$$

これをuに代入すると、

$$u^2 = \frac{S^2 + T^2}{2} = \frac{(X^2 + Y^2)^2 + (X^2 - Y^2)^2}{2} = X^4 + Y^4$$

ピタゴラス数とフェルマーの最終定理(7)

後は、

$$u^2 = X^4 + Y^4$$

のuがzより小さいことを確認すればよい。

$$z = \frac{s^2 + t^2}{2} = \frac{(u^2 + 2v^2)^2 + (u^2 - 2v^2)^2}{2} = u^4 + 4v^4$$

より、$u < z$は明らか。

よって、$n = 4$のときのフェルマーの最終定理に解は存在しない。

法pでの平方数

法pでの平方数(1)

例：

$$0^2 \equiv 0 \ (mod\ 7)$$
$$1^2 \equiv 1 \ (mod\ 7)$$
$$2^2 \equiv 4 \ (mod\ 7)$$
$$3^2 \equiv 2 \ (mod\ 7)$$
$$4^2 \equiv 2 \ (mod\ 7)$$
$$5^2 \equiv 4 \ (mod\ 7)$$
$$6^2 \equiv 1 \ (mod\ 7)$$

0でない数がpを法として平方数に合同なとき、**pを法とした平方剰余**と呼ぶ。

そうでないとき、その数を**pを法とした平方非剰余**と呼ぶ。

法pでの平方数(2)

$$(p-b)^2 \equiv p^2 - 2pb + b^2 \equiv b^2 \ (mod\ p)$$

より、0でない数の平方を奇素数pを法として全て書き出すには、

$$1^2, 2^2, 3^3, \cdots, \left(\frac{p-1}{2}\right)^2 \ (mod\ p)$$

だけ計算すればよい。また、平方剰余な数と非平方剰余な数は同数$(p-1)/2$個ある。

法pでの平方数の(3)

証明:

$$1^2, 2^2, 3^3, \cdots, \left(\frac{p-1}{2}\right)^2 \ (mod\ p)$$

が全て異なることを示せばよい。$b_1^2 \equiv b_2^2\ (mod\ p)$とすると、
pは$b_1^2 - b_2^2 = (b_1 - b_2)(b_1 + b_2)$を割る

ところが、$2 \leq b_1 + b_2 \leq p - 1$なので$p$で割り切れない。

$|b_1 - b_2| < (p-1)/2$ なので、$b_1 - b_2$がpで割れるためには、$b_1 - b_2 = 0 \Leftrightarrow b_1 = b_2$でなくてはならない。

法pでの平方数(4)

ルジャンドル記号

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & a\text{は}p\text{を法とした平方剰余} \\ -1 & a\text{は}p\text{を法とした非剰余} \end{cases}$$

と定める。このとき、オイラーの基準

$$a^{(p-1)/2} \equiv \left(\frac{a}{p}\right) \ (mod\ p)$$

が成り立つ(証明は今回は省きます)。

法pでの平方数(5)

平方剰余の相互法則(第１法則):

-1はpを法として平方剰余⇔ $p \equiv 1\ (mod\ 4)$のとき

-1はpを法として非剰余⇔ $p \equiv 3\ (mod\ 4)$のとき

証明:

オイラーの基準より

$$(-1)^{(p-1)/2} = \left(\frac{-1}{p}\right)$$

$p = 4k + 1$のとき、$(-1)^{2k} = 1 \equiv \left(\frac{-1}{p}\right)$

$p = 4k + 3$のとき、$(-1)^{2k+1} = -1 \equiv \left(\frac{-1}{p}\right)$

法pでの平方数 (6)

$1(mod\ 4)$の素数定理:4を法として１に合同な素数が無数に存在する。

証明：

4を法として1に合同な素数のリスト$p_1, p_2, \cdots, p_r$が与えられたとする。

$$A = (2p_1p_2 \cdots p_r)^2 + 1$$

を素因数分解して

$$A = q_1q_2 \cdots q_s$$

とする。p_iのいずれもAを割らないので、$q_1, q_2, \cdots, q_s$は元のリストにはない素数。Aは奇数なので、q_iも奇数。$x = 2p_1p_2 \cdots p_r$として、

$$x^2 + 1 = A \equiv 0\ (mod\ q_i) \Leftrightarrow x^2 \equiv -1\ (mod\ q_i)$$

平方剰余の相互法則より、$q_i \equiv 1\ (mod\ 4)$

法pでの平方数(7)

平方剰余の相互法則(第２法則)(証明略)

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & p \equiv 1\text{または}7\ (mod\ 8) \\ -1 & p \equiv 3\text{または}5\ (mod\ 8) \end{cases}$$

また、pと互いに素な自然数a, bに対して

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

が成り立つ。(証明略)特に、$a = q_1 q_2 \cdots q_r$と素因数分解されるならば、

$$\left(\frac{a}{p}\right) = \left(\frac{q_1}{p}\right)\left(\frac{q_2}{p}\right)\cdots\left(\frac{q_r}{p}\right)$$

法pでの平方数 (8)

平方剰余の相互法則:

p, qを相異なる奇素数とするときに、

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$$

が成り立つ。これを用いると、自然数nに対して、p, qの上下を適宜入れ替えることで

$$\left(\frac{q}{p}\right) = \left(\frac{q-np}{p}\right)$$

となるので計算を楽にできる。

素数と平方和とガウス素数

素数と平方和(1)

奇素数pが平方和で表せるなら、$p \equiv 1(mod\ 4)$

証明：

$$p = a^2 + b^2$$

pが奇数なので、aとbは一方が奇数でもう一方が偶数である。

$$a = 2n + 1, b = 2m$$

とおくと、

$$p = a^2 + b^2 = 4n^2 + 4n + 1 + 4m^2 \equiv 1\ (mod\ 4)\square$$

逆に、$p \equiv 1(mod\ 4)$のとき、pは平方和で表せる。(証明略)

素数と平方和とガウス素数(1)

ガウス整数：

a, bを自然数、iを虚数とするとき、

$$a + bi$$

をガウス整数と呼ぶ。

ガウス整数はその表し方に**単数**分の任意性がある。ここで、単数とは

$$1, -1, i, -i$$

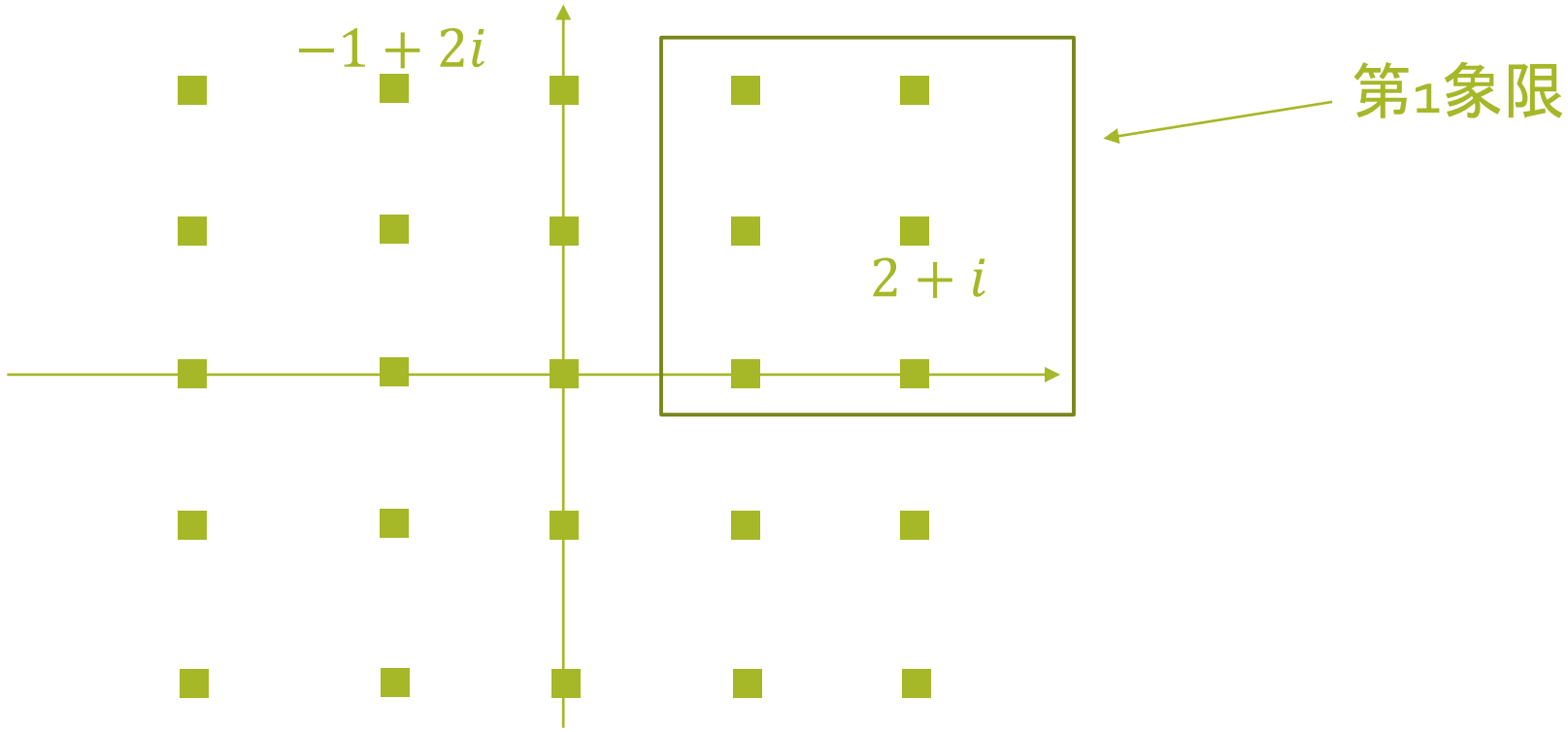
のことである。例えば、

$$a + bi = (-1)(-a - bi)$$
$$a + bi = -i(-b + ai)$$

従って、ガウス整数を素因数分解しようとすると、複素数平面乗で第1象限～第4象限までの素数の取り方があり得る。

素数と平方和とガウス素数(2)

ガウス整数は複素数平面上の格子点からなっている。



素数と平方和とガウス素数(3)

素因数分解の例：

$$2 = (1+i)(1-i)$$
$$5 = (1+2i)(1-2i)$$

ガウス素数は、複素数平面上の第１象限に定めると、

(i)$1+i$

(ii)$p \equiv 3\ (mod\ 4)$の$\mathbb{N}$の素数

(iii)$p \equiv 1\ (mod\ 4)$の$\mathbb{N}$の素数とし、$p = u^2 + v^2$と表した時の$u + vi$

のみである。

また、ガウス整数は単数$(\pm 1, \pm i)$とガウス素数の積で順序の違いを除いて一意的に表せる。

FoxQからの挑戦状１

p, q, rを素数、kを自然数とし次の式を考える。

$$p^2 + \left(2^k q\right)^2 = r^2 \ \ldots\ldots ①$$

（１）$k = 1$のとき、①式を満たすp, q, rを全て求めよ。

（２）$k = 2$のとき、①式を満たすp, q, rを全て求めよ。

（３）$k \geq 3$のとき、①式を満たすp, q, rは存在しないことを示せ。

懸賞問題のルール

①(3)番まで最初に解けた人に、Amazonギフト券3000円分をプレゼント!

②2番目以降は、(2)(3)まで解けた人の中から抽選でAmazonギフト券3000円分(2名)か図書カード500円分(5名)をプレゼント!

③抽選はランダムでつどい2日目閉会式前に小教室で(小教室が空いてない場合大教室で)、(3)を解けた人から優先的に行います。(2)まで解けた人にもチャンスあり!

④**解答はtwitterで、リプで「〇番まで解けたよ」と報告してからDMに送ってください。Twitterをやってない人は直接FoxQまで解答を提出しに来てください。**(2)までの解答は素数のみで結構です。(3)は証明の方針を書いて送ってください。後で、解答をチェックします。

FoxQからの観賞用問題

p, q を素数、 n, k, a, b を自然数とし、次の式を考える。

$$p^a + \left(2^k q\right)^b = n^2 \ \ldots\ldots ①$$

pと$2^k q$が原始ピタゴラス数の小さい2数のとき、①式を満たす

$$(p, q, k, a, b)$$

の組を全て求めよ。

観賞用問題が解けた方への懸賞

①最初に解けた方(先着1名様)にAmazonギフト券3000円分をプレゼント!

②正直そこそこ難しいので、締切は来週の金曜日11月1日までとします。

③解答はリプで送ってもらっても、紙で直接提出していただいてもどちらでもOkです。(p, q, k, a, b)の組を送るだけでも結構です。その場合、後で解答の詳細をざっくりお聞きします。

④関西すうがく徒のつどい終了後に解けた場合、懸賞品の受け渡しは、数学デーin大阪(毎週水曜または金曜に開催)または第6回関西日曜数学友の会(11月2日)にて行います。Twitterでリプして、希望の日時を指定してください。お互いの都合の合う日に会いましょう。

FoxQの予想(未解決、大元になった問題)

A, B(偶数)を原始ピタゴラス数の内、小さい2数とする。このとき、
自然数a, b, nに対して次の式を考える。

$$A^a + B^b = n^2 \ \ldots\ldots ①$$

①式を満たす(a, b)の組は、$(A, B) = (9,40)$の場合を除いて、たかだか2組のみである。ちなみに、

$$9^a + 40^b = n^2$$

は解

$$(a, b) = (1,1), (1,3), (2,1), (2,2)$$

の４つのみである。そこで、より弱く①式が任意の(A, B)に対して、
高々4個の解(a, b)を持つことも言えそうだ。

類似した予想

"The Diophantine equation $x^2 + q^m = p^n$(1993,Nobuhiro Terai)"

原始ピタゴラス数の3つ組の大きい方をC、小さい方の2数の内奇数をAとするとき、

$$A^a + n^2 = C^c$$

となるのは、$(a, c) = (2,2)$に限る。こちらには$(9,40)$のようなマジックナンバーは登場しない。