Questions about Powers of Numbers

Barry Mazur

Number theory has quite a few famous ancient and modern problems that can be asked in not too technical, almost premathematical, language:

- questions about prime numbers and their "placement" among all numbers (e.g., the Goldbach conjecture, the twin prime conjecture, the "Schinzel hypothesis" predicting when there are an infinite number of prime number values of a given polynomial, etc.);

and also

- questions about the behavior of the sets of "perfect powers" under simple arithmetic operations.

It is this second type of question that we will be discussing here as a way of introducing some basic issues in contemporary number theory. More specifically, we want to stay on the level of fairly elementary mathematics, holding back from any specific discussion of advanced topics (e.g., the arithmetic theory of elliptic curves, and modular forms), and to give, nevertheless, a hint of why certain constructions "coming from" the theory of elliptic curves (see the "quadratic and sextic transfers" below) find a very natural place in the study of problems involving integers. We will also see why the Mordell Equation, $y^2 + x^3 = k$, plays a pivotal role. At the same time, I hope this article serves as an elementary introduction to the still unresolved "*ABC*-Conjecture" due to Masser and Oesterlé. It also gives a pretext for asking related questions (called "(a, b, c)-questions" below), many of which have not yet been treated in the literature and for which, perhaps, the "circle method" may provide at least partial answers.[1]

Barry Mazur is professor of mathematics at Harvard University. His e-mail address is mazur@math.harvard.edu.

Problems about Perfect Powers

A *perfect power* is the n-th power of an integer for some natural number $n > 1$. These have attracted attention from the earliest times, beginning with perfect squares, which arise in the Pythagorean Theorem, applied to right-angle triangles all three of whose sides are integral multiples of a given unit. Of course, perfect squares arise in other ways as well; consider Fibonacci's reflection in the translation [F] of his treatise on perfect squares, *Liber Quadratorum*, in 1225:

> I thought about the origin of all square numbers and discovered that they arise out of the increasing sequence of odd numbers; for the unity is a square, namely 1; to this unity is added 3, making the second square, namely 4, with root 2; if the sum is added to the third odd number, namely 5,....

There is no end of famous problems regarding the most simple-seeming questions of placement of perfect powers, and sums of them, on the number line:

- **Fermat**. For $n > 2$ the sum of two n-th powers is never an n-th power.

[1] *The circle method, a powerful Fourier analytic technique designed for applications to number theory, will occasionally be alluded to in this article but will not be discussed in detail; the reader need not know about the circle method to understand the article.*

- **Catalan**, 1844 (cf. [R], [B2]). The numbers 8 and 9 are the only consecutive perfect powers.
- **Waring Problems**. This is a host of problems having to do with the number of ways an integer can be written as a sum of k "perfect" n-th powers. One does not have to go far to come to an unsolved problem among these Waring problems. For example, it is guessed that any integer not congruent to 4 or 5 modulo 9 can be expressed as a sum of three cubes, but to tackle such a question seems to be out of range of any of the available techniques.

Also, there is the problem (at first glance, it is somewhat curious to single this problem out!) of finding for any fixed integer k all integral solutions (x, y) to the **Mordell Equation**

$$Y^2 - X^3 = k,$$

where x and y are relatively prime integers.

What do we know about these problems?

As for Fermat's Last Theorem, we now have a proof of it, thanks to the celebrated efforts of Wiles (1995).

In the direction of the Catalan Problem, we know, thanks to a 1976 paper by Tijdeman [T], who used Baker's theory of lower bounds for nonvanishing linear forms in logarithms [B1], that there is only a *finite* set of pairs of consecutive perfect powers. By work of Langevin, an upper bound for a perfect power whose successor is also a perfect power can be computed from Tijdeman's proof to be

$$e^{e^{e^{e^{730}}}}.$$

As for the Mordell Equation, a general theorem of Siegel (1929) guarantees that for a given nonzero integer k the equation has only a finite number of integral solutions (as does any affine curve of genus > 0 over the ring of integers). Moreover, much explicit work has been done toward finding concretely the solutions for given values of $k < 100,000$ (cf. [G-P-Z]).

But, for the moment, let me say that this Mordell Equation, special as it may seem, is a central player in the Diophantine drama and in a certain sense "stands for" the arithmetic theory of elliptic curves. One of the objects of this article is to give hints about why the Mordell Equation plays this central role. The proposition in the last section of the article gives one relationship of the kind we have in mind.

If one views each of the problems above as "Diophantine", i.e., as the problem of finding integral solutions to specific algebraic equations, one is struck by how specific indeed these equations are. To emphasize the point, I will label all of these problems about perfect powers as **sharp Diophantine problems**. To nudge ourselves towards a more flexible type of problem that still carries much of the flavor of the ones we have reviewed, why not generalize somewhat the notion of "perfect power" and deal instead with integers possessing comparatively large perfect power divisors? We will make this notion precise below and then formulate what I want to call **rounded Diophantine problems**. I have two reasons for doing this.

My main reason for considering this kind of generalization is that it is a leisurely way of getting some intuition for, and appreciation of, the recent *ABC*-conjecture due to Masser and Oesterlé. The current view of this conjecture is that it lies at the core of arithmetic. Nevertheless, it has the simplicity of any one of the grand "direct" unlearned questions about numbers.

A second reason for the generalization of "perfect power" comes from thinking about the circle method, which is the key technique that is brought to bear on Waring-type problems: this method has the disturbing feature (disturbing, at least, to people like me who are not expert in it) of *not really caring about the particular nature of the equation it is solving*. It would seem that all one has to "tell" the circle method in order to get it going is the degree of an equation, the number of variables involved, and the codimension of its singularity locus. Perhaps, then, the circle method, applied to problems about perfect powers, is also effective in estimating the number of solutions to some problems having to do with integers possessing comparatively large perfect power divisors. We will formulate below such problems, which have the further advantage that they can be stated in relatively nontechnical language.[2]

Powered Numbers

Motivated by the use of the term *radical* in ring theory, one defines the **radical** of a nonzero integer N, denoted $\mathrm{rad}(N)$, as the product of all the prime divisors of N; so $\mathrm{rad}(-1) = 1$, $\mathrm{rad}(24) = 6$, etc.

Definition. For N an integer other than 0 and ± 1, the **power function** of N, denoted $P(N)$, is the real-valued function

$$P(N) = \frac{\log |N|}{\log \mathrm{rad}(N)}.$$

It is reasonable to simply convene $P(\pm 1) := \infty$ so that the power function is defined for all nonzero integers. We have that $P(N) \geq 1$ and, for $N > 1$, $P(N) = 1$ if and only if N is "squarefree", i.e., if and only if N is not divisible by any perfect square > 1. If N is a perfect n-th power, we have that $P(N) \geq n$.

[2] *Nevertheless, they are reminiscent of the constellation of more precise (but quite technical) conjectures predicting the asymptotics of rational points of bounded height in varieties with ample anticanonical bundle—work initiated by Manin and continued by Batyrev, Franke, Peyre, Strauch, and Tschinkel.*

For $a > 1$ a real number, by an **a-powered number** let us mean a nonzero integer N with $P(N) \geq a$. We will want to study the properties of the set of a-powered numbers—the "placement" of these sets among all integers, the behavior of these sets under simple arithmetic operations.

As a way of introduction, let us first answer the question of "how many" integers N there are with $P(N) = 1$. More exactly, for a positive real number X let $Sq.free(X)$ denote the number of squarefree integers N in the interval $1 < N < X$. How fast does $Sq.free(X)$ tend to ∞ with X?

The answer, which involves a small piece of "sieve theory" (legacy of Eratosthenes), has been known for quite a while, and I will review the basic idea behind it. The first step in setting up our sieve is to arrange "in a line" all the integers N in the range $1 < N < X$. There are roughly X of them. Next, so as not to get confused by too many numbers appearing in our calculation, let us rename the prime numbers as $p_1, p_2, \ldots$ in increasing order, so that, in fact, p_1 is the prime number 2; p_2 is, in fact, the prime number 3, etc. We will be sifting our set of natural numbers

$$1, 2, \ldots, N, \ldots < X$$

using a series of sieves with ever finer meshes; we will see what these are in a moment. The set of integers that remain after this process will be precisely the squarefree integers. The *first sieve* allows only those integers that are *not* divisible by the square of the first prime number, i.e., by p_1^2, to remain in our set. That is, we cross off all integers N in our set that are divisible by p_1^2 (= 4). This is a good thing to do, for surely none of these N's are squarefree. After having crossed these off, we are left with roughly $X - X/p_1^2 = \left(1 - \frac{1}{p_1^2}\right) \cdot X$ remaining integers in our set. Taking this once-sifted set of roughly $\left(1 - \frac{1}{p_1^2}\right) \cdot X$ integers, we now want to subject it to our *second sieve*, where we cross off those integers N that are divisible by the square of the second prime number, i.e., divisible by p_2^2(= 9), for, again, surely none of these N's are squarefree. Let us estimate how many integers now remain. One finds that at this stage, after numbers divisible by p_1^2 and p_2^2 are crossed off the set of all integers from 1 to X, roughly $\left(1 - \frac{1}{p_1^2} - \frac{1}{p_2^2} + \frac{1}{(p_1 p_2)^2}\right) \cdot X$ integers remain. The point here is that if we had not included the third term, $+\frac{1}{(p_1 p_2)^2}$, we would have (erroneously) counted *twice* "as removed" all the integers N that are divisible by $(p_1 p_2)^2$—the first time because N is divisible by p_1^2 and a second time because N is divisible by p_2^2. Here we have quietly used the fact that if an integer is divisible by p_1^2 and by p_2^2, then it is also divisible by $(p_1 p_2)^2$.

Since

$$\left(1 - \frac{1}{p_1^2} - \frac{1}{p_2^2} + \frac{1}{(p_1 p_2)^2}\right) \cdot X = \left(1 - \frac{1}{p_1^2}\right)\left(1 - \frac{1}{p_2^2}\right) \cdot X,$$

we can see the pattern that is emerging. Sifting over all primes p that could possibly contribute to a square factor in an integer of size $< X$, i.e., over all prime numbers p such that $p^2 \leq X$, we get

$$Sq.free(X) = \prod_{p=2,3,\ldots} \left(1 - \frac{1}{p^2}\right) \cdot X + \text{Error term},$$

where the product is over all the prime numbers p with $p^2 \leq X$. Of course, this is meaningless unless we can control the error term. To give the answer in a clean form, we observe that the product $\prod_{p=2,3,\ldots} \left(1 - \frac{1}{p^2}\right) \cdot X$ does not change much in comparison with X if we simply extend the product over all prime numbers p rather than stopping when $p^2 \leq X$. A standard calculation gives that the "Error term" is bounded in absolute value by a constant times $\sqrt{X}$, as X tends to ∞. This gives us

$$Sq.free(X) = \prod_{p \text{ prime}} \left(1 - \frac{1}{p^2}\right) \cdot X + O(\sqrt{X}).$$

Now it is time to recall two wonderful equalities of Euler:

$$\frac{\pi^2}{6} = \sum_{n=1}^{\infty} \frac{1}{n^2} = \prod_{p \text{ prime}} \frac{1}{\left(1 - \frac{1}{p^2}\right)}.$$

These give us, as a final answer,

$$Sq.free(X) = \frac{6}{\pi^2} \cdot X + O(\sqrt{X}) = 0.6079 \cdot X + O(\sqrt{X}).$$

Speaking loosely, the chances are six in ten that a given integer is squarefree.

Question. If one works with the ring of polynomials in one variable t over a field rather than with the ring of integers, it is a very rapid calculation to determine, for a given polynomial $f(t)$, whether or not f is squarefree, the necessary and sufficient condition being that the greatest common divisor of f and its derivative be 1. Is there an algorithm to determine whether a rational integer is squarefree that is asymptotically any quicker than just factoring the integer?

For real numbers $a \geq 1$ and X let $S(a; X)$ denote the number of integers $1 \leq N < X$ such that $P(N) \geq a$, i.e., the number of a-powered numbers less than X. As Andrew Granville explained to me, an easy argument gives that for fixed $a \geq 1$ and for any $\epsilon > 0$ we have

$$X^{1/a-\epsilon} < S(a;X) < X^{1/a+\epsilon}$$

as X tends to ∞. We will abbreviate this type of estimate as $S(a;X) \approx X^{1/a}$, emphasizing that $S(a;X)$ grows very roughly like $X^{1/a}$. This is a good thing for us insofar as $X^{1/a}$ is also the rate of growth of "perfect a-th powers"; i.e., by generalizing from "perfect a-th powers" to "a-powered numbers" we have not, at least, changed the rough asymptotics.

Linear Relations among Powered Numbers

We are now ready to raise a rounded Diophantine question that has at least a remote connection to each of the problems in our illustrative list. Fix real numbers $a, b, c \geq 1$, and another real number X. Consider the set $S(a,b,c;X)$ of triples (A,B,C) of relatively prime nonzero integers whose sum is zero, such that $|A|, |B|, |C| < X$ and such that

$$P(A) \geq a, \quad P(B) \geq b, \quad P(C) \geq c;$$

i.e., A is a-powered, B is b-powered, and C is c-powered.

(a,b,c)-Question. How fast can we expect the cardinality of the set $S(a,b,c;X)$ to grow, if at all, for fixed $a, b, c \geq 1$ and X tending to ∞?

Here is the typical "secret calculation" that is popular to make to come up with an "expected rate of growth" in this circumstance. But it is unlikely that one could come up with a *proof* that these asymptotics are correct just by pursuing the argument that we will give!

Ignoring for the moment the requirement that A, B, C be relatively prime and that they sum to 0 and remembering that the A's are chosen from a set of roughly $X^{1/a}$ elements, the B's from a set of roughly $X^{1/b}$ elements, and similarly for the C's, we have roughly $X^{1/a+1/b+1/c}$ triples (A,B,C) with the requisite lower bounds on their power functions. The requirement that A, B, C be relatively prime should not change the asymptotics, but the requirement that they sum to 0 should. The expression $|A+B+C|$ is bounded by a constant (3, in fact) times X, and so the "chances" that the sum be zero (provided that no other mitigating large effect has been ignored—an important proviso) is inversely proportional to X; call it X^{-1}. Feeding all this information into our calculation, we might then be led to "expect"[3] that the cardinality of $S(a,b,c;X)$ is comparable to $X^{1/a+1/b+1/c-1}$.

How do we interpret this "expectation"? Let us refer to $d := 1/a + 1/b + 1/c - 1$ as the **basic exponent** of our problem. Clearly our expectations are quite different depending upon the two cases:

$$d < 0 \quad \text{and} \quad d \geq 0.$$

[3] *The heuristic calculation we have outlined to get "expected asymptotics" can be altered to fit a number of other related problems, but of course it never provides any logical justification for the answers it yields!*

Aside. This dichotomy is the straight analogue for these rounded Diophantine questions of the distinction in the theory of Riemann surfaces of the genus of the surface being ≥ 2 or ≤ 1: in Riemannian or Kahlerian geometry it is the analogue of the distinction between *hyperbolic and nonhyperbolic* or between spaces that are negatively curved and those that are not; in algebraic geometry it is the distinction between having the canonical line bundle *ample* or not.

Let us consider each of the cases separately.

When the Basic Exponent d Is Nonnegative

Question ($d \geq 0$). If the basic exponent d is positive, i.e., if

$$1/a + 1/b + 1/c > 1,$$

does the cardinality of $S(a,b,c;X)$ tend to ∞ as X grows; and, more specifically, if $d \geq 0$, does it admit the asymptotics

$$\text{card } S(a,b,c;X) \approx X^d \ ?$$

The answer to the question is not known in full generality. To answer this question affirmatively would break naturally into two tasks: showing that $X^{d+\epsilon}$ is an upper bound (for sufficiently large X) and showing that $X^{d-\epsilon}$ is a lower bound. The problem of showing $X^{d-\epsilon}$ to be a lower bound is in the spirit of recent work proving that certain polynomial equations have many solutions. We will give examples of such theorems later. But here is some vocabulary to talk about the lower-bound aspect of this conjecture. Let $S(a,b,c)$ be the set of all solutions, i.e., the union of all $S(a,b,c;X)$. Suppose we are given a subset $\mathcal{A}(a,b,c) \subset S(a,b,c)$ of solutions, with $d = 1/a + 1/b + 1/c - 1$ positive. Let us say that $\mathcal{A}(a,b,c)$ is an **ample set of solutions** if it has at least the expected asymptotics, that is, if

$$\left| \left\{ (A,B,C) \in \mathcal{A}(a,b,c) \;\middle|\; \begin{array}{l} |A| \leq X, \\ |B| \leq X, \\ |C| \leq X \end{array} \right\} \right| \ > \ X^{d-\epsilon},$$

for any positive ϵ and for sufficiently large X.

Now there are two facts worth mentioning before we get any further into the discussion. The first is the curious fact that for some of the cases where a, b, c are all integers with $d > 0$ (we will enumerate all these cases below) there exists a *single* Diophantine equation involving perfect powers whose solutions already provide ample sets of solutions to the rounded (a,b,c)-question. The second is that there is a curious malleability in (a,b,c)-questions that enables one to convert ample sets of solutions for certain (a,b,c)-questions to ample sets for (a',b',c')-questions. We will examine these issues below.

When a, b, c Are Natural Numbers and $d > 0$

Here we get lots of (a, b, c')-solutions when $d > 0$ for c' arbitrarily close to c from single Diophantine equations, for example:

$$x^a + y^b = Ez^c$$

for E a specific nonzero integer.

The full list of natural-number triples (a, b, c) with $a \le b \le c$ and $d \ge 0$ is given in the following table.

a	b	c	d
1	$*$	$*$	$*$
2	2	$*$	$*$
2	3	3	1/6
2	3	4	1/12
2	3	5	1/30
2	3	6	0
3	3	3	0

It is interesting to try to find ample sets of solutions, as defined above (coming from a single Diophantine equation), for the entries with $d > 0$. For example, one might consider the second line of the table and try to prove that there are ample sets of $(2, 2, c)$-solutions coming from solutions to the Diophantine equation

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

alone. In the particular case where $c = 2$, the Pythagorean triples alone form an ample set.

For a discussion of Diophantine equations relevant to the above table, one can consult [D-G]. (In view of the proposition at the end of this article, the next-to-last entry of the above table is particularly worth thinking about!)

The (a, b, c)-Question for Small Values of a, b, c

Trevor Wooley informs me that by means of the circle method he can give an affirmative answer to the (a, b, c)-question when $a, b, c \le 6/5$.

The (a, b, c)-Question for Negative d

Here we return to our original "secret calculation" to ponder what the calculation might be saying when it predicts asymptotics of $X^{d\pm\epsilon}$ for $d < 0$. The easy guess is that for a triple (a, b, c) with $d < 0$ we might hope for

Conjecture *((a, b, c)-Conjecture). If $1/a + 1/b + 1/c < 1$, then there are, in total, only finitely many triples A, B, C of relatively prime nonzero integers with sum zero such that*

$$P(A) \ge a, \quad P(B) \ge b, \quad P(C) \ge c.$$

But let us be more ambitious.

Conjecture *(Uniform Conjecture for Negative d). Let d_0 be any negative real number. There are, in total, only finitely many triples A, B, C of relatively prime nonzero integers with sum zero such that*

$$P(A) \ge a, \quad P(B) \ge b, \quad P(C) \ge c,$$

with

$$d = 1/a + 1/b + 1/c - 1 \le d_0 < 0.$$

Aside. Both the (a, b, c)-Conjecture and the Uniform Conjecture for Negative d have the current status of having been verified in *no* case. The Uniform Conjecture implies, of course, the (a, b, c)-Conjecture for any triple (a, b, c) with negative d. The Uniform Conjecture is, in turn, implied by Masser-Oesterlé's "official" ABC-Conjecture.[4] But even before we get to the "official" conjecture, here are some implications of the conjectures we have already formulated.

(1) The (a, b, c)-Conjecture with $a = 2$, $b = 3$, and $c = 1000$ implies that there are only finitely many solutions to the Catalan problem. In fact, one can take c to be any real number > 6. To see this implication, first note that given a solution to the Catalan problem, i.e., if we are given two consecutive perfect powers $v^n = u^m \pm 1$ arranged so that $2 \le m \le n$, we have that $n \ge 3$. Then recall that the power function of the integers ± 1 is $\infty > 1000$, so that a solution to the Catalan Problem gives a triple of integers with sum zero having greatest common divisor equal to 1 for which the power function takes values greater than or equal to 2, 3, and 1000 respectively.[5]

(2) By similar reasoning, the (a, b, c)-Conjecture for *any* particular choice of (a, b, c) with $d < 0$ implies that there are only finitely many exponents n for which the Fermat Equation

$$X^n + Y^n = Z^n$$

has nontrivial solutions. Here "nontrivial" has the usual meaning: $XYZ \ne 0$.[6]

(3) Fix a triple of nonzero integers (U, V, W) and consider the generalized Fermat Equation of exponent $n \ge 0$ given by

$$UX^n + VY^n + WZ^n = 0.$$

The (a, b, c)-Conjecture for *any* particular choice of (a, b, c) with $d < 0$ implies that there are only finitely many exponents n for which the generalized

[4] *In my opinion, the Uniform Conjecture provides some immediate motivation for the ABC-Conjecture.*

[5] *Of course, as we have already remarked, we know the conclusion of statement (1) without using any conjecture, thanks to the work of Tijdeman [T], but the point of the exercise is simply to emphasize the strength of the assertions made by (a,b,c)-type conjectures.*

[6] *Again, of course, we now know the conclusion of statement (2) with greater precision, thanks to the work of Wiles.*

Fermat Equation of exponent n has solutions with X, Y, Z all of absolute value greater than 1.[7]

The "Official" ABC-Conjecture

By an ABC-**solution** let us mean a triple of nonzero relatively prime integers (A, B, C) whose sum is zero. Define the **power** $P(A, B, C)$ of an ABC-solution (A, B, C) to be

$$P(A, B, C) = \frac{\log \max(|A|, |B|, |C|)}{\log \operatorname{rad}(ABC)}.$$

***Conjecture** (Masser-Oesterlé's ABC-Conjecture). For any real number $\eta > 1$ there are only finitely many ABC-solutions with power $P(A, B, C) \geq \eta$.*

Masser-Oesterlé's ABC-Conjecture implies the Uniform Conjecture for Negative d. Conversely, the Uniform Conjecture for Negative d implies a weaker version of Masser-Oesterlé's ABC-Conjecture; namely, it implies that there is a maximum power of any ABC-solution.

Elkies and Kanapka have tabulated all ABC-solutions with $\log \max(|A|, |B|, |C|) < 2^{32}$ and with power $P(A, B, C) > 1.2$. The four "top" ABC-solutions in this range are:

$$2 + 3^{10} \cdot 109 + (-23^5) = 0,$$

discovered by Reyssat and having power $1.629912\ldots$;

$$11^2 + 3^2 5^6 7^3 + (-2^{21} 23) = 0,$$

discovered by de Weger and having power $1.625991\ldots$;

$$283 + 5^{11} 13^2 + (-2^8 3^8 17^3) = 0,$$

discovered by Browkin-Brzezinski and having power $1.580756\ldots$; and

$$1 + 2 \cdot 3^7 + (-5^4 7) = 0,$$

discovered by de Weger and having power $1.567887\ldots$.

Rounded Waring-Type Problems

There is the following natural extension of the above problem to m integers, where $m \geq 3$. Consider the following set D in $\mathbb{R}^m$, a kind of sconce:

$$D = \left\{ (a_1, a_2, \ldots, a_m) \in \mathbb{R}^m \;\middle|\; \begin{array}{l} a_j \geq 1, \\ j = 1, \ldots, m, \\ \text{and} \\ d = \sum_{j=1}^{m} \frac{1}{a_j} - 1 \\ \quad > 0 \end{array} \right\}.$$

Let $S(a_1, a_2, \ldots, a_m; X)$ denote the number of m-tuples of integers $A_1, A_2, \ldots, A_m$ that are pairwise relatively prime, have sum 0, are all of absolute value $< X$, and are such that A_j is an a_j-powered number for $j = 1, \ldots, m$. Might one expect, using the analogous rough calculation as above, that for $(a_1, a_2, \ldots, a_m) \in D$ (or at least in some large subregion of D), we have

$$S(a_1, a_2, \ldots, a_m; X) \approx X^d\,?$$

The Transferability of (a, b, c)-Questions

View, for a moment, the letters A, B, and C as independent variables.

Definition. By a **transfer** τ of degree n let us mean a transformation

$$(A, B, C) \longmapsto (A_1, B_1, C_1)$$

such that

1. A_1, B_1, C_1 are nontrivial homogeneous forms, each of degree n, with rational coefficients in the variables A, B, C;
2. the sum $A_1 + B_1 + C_1$ is in the ideal generated by $A + B + C$ in the polynomial ring $\mathbb{Q}[A, B, C]$); and
3. the homogeneous forms A_1, B_1, C_1 have *integral* values on integral ABC-solutions.

By the **defect** of a transfer τ let us mean the *smallest* positive integer G (or ∞ if there is none) such that, for any triple of relatively prime integers (α, β, γ) constituting an ABC-solution, the greatest common divisor of the triple of integers

$$A_1(\alpha, \beta, \gamma), \quad B_1(\alpha, \beta, \gamma), \quad C_1(\alpha, \beta, \gamma)$$

divides G.

Examples. The quadratic transfer. Consider the transformation

$$\tau_2 : (A, B, C) \longmapsto (A_1, B_1, C_1)$$

with

$$\begin{aligned} A_1 &= (A - C)^2, \\ B_1 &= -B^2, \\ C_1 &= 4AC. \end{aligned}$$

The defect of this transfer is $G = 4$. Since, up to sign, both A_1 and B_1 are perfect squares, we have that for every (a, b, a)-powered solution (A, B, C) satisfying the congruence conditions above, the triple $(A_1/\gamma, B_1/\gamma, C_1/\gamma)$ will be an ABC-solution in $S(2 - \epsilon, 2b - \epsilon, a - \epsilon)$, where γ is the greatest common divisor of (A_1, B_1, C_1) and where ϵ is small when C_1 is large. Here the annoying ϵ comes from the fact that the defect is > 1.

The sextic transfer. Consider the transformation

$$\tau_6 : (A, B, C) \longmapsto (A_1, B_1, C_1)$$

with

$$\begin{aligned} A_1 &= \{AB + BC + AC\}^3, \\ B_1 &= \left\{ \frac{(A - B)(B - C)(A - C)}{2} \right\}^2, \\ C_1 &= -3 \left\{ \frac{3(ABC)}{2} \right\}^2. \end{aligned}$$

[7] *Here we do not know the conclusion of statement (3) for general U, V, W satisfying the stated conditions.*

Here A_1, B_1, C_1 are homogeneous symmetric sextic forms in A, B, C, and one checks that the equality $A + B + C = 0$ implies $A_1 + B_1 + C_1 = 0$. The fact that there are 2's in the denominators of the terms above need not bother us, for the numerators will always be even, provided A, B, C are integers summing to zero. If also A, B, C have greatest common divisor equal to 1, then A_1, B_1, C_1 will have greatest common divisor at most 27; i.e., the defect of the sextic transfer is $G = 27$. This is a minor annoyance, but not a serious one.[8] The most evident fact about this transformation, $(A, B, C) \mapsto (A_1, B_1, C_1)$, is that A_1 is a perfect cube and B_1 a perfect square, so that the triple (A_1, B_1, C_1) is a solution to the Mordell Equation

$$Y^2 + X^3 = k,$$

with $Y = \frac{(A-B)(B-C)(A-C)}{2}$, $X = AB + BC + AC$, and $k = -3\left\{\frac{3(ABC)}{2}\right\}^2$. Except for the annoying power of 3, C_1 has quite a nice formula: if, for example, A, B, and C are a-powered, then C_1 is $(2a - \delta)$-powered, where δ is small when C_1 is large. For any real number $a < 3$, this transformation will induce a mapping

$$S(a, a, a; X) \longrightarrow S(3 - \delta, 2 - \delta, 2a - \delta; \kappa \cdot X^6),$$

where κ is a small constant and δ can be made as small as one likes by restricting attention to ABC-solutions of large enough absolute values. The reason for the presence of δ is the "annoying" factor of 3 that we mentioned. This mapping may have some minor failures: B_1 could be zero or the mapping may fail to be one-one. But at least it behaves, in terms of the rough asymptotics that we are considering, just as well as if it were always defined and one-one. Put $d = 3/a - 1$ and $d_1 = d/6 = \left(\frac{1}{3} + \frac{1}{2} + \frac{1}{2a} - 1\right)$, so that d is the expected exponent for $S(a, a, a; X)$ and d_1 for $S(3, 2, 2a; X)$.

The existence of the quadratic and sextic transfers has implications for the questions under discussion, both for negative and positive exponent d, so it might pay to review a surprising feature of both of these transfers, $T : (A, B, C) \mapsto (A', B', C')$, that make them particularly helpful to use in (a, b, c)-problems. Let us define a transfer T of degree n to be "(a, b, c)-**good**" if there are real numbers a', b', c' such that

$$\frac{1}{a} + \frac{1}{b} + \frac{1}{c} - 1 = n \cdot \left\{\frac{1}{a'} + \frac{1}{b'} + \frac{1}{c'} - 1\right\}$$

and T transfers (a, b, c)-solutions (A, B, C) to $(a' - \epsilon, b' - \epsilon, c' - \epsilon)$-solutions, where $\epsilon > 0$ may be taken to be arbitrarily small if we restrict to (a, b, c)-solutions (A, B, C) with $\max\{|A|, |B|, |C|\}$ sufficiently large.

One easily checks that the quadratic transfer is "(a, b, a)-good" for any choice of a and b, while the previous discussion tells us that the sextic transfer is "(a, a, a)-good" for any choice of a.

Implications for Positive Exponent d

When d is positive, an (a, b, c)-good transfer T enables one to pass from ample sets of (a, b, c)-solutions to ample, or nearly ample, sets of (a', b', c')-solutions. The following fact illustrates matters.

Fact. If $d = 3/a - 1$ and $d_1 = \frac{1}{3} + \frac{1}{2} + \frac{1}{2a} - 1$, and if for a given value of a with $1 < a < 3$, $|S(a, a, a; X)| > X^{d-\epsilon}$ for all positive ϵ, then

$$|S(3 - \delta, 2 - \delta, 2a - \delta; X)| > X^{d_1 - \epsilon}$$

for any $\delta > 0$ and for all sufficiently large X.

Proof. This is a straightforward verification, the arithmetic behind it being just that

$$d = \frac{3}{a} - 1 = 6 \cdot \left(\frac{1}{3} + \frac{1}{2} + \frac{1}{2a} - 1\right),$$

i.e., the sextic transfer is (a, a, a)-good.

Implications for Negative Exponent d

We have already discussed the classical Diophantine problem posed by the generalized Fermat Equation

$$UX^n + VY^n + WZ^n = 0$$

for a fixed triple of nonzero integers (U, V, W). Consider the corresponding rounded Diophantine problem given by the (a, b, c)-Conjecture with $a = b = c$ and with $d = 3/a - 1$ negative. We can restate it as follows.

Conjecture *(Rounded Fermat-Type Conjecture). Let $a > 3$. There are only finitely many triples of relatively prime a-powered integers (A, B, C) such that $A + B + C = 0$.*

The sextic transfer allows us to connect the Rounded Fermat-Type Conjecture with the Mordell Equation. To prepare for this, let us formulate the following conjecture.

Conjecture *(Conjecture about Sums of Squares and Cubes). For any $\alpha > 6$ and positive integer G, there are only finitely many α-powered numbers k for which the Mordell Equation*

$$y^2 + x^3 = k$$

has a solution in nonzero integers (x, y) with greatest common divisor $\le G$.

It is easy to see that the ABC-Conjecture of Masser-Oesterlé implies the Conjecture about Sums of Squares and Cubes.

[8] *Readers familiar with the theory of elliptic curves may recognize this transformation, $(A,B,C) \mapsto (A_1,B_1,C_1)$, as giving the values of the modular invariants c_4, c_6, and Δ of the Frey elliptic curve corresponding to (A,B,C).*

Proposition. *The Conjecture about Sums of Squares and Cubes implies the Rounded Fermat-Type Conjecture.*

The essential mechanism behind the proof of this proposition (and a number of its variants) has long been known (by Oesterlé, Szpiro, Hindry; see [O]). It has been phrased in the literature using the vocabulary of the arithmetic of elliptic curves. In the proof below we shall use the Conjecture about Sums of Squares and Cubes with $G = 27$.

Proof of the Proposition. Let us assume that the Rounded Fermat-Type Conjecture is false, so that for some real number $a > 3$ we have infinitely many triples of relatively prime a-powered integers (A, B, C) such that $A + B + C = 0$. We have that $|ABC|$ tends to infinity as we run through our sequence of triples (A, B, C). Apply the sextic transfer to each of the triples in this sequence to obtain again infinitely many triples (A_1, B_1, C_1), where A_1 is a perfect cube and B_1 is a perfect square. Writing $A_1 = x^3$, $B_1 = y^2$, and $C_1 = -k$, we obtain an infinite set of solutions to the Mordell Equation with greatest common divisor dividing 27. It remains to estimate the powers of the integers $k = 3(3ABC/2)^2$ that occur. Since $|ABC|$ tends to infinity, $P(k)$ will approach $P(ABC^2) = 2 \cdot P(ABC) \geq 2a$ in the limit. Since $a > 3$, we may take $e = a + 3$ and obtain a contradiction to the Conjecture about Sums of Squares and Cubes, thereby proving the proposition.

The proposition suggests that we focus on finding pairs of relatively prime integers (u, v) such that $P(u^2 + v^3)$ is large. Apart from the Catalan solution $(u, v) = (3, -2)$, a few known ones where $u^2 + v^3$ is plus-or-minus a *perfect* power are $13^2 + 7^3 = 2^9$, $71^2 + (-17)^3 = 2^7$, and the following other larger ones recently found by Beukers and Zagier:

$$21063928^2 + (-76271)^3 = 17^7,$$
$$2213459^2 + 1414^3 = 65^7,$$
$$15312283^2 + 9262^3 = 113^7,$$
$$30042907^2 + (-96222)^3 = 43^8,$$
$$1549034^2 + (-15613)^3 = -33^8.$$

Noam Elkies communicated to me the following solution of the Mordell Equation:

$$23053^2 - 505^3 = 3 \cdot 2^{27};$$

here $P(3 \cdot 2^{27}) = 11.05817\ldots$. Can one find relatively prime u and v such that $P(u^2 + v^3) \geq 12$? It would be good to gain enough insight to be able to offer a plausible prediction of a specific upper bound B for P of integers of the form $u^2 + v^3$, other than the Catalan solution, with u and v relatively prime.

References

I. Expository books and articles

[Co] D. Cox, Introduction to Fermat's Last Theorem, *Amer. Math. Monthly* **101** (1994), 3–14.

[F] Fibonacci (Leonardo Pisano), *The Book of Squares*, annotated English translation by L. E. Sigler, Academic Press, 1987.

[G] F. Gouvea, A marvelous proof, *Amer. Math. Monthly* **101** (1994), 203–222.

[H-R] B. Hayes and K. Ribet, Fermat's Last Theorem and modern arithmetic, *American Scientist* **82** (1994), 144–156.

[Ma] B. Mazur, Number theory as gadfly, *Amer. Math. Monthly* **98** (1991), 593–610.

[Mau] R. D. Mauldin, A generalization of Fermat's Last Theorem: The Beal conjecture and prize problem, *Notices Amer. Math. Soc.* **44** (Dec. 1997), 1436–1437.

[We] A. Weil, *Number Theory: An Approach through History from Hammurapi to Legendre*, Birkhäuser, 1984.

II. References

[B1] A. Baker, *Transcendental Number Theory*, Cambridge University Press, 1975.

[B2] ———, Review of *Catalan's Conjecture* by Paulo Ribenboim, *Bull. Amer. Math. Soc.* (N.S.) **32** (1995), 110–112.

[B-F-G-S] J. Browkin, M. Filaseta, G. Greaves, and A. Schinzel, Squarefree values of polynomials and the *abc*-conjecture, *Sieve Methods, Exponential Sums, and Their Applications in Number Theory* (Cardiff, 1995), London Math. Soc. Lecture Note Series, vol. 237, Cambridge University Press, 1997, pp. 65–85.

[D-G] H. Darmon and A. Granville, On the equations $z^m = F(x, y)$ and $Ax^p + By^q = Cz^r$, *Bull. London Math. Soc.* **27** (1995), 513–543.

[F-G] M. Filaseta and S. Konyagin, On a limit point associated with the *abc*-conjecture, *Colloq. Math.* **76** (1998), 265–268.

[G-P-Z] J. Gebel, A. Pethö, and H. Zimmer, Computing integral points on Mordell's elliptic curves, *Collect. Math.* **48** (1997), 115–136.

[M] D. Masser, Open problems, *Proc. Sympos. Analytic Number Theory* (W. W. L. Chen, ed.), Imperial College, London, 1985.

[O] J. Oesterlé, Nouvelles approches du "théorème" de Fermat, *Astérisque* **161/162** (1988), 165–186.

[R] P. Ribenboim, *Catalan's Conjecture*, Academic Press, 1994.

[T] R. Tijdeman, On the equation of Catalan, *Acta Arith.* **29** (1976), 197–209.