$a^2 + b^2 = c^2 \quad (x-y)(x+y) = x^2 - y^2 \quad x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a} \quad \sin(A \pm B) = \sin A \cos B \pm \cos A \sin B \quad \ldots b = b \quad d = \frac{|ax_0 + by_0 + c|}{\sqrt{a^2 + b^2}}$

$(ax+by)^2 \leq (a^2+b^2)(x^2+y^2) \quad \lim_{h \to 0} \frac{f(x+h) - f(x)}{h} \quad e = \lim_{n \to \infty} \left(1 + \frac{1}{n}\right)^n \quad \int_a^b f'(x)dx = f(b) - f(a) \quad \frac{X - \mu}{\sigma/\sqrt{n}} \to N(\ldots) = \frac{f(b) - f(a)}{b - a} \quad \frac{x^2}{a^2} + \frac{y^2}{b^2} = 1$

$r = \frac{ep}{1 + e\cos\theta} \quad (\cos\theta + i\sin\theta)^n = \cos(n\theta) + i\sin(n\theta) \quad f(x) = \sum_{n=0}^{\infty} \frac{f^{(n)}(a)}{n!}(x-a)^n \quad \nabla^2 u = 0 \quad e^{ix} = \cos x + i \sin x \quad \nabla^2 f = \frac{\partial^2 f}{\partial x^2} + \frac{\partial^2 f}{\partial y^2} + \ldots f(x)e^{-2\pi i x\xi}dx \quad \sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}$

$y' + p(x)y = q(x) \quad \iint_D f(x,y)dxdy \quad \mathcal{L}\{f(t)\} = \int_0^{\infty} e^{-st} f(t)dt \quad \sum_{n=0}^{\infty} a_n(x-c)^n \quad n! \sim \sqrt{2\pi n}\left(\frac{n}{e}\right)^n \quad \varphi(ab) = \varphi(a)\varphi(b) \quad \nabla \times F = \ldots \iint_S F \cdot dS \quad \oint_C f(z)dz = 0$

$\int_{-\infty}^{\infty} e^{-x^2}dx = \sqrt{\pi} \quad H_n(X) = Z_n(X)/B_n(X) \quad {}_2F_1(a,b;c;z) = \sum_{n=0}^{\infty} \frac{(a)_n(b)_n}{(c)_n}\frac{z^n}{n!} \quad \oint_C \frac{f(z)}{z-a}dz = 2\pi i f(a) \quad H_n(X) = \ker \ldots \frac{1}{n^s} \quad z_{n+1} = z_n^2 + c$

$J_n(x) = \frac{1}{\pi}\int_0^{\pi} \cos(n\theta - x\sin\theta)d\theta \quad \int_0^{\infty} \frac{x^{s-1}}{e^x - 1}dx = \Gamma(s)\zeta(s) \quad T(\varphi) = \int_{-\infty}^{\infty} T(x)\varphi(x)dx \quad \eta(\tau) = e^{\pi i\tau/12}\prod_{n=1}^{\infty}(1 - e^{2\pi i n\tau}) \quad H(x,y) = \frac{1}{2\pi i}\int_L \ldots \geq n\mathrm{vol}(S)^{\frac{n-1}{n}} \ldots(B_1)^{\frac{1}{n}}$

INFINITY

目次

群か群じゃないかクイズ　H3 丸岡亮太

素数の整数問題を解く　H2 加野琢雲

共円ゲーム　M3 小山遼大郎

第 79 回灘校文化祭
数学研究部部誌

May 2-3,2025

公式 HP

数学研究部　2025 年部誌

目次

P2〜P7	群か群じゃないかクイズ	高校三年　丸岡亮太
P8〜P14	素数の整数問題を解く	高校二年　加野琢雲
P15〜P22	共円ゲーム	中学三年　小山遼大郎

まえがき

第 79 回文化祭 weave へようこそ！　そしてこの部誌を手に取っていただきありがとうございます。この部誌の校正・編集を担当しました数学研究部部長の佐藤実と申します。第 79 回灘校文化祭も前年に引き続き無制限での開催となり、数学研究部でも部員が文化祭に向けてますます活動に励んでいます。

この部誌は、日頃数学について勉強、研究している部員が興味の湧いた事柄についてさらに深く学んでみたことが書かれています。その内容は多種多様で、その難易度も様々です。今年も現代数学や競技数学そしてパズルゲームと幅広いトピックを扱っています。きっと読者の皆様にも興味を持ってもらえる記事があるはずです。それらを通して部員の伝えたい数学の面白さや、部員の情熱を感じ取って頂ければ幸いです。

また、今年の文化祭で数学研究部は「部誌の配布」以外にも、「灘中入試模試・和田杯の配布」「数研遊戯の開催」を行っています。灘中入試模試・和田杯は部員が一年間かけて作成した問題が集められています。どれも難しい問題ばかりですが、頭を使って問題を考える楽しさを感じてください。数研遊戯は来場されたお客さんと部員が、「シンプルだけど奥深いゲーム」で対戦するものです。小山君が部誌のテーマとして取り扱っている「共円ゲーム」というものが今年から追加されました。(P15〜参照) 数研ブースに来られた際は一度遊んでみてはいかがでしょうか。

まだまだ書きたいことがあるのですが長文となってしまいましたのでこの辺りで失礼します。それでは部誌をお楽しみくださいませ。

高校三年　佐藤実

群か群じゃないかクイズ

高校３年　丸岡亮太

※この記事は中高生以上の初学者向けに書かれているため、所々数学的に曖昧な表現を含みますが、ご了承ください。また、群を知らない人は 1 章から、群を知っている人は、4 章から読み始めることを推奨します。

1　はじめに

本日は第 79 回灘校文化祭「WEAVE」にお越しいただきありがとうございます。

突然ですが「群」という概念をご存知でしょうか。大学以上の数学をやったことがある人なら知っているかもしれませんが、初めて聞いたという方も多いと思うので、「群」について少し説明します。すでに知っている方は読み飛ばしていただいて構いません。

「群」の具体的な定義は第 3 章に記してありますので、ここでは「群」が一体どのような概念なのかを噛み砕いて説明します。「群」とは現代数学（大学以降の数学）において最も重要な概念の一つです。高校の数学をやったことがあるならば、多くの人は「集合」について知っているはずです。数や物の集まりのことですね。集合は非常に幅広く適応される概念で、「同じクラスの人の集合」や「日本の都道府県の集合」なども存在します。そして、その「集合」に新たなシステムを加えてリフォームしたのが「群」という概念です。

「群」が「集合」と決定的に異なるのは、「（二項）演算」という仕組みが内蔵されていることです。「演算」とは、集合に含まれる 2 つの要素を組み合わせて、別の要素を作るもののことを言います。例えば「$1 + 2 = 3$」における「$+$」が演算に該当します。一般的な集合ではこのような演算は定義されていません。先ほど例に挙げた「日本の都道府県の集合」であれば、「兵庫県＋大阪府」なんていう計算はできませんよね（定義すれば別ですが）。このように「集合」という曖昧で扱いづらい概念に「演算」という道具を与えて扱いやすくしたものが「群」というわけです。

2　用語の説明

群の定義をする前に、基本となる用語や記号の説明をしておきます。もし以降でわからない単語や記号があれば、ここを参照してください。

元 集合の要素のことです。全く同じ意味ですが慣例に従い、元と呼ぶことにします。

空集合 含まれる元がない集合のことです。元が 0 個でも数学的には「集合」です。

$\times$ 皆さんが日常でよく使う、掛け算のことを指します。7 の段は覚えなくていいです。
$+$ 皆さんが日常でよく使う、足し算のことを指します。7 の段は 7 から毎回 7 を足していけばいいだけです。
$\cdot$ 群における演算のことを指します。掛け算のことではないので気をつけましょう。
$\mathbb{N}$ 正の整数全体の集合のことです。0 は含まないことに注意してください。
$\mathbb{Z}$ 整数全体の集合のことです。
$\mathbb{R}$ 実数全体の集合のことです。
$\in$ $x \in G$ で x は集合 G に含まれるという意味になります。
$\{\ a, b\ \}$ a と b の二つの元からなる集合を示します。
$\cup$ $A \cup B$ で A と B の和集合を指します。和集合とは、A と B という二つの集合に含まれる全ての元からなる集合です。

3 群の定義

では、具体的に「群」がどのように定義されるのかを見ていきましょう。

定義. G を空集合ではない集合とする。G 上の演算 $\cdot$ が定義されていて、次の性質を満たすとき、G を群という。

1. すべての $a \in G$ に対して $a \cdot e = e \cdot a = a$ が成り立つような元 e が存在する。（単位元と呼ばれる）
2. すべての $a \in G$ に対して $b \in G$ が存在して $a \cdot b = b \cdot a = e$ となる。この元 b は逆元と呼ばれ、a^{-1} と書く。
3. （結合法則）すべての $a, b, c \in G$ に対して $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ が成り立つ。

一見わかりにくいと思うので、集合 G を整数全体の集合 $\mathbb{Z}$、演算 $\cdot$ を足し算として考えてみましょう。

1. まず、単位元 e に該当する元が無いか考えてみましょう。何を足しても値が変わらない数です。そう。「0」ですね。つまりこの場合は $e = 0$ となり上の (1) を満たします。
2. 次に逆元の存在を確認しましょう。例えば、1 という整数に何を加えたら単位元（ここでは 0）になるでしょうか。そう、「-1」です。他の整数に関してもマイナスをつければ逆元になるので、全ての元に対して逆元が存在し、(2) を満たします。
3. 最後に結合法則です。全ての元に対して、$(a + b) + c = a + (b + c)$ が成り立ちます。よって、(3) を満たします。

大体の雰囲気が掴めたでしょうか？このように群とは集合と演算が与えられていて、上の 3 つの条件を満たす物のことを指します。

4　クイズの説明

ここからが本題です。これまで説明した「群」という概念は数学的に非常に重要な意味を持っています。では、「群かどうかを見分ける力」もまた同様に重要な意味を持つのでは無いでしょうか。ということで私は「群か群じゃないかクイズ」という数学界隈に革新をもたらす新たなクイズを作りました。ルールは以下の通りです。

・最初に集合と演算が与えられる

・回答者はそれをみて制限時間内に群かどうかを判断する。

非常にシンプルですね。制限時間はそれぞれの実力に合った時間を設定することをお勧めします。ある程度数学を知っている人（理系高校生程度）はおそらく 20 秒が適正です。これを数研の講義でやったところ、案外好評だったため、**味を占めて**部誌に載せることになりました。何はともあれ、例題をやってみましょう。

例題 1

集合：整数全体の集合

演算：$a \cdot b = a + b$

これは 3 章で挙げた例と全く同じですね。これは群になります。なので「群」と回答してください。

例題 2

集合：実数全体の集合

演算：$a \cdot b = a \times b$

1. 単位元は 1 です。
2. 0 をかけて 1 にはなる数は存在しません。つまり、0 の逆元が存在しないため、これは群になりません。ですので、「群じゃない」と回答してください。

このような感じで扱う集合と演算が与えられて、それらが群になるかを判断するのが「群か群じゃないかクイズ」です。なんとなくわかったでしょうか。では、早速問題を解いていきましょう！全部で 5 問あります。

5　群か群じゃないかクイズ

問題 1. 集合：正の有理数全体の集合　　演算：$a \cdot b = a \times b$

問題 2. 集合：正の実数全体の集合　　演算：$a \cdot b = \dfrac{a \times b}{a + b}$

問題 3. 集合：$\{a, b\}$　　演算：$a \cdot a = b \cdot b = a \quad a \cdot b = b \cdot a = b$

問題 4. 集合：$\mathbb{R} \cup \{\infty\}$（$\infty$ と実数全体からなる集合）　　演算：$a \cdot b = a \times b$

∞ は掛け算について以下の性質を満たすように定義します。（a は 0 以外の全ての実数）

$$\infty \times 0 = 0 \times \infty = 1 \quad \infty \times a = a \times \infty = \infty$$

問題 5. 集合：1 と無理数全体からなる集合　　演算：$a \cdot b = a \times b$

群の定義（再掲）
G を空集合ではない集合とする。G 上の演算 $\cdot$ が定義されていて、次の性質を満たすとき、G を群という。

1. すべての $a \in G$ に対して $a \cdot e = e \cdot a = a$ が成り立つような元 e が存在する。
2. すべての $a \in G$ に対して $b \in G$ が存在して $a \cdot b = b \cdot a = e$ となる。
3. すべての $a, b, c \in G$ に対して $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ が成り立つ。

6　解説

さて、解いてみた手応えはどうでしょうか。出来がどうであれ、この一連の流れを通して、群の 3 つの条件についての理解が深まったのでは無いでしょうか。正直にいうと、このクイズは、答えが合っているかどうかは重要ではなく、群かどうかを検証するプロセスが重要なのです。ですので、すでにこの記事は役目を果たしています。しかし、多くの人は答えが知りたいと思いますので、その場合は以下の解答をご覧ください。

解説 1. 集合：有理数全体の集合　　演算：$a \cdot b = a \times b$

群の定義を順番に確認しましょう。まず、1 をどんな数にかけても値は変わらないため、1 が単位元です。また、正の有理数に対して、その逆数も正の有理数になります。この場合逆数は逆元になるので逆元も存在します。最後に、結合法則は明らかに満たします。よって、答えは「群」です。

解説 2. 集合：正の実数全体の集合　　演算：$a \cdot b = \dfrac{a \times b}{a + b}$

一見演算が複雑で面倒そうですが、やることは同じです。単位元 e が存在すると仮定すると、$\dfrac{a \times e}{a + e} = a$ となります。両辺を $a + e$ 倍すると、$a \times e = a \times (a + e)$ になります。よって、$a \times a = 0$ となります。しかし $a > 0$ のため矛盾します。よって単位元は存在しません。答えは「群じゃない」です。

解説 3. 集合：$\{a, b\}$　　演算：$a \cdot a = b \cdot b = a \quad a \cdot b = b \cdot a = b$

この問題で扱う集合には要素が 2 つしかありません。そして、演算は考えられる 4 つのパターンに対して個別に定義してあります。ですが、考えることは同じです。まず、a が単位元に該当します。そして、a の逆元は a、b の逆元は b です。そして、結合法則ですが、これは検証が面倒なように思われます。しかし演算をよくみると、各辺において b の項の個数の偶奇が保存されていることがわかります。つまり、計算は全て b の個数の偶奇によって定まるため、どのような順序で計算しても同じになります。よって答えは「群」です。

解説 4. 集合：$\mathbb{R} \cup \{\infty\}$（$\infty$ と実数全体からなる集合）　　演算：$a \cdot b = a \times b$

∞ は掛け算について以下の性質を満たすように定義します。（a は 0 以外の全ての実数）

$$\infty \times 0 = 0 \times \infty = 1 \quad \infty \times a = a \times \infty = \infty$$

∞ という特殊な記号が用いられていますが、やはりやることは同じです。まず、単位元は 1 なので存在します。また、0 と ∞ 以外は、逆元は逆数を取れば良いので存在します。そして 0 の逆元は ∞、∞ の逆元は 0 なのですべての元に対して逆元が存在します。最後に、結合法則ですが、「掛け算だしどうせ成り立つでしょ」と思って軽く検証していると痛い目に遭います。例えば、

$$2 \times (0 \times \infty) = 2 \times 1 = 2$$
$$(2 \times 0) \times \infty = 0 \times \infty = 1$$

つまり、$2 \times (0 \times \infty) \neq (2 \times 0) \times \infty$ となり結合法則は成り立っていないことがわかりま

す。よって答えは「群じゃない」です。

解説 5. 集合：1 と無理数全体の集合　　演算：$a \cdot b = a \times b$

これも同様に確認していきましょう。まず、明らかに単位元は 1 です。また、無理数の逆数を取るとその値もまた無理数なので逆元が存在します。そして、先ほどの問題と違い、0 や ∞ のような特殊な元は存在せず、どの元に対しても普通の掛け算なので結合法則が成り立ちます。よって答えは「群」です。
と、考えた人が多かったのでは無いでしょうか。答えは「群じゃない」です。3 つの条件を満たしているのにおかしいと思うかもしれませんが、実はこの問題には巧妙な罠が仕組まれています。第 1 章でも述べたとおり、演算とは、集合の要素 2 つから新たに要素を取り出すものです。また、群の定義では「G 上の演算 $\cdot$」と述べられています。しかし、この問題の場合、$\sqrt{2} \times \sqrt{2} = 2$ であり、2 は扱っている集合には含まれません。つまり、そもそも、これらは演算の条件を満たしていないのです。

7　終わりに

いかかでしたか？前にも述べましたが、「群か群じゃないかクイズ」は、元々は数研の講義で実際に実施したもので、案外評判が良かったので今回の部誌にも載せる運びとなりました。初学者の方にはなかなか難しく感じられたかもしれませんが、なんとなく群に関するイメージを掴めたのではないかと思います。これを通して現代数学により興味を持っていただければ幸いです。ここまで読んでいただき、ありがとうございました。

8　参考文献

代数学 1　群論入門　雪江明彦　2010 年 11 月 25 日　日本評論社

素数の整数問題を解く

高校 2 年　加野琢雲

1　はじめに

こんにちは、79 回生の加野琢雲と申します。早いものでもう高校二年生になるそうです。普段は競技数学と競技プログラミングをしています。

ここで少し、競技数学について説明させてください。競技数学は、競技として数学の問題を解くものです。主に高校数学の範囲の幅広い問題を扱い、数学オリンピックや Online Math Contest(OMC) などのコンテストが開催されています。

さて、今回は競技数学の整数問題、そのなかでも素数に焦点を当てたものをテーマとして、それらを解くための手法を紹介します。

第 2 章では因数分解、第 3 章では mod を紹介します。素因数を取る、位数を考えるなど手法は他にもあるのですが、今回は大学入試や比較的低難度の競技数学の整数問題でよく出る 2 つに絞っての紹介です。お楽しみください。

2　因数分解

まず紹介する手法は、因数分解です。素数は約数が非常に限られているため、因数分解をして (整数) $\times$ (整数) $=$ (素数の積) の形にすることでうまくいくことが多いです。

ここからは、問題を解きながらの紹介になります。

例題 1. 素数 p であって、$p+1$ が平方数となるものを全て求めよ。(OMCB012-A)

整数 n を用いて $p+1=n^2$ と置くと、 $(n+1)(n-1)=p$ と変形できます。ここで、素数 p の正の約数は $1, p$ のみですから、$(n+1, n-1)=(p,1)$ がわかります。 $n-1=1$ より、$p=n+1=\mathbf{3}$ が答えです。

因数分解するとそれぞれの因数についての情報が得られてうれしいです。

さて、次の問題です。

例題 2. 素数の組 (p,q) であって、p^3+q^2 が平方数となるものを全て求めよ。(自作)

先ほどと似たような因数分解ができます。$p^3+q^2=n^2$ と置くと、$(n+q)(n-q)=p^3$ と変形できます。

p^3 の正の約数は $1,p,p^2,p^3$ の 4 つなので、$(n+q,n-q)=(p^3,1),(p^2,p),(p,p^2),(1,p^3)$ のいずれかです。ここで $n+q>n-q$ なので、$(p,p^2),(1,p^3)$ は不適です。したがって、残りの 2 つを考えます。

$(n+q,n-q)=(p^3,1)$ のとき、$2q=p^3-1=(p-1)(p^2+p+1)$ となります。$p^2+p+1>2$ なので、$(p-1,p^2+p+1)=(2,q),(1,2q)$ のいずれかです。$p=3,2$ を調べると、$(p,q)=(3,13)$ が適します。

$(n+q,n-q)=(p^2,p)$ のとき、$2q=p^2-p=p(p-1)$ となります。$p>p-1$ に注意すると、$(p,p-1)=(2q,1),(q,2)$ のいずれかであり、$q=1,3$ となります。このうち、$(p,q)=(3,3)$ が適します。

以上より、求める組 (p,q) は $(\mathbf{3},\mathbf{13}),(\mathbf{3},\mathbf{3})$ です。

今回は、因数分解をした後にも一工夫が必要でした。このような問題は多く、因数分解から得た情報をどう活用するか考えるのが大事です。

例題 3. 素数の組 (p,q,r) であって、$p^3-q^3=r+12pq+64$ を満たすものを全て求めよ。(OMC242-B)

因数分解に目を凝らすと、$a^3+b^3+c^3-3abc$ の形が見えてきます。$r=p^3-q^3-64-12pq=(p-q-4)(p^2+q^2+pq+4p-4q+16)$ で、ここで $p>q$ より $p^2+q^2+pq+4p-4q+16>0$ 、したがって $p-q-4=1$ です。さらに、偶奇を考えると $q=2$ が分かり、最終的には $(p,q)=(\mathbf{7},\mathbf{2})$ と求められます。

因数分解するときに注意すべきなのは、両辺ともに積の形にするということです。今回の問題では、$(p-q)(p^2+pq+q^2)=r+12pq+64$ と変形することもできますが、右辺が因数分解できていないため良い情報を得ることができません。うまい変形を考えましょう。

例題 4. 素数の組 (p,q,r) であって、$15p+7pq+qr=pqr$ を満たすものを全て求めよ。(OMCB021-D)

p が含まれている項をまとめると $qr = p(qr - 7q - 15)$ となります。したがって、$p = q$ または $p = r$ となります。

$p = q$ のとき、$r = qr - 7q - 15$ となり、変形すると $(q-1)(r-7) = 22$ となります。この式を満たす (q, r) は $(2, 29)$ のみです。

$p = r$ のとき、$q = qr - 7q - 15$ となり、変形すると $q(r-8) = 15$ となります。この式を満たす (q, r) は $(5, 11)$ および $(3, 13)$ です。

以上より、求める組 (p, q, r) は $(\mathbf{2}, \mathbf{2}, \mathbf{29}), (\mathbf{11}, \mathbf{5}, \mathbf{11}), (\mathbf{13}, \mathbf{3}, \mathbf{13})$ です。

$pq + ap + bq + c = 0$ みたいな式を $(p+b)(q+a) = ab - c$ に変形して解くことは（素数に限らず）よくあります。定数はいくらでもまとめられることは意識しておきましょう。

次がこの章で紹介する最後の問題です。

例題 5. 素数の組 (p, q) であって、$p^5 + p^3 + 2 = q^2 - q$ を満たすものを全て求めよ。(AMO2014)

まずは因数分解、今回は $p^3(p^2+1) = (q+1)(q-2)$ と変形できます。

ここで、$q+1$ と $q-2$ の最大公約数は 1 または 3 です。

$p = 3$ のとき、$(q+1)(q-2) = 270$ となり、この式を満たす q は $q = 17$ です。

一方、$p \neq 3$ のとき、$q+1$ または $q-2$ のいずれかが p^3 で割り切れることになります。したがって、不等式 $q \geq p^3 - 1, \quad q \leq p^2 + 3$ が成り立ちます。これを満たすには $p = 2$ が必要であり、このとき $q = 7$ となります。

以上より、求める組 (p, q) は $(\mathbf{3}, \mathbf{17}), (\mathbf{2}, \mathbf{7})$ です。

この問題では、因数分解した後、因数の素因数について考え、不等式評価を行いました。最大公約数を考慮して素因数を調べる手法はよく見かけるので覚えておきましょう。

3 mod

この章では、 mod を使う解き方を紹介します。mod とは余りのことで、mod2 は 2 で割った余りを表します。素数の問題で mod が使える背景には、素数が絡むと余りとしてあり得る値が少なくなることが多い、というのがあります。

特によく登場する mod2, 3, 5 を各節に分けて紹介します。

3.1　mod 2（偶奇）

偶奇は必ず見ましょう。偶奇で一発という問題は少ないですが、初手で偶奇を見ることは多いです。

例題 6. $p \geq q \geq r$ なる素数の組 (p, q, r) であって、$p + q + r + 89 = pqr$ を満たすものを全て求めよ。(自作・OMC191-D の部分問題)

この問題は mod2 だけで終わります。

p, q, r が全て奇数であるとき、左辺は偶数、右辺は奇数となり、矛盾します。よって $r = 2$ がわかります。$p + q + 91 = 2pq$ となりますが、ここで p, q がいずれも奇数であるとき、左辺は奇数、右辺は偶数となり、矛盾します。よって $q = 2$ がわかります。

以上より、求める組 (p, q, r) は $(\mathbf{31}, \mathbf{2}, \mathbf{2})$ です。

例題 7. 素数の組 (p, q) であって、$p^3 + 3q^3 - 32$ が素数であるものを全て求めよ。(JJMO2022 本選 1)

まず、$p^3 + 3q^3 - 32 = 2$ となるような p, q は存在しません。したがって、$p^3 + 3q^3 - 32$ は奇数であることがわかります。

次に、p, q がいずれも奇数であるとき、$p^3 + 3q^3 - 32$ は偶数となり、矛盾します。よって、p または q のいずれかは 2 でなければなりません。

$p = 2$ のとき、$3q^3 - 24 = 3(q^3 - 8)$ は素数となり得ないため不適です。

次に、$q = 2$ のとき、$p^3 - 8 = (p - 2)(p^2 + 2p + 4)$ となります。これが素数となるためには $p^2 + 2p + 4 > 1$ である必要があり、したがって $p - 2 = 1$ でなければなりません。このとき、$(p, q) = (3, 2)$ となり、成立します。

以上より、求める組 (p, q) は $(\mathbf{3}, \mathbf{2})$ です。

このように、偶奇を見た後に、因数分解などのほかの手法を使うことも多いです。

3.2　mod 3

3 で割った余りを考えることも多いです。大学入試では、京大がよく出しています。

早速、京大の問題から見ていきましょう。

例題 8. 素数の組 (p, q) であって、$p^q + q^p$ が素数であるものを全て求めよ。(京大 2016 理系)

まず、偶奇を見ます。$p^q+q^p>2$ より、p^q+q^p は奇数です。p,q がいずれも奇数であると仮定すると、p^q+q^p は偶数となり、矛盾します。よって、p,q のいずれかは 2 です。

$q=2$ とすると、p^2+2^p となります。ここで、3 で割った余りを見ると、$p^2 \mod 3$ は $p=3$ のとき 0、それ以外のとき 1 となり、$2^p \mod 3$ は $p=2$ のとき 1、それ以外のとき 2 であることが分かります。よって、p が 2 でも 3 でもないときは、p^2+2^p が 3 で割り切れます。$p^2+2^p>3$ なので、素数ではなく不適です。

よって、$p=2$ または $p=3$ の場合のみ調べると、$(p,q)=(3,2)$ を得ます。$p=2$ のときも同様に、$(p,q)=(2,3)$ です。

以上より、求める組 (p,q) は $(\mathbf{3},\mathbf{2}),(\mathbf{2},\mathbf{3})$ です。

累乗が絡むと mod が刺さりやすいです。特に、mod 3 は平方数に強いです。

例題 9. 素数の組 (p,q,r) であって、$p-q-8, q-r-8$ がいずれも素数であるものを全て求めよ。(一橋大 2014)

まず、偶奇で絞ります。$p>q>r$ がわかるので、p,q は奇数です。したがって、$p-q-8$ は偶数であるため、2 であるとわかります。これにより、$p-q=10$ を得ます。

次に、$q-r-8=s$ と置きます。偶奇を見ると、r,s のいずれかは偶数です。

$r=2$ のとき、$q-s=10$ です。ここで mod3 を見ます。p,q,s を 3 で割った余りは全て異なりますから、いずれか 1 つは 3 です。$p>q>s$ より、$s=3$ です。このとき $p=23, q=13$ で適します。

$s=2$ のとき、$q-r=10$ です。$r=2$ のときと同様に $(p,q,r)=(23,13,3)$ が適することがわかります。

以上より、求める組 (p,q,r) は $(\mathbf{23},\mathbf{13},\mathbf{3}),(\mathbf{23},\mathbf{13},\mathbf{2})$ です。

余りが異なることを利用して絞ることもあります。

3.3 mod 5

mod2 や mod3 に比べると頻度は落ちますが、ときどき使います。

例題 10. $p, 2p+1, 4p-1, 6p-1, 8p+1$ がいずれも素数であるような p を全て求めよ。(一橋大 2015)

5 つも数があれば、一つくらいは 5 で割り切れるのではないかと考えます。その通りです。確かめましょう。

p を 5 で割った余りが次のようになります。

- $p \equiv 0 \pmod 5$ のとき、p が割り切れる。
- $p \equiv 1 \pmod 5$ のとき、$6p-1$ が割り切れる。
- $p \equiv 2 \pmod 5$ のとき、$2p+1$ が割り切れる。
- $p \equiv 3 \pmod 5$ のとき、$8p+1$ が割り切れる。
- $p \equiv 4 \pmod 5$ のとき、$4p-1$ が割り切れる。

5 で割り切れる素数は 5 しか存在しないため、それぞれが 5 となるときを調べると $p = \mathbf{2}, \mathbf{5}$ で成立します。

例題 9 と同じ考え方を mod5 でする、という問題でした。

次で最後の問題です。

例題 11. 素数の組 (p,q,r) であって、$3p+q=r^4$ を満たすものを全て求めよ。(自作・OMC108-C)

まずは偶奇を考えます。p,q,r のいずれかは 2 です。

$p=2$ のとき、$6+q=r^4$ となります。ここで、mod5 の出番です。$r \neq 5$ のとき、r^4 を 5 で割った余りは常に 1 となります。q を 5 で割った余りが 0 となるため、$q=5$ ですが、不適です。$r=5$ のとき、$q=619$ で適しています。

次に、$q=2$ のとき、$3p+2=r^4$ となりますが、$r^4 \mod 3$ は 0 か 1 しかあり得ず、不適です。

$r=2$ のとき、$3p+q=16$ となり、調べると、$(p,q)=(3,7)$ が適します。

以上より、求める組 (p,q,r) は $(\mathbf{2},\mathbf{619},\mathbf{5}),(\mathbf{3},\mathbf{7},\mathbf{2})$ です。

4　おわりに

以上で手法の紹介は終わりです。いかがだったでしょうか。素数の整数問題の面白さを感じていただけたなら嬉しいです。最後に演習問題をつけているので、ぜひ解いてみてください。答えは読者への課題とします。

4.1　余談

例題のいくつかの問題は、「はじめに」で紹介した Online Math Contest (OMC) から取ってきています。その中でも、例題 6 と例題 11 は私が作った問題です。

OMC には問題作成機能があり、一定の条件（rating が 1400 以上）を満たしたユーザーは、自作の問題を提出することができ、提出された問題は運営の審査を通過すれ

ばコンテストに出題されます。

自分の作った問題をみんなに解いてもらいたい！という方は、ぜひ OMC を始めてみてください。コンテストに参加する数百人に解いてもらうチャンスです。

4.2 演習問題

問題 1. 素数の組 (p, q) であって、 $p^2 - 1 = 24q$ を満たすものを全て求めよ。(奈良女子大 2021)

問題 2. 素数の組 (p, q) であって、 $pq + r^4 = s^4$ を満たすものを全て求めよ。(OMCB005-D)

問題 3. 正整数 m, n と 3 以上の素数 p, q が $pm^2 + 1024q^n = q^{3n}$ を満たしている。p としてあり得るものを全て求めよ。(OMC223-D)

問題 4. 素数の組 (p, q, r) であって、$p^{6p} + q^p + r^p = (q + r)^p + 54$ を満たすものを全て求めよ。(OMCB009-D)

問題 5. 素数の組 (p, q, r, s) であって、$p^3q + r^2 = s^2$ を満たすものを全て求めよ。(OMC141-F)

共円ゲーム

中学3年　小山遼大郎

1　共円とは？

「いくつかの点が共円」とはそれらの点全てが同一円周上にある点の関係のことを指し、主に同一平面上にある相異なる 4 点以上の点に対して使います。考える点が 3 つ以下の場合、それらを全て通る様な円は必ず 1 つ以上存在するためです。[1)] 初等幾何の分野ではよく共円を用いて問題を解いたり作ったりします。では共円はどのようなときに成り立つのでしょうか。

4 つの点 (A, B, C, D とする) がこの順に共円であることと、次のことは同値です；

直線 AD に関して B, C が同じ側にある場合 $\angle ABD = \angle ACD$

直線 AD に関して B, C が反対側にある場合 $\angle ABC + \angle CDA = \angle 180°$

また、$AB \cdot CD + BC \cdot DA = AC \cdot BD$ を満たすとき、$AO = BO = CO = DO$ を満たすような点 O が存在するときや、直線 AB, CD の交点 P が $AP \cdot BP = CP \cdot DP$ を満たすときにも 4 点 A, B, C, D は共円となります。（ただし、点 A, B, C, D, P, O はどれも無限遠点ではありません。)

2　共円ゲームとは？

共円ゲーム[2)] とは以下のルールに則って 2 人以上で行うゲームです。

- 置かれている碁石のうちどの 4 点も「共円」になってはいけないという制約のもと碁石を置いていく（*1 同様、4 つ以上の点が同一直線上にあるのは半径無限大の円周上にあるという解釈をするので、共円であるとみなします)。
- 共円を作ってしまった場合、他人にそれを指摘されると負け。
- 指摘されなければセーフ。

通常は (整数)×(整数)、1 マス 1×1 のマス目を用いますが、正三角形型の格子や縦横比 $1 : \sqrt{3}$ の格子を用いたり、いろいろアレンジを加えることができます。

この先は、共円ゲームやそのアレンジについていろいろ書いていきます。共円ゲー

1）　3 つの点が同一直線上にあるとき、それらを全て通る円は半径無限大の円とみなす。

2）　春合宿という、数学オリンピックの代表選抜の役割を担う合宿で遊ばれていたらしい。正式名称は不明ですが、ここでは共円ゲームと呼称します。

ムの戦略はまだ経験不足のためよくわからないので、共円の見つけ方を中心に述べていこうと思います。

3　共円の種類 (通常マス)

共円ゲームをやるにあたって、どのような共円があるのかを知るのは最も大事なことです。「当たり前でしょ！」と思うような共円もあれば「いやいや気づかんわ」と思わず言いたくなるものもあります。経験上、当たり前といえる共円こそ案外見つかりません。（特に同一直線上に 4 つの点を並べそうになってしまう）

3.1　自明な共円

(1.a) 長方形

対角線の交点と各頂点の距離が等しいので、その交点が円の中心となります。

(1.b) 等脚台形

向かい合う頂点の和が 180° となるので、共円です。

個人的な意見としては、等脚台形の共円は気付きにくく、思わず置きそうになってしまいます。等脚台形は角度に自由度があるので気付きにくくなってしまうのです。辺がマスと平行でない長方形もまた気づきにくいです。

3.2　見つけにくい共円

先ほどあげた共円はまだ見つけやすいですが、以下の共円はすぐには気づけません。経験を積むにつれすぐにわかる様になってくるかも？（そもそもそこまでこのゲームで経験を積むことはあるのか…？）

(2.a) 八角形の頂点

以下の図 1 に示した 8 つの頂点のうち 4 つを選んだものは共円になります。相手に仕掛けるのに適しています。

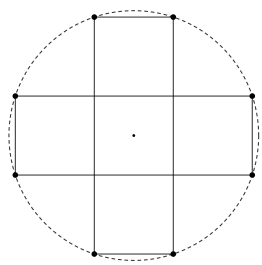

図 1

(2.b) 3 : 4 : 5 の直角三角形が隠れた六角形 1

以下の図 2 に示した 6 つの頂点のうち 4 つを選んだものは共円になります。これは三辺の比が 3 : 4 : 5 である三角形が直角三角形になることを利用した共円です。円の中心は格子点でなければいけないので、共円を見極めるのは難しいです。ただ、この場合はどの 4 点を選んでも選んだ頂点が成す四角形は等脚台形または向かい合う角がどちらも 90° の四角形（長方形含む）となります。そのことから考えて、相似や正多角形から 90° の角を見つけ出すことが共円の検証に重要な手段と言えるかもしれません。

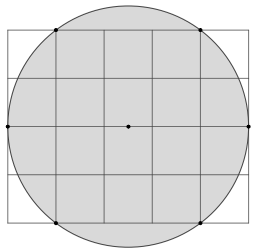

図 2

(2.c) 3 : 4 : 5 の直角三角形が隠れた六角形 2

以下の図 3 に示した 12 個の頂点のうち 4 つを選んだものは共円となります。この共円も 3 : 4 : 5 の共円を利用したものですが、$\tan\alpha = \frac{1}{2}, \tan\beta = \frac{1}{3}$ を満たす $0 < \alpha, \beta < \frac{\pi}{2}$ が $\alpha + \beta = \frac{\pi}{4}$ を満たすことからも共円が言えます。これはより一般に $\tan x = a, \tan y = \frac{1-a}{1+a}$ を満たす実数 $0 < x, y < \frac{\pi}{2}$ が存在すれば $x + y = \frac{\pi}{4}$ が成り立ちます。格子の数を増やせばこれらのことを利用してより複雑な共円を検証できます。

（証明）加法定理より $\tan(x+y) = \frac{\tan x + \tan y}{1 - \tan x \tan y}$ をみたすので、それに $\tan x = a, \tan y = \frac{1-a}{1+a}$ を代入すると $\tan(x + y) = 1$、すなわち $x + y = 45^\circ$ が得られる。

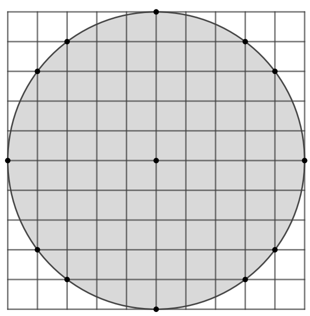

図 3

(2.d) $a^2+b^2=c^2+d^2$ を用いた共円 (図 4 は $a=1,b=7,c=d=5$ のとき)

$a^2+b^2=c^2+d^2$ を満たす整数の組 (a,b,c,d) は、$a^2-c^2=d^2-b^2$ を満たす、つまり $(a+c)(a-c)=(d+b)(d-b)$ を満たす (a,b,c,d) を探すことで求まります。（$48,60$ などの約数の多い数を偶奇の等しい 2 つの整数の積に分解すればこの組が見つけやすいです）特に $c=d$ の時は、$a^2+b^2=2c^2$ です。$(\frac{a+b}{2})^2+(\frac{a-b}{2})^2=c^2$ を満たす整数の組 $(\frac{a+b}{2},\frac{a-b}{2},c)$ は、直角三角形の 3 辺の長さの組としてありうる整数の組[3]と一致させることができるので、$(a,b,c)=(17,7,13)$ や $(a,b,c)=(23,7,17)$ などの組を見つけることができます。

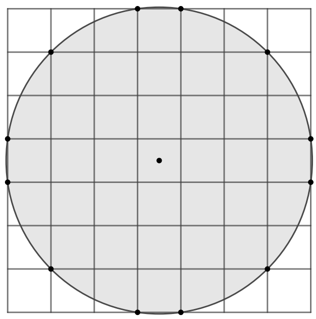

図 4

4　共円をいろんな種類の格子に拡張してみよう！

ここまでは通常の (縦と横の長さが等しい) 格子を用いていきましたが、4 ではアレンジを加えた時の共円について考えます。

4.1　$1\times\sqrt{3}$ の格子・正三角形型の格子

マスの形が長方形であるため、長方形や等脚台形などの共円は絡んできますし、それによく悩まされます。以下では 3 と同様に見つけにくいものについて記します。

(1.a) 直角を利用したもの

直角三角形の直角の頂点から対辺に垂線をおろすと、分けられた 2 つの直角三角形は相似になるので、その性質を使えば直角三角形を見つけることができます。(図 5 はその典型例です) 点を選ぶ位置を変えると、長方形や等脚台形なども作れます ((1.a) に注意をし過ぎているとこれら自明な共円に気づけません。これは本当に気づかない)

3)　ピタゴラス数とも言います。$(3,4,5)$ や $(5,12,13)$ などが有名ですね。

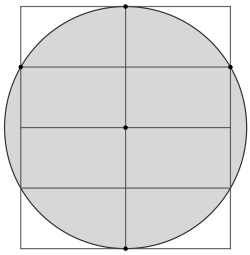

図 5

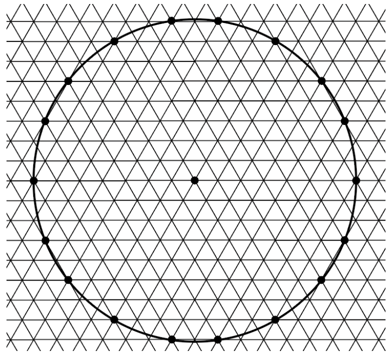

図 6

図 6 は正三角形型の格子における気づきにくい共円の例です（ある程度の格子点の多さが必要)。上記の直角三角形からも言うことができますが、図 7 において $\alpha = 120°, \beta = \gamma = 60°$ が成り立つのを利用してもこれを言うことができます。

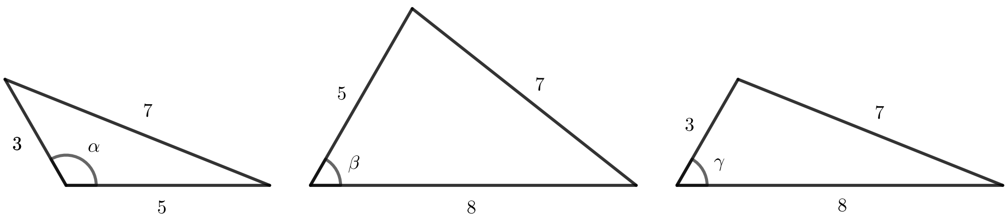

図 7

4.2　立体格子を用いた共円（？）

さらに拡張して、3 次元立体格子を考えてみることにします（どうやって碁石を置くのでしょうか…)。見出しタイトルには共円と書きましたが、正しくは共球というべきでしょう。以下では空間上のある **5** 点が同一球面上にあることを共球と呼ぶことにします。

(2.a) 26 面体の共球

図 8 の灰色の点 24 個は共球である（中心は点 O）(3.2.a) の立体版と考えるとわかりやすいです。

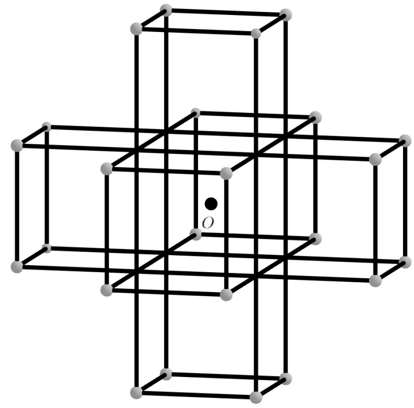

図 8

中心の立方体から伸びている立方体の数を 1 個ではなく 2 個や 3 個にしても、O からの距離が等しいことは変わらないため、共球であることは簡単に言えます。

(2.b) $a^2+b^2+c^2=d^2+e^2+f^2$ を用いた共球（図は $(a,b,c,d,e,f)=(1,1,4,0,3,3)$ の時[4)]）

$a^2+b^2+c^2=d^2+e^2+f^2$ を満たす整数の組 (a,b,c,d,e,f) は、(3.2.d) と同様に $(a+d)(a-d)+(b+e)(b-e)+(c+f)(c-f)=0$ を満たす整数の組 (a,b,c,d,e,f) に等しい。そこで、$(a+d)(a-d)=X,(b+e)(b-e)=Y,(c+f)(c-f)=Z$ とすると、$X+Y+Z=0$ を満たすよう適切に整数 X,Y,Z を定めれば (a,b,c,d,e,f) の組はいくらでも作れます。例えば図は $X=1,Y=-8,Z=7$ のときです。ちなみに X,Y,Z がいずれも偶奇の等しい 2 整数の積であることを考えると、4 を法として 2 と合同な数は X,Y,Z になり得ないことがわかります。よって (X,Y,Z) が (mod4) で合同である整数の組 (順序の違いは区別しない) は $(0,0,0),(1,3,0)$ だけです。ちなみに，図 9 の 6 つの点は正六角形を成しています。わかりやすそうで意外と分からないものです。

5　おまけ（共円ゲームとは関係ないです）

三角形の外心を座標計算で求めてみた。 計算が地獄だったので、5.2 からは少しの計算とその後の過程を書くことにしました。

4）　図の簡略化のため $x\geq 0,y\geq 0,z\geq 0$ の部分のだけを書きました。

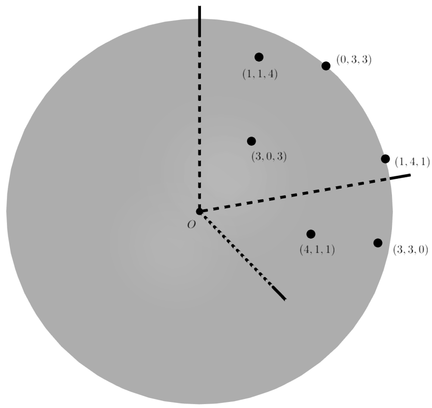

図 9

5.1

実数 $x_1, x_2, x_3, y_1, y_2, y_3$ について、3 点 $(x_1, y_1), (x_2, y_2), (x_3, y_3)$ の外心の座標を求めてみましょう。その外心の座標を (a, b) とおきます。このとき、$(x_1 - a)^2 + (y_1 - b)^2 = (x_2 - a)^2 + (y_2 - b)^2 = (x_3 - a)^2 + (y_3 - b)^2$ が成り立ちます。
よって、${x_1}^2 - {x_2}^2 + {y_1}^2 - {y_2}^2 - 2\ a(x_1 - x_2) + b(y_1 - y_2)\ = 0 \cdots ①$
同様に ${x_2}^2 - {x_3}^2 + {y_2}^2 - {y_3}^2 - 2\ a(x_2 - x_3) + b(y_2 - y_3)\ = 0 \cdots ②$
が得られます。よって、$① \times (y_2 - y_3) - ② \times (y_1 - y_2)$ より a が、$① \times (x_2 - x_3) - ② \times (x_1 - x_2)$ より b が求まります。$a = \dfrac{({x_1}^2 + {y_1}^2)(y_2 - y_3) + ({x_2}^2 + {y_2}^2)(y_3 - y_1) + ({x_3}^2 + {y_3}^2)(y_1 - y_2)}{(x_1 - x_2)(y_2 - y_3) - (x_2 - x_3)(y_1 - y_2)}$
$b = \dfrac{({x_1}^2 + {y_1}^2)(x_2 - x_3) + ({x_2}^2 + {y_2}^2)(x_3 - x_1) + ({x_3}^2 + {y_3}^2)(x_1 - x_2)}{(y_1 - y_2)(x_2 - x_3) + (y_2 - y_3)(x_1 - x_2)}$ (b は a の x と y を入れ替えたものと言えます)

5.2

実数 $x_1, x_2, x_3, y_1, y_2, y_3, z_1, z_2, z_3$ について、3 点 $(x_1, y_1, z_1), (x_2, y_2, z_2), (x_3, y_3, z_3)$ の成す三角形の外心の座標を求めてみましょう。その外心の座標を (a, b, c) とおきます。x 座標、y 座標にのみ着目すれば 5.1 より (a, b) は求まるので、同じように y 座標、z 座標にのみ着目すれば、

$$b = \frac{({y_1}^2 + {z_1}^2)(z_2 - z_3) + ({y_2}^2 + {z_2}^2)(z_3 - z_1) + ({y_3}^2 + {z_3}^2)(z_1 - z_2)}{(y_1 - y_2)(z_2 - z_3) - (y_2 - y_3)(z_1 - z_2)}$$
$$c = \frac{({y_1}^2 + {z_1}^2)(y_2 - y_3) + ({y_2}^2 + {z_2}^2)(y_3 - y_1) + ({y_3}^2 + {z_3}^2)(y_1 - y_2)}{(z_1 - z_2)(y_2 - y_3) + (z_2 - z_3)(y_1 - y_2)}$$

あとはこの 2 式と、5.1 で得られた 2 式から b 同士[5]で通分して、適切に a, c も分母を

5) 英語とは無関係。

揃えればよいです。

そして、それで得られた (a, b, c) を用いて、同一球面上にある 4 点の座標からその球の中心の座標を求めることができます。ある球面上に存在する点 A, B, C, D について、$\triangle ABC, BCD$ の外心を求め、それぞれを O_1, O_2 とします。このとき、O_1 は面 ABC と球の交面（円となる）の中心となり、O_2 についても同様のことが言えるので、O_1 を通り面 ABC に垂直な直線と O_2 を通り面 BCD に垂直な直線は球の中心 O で交わることが示せました（記号は図 10 参照）。

このことを使えば、計算の作業過程を単純化できます。（ただし簡単なわけではないのですが...）

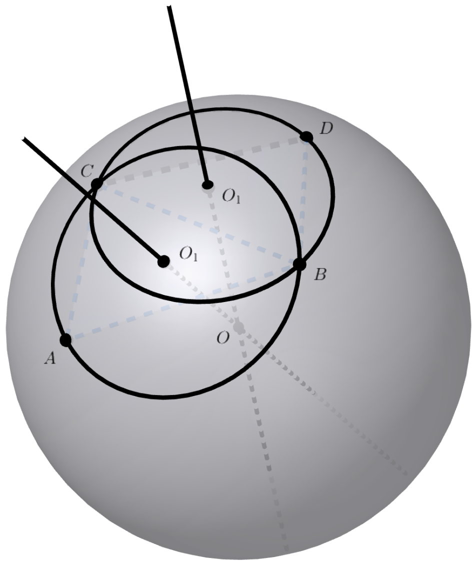

図 10

最後まで読んでいただきありがとうございます！

以下のリンクから過去の部誌も読めます。ぜひお読みになってみてください。

数研公式 HP