解答例

STEP I 2014、第 1 問

純粋数学 • 平方の差

> **STEP I 2014、問 1**
>
> 先に進む前に、まず問題を読んでおこう。問題は STEP Support Programme の問題データベースにある：
>
> step.maths.org/questions/14-s1-q1

鍵となる考え方

すべては一つの因数分解（factorisation）$a^2 - b^2 = (a-b)(a+b)$ に基づいている。n を二つの平方数の差（difference of two squares）として表すことは、$n = de$ と表すことと同じである。ただし $d = a - b$、$e = a + b$ である。さらに d と e の差は偶数 $2b$ であるから、両者の偶奇（parity）は一致しなければならない。このことに気づけば、どの小問も、偶奇の等しい因数の組（factor pair）についての問題になる。

解答

以下、a と b は非負整数（non-negative integer）とする。$n = a^2 - b^2$ かつ $n \geq 1$ ならば $a > b$ であるから、表し方は常に $a > b \geq 0$ を満たす組 (a, b) として列挙できる。

小問 (i)

$$3 = 2^2 - 1^2, \quad 5 = 3^2 - 2^2, \quad 8 = 3^2 - 1^2, \quad 12 = 4^2 - 2^2, \quad 16 = 5^2 - 3^2.$$

（16 については、すぐに思いつく $4^2 - 0^2$ は許されない。平方数は零でないものでなければならないからである。）

小問 (ii)

連続する二つの平方数の差は奇数である：$(m+1)^2 - m^2 = 2m + 1$。したがって、任意の奇数 $2m + 1$（ただし $m \geq 0$）は

$$2m + 1 = (m+1)^2 - m^2.$$

と表される。

小問 (iii)

二つ離れた数の平方の差は 4 の倍数である：$(k+1)^2-(k-1)^2=4k$。$k\geq 1$ のとき $k+1$ と $k-1$ はともに非負であるから、

$$4k=(k+1)^2-(k-1)^2.$$

である。$k=0$ のときは単に $0=0^2-0^2$（または 1^2-1^2）である。

小問 (iv)

すべての平方数は、4 で割った余りが 0 または 1 である：$(2m)^2=4m^2$、$(2m+1)^2=4(m^2+m)+1$。したがって a^2-b^2 を 4 で割った余りは

$$0-0=0,\quad 1-1=0,\quad 1-0=1\quad \text{または}\quad 0-1\equiv 3\pmod 4,$$

のいずれかであり、2 になることはない。よって、$4k+2$ の形の数は二つの平方数の差として表せない。

（同値な言い方をすれば：$(a-b)(a+b)=4k+2$ ならば、$a-b$ と $a+b$ の偶奇は一致する。ともに奇数なら積は奇数であり、ともに偶数なら積は 4 で割り切れる。いずれの場合も $4k+2$ にはならない。）

小問 (v)

$pq=a^2-b^2=(a-b)(a+b)$（ただし $a>b\geq 0$）と仮定する。$d=a-b$、$e=a+b$ とおく。すると d と e は正の整数で、$d\leq e$ かつ $de=pq$ を満たす。逆に、$d\leq e$ で d、e の偶奇が一致するような任意の分解 $pq=de$ から、ちょうど一つの表し方

$$a=\frac{e+d}{2},\qquad b=\frac{e-d}{2},$$

が得られ、これらは非負整数である。したがって、pq の表し方は、そのような因数の組 (d,e) と一対一に対応する。

? **考えてみよう** ここで d と e の偶奇が常に一致するのはなぜか。また、組が二つしかないのはなぜか。

p と q は奇素数（odd prime）であるから pq は奇数であり、pq の約数（divisor）はすべて奇数なので、偶奇の条件は自動的に満たされる。$p\leq q$ とする。素因数分解の一意性（unique factorisation）により、$d\leq e$ を満たす因数の組は

$$(d,e)=(1,pq)\qquad \text{および}\qquad (d,e)=(p,q).$$

に限られる。（これは $p=q$ のときも正しい。p^2 の約数は 1、p、p^2 である。）これらから

$$pq=\left(\frac{pq+1}{2}\right)^2-\left(\frac{pq-1}{2}\right)^2 \qquad \text{および} \qquad pq=\left(\frac{p+q}{2}\right)^2-\left(\frac{q-p}{2}\right)^2.$$

が得られる。この二つの表し方は異なる。$d=a-b$ の値がそれぞれ 1 と p であり、$p\geq 3$ だからである。したがって、pq は二つの平方数の差として、ちょうど二通りに表される。例えば $15=8^2-7^2=4^2-1^2$ である。$p=q$ のとき二つ目の表し方は p^2-0^2 となるが、零でない平方数を要求しているのは小問 (i) だけなので、ここではこれも許される。

$q=2$ のとき、この結果は成り立た**ない**。このとき $pq=2p$ で p は奇数であり、$p=2m+1$ とおくと $2p=4m+2$ となる。小問 (iv) により、$2p$ はどのようにしても二つの平方数の差として表せない。（因数の組 $(1,2p)$ と $(2,p)$ は、いずれも一方が奇数で他方が偶数である。）

小問 (vi)

小問 (v) と同様に、675 の表し方は、因数の組 $675=de$ のうち $d\leq e$ で d、e の偶奇が一致するものに対応する。675 は奇数なので約数はすべて奇数であり、どの因数の組も数に入る。

さて、$675=27\times 25=3^3\times 5^2$ であり、約数は $(3+1)(2+1)=12$ 個ある。約数は $d\leftrightarrow 675/d$ によって対をなし、675 は完全平方数（perfect square）ではない（$26^2=676$）から、自分自身と対になる約数はない。したがって、組は $12/2=6$ 個ある：

(d,e)	$(1,675)$	$(3,225)$	$(5,135)$	$(9,75)$	$(15,45)$	$(25,27)$
(a,b)	$(338,337)$	$(114,111)$	$(70,65)$	$(42,33)$	$(30,15)$	$(26,1)$

よって、675 は二つの平方数の差として、相異なるちょうど **6** 通りに表される。

考えてみよう (a,b) と $(-a,b)$、あるいは a^2-b^2 と $-(b^2-a^2)$ は、異なる表し方として数えるべきだろうか。

そうではない。問題ではすべてを非負整数に制限しており、$a^2-b^2=675>0$ から $a>b$ が従う。したがって、各表し方は $a>b\geq 0$ を満たす一つの組 (a,b) であり、ここで数えたのはまさにこれである。

検算

▶ 表の抜き取り確認：$26^2-1^2=676-1=675$、$30^2-15^2=900-225=675$。

- 小問 (ii)〜(iv) を合わせると、$n \geq 1$ が二つの平方数の差として表せるのは、$n \not\equiv 2 \pmod 4$ のとき、かつそのときに限る。2000 までのすべての n についてコンピュータで確認した結果はこれと一致する。また、pq の表し方が $p \leq q < 200$ を満たすすべての奇素数に対してちょうど二通りであり、$2p$ には表し方が一つもないことの確認結果も一致する。
- すべての b にわたって探索すると、675 の表し方はちょうど六つ、すなわち表にある六つが見つかる。

よくある間違い

- 偶奇の条件を忘れる：$(2, p)$ のような組を $2p$ に対して数えてしまう。これは整数でない $a = \frac{p+2}{2}$ を与える。
- 小問 (v) で $p = q$ の場合を見落とす、あるいはそこで $p^2 - 0^2$ を除外してしまう。小問 (i) 以外では零が許される。
- 小問 (vi) で、約数の個数（12）を、因数の組の個数（6）の代わりに数えてしまう。

STEP のその先へ

ここに見られる、表し方の個数が n の約数によって支配されるというパターンは、初等整数論（elementary number theory）に典型的なものである。よく知られた類似の結果に、二つの平方数の和に関するフェルマー（Fermat）の定理がある：奇素数が $x^2 + y^2$ と表せるのは、それが $1 \bmod 4$ であるとき、かつそのときに限る。この主張はガウス整数（Gaussian integers）$a + bi$ を用いて鮮やかに証明される。さらに知りたければ、Davenport, *The Higher Arithmetic*（整数論の入門書）を読むとよい。

Beyond STEP 解答集：https://beyondstep.keithmcnulty.org/ja/。解答本文は CC0 1.0 である。問題そのものは © Cambridge University Press & Assessment に帰属し、ここには掲載していない。英語版から機械翻訳したものであり、まだ校閲を経ていない。