New Looks at Old Number Theory

Aimeric Malter, Dierk Schleicher, and Don Zagier

Abstract. We present three results of number theory that all have classical roots, but also modern aspects. We show how to (1) systematically count the rational numbers by iterating a simple function, (2) find a representation of any prime congruent to 1 modulo 4 as a sum of two squares by using simple properties of involutions and pairs of involutions, and (3) find counterexamples to Euler's conjecture that a fourth power can never be the sum of three fourth powers by using properties of quadratic polynomials with rational coefficients.

This paper consists of three parts—of varying authorship, style, and length—having in common only that each of them relates to the talks on number theory given by the third-named author at the Bremen Summer School in 2011, that each describes a new aspect of a classical topic of number theory, and that each of them, we hope, will entertain and edify the reader. The first section, called "Counting the Rationals," had its origin in a very small part of the Bremen talks in which the speaker briefly described a beautiful construction that he had once been shown (but whose provenance or inventor he did not even know), that permitted a systematic walk through the positive rationals, starting at 0 and at each step following the simple and systematic rule

$$x \mapsto \frac{1}{2\lfloor x \rfloor + 1 - x} \qquad (\lfloor x \rfloor = \text{integer part of } x)$$

to get to the next number. This inspired the first-named author, who at 13 was the youngest participant in the Summer School, to write an extensive essay working out a detailed proof and various further properties of this surprising construction. This essay was submitted to the German competition "Jugend Forscht," where it won the first prize at the Junior Level, and the first section of the current paper is a reworking of it by the first two authors. The second section, written by the second two authors, is an interlude on involutions and their use in number theory, suggested by an observed similarity between a much earlier article by one of us (giving a super-short, though far from transparent, proof of Fermat's famous theorem that every prime of the form $4k + 1$ is a sum of two square numbers) and the argument used in the first section on counting rationals. Finally, the third (and longest) section, subtitled "A Cautionary Tale" because it includes not just one, but *two* salutary lessons for aspiring number-theorists, was written by the third author alone some 25 years ago, but not published at the time. It tells the story of a very famous wrong conjecture in number theory made by the great Euler himself in 1769 and of its very-very-nearly-simultaneous disproof by two people, working independently of one another, some 220 years later. Apart from also having been presented at the Bremen lectures, this third section has little to do with the others beyond the fact that Euler's conjecture was an attempted generalization of Fermat's Last Theorem, which itself grew out of Fermat's study of sums of two squares. But, as we have said, the only true common theme of the three parts of the paper is that each presents a piece of number theory that we hope the reader will find accessible, instructive, and enjoyable.

http://dx.doi.org/10.4169/amer.math.monthly.120.03.243
MSC: Primary 11A41, Secondary 03E10; 11D25

PART I. COUNTING THE RATIONALS.

1. INTRODUCTION. The goal here is to breathe new life into the following hoary theorem.

Theorem 1. *The rational numbers are countable.*

In other words, there is a bijection from the natural numbers to the rationals. This result, originally proved by Cantor in 1873, is of course very well known. The standard proof involves representing the rational number p/q (with $p \in \mathbb{Z}$, $q \in \mathbb{N}$) by the point (p, q) in the upper half plane, then finding a zig-zag path through all points in the half plane with integer coordinates, forgetting all those where p and q are not coprime, and listing all remaining integer points (p, q) in the order visited.

This of course yields a bijection, but it is not very explicit: How can a path through the half plane be described explicitly most easily, and how often do we visit non-coprime fractions that should be ignored? What is the rational number immediately after, or before, a given number? Finally, what is the 25th rational number in this bijection, or which natural number does the fraction $5/17$ correspond to?

We will now describe a different bijection between natural and rational numbers that seems much "nicer." Even though it has old roots, it was discovered relatively recently, and it is also known and documented in the literature, most prominently in [**1**]. However, it does not seem to be as well known among mathematicians as it deserves to be; at the Bremen summer school, when this bijection was presented, it was known to very few people and raised significant interest.

One version of our main result can be stated as follows. It was discovered only a few years ago by Moshe Newman, solving a problem posed by Donald Knuth [**4**] that was based on a paper by Neil Calkin and Herbert Wilf [**2**].

Theorem 2. *The map*

$$S(x) = \frac{1}{2\lfloor x \rfloor - x + 1} \tag{1}$$

has the property that among the sequence $S(0)$, $S(S(0))$, $S(S(S(0)))$, ... *every positive rational number appears once and only once.*

Therefore, if we write $S^n(x)$ for the nth iterate of S, then we obtain an explicit bijection $F\colon \mathbb{N} \to \mathbb{Q}^+$ by $F(n) = S^n(0)$. (We use the convention $\mathbb{N} = \{1, 2, 3, \ldots\}$.) We will try to explain that this bijection can be found in a rather natural way and show some of its many beautiful properties.

Note. The sequence through the (positive) rationals is implicit in the work of Stern in 1858 [**6**], but this was before Cantor's work, so at the time nobody had thought of the concept of countability of the rationals. See also [**5**].

2. THE EUCLID TREE. Our first step is to arrange the *coprime* pairs $(p, q) \in \mathbb{N} \times \mathbb{N}$ in the form of a simple dyadic tree, so that this tree will represent all numbers $p/q \in \mathbb{Q}^+$ exactly once.

Given a pair $(p, q) \in \mathbb{N} \times \mathbb{N}$, the way to find out whether it is coprime is to apply Euclid's algorithm:

- if $p = q$, then the pair is coprime if $p = q = 1$ and not if $p = q > 1$;
- if $p \neq q$, then replace (p, q) by $(p, q - p)$ if $p < q$, or by $(p - q, q)$ if $p > q$, and repeat the procedure.

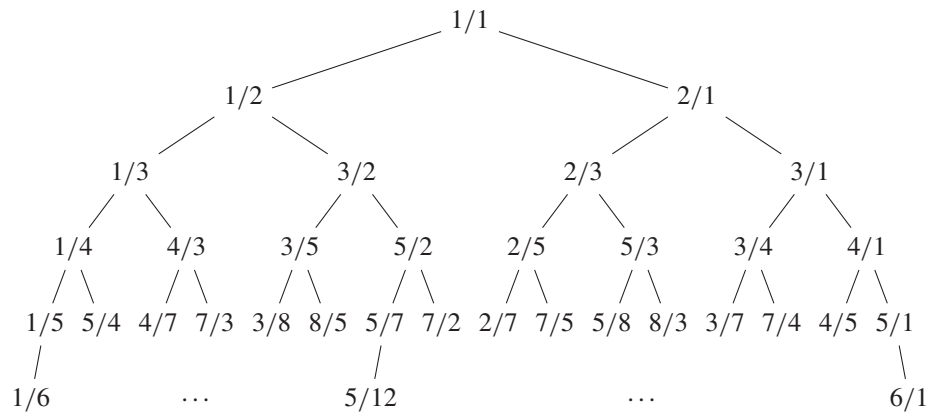
In other words, we keep subtracting the smaller from the larger number until both are equal, and once that is the case, then the resulting number is the greatest common divisor of the original numerator and denominator.

Turning this around, each pair (p, q) has exactly two predecessors $(p, p+q)$ and $(p+q, q)$ under the Euclidean algorithm, and if we start with the pair (1, 1) and write the two predecessors under each point, with the smaller one on the left, we obtain an infinite tree that contains exactly those points (p, q) with coprime p, q, and each of these pairs appears exactly once (because the tree encodes the unique path from (p, q) to (1, 1) under the Euclidean algorithm).

Since we know that all points (p, q) have coprime p and q, we can represent them as $x = p/q$. This means the tree is generated by starting with a "root" $x = 1$ and then applying the rule

$$\begin{array}{ccc} & x = p/q & \\ {\scriptstyle A_0}\swarrow & & \searrow{\scriptstyle A_1} \\ x/(x+1) = p/(p+q) & & x+1 = (p+q)/q \end{array} \tag{2}$$

recursively to each vertex. This generates a tree that we will call the *Euclid tree* and that contains all positive rationals exactly once; its first few lines are shown in the figure below. (This tree goes back essentially to the work of Stern in 1858 [**6**] and was publicized more recently by Calkin and Wilf in [**2**]; it is sometimes called the *Calkin-Wilf-tree*.)



Observe that for any number $x = p/q$, the rightmost (and largest) daughter after n generations is $(p+nq)/q = x+n$, and quite symmetrically the leftmost (and smallest) daughter is $p/(np+q) = x/(nx+1)$.

3. A SEQUENCE THROUGH THE POSITIVE RATIONALS. In order to find a sequence that visits all rationals exactly once, we can simply march through the Euclid tree "breadth first," i.e., line by line, so we get the sequence

n	1	2	3	4	5	6	7	8	9	10	11	⋯
$F(n)$	1	$\frac{1}{2}$	2	$\frac{1}{3}$	$\frac{3}{2}$	$\frac{2}{3}$	3	$\frac{1}{4}$	$\frac{4}{3}$	$\frac{3}{5}$	$\frac{5}{2}$	⋯

(3)

This solves the first problem in the original approach: We have a natural way of marching through the positive rationals, and we don't have to worry about duplicates and omitting those that are not in lowest terms.

It turns out that our second goal, specifying this sequence explicitly, is just as easy: There is a simple way to go from any rational number in the sequence to the next.

To see this, consider any vertex x in the Euclid tree with its two daughter vertices $x/(x+1)$ and $x+1$, so if we set $y = x/(x+1)$ as the left daughter, then the right daughter is $x+1 = 1/(1-y)$; this gives a simple formula to go from one rational to the next in our sequence, provided the initial number is a "left daughter." Note that in this case we have $0 \le y < 1$ and hence $\lfloor y \rfloor = 0$, so the successor $1/(1-y)$ of y is indeed given by (1).

Now suppose we are at some right daughter y and want to find the successor in the sequence (i.e., the rational number to the right of it in the tree). This depends on how many generations ago the two fractions have a common parent; let k be this number of generations. (For instance, the fraction $7/3$ and its successor $3/8$ have $k = 3$.) Let $x = p/q$ be the common parent k generations ago. The number y is generated from p/q by taking the "left daughter" $p/(p+q)$, followed by taking $(k-1)$ "right daughter steps," so

$$y = \frac{p + (k-1)(p+q)}{p+q} = k - 1 + \frac{p}{p+q}. \tag{4}$$

Similarly, the successor to y is constructed from p/q by taking one right daughter step, then $k-1$ left daughter steps. This is the number

$$z = \frac{p+q}{q + (k-1)(p+q)} = \frac{1}{\frac{q}{p+q} + (k-1)}. \tag{5}$$

But how can we go from y to z? Observe that $k - 1 = \lfloor y \rfloor$ and

$$\frac{p}{p+q} = y - \lfloor y \rfloor.$$

So we simply have

$$z = \frac{1}{1 - (y - \lfloor y \rfloor) + \lfloor y \rfloor} = \frac{1}{2\lfloor y \rfloor - y + 1} = S(y). \tag{6}$$

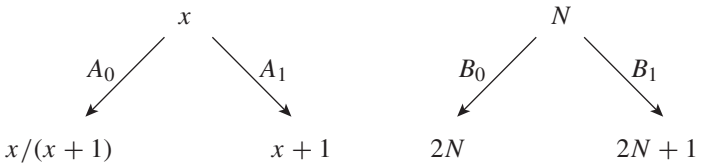
(We observe that the case we considered first, when $y = x/(x+1)$ and $z = x+1$ were the left and right daughters of the same parent, is just the special case $k = 1$ of this argument.)

All this works within each line of the tree; we still have to consider the case that y is the last number within one line, so $y = n$ is an integer. The successor of n should be $1/(n+1)$, and luckily this is just what our formula (1) produces.

Miracle or not: This concludes the proof of Theorem 2. ∎

4. FINDING THE POSITION OF A GIVEN FRACTION. We promised a simple algorithm to tell at which position in our sequence a given positive rational number is, and vice versa. We had defined a bijection $F: \mathbb{N} \to \mathbb{Q}^+$ by setting $F(n) = S^n(0)$, where S is the "successor function" defined by (1). Denote the inverse of F by $N: \mathbb{Q}^+ \to \mathbb{N}$, giving the position in the sequence for any positive rational. Since every

vertex in the Euclid tree has two daughter vertices, the positions in the sequence are as follows:



where in the diagram on the right-hand side we indicated at which position in the sequence the numbers on the left are. If a vertex in the tree has a rational number x that is at position N in the sequence, then its left daughter vertex has value $A_0(x) = x/(x+1) < 1$ and position $B_0(N) = 2N$, while the right daughter vertex has value $A_1(x) = x + 1 > 1$ and position $B_1(N) = 2N + 1$.

This leads to the recursive formula

$$N(x) = \begin{cases} 1 & \text{if } x = 1, \\ 2N(x/(1-x)) & \text{if } x < 1, \\ 2N(x-1)+1 & \text{if } x > 1. \end{cases}$$

Note that as this definition is applied recursively, the successive arguments of N perform the Euclidean algorithm of the pair $(x, 1)$ (or of (p, q) when $x = p/q$). Given an $x \in \mathbb{Q}^+$, the Euclidean algorithm allows us to express it as $x = A_{i_r} \dots A_{i_1}(1)$, where r is the number of steps that need to be performed—or equivalently, that x is in line $r + 1$ of the tree (counting so that $1/1$ is in line 1). The position $N(x)$ then satisfies

$$\begin{aligned} N(x) &= N(A_{i_r} \dots A_{i_1}(1)) \\ &= B_{i_r} \dots B_{i_1}(1) \\ &= 2^r + 2^{r-1} i_1 + 2^{r-2} i_2 + \cdots + i_r \\ &= (1, i_1, \dots, i_r)_2 \end{aligned} \tag{7}$$

so we immediately get the binary decomposition of N.

We illustrate this by a simple example, say $p/q = 5/12$. By running the Euclidean algorithm, we obtain

$$(5, 12) \mapsto (5, 7) \mapsto (5, 2) \mapsto (3, 2) \mapsto (1, 2) \mapsto (1, 1).$$

Since this ends in $(1, 1)$, we have verified that indeed 5 and 12 are coprime. We know further that $5/12$ is in line $r = 6$ of the tree, and hence between positions $2^{r-1} = 32$ and $2^r - 1 = 63$. In binary, we are between positions 100000_2 and 111111_2. In each of the five steps of the Euclidean algorithm, we had to subtract from either the numerator or denominator. This means in the tree that we had to choose either the left or the right branch, and as this chooses the left or right half of the remaining tree below the current node, this specifies one binary digit of N (keep in mind that the Euclidean algorithm traverses the tree from x up to 1, so the binary digits of N are produced in reverse order). In our case, the order of branches from the top down to $5/12$ is LRRLL, so $N(5/12) = 101100_2 = 44$, as the reader can verify by looking at the beginning of the Euclid tree as given in §2.

The converse is equally straightforward: To find $F(44)$, we write $44 = 101\,100_2$, and then $F(44) = A_0(A_0(A_1(A_1(A_0(1))))) = 5/12$.

This method is very efficient and works well even in much less trivial cases, especially if we speed up the Euclidean algorithm by subtracting the smaller number from the larger one as often as possible. For instance, for the fraction 332/147, this accelerated algorithm looks like

$$(332, 147) \overset{A_1^{-2}}{\longmapsto} (38, 147) \overset{A_0^{-3}}{\longmapsto} (38, 33) \overset{A_1^{-1}}{\longmapsto} (5, 33)$$
$$\overset{A_0^{-6}}{\longmapsto} (5, 3) \overset{A_1^{-1}}{\longmapsto} (2, 3) \overset{A_0^{-1}}{\longmapsto} (2, 1) \overset{A_1^{-1}}{\longmapsto} (1, 1)$$

(*Remark*: this is nothing other than the continued fraction expansion

$$2 + 1/(3 + 1/(1 + 1/(6 + 1/(1 + 1/(1 + 1/(1 + 1))))))$$

of 332/147), so

$$N\left(\frac{332}{147}\right) = B_1^2 B_0^3 B_1 B_0^6 B_1 B_0 B_1(1) = 1101000000100011_2 = 53283.$$

Note that, despite the somewhat mysterious appearance of the formula in (1), our sequence of rational numbers is actually completely determined by the Euclidean algorithm, specifying the position of p/q by a binary coding of the steps in this algorithm, so it is in fact a very natural sequence.[1] It is surprising that it was discovered only quite recently. This shows that even today and even at an elementary level, mathematics still provides room for interesting discoveries!

5. FURTHER PROPERTIES OF OUR TREE AND SEQUENCE. The Euclid tree and our iteration sequence have many further interesting properties. We already noted that, essentially by construction, the rth line of the tree consists of those numbers that take $r - 1$ steps in the Euclidean algorithm to land at (1, 1). A similar observation is that, when writing any fraction p/q (as always in lowest terms) as a continued fraction

$$\frac{p}{q} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ddots + \cfrac{1}{a_k}}},$$

then $a_0 + a_1 + \cdots + a_k$ equals the number of the line, so all fractions in a given line have the same sum of their continued fraction entries.

So we understand which rational numbers are in which lines; but how are these numbers ordered within the line? Here is the answer.

Theorem 3. *The 2^{r-1} numbers in line r in the Euclid tree are ordered as follows: Label these 2^{r-1} numbers $x_0, \ldots, x_{2^{r-1}-1}$ and for $k \in \{0, \ldots, 2^{r-1} - 1\}$ denote by $\varphi(k) \in \{0, \ldots, 2^{r-1} - 1\}$ the position of x_k when these numbers are reordered by increasing size. Then the binary representation of $\varphi(k)$ equals that of k in reverse order of binary digits (as binary numbers with r places).*

[1] We did have one choice: The order of the two lower vertices in (2) (or equivalently whether to traverse the lines of the Euclid tree left to right or right to left). The other choice would lead to a different sequence of fractions with successor function: $x \mapsto 2\lfloor 1/x \rfloor - 1/x + 1$.

For example, the number $3/8$ is in line 4 and it has position $4 = 0100_2$ from the left (starting the count at 0), so ordered by size it should have position $0010_2 = 2$ (starting at 0 again): Indeed, the smallest numbers in this line are $1/5, 2/7, \mathbf{3/8}, 3/7 \ldots$.

To see that this is true, observe that the left daughter in the tree of p/q is $p/(p+q) < 1$, while the right daughter is $(p+q)/q > 1$. All even numbered elements of our sequence are thus smaller than all odd numbered ones: The least significant bit in the position within any line is the most significant bit when ordering by size. Similarly, among the odd elements in the sequence (those with last position bit 1), the elements are greater than 2 if and only if the last two bits are 11 (so we have a right daughter of a right daughter), and they are less than 2 if the last two bits are 01 (for a right daughter of a left daughter). Similar arguments hold for all bit sequences, and this proves our observation.

The Euclid tree is constructed in a symmetric way: Reflecting it horizontally (interchanging left and right) interchanges the number p/q with q/p. This gives a simple way to find the predecessor $P(x)$ of any rational number $x = p/q$ in our sequence: Reflect horizontally, find the successor, and reflect back. In other words, the predecessor of x is $P(x) = 1/S(1/x)$. There is an exception if a line break gets in the way: The first number in line n is $1/n$, and its predecessor is simply $n-1$. This can be verified easily.

It is not hard to give an explicit formula for the inverse P of S. If $y = S(x) = \frac{1}{2\lfloor x\rfloor - x + 1}$, then $1/y - 1 = 2\lfloor x\rfloor - x$, and from this it is easy to check that $x = -1/y - 1 + 2\lceil 1/y\rceil$. (This agrees with our previous formula $P(y) = 1/S(1/y)$ if we observe that the exceptional case occurs when $1/y$ is an integer, so that $\lceil 1/y\rceil = \lfloor 1/y\rfloor$.) We can also write the formula for P as

$$P(y) = -1/y - 1 - 2\lfloor -1/y\rfloor. \tag{8}$$

We will discuss where this comes from in Part II.

This backwards iteration can be applied beyond the fraction $1/1$ that we initially started with. We obtain

$$\cdots \mapsto 2 \overset{P}{\mapsto} 1/2 \overset{P}{\mapsto} 1 \overset{P}{\mapsto} 0 \overset{P}{\mapsto} \infty \overset{P}{\mapsto} -1 \overset{P}{\mapsto} -2 \overset{P}{\mapsto} -1/2 \mapsto \cdots.$$

The backwards iteration naturally runs through 0, then ∞, and then visits all negative rationals in a similar order as the positive ones: If $x \notin \mathbb{Z}$, then it is easily checked that $S(-x) = -S(x)$, so every line of our "positive" tree becomes a line in the "negative" tree that is traversed in the same order. However, while $S(n) = 1/n$ for integers $n > 0$, we have $S(-n) = -1/(n-1)$, so when S has traversed a line in the "negative" Euclid tree, it jumps to the previous line, until it eventually comes to $-1/2 \overset{S}{\mapsto} -2 \overset{S}{\mapsto} -1 \overset{S}{\mapsto} \infty \overset{S}{\mapsto} 0 \overset{S}{\mapsto} 1 \mapsto \cdots$ and then traverses the "positive" tree as described above. Together, this provides a simple and natural bijection between $\mathbb{Q}$ and $\mathbb{Z} \smallsetminus \{0\}$, or between $\mathbb{Q} \cup \{\infty\}$ and $\mathbb{Z}$. In a more erudite language, we can say that the maps S and $P = S^{-1}$ define an action of the group $\mathbb{Z}$ on the set $\mathbb{P}^1(\mathbb{Q}) = \mathbb{Q} \cup \{\infty\}$ and that this action is simply transitive, i.e., is free and has only one orbit.

Among the many interesting properties of the tree and the sequence, let us mention one more.

Theorem 4. *Any two successive fractions p_k/q_k and p_{k+1}/q_{k+1} have the property that $p_{k+1} = q_k$.*

Proof. This follows immediately from equations (4) and (5) (observing that the inductive hypothesis that p and q are coprime implies that both fractions are already in lowest terms). ∎

Therefore, our sequence of fractions is already determined by the sequence (q_k) of denominators. That sequence has in fact been known for a long time under the name of *Stern's diatomic sequence*, and it has various nice properties. Our denominators are defined so that they satisfy the simple recursive relation $q_{2k} = q_k + q_{k-1}$ (left daughters) and $q_{2k+1} = q_k$ (right daughters), together with the initial conditions $q_1 = 1$ and $q_0 = 1$; these define the sequence q_k completely.

The sequence (q_k) can be interpreted as the number of different representations of k as sums of powers of two, subject to the condition that each power of two be used at most *twice* (if we are allowed to use each power of two only once, we get the usual binary decomposition of k, and this is unique). For instance, $5 = 4 + 1 = 2 + 2 + 1$ has two representations, while $6 = 4 + 2 = 4 + 1 + 1 = 2 + 2 + 1 + 1$ has three, and $7 = 4 + 2 + 1$ has a unique such decomposition. Thus $q_5 = 2$, $q_6 = 3$, and $q_7 = 1$. This is also seen easily: Any such representation of an odd number $2k + 1$ must involve a single term 1 and all other summands must be even, whence $q_{2k+1} = q_k$. Any representation of $2k$ either has no 1 term or two 1 terms. Striking the last binary zero in the remaining terms, we obtain a representation of k or of $k - 1$, respectively. This shows indeed $q_{2k} = q_k + q_{k-1}$ as required.

Our sequence of denominators $1, 2, 1, 3, 2, 3, 1, 4, \ldots$ represents the Euclid tree, and thus our sequence of fractions completely. In particular, each pair (p, q) of coprime positive numbers must appear exactly once in this sequence as subsequent entries.

Many more interesting properties can be discovered in this context, and we invite the readers to explore these!

PART II. AN INTERLUDE ON INVOLUTIONS.

6. INVOLUTIONS AND FERMAT'S THEOREM ON SUMS OF 2 SQUARES.

In this section, we will recall an argument given by one of us many years ago in which a simple property of involutions was used to give a very short, albeit not very transparent, proof of Fermat's famous theorem on sums of two squares.

Theorem 5. *Every prime* $p \equiv 1 \pmod 4$ *is the sum of two squares.*

We then show how an idea about *pairs* of involutions can be used to make this proof effective and somewhat more comprehensible.

We begin by reviewing some basic notions and terminology. An *involution* on a set X is a bijection from X to itself that is equal to its own inverse. Thus an involution α sends each point P of X to a point $Q = \alpha(P)$ also belonging to X in such a way that applying α to Q brings one back to the starting point P. Of course, it may happen that $Q = P$. In this case, we call P a *fixed point* of α. The set of all fixed points of α is denoted by $\mathrm{Fix}(\alpha)$. If this set is empty, the involution α is said to be *free*. As an example, the action of α on $X \setminus \mathrm{Fix}(\alpha)$, the complement of its fixed-point set, is always free.

Since a set X with a free involution gets partitioned up into disjoint pairs of points $(P, \alpha(P) = Q \neq P)$, it is clear that if X is finite then it must necessarily have an even cardinality. Combining this general observation with the previous remark about

$X \setminus \mathrm{Fix}(\alpha)$, we see that the cardinality of the fixed point set of *any* involution on a finite set X has the same parity as the cardinality of X itself: They are both odd or both even. In particular, this parity is independent of the involution, so that (denoting cardinality by "#") we have the following useful principle.

Principle 1. If α and β are two involutions on the same finite set, then

$$\#\mathrm{Fix}(\alpha) \equiv \#\mathrm{Fix}(\beta) \pmod 2. \tag{9}$$

As a special case, since 1 is odd and 0 isn't, we have the following.

Principle 2. If α and β are involutions on the same finite set, and if α has *exactly one* fixed point, then β has *at least one* fixed point.

In [**7**], Principle 2 was used to give an ultra-short ("one-sentence") proof of Fermat's famous theorem that any prime number of the form $p = 4k + 1$ is a sum of two integral squares. This proof, which was a stripped-down-to-the-bare-essentials version of previous much longer proofs by Liouville and Heath-Brown, went as follows. Take X to be the (clearly finite) set

$$X = X(p) = \{(a, b, c) \in \mathbb{N}^3 \mid p = a^2 + 4bc\}, \tag{10}$$

and define the first involution α on X by the rather complicated formula[2]

$$\alpha : (a, b, c) \mapsto \begin{cases} (a + 2c, c, b - a - c) & \text{if } a < b - c, \\ (2b - a, b, a - b + c) & \text{if } b - c < a < 2b, \\ (a - 2b, a - b + c, b) & \text{if } a > 2b, \end{cases} \tag{11}$$

and define the second involution β by the much simpler formula

$$\beta : (a, b, c) \mapsto (a, c, b). \tag{12}$$

Then α is easily seen to have the unique fixed point[3] $(1, 1, k)$, and the fixed point of β whose existence is ensured by Principle 2 is our desired solution of the equation $p = a^2 + 4b^2$.

However, this proof, though leaving little to be desired in terms of brevity, has two defects. First of all, the definition (11) is complicated and unmotivated. We can do nothing about this. (As mentioned, the proof was constructed by taking earlier and more natural constructions by Liouville and Heath-Brown and then artificially removing and inserting extra bits of sets to get down to a final formula that could be presented in one sentence.) But apart from this, the proof is, on the face of it, totally non-effective: One knows that the involution β must have a fixed-point, but apparently has no idea where. (Indeed, fixed-point theorems, of which there are many in topology and in functional analysis, are the standard example of intrinsically non-constructive proofs in mathematics.) But actually—as both the author and several readers of [**7**] noticed after its publication—this is not the case. Principle 2 can be refined to give an algorithmic way to obtain a fixed-point of β from the fixed-point of α, and applying

[2]Of course, one has to check that α is always defined, maps X to itself, and is its own inverse, but each of these verifications is straightforward. (For the last, one notices that the first and third cases in (11) are interchanged, and the second case preserved, when one iterates α.) A more detailed exposition than the one given here can be found in [**1**].

[3]It is only here that we use that $p \equiv 1 \pmod 4$; if p were congruent to -1 modulo 4, then the argument would break down, and indeed it is easy to see that in that case p is not a sum of two squares.

this refined principle to the special situation of the involutions (11) and (12) gives an entirely *effective*, although not very *efficient*, way to find the decomposition of a prime number $p = 4k + 1$ into two squares.[4] We discuss this in the next section.

7. PAIRS OF INVOLUTIONS. Suppose we are given any two involutions α and β on a finite or infinite set X, and a fixed point of one of them. What can we then do? In the game of bridge there is a useful (and, by the way, completely mathematical) principle called the "principle of restricted choice" that can be very helpful when one is faced with making a delicate decision. Here we are in the even more fortunate situation of having no choice at all. Since all that has been given to us is a pair of involutions and a fixed point P of, say, α, all that we can really do is to look at the point P and try applying the involutions. And applying α is pointless, since it merely leaves us at our starting point, so actually the only thing we can do is apply β. This gives a new point, say Q, and again we have no choice at all on how to proceed: This time applying β is pointless, since it would just bring us back to P again, and we have no other involutions to apply except α, so we apply α to Q to get a third point R. To this point, we can only apply β again, and so forth. If the set X is infinite, this process may perfectly well continue forever—we will see an example of this below—but if it is finite then "something must give": If we number our sequence $(P, Q, R, \ldots)$ more intelligently as $(P_0, P_1, P_2, \ldots)$, then the finiteness of X implies that for some n the successor of P_n must for the first time be a point that is already on the list. That successor cannot be P_0 (unless $n = 0$ and the initial point P happened to be a fixed point of β as well as of α), because then P_n would coincide with P_1 and its successor would not be the first occurrence of a repetition, and it cannot be P_m for any m strictly between 0 and n, since then P_m would have three distinct images P_{m-1}, P_{m+1} and P_n under only two involutions, so it must be P_n itself. In other words, we must eventually get to a point P_n that is distinct from $P_0 = P$ (unless P was a fixed point of both α and β) and that is itself a fixed point of either α or β, depending on which involution was used to get us from P_{n-1} to P_n (or equivalently, whether n is even or odd).

To state the conclusion we have reached more formally, let us denote by $\mathcal{F}$ the disjoint union of $\mathrm{Fix}(\alpha)$ and $\mathrm{Fix}(\beta)$ (as opposed to their union as subsets of X; this means that any points of X that happen to be fixed points of both α and β will be counted twice in $\mathcal{F}$). Then we have constructed a free involution on $\mathcal{F}$, namely, the map ρ that assigns to the initial fixed point $P = P_0$ the final point P_n of the chain of successive images of P under alternating applications of the involutions α and β. (It is an involution because if we start with P_n, then we simply go down the same chain backwards and end up at P_0. It is free because even in the limiting case when our initial point $P = P_0$ happened to be a fixed point of both involutions, so that $n = 0$ and $P_n = P_0$, the points P_0 and P_n coincide as elements of X but are counted as distinct elements of $\mathcal{F}$, the first belonging to $\mathrm{Fix}(\alpha)$ and the second to $\mathrm{Fix}(\beta)$.) Summarizing, we have proved the following.

[4]The difference between "effective" and "efficient" can be illustrated clearly by contrasting the method explained in §7 with another method to solve the same problem. Choose a "random" number $n \pmod p$ and raise n to the kth power mod p (this can be done very quickly by a small number of multiplications mod p by writing k in binary). Half the time this will equal $\pm 1 \pmod p$, but half the time it will give a solution i of $i^2 \equiv -1 \pmod p$. Then if we apply the Euclidean algorithm to get a sequence of numbers $p, i, j, \ldots, x, y, \ldots, 1, 0$, with x and y being the first two numbers less than $\sqrt{p}$, one can show that $x^2 + y^2 = p$. This is extremely *efficient*, typically taking time of the order of $\log p$, rather than $\sqrt{p}$ like the method we describe, but it is not *effective* because the step "choose a random number" cannot be implemented by an algorithm that guarantees success in a short time.

Principle 3. Let α and β be two arbitrary involutions on a finite set X. Then there is a canonically defined free involution ρ on the disjoint union of the fixed-point sets of α and β.

Notice that this principle refines Principle 1, because if a finite set admits a free involution, then its cardinality has to be even, and the cardinality of $\mathcal{F}$ is the sum of the cardinalities of $\mathrm{Fix}(\alpha)$ and $\mathrm{Fix}(\beta)$. And it also leads to an effective version of Principle 2, because if α has a unique fixed point P, then $\rho(P)$ is necessarily a fixed point of the other involution β. In particular, we now have an effective version of Fermat's two-squares theorem, by taking X, α and β as in (10), (11), and (12) and applying ρ to the fixed point $(1, 1, k)$ of α to obtain a fixed point of β. As an example, consider the prime $p = 73 = 4k + 1$ with $k = 18$. The successive images of the fixed point $(1, 1, 18)$ of α under successive applications of the involutions β and α are

$$\begin{aligned}(1,1,18) &\overset{\beta}{\mapsto} (1,18,1) \overset{\alpha}{\mapsto} (3,1,16) \overset{\beta}{\mapsto} (3,16,1) \overset{\alpha}{\mapsto} (5,1,12)\\ &\overset{\beta}{\mapsto} (5,12,1) \overset{\alpha}{\mapsto} (7,1,6) \overset{\beta}{\mapsto} (7,6,1) \overset{\alpha}{\mapsto} (5,6,2)\\ &\overset{\beta}{\mapsto} (5,2,6) \overset{\alpha}{\mapsto} (1,9,2) \overset{\beta}{\mapsto} (1,2,9) \overset{\alpha}{\mapsto} (3,2,8)\\ &\overset{\beta}{\mapsto} (3,8,2) \overset{\alpha}{\mapsto} (7,2,3) \overset{\beta}{\mapsto} (7,3,2) \overset{\alpha}{\mapsto} (1,6,3)\\ &\overset{\beta}{\mapsto} (1,3,6) \overset{\alpha}{\mapsto} (5,3,4) \overset{\beta}{\mapsto} (5,4,3) \overset{\alpha}{\mapsto} (3,4,4),\end{aligned}$$

landing at a fixed point of β as promised and giving the desired decomposition $73 = 3^2 + 4 \cdot 4^2 = 3^2 + 8^2$.

Let us look at this argument and this example a little more closely. The reasoning we used to prove Principle 3 actually gives a complete description of the set of orbits of a finite set X under the action of the group of permutations of X generated by two involutions α and β: These orbits are either *paths* connecting two fixed points P and $\rho(P)$ of the two involutions α or β (including the degenerate case when $P = \rho(P)$ is a fixed point of both involutions and the "path" reduces to a single point), or else *cycles* of even length in which pairs of adjacent elements are interchanged alternately by α and by β. In the numerical example for $p = 73$ just given, the 21 elements of $X(p)$ form a single orbit, which is a path going from the unique fixed point $(1, 1, 18)$ of α to the unique fixed point $(3, 4, 4)$ of β. The same thing happens for all primes $p = 4k + 1$ less than 229, but for this prime we find *two* orbits, a path of length 15 connecting the unique fixed point $(1, 1, 57)$ of α to the unique fixed point $(15, 1, 1)$ of β and a cycle of length 14 whose elements are related alternately by α and β. Without going into further detail, we mention that this is connected with—indeed, equivalent to—the fact that the quadratic number field $\mathbb{Q}(\sqrt{229})$ has class number bigger than one, i.e., that unique prime factorization fails to hold in this field.[5] A famous conjecture due to Henri Cohen and Hendrik Lenstra says that this property holds for only about 11% of all primes of the form $p = 4k + 1$, which means that almost 90% of the time our algorithm for decomposing p into squares is maximally inefficient, forcing us to look at every single element of X before finding the one that we care about!

Finally, we note that our arguments apply equally well to the case of infinite sets X and give a complete description of the possible shapes of all orbits of X under the group generated by two arbitrary involutions α and β. These orbits are either paths

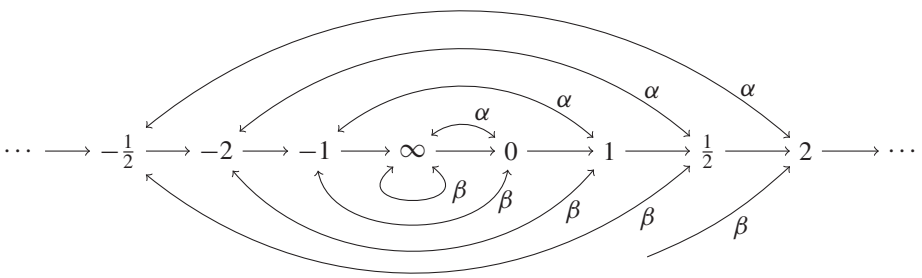
[5] In general, the class number h of $\mathbb{Q}(\sqrt{p})$ is an odd integer and the set $X(p)$ will decompose into one path joining the unique fixed points of α and β and $(h-1)/2$ cycles of even length.

of finite length joining a fixed point P of one of the involutions to another such fixed point $\rho(P)$ (which may coincide with P if P was a fixed point of both involutions), or else cycles of even finite length as before, or else semi-infinite paths that start at a fixed point of α or β and then continue infinitely in one direction by applying the two involutions in alternation, or else doubly infinite paths in which all points are obtained from any initial point by applying the two involutions in alternation.[6]

A nice example of this is provided by the construction that was described in the section on "counting rationals". Here we take for X the set $\mathbb{Q} \cup \{\infty\}$ and for α and β the two maps from X to itself defined by

$$\alpha(x) = -\frac{1}{x}, \qquad \beta(x) = x - 2\lfloor x \rfloor - 1 \tag{13}$$

(with the obvious interpretations $\alpha(0) = \infty, \alpha(\infty) = 0, \beta(\infty) = \infty$). It is clear that α is an involution without any fixed point. The map β is also an involution (because if $x \in \mathbb{Q}$ has integer part n, then $\beta(x) = x - 2n - 1$ has integer part $-n - 1$, so $\beta(\beta(x)) = x - 2n - 1 - 2(-n - 1) - 1 = x$), and has no fixed points except ∞ (because if $x \in \mathbb{Q}$, then x and $\beta(x)$ differ by an odd integer). The map S defined in (1) is just the composite $\alpha \circ \beta$ of these two involutions. This makes it evident that S is a bijection, with inverse given by $P = S^{-1} = (\alpha \circ \beta)^{-1} = \beta^{-1} \circ \alpha^{-1} = \beta \circ \alpha$, explaining formula (8). The set $\mathcal{F} = \mathrm{Fix}(\alpha) \,\dot\cup\, \mathrm{Fix}(\beta)$ in this case consists of a single point $\{\infty\} = \mathrm{Fix}(\beta)$ (here $\mathcal{F}$ need not have even cardinality because X is not finite!), and the entire analysis given in Part I can be summarized as saying that the set $\mathbb{Q} \cup \{\infty\}$ consists of a single orbit under the action of the group generated by α and β, this orbit being a semi-infinite line starting at ∞ and proceeding by applying the two involutions alternatingly, as illustrated by the following picture.



(Note that while the straight line shows a bi-infinite orbit, the common orbit of α and β is semi-infinite starting at ∞.)

PART III. ON EULER'S CONJECTURE: A CAUTIONARY TALE

8. AN ILL-FATED CONJECTURE... In this last part of the paper (written, as already mentioned, by the third author alone some 25 years ago, and hence told in the first person), I will tell the story of the equation

$$z^4 = x^4 + y^4 + w^4 \tag{14}$$

[6]The reader may recognize a certain similarity to the proof of the famous Schröder-Bernstein theorem, stating that if any two sets A, B have an injection $\alpha\colon A \to B$ and an injection $\beta\colon B \to A$, then there is a bijection from A to B: This theorem is proved by considering iterated preimages of α and β and partitioning $A \,\dot\cup\, B$ into orbits.

and of my own encounter with it. This is a very famous Diophantine equation, because it was the subject of a conjecture of Euler's that survived for nearly a quarter of a millennium before finally being disproved. The story has both amusing and instructive aspects.

The origin of equation (14) is as follows. Euler knew of Fermat's famous "last theorem" asserting that no nth power of a positive integer is the sum of two nth powers of integers if $n > 2$, and had himself given a proof (although opinions differ today whether it was complete) of the correctness of this assertion for $n = 3$. Trying to "go Fermat one better," he conjectured that in fact an nth power can never be decomposed into the sum of fewer than n nth powers, i.e., that the equation

$$x_1^n = x_2^n + \cdots + x_n^n \tag{15}$$

has no non-trivial solutions in non-negative integers. This conjecture remained open until 1967, when Lander and Parkin found the counterexample

$$144^5 = 27^5 + 84^5 + 110^5 + 133^5 \quad (= 61\,917\,364\,224)$$

for $n = 5$ by a direct computer search (that can now be performed on a desktop computer in under 3 minutes). However, the seemingly simpler case of 4th powers still remained open for many years.

Actually, Euler's conjecture was not a very smart one (as the Japanese say, "even monkeys fall from trees!"), because a very simple probabilistic argument shows that it is likely to be false for every value of n. This argument goes as follows. Consider all n-tuples $(x_1, \ldots, x_n)$ of positive integers for which x_1 has exactly k decimal digits and each other x_i is less than x_1. The number of such n-tuples is of the order of 10^{nk} (more precisely, it is between $c_1 \cdot 10^{nk}$ and $c_2 \cdot 10^{nk}$ for some constants $c_2 > c_1 > 0$), and for each n-tuple the difference $x_1^n - x_2^n - \cdots x_n^n$ lies in the interval $[-(n-1)10^{kn}, 10^{kn}]$, whose length is also of the order of 10^{nk}, so unless something funny is going on, the expected number of n-tuples for which this difference is zero should be a positive number p depending on n but not on k. (Think of throwing 1 million marbles at random into 5 million holes; then the average number landing in each box box is $1/5$, and the expected number landing in any *given* box is the same number.) Letting k go to infinity, we see that the number of expected solutions of (15) should be infinite, but the set of these solutions should be very sparse, with the number of solutions having $\leq K$ digits growing only like some positive (and possibly quite small) multiple of K as $K \to \infty$. And this means two things: First, that we should *not* conjecture that (15) is insoluble, and second, that (if we have the good fortune to live in the pre-computer age) we should *not* attempt to find counterexamples by hand! This leads us to formulate the following.

First moral. If you are a number theorist, even a very great one, then you shouldn't make conjectures unless you not only have numerical evidence, but have thought about the heuristic aspects of your assertion!

9. ...AND AN ILL-FATED COUNTEREXAMPLE. My own contact with equation (14) was as follows. During the winter semester of 1986, when I was visiting the MSRI in Berkeley, I gave a semi-popular talk on Diophantine equations. After the talk, a man called de Vogelaere came up to me to ask whether I knew of or had ever thought about this equation and to explain to me the approach that he had been pursuing. Of course I knew the problem (it is discussed in the famous *Introduction to the Theory of Numbers* by Hardy and Wright, which I had received as a teenager and read until

my copy of it was falling apart), but I had never worked on it myself, and was very intrigued by the method he showed me.

De Vogelaere's basic idea was to simplify the problem by looking first at the easier equation

$$z^4 = x^4 + y^4 + t^2, \tag{16}$$

i.e., to replace the final fourth power in (14) by a "mere" square, to try to find as many solutions of this new equation as possible, and then to investigate the conditions making it possible or likely for t itself to be a square w^2, thus solving the original problem. A parametric solution (i.e., an infinite family of solutions given by polynomials)

$$(x^2 + x + 1)^4 = x^4 + (x + 1)^4 + (x^4 + 2x^3 + 3x^2 + 2x)^2 \tag{17}$$

of (16) had already been given by Escott in 1895, as de Vogelaere told me. It is more convenient to write this solution in homogeneous form as $z = u^2 + uv + v^2$, $x = uv$, $y = uv + v^2$ and $t = u^4 + 2u^3v + 3u^2v^2 + 2uv^3$, or in an abbreviated notation as $z = [1, 1, 1]$, $x = [0, 1, 0]$, $y = [0, 1, 1]$, $t = [1, 2, 3, 2, 0]$, and we will do this from now on. This particular solution of (16) can never lead to a solution of the original equation (14), because the Diophantine equation $w^2 = x^4 + 2x^3 + 3x^2 + 2x$ has no non-trivial rational solutions,[7] but de Vogelaere had found a lot of other parametric solutions of (16) of the same general type, the simplest two being

$$z = [9, 3, 3], \quad x = [8, 1, 1], \quad y = [4, -1, 2], \quad t = [47, 74, 49, 22, 8] \tag{18}$$

and (omitting t from now on, since it can be deduced from the others)

$$z = [33, 3, 3], \quad x = [17, 11, -2], \quad y = [8, 17, 1], \tag{19}$$

and one of the most complicated being

$$\begin{aligned} z &= [2\,577\,229\,375,\ -1\,371,\ 3\,525], \\ x &= [2\,232\,368\,805,\ 1\,861\,583,\ -2\,980], \\ y &= [968\,648\,234,\ 4\,964\,967,\ -1\,400]. \end{aligned} \tag{20}$$

Each of these solutions also had a "companion" with the same z and x but different y and t, e.g., $y = [7, 5, 2]$, $t = [8, -10, 31, 10, 8]$ for (18) or $y = [32, -1, -2]$ for (19).

De Vogelaere's question was whether his approach could be systematized and whether it could potentially ever lead to a solution of the original equation (14). Specifically, one would like to:

(i) show that there are infinitely many parametric solutions of (16) of Escott–de Vogelaere type;

(ii) find necessary constraints on the coefficients of the parametric solutions in order that the quartic polynomial $t(u, v)$ has a chance to take on a square value; and then

[7] *Proof* (for experts): Write the equation as $\eta^2 = (\xi + 1)(2\xi^2 + \xi + 1)$ with $\eta = w/x^2$ and $\xi = 1/x$, defining an elliptic curve E over $\mathbb{Q}$. The point $P = (0, 1)$ has order 4, and any solution has $\xi + 1 = \square$ or $\xi + 1 = 2 \cdot \square$, so has the form either $2Q$ or $2Q + P$ for some $Q \in E(\mathbb{Q})$. This proves that $E(\mathbb{Q})/2E(\mathbb{Q})$ injects into $\mathbb{Z}/2\mathbb{Z}$ and hence that $\mathrm{rank}(E) = 0$ and $E(\mathbb{Q}) \cong \mathbb{Z}/4\mathbb{Z}$.

(iii) sieve out the parametric solutions that fail to satisfy these conditions and test one or several of the surviving ones numerically to see if it yields a solution of (14).

During the next three or four months, I came back to these questions several times and was able to do parts (i) and (ii). The method and results are described below. At the end of my Berkeley stay, I went for a very memorable two-month visit to Moscow, where I continued to think about the problem and succeeded in doing part (iii) as well, finding (again, as described below) that the first two parametric solutions of (16) that had a chance of yielding square values of t had t-polynomials given by

$$t_1(u, v) = [184 \cdot 233^2, 320\,922 \cdot 233, 130\,661\,741, 320\,922 \cdot 313, 184 \cdot 313^2],$$

$$t_2(u, v) = [3\,697 \cdot 137^2, 2\,372\,652 \cdot 137, 573\,811\,862, 2\,372\,652 \cdot 193, 3\,697 \cdot 193^2].$$

It remained only to try some small integral values of u and v to see if either of these, or any of the further parametrizations on my list of possible candidates, ever gave rise to a square. But of course no computers were available to visitors in the Soviet Union at that time, and this was before the days when people had personal computers that they took with them on trips, so that all I had at my disposal was a Hewlett-Packard electronic calculator. It was programmable in BASIC, so I could write the simple loop to compute $t_1(u, v)$ for integers u and v going up to 100 in absolute value, but unfortunately the calculator could not display integers of more than 13 digits, and this bound was exceeded for u and v in the range in question. Of course I could have looked for pairs (u, v) with $\sqrt{t_1(u, v)}$ very near an integer, and then checked these cases by calculating modulo some moderate-sized integers or simply by multiplying everything out by hand, but I had no reason to think that there was any hurry or any reason to take so much trouble. Unfortunately, I was wrong: When I returned to Bonn at the end of my Moscow stay, I was met by my friend and collaborator Dick Gross, who told me excitedly that a famous question of Diophantine Analysis posed by Euler had just been solved by the very young mathematician Noam Elkies. I immediately went to the computer of our institute (a very primitive one indeed, but still a lot better than a pocket calculator!) to type in and run my own program, and within seconds discovered that $t_1(61, 5)$ was equal to $15\,365\,639^2$, leading to the explicit solution

$$20\,615\,673^4 = 18\,796\,760^4 + 2\,682\,440^4 + 15\,365\,639^4 \tag{21}$$

of (14), so that I too had solved Euler's problem. But it was too late: On a problem that had been open for well over two centuries, I had been scooped by just a few days. Needless to say, I immediately went out and bought a portable computer (a Toshiba) that thenceforth accompanied me everywhere. So we can formulate the following.

Second moral. If you are a number theorist, then buy a laptop, learn how to use it, and never leave home without it!

My solution and Elkies's were quite similar in essence, although rather different in presentation, and the numerical solution (21) also happened to be the same as the first solution produced by his method (even though a brute force computation by multiple computers running in parallel that was performed shortly afterwards revealed that it is in fact the second smallest integer solution, the smallest being $422\,481^4 = 414\,560^4 + 95\,800^4 + 217\,519^4$), so that in the end I did not publish my solution at that time. But since the method is quite pretty and reasonably elementary, and aroused interest in Bremen, I decided to include it, very belatedly, in the present paper.

10. QUADRICS TANGENT TO THE FERMAT QUARTIC. The key observation is that any three expressions x, y, z given as homogeneous quadratic polynomials in two variables u and v automatically satisfy a homogeneous quadratic equation $Q(x, y, z) = 0$. (*Proof*: Each of the six expressions x^2, y^2, z^2, xy, xz, and yz is a linear combination of the five monomials u^4, u^3v, u^2v^2, uv^3, and v^4, so there must be a linear relation between them.) The converse is true over $\mathbb{C}$ but not over $\mathbb{Q}$: If Q is a homogeneous quadratic polynomial with rational coefficients, the solutions of $Q(x, y, z) = 0$ can be given parametrically by three binary quadratic forms with rational coefficients if and only if there is at least one rational solution.[8]

In particular, each of the Escott–de Vogelaere parametric solutions of (16) corresponds to a quadratic relation, these relations for the four parametrizations (17), (18), (19), and (20) being

$$\begin{aligned} &x^2 + y^2 - xy + xz - yz = 0, \\ &5x^2 + 5y^2 + xy + 4z^2 - 7xz - 7yz = 0, \\ &13x^2 + 13y^2 - 17xy - 4z^2 + 7xz - 7yz = 0, \text{ and} \\ &4\,261\,205\,(x^2 + y^2 - xy) - 1\,763\,124\,(xy + z^2) \\ &\quad + 152\,303(yz - xz) = 0, \end{aligned} \tag{22}$$

respectively. Since these quadrics solve (16), they have the magic property

$$Q(x, y, z) = 0 \Longrightarrow z^4 - x^4 - y^4 \text{ is a square.} \tag{23}$$

This suggests breaking up our problem into three sub-problems.

1. What is the general form of the quadric Q satisfying (23)?
2. Of these, which have a rational solution (and hence lead to a parametric solution of (16) à la Escott or de Vogelaere)? Are there infinitely many?
3. Among the parametric solutions obtained, are there any for which t could be a square? Are there criteria to eliminate the others?

We discuss the first of these questions now, and the two others in §11 and §12.

Write F for the expression

$$F(x, y, z) = z^4 - x^4 - y^4 \tag{24}$$

so that $F = 0$ is the equation of the Fermat quartic curve in $\mathbb{P}^2$. Then equation (23) simply says that F is a square modulo Q, i.e.,

$$F(x, y, z) = R(x, y, z)^2 - Q(x, y, z)S(x, y, z) \tag{25}$$

for some polynomials $R(x, y, z)$ and $S(x, y, z)$, which by considerations of degree are seen to also be quadratic forms in x, y, z. In particular, for the Escott solution (17), with $Q = Q_0$ as in (22), this is given by

[8]This principle—that a quadratic equation with rational coefficients having one rational solution then has infinitely many (and can be described parametrically) goes back all the way to Diophantus. To prove this, let P be the given point with rational coordinates on the quadric (= set of solutions of the quadratic equation); then any line through P given by an equation with rational coefficients intersects the quadric in a second point with rational coordinates.

$$\begin{aligned} Q_0(x, y, z) &= x^2 + y^2 - xy + xz - yz, \\ R_0(x, y, z) &= z^2 - (x - y)^2, \\ S_0(x, y, z) &= 2(x^2 + y^2 - xy - xz + yz). \end{aligned} \tag{26}$$

But the expression $R^2 - QS$ is (up to a factor $1/4$) just the discriminant of the quadratic form $Q\xi^2 + 2R\xi\eta + S\eta^2$, and it is well known that this discriminant is invariant under the action of $SL_2(\mathbb{Q})$, i.e., under linear transformations of the form $(\xi\,\eta) \mapsto (\xi\,\eta)M$ where $M = \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right)$ is a 2×2 matrix with determinant $\alpha\delta - \beta\gamma = 1$. Hence, we can get infinitely many new solutions of (25) by applying arbitrary matrices

$$\left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right) \in SL_2(\mathbb{Q})$$

to the special solution (26). These take the form

$$\begin{aligned} Q(x, y, z) &= \alpha^2 Q_0 + 2\alpha\beta R_0 + \beta^2 S_0, \\ R(x, y, z) &= \alpha\gamma Q_0 + (\alpha\delta + \beta\gamma) R_0 + \beta\delta S_0, \\ S(x, y, z) &= \gamma^2 Q_0 + 2\gamma\delta R_0 + \delta^2 S_0. \end{aligned} \tag{27}$$

For the moment we are interested only in the formula for Q. We have proved the following.

Proposition 6. *Let $A, B, C \in \mathbb{Q}$ be given by*

$$A = \alpha^2 - 2\alpha\beta + 2\beta^2, \quad B = 2\alpha\beta, \text{ and } \quad C = \alpha^2 - 2\beta^2 \tag{28}$$

for two rational numbers α, β. Then the quadric

$$Q_{A,B,C}(x, y, z) = A(x^2 - xy + y^2) + B(xy + z^2) + C(xz - yz) \tag{29}$$

satisfies (23).

At this point the reader who is getting fatigued can—and is urged to—skip straight to Section 13, since Proposition 6 is the essence of the construction and the remaining arguments below, whose proofs will be given in a very abbreviated form, merely describe some refinements.

We observe first that the numbers A, B, C given by (28) satisfy

$$A^2 + 2AB - B^2 - C^2 = 0, \tag{30}$$

and conversely, all solutions of (30) are given (up to a constant multiple which is of no interest to us) by (28), so we could equally have formulated Proposition 6 by saying that, for any triple (A, B, C) satisfying (30), the quadric (29) has the property (23). We now show that we are not losing anything this way: Through any rational solution of (16) at least one of the quadrics $Q_{(A,B,C)}$ passes.

Proposition 7. *Any solution $(z, x, y, t) = (\zeta, \xi, \eta, \tau)$ of* (16) *satisfies $Q_{(A,B,C)}(\xi, \eta, \zeta) = 0$ for some rational A, B, C satisfying equation* (30).

Proof. Take

$$\begin{aligned} A &= (\xi^2+\zeta^2)(\eta^2+\zeta^2), \\ B &= -\xi\eta(\xi^2+\eta^2+\zeta^2-\xi\eta) - \tau\zeta(\xi-\eta), \text{ and} \\ C &= -\zeta(\xi-\eta)(\xi^2+\eta^2+\zeta^2) + \tau(\xi\eta+\zeta^2). \end{aligned} \tag{31}$$

Check that $Q_{(A,B,C)}(\xi, \eta, \zeta) = 0$ and that (30) holds. ∎

Since this proof is a little abrupt, we explain where equations (31) came from. Solving the desired equation $Q_{(A,B,C)}(\xi, \eta, \zeta) = 0$ (with $Q_{(A,B,C)}$ defined as in (29)) for C gives

$$C = \frac{A(\xi^2 - \xi\eta + \eta^2) + B(\xi\eta + \zeta^2)}{(\eta - \xi)\zeta}. \tag{32}$$

Substituting this equation into (30) gives a quadratic equation for the ratio $A : B$. The condition that this equation have a rational solution is that its discriminant is a square. By direct calculation, we find that the discriminant in question is (up to the square of a rational function of ξ, η, ζ) equal to the Fermat quartic $F = \zeta^4 - \eta^4 - \xi^4$. By assumption, this is a square, so the quadratic equation has a rational solution. Computing this solution $A : B$ by the high school formula and substituting for C from (32) gives equations (31).

Note for experts: We observe that property (23) has a geometrical interpretation as saying that the quadric $Q = 0$ in $\mathbb{P}^2$ (a genus 0 curve) and the Fermat quartic $F = 0$ in $\mathbb{P}^2$ (a genus 3 curve) are tangent (more precisely: have even intersection multiplicity) at all points of intersection, i.e., they are tangent at 4 points (some of which may coincide). Let $\widetilde{\mathbb{P}^2}$ be the double cover of $\mathbb{P}^2$ branched along $F = 0$ (i.e., the surface given by equation (16)) and $\widetilde{Q}$ the inverse image of Q in $\widetilde{\mathbb{P}^2}$. If Q and F were in general position, they would have 8 transverse intersection points and $\widetilde{Q}$ would be a double cover of $\mathbb{P}^1$ branched at 8 points (genus 3). The fact that Q and F are in fact tangent at four points says that $\widetilde{Q}$ is an unramified cover of Q, i.e., consists of two curves of genus 0; so if Q has a rational point, then so does each component of $\widetilde{Q}$, and this is the reason that we have a parametric solution of (16) over $\mathbb{Q}$.

11. EXISTENCE OF A RATIONAL POINT ON $Q = 0$. We now turn to the second question in §10, viz., the question when one of the quadrics (29) has a rational zero. We will give a necessary and sufficient condition for this and show that this condition is fulfilled infinitely often. We may assume that A, B, C are given by (28), since—as remarked before—any triple satisfying (30) looks like this up to a rational multiple.

Proposition 8. *Let $\alpha, \beta \in \mathbb{Q}$ and $Q = Q_{A,B,C}$ be the quadratic form defined in Proposition 6. Then $Q(x, y, z) = 0$ has a non-trivial rational solution if and only if each of the two numbers $A + B = \alpha^2 + 2\beta^2$ and $A - B = \alpha^2 - 4\alpha\beta + 2\beta^2$ is a sum of two (rational) squares.*

Proof. A famous theorem of Minkowski says that a quadratic equation $Q = 0$ with rational coefficients has a rational solution if and only if it has a real solution and a p-adic solution (or equivalently, a solution modulo p^n for all n) for all primes p. A result of Hilbert implies that it suffices to check only odd p. The discriminant of Q (given by

equations (28) and (29) with α and β chosen integral and coprime) is (up to sign and a power of 2) equal to $AB(A-B)(A+B)$, so we only have to worry about primes dividing this. One easily checks that if p is an odd prime dividing AB (i.e., $\alpha \equiv 0$ or $\beta \equiv 0$ or $\alpha \equiv (1+i)\beta \pmod{p}$ with $i^2 \equiv -1$), then $Q=0$ has a p-adic solution. If p divides $A+B=\alpha^2+2\beta^2$ to an odd power, then $Q \equiv \square - 2\cdot\square$, so $Q=0$ has a solution in the field $\mathbb{Q}_p$ of p-adic numbers if and only if 2 has a square root in this field, i.e., if $p \equiv \pm 1 \pmod 8$. But since $p|(\alpha^2+2\beta^2)$ also implies $p \equiv 1$ or $3 \pmod 8$, this congruence is equivalent to $p \equiv 1 \pmod 8$, and also to $p \equiv 1 \pmod 4$. Hence, we need that $\alpha^2+2\beta^2$ is a square or twice a square times a product of primes $\equiv 1 \pmod 4$, i.e., is a sum of two squares. Similarly, if $p^{\text{odd}}||(A-B)=(\alpha-2\beta)^2-2\beta^2$, then $Q=\square+2\cdot\square$, so $Q=0$ has a solution in $\mathbb{Q}_p \iff p \equiv 1$ or $3 \pmod 8 \iff$ (since $p \equiv \pm 1 \pmod 8$ anyway) $p \equiv 1 \pmod 4$. Also at the infinite place we find that $\alpha^2-4\alpha\beta+2\beta^2$ must be positive if Q is to be indefinite. Hence $\alpha^2-4\alpha\beta+2\beta^2$ is again (a square or twice a square times) a product of primes $\equiv 1 \pmod 4$, i.e., it is a sum of two squares. This proves the proposition. ∎

In Table 1 we tabulate all α and β satisfying

$$\alpha, \beta \in \mathbb{Z}, \quad \alpha > 0, \quad \alpha \text{ odd}, \quad \beta \text{ even}, \quad (\alpha, \beta) = 1 \tag{33}$$

and the criterion of Proposition 8 and with $\alpha^2+2\beta^2 \le 200$. For each α, β we give the numbers A, B, C defined by (28) and a non-trivial solution (ξ, η, ζ) of $Q_{(A,B,C)}(\xi, \eta, \zeta) = 0$ as promised by the proposition. Note that (33) involves no loss of generality: We can clearly assume that α and β are coprime integers with $\alpha > 0$ (since multiplying α and β by a rational number has no effect), and then we can assume α is odd because if α is even (and hence β odd) then replacing α, β by $\beta, \frac{1}{2}\alpha$ gives a new solution (it replaces A, B, C by $\frac{1}{2}A, \frac{1}{2}B, -\frac{1}{2}C$) with α odd; and once α is odd, β is automatically even since otherwise $\alpha^2+2\beta^2 \equiv 3 \pmod 4$ is not a sum of two squares.

Table 1. The first quadrics (29) having a rational zero (ξ, η, ζ)

	α	β	A	B	C	ξ	η	ζ
*	1	0	1	0	1	0	0	1
	1	2	5	4	−7	2	−1	3
	1	−2	13	−4	−7	2	−1	3
	1	6	61	12	−71	22	6	59
	1	−6	85	−12	−71	6	−2	7
	3	−2	29	−12	1	6	3	7
	3	−4	65	−24	−23	2	1	−3
	3	8	89	48	−119	12	−3	13
	3	−8	185	−48	−119	14	10	−27
*	5	−8	233	−80	−103	20	5	21
*	7	−4	137	−56	17	38	2	63
	7	−6	205	−84	−23	−30	3	55
	9	2	53	36	73	−6	2	7
	9	−4	185	−72	49	12	4	−13
	11	−6	325	−132	49	1056	924	1237

Proposition 9. *There are infinitely many ratios $\alpha : \beta \in \mathbb{Q}$ such that the quadric defined in Proposition 6 has a rational point.*

Proof. We use the proof of Proposition 7. Take one of the parametric families of solutions of (16), say Escott's solution (17). It gives infinitely many rational solutions (ξ, η, ζ, τ). For each of these, equations (31) give two quadrics of the form (29) passing through (ξ, η, ζ) (since we can take τ or $-\tau$ as the square root of $\zeta^4 - \xi^4 - \eta^4$). One of these is the quadric we started with, but the other is new, so we get infinitely many quadrics of the required form having at least one rational point. This proves the proposition. ∎

We get an actual formula by applying the above procedure to Escott's solution (17); this gives, after some calculation,

$$\begin{aligned} A &= [1, 4, 12, 22, 31, 30, 20, 8, 2], \\ B &= [0, 0, -2, -6, -12, -14, -10, -4, 0], \\ C &= [-1, -4, -10, -16, -15, -8, 2, 4, 2], \end{aligned} \tag{34}$$

(the notation is as before, so these are homogeneous polynomials of degree 8, $A = u^8 + 4u^7v + \cdots + 2v^8$, etc.). This can be checked by brute force to satisfy (30) and the condition $Q_{(A,B,C)}(uv, uv + v^2, u^2 + uv + v^2) = 0$, and it fulfills the criterion of Proposition 8 because

$$A + B = [1, 1, 1]^4 + [0, 1]^8, \quad A - B = [1, 2, 5, 4, 1]^2 + [0, 0, 0, 2, 1]^2.$$

12. ELIMINATING UNPRODUCTIVE PARAMETRIC SOLUTIONS. We now study the quadrics Q given by (28) and (29) with (α, β) satisfying the condition of Proposition 8. The first 15 pairs are given in Table 1. Assume we have found a solution of $Q(\xi, \eta, \zeta) = 0$ (e.g., by trial and error; explicit solutions are given in Table 1 for each pair listed there). Then the parametric family à la Escott–de Vogelaere can be given by

$$\begin{aligned} x &= [A\xi, C(\eta - \xi) - 2B\zeta, (B - A)\eta], \\ y &= [A\eta, -C(\eta - \xi) + 2B\zeta, (B - A)\xi], \text{ and} \\ z &= [A\zeta, (B - 3A)(\eta - \xi) + 2C\zeta, (A - B)\zeta]. \end{aligned} \tag{35}$$

(To obtain these formulas, make the values corresponding to $v = 0$ and $u = 0$ proportional to the known solutions (ξ, η, ζ) and $(\eta, \xi, -\zeta)$, and then solve for the middle coefficients; we suppress the details.) The corresponding value of the polynomial $t = t(u, v)$ is

$$t = [A^2\lambda, A\mu, \nu, (A - B)\mu, (A - B)^2\lambda], \tag{36}$$

where

$$\begin{aligned} \lambda &= \zeta^2 - (\xi - \lambda)^2 + \frac{2B}{A + B - C}(\xi^2 - \xi\eta + \eta^2 + \xi\zeta - \eta\zeta) \\ &= \frac{A - B}{C}(\xi^2 - \xi\eta + \eta^2) - \frac{A + B}{C}(\xi\eta + \zeta^2), \end{aligned} \tag{37}$$

$$\begin{aligned} \mu &= 2(B + A)(\xi^2 + \xi\eta + \eta^2) + 2(B - 2A)\zeta^2, \text{ and} \\ \nu &= C(A - B)(\xi^2 + \eta^2) + 2C(A + B)\xi\eta + 2C(2B - 3A)\zeta^2 \\ &\quad - 4(2A^2 - 2AB + B^2)\zeta(\xi - \eta). \end{aligned} \tag{38}$$

(This can be obtained from $t = R$ in (27), with x, y, z substituted from (35) and γ, δ most conveniently chosen to be $0, \alpha^{-1}$.)

We are interested in those values of $\alpha : \beta$ for which (36) can be a square or the negative of a square. Here we have the following criterion, analogous to Proposition 8.

Proposition 10. *In order for the family of solutions associated to* (α, β) *to have an element with* $t = \pm\square$*, it is necessary that* $A = \alpha^2 - 2\alpha\beta + 2\beta^2$ *and* $A + 2B = \alpha^2 + 2\alpha\beta + 2\beta^2$ *(as well as* $A + B = \alpha^2 + 2\beta^2$ *and* $A - B = \alpha^2 - 4\alpha\beta + 2\beta^2$*) contain no odd prime* $\not\equiv 1 \pmod 8$ *to an odd power.*

Proof. This is similar to Proposition 8, so we only sketch it. If p is an odd prime dividing $\alpha^2 - 2\alpha\beta + 2\beta^2$ to an odd power, then $\alpha/\beta = 1 + i$ with $i^2 \equiv -1 \pmod p$ (so p must be $\equiv 1 \pmod 4$). Then the Q and R of (27) are given by

$$Q \equiv (2 + 2i)(\xi^2 - \xi\eta + \eta^2) + (2i - 2)(\xi\zeta - \eta\zeta),$$
$$R \equiv i(\xi^2 - \xi\eta + \eta^2) + (\zeta^2 + \xi\eta) + (1 + i)(\xi\zeta - \eta\zeta),$$

and therefore

$$Q - 2R \equiv -2i(\xi - \eta - i\zeta)^2.$$

Hence a solution of $Q = 0, R = \square$ is possible only if i is a square (mod p), i.e., if $p \equiv 1 \pmod 8$. Similar arguments apply for $p \mid \alpha^2 + 2\alpha\beta + 2\beta^2$. ∎

13. SEARCHING FOR SOLUTIONS OF $z^4 = w^4 + x^4 + y^4$. Of the 15 pairs in Table 1 satisfying the criteria of Proposition 8, only the three marked with an asterisk satisfy the extra criteria of Proposition 10. The first of these corresponds to the Escott parametrization (17), which we have already seen does not lead to a solution of (14). Substituting from (35)–(37), we find that the parametric solutions of (16) corresponding to the other two pairs are (x_1, y_1, z_1) and (x_2, y_2, z_2) with

$$x_1 = [20 \cdot 233,\ 4\,905,\ -5 \cdot 313], \qquad x_2 = [38 \cdot 137,\ 6\,444,\ -2 \cdot 193],$$
$$y_1 = [5 \cdot 233,\ -4\,905,\ -20 \cdot 313], \qquad y_2 = [2 \cdot 137,\ -6\,444,\ -38 \cdot 193],$$
$$z_1 = [21 \cdot 233,\ 7\,359,\ 21 \cdot 313], \qquad z_2 = [63 \cdot 137,\ 18\,954,\ 63 \cdot 193],$$

and with the t-polynomials $t_j = t_j(u, v)$ already given in §9. As already mentioned there, a direct search yields the solution $t_1(61, 5) = 15\,365\,639^2$, leading to the solution (21) of Euler's equation (14),[9] while the equations $t_2(u, v) = \pm w^2$ have no solutions with $0 < \max(|u|, |v|) \le 500$. Extending Table 1 to the larger search limit $\alpha^2 + 2\beta^2 \le 1000$ (rather than ≤ 200) gives six further pairs $(\alpha, \beta) = (1, -20)$, $(5, 12)$, $(9, -20)$, $(15, -8)$, $(25, 4)$ and $(27, -8)$ satisfying the criteria of both Proposition 8 and Proposition 10. (This shows the usefulness of these criteria, which get us down to only 9 candidates out of 451 pairs (α, β) in this search range satisfying (33).) The third of these gives the parametric solution

[9] This will then lead to infinitely many further solutions of (14), since the point $(61/5, 15365639/25)$ on the elliptic curve $Y^2 = t_1(X, 1)$ has infinite order and hence gives infinitely many further solutions by repeatedly applying the well-known duplication process of Diophantus and Fermat.

$$x_3 = [395, 1599, 160],$$
$$y_3 = [580, 809, -711],$$
$$z_3 = [1\,029, 249, 889],$$
$$t_3 = [-991\,784, -30\,058, -538\,587, 1\,513\,022, 606\,960],$$

of (16). The polynomial $t_3(u, v)$ has the square value $t_3(13, 15) = 217\,519^2$, leading to the minimal solution of (14) that was already given in §9.

REFERENCES

1. M. Aigner, G. M. Ziegler, *Proofs from the Book*, fourth edition, Springer-Verlag, Heidelberg, 2010.
2. N. Calkin, H. S. Wilf, Recounting the rationals, *Amer. Math. Monthly* **107** 4 (2000) 360–363, available at http://dx.doi.org/10.2307/2589182.
3. N. Elkies, On $A^4 + B^4 + C^4 = D^4$, *Math. Comp.* **51** 184 (1988) 825–835.
4. D. E. Knuth, Problem 10906, *Amer. Math. Monthly*; solution by M. Newman, *Amer. Math. Monthly* **110** 7 (2003) 642–643, available at http://dx.doi.org/10.2307/3647762.
5. D. H. Lehmer, On Stern's diatomic series, *Amer. Math. Monthly* **36** 2 (1929) 59–67, available at http://dx.doi.org/10.2307/2299356.
6. M. A. Stern, Ueber eine zahlentheoretische Function, *J. Reine Angew. Mathematik* **55** (1858) 193–220, available at http://dx.doi.org/00754102.
7. D. Zagier, A one-sentence proof that every prime $\equiv 1 \pmod 4$ is a sum of two squares, *Amer. Math. Monthly* **97** 2 (1990) 144, available at http://dx.doi.org/10.2307/2323918.

AIMERIC MALTER is a high school student in Bremerhaven, Germany. At age 13, he was the youngest participant at the International Mathematical Summer School for Students in Bremen in 2011. He enjoyed the presentations and the interesting people he met there and hopes to be invited again in the future. One of the talks by Don Zagier inspired him to carry out a research project for the German student competition "Jugend forscht," where he won the first prize on the junior level. One year after the summer school, he completed the mathematics part of the high school curriculum. Aimeric likes to go swimming, indoors and outdoors.
Azaleenweeg 16, D-27578 Bremerhaven, Germany
frenchgott@live.de

DIERK SCHLEICHER is professor of mathematics at Jacobs University Bremen. Much of his research is on dynamical systems, especially the theory of iteration and complex dynamics. He enjoys the international spirit in mathematical research; before and after his Ph.D. at Cornell University, he spent longer periods of time at Princeton, Berkeley, Paris, München, Toronto, and Providence, and many shorter ones in Russia and elsewhere. One of his main professional goals is to bring together leading mathematicians of today and tomorrow, for instance by organizing events such as the 50th anniversary of the International Mathematical Olympiad, and of course summer schools such as the one that brought together his co-authors Don and Aimeric. In his free time, he enjoys outdoor activities such as kayaking, sailing, paragliding, and outdoor swimming.
Research I, Jacobs University, Postfach 750 561, D-28725 Bremen, Germany
dierk@jacobs-university.de

DON ZAGIER is a scientific member and director of the Max Planck Institute for Mathematics in Bonn and professor of number theory at the Collège de France in Paris. His mathematical interests center around number theory (especially the theory of modular forms) and its applications in topology, algebraic geometry, and mathematical physics, but he is happy to work on any problem that involves enough computation. Having lived in more than half a dozen countries, and having fallen in love with mathematics and gone through school and university at a very early age, he too is very enthusiastic about activitues that encourage the love of mathematics in young students and that bring together people from different countries. His main hobbies are languages and piano; his favorite sports, skiing and sudoku.
Max Planck-Institut für Mathematik, Vivatsgasse 7, D-53111 Bonn, Germany,
and Collège de France, 3 rue d'Ulm, 75005 Paris, France
don.zagier@mpim-bonn.mpg.de