# Efficient experimental mathematics for combinatorics and number theory

## Alin Bostan

## **Vienna Summer School of Mathematics**

Weissensee, Austria

September 23–27, 2019

Alin Bostan

Efficient experimental mathematics for combinatorics and number theory

## **Problem Session 1**

1. What is the value of

$$\cos\left(\frac{\pi}{7}\right) - \cos\left(\frac{2\pi}{7}\right) + \cos\left(\frac{3\pi}{7}\right)$$
?

2. Show that number of ways one can change any amount of banknotes of  $10 \in 20 \in ...$  using coins of 50 cents,  $1 \in and 2 \in is$  always a perfect square.

 $3^{\star\star\star}$ . Show that if *a*, *b*, *q* are positive integers with

$$q = \frac{a^2 + b^2}{ab + 1}$$

then *q* is a perfect square.

## 2. A money changing problem

Question<sup>†</sup>: The number of ways one can change any amount of banknotes of  $10 \in 20 \in ...$  using coins of 50 cents,  $1 \in$  and  $2 \in$  is always a perfect square.





<sup>†</sup> Inspired by Pb. 1, Ch. 1, p. 1, vol. 1 of Pólya and Szegö's Problems Book (1925).

## 2. A money changing problem

Question<sup>†</sup>: The number of ways one can change any amount of banknotes of  $10 \in 20 \in ...$  using coins of 50 cents,  $1 \in$  and  $2 \in$  is always a perfect square.





▷ This is equivalent to finding the number  $M_{20k}$  of solutions  $(a, b, c) \in \mathbb{N}^3$  of a + 2b + 4c = 20k.

<sup>†</sup> Inspired by Pb. 1, Ch. 1, p. 1, vol. 1 of Pólya and Szegö's Problems Book (1925).

## 2. A money changing problem

Euler-Comtet's denumerants: 
$$\sum_{n \ge 0} M_n x^n = \frac{1}{(1-x)(1-x^2)(1-x^4)}$$

- > f:=1/(1-x)/(1-x^2)/(1-x^4):
- > S:=series(f,x,201):
- > [seq(coeff(S,x,20\*k),k=1..10)];

[36, 121, 256, 441, 676, 961, 1296, 1681, 2116, 2601]

> subs(n=20\*k,gfun[ratpolytocoeff](f,x,n)):

$$\frac{17}{32} + \frac{(20k+1)(20k+2)}{16} + 5k + \frac{(-1)^{-20k}(20k+1)}{16} + \frac{5(-1)^{-20k}}{32} + \sum_{\alpha^2 + 1 = 0} \left( -\frac{(\frac{1}{16} - \frac{1}{16}\alpha)\alpha^{-20k}}{\alpha} \right)$$

> value(subs(\_alpha^(-20\*k)=1,%)):
> simplify(%) assuming k::posint:

> factor(%);

 $(5k+1)^2$ 

What is the value of

$$\cos\left(\frac{\pi}{7}\right) - \cos\left(\frac{2\pi}{7}\right) + \cos\left(\frac{3\pi}{7}\right)$$
?

First evaluate numerically:

> v:=cos(Pi/7) - cos(2\*Pi/7) + cos(3\*Pi/7): > evalf(v,20);

### 0.50000000000000000000

There is no doubt about the value to be proven. Let's apply a hammer:

> simplify(v);

## $\frac{1}{2}$

▷ But do you trust this hammer? What really happened behind the scene?

Compute the value

$$v = \cos\left(\frac{\pi}{7}\right) - \cos\left(\frac{2\pi}{7}\right) + \cos\left(\frac{3\pi}{7}\right)$$

Compute the value

$$v = \cos\left(\frac{\pi}{7}\right) - \cos\left(\frac{2\pi}{7}\right) + \cos\left(\frac{3\pi}{7}\right)$$

▷ If  $a = \pi/7$  and  $x = e^{ia}$ , then  $x^7 = -1$  and  $\cos(ka) = \frac{x^k + x^{-k}}{2}$ 

Compute the value

$$v = \cos\left(\frac{\pi}{7}\right) - \cos\left(\frac{2\pi}{7}\right) + \cos\left(\frac{3\pi}{7}\right)$$

▷ If  $a = \pi/7$  and  $x = e^{ia}$ , then  $x^7 = -1$  and  $\cos(ka) = \frac{x^k + x^{-k}}{2}$ ▷ Since  $x \in \overline{\mathbb{Q}}$ , any polynomial expression in the  $\cos(ka)$  is in  $\mathbb{Q}(x)$ , thus in  $\overline{\mathbb{Q}}$ 

Compute the value

$$v = \cos\left(\frac{\pi}{7}\right) - \cos\left(\frac{2\pi}{7}\right) + \cos\left(\frac{3\pi}{7}\right)$$

▷ If  $a = \pi/7$  and  $x = e^{ia}$ , then  $x^7 = -1$  and  $\cos(ka) = \frac{x^k + x^{-k}}{2}$ ▷ Since  $x \in \overline{\mathbb{Q}}$ , any polynomial expression in the  $\cos(ka)$  is in  $\mathbb{Q}(x)$ , thus in  $\overline{\mathbb{Q}}$ ▷ In particular  $v = F(x) = \frac{N(x)}{D(x)}$  is an algebraic number

- > f:=cos(a) cos(2\*a) + cos(3\*a);
- > expand(convert(f,exp)):
- > F:=normal(subs(exp(I\*a)=x,%));

$$\frac{x^6 - x^5 + x^4 + x^2 - x + 1}{2 \, x^3}$$

Compute the value

$$v = \cos\left(\frac{\pi}{7}\right) - \cos\left(\frac{2\pi}{7}\right) + \cos\left(\frac{3\pi}{7}\right)$$

▷ If  $a = \pi/7$  and  $x = e^{ia}$ , then  $x^7 = -1$  and  $\cos(ka) = \frac{x^k + x^{-k}}{2}$ ▷ Since  $x \in \overline{\mathbb{Q}}$ , any polynomial expression in the  $\cos(ka)$  is in  $\mathbb{Q}(x)$ , thus in  $\overline{\mathbb{Q}}$ ▷ In particular  $v = F(x) = \frac{N(x)}{D(x)}$  is an algebraic number

- > f:=cos(a) cos(2\*a) + cos(3\*a);
- > expand(convert(f,exp)):
- > F:=normal(subs(exp(I\*a)=x,%));

$$\frac{x^6 - x^5 + x^4 + x^2 - x + 1}{2 \, x^3}$$

▷ Get polynomial in  $\mathbb{Q}[t]$  with root *v*: resultant  $\operatorname{Res}_x(x^7 + 1, t \cdot D(x) - N(x))$ 

> factor(resultant(x<sup>7</sup>+1,t\*denom(F)-numer(F),x));

 $-2(t+3)(2t-1)^{6}$ 

## 1. The "official" solution

What is the value of

$$\cos\left(\frac{\pi}{7}\right) - \cos\left(\frac{2\pi}{7}\right) + \cos\left(\frac{3\pi}{7}\right)?$$

Second solution. By considering the identity

$$\cos\frac{5\pi}{7} = \cos\left(\pi - \frac{2\pi}{7}\right) = -\cos\frac{2\pi}{7}$$

(1) can be rewritten as

(2) 
$$\cos \frac{\pi}{7} + \cos \frac{3\pi}{7} + \cos \frac{5\pi}{7} = \frac{1}{2}.$$

Denote the left hand side of (2) by K and apply

 $2 \sin x \cos y = \sin(x+y) - \sin(y-x).$ Using the notation  $\alpha = \frac{\pi}{7}$  and taking  $\sin \alpha = \sin 6\alpha$  into account we get  $K \cdot 2 \sin \alpha = 2 \sin \alpha \cos \alpha + 2 \sin \alpha \cos 3\alpha + 2 \sin \alpha \cos 5\alpha =$   $= \sin 2\alpha + \sin 4\alpha - \sin 2\alpha + \sin 6\alpha - \sin 4\alpha = \sin 6\alpha = \sin \alpha,$ 

implying

$$K = \frac{1}{2}$$

Alin Bostan

## 1. Conclusions

What is the value of

$$\cos\left(\frac{\pi}{7}\right) - \cos\left(\frac{2\pi}{7}\right) + \cos\left(\frac{3\pi}{7}\right)?$$

▷ There are several "human solutions", and all use one or several "tricks".

- ▷ They are elementary, high-school level, but ingenious and ad-hoc.
- ▷ The computerized one is less elementary (it uses an elimination tool, the resultant), but is uniform: it applies to any similar expression, e.g.,

$$\frac{\sin\frac{2\pi}{7}}{\sin^2\frac{3\pi}{7}} - \frac{\sin\frac{\pi}{7}}{\sin^2\frac{2\pi}{7}} + \frac{\sin\frac{3\pi}{7}}{\sin^2\frac{\pi}{7}}$$

or

$$\sqrt[3]{\cos\frac{2\pi}{7}} + \sqrt[3]{\cos\frac{4\pi}{7}} + \sqrt[3]{\cos\frac{8\pi}{7}}$$

▷ Treating these humanly requires special abilities; using a computer, this becomes routine.

## 3. Another beautiful problem on perfect squares

Show that if *a*, *b*, *q* are positive integers with

$$q = \frac{a^2 + b^2}{ab + 1}$$

then *q* is a perfect square.

[Beck, 1988]

## 3. "A very difficult problem"

This problem was proposed by the German Federal Republic at the XXIX. IMO in Canberra, 1988. The Australian Problem Comittee liked it very much, but nobody on the Comittee could solve it. Among the members of the Comittee were George Szekeres and his wife, both famous problem solvers and problem creators. So it was proposed to the four most eminent number theorists of Australia. Each one worked on the problem for six hours, but no one was able to solve it. To make the story short the problem was chosen for the Olympiad and eleven high school students produced complete solutions. The future of mathematics looks bright!

Suppose we are mathematicians of average ability, but we have a computer at our disposal. We will show that then this problem becomes comparatively simple.



### Engel, 1993: Exploring Mathematics with Your Computer

## 3. Generate data and make a first conjecture

```
> A:=[]: B:=[]: Q:=[]:
> for a to 7 do
   for b from a to 1000 do
>
    q:=(a<sup>2+b</sup>2)/(a*b+1);
>
>
     if whattype(q)=integer then
         A:=[op(A),a]: B:=[op(B),b]: Q:=[op(Q),q]:
>
>
    fi;
>
    od:
> od:
> A; B; Q;
> interp(A,B,m), interp(A,Q,m);
```

[1, 2, 3, 4, 5, 6, 7][1, 8, 27, 64, 125, 216, 343] [1, 4, 9, 16, 25, 36, 49]  $m^3, m^2$ 

```
> A:=[]: B:=[]: Q:=[]:
> for a to 7 do
   for b from a to 1000 do
>
   q:=(a^2+b^2)/(a*b+1);
>
>
  if whattype(q)=integer then
>
         A:=[op(A),a]: B:=[op(B),b]: Q:=[op(Q),q]:
>
   fi;
>
   od:
> od:
> A; B; Q;
> interp(A,B,m), interp(A,Q,m);
```

[1, 2, 3, 4, 5, 6, 7][1, 8, 27, 64, 125, 216, 343][1, 4, 9, 16, 25, 36, 49] $m^{3}.m^{2}$ 

▷ At this point, the only solution seems to be the infinity family

 $(a,b,q) = (m,m^3,m^2)$ 

```
> for a to 150 do
> for b from a to 1000 do
> q:=(a^2+b^2)/(a*b+1);
> if whattype(q)=integer then print([a,b,q]) fi;
> od:
> od:
```

[ 1	2	3	4	5	6	7	8	8	9	10	27	30	112
1	8	27	64	125	216	343	30	512	729	1000	240	112	418
1	4	9	16	25	36	49	4	64	81	100	9	4	4

13 / 22

```
> for a to 150 do
       for b from a to 1000 do
>
>
    q:=(a^2+b^2)/(a*b+1);
>
    if whattype(q)=integer then print([a,b,q]) fi;
> od:
> od:

      2
      3
      4
      5
      6
      7
      8
      8
      9

      8
      27
      64
      125
      216
      343
      30
      512
      729

      4
      9
      16
      25
      36
      49
      4
      64
      81

                                                                                               10
                                                                                                          27
                                                                                                                      30
                                                                                                                                112
                                                                                             1000
                                                                                                          240
                                                                                                                  112
                                                                                                                               418
                                                                                                                       4
                                                                                              100
                                                                                                            9
                                                                                                                                  4
```

▷ Thus, the initial conjecture was false.

```
> for a to 150 do
> for b from a to 1000 do
> q:=(a^2+b^2)/(a*b+1);
> if whattype(q)=integer then print([a,b,q]) fi;
> od:
> od:
> od:
1 2 3 4 5 6 7 8 8 9 10 27 30 112
1 8 27 64 125 216 343 30 512 729 1000 240 112 418
1 4 9 16 25 36 49 4 64 81 100 9 4 4
```

▷ Thus, the initial conjecture was false.

▷ Look at the triples giving the same *q*, e.g., q = 4. Do you see any pattern?

13 / 22

```
> for a to 150 do
> for b from a to 1000 do
> q:=(a^2+b^2)/(a*b+1);
> if whattype(q)=integer then print([a,b,q]) fi;
> od:
> od:
```

l	T	2	3	4	5	0	/	0	0	9	10	27	30	112	
	1	8	27	64	125	216	343	30	512	729	1000	240	112	418	
	1	4	9	16	25	36	49	4	64	81	100	9	4	4	_

▷ Thus, the initial conjecture was false.

▷ Look at the triples giving the same *q*, e.g., q = 4. Do you see any pattern?

▷ Yes! The first component of each red triple is the second component of the preceding red triple.

```
> for a to 150 do
> for b from a to 1000 do
> q:=(a^2+b^2)/(a*b+1);
> if whattype(q)=integer then print([a,b,q]) fi;
> od:
> od:
```

1	2	3	4	5	6	7	8	8	9	10	27	30	112	
1	8	27	64	125	216	343	30	512	729	1000	240	112	418	
1	4	9	16	25	36	49	4	64	81	100	9	4	4	

▷ Thus, the initial conjecture was false.

▷ Look at the triples giving the same *q*, e.g., q = 4. Do you see any pattern?

▷ Yes! The first component of each red triple is the second component of the preceding red triple.

▷ Moral: this suggests the transformation:  $(a, b, q) \rightarrow (c, a, q)$  for some *c* 

$$\frac{a^2 + b^2}{ab + 1} = q \in \mathbb{N} \tag{(\star)}$$

$$\frac{a^2 + b^2}{ab + 1} = q \in \mathbb{N} \tag{(\star)}$$

▷ We may assume  $q \ge 1$  and  $0 \le a < b$ 

$$\frac{a^2 + b^2}{ab + 1} = q \in \mathbb{N} \tag{(\star)}$$

 $\triangleright$  We may assume  $q \ge 1$  and  $0 \le a < b$ 

▷ *b* is a root of the polynomial  $x^2 - (qa)x + (a^2 - q) = 0$ 

$$\frac{a^2 + b^2}{ab + 1} = q \in \mathbb{N} \tag{(\star)}$$

- $\triangleright$  We may assume  $q \ge 1$  and  $0 \le a < b$
- ▷ *b* is a root of the polynomial  $x^2 (qa)x + (a^2 q) = 0$

▷ The other root, *c*, satisfies (by def.) 
$$\frac{a^2 + c^2}{ac + 1} = q \in \mathbb{N}$$

$$\frac{a^2 + b^2}{ab + 1} = q \in \mathbb{N} \tag{(\star)}$$

- $\triangleright$  We may assume  $q \ge 1$  and  $0 \le a < b$
- ▷ *b* is a root of the polynomial  $x^2 (qa)x + (a^2 q) = 0$

▷ The other root, *c*, satisfies (by def.)  $\frac{a^2 + c^2}{ac + 1} = q \in \mathbb{N}$ 

▷ *c* satisfies c + b = qa, thus  $c \in \mathbb{Z}$ ; since ca + 1 > 0, it follows  $c \in \mathbb{N}$ 

$$\frac{a^2 + b^2}{ab + 1} = q \in \mathbb{N} \tag{(\star)}$$

- $\triangleright$  We may assume  $q \ge 1$  and  $0 \le a < b$
- ▷ *b* is a root of the polynomial  $x^2 (qa)x + (a^2 q) = 0$

▷ The other root, *c*, satisfies (by def.)  $\frac{a^2 + c^2}{ac + 1} = q \in \mathbb{N}$ 

- ▷ *c* satisfies c + b = qa, thus  $c \in \mathbb{Z}$ ; since ca + 1 > 0, it follows  $c \in \mathbb{N}$
- rightarrow c satisfies  $c + b = qa < \frac{a^2}{b} + b \le 2b$ , hence c < b

$$\frac{a^2 + b^2}{ab + 1} = q \in \mathbb{N} \tag{(\star)}$$

- $\triangleright$  We may assume  $q \ge 1$  and  $0 \le a < b$
- ▷ *b* is a root of the polynomial  $x^2 (qa)x + (a^2 q) = 0$

▷ The other root, *c*, satisfies (by def.)  $\frac{a^2 + c^2}{ac + 1} = q \in \mathbb{N}$ 

- ▷ *c* satisfies c + b = qa, thus  $c \in \mathbb{Z}$ ; since ca + 1 > 0, it follows  $c \in \mathbb{N}$
- rightarrow c satisfies  $c + b = qa < \frac{a^2}{b} + b \le 2b$ , hence c < b

▷ (Intermediate) conclusion: for fixed  $q \ge 1$ , any solution  $(a, b) \in \mathbb{N}^2$  of  $(\star)$  with  $0 \le a < b$  generates another solution  $(c, a) \in \mathbb{N}^2$ , with  $0 \le ca < ba$ 

$$\frac{a^2 + b^2}{ab + 1} = q \in \mathbb{N} \tag{(\star)}$$

- $\triangleright$  We may assume  $q \ge 1$  and  $0 \le a < b$
- ▷ *b* is a root of the polynomial  $x^2 (qa)x + (a^2 q) = 0$

▷ The other root, *c*, satisfies (by def.)  $\frac{a^2 + c^2}{ac + 1} = q \in \mathbb{N}$ 

- ▷ *c* satisfies c + b = qa, thus  $c \in \mathbb{Z}$ ; since ca + 1 > 0, it follows  $c \in \mathbb{N}$
- ▷ *c* satisfies  $c + b = qa < \frac{a^2}{b} + b \le 2b$ , hence c < b

▷ (Intermediate) conclusion: for fixed  $q \ge 1$ , any solution  $(a, b) \in \mathbb{N}^2$  of  $(\star)$  with  $0 \le a < b$  generates another solution  $(c, a) \in \mathbb{N}^2$ , with  $0 \le ca < ba$ 

 $\triangleright$  (Final) argument by going downwards in this family of solutions in  $\mathbb{N}^2$ :

$$\frac{a^2 + b^2}{ab + 1} = q \in \mathbb{N} \tag{(\star)}$$

- $\triangleright$  We may assume  $q \ge 1$  and  $0 \le a < b$
- ▷ *b* is a root of the polynomial  $x^2 (qa)x + (a^2 q) = 0$

▷ The other root, *c*, satisfies (by def.)  $\frac{a^2 + c^2}{ac + 1} = q \in \mathbb{N}$ 

- ▷ *c* satisfies c + b = qa, thus  $c \in \mathbb{Z}$ ; since ca + 1 > 0, it follows  $c \in \mathbb{N}$
- ▷ *c* satisfies  $c + b = qa < \frac{a^2}{b} + b \le 2b$ , hence c < b

▷ (Intermediate) conclusion: for fixed  $q \ge 1$ , any solution  $(a, b) \in \mathbb{N}^2$  of  $(\star)$  with  $0 \le a < b$  generates another solution  $(c, a) \in \mathbb{N}^2$ , with  $0 \le ca < ba$ 

▷ (Final) argument by going downwards in this family of solutions in  $\mathbb{N}^2$ : Replace (a, b) by (c, a), and repeat. The process must stop at some (x, y) with xy = 0, thus  $q = x^2 + y^2 = \max(x, y)^2$ .

## 3. Additional remarks

$$\frac{a^2+b^2}{ab+1} = q \in \mathbb{N} \tag{(\star)}$$

▷ One can show that  $q = \text{gcd}(a, b)^2$ .

 $\triangleright$  One can show that all the solutions of ( $\star$ ) are given by:

$$(a, b, q) = (x_{n-1}, x_n, m^2)$$

where  $m \in \mathbb{N}$  and  $(x_n)_n = (0, m, m^3, m^5 - m, m^7 - 2m^3, ...)$  given by

 $x_0 = 0$ ,  $x_1 = m$ ,  $x_{n+1} = m^2 x_n - x_{n-1}$ , for all  $n \ge 1$ 

 $\triangleright$  E.g., for n = 0 one gets the infinite (trivial) family:

 $(a,b,q) = (0,m,m^2)$ 

 $\triangleright$  For n = 1 one gets the infinite family found by the first guessing:

 $(a,b,q) = (m,m^3,m^2)$ 

▷ In fact,  $x_n = m U_{n-1}\left(\frac{m^2}{2}\right)$ , with  $U_n$  = Chebychev polynomial of 2nd kind

the problem was chosen for the Olympiad and eleven high school students produced complete solutions. The future of mathematics looks bright!

- 1. Nicusor Dan (ROM): Romanian Academy's Institute of Math, Bucharest
- 2. Adrian Vasiu (ROM): Binghamton University
- 3. Hongyu He (CHN): Louisiana State University
- 4. Xi Chen (CHN): University of Alberta, Canada
- 5. Nicolai Filonov (USS): Laboratory of Mathematical Physics, St. Petersburg
- 6. Sergei Ivanov (USS): University of Illinois
- 7. Emanouil Atanassov (BUL): Dpt Grid Technologies & Applications, Sofia
- 8. Zvezdelina Stankova (BUL): University of California, Berkeley
- 9. Ravi Vakil (CAN): Stanford University
- 10. Wolfgang Stöcher (AUT): SKF Österreich AG
- 11. Ngô Bào Châu (VIE): University of Chicago

## 3. Conclusions

- ▷ This is an extremely difficult question.
- ▷ [Campbell, 1988] "The most difficult question ever set at an IMO" (< 2007)
- ▷ There is essentially one known solution; and variants use Fermat descent.
- ▷ This is the reason why (only?) 11 IMO participants solved it.



▷ Moral: With a computer at our disposal, this difficult problem becomes comparatively simple

▷ This is very similar to what happens in research: when facing a completely new and difficult question, experimental math can be of great help

## 3. More related problems

1. Show that if *a*, *b*, *q* are positive integers such that

$$0 < a^2 + b^2 - abq \le q$$

then  $a^2 + b^2 - abq$  is a perfect square.

2. Show that if *a*, *b*, *q* are positive integers with

$$q = \frac{a^2 + b^2 + 1}{ab + 1}$$

1

then q - 1 is a perfect square.

3. Show that if *a*, *b*, *q* are positive integers with

$$q = \frac{a^2 + ab + b^2}{ab + 1}$$

then *q* is a perfect square.

4. (i) Find infinitely many pairs of integers a, b, with 1 < a < b, so that  $q := (a^2 + b^2 - 1)/(ab)$  in an integer. (ii) With *a*, *b* and *q* as in (i), what are the possible values of *q*? [Guy & Nowakowski, 1992]

Efficient experimental mathematics for combinatorics and number theory

[Weber, 1994]

[Engels, 1993]

[Shirali, 1989]

## 3. More related problems

5. Show that if *a*, *b*, *q* are positive integers with

$$q = \frac{a^2 + b^2 + 1}{ab}$$

then q = 3.

[Schinzel, Sierpinski, 1955]

6. Show that if *a*, *b*, *q* are positive integers such that

$$q = \frac{a^2 + b^2}{ab - 1}$$

then q = 5. [Weber, 1994] 7. If  $a, b \in \mathbb{N}^*$  with  $\frac{a^2+b^2-a}{2ab} \in \mathbb{N}$  then *a* is a perfect square. [Shirali, 2003]

8. Show that if *a*, *b*, *q* are positive integers with

$$q = \frac{(4a^2 - 1)^2}{4ab - 1}$$

then a = b.

9. Determine all pairs (a, b) of positive integers such that

$$\frac{a^2}{2ab^2 - b^3 + 1}$$

is a positive integer.

[Ivanov, 2003]

[Ge, 2007]

## 3. More related problems

10. Find infinitely many triples (a, b, c) of positive integers in arithmetic progression such that ab + 1, bc + 1, ca + 1 are all perfect squares. [Deshpande, 1997]

11. If *a*, *b*, *c* are positive integers, then (ab + 1)(bc + 1)(ca + 1) is a perfect square if and only if ab + 1, bc + 1, and ca + 1 are all perfect squares. [Kedlaya, 1998]

12. Show that if *a*, *b*, *c*, *r* are positive integers with

$$r = \frac{a^2 + b^2 + c^2}{abc + 1}$$

then r is the sum of two positive squares.

[Vandervelde, 2013]

13. Show that if *a*, *b*, *c*, *d*, *s* are positive integers with

$$s = \frac{a^2 + b^2 + c^2 + d^2}{abcd + 1}$$

then *s* is either equal to 1, 2, or is the sum of three positive squares.

[Vandervelde, 2013]

**Def**. A *Diophantine k-tuple* is a set of *k* positive integers  $\{a_1, ..., a_k\}$  such that  $a_i a_j + 1$  is a perfect square for all  $1 \le i < j \le k$ .

Problem [Diophantus of Alexandria, ~250]: Characterize all Diophantine k-tuples

▷ [Fermat, 1670]: first Diophantine quadruple, {1,3,8,120}

$$1 \times 3 + 1 = 2^{2}, \quad 1 \times 8 + 1 = 3^{2}, \quad 3 \times 8 + 1 = 5^{2},$$
  
$$1 \times 120 + 1 = 11^{2}, \quad 3 \times 120 + 1 = 19^{2}, \quad 8 \times 120 + 1 = 31^{2}$$

Thm. [Euler, 1783]: There are infinitely many Diophantine quadruples, e.g.,

$${r-1, r+1, 4r, 16r^3-4r}$$

Thm. [Dujella, 2004]:  $k \le 5$ , i.e. there does not exist any Diophantine sextuple

Thm. [He, Togbé, Ziegler, 2019]:  $k \le 4$ , i.e. there is no Diophantine quintuple

Thm. [Hoggatt, Bergum, 1977]: If  $(F_n)_n$  is the Fibonacci sequence, then  $\{F_{2n}, F_{2n+2}, F_{2n+4}, 4F_{2n+1}F_{2n+2}F_{2n+3}\}$  is a Diophantine quadruple

**Thm.** [Arkin, Hoggatt, Strauss, 1979]: Every Diophantine triple can be extended to a Diophantine quadruple: if  $ab + 1 = r^2$ ,  $ac + 1 = s^2$ ,  $bc + 1 = t^2$ , let  $d_+ = a + b + c + 2abc + 2rst$ , then  $\{a, b, c, d_+\}$  is a Diophantine quadruple:

 $ad_+ + 1 = (at + rs)^2$ ,  $bd_+ + 1 = (bs + rt)^2$ ,  $cd_+ + 1 = (cr + st)^2$ .

▷ Still open: Every Diophantine quadruple is of this form!

 $\triangleright > 400 \text{ refs. on https://web.math.pmf.unizg.hr/~duje/ref.html}$