On Number Theory and Kustaa Inkeri

Alfred J. van der Poorten

Of course, I too was fascinated by Fermat's Last Theorem as a teenager. I read 'The Last Theorem' of E. T. Bell — I had found it in my local library — and loved 'The Devil and Simon Flagg', by Arthur Porges*. Curiously, perhaps, it was not these things that made me decide to study mathematics rather than physics at university. In 1960, during the year I spent in Israel after finishing high school, I found I could not afford to buy science fiction books — which I might finish in an hour and could not reread more than four or five times. Instead, I bought the Dover edition of Konrad Knopp's *Function Theory*. Its three volumes, and two additional volumes of problems, kept me happily occupied for many months. I decided I wanted to be taught some of the background mathematics. But I remained too sensible, perhaps too conservative, to spend serious time on Fermat's Last Theorem. I knew only amateurs did that.

Sure, I gave the FLT a month of my time each year. I still believe — well, sort of — that it must be possible to prove directly that $\sqrt[n]{1-x^n}$ takes a rational value for rational $x \neq 0$ only if $n = 1$ or 2. But my first noteworthy mathematical contact with Fermat's Last Theorem surely came from reading Kustaa Inkeri's 'A note on Fermat's conjecture' [13]. I wrote to Inkeri, explaining that the implications of Baker's inequalities now were known to include a control on the exponent, in the sense of Tijdeman and Schinzel [26], and consequently [25].

In his foreword 'Kustaa Inkeri: Portrait of a Mathematician' to the collected papers of Kustaa Inkeri [21], Tauno Metsänkylä writes: "For the mathematical community, Kustaa Inkeri is the author of significant papers on number theory, especially on topics related to Fermat's Last Theorem. Finnish mathematicians know Inkeri as the founder of the school of number theory in Finland. At the University of Turku, many of us still think of Inkeri as the Head of the Mathematics Department, a position he held for about 20 years."

For me, Kustaa Inkeri was a generous correspondent who promptly invited me to join him as co-author in a paper he drafted based in part on my letter

*To earn my pocket money I worked for a local pharmacy 1956–58 delivering orders. To my great fortune, the pharmacist was a science fiction reader who subscribed to all the science fiction magazines. That's how I met Simon Flagg, in the British edition of the Magazine of Fantasy and Science Fiction. Actually, that's also how I learned about E. T. Bell. I first read several of John Taine's science fiction novels (*Seeds of Life*, and *The Greatest Adventure*), and then discovered that Taine also wrote about mathematics, under his real name, Eric Temple Bell.

to him [16]†. Then, moreover, it happened that ICM'78, about to take place in Helsinki, brought me to Finland. My family and I were invited to spend a week in Turku. We first met Tauno, who looked after us at Inkeri's behest, we renewed acquaintance with Matti Jutila — whom we had first met in Debrecen in 1974 — and we were entertained everywhere, including an evening with Veikko Ennola, and a delightful lunch with Inkeri hosted by his daughter‡. I also recall that 'public demand' — more precisely, Kustaa Inkeri's urgings — required me to give the very first of what eventually became some four dozen lectures on Apéry's proof of the irrationality of $\zeta(3)$; see [23].

Twenty-one years later, my wife, Joy, and I are honoured and delighted to be invited back to Turku for the present meeting.

1. Fermat's Last Theorem

In recent years I have said and written [24] far too much about the FLT to want to add greatly to it here. So, let me begin my remarks by quoting myself. In Chapter V of [24] I mention that:

> of April 1994, Henri Darmon e-perpetrated the following announcement:
>
> > amazing development today on Fermat's Last Theorem. Noam Elkies has announced a counterexample, so that FLT is not true after all! He spoke about this at the Institute today. The solution to Fermat that he constructs involves an incredibly large prime exponent (larger than 10^{20}), but it is constructive. The main idea seems to be a kind of Heegner-point construction, combined with a really ingenious descent for passing from the modular curves to the Fermat curve. The really difficult part of the argument seems to be to show that the field of definition of the solution (which, a priori, is some ring class field of an imaginary quadratic field) actually descends to $\mathbb{Q}$. I wasn't able to get all the details, which were quite intricate ... .
> >
> > So it seems that the Shimura–Taniyama Conjecture is not true after all. The experts think that it can still be salvaged, by extending the concept of

†Notice its date, 1980, of publication. It was this, I think, that led to a later exchange with Andrzej Schinzel, which I report in Chapter V of *Notes on Fermat's Last Theorem* as follows: "The dates now surprise me and remind me of the extraordinary delays then current in publication. Some years later John Loxton and I accidentally dedicated our article ('An awful problem about integers in base 4', to Paul Erdős on his 75th birthday, *Acta Arith.* **49** (1987), 193–203) to the 80th birthday of Paul Erdős (rather than his 75th), leading Schinzel to say archly that he accepted the paper subject to one change, unless we wanted it kept back for five years. I was able to retort that my error was understandable given the way that Erdős carried on about his age — smile from Schinzel — and that, anyhow, given *Acta Arithmetica* delays, it was probably spot on — laughter from everyone else."

‡No, that's not quite right. Liisa Vainio came as designated driver, and principal English speaker.

> automorphic representation, and introducing a notion of "anomalous curves" that would still give rise to a "quasi-automorphic representation".

> I noted that the actual construction of his anomalous solution would have been quite some feat on Elkies' part*, given that such a solution would, according to Inkeri's results, necessarily involve numbers at least some 10^{21} digits long.

When I wrote that retort, I was recalling Inkeri's striking result [9] to the effect that, say, $y > \frac{1}{2}p^{3p-1}$ in any putative solution of Fermat's equation with exponent p. I was also thinking of the computations [5]†, whereby we knew *ante* Wiles that in any case $p > 4 \cdot 10^6$.

I was particularly intrigued by Inkeri's mention of Abel's equation, the special case of $x^n + y^n = z^n$ when one of x, y, or z is a power of a prime. Supposing $0 < x < y < z$, one requires only elementary ideas to find that x must be the prime power. In fact x must be prime, $z = y + 1$, the exponent n must be a prime p, and $p\big|y(y+1)$. Notwithstanding all that, Wiles's argument remains the only proof even of this very special case. Mind you, the case $z - y = 1$ actually *is* more difficult than $z - y = k > 1$. However, back then Inkeri and I could prove that *either* $y - x$ is relatively large, both in the ordinary and in the l-adic sense for every prime l. More specifically, if $y - x$ is bounded in a putative solution to Fermat's equation then so is the exponent and each of the variables. All this was fairly clear to those of us familiar with Baker's method. Independently, Cameron Stewart [29] announced similar results.

Inkeri's careful comments [14] on some of the more detailed erroneous proofs of Fermat's Last Theorem will remain of value to those of us still burdened by a stream of purported 'simple proofs' of the FLT.

2. Catalan's Equation

In [11], Inkeri shows that if $x^p - y^q = 1$ in integers x, y and odd primes p and q, where $p \equiv 3 \pmod 4$ and q does not divide the class number of the quadratic number field $\mathbb{Q}(\sqrt{-p})$, then $p^{q-1} \equiv 1 \pmod{q^2}$, $q^2\big|x$ and $y \equiv -1 \pmod{q^{2p-1}}$. In [15], Inkeri deals with arbitrary odd prime exponents. He shows that if q does not divide class number h_p of the cyclotomic number field $\mathbb{Q}(\zeta_p)$ generated by a primitive p-th root of unity, then $q^2\big|x$ and $p^{q-1} \equiv 1 \pmod{q^2}$. There's of course a little more to it than just this, but it remains instructive to see that in a certain sense the most sophisticated fact we need to know is that $\gcd\big(x-y, (x^p - y^p)/(x-y)\big) = 1$ or p.

In 1974, Tijdeman [31] proved that Catalan's equation has at most finitely many solutions by providing explicit upper bounds for the exponents (and thence

*Incidentally, Elkies was just an innocent bystander in this affair, with his prowess borrowed to lend credence to the claims.

†In [24] a mispaste led me to omit to mention Reijo Ernvall as a co-author

for $|x|$, and $|y|$). Those bounds have been considerably sharpened since, but are still somewhat too large to allow Inkeri's results finally to verify Catalan's suggestion that $3^2 - 2^3 = 1$ displays the only case of 'perfect powers' differing by 1.

In curious contrast, the equation $x^u - y^v = k$ with k different from ± 1 has remained inaccessible. I could prove [22], using a p-adic variant of Tijdeman's argument that, given the prime factors of k, all solutions to $x^u - y^v = k^{uv}$ are bounded; but that's just the p-adic variant of Catalan's equation.

We now know that Inkeri's criteria are of real value in the efforts to complete the proof of Catalan's conjecture, that is in filling the gap between the case $2^3 - 3^2 = 1$ and the bound on the exponents in $x^p - y^q = 1$ entailed by sharpenings of Tijdeman's argument. I expect that Yann Bugeaud and/or Maurice Mignotte will report on recent advances in that work.

3. Irrationality of e and π

Elementary books often make rather a fuss about the irrationality of numbers such as $\sqrt{2}$. But their irrationality really is a trivial matter. If a number α is known to be algebraic, then presumably one knows that it is a zero of some polynomial $sX^n + a_1X^{n-1} + \cdots + a_{n-1}X + a_n$ with integer coefficients. Then α is rational if and only if $s\alpha$ is a rational integer. For example, $\sqrt[3]{2}$ is irrational just because plainly $1 < \sqrt[3]{2} < 2$, so $\sqrt[3]{2}$ is not a *rational* integer.

However, suppose the given number is not obviously algebraic. Then one can do little better than remark that if α is rational then there is some integer $s > 0$ so that for all integers q the distance $\|q\alpha\|$ of $q\alpha$ from the nearest integer is either zero or is at least $1/s$. It may be quite difficult to decide whether a given number is, or is not, rational. The most interesting cases of course are π, and e.

As it happens one can show that e has a Hurwitz-periodic, and thus a nonterminating continued fraction

$$e - 1 = [\,\overline{1\,,\,1\,,\,2h}\,] = [1\,,\,1\,,\,2\,,\,1\,,\,1\,,\,4\,,\,1\,,\,1\,,\,6\,,\,1\,,\,\ldots]$$

so e is indeed irrational. However, we don't need all that.

Notice that the sum

$$e^{-1} = \sum\nolimits_{h\geq 2}(-1)^h/h!$$

is alternating with terms of decreasing size. Hence $(-1)^{n+1}n!/e$ differs by an integer from

$$\begin{aligned} 1/(n+1) - \big(1/(n+1)(n+2) - 1/(n+1)(n+2)(n+3)\big) - \cdots \\ = \big(1/(n+1) - 1/(n+1)(n+2)\big) + \cdots\,. \end{aligned}$$

It follows that $1/(n+1) > \|n!\,e^{-1}\| > 0$, so, §**??**, e^{-1} and thus also e is irrational. It also follows that $\|n!\,e^{-1}\| > 1/(n+2)$ for all positive integers n, so yet more obviously $1/e$ cannot be rational.

As for π, the most immediate argument I remember [27] is less straightforward. Set

$$n!J_n = \int_0^\pi (\pi x - x^2)^n \sin x\, dx.$$

Then integration by parts yields the recurrence relation

$$J_{n+2} = (4n+6)J_{n+1} - \pi^2 J_n$$

whence the supposition that $\pi^2 = r/s$ plainly implies the integrality of $s^n J_n$ for all $n \geq 0$. However, easily, $0 < s^n J_n \leq \pi(r/4)^n/n!$. The two facts just cited are plainly incompatible for sufficiently large n. Thus π^2 is irrational, and that entails that also π is irrational.

An interesting note [10] 'The irrationality of π^2' by Inkeri recalls Hermite's argument; the above is an elegant variant of that.

I do not recall any proof of the transcendence of e or π that seems quite as accessible as these irrationality proofs; an arguable exception is that of Niven [20], Chapter 9. The difficulty is, I think, that elegant transcendence proofs rely on implicit constructions. That notion is somehow more sophisticated than anything in the above arguments.

4. Perfect Powers with Identical Digits

The diophantine equation $y^q = a(x^n - 1)/(x-1)$ has long been the subject of study, not least by Kustaa Inkeri [12]. For $a = 1$, Ljunggren [18] had dealt with the case $q = 2$ and Nagell [19] with the cases $3\,|\,n$ and $4\,|\,n$. Here, a longstanding conjecture suggests that there are only finitely many solutions; likely just those given by

$$\frac{3^5-1}{3-1} = 11^2, \quad \frac{7^4-1}{7-1} = 20^2 \quad \text{and} \quad \frac{18^3-1}{18-1} = 7^3.$$

Yann Bugeaud and Maurice Mignotte combine several methods in diophantine approximation (see also [4]), including a useful new lower bound for linear forms in two p-adic logarithms [3], together with extensive computer calculations to make very considerable impact on the problem. In particular they settle the conjecture for an extended range of small integers x, and, in effect, for x a power of a prime. These results solve an old problem in showing in particular that

$$x = 11\ldots11\,,$$

with all its digits equal to 1 in base 10, cannot be a pure power, other than for the trivial case $x = 1$.

5. Representation of Integers in the Form $Ax^2 + 2Bxy + Cy^2$

The matter of representation of integers by quadratic forms is one of the oldest problems of number theory. Of course, the real issue is to explain just which integers are represented, and why, but it certainly is also of interest actually to find representations. My following remarks are a minor variant on known algorithms for determining representations by definite forms. The idea is conveniently illustrated by a toy example.

Consider the problem of finding nonnegative integers x and y so that

$$173 = 2x^2 + 3y^2 .$$

We first solve the congruence $z^2 \equiv -3 \cdot 2 \pmod{173}$. Indeed $72^2 = 30 \cdot 173 - 6$. Accordingly we study the matrix

$$M = \begin{pmatrix} 173 & 72 \\ 72 & 30 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 14 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 6 \end{pmatrix} .$$

Here I have effected the decomposition by the Euclidean algorithm on the rows of M, with the details given by the array

	173	72
2	72	30
2	29	12
2	14	6
14	1	0
	0	6

Dually, we might have performed the Euclidean algorithm on the columns of M, obtaining

	2	2	2	14	
173	72	29	14	1	0
72	30	12	6	0	6

It yields the transpose of the previous decomposition, namely

$$M = \begin{pmatrix} 173 & 72 \\ 72 & 30 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 6 \end{pmatrix} \begin{pmatrix} 14 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix} .$$

But something is clearly wrong here. M is a symmetric matrix, yet our methods of decomposition destroy that symmetry. So we try again, working symmetrically both by row and by column. Our working begins with the two steps

$$\begin{array}{cccc}
 & & 2 & \\
 & & & \\
 & 173 & 72 & \\
2 & 72 & 30 & 12 \\
 & 29 & 12 & 5
\end{array}$$

reporting that

$$M = \begin{pmatrix} 173 & 72 \\ 72 & 30 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 30 & 12 \\ 12 & 5 \end{pmatrix} \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix} .$$

Ultimately, we have

$$\begin{array}{cccccc}
 & & 2 & 2 & 1 & \\
 & & & & & \\
 & 173 & 72 & & & \\
2 & 72 & 30 & 12 & & \\
2 & 29 & 12 & 5 & 2 & \\
1 & & 6 & 2 & 2 & 0 \\
 & & & 3 & 0 & 3
\end{array}$$

showing that

$$M = \begin{pmatrix} 173 & 72 \\ 72 & 30 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix} .$$

The array

$$\begin{array}{ccccc}
 & & 2 & 2 & 1 \\
0 & 1 & 2 & 5 & 7 \\
1 & 0 & 1 & 2 & 3
\end{array}$$

details the computation

$$\begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 7 & 5 \\ 3 & 2 \end{pmatrix} .$$

So we have

$$M = \begin{pmatrix} 173 & 72 \\ 72 & 30 \end{pmatrix} = \begin{pmatrix} 7 & 5 \\ 3 & 2 \end{pmatrix} \begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix} \begin{pmatrix} 7 & 3 \\ 5 & 2 \end{pmatrix}$$

and, indeed,

$$2 \cdot 7^2 + 3 \cdot 5^2 = 173 .$$

Theorem 5.1. *Let m be a positive integer, and suppose that $z^2 \equiv -m \pmod{n}$. Set $k = (z^2+m)/n$. Then there is a unimodular nonnegative integer matrix* $\begin{pmatrix} x & x' \\ y & y' \end{pmatrix}$

and integers a, b and c satisfying $0 \le b < a$, $0 \le b < c$ and $ac - b^2 = m$, so that

$$M = \begin{pmatrix} n & z \\ z & k \end{pmatrix} = \begin{pmatrix} x & y \\ x' & y' \end{pmatrix} \begin{pmatrix} a & b \\ b & c \end{pmatrix} \begin{pmatrix} x & x' \\ y & y' \end{pmatrix},$$

and plainly

$$n = ax^2 + 2bxy + cy^2 .$$

Conversely, every such representation of n is obtained from a solution of $z^2 \equiv -m \pmod{n}$ in the manner just detailed.

There's nothing much to prove here except perhaps some trite lemmas on row and column decomposition of positive integer matrices.

Nonetheless, to add some conviction, let me detail the case $83 = 2x^2+2xy+3y^2$. Here $m = 5$ and $59^2 + 5 = 42 \cdot 83$. Indeed

$$\begin{array}{cccccc}
 & & 1 & 2 & 1 & \\
 & & & & & \\
 & 83 & 59 & & & \\
1 & 59 & 42 & 17 & & \\
2 & 24 & 17 & 7 & 3 & \\
1 & & 8 & 3 & 2 & 1 \\
 & & & 4 & 1 & 3
\end{array}$$

and the continued fraction $[1\,,\,2\,,\,1\,]$ is $4/3$ whilst $[1\,,\,2\,] = 3/2$. Hence

$$2 \cdot 4^2 + 2 \cdot 4 \cdot 3 + 3 \cdot 3^2 = 83 .$$

My one innovation, if there is one at all, is the idea of symmetric decomposition of symmetric integer matrices. Otherwise, I describe the well known algorithm sometimes attributed* to Cornacchio; an allusion to the contribution of Serret and Hermite might also be appropriate. In the particular case $m = 1$, thus the case of representation as a sum of two squares, the matrix M is unimodular and its symmetry is precisely the symmetry of the continued fraction expansion of n/z. In [28], H. J. S. Smith gives a cute proof that there is a z so that p/z has a symmetric continued fraction expansion whenever p is a prime $\equiv 1 \pmod 4$; we repeat that delightful story in [7]. The general algorithm is analysed in [8]; this is also a good source for references. Those include [32], which makes fairly heavy weather of precisely the issues exposed by my present remarks.

Of course, I hide the real problem, namely that of finding a square root of $-m$ mod n. Nonetheless, it seems worth emphasising that if one has chanced upon a solution of that congruence then of course the symmetric decomposition displays a representation by some quadratic form of appropriate discriminant.

*For example in the fine text: Frits Beukers, *Getaltheorie voor Beginners*, Epsilon Uitgaven, Utrecht, 1999, which provoked my present remarks.

I conclude with some useful small examples to assist the reader in convincing her friends of the practicality of my remarks:

$$544^2 \equiv -6 \pmod{4054} \quad \text{with} \quad \begin{aligned} 544^2 &= 4054 \cdot 73 - 6 \\ 53^2 &= 134 \cdot 21 - 5 \\ 110^2 &= 269 \cdot 45 - 5 \\ 11^2 &= 61 \cdot 2 - 1. \end{aligned}$$

6. An Extraordinary Integral

It is, at first glance, a startling suggestion that

$$\int \frac{6x\,dx}{\sqrt{x^4+4x^3-6x^2+4x+1}} = \log\Big(x^6+12x^5+45x^4+44x^3-33x^2+43 \\ + (x^4+10x^3+30x^2+22x-11)\sqrt{x^4+4x^3-6x^2+4x+1}\Big).$$

However, differentiating both sides of the allegation readily confirms the claim. Specifically, denote by $a(x)$, $b(x)$, and $D(x)$ the polynomials so that $a+b\sqrt{D}$ denotes the argument of the logarithm above. The claim is then equivalent to

$$6x/\sqrt{D} = \big((2b'D+bD')+2a'\sqrt{D}\big)/2\sqrt{D}(a+b\sqrt{D})\,.$$

But, $a'/b = 6x$. Thus it suffices that also $(2b'D+bD')/2a = 6x$, and this is readily confirmed.

The argument just given is a fine example of a valid proof that is nonetheless utterly valueless — it explains nothing. We do a little better on noting that the last fact we were to show is

$$(2b'D+bD')/2a = a'/b, \quad \text{or} \quad 2a'a-(2b'bD+b^2D') = 0\,.$$

It is then plain that necessarily $b\big|a'a$ in the appropriate polynomial ring, and that

$$a^2-Db^2 = (x^6+12x^5+45x^4+44x^3-33x^2+43)^2 \\ -(x^4+4x^3-6x^2+4x+1)\cdot(x^4+10x^3+30x^2+22x-11)^2$$

must be a constant, namely $43^2-11^2 = 2^6\cdot 3^3$. It follows that $b\big|a'$.

We now do glimpse an explanation, because the argument just suggested is reversible. Accordingly, let $D(x)$ denote a polynomial in x over some field $\mathbb{F}$ of characteristic zero. We will see that we will need to suppose that D is of even degree $2g+2$, some nonnegative g, and that the leading coefficient of D is a square in $\mathbb{F}$. Then $D(x)$ has a square root in the field $\mathbb{F}((x^{-1}))$ of Laurent series in x^{-1} over $\mathbb{F}$.

Theorem 6.1. *Suppose there are polynomials $p(x)$ and $q(x)$ so that*

$$p(x)^2 - D(x)q(x)^2$$

is a nonzero element of $\mathbb{F}$. Set $f(x) = p'(x)/q(x)$. Then f is a polynomial of degree g, and

$$\int \frac{f(x)dx}{\sqrt{D(x)}} = \log\bigl(p(x) + q(x)\sqrt{D(x)}\,\bigr).$$

Conversely, given such an indefinite integral, it follows that $f(x)$ is a polynomial of degree g and that $p(x) + q(x)\sqrt{D(x)}$ is a unit in the domain $\mathbb{F}[x, \sqrt{D(x)}\,]$.

Proof. Given that $p(x)^2 - D(x)q(x)^2$ is constant, we have p, q are relatively prime as polynomials so $2p'p - 2q'qD - q^2D' = 0$ entails $q\big|p'$, $(2q'D + qD')/2p = p'/q$ and so $(p(x) + q(x)\sqrt{D(x)}\,)'/(p(x) + q(x)\sqrt{D(x)}\,) = f(x)/\sqrt{D(x)}$ with $f = p'/q$.

As for $p(x)^2 - D(x)q(x)^2$ having to be a unit, that is of course an *of course*! Given the integral, one adds it to its conjugate — thus with $\sqrt{D(x)}$ replaced by $-\sqrt{D(x)}$, to see that $\log\bigl(p^2 - D(x)q^2\bigr)$ — being an integral of 0 — *must* be constant; that is that $p(x) + q(x)\sqrt{D(x)}$ is a unit as claimed. ☐

Remark. By $p(x)^2 - D(x)q(x)^2$ constant and $\deg q(x) = n$, say, we have $\deg p(x) = n + g + 1$, so $\deg f(x) = \deg p'(x) - \deg q(x) = g$.

The existence of quasi-elliptic integrals goes back at least to work of Abel [1]; later, Chebychev [30] explains the phenomenon in terms of periodic continued fraction expansion of $\sqrt{D(x)}$.

Nowadays, we recognise that the presence of a nontrivial unit $p(x)+q(x)\sqrt{D(x)}$, say of degree s, reports the existence of some principal divisor $s(\infty_+ - \infty_-)$. In other words, the divisor $\infty_+ - \infty_-$ is a torsion divisor on the Jacobian of the curve $y^2 = D(x)$. Specifically, in the elliptic case $g = 1$, or $\deg D(x) = 4$, there is a torsion point 'at infinity' on the curve; see [2].

Readers wishing to produce new surprising integrals of their own may be helped by a sampling of examples of hyperelliptic curves $y^2 = D(x)$ provided to me by my student Xuan Chuong Tran. The integers on the left are the length of the period of the continued fraction expansion of $\sqrt{D(x)}$. Those on the right are the degree of the first unit produced, and thus the order of the torsion divisor responsible for the existence of the unit suggested by the number on the left.

6	$y^2 = x^4 + 2x^3 + 9x^2 + 24x + 16$	7
14	$y^2 = x^4 + 2x^3 - 11x^2 + 12x + 132$	8
8	$y^2 = x^4 + 2x^3 - 15x^2 + 8x + 40$	9
18	$y^2 = x^4 + 2x^3 - 419x^2 + 4332x - 12924$	10
22	$y^2 = x^4 + 2x^3 - 503x^2 + 336x + 81984$	12
42	$y^2 = 4x^6 - 60x^5 + 249x^4 - 192x^3 + 90x^2 - 36x + 9$	27

Notice that when $g = 1$ and the torsion r is odd one immediately obtains a unit of norm 1. The final example is one of the many curves produced by Franck

Leprévost, see [17] and other of his papers, of genus 2 and higher, and with torsion divisor of high order on its Jacobian. Other examples may be found in [6].

Acknowledgement. This work is in part supported by a Grant from the Australian Research Council.

References

[1] N. H. Abel, 'Über die Integration der Differential-Formel $\rho\,dx/\sqrt{R}$, wenn R und ρ ganze Funktionen sind', J. für Math. **1** (1826), 185–221.

[2] William W. Adams and Michael J. Razar, 'Multiples of points on elliptic curves and continued fractions', *Proc. London Math. Soc.* **41** (1980), 481–498.

[3] Y. Bugeaud, 'Linear forms in p-adic logarithms and the Diophantine equation $(x^n - 1)/(x - 1) = y^q$ ', *Math. Proc. Camb. Philos. Soc.* **127** (1999), 373–381.

[4] Y. Bugeaud, M. Mignotte, Y. Roy and T. N. Shorey, 'The Diophantine equation $(x^n - 1)/(x - 1) = y^q$ has no solution with x square', *Math. Proc. Camb. Philos. Soc.* **127** (1999), 353–372.

[5] J. P. Buhler, R. E. Crandall, R. Ernvall and T. Metsänkylä, 'Irregular primes and cyclotomic invariants to four million' *Math. Comp.* **61** (1993), 151–153.

[6] J. W. S. Cassels and E. V. Flynn, *Prolegomena to a Middlebrow Arithmetic of Curves of Genus* 2, LMS Lecture Notes 230, Cambridge UP, 1996.

[7] Michel Dekking, Michel Mendès France and Alfred J van der Poorten, 'FOLDS!' II: 'Symmetry disturbed', *The Mathematical Intelligencer* **4** (1982), 173–181.

[8] Kenneth Hardy, Joseph B. Muskat and Kenneth S. Williams, 'A deterministic algorithm for solving $n = fu^2 + gv^2$ in coprime integers u and v', *Math. Comp.* **55** (1990), 327–343.

[9] K. Inkeri, 'Abschätzungen für eventuelle Lösungen der Gleichung im Fermatschen Problem', *Ann. Univ. Turku*, Ser. A, **16** (1953), 1–9.

[10] K. Inkeri, 'The irrationality of π^2', *Nord. Mat. Tidsskr.* **8** (1960), 10–16.

[11] K. Inkeri, 'On Catalan's problem', *Acta Arith.* **9** (1964), 285–290.

[12] K. Inkeri, 'On the Diophantine equation $a(x^n - 1)/(x - 1) = y^m$', *Acta Arith.* **21** (1972), 299–311.

[13] K. Inkeri, 'A note on Fermat's conjecture', *Acta Arith.* **29** (1976), 251–256.

[14] K. Inkeri, 'On certain equivalent statements for Fermat's last theorem — with requisite corrections', *Ann. Univ. Turku*, Ser. A, I **186** (1984), 12–22.

[15] K. Inkeri, 'On Catalan's conjecture', *J. Number Th.* **34** (1990), 142–152.

[16] K. Inkeri and A. J. van der Poorten, 'Some remarks on Fermat's conjecture', *Acta Arith.* **36** (1980), 107–111.

[17] Franck Leprévost, 'Points rationnels de torsion de jacobiennes de certaines courbes de genre 2', *C. R. Acad. Sci. Paris Sr. I Math.* **316** (1993), 819–821.

[18] W. Ljunggren, 'Noen Setninger om ubestemte likninger av formen $(x^n-1)/(x-1) = y^q$ ', *Norsk. Mat. Tidsskr.* **25** (1943), 17–20.

[19] T. Nagell, 'Note sur l'équation indéterminée $(x^n-1)/(x-1) = y^q$ ' *Norsk. Mat. Tidsskr.* **2** (1920), 75–78.

[20] Ivan Niven, *Irrational Numbers*, Carus Monographs 11, Mathematical Association of America, 3rd Printing, 1967.

[21] *Collected Papers of Kustaa Inkeri*, Tauno Metsänkylä and Paulo Ribenboim, eds; Queen's Papers in Pure and Applied Mathematics **91** (1992), Kingston, Ontario, Canada.

[22] A. J. an der Poorten, 'Effectively computable bounds for the solutions of certain diophantine equations', *Acta Arith.* **33** (1977), 193–207.

[23] Alfred van der Poorten, 'A proof that Euler missed ... Apéry's proof of the irrationality of $\zeta(3)$; An informal report', *The Mathematical Intelligencer* **1** (1979), 195-203.

[24] Alf van der Poorten, *Notes on Fermat's Last Theorem*, (New York, N. Y.: Wiley-Interscience, 1996), xvi+222pp.

[25] A. J. an der Poorten, A. Schinzel, T. N. Shorey and R. Tijdeman, 'Applications of the Gel'fond-Baker method to Diophantine equations', in *Transcendence theory: advances and applications* (Proc. Conf. Univ. Cambridge, Cambridge, 1976), pp59–77, Academic Press, London, 1977.

[26] A. Schinzel and R. Tijdeman, 'On the equation $y^m = P(x)$', *Acta Arith.* **31** (1976), 199–204.

[27] E. M. Schröder, 'Zur Irrationalität von π^2 und π (On the irrationality of π^2 and π)' *Mitt. Math. Ges. Hamburg* **13** (1993), 249.

[28] H. J. S. Smith, 'De compositione numerorum primorum formae $4\lambda+1$ ex duobus quadratis', *J. Reine Angew. Math.* (Crelle), **50**, 1855, 91–92.

[29] C. L. Stewart, 'A note on the Fermat equation', *Mathematika* **24** (1977), 130–132.

[30] P. Tchebicheff, 'Sur l'intégration des différentielles qui contiennent une racine carrée d'un polynome du troisième ou du quatrième degré', *Journal des math. pures et appl.* **2** (1857), 168–192; and 'Sur l'intégration de la différentielle $\frac{x+A}{\sqrt{x^4+\alpha x^3+\beta x^2+\gamma x+\delta}}$', *ibid.* **9** (1864), 225–246.

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

[32] P. Wilker, 'An efficient algorithmic solution of the diophantine equation $u^2+5v^2 = m$', *Math. Comp.* **35** (1980), 1347–1352.

Address of the author:

Department of Mathematics
Macquarie University
Sydney 2109, Australia