19
No 1

Comptes rendus mathématiques
Mathematical Reports

JUNE / JUIN 1997

IN THIS ISSUE / DANS CE NUMÉRO

Letter from the Editors-in-Chief

The present Volume begins a new format of Comptes rendus mathématiques - Mathematical Reports. It is exceptional in that it will contain only two issues. The future volumes will contain four issues each.

The main objective of Comptes rendus mathématiques - Mathematical Reports remains the quick publication of short Research announcements, or short complete papers. In addition, we will publish invited Research-Expository papers that will provide useful surveys to the mathematical community.

The instructions on how to submit articles may be found at the back of this issue.

Lettre des rédacteurs-en-chef

Ce volume introduit un nouveau format pour les Comptes rendus mathématiques - Mathematical Reports. Il ne comprendra que deux numéros alors que les prochains volumes en comprendront quatre.

L'objectif principal des Comptes rendus - Mathematical Reports demeure une publication rapide de courtes annonces de recherche, ou même de courts articles complets. De plus, nous publierons des articles par invitation ayant pour but d'expliquer et mieux faire connaître certains travaux de recherche à la communauté.

Les instructions pour un soumission d'articles se trouvent au dos de ce numéro.

Vlastimil Dlab
M. Ram Murty

C. R. Math. Rep. Acad. Sci. Canada Vol. **19** (1), 1997 pp. 3–14

FALTINGS PLUS EPSILON, WILES PLUS EPSILON, AND THE GENERALIZED FERMAT EQUATION

H. DARMON

Wiles' proof of Fermat's Last Theorem puts to rest one of the most famous unsolved problems in mathematics, a question that has been a wellspring for much of modern algebraic number theory. While celebrating Wiles' achievement, one also feels a twinge of regret at Fermat's demise. Is the Holy Grail of number theorists to become a mere footnote in the history books?

Hoping to keep some of the spirit of Fermat alive, I would like to discuss the *generalized Fermat equation*

$$x^p + y^q = z^r, \tag{1}$$

where p, q and r are fixed exponents. As in the case of Fermat's Last Theorem, one is interested in *integer solutions* (x, y, z), which are *non-trivial* in the sense that $xyz \neq 0$.

One might expect the equation above to have no such solutions if the exponents p, q, and r are large enough. But observe that, if $p = q$ is odd, and $r = 2$, then any solution to $a^p + b^p = c$ (of which there is an abundant supply!) yields the solution $(ac, bc, c^{\frac{p+1}{2}})$ to the equation $x^p + y^p = z^2$. A similar construction works whenever the exponents p, q, and r are pairwise coprime. However, the solutions produced in this way are not very interesting: the integers x, y and z have a large common factor.

Accordingly, one calls a solution (x, y, z) to the generalized Fermat equation *primitive* if $\gcd(x, y, z) = 1$.

MAIN QUESTION. *What are the non-trivial primitive solutions to the generalized Fermat equation?*

In [DG], Andrew Granville and I made the following conjecture:

GENERALIZED FERMAT CONJECTURE. *If* $\frac{1}{p} + \frac{1}{q} + \frac{1}{r} < 1$, *then the generalized Fermat equation has no non-trivial primitive solutions except the following:*

$$1^n + 2^3 = 3^2, \quad 2^5 + 7^2 = 3^4, \quad 7^3 + 13^2 = 2^9, \quad 2^7 + 17^3 = 71^2, \quad 3^5 + 11^4 = 122^2,$$

$$17^7 + 76271^3 = 21063928^2, \quad 1414^3 + 2213459^2 = 65^7, \quad 9262^3 + 15312283^2 = 113^7,$$

This is a transcription of the author's Aisenstadt prize lecture given at the CRM in March 1997. It is a pleasure to thank Andrew Granville and Loïc Merel for stimulating collaborations related to the topics of this essay, as well as Dan Abramovich for many helpful conversations over the years. This research was supported by CICMA and by grants from the Sloan Foundation, NSERC and FCAR.

Received by the editors May 21, 1997.

$$43^8 + 96222^3 = 30042907^2, \quad 33^8 + 1549034^2 = 15613^3.$$

This conjecture is really more of a "provocation", to borrow a term from Barry Mazur. (The five larger solutions were found by a computer search by Beukers and Zagier, after I had conjectured that they did not exist!) But as a measure of the stock I now place in the conjecture, I will offer a reward of

$$300\left(\frac{1}{\frac{1}{p}+\frac{1}{q}+\frac{1}{r}}-1\right)$$

(Canadian) dollars for a non-trivial primitive solution to $x^p+y^q=z^r$ which does not appear in the above list.

M-curves. The solutions of the Fermat equation $x^n+y^n=z^n$ correspond to rational points on an algebraic curve of genus $(n-1)(n-2)/2$. Because equation (1) is not homogeneous in general, its non-trivial solutions correspond to integer points on an affine surface, which is frequently rational (whenever p, q and r are pairwise coprime, for example) and has a complicated singularity at the origin – the primitive solutions corresponding to points which are also integral relative to this singular point.

The multiplicative group also acts on the surface given by equation (1), by

$$\lambda(x,y,z) = (\lambda^{qr}x, \lambda^{pr}y, \lambda^{pq}z),$$

and so it is tempting to view the surface (1) as a curve in some kind of "weighted projective space". This can be done, but this curve is frequently rational, and the primitive solutions do not have a very natural interpretation. Nonetheless, in this diophantine study one is reluctant to abandon the well-tended landscape of curves for the untamed wilds of (singular) algebraic surfaces.

As it turns out, a better framework for discussing primitive solutions of the generalized Fermat equation is supplied by the notion of a *curve with multiplicities*, or an M-curve, which is defined as follows:

DEFINITION. An M-curve over a field K is a smooth projective curve X/K, together with the assignment, for each point $P \in X(K)$, of a *multiplicity* $m_P \in \{1,2,3,\ldots\} \cup \{\infty\}$, such that $m_P = 1$ for all but finitely many P.

NOTATION. We denote by

$$\mathbf{X} = (X; P_1, m_1; P_2, m_2; \ldots; P_r, m_r)$$

the M-curve whose underlying projective curve is X, and such that $m_{P_i} = m_i$, and $m_Q = 1$ if $Q \notin \{P_1, \ldots, P_r\}$.

REMARK. Our primary interest being Diophantine, we will mainly consider the case where K is a number field. In this case, we extend X to a smooth proper

model $\mathcal{X}$ over $\mathcal{O}_{K,S}$, the ring of S-integers of K, where S is a finite set of primes containing the primes of bad reduction for X. For example, one could work with a minimal model for X, but this is not necessary: the statements that will be made later will be true for any choice of $\mathcal{X}$. Having fixed such a model $\mathcal{X}$ allows us to talk about $X(A) := \mathcal{X}(A)$ for any $\mathcal{O}_{K,S}$-algebra A. Note that since $\mathcal{X}$ is proper, $X(\mathcal{O}_{K,S}) = X(K)$.

INTERSECTION NUMBERS. If P and Q are distinct K-rational points of X (giving rise to sections on $\mathcal{X}$ over $\mathrm{Spec}(\mathcal{O}_{K,S})$) and $v \notin S$ is a place of K with associated prime ideal $\mathfrak{p}_v$, define the *arithmetic intersection number* $(P \cdot Q)_v$ as follows: it is the largest positive integer m such that P and Q have the same image in $\mathcal{X}(\mathcal{O}_{K,S}/\mathfrak{p}_v^m)$. Of course, this arithmetic intersection number depends on the model $\mathcal{X}$ for X chosen above. But given any two models $\mathcal{X}$ and $\mathcal{X}'$, the arithmetic intersection numbers $(P \cdot Q)_v$ agree for all but finitely many places v.

DEFINITION. An S-integral point on $\mathbf{X}$ is a point $Q \in X(K)$ satisfying:

$$(Q \cdot P)_v \equiv 0 \pmod{m_P}, \qquad \forall\, P \in X(K), \quad v \notin S.$$

The set of S-integral points on $\mathbf{X}$ is denoted $\mathbf{X}(\mathcal{O}_{K,S})$.

This definition is completed by the following remarks:

1. We adopt the convention that a congruence modulo ∞ is an equality. In this way, the S-integral points on $\mathbf{X} = (X; P_1, \infty; P_2, \infty; \ldots; P_r, \infty)$ are just the S-integral points on $\mathcal{X}$, relative to the effective divisor $P_1 + \cdots + P_r$.
2. A smooth projective curve is a special case of an M-curve (where one assigns a multiplicity of 1 to every K-rational point). In that case, the set $\mathbf{X}(\mathcal{O}_{K,S})$ of S-integral points is equal to the set $X(K)$ of K-rational (or, equivalently, integral) points on the underlying projective curve.
3. A *caveat*: Note that the definition of $\mathbf{X}(\mathcal{O}_{K,S})$ depends on the choice of model $\mathcal{X}$ of X over $\mathcal{O}_{K,S}$. So one must take this model as part of the defining data for the M-curve $\mathbf{X}$. In what follows, we will often abuse notations and speak of the S-integral points on $\mathbf{X}$.

The motivating example. If $X = \mathbb{P}^1$, with its usual model over $\mathbb{Z}$, then the rational points on X are identified with the set $\mathbb{Q} \cup \{\infty\}$. If $t \in X(\mathbb{Q}) - \{\infty\}$, then, writing $t = \frac{a}{b}$ as a fraction in lowest terms, we have

$$(t \cdot 0)_v = \mathrm{ord}_v(a); \quad (t \cdot 1)_v = \mathrm{ord}_v(a-b); \quad (t \cdot \infty)_v = \mathrm{ord}_v(b). \tag{2}$$

Let $\mathbb{P}^1_{p,q,r}$ denote the M-curve $(\mathbb{P}^1; 0, p; 1, q; \infty, r)$. Then an integral point on $\mathbb{P}^1_{p,q,r}$ corresponds to a rational number $t = \frac{a}{b}$ in lowest terms such that, for all rational primes v:

$$\mathrm{ord}_v(a) \equiv 0 \pmod{p}; \quad \mathrm{ord}_v(a-b) \equiv 0 \pmod{q}; \quad \mathrm{ord}_v(b) \equiv 0 \pmod{r}.$$

By the unique factorization in $\mathbb{Z}$, it follows that

$$a = \pm x^p, \quad a - b = \pm y^q, \quad b = \pm z^r,$$

so that (x, y, z) is a primitive solution to the equation

$$\pm x^p \pm y^q = \pm z^r.$$

Hence, the integral points on the M-curve $\mathbb{P}^1_{p,q,r}$ correspond to primitive solutions of the generalized Fermat equation (up to a small sloppiness in signs, which matters only when more than two of p, q and r are even).

ANOTHER EXAMPLE. Let $f(x, y) = (x - \alpha_1 y) \cdots (x - \alpha_r y)$ be a square-free homogeneous polynomial of degree r with coefficients in $\mathbb{Z}$. Let K be the extension of $\mathbb{Q}$ generated by the α_i, and let S be the set of primes of K dividing $\mathrm{Disc}\big(f(x, 1)\big)$. Then a solution of the equation $z^m = f(x, y)$ studied in [DG] gives rise to an S-integral point $t = \frac{x}{y}$ on the M-curve over K

$$\big(\mathbb{P}^1; \alpha_1, m; \alpha_2, m; \ldots; \alpha_r, m; \infty, m/\gcd(m, r)\big).$$

Maps between M-curves. The M-curves form a category, which ought to be thought of as a natural "enlargement" of the category of curves. We describe now what are the morphisms in this category.

Let $\mathbf{X}$ and $\mathbf{Y}$ be M-curves over K, and let X and Y be the underlying smooth projective curves. If π is any morphism (defined over K) from X to Y, and P is a closed point of X, we denote by $e_\pi(P)$ the ramification index of π at the point P.

DEFINITION. A morphism $\pi: \mathbf{X} \longrightarrow \mathbf{Y}$ is a smooth proper morphism $\pi: X \longrightarrow Y$ with the property that, for all closed points $P \in X$,

$$m_{\pi(P)} \text{ divides } e_\pi(P) m_P.$$

The ratio $e_\pi(P) m_P / m_{\pi(P)}$ is called the *ramification index* of π at P, and is denoted $e_\pi(P)$.

DEFINITION. The morphism π is called *unramified* if $e_\pi(P) = 1$ for all closed points P. The degree of π is simply defined to be the degree of the underlying curve morphism π.

By enlarging the set S if necessary, we can assume (and always will, from now on) that π extends to a smooth proper morphism over $\mathcal{O}_{K,S}$ between our chosen S-integral models for X and Y. Once this is done, we have the following statement which justifies our definition of morphisms:

PROPOSITION. *Let $\pi: \mathbf{X} \longrightarrow \mathbf{Y}$ be a morphism of M-curves over K. Then*

$$\pi\big(\mathbf{X}(\mathcal{O}_{K,S})\big) \subset \mathbf{Y}(\mathcal{O}_{K,S}).$$

The fact that the morphism $\pi: \mathbf{X} \longrightarrow \mathbf{Y}$ sends S-integral points to S-integral points follows directly from the behaviour of the intersection number under smooth proper morphisms.

The Chevalley-Weil theorem. If $\pi: \mathbf{X} \dashrightarrow \mathbf{Y}$ is a morphism of M-curves, and P is an S-integral point on $\mathbf{Y}$, denote by $K(\pi^{-1}(P))$ the smallest field extension of K over which the points in the inverse image of P by π are defined. The "'lifting problem", broadly stated, is the question of controlling the field $K(\pi^{-1}(P))$ - say, by bounding a priori its degree, ramification, or discriminant. For example, when does an S-integral point of $\mathbf{Y}$ necessarily lift to an S-integral point on $\mathbf{X}$, by π? The following is the classical theorem of Chevalley-Weil (cf. [La], ch. 2, §8) for M-curves:

CHEVALLEY-WEIL THEOREM. *If π is unramified, then $K(\pi^{-1}(P))$ is unramified outside of S for all $P \in \mathbf{Y}(\mathcal{O}_{K,S})$.*

This theorem is quite familiar in the case of curves:

1. If $\pi: E \longrightarrow E$ is an isogeny of elliptic curves over K, then π is unramified. If S is a set of places containing the bad reduction primes for E and those dividing the degree of π, and P is any point in $E(K)$, then $\pi^{-1}(P)$ is an extension of K which is unramified outside S. This theorem plays a key role in the proof of the (weak) Mordell-Weil theorem.
2. The group of S-units in a number field K give rise to S-integral points on the M-curve $\mathbb{G}_m := (\mathbb{P}^1; 0, \infty; \infty, \infty)$. The morphism $\mathbb{G}_m \longrightarrow \mathbb{G}_m$ which sends x to x^m is unramified, and indeed the field obtained by adjoining to K an m-th root of an S-unit is unramified outside the places in S and those dividing m. (For which the morphism has "bad reduction".)

For further discussion, and a proof of the Chevalley-Weil theorem for M-curves when the underlying curve is $\mathbb{P}_1$, see [Be].

Orbifolds, and the topology of M-curves. If X is a projective curve, its complex points $X(\mathbb{C})$ form a compact Riemann surface in a natural way. For each $P \in X(\mathbb{C})$, let t_P denote a uniformizing element for the local ring of $X(\mathbb{C})$ at P.

One can associate to the data $\mathbf{X}$ an *orbifold*, denoted $\mathbf{X}(\mathbb{C})$. Its underlying set is the same as that of the Riemann surface $X(\mathbb{C})$, but its sheaf of analytic functions is defined differently: a function is now said to be locally analytic at P on the orbifold $\mathbf{X}(\mathbb{C})$ if its image in the local ring $\mathbb{C}[[t_P]]$ belongs to the subring $\mathbb{C}[[t_P^{m_P}]]$. One denotes by $\mathcal{O}_{\mathbf{X},P} = \mathbb{C}[[t_P^{m_P}]]$ the ring of locally analytic functions on $\mathbf{X}$ at P.

A morphism $\pi: \mathbf{X}(\mathbb{C}) \longrightarrow \mathbf{Y}(\mathbb{C})$ of orbifolds is simply an analytic morphism $\pi: X(\mathbb{C}) \longrightarrow Y(\mathbb{C})$ of the underlying Riemann surfaces with the property that $\pi^*(\mathcal{O}_{\mathbf{Y},\pi(P)}) \subset \mathcal{O}_{\mathbf{X},P}$, where $\pi^*(f) := f\pi$ is the pullback of f by π.

With these definitions, the reader will check that the assignment $\mathbf{X} \mapsto \mathbf{X}(\mathbb{C})$ defines a functor from the category of M-curves to the category of orbifolds which extends the usual functor sending a curve X to its underlying Riemann surface $X(\mathbb{C})$.

The Euler characteristic of a Riemann surface is defined for orbifolds by the more general formula:

$$\chi(\mathbf{X}(\mathbb{C})) = 2 - 2g(X(\mathbb{C})) - \sum_P \left(1 - \frac{1}{m_P}\right),$$

where $g(X(\mathbb{C}))$ is the genus of the Riemann surface $X(\mathbb{C})$, and the sum is taken over all points of $X(\mathbb{C})$, with the obvious convention that $\frac{1}{\infty} = 0$. Note that almost all the terms in the sum are equal to 0. If $\mathbf{X}$ is a projective curve, then this is the usual Euler characteristic; in general, it is a rational number.

RIEMANN-HURWITZ THEOREM. If $\pi: \mathbf{X} \longrightarrow \mathbf{Y}$ is a degree d morphism of M-curves, then

$$\chi(\mathbf{X}(\mathbb{C})) = d\chi(\mathbf{Y}(\mathbb{C})) - \sum_P (e_\pi(P) - 1),$$

where the sum is taken over the points of $X(\mathbb{C})$. For Riemann surfaces, this is the usual Riemann-Hurwitz formula. The proof in the case of orbifolds proceeds by a direct reduction to the case of Riemann surfaces.

A covering lemma. The following lemma allows us to reduce diophantine questions about M-curves to similar questions about curves, for which they have been more studied.

COVERING LEMMA. *If $\mathbf{X}$ is an M-curve over K with $\chi(\mathbf{X}) < 0$, then there exists a curve $\tilde{X}$ defined over some number field M, and an unramified morphism of M-curves $\pi: \tilde{X} \longrightarrow \mathbf{X}$ defined over M.*

PROOF. This result follows directly from Riemann's existence theorem: the issue is to produce a covering of the curve X, with "'prescribed ramification data". See for example [Se1].

Faltings plus epsilon. We remind the reader of Faltings' theorem for curves, formerly known as the Mordell conjecture:

FALTINGS' THEOREM. *If X is a projective curve over K with $\chi(X) < 0$, then $X(K)$ is finite.*

The theorem "Faltings plus epsilon" alluded to in the title is simply the Mordell conjecture for M-curves.

THEOREM (FALTINGS PLUS EPSILON). *If $\mathbf{X}$ is an M-curve over K with $\chi(\mathbf{X}) < 0$, then $\mathbf{X}(\mathcal{O}_{K,S})$ is finite.*

PROOF. (Cf. [DG], sec. 3.)

1. By Riemann's existence theorem, there is an unramified morphism

$$\pi: \tilde{X} \longrightarrow \mathbf{X},$$

where $\tilde{X}$ is a curve defined over some number field $M \supset K$. We extend this morphism to a smooth proper morphism over $\mathcal{O}_{M,S'}$, where S' is some finite set of places of M containing all the places above those in S.

2. If P is a point of $\mathbf{X}(\mathcal{O}_{M,S'})$, then P lifts to a point in $\tilde{X}(M_P)$, where M_P is an extension of M of degree at most d, which is unramified outside S', by the Chevalley-Weil theorem. By a theorem of Minkowski, there are finitely many such fields M_P. Let L be the compositum of all of them. It is of finite degree over K, and

$$\pi(\tilde{X}(L)) \supset \mathbf{X}(\mathcal{O}_{M,S'}) \supset \mathbf{X}(\mathcal{O}_{K,S}). \tag{3}$$

3. By the Riemann-Hurwitz formula,

$$\chi(\tilde{X}) = d\chi(\mathbf{X}) < 0.$$

Therefore $\tilde{X}(L)$ is finite by Faltings' theorem. Hence so is $\mathbf{X}(\mathcal{O}_{K,S})$, by (3). The theorem follows.

REMARKS.

1. Note that Faltings plus epsilon, applied to the M-curve

$$(\mathbb{P}^1; 0, \infty; 1, \infty; \infty, \infty)$$

gives Siegel's theorem on the finiteness of S-integral points on $\mathbb{P}^1 - \{0, 1, \infty\}$. Siegel's proof is more difficult than the one given above, because Siegel did not have the luxury of invoking Faltings' theorem. But unramified coverings of $\mathbb{P}^1 - \{0, 1, \infty\}$ also play an important role in Siegel's original proof.

2. Of course, the deepest ingredient in the proof of "Faltings plus epsilon" is Faltings' theorem invoked in step 3. The reduction to Faltings' theorem in the case of curves exploits the Chevalley-Weil theorem and the finiteness theorem of Minkowski in much the same way that it is used by Weil in his proof of the weak Mordell-Weil theorem for elliptic curves and abelian varieties. Weil's proof has its roots directly in Fermat's method of descent. Another connection between Fermat and "Faltings plus epsilon" is given by the following corollary:

COROLLARY. *If* $\frac{1}{p} + \frac{1}{q} + \frac{1}{r} < 1$, *then the generalized Fermat equation* $x^p + y^q = z^r$ *has only finitely many primitive integer solutions.*

PROOF. The primitive solutions to the generalized Fermat equation give rise to integral points on the M-curve $\mathbb{P}^1_{p,q,r}$. But

$$\chi(\mathbb{P}^1_{p,q,r}) = \frac{1}{p} + \frac{1}{q} + \frac{1}{r} - 1 < 0,$$

so that $\mathbb{P}^1_{p,q,r}(\mathbb{Z})$ is finite, by "Faltings plus epsilon".

Beyond Faltings? Admittedly, mere finiteness of the solution set for a given (p, q, r) is not all that is wanted. But the proof of "Faltings plus epsilon" suggests a *general program* for studying the generalized Fermat equation $x^p + y^q = z^r$.

1. THE GEOMETRIC STEP. Find an "explicit" unramified covering

$$\pi: X \longrightarrow \mathbb{P}^1_{p,q,r},$$

where X is a projective curve. By explicit, we mean one whose field of definition, and set of primes of bad reduction, can be controlled, and are not too large.

2. THE ARITHMETIC STEP. Understand the lifting problem, i.e, show that a point in $\mathbb{P}^1_{p,q,r}(\mathbb{Z})$ necessarily lifts to a point in $X(\mathbb{Q})$, or in $X(K)$ where K is a specific extension of the rationals which is not too large.

3. THE DIOPHANTINE STEP. Analyze carefully, and bound, the rational points on X, or those defined over the field K obtained in step 2.

The Fermat equation. To apply this general program to the study of the usual Fermat equation $x^p + y^p = z^p$, (where p is, say, an odd prime) one needs to start with an unramified covering of the M-curve $\mathbb{P}^1_{p,p,p}$, i.e., a covering $X \longrightarrow \mathbb{P}^1$ which is unramified over $\mathbb{P}^1 - \{0, 1, \infty\}$ and such that the ramification indices of all the points lying above 0, 1 and ∞ are equal to p.

The first example of such a covering that comes to mind is, of course, the Fermat curve itself. If F is the curve defined by the equation $x^p + y^p = 1$, then the map $\pi: F \longrightarrow \mathbb{P}^1_{p,p,p}$ which sends (x, y, z) to $t = \frac{x^p}{z^p}$ is an unramified morphism of degree p^2. It has good reduction outside p, and it even becomes a Galois covering over the field $\mathbb{Q}(\zeta_p)$ of pth roots of unity, with Galois group $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. The lifting problem in this case is tautological: a point on $\mathbb{P}^1_{p,p,p}(\mathbb{Z})$ lifts to a rational point on the Fermat curve. This leads (in a roundabout way) to the traditional geometric approach to Fermat's Last Theorem.

One can also consider the curve X whose function field is the fraction field of

$$\mathbb{Q}[X, Y, (X + \zeta_p^j Y)^{\frac{1}{p}}]/(X^p + Y^p - 1),$$

where ζ_p is a primitive p-th root of unity. It is an extension of $\mathbb{Q}(\zeta_p, X^p/Y^p)$ of degree p^{p+1} which has a solvable Galois group. A point in $\mathbb{P}^1_{p,p,p}(\mathbb{Z})$ lifts to a point on this curve defined over a field K which is an abelian extension of $\mathbb{Q}(\zeta_p)$ unramified outside of p. A more careful analysis allows one to analyze the ramification at p precisely, and in understanding the possible fields K that could arise in the lifting problem one is led to questions about the p-part of the ideal class group of the cyclotomic fields $\mathbb{Q}(\zeta_p)$. This is the basis for the attack on Fermat's Last theorem initiated by Kummer via the theory of cyclotomic fields. To this day, a proof of Fermat's Last Theorem based on the covering $X \longrightarrow \mathbb{P}^1_{p,p,p}$ remains elusive, although a number of deep results in this direction have been

obtained. The proof of Fermat's Last Theorem completed by Andrew Wiles had to rely on a completely different covering arising from modular curves. Here are the main lines of the proof of Fermat's last theorem, following the 3-step program described above.

STEP 1. THE GEOMETRIC STEP: MODULAR CURVES, AND THE HELLEGOUARCH-FREY TRICK. Explicit unramified covering of $\mathbb{P}^1_{p,p,p}$ can be obtained from modular curves. More precisely, the modular curve $X(2)$ which classifies elliptic curves together with a basis of points of order 2 is isomorphic to $\mathbb{P}^1$, and is given by the classical λ-line of Legendre, the universal elliptic curve over it being described by the equation

$$y^2 = x(x-1)(x-\lambda).$$

The curve $X(2)$ has three cusps associated to elliptic curves with degenerate reduction, which are given by the values $\lambda = 0, 1, \infty$. Let $X(2)_{p,p,p}$ denote the M-curve whose underlying curve is $X(2)$, with a multiplicity of p attached to each of the three cusps. Let $X(2p)$ be the usual modular curve which classifies elliptic curves with a basis of $2p$-division points. Then the natural projection

$$\pi_{Frey}: X(2p) \longrightarrow X(2)_{p,p,p}$$

is unramified, and has good reduction outside of $2p$.

The M-curve $X(2)_{p,p,p}$ is a model for $\mathbb{P}^1_{p,p,p}$, and its integral points correspond to Frey curves via the moduli interpretation. More precisely, the point $\lambda = -a^p/b^p$ of $X(2)_{p,p,p}$ (where $a^p + b^p = c^p$) corresponds to the curve $y^2 = x(x-1)(x+\frac{a^p}{b^p})$, which is a twist of the Frey curve

$$y^2 = x(x-a^p)(x+b^p).$$

The field $K = \pi^{-1}_{Frey}(\lambda)$ is closely related to the field of definition of the p-division points of this Frey curve. One is thus led to consider the p-division field of the Frey curve. (In fact, it is better to rigidify the situation somewhat, and consider the mod p Galois representation attached to the p-torsion points of the Frey curve, instead of merely the field cut out by this representation.)

STEP 2. THE ARITHMETIC STEP: THE RIBET-WILES THEOREM. Because the covering $\pi: X(2p) \longrightarrow X(2)_{p,p,p}$ is unramified and has good reduction outside of $2p$, the field $\pi^{-1}(\lambda)$ is unramified[1] outside of $2p$, for all $\lambda \in X(2)_{p,p,p}$. The work of Frey, Mazur, Serre, Ribet, and finally Wiles was directly concerned with the lifting problem associated to this covering. Let $X_0(2,p)$ be the modular curve which classifies elliptic curves with full level 2 structure and a rational subgroup of order p. This curve has 6 cusps, of which 3 are unramified for the natural projection $X_0(2,p) \longrightarrow X(2)$. Let $X_0(2,p)_{p,p,p}$ be the M-curve obtained from $X_0(2,p)$ by assigning a multiplicity of p to each of these three cusps. Then the covering $X_0(2,p)_{p,p,p} \longrightarrow X(2)_{p,p,p}$ is unramified.

[1] This can also be seen by analyzing directly the field of p-division points of the Frey curve, using Tate's analytic theory.

RIBET-WILES THEOREM. *A point in $X(2)_{p,p,p}(\mathbb{Z})$ lifts to an integral point on $X_0(2,p)_{p,p,p}(\mathbb{Z})$.*

It seems tempting to tackle this statement head on, and try to supply a direct proof. Yet a staggering amount of difficult mathematics is involved in Ribet and Wiles' argument, which rests on the deep interplay between Galois representations and modular forms. We will not even begin to scratch the surface here! An expository account of parts of their proof (described along more conventional lines) can be found in [DDT], [Se2], [Ri1] and [Wi].

STEP 3. THE DIOPHANTINE STEP: MAZUR'S THEOREM. It turns out that the Diophantine step (step 3) had been handled earlier by Mazur in his fundamental papers [Ma1] and [Ma2] on the Eisenstein ideal. In particular, it follows from Mazur's results that

THEOREM (MAZUR). *A point in $X(2)_{p,p,p}(\mathbb{Z})$ does not lift to an integral point on $X_0(2,p)_{p,p,p}(\mathbb{Z})$.*

PROOF. The Frey curve associated to $\lambda = -a^p/b^p$ is a twist of a semistable elliptic curve. Mazur shows that such a curve cannot have a rational subgroup of order p for $p \geq 5$. The result follows.

Combining the theorems of Ribet-Wiles and Mazur gives a contradiction, and Fermat's Last Theorem follows.

Modular curves and the generalized Fermat equation. Since coverings coming from modular curves have been so effective in proving Fermat's Last Theorem, it is natural to ask the following question:

QUESTION. What are the unramified coverings of $\mathbb{P}^1_{p,q,r}$ arising from modular curves? The modular curve $X_0(2)$ has two cusps, and a special point P_{1728} corresponding to an elliptic curve with invariant $j = 1728$, at which the natural map to the j-line is unramified. Let $X_0(2)_{2,p,p}$ be the M-curve whose underlying curve is $X_0(2) \simeq \mathbb{P}^1$, and where a multiplicity of 2 has been assigned to P_{1728}, and a multiplicity of p to each of the two cusps. There is an isomorphism of $X_0(2)_{2,p,p}$ with $\mathbb{P}^1_{2,p,p}$ defined over $\mathbb{Z}[\frac{1}{2}]$. If $X(2,p)$ is the curve which classifies elliptic curves with a point of order 2 and full level p structure, then the natural projection

$$X(2,p) \longrightarrow X_0(2)_{2,p,p}$$

is unramified and has good reduction outside of $2p$.

Likewise, the modular curve $X_0(3)$ has two cusps, and a special point P_0 corresponding to an eliptic curve with invariant $j = 0$, at which the natural map to the j-line is unramified. We define the M-curve $X_0(3)_{3,p,p}$ by assigning a multiplicity of 3 to P_0, and p to each of the cusps; using the same notation as before, we find that the covering

$$X(3,p) \longrightarrow X_0(3)_{3,p,p}$$

is unramified and has good reduction outside of $3p$.

By exploiting these two coverings, and following the Mazur-Ribet-Wiles approach, Loïc Merel and I proved the following theorem [DM] towards the generalized Fermat conjecture, which is the theorem"Wiles plus epsilon" referrred to in the title:

THEOREM (WILES PLUS EPSILON). *1. The equation $x^n + y^n = z^2$ has no non-trivial primitive solution for $n \geq 4$.*

2. If the Shimura-Taniyama conjecture is true, then the equation $x^n + y^n = z^3$ has no non-trivial primitive solution for $n \geq 3$.

The Shimura-Taniyama conjecture needs to be assumed for part 2 because the elliptic curves that arise in the proof are not known to be modular, in spite of the recent work of Conrad, Diamond and Taylor: their conductor is frequently divisible by 27.

Can one go further than this? Here is a table listing the exponents (p, q, r) for which one might tackle the generalized Fermat equation by exploiting a "Frey curve" construction.

(p,q,r)	Frey curve for $a^p + b^q = c^r$	Δ
$(2,3,p)$	$y^2 = x^3 + 3bx + 2a$	$-2^6 3^3 c^p$
$(3,3,p)$	$y^2 = x^3 + 3(a-b)x^2 + 3(a^2 - ab + b^2)x$	$-2^4 3^3 c^{2p}$
$(4,p,4)$	$y^2 = x^3 + 4acx^2 - (a^2 - c^2)^2 x$	$2^6(a^2 - c^2)^2 b^{2p}$
$(5,5,p)$	$y^2 = x^3 - 5(a^2 + b^2)x^2 + 5\frac{a^5+b^5}{a+b}x$	$2^4 5^3 (a+b)^2 c^{2p}$
$(7,7,p)$	$y^2 = x^3 + (a^2 + ab + b^2)x^2$ $-(2a^4 - 3a^3b + 6a^2b^2 - 3ab^3 + 2b^4)x$ $-(a^6 - 4a^5b + 6a^4b^2 - 7a^3b^3 + 6a^2b^4 - 4ab^5 + b^6)$	$2^4 7^2 (\frac{a^7+b^7}{a+b})^2$
$(p,p,2)$	$y^2 = x^3 + 2cx^2 + a^p x$	$2^6(a^2b)^p$
$(p,p,3)$	$y^2 + cxy = x^3 - c^2x^2 - \frac{3}{2}cb^p x + b^p(a^p + \frac{5}{4}b^p)$	$3^3(a^3b)^p$
(p,p,p)	$y^2 = x(x - a^p)(x + b^p)$	$2^4(abc)^{2p}$

The cases of exponents $(p, p, 2)$ and $(p, p, 3)$ are disposed of in [DM], and the results proved there also imply that the equation with exponents $(4, p, 4)$ has no non-trivial primitive solution for $p > 2$. (Cf. [Da].) But the methods used by Frey, Serre, Mazur, Ribet and Wiles to eventually resolve Fermat's Last Theorem are extremely delicate, particularly as concerns the Ribet-Wiles lifting theorem. For the other triples of exponents, one seems to run into difficulties caused by the presence of modular forms. In spite of this, A. Kraus [Kr] has obtained some partial results in the case of exponent $(3, 3, p)$, which imply in particular that the associated generalized Fermat equation has no non-trivial primitive solution when $17 \leq p \leq 10000$.

In conclusion, here are two questions:

1. Can one refine the existing techniques based on elliptic curves, modular forms, and Galois representations to prove the generalized Fermat conjecture for all the exponent listed in the above table?
2. Can one find other examples of unramified coverings $X \longrightarrow \mathbb{P}^1_{p,q,r}$ (admitting, perhaps, a nice moduli-theoretic interpretation) for which a program of attack similar to the one of Mazur, Ribet and Wiles can be carried out?

These questions may appear ambitious, especially the second. Of course, the generalized Fermat equation fits right into the body of questions addressed by the famous abc conjecture, which has received much recent attention although a proof seems nowhere in sight. Thus we can hope that the Queen of Mathematics will hold on to the mystery of the generalized Fermat equation for at least a few more decades, to the bafflement (and delight) of number theorists, amateur and professional alike.

References

[Be] S. Beckmann, *On extensions of number fields obtained by specializing branched coverings*, Jour. für die reine und ang. Math. **419** (1991), 27–53.

[Da] H. Darmon, *The equation* $x^4 - y^4 = z^p$, C.R. Math. Rep. Acad. Sci. Canada. **XV** No. 6 (1993) pp. 286–290.

[DDT] H. Darmon, F. Diamond, R. Taylor, *Fermat's Last Theorem*, Current Developments in Math, Vol. **1**, pp. 1–157, International Press, 1996.

[DG] H. Darmon, A. Granville, *On the equations* $x^p + y^q = z^r$ *and* $z^m = f(x, y)$, Bulletin of the London Math. Society, no 129, **27** part 6, November 1995, pp. 513–544.

[DM] H. Darmon, L. Merel, *Winding quotients and some variants of Fermat's Last Theorem*, Journal für die Reine und Angewandte Mathematik, to appear.

[Kr] A. Kraus, *Sur l'équation* $a^3 + b^3 = c^p$, J. of Experimental Math., to appear.

[La] S. Lang, Fundamentals of Diophantine Geometry, Springer-Verlag, 1983.

[Ma1] B. Mazur, *Modular curves and the Eisenstein ideal*, Publ. Math. IHES **47** (1977) 33–186.

[Ma2] B. Mazur, *Rational isogenies of prime degree*, Inv. Math. **44** (1978), 129–162.

[Ma3] B. Mazur, *Questions about number*, in: New Directions in Mathematics, to appear.

[Ri1] K. Ribet, *On modular representations of* $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ *arising from modular forms*, Invent. Math. **100** (1990), 431–476.

[Ri2] K. Ribet, *On the equation* $a^p + 2^\alpha b^p + c^p = 0$, Acta Arithmetica, to appear.

[Se1] J.-P. Serre, Topics in Galois Theory, Jones and Bartlett, 1992.

[Se2] J.-P. Serre, *Sur les représentations modulaires de degré 2 de* $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$, Duke Math. J. Vol. **54** no. 1 (1987), 179–230.

[TW] R. Taylor and A. Wiles, *Ring theoretic properties of certain Hecke algebras*, Annals of Math. **141**, No. 3, 1995, pp. 553–572.

[Wi] A. Wiles, *Modular elliptic curves and Fermat's last theorem*, Annals of Math. **141**, No. 3, 1995, pp. 443–551.

Department of Mathematics and Statistics
McGill University
Montreal, Quebec, H3A 2K6

C. R. Math. Rep. Acad. Sci. Canada Vol. **19** (1), 1997 pp. 15–20

THE SCHUR PROPERTY AND THE WRNP FOR SUBMODULES OF THE DUAL OF THE FOURIER ALGEBRA $A(G)$

EDMOND E. GRANIRER, F. R. S. C.

ABSTRACT. A particular case of our main result is the

THEOREM. *Let G be a locally compact group $F \subset G$ be a closed subset. Assume that $H \cap G$ contains a perfect set for some closed subgroup H for which H_d is amenable. Then $A(F)$ contains an isomorph of ℓ^1. Consequently $A(F)^*$ has neither the* WRNP *nor the Schur property* (SP). *The result holds for the Herz algebras $A_p(G)$, $p \neq 2$ if G is amenable.*

As known, if G is abelian and F is compact and scattered then $A(F)$ does not contain ℓ^1 and $A(F)^*$ has the RNP and the SP.
The above improves a result of Lust-Piquard [LP] and of ours [Gr].

RÉSUMÉ. Notre resultat implique le

THÉORÈME. *Soit G un groupe localement compact $F \subset G$ fermé, $H \subset G$ un subgroupe fermé tel que H_d est moyenable. Supposons que $H \cap F$ contient un ensemble parfait. Alors $A(F)$ contient ℓ^1. Par conséquence $A(F)^*$ ne possède ni le* WRNP *ni la propriété de Schur* (SP).

Comme il est connu si G est abelien et F est un compact dispersé, $A(F)^*$ possède le RNP ainsi que le SP. Le résultat améliore un résultat de Lust-Piquard [LP] ainsi que le notre [Gr].

1. **Introduction.** Let G be a locally compact group (l.c.gp.) and G_d denote G with discrete topology. Let J be a closed ideal of the Fourier algebra $A = A(G)$ of G (see [Ey]). Let $Z(J) = \{x \in G : v(x) = 0 \text{ for } v \in J\}$. If $F \subset G$ is closed let $I_F = \{v \in A : v = 0 \text{ on } F\}$.

Let A/J (or $A(F) = A/I_F$) be the quotient algebra and $\mathbf{P} = (A/J)^*$ its dual. For $\Phi \in A^*$ let supp Φ stand for the support of Φ as defined in [Ey] p. 224 and let $\mathrm{PM}(F) = \{\Phi \in A^* : \text{supp } \Phi \subset F\}$. Thus $A^* = \mathrm{PM}(G)$, a digression from the notation in [Ey].

If $\mathbf{Q} \subset \mathrm{PM}(G)$ let $\mathbf{Q}_c$ be the norm closure in $\mathrm{PM}(G)$ of $\{\Phi \in \mathbf{Q} : \text{supp } \Phi \text{ is compact}\}$.

Supported by an NSERC grant A3016.
Received by the editors February 2, 1997.
AMS subject classification: Primary: 42B15, 22D15, 46B22; Secondary: 43A15, 46B20, 46E15.
Key words and phrases: Fourier algebra, locally compact group, quotient algebra, convolution operator, Schur property, WRNP.

The Banach space X has the *Schur Property* (SP) if weakly convergent sequences in X are norm convergent. For the RNP [WRNP] for X see [DU] p. 61 [see [Sa] p. 416] respectively. As known, the dual X^* has the WRNP iff X does not contain (an isomorphic copy of) ℓ^1 (see [Ja], [Mu], [Sa]).

For *abelian* G the following is known: If F is compact and scattered (*i.e.* any closed subset has an isolated point) then $\mathrm{PM}(F)$ has both the RNP and the SP. (*i.e.* $\mathrm{PM}(F)$ "behaves" like ℓ^1). This is a consequence of Loomis' lemma [Lo]. This has been substantially improved for abelian G and $1 < p \leq 2$, by Lust-Piquard [LP] to the Herz algebras $A_p(G)$ (see [Hz1]). Namely:

(a) If F is compact and scattered then $\mathrm{PM}_p(F)$ has both the RNP and the SP.

(b) If F is compact and contains a perfect set then $\mathrm{PM}_p(F)$ has neither the RNP nor the SP.

Our theorem 1 in [Gr] improves part of (b) and shows in particular:

(b′) If G_d is *amenable* and F contains some compact perfect *metrisable* set K then $\mathrm{PM}_p(F)$ does not have even the WRNP thus has ℓ^∞ as a quotient.

A particular case of the main result of this paper shows that even if K is not metrisable and G_d is not amenable but a weaker condition is imposed on F then (b′) still holds and in addition $\mathrm{PM}_p(F)$ does not have the SP.

The main results of the paper are:

THEOREM. *Let G be a l.c.gp. and J be a closed ideal in $A = A(G)$. Assume that $Z(J) \cap H$ contains a perfect set for some closed subgroup H such that H_d is amenable. Then $A(G)/J$ contains ℓ^1.*

If $1 < p < \infty$ and $p \neq 2$ then $A(G)$ can be replaced by $A_p(G)$ provided G is amenable.

COROLLARY. *Hence each of $\mathbf{P} = (A/J)^*$ and $\mathbf{P}_c$ has neither the* WRNP *nor the* SP, *and both have ℓ^∞ as a quotient.*

If $1 < p < \infty$ and $p \neq 2$ then $A(G)$ can be replaced by $A_p(G)$ provided G is amenable.

We do not know how to omit the condition that H_d is amenable even for the compact group $G = \mathrm{SO}(3)$. We also note that the abelian methods used in [LP] are not available in our case.

SOME NOTATION. For $A(G)[A_p(G)]$ see [Ey] [see [Hz1]], with a few exceptions. Namely $A(G)^* = \mathrm{PM}(G)$. $\lambda[\lambda_d]$ denotes the left regular representation of G on $L^2(G)[\ell^2(G_d)]$. If $\mu \in M(G)$ (the bounded Borel measures on G) let

$(\lambda, \mu, u) = \int u \, d\mu$ for $u \in A(G)$. $\delta_x \in M(G)$ denotes the point mass at $x \in G$. Let $1_L(x) = 1, [0]$ if $x \in L$ [if $x \notin L$]. Let $\mathrm{PF}(G)$ denote the norm closure of $\{\lambda f : f \in L^1(G)\}$ in $\mathrm{PM}(G)$.

For amenable l.c.gps. see Paterson [Pa].

If X, Y are Banach spaces (see [LT]) then Y is a quotient of X if Y is isomorphic to a quotient of X. X is said to contain ℓ^1 if X contains an isomorph of ℓ^1, see [LT].

2. The Proofs.

PROOF OF THE THEOREM. Let $K \subset Z(J) \cap H$ be a perfect set. Let $O \subset G$ be open with (closure) cl O being compact and such that $O \cap K \neq \emptyset$. If $a \in O \cap K$, there is a net $k_\alpha \in K$ such that $k_\alpha \to a$ and $k_\alpha \neq a$ for all α. Hence for some α_0, $k_\alpha \in O \cap K$ if $\alpha \geq \alpha_0$. Thus a is an accumulation point of $O \cap K$ and so is any $b \in$ cl $(O \cap K)$. Thus $K_1 =$ cl $(O \cap K)$ is a perfect compact subset of K. Now by Rudin ([Ru], thm. 8) K_1 contains a countable subset D, which is dense in itself. Thus $K_0 =$ cl D is a separable perfect compact subset of K, hence of $Z(J) \cap H$.

Let now L be the countable group generated algebraically by D. Then 1_L is a positive definite function on G_d. Since $L_d \subset H_d$, L_d is amenable. Hence there exists a sequence of positive definite functions with finite support $v_n \in A(L_d)$, such that $v_n(x) \to 1$ for all $x \in L$. We can assume, by dividing by $v_n(e) = \|v_n\|$, that $1 = v_n(e) = \|v_n\|$. Let u_n be defined on G by $u_n(x) = v_n(x)$ if $x \in L$, and $u_n(x) = 0$ if $x \notin L$. Then by [Hz1] prop. 5, p. 106, $u_n \in A(G_d)$ and $\|u_n\| = \|v_n\| = v_n(e) = u_n(e)$. Hence u_n is positive definite and $u_n(x) \to 1_L(x)$ for all $x \in G$. Hence $1_L \in B_{\lambda_d}(G_d)$ by [Ey] prop. 1.21. It follows that

$$(*) \qquad \begin{aligned} \left|\left(1_L, \sum_{i=1}^n \alpha_i \lambda \delta_{x_i}\right)\right| &= \left|\sum_{i=1}^n \alpha_i 1_L(x_i)\right| \leq \left\|\sum_{i=1}^n \alpha_i \lambda \delta_{x_i}\right\|_{\mathrm{PF}_2(G_d)} \\ &\leq \left\|\sum_{i=1}^n \alpha_i \lambda \delta_{x_i}\right\|_{\mathrm{PM}_2(G)} \end{aligned}$$

where the first inequality holds since $1_L(e) = 1 = \|1_L(e)\|_{B_\lambda(G_d)}$, and the second by [DR] thm. 2.5, p. 438.

Now by Herz's main theorem in [Hz2], the embedding $\mathrm{PM}_p(G) \subset \mathrm{PM}_2(G)$ is a contraction if G is amenable, which is assumed if $p \neq 2$. Define now the linear

functional F by $(F, \sum_1^n \alpha_i \lambda\delta_{x_i}) = \sum_i^n \alpha_i 1_L(x_i)$. Then

$$(**) \qquad \left|\left(F, \sum_1^n \alpha_i \lambda\delta_{x_i}\right)\right| \leq \left\|\sum_1^n \alpha_i \lambda\delta_{x_i}\right\|_{\mathrm{PM}_p(G)} \quad \text{if } p \neq 2.$$

Let now, by Hahn-Banach, F_1 be a norm preserving extension of F to all of $\mathrm{PM}_p(G)$, where p is fixed in $1 < p < \infty$, where we assume that G is amenable only in case $p \neq 2$. If $p = 2$ [$p \neq 2$] then such F_1 exists by (*) [by (**)] respectively. Let F_0 be the restriction of F_1 to $\mathbf{P} = (A_p/J)^*$.

Restrict now F_0 to the w^* compact set $K_0^{\mathbf{P}} = \{\lambda\delta_x : x \in K_0\} \subset \mathbf{P}$ where $K_0 = \mathrm{cl}\ D$. If $M = L \cap K_0$ then $(F_0, \lambda\delta_x) = (F, \lambda\delta_x) = 1_M(x)$, if $x \in K_0$. Now M is a countable dense subset of the perfect compact set K_0, since $D \subset M$. And $\{x \in K_0 : x \notin M\}$ is also dense in K_0 by Baire category, or see [Gr] p. 41. Hence $1_M(x)$, as a function on K_0, has no point of continuity. Thus F_0, restricted to the w^* compact set $K_0^{\mathbf{P}} \subset \mathbf{P}$ (which is homeomorphic to K_0), has no point of w^* continuity.

We apply now Theorem 1 of E. Saab [Sa] to the Banach space $\mathbf{P} = (A_p/J)^*$, and get that $\mathbf{P}$ does not have the WRNP. Hence A_p/J contains a subspace $\mathbf{N}$ isomorphic to ℓ^1. ∎

PROOF OF THE COROLLARY. Let $\mathbf{N}$ be the space defined above. Let $t: \mathbf{P} \to \mathbf{N}^*$ be the restriction map given by $(t\Phi, h) = (\Phi, h)$, for $h \in \mathbf{N}$. Then t is continuous and onto $\mathbf{N}^*$. Thus $\mathbf{P}$ has ℓ^∞ as a quotient. Apply now this fact to $\mathbf{P}_0 = (A_p/I_{K_0})^*$, where K_0 was defined above. Then A_p/I_{K_0} contains ℓ^1, hence by H. Rosenthal theorem 3(10), and noting that the separability of B is not used there, we get that $\mathbf{P}_0$ (and since $\mathbf{P}_0 \subset \mathbf{P}_c$) and $\mathbf{P}_c$, contain $L^1[0,1]$. Using now a result of Ghoussoub and P. Saab in [GS], namely that a Banach space with the WRNP cannot contain $L^1[0,1]$, we get that $\mathbf{P}_c$ does not have the WRNP. Thanks are due to E. Saab for this $L^1[0,1]$ argument.

As for the SP, by Diestel [Di] p. 212, if the dual X^* has the SP, then X does not contain ℓ^1. Hence $\mathbf{P}$ does not have the SP, since A_p/J contains ℓ^1. Applying this to $\mathbf{P}_0 = (A_p/I_{K_0})$ we get that $\mathbf{P}_0$ (and since $\mathbf{P}_0 \subset \mathbf{P}_c$) and also $\mathbf{P}_c$ does not have the SP. ∎

REMARKS. 1. The above theorem should hold without any assumption on the closed subgroup H. We used above that the subgroup L_d is amenable, hence the linear functional $\left(F, \sum \alpha_i \lambda\delta_{x_i}\right) = \sum \alpha_i 1_L(x_i)$ is continous, on the linear span of $\{\lambda\delta_x : x \in G\}$ equipped with $\mathrm{PM}_2(G_d)$ norm. Thus 1_L is a pointwise limit

of positive definite functions in $B_\lambda(G)$ (*i.e.* $B(G)$, if G is amenable). But there exists a subgroup L of the compact group $G = SO(3)$ for which 1_L cannot be approximated in this way. Namely let L be the subgroup generated algebraically by the 3 rotations about the x, y, z axes in R^3 with angle $\arccos(-3/5)$. Then by Bekka and Valette [BV] p. 4 and by P. Sarnak [Sar] Ch. 2. (2.5) L is the required subgroup. Our proof fails if this L is the subgroup generated by D in the proof above.

2. If $G = R$ and F is a Helson perfect compact set then $A(F) = C(F)$ *does not contain a complemented copy* of ℓ^1. If however $F \subset R$ is the 1/3 Cantor set or any other symmetric set then $A(F)$ contains a *complemented* copy of ℓ^1 (see [Gr] p. 42 and use [LT] p. 103).

3. Lust-Piquard uses in the proof of (b) in the introduction that any perfect set $F \subset G$ contains a perfect Helson set E, a result of Varopoulos ([Va] Ch. 4.3). Hence $\mathrm{PM}_2(E) = M(E) = \mathrm{PM}_p(E)$, and as known $M(E)$ has neither the RNP nor the SP. This result of [Va] is not available for *nonabelian* G. Furthermore, to show that $\mathrm{PM}_p(F)$ does not have the SP we need to show first that A_p/J contains ℓ^1, *i.e.* that $\mathbf{P}$ does not have the WRNP (the RNP is not enough).

4. R. C. James has shown that there exist Banach spaces X such that X^* has the WRNP but not the RNP ([DU] p. 214). Lust-Piquard's combined with our result show, for abelian G, that $\mathbf{P} = (A_p/J)^*$ cannot be such a James space, for any closed ideal J.

Question: Does some perfect subset F of $G = \mathrm{SO}(3)$ exist, such that $\mathrm{PM}_p(F)$ does not have ℓ^∞ as a quotient, for some $p > 1$?

References

[BV] M. E. B. Bekka and A. Valette, *On duals of Lie groups made discrete.* J. reine angew. Math. **439**(1993), 1–10.

[DU] J. Diestel and J. J. Uhl Jr, *Vector Measures.* In: Mathematical Surveys **15**. Amer. Math. Soc., 1977.

[Di] J. Diestel, *Sequences and series in Banach Spaces.* Grad. Texts in Math. Springer-Verlag, 1984.

[DuR] C. Dunkl and D. Ramirez, *C^* algebras generated by Fourier-Stieltjes transforms.* Trans. Amer. Math. Soc. **164**(1972), 435–441.

[Ey] P.Eymard. *L'algebre de Fourier d'un groupe localement compact.* Bull. Soc. Math. France, **92**(1964) 181–236.

[GS] N. Ghoussoub and P. Saab, *On the Weak Radon Nikodym property.* Proc. Amer. Math. Soc. **81**(1981), 81–84.

[Gr] E. E. Granirer, *On convolution operators with small support which are far from being convolution by a bounded measure.* Colloq. Math. **67**(1994), 33–60.

[GrE] E. E. Granirer, *Erratum to "On convolution operators with small support ...".* Colloq. Math. **69**(1995), 155.

[Hz1] C. Herz, *Harmonic synthesis for subgroups.* Ann. Inst. Fourier (Grenoble) **23**(1973), 91–123.

[Hz2] C. Herz, *The theory of p-spaces with an application to convolution operators.* Trans. Amer. Math. Soc. **154**(1971), 69–82.

[Ja] L. Janicka, *Some measure-theoretical characterisations of Banach spaces not containing* ℓ^1. Bull. Acad. Pol. Sci. Ser. Math. **27**(1979), 561–565.

[LP] F. Lust-Piquard, *Means on* $CV_p(G)$*-subspaces of* $CV_p(G)$ *with the* RNP *and the Schur property.* Ann. Inst. Fourier (Grenoble) **39**(1989), 969–1006.

[Lo] L. H. Loomis, *The spectral characterisation of a class of almost periodic functions.* Ann. of Math. **72**(1960), 362–368.

[LT] J. Lindenstrauss and L. Tzafriri, *Classical Banach spaces. Vol. 1.* Springer-Verlag, 1977.

[Mu] K. Musial, *The weak Radon-Nikodym property for Banach spaces.* Studia. Math. **64** (1978), 151–174.

[Pa] A. L. T. Paterson, *Amenability.* In: Mathematical Surveys and Monographs **29**. Amer. Math. Soc., 1988.

[Ro] H. Rosenthal, *Some recent discoveries in the isomorphic theory of Banach spaces.* Bull. Amer. Math. Soc. **54**(1978), 803–831.

[Ru] W. Rudin, *Averages of continuous functions on compact spaces.* Duke Math. J. **25**(1958), 197–204.

[Sa] E. and P. Saab, *A dual geometric characterisation of Banach spaces not containing* ℓ^1. Pac. J. Math. **105**(1983), 415–425.

[Sar] P. Sarnak, *Some applications of modular forms.* Cambridge University Press, 1990.

[Va] N. Th. Varopoulos, *Tensor algebras and Harmonic analysis.* Acta Math. **119**(1967), 51–112.

Mathematics Department
University of British Columbia
Vancouver, B. C. V6T 1Y4
email: garnirer@math.ubc.ca

C. R. Math. Rep. Acad. Sci. Canada Vol. **19** (1), 1997 pp. 21–23

NOTE ON EXTENSIONS $R[\alpha]$ AND $R[\alpha] \cap R[\alpha^{-1}]$ OF AN INTEGRAL DOMAIN R

TAKASI SUGATANI AND KEN-ICHI YOSHIDA

Presented by Kunio Murasugi, F. R. S. C.

ABSTRACT. Let R be an integral domian and α be an anti-integral element over R. We give a condition for $R[\alpha] \cup R[\alpha^{-1}]$ to be integrally closed in $R[\alpha]$ provided that $R[\alpha] \cup R[\alpha^{-1}]$ is seminormal in $R[\alpha]$. We further give an example that $R[\alpha] \cup R[\alpha^{-1}]$ being seminormal in $R[\alpha]$ does not imply that $R[\alpha] \cup R[\alpha^{-1}]$ is integrally closed in $R[\alpha]$

1. **Introduction.** Let R be an integral domain with quotient field K and let L be an algebraic field extension of K. Let α be a nonzero element of L. Let $R[X]$ denote a polynomial ring, and let $\pi: R[X] \to R[\alpha]$ be the R-algebra homomorphism sending X to α. Let $\varphi_\alpha(X)$ be the monic minimal polynomial of α over K with $\deg \varphi_\alpha(X) = d$ and write $\varphi_\alpha(X) = X^d + \eta_1 X^{d-1} + \cdots + \eta_d$. Let $I_{[\alpha]} := \bigcap_{i=1}^{d} (R :_R \eta_i)$. The element α is called an *anti-integral* element of degree d over R if $\operatorname{Ker} \pi = I_{[\alpha]} \varphi_\alpha(X) R[X]$. (See [5] for details.) We put $R(\alpha) = R[\alpha] \cap R[\alpha^{-1}]$. It then follows that $R(\alpha)$ is an integral extension of R [2, Exercise 4, p. 12], and $R(\alpha) = R$ if α is an anti-integral element of degree one over R [3], [5].

Our objective is to give a condition for $R(\alpha)$ to be integrally closed in $R[\alpha]$.

All rings are commutative with identity, and our general references for undefined terminology are [2] and [4].

The following facts are stated under the assumption that R is Noetherian, but the proofs do not require the Noetherian assumption.

FACT 1 ([6, THEOREM 5]). If both α and α^{-1} are anti-integral over R and $I_{[\alpha]}$ is a radical ideal of R, then $R(\alpha)$ is integrally closed in $R[\alpha]$.

FACT 2 ([1, THEOREM 6]). α is anti-integral over R if and only if α^{-1} is.

An immediate consequence of these facts is:

THEOREM 3. *Assume that α is anti-integral over R and that $I_{[\alpha]}$ is a radical ideal of R. Then $R(\alpha)$ is integrally closed in $R[\alpha]$.*

REMARK 4. Let k be a field, and let s, t be two indeterminates. Consider the ring $R = k + tk(s)[[t]]$, a subring of the formal power series ring $k(s)[[t]]$. Then it

Received by the editors February 14, 1997.
AMS subject classification: No AMS Numbers supplied.

is readily seen that R is integrally closed in the quotient field $k(s)[[t]][t^{-1}]$. Now by [4, (11.13)] we see that $\alpha = t^{-1}$ is anti-integral over R with $I_{[\alpha]} = tR$. This observation shows that the converse of Theorem 3 does not hold.

The following is proved in [1, Theorem 1] in a slightly different form, but it is easy to see that the proof ensures us, without the assumption that R is Noetherian, this form.

PROPOSITION 5. *Assume that α is an anti-integral element of degree d over R. Then $R(\alpha) = R \oplus I_{[\alpha]}\zeta_1 \oplus \cdots \oplus I_{[\alpha]}\zeta_{d-1}$ (direct sum), where $\zeta_i = \alpha^i + \eta_1\alpha^{i-1} + \cdots + \eta_{i-1}\alpha, i = 1, \ldots, d-1$.*

REMARK 6. For an anti-integral element α over R, one can see easily that (1) $R(\alpha)$ is a finite R–module if and only if $I_{[\alpha]}$ is a finitely generated ideal of R and (2) $R(\alpha)$ is Noetherian if and only if R is.

Now we recall that a subring A of a ring B is *seminormal in B* if whenever $b \in B$ with $b^2, b^3 \in A$ implies $b \in A$.

THEOREM 7. *Assume that α is an anti-integral element of degree d over R with the minimal polynomial $\varphi_\alpha(X) = X^d + \eta_1 X^{d-1} + \cdots + \eta_d$. Assume that $\eta_1 \in I_{[\alpha]} :_K I_{[\alpha]}$ if $d = 1$, and $\eta_1, \eta_2 \in I_{[\alpha]} :_K I_{[\alpha]}$ if $d \geq 2$. If $R(\alpha)$ is seminormal in $R[\alpha]$, then $R(\alpha)$ is integrally closed in $R[\alpha]$.*

Proof. By Theorem 3, we need only show that $I_{[\alpha]}$ is a radical ideal of R. To this end, let $a \in R$ such that $a^2 \in I_{[\alpha]}$.

Assume that $d = 1$. Since $a^2\eta_1 \in I_{[\alpha]}$, it follows that $(a\eta_1)^2 \in R$. Similarly, $(a\eta_1)^3 \in R$. Now $R = R(\alpha)$ is seminormal in $R[\alpha]$. We have $a \in I_{[\alpha]}$.

Assume that $d = 2$. Then we have

$$(a\zeta_1)^2 = a^2\alpha^2 = -a^2\eta_1\alpha - a^2\eta_2 = -a^2\eta_1\zeta_1 - a^2\eta_2$$

and

$$\begin{aligned}(a\zeta_1)^3 &= a^3(-\eta_1\alpha^2 - \eta_2\alpha)\\ &= a^3\big(\eta_1(\eta_1\alpha + \eta_2) - \eta_2\alpha\big)\\ &= a^3({\eta_1}^2 - \eta_2)\zeta_1 + a^3\eta_1\eta_2.\end{aligned}$$

Note that $a^3{\eta_1}^2 = \eta_1(a^3\eta_1) \in \eta_1 I_{[\alpha]} \subseteq I_{[\alpha]}$. It follows from Proposition 5 that $(a\zeta_1)^2, (a\zeta_1)^3 \in R(\alpha)$, and hence $a\zeta_1 \in R(\alpha)$. Now the representation $R(\alpha) = R \oplus I_{[\alpha]}\zeta_1 \oplus \cdots \oplus I_{[\alpha]}\zeta_{d-1}$ is a direct sum, which in turn implies that $a \in I_{[\alpha]}$.

Assume that $d = 3$. Then we have

$$(a\zeta_1)^2 = a^2(\alpha^2 + \eta_1\alpha) - a^2\eta_1\alpha = a^2\zeta_2 - a^2\eta_1\zeta_1$$

and

$$\begin{aligned}(a\zeta_1)^3 &= a^3(-\eta_1\alpha^2 - \eta_2\alpha - \eta_3)\\ &= -a^3\eta_1(\alpha^2 + \eta_1\alpha) + a^3({\eta_1}^2 - \eta_2)\alpha - a^3\eta_3\\ &= -a^3\eta_1\zeta_2 + a^3({\eta_1}^2 - \eta_2)\zeta_1 - a^3\eta_3.\end{aligned}$$

We see as in the above case that $(a\zeta_1)^2, (a\zeta_1)^3 \in R(\alpha)$, and hence $a\zeta_1 \in R(\alpha)$. Therefore $a \in I_{[\alpha]}$.

Assume that $d \geq 4$. Then we have

$$(a\zeta_1)^2 = a^2(\alpha^2 + \eta_1\alpha) - a^2\eta_1\alpha = a^2\zeta_2 - a^2\eta_1\zeta_1$$

and

$$\begin{aligned}(a\zeta_1)^3 &= a^3(\alpha^3 + \eta_1\alpha^2 + \eta_2\alpha) - a^3\eta_1(\alpha^2 + \eta_1\alpha) + a^3({\eta_1}^2 - \eta_2)\alpha\\ &= a^3\zeta_3 - a^3\eta_1\zeta_2 + a^3({\eta_1}^2 - \eta_2)\zeta_1.\end{aligned}$$

Then as in the same manner we have $a \in I_{[\alpha]}$. Hence $I_{[\alpha]}$ is a radical ideal of R. Thus $R(\alpha)$ is integrally closed in $R[\alpha]$.

Finally, we give an example showing that the condition that α is anti-integral over R and $R(\alpha)$ is seminormal in $R[\alpha]$, does not imply that $R(\alpha)$ is integrally closed in $R[\alpha]$.

EXAMPLE 8. Let denote by $\mathbb{C}$ and $\mathbb{R}$ the complex number field and the real number field, respectively. Let t be an indeterminate. Consider the ring $R = \mathbb{R} + t\mathbb{C}[[t]]$, the subring of the formal power series ring $\mathbb{C}[[t]]$ over $\mathbb{C}$. Let $\alpha = t^{-1}$. Then it can be easily checked that α is anti-integral over R [5, Theorem 2.11], and $R(\alpha) = R$ is seminormal, but not integrally closed in $R[t^{-1}]$, the quotient field of R.

REFERENCES

1. M. Kanemitsu and K. Yoshida, *Some properties of extensions $R[\alpha] \cap R[\alpha^{-1}]$ over Noetherian domains R.* Comm. in Alg., **23**(1995), 4501–4507.
2. I. Kaplansky, *Commutative Rings.* Univ. Chicago Press, Chicago/London, 1974.
3. A. Mirbagheri and L. J. Ratliff, Jr., *On the intersection of two overrings.* Houston J. Math., **8**(1982), 525-535.
4. M. Nagata, *Local Rings*, Interscience Tracts in Pure and Appl. Math., No. 13, Interscience, New York, 1962.
5. S. Oda, J. Sato and K. Yoshida *High degree anti-integral extensions of Noetherian domains* Osaka J. of Math., **30**(1993), 119-135.
6. S. Oda, T. Sugatani and K. Yoshida *On extensions $R[\alpha] \cap R[\alpha^{-1}]$ of Noetherian domains R.* Math. J. Toyama Univ., **16**(1993), 109–117.

Department of Mathematics
Toyama University
Gofuku, Toyama 930
Japan

Department of Applied Mathematics
Okayama University of Science
Ridai-cho, Okayama 700
Japan

C. R. Math. Rep. Acad. Sci. Canada Vol. **19** (1), 1997 pp. 24–27

MEAN VALUE THEOREM IN TOPOLOGICAL VECTOR SPACES

LIAQAT ALI KHAN

Presented by G. F. D. Duff, F. R. S. C.

ABSTRACT. In this note we establish the mean value theorem and the mean value inequality for class of Gateaux differentiable functions $f: X \to Y$, where X and Y are topological vector spaces. We also give a shorter proof of a result of Aberbukh-Smolyanov on the mean value inclusion assuming Y a locally convex space.

Throughout this note X and Y denote Hausdorff topological vector spaces (both over the field R of real numbers), and A $\subseteq$ X an open set. A function $f: A \to Y$ is said to be *Gateaux differentiable* at $x_0 \in A$ if there exists a mapping from X into Y, denoted by $f'(x_0)$, such that, given any $z \in X$ and a balanced neighbourhood V of 0 in Y, there exists a $\delta > 0$ satisfying

$$\big(f(x_0 + tz) - f(x_0)\big)/t - f'(x_0)(z) \in V$$

whenever $0 < |t| < \delta$; $f'(x_0)$ is called the *Gateaux derivative* of f at x_0 and we briefly write as

$$f'(x_0)(z) = \lim_{t \to 0} \big(f(x_0 + tz) - f(x_0)\big)/t, \quad z \in X. \tag{1}$$

Some authors also require $f'(x_0)$ to be "linear", but we do not need it in our proofs. Note that a Gateaux differentiable function need not be continuous. For example, the function $f: R^2 \to R$, given by $f(x) = a^2b/(a^2 + b^2)$ if $x = (a, b) \neq 0$ and $f(0) = 0$, is not continuous at $x = 0$ although $f'(0) = f$ exists.

A useful reference for the background of the results of this paper is [3]; see also [1, 2, 5, 6]. Our proofs use the techniques similar to the ones used by Vainberg [6] in the case where X and Y are normed spaces.

We first consider the Lagrange form of the mean value theorem for real-valued functions on X.

THEOREM 1. *Let $g: A \to R$ be a function continuous and Gateaux differentiable at each point of the segment $[x_0, x_0 + h]$ in A. Then there exists a $\vartheta \in (0, 1)$ such that*

$$g(x_0 + h) - g(x_0) = g'(x_0 + \vartheta h)(h).$$

Received by the editors March 4, 1997.
AMS subject classification: 58C20, 26A24, 26E20, 46A03.

PROOF. Define $\phi\colon [0,1] \to R$ by $\phi(t) = g(x_0 + th)$. Then ϕ is differentiable on [0,1]. In fact, using (1), we obtain

$$\begin{aligned}\phi'(t) &= \lim_{\Delta t \to 0} \big(g(x_0 + (t + \Delta t)h) - g(x_0 + th)\big)/\Delta t \\ &= g'(x_0 + th)(h).\end{aligned}$$

By the classical mean value theorem, there exists a $\vartheta \in (0,1)$ such that $\phi(1) - \phi(0) = \phi'(\vartheta)$. Hence

$$g(x_0 + h) - g(x_0) = \phi(1) - \phi(0) = g'(x_0 + \vartheta h)(h).$$

An exact analogue of Theorem 1 for vector-valued functions need not hold as is shown by the function $f\colon [0, 2\pi] \to R^2$ defined by $f(x) = (\cos x, \sin x)$. However, for the class of these functions, the following version of the mean value theorem holds.

THEOREM 2. *Suppose Y has a non-trivial (real) continuous dual Y' and let $f\colon A \to Y$ be a function continuous and Gateaux differentiable at each point of the segment $[x_0, x_0 + h]$ in A. Then, given $u \in Y'$, there exists a $\vartheta \in (0,1)$ such that*

$$\langle f(x_0 + h) - f(x_0), u\rangle = \langle f'(x_0 + \vartheta h)(h), u\rangle. \tag{2}$$

PROOF. Define $g\colon [x_0, x_0 + h] \to R$ by $g(x) = \langle f(x), u\rangle$. Then it follows from the linearity and continuity of u that $g'(x)(h) = \langle f'(x)(h), u\rangle$. By Theorem 1, there exists a $\vartheta \in (0,1)$ such that $g(x_0 + h) - g(x_0) = g'(x_0 + \vartheta h)(h)$. This establishes (2).

The above result clearly reduces to Theorem 1 when $Y = R$.

THEOREM 3 (MEAN VALUE INEQUALITY). *Under the hypothesis of Theorem 2, given a continuous seminorm p on Y, there exists a $\vartheta \in (0,1)$ such that*

$$p\big(f(x_0 + h) - f(x_0)\big) \le p\big(f'(x_0 + \vartheta h)(h)\big). \tag{3}$$

PROOF. By the analytic form of the Hahn-Banach theorem ([4], Theorem 8, Sec, 17.3), we can choose a u ($\neq 0$) $\in Y'$ such that $\langle y, u\rangle \le p(y)$ for all $y \in Y$ and $\langle f(x_0 + h) - f(x_0), u\rangle = p\big(f(x_0 + h) - f(x_0)\big)$. By Theorem 2, there exists a $\vartheta \in (0,1)$ such that

$$\langle f(x_0 + h) - f(x_0), u\rangle = \langle f'(x_0 + \vartheta h)(h), u\rangle.$$

Consequently, we obtain (3).

As an application of the above theorem, we obtain

COROLLARY. *Supose Y is locally convex and $A \subseteq X$ an open connected set, and let $f: A \to Y$ be continuous and Gateaux differentiable at each point of A. If $f'(x) = 0$ for each $x \in A$, then f is constant on A.*

PROOF. Fix $x_0 \in A$, and let $B = \{x \in A : f(x) = f(x_0)\}$. Clearly, B is non-empty and closed in A. B is also open in A, as follows. Let $x \in B$. Choose a balanced neighbourhood V of 0 in X such that $U = x + V \subseteq A$. Then, for each $y \in U, [x, y] \subseteq U$. Hence, for each $y \in U$ and any continuous seminorm p on Y, it follows from Theorem 3 and the hypothesis that

$$p(f(y) - f(x)) \leq \sup_{z \in [x,y]} p(f'(z)(y - x)) = p(0) = 0.$$

Since Y is Hausdorff, $f(y) = f(x)$ for all $y \in U$. Hence $U \subseteq B$. Since A is connected, $B = A$. Thus $f(x) = f(x_0)$ for all $x \in A$.

As regards the mean value inclusion, the following general result is given in ([1], Theorem 1.8); see also ([5], Theorem 1). Using the separation form of the Hahn-Banach Theorem, we give below a shorter and direct proof of it.

THEOREM 4 (MEAN VALUE INCLUSION). *Suppose Y is a locally convex topological vector space. Then, under the hypothesis of Theorem 2,*

$$f(x_0 + h) - f(x_0) \in \overline{\text{co}}.(B)$$

where $B = \{f'(x)(h) : x \in [x_0, x_0 + h]\}$ and $\overline{\text{co}}.(B)$ is the closed convex hull of B.

PROOF. Suppose $f(x_0 + h) - f(x_0) \notin \overline{\text{co}}.(B)$. By ([4], Theorem 2, Sec. 20.7), there exists a u ($\neq 0$) $\in Y'$ and an $r \in R$ such that

$$\langle y, u \rangle \leq r < \langle f(x_0 + h) - f(x_0), u \rangle \tag{4}$$

for all $y \in \overline{\text{co}}.(B)$. Define $\phi: [0, 1] \to R$ by $\phi(t) = \langle f(x_0 + th), u \rangle$. Then $\phi'(t) = \langle f'(x_0 + th)(h), u \rangle$. There exists a $\vartheta \in (0, 1)$ such that $\phi(1) - \phi(0) = \phi'(\vartheta)$. Then

$$\langle f(x_0 + h) - f(x_0), u \rangle = \phi(1) - \phi(0) = \langle f'(x_0 + \vartheta h)(h), u \rangle,$$

which contradicts (4).

REMARK. Theorem 4 need not hold if Y is not locally convex, or if $\overline{\text{co}}.(B)$ is replaced by $\bar{B}$ or co.(B). This follows from ([1], Example 1.23–1.25).

ACKNOWLEDGEMENT. The author would like to thank Professor Abdus Salam, the International Atomic Energy Agency and UNESCO for hospitality at the International Centre for Theoretical Physics, Trieste.

REFERENCES

1. V. I. Aberbukh and O. G. Smolyanov, *The Theory of differentiation in linear topological spaces.* Russian Math Surveys 22 **6**(1967), 201–258.
2. J. Dieudonne, *Foundations of Modern Analysis.* Academic Press, London, 1969.
3. M. Furi and M. Martelli, *On the mean value theorem, inequality and inclusion.* Amer. Math. Monthly **98**(1991), 840–846.
4. G. Köthe, *Topological Vector Space I.* Springer-Verlag, New York, 1969.
5. R. M. McLeod, *Mean value theorems for vector-valued functions.* Proc. Edinburgh Math. Soc. **14**(1965), 197–209.
6. M. M. Vainberg, *Variational Methods for Study of Non-Linear Operators.* Holden-Day, San Francisco, 1964.

Department of Mathematics
King Abdul Aziz University
P.O.Box 9028, Jeddah - 21413
Saudi Arabia

C. R. Math. Rep. Acad. Sci. Canada Vol. **19** (1), 1997 pp. 28–32

A EUCLIDEAN RING CONTAINING $\mathbb{Z}\left[\sqrt{14}\right]$

DAVID A. CARDON

Presented by M. Ram Murty, F. R. S. C.

ABSTRACT. We show that the ring $\mathbb{Z}\left[\sqrt{14}, 1/2\right]$ is Euclidean and that this ring admits a totally multiplicative Euclidean function. This example is interesting because it is related to the ring $\mathbb{Z}\left[\sqrt{14}\right]$ which is conjectured to be Euclidean but for which a proof is lacking.

RÉSUMÉ. Nous montrons que l'anneau $\mathbb{Z}\left[\sqrt{14}, 1/2\right]$ est euclidien et que cet anneau admet une fonction euclidienne totalement multiplicative. Cet exemple est intéressant car il est relié à l'anneau $\mathbb{Z}\left[\sqrt{14}\right]$, qui est conjecturé être euclidien.

Considerable effort has been spent in trying to classify the Euclidean number fields (see Lemmermeyer [8]). An integral domain R is called *Euclidean* if there is a function $\phi : R \to \{0, 1, 2, \ldots\}$ such that $\phi(a) = 0$ if and only if $a = 0$ and for every $a, b \in R$, $b \neq 0$, there exist $q, r \in R$ such that $a = bq + r$ with $\phi(r) < \phi(b)$. A number field is said to be Euclidean when its ring of integers is Euclidean.

Of the finite number of known examples of Euclidean number fields many are norm-Euclidean; that is, ϕ is the absolute value of the norm. It is well known that there are only finitely many norm-Euclidean real quadratic number fields. However, Weinberger [11] proved that if one assumes an appropriate Riemann Hypothesis then a ring of algebraic integers which is a principal ideal domain and has infinitely many units is Euclidean. Lenstra [9] extended Weinberger's result to rings of S-integers and gave an explicit Euclidean function. Clark [3] found the first example of a real quadratic number field that is Euclidean but not for the norm, the field being $\mathbb{Q}(\sqrt{69})$. Weinberger's result predicts that $\mathbb{Q}(\sqrt{14})$ as well as many other number fields should also be Euclidean.

Without using a Riemann hypothesis Samuel [10] and Bedocchi [2] provide evidence that suggests $\mathbb{Z}[\sqrt{14}]$ might be Euclidean. In this paper we will show that the related ring $\mathbb{Z}[\sqrt{14}, 1/2]$ is Euclidean with a completely multiplicative Euclidean function. Harper [5], by a more complicated method than that presented here, has shown that $\mathbb{Z}[\sqrt{14}, 1/p]$ is Euclidean for every prime p. However,

Research partially supported by NSERC
Received by the editors May 7, 1997.
AMS subject classification: 11R04.
Key words and phrases: Euclidean rings, algebraic number theory.

the Euclidean functions constructed by that argument are not completely multiplicative.

PROPOSITION 1. *Let* $\eta = 4 + \sqrt{14}$. (*This is the prime above* 2 *in the ring* $\mathbb{Z}[\sqrt{14}]$.) *The ring* $\mathbb{Z}[\sqrt{14}, 1/2]$ *is Euclidean with a completely multiplicative Euclidean function* ϕ *given by*

$$\phi(x) = |\mathrm{Norm}(x')|$$

where $\mathrm{Norm}(a + b\sqrt{14}) = a^2 - 14b^2$ *denotes the norm of an element in* $\mathbb{Q}(\sqrt{14})$ *and* x *is written as* $x = x'\eta^\alpha$ *such that* x' *contains no power of* η.

The proposition says that if 2 is made into a unit then the ring $\mathbb{Z}[\sqrt{14}]$ becomes the Euclidean ring $\mathbb{Z}[\sqrt{14}, 1/2]$. The Euclidean function given above is the absolute norm in the ring $R = \mathbb{Z}[\sqrt{14}, 1/2]$. Thus, $\phi(x) = |R/(x)|$ which is the number of number of cosets modulo the principal ideal (x). This is also called the S-norm on $\mathbb{Q}(\sqrt{14})$ where S is the set consisting of the archimedean primes and the prime $\eta = 4 + \sqrt{14}$. The proof of proposition 1 will follows from lemmas 2 and 3 below.

Each element $\alpha + \beta\sqrt{14} \in \mathbb{Q}(\sqrt{14})$ may be thought of as a point (α, β) in the plane $\mathbb{R}^2$. We will use a geometrical argument for the quadratic form $F(x, y) = x^2 - 14y^2$ which represents the norm of $x + y\sqrt{14}$. Let Λ be the lattice of points with integer coordinates in $\mathbb{R}^2$. Every point in $\mathbb{R}^2/\Lambda$ may be represented by a point in the fundamental domain

$$D_\Lambda = \{(x, y) \,|\, 0 \le x < 1 \text{ and } 0 \le y < 1\}.$$

Let T be the linear transformation T on $\mathbb{R}^2$ given by

$$(x', y') = T(x, y) = (15x + 56y, 4x + 15y).$$

Then $F(x', y') = F(x, y)$. The transformation T is referred to as an *automorph* in [1]. The powers of T are related to the solutions of the Pellian equation $x^2 - 14y^2 = 1$. For a given lattice L in $\mathbb{R}^2$ define the inhomogeneous minimum of a point $(x, y) \in \mathbb{R}^2$ to be

$$M_L(x, y) = \liminf_{(a,b)\in L} |F(x + a, y + b)|.$$

Then it is apparent (as explained in [1]) that $M_L(x, y) = M_L(T(x, y))$. If it were the case that $M_\Lambda(x, y) < 1$ for every $(x, y) \in \mathbb{Q}^2$ we could deduce that $\mathbb{Z}[\sqrt{14}]$ was norm-Euclidean. Although this is not the case, the following lemma shows it is almost true.

LEMMA 2. $M_\Lambda(x, y) < 1$ *unless* $(x, y) \equiv (1/2, 1/2) \bmod \Lambda$. *In the exceptional case,* $M_\Lambda(1/2, 1/2) = 5/4$.

REMARK. Lemmas 2 and 3 are given as Propositions 3.1 and 3.2 in [2]; however, the proof given here is simpler.

PROOF OF LEMMA 2. It is sufficient to prove the lemma for points in D_Λ. We first show the lemma is true for points not too close to $(1/2, 1/2)$.

Consider the vectors $\bar{e}_1 = (\sqrt{14/15}, 1/\sqrt{15})$ and $\bar{e}_2 = (\sqrt{14/15}, -1/\sqrt{15})$. Then $\bar{e}_1$ and $\bar{e}_2$ are normalized eigenvectors of T such that $T(\bar{e}_1) = u\bar{e}_1$ and $T(\bar{e}_2) = u^{-1}\bar{e}_1$ where $u = 15 + 4\sqrt{14}$. Let $\epsilon = \frac{1}{2u}$ and let P be the diamond shaped region

$$P = \{(x, y) \in \mathbb{R}^2 \mid (x, y) = (1/2, 1/2) + \alpha\bar{e}_1 + \beta\bar{e}_2, |\alpha| < \epsilon, |\beta| < \epsilon\}.$$

We divide the square D_Λ into very small squares and check by computer that each of the small square has a translate modulo Λ lying strictly between the hyperbolas $F(x, y) = \pm 1$ unless the small square is entirely contained in the region P.

To deal with the exceptional points lying inside P we note that $(1/2, 1/2)$ is a fixed point of T modulo Λ. If $(x, y) = (1/2, 1/2) + \alpha\bar{e}_1 + \beta\bar{e}_2 \in P$ and $\alpha \neq 0$, choose the smallest $k > 0$ such that $|\alpha u^k| > \epsilon$ but $|\alpha u^{k-1}| < \epsilon$. Then $T^k(x, y) \in D_\Lambda \bmod \Lambda$, but $T^k(x, y) \notin P \bmod \Lambda$. This shows that (x, y) has a representative $(\tilde{x}, \tilde{y})$ with $F(\tilde{x}, \tilde{y}) < 1$ so that $M_\Lambda(x, y) < 1$. If $\beta \neq 0$ we argue similarly using negative powers of T.

The value $M_\Lambda(1/2, 1/2) = 5/4$ dates back to Heinhold [7].

The following modification of the previous lemma applies to arithmetic in $\mathbb{Z}[\sqrt{14}]$ modulo an ideal.

LEMMA 3. *Let $a, b, c, d \in \mathbb{Z}$.*

1. *Suppose c and d are not both even. Then there is a representative $\tilde{a} + \tilde{b}\sqrt{14}$ of $a + b\sqrt{14}$ modulo $c + d\sqrt{14}$ such that*

$$N(\tilde{a} + \tilde{b}\sqrt{14}) < N(c + d\sqrt{14}).$$

2. *If c and d are both even, the first part of the lemma holds except that the smallest representative of $(\frac{c}{2} + \frac{d}{2}\sqrt{14})(1 + \sqrt{14})$ modulo $c + d\sqrt{14}$ has absolute norm $\frac{5}{4}N(c + d\sqrt{14})$.*

PROOF. Let Λ be the lattice of points with generators $(1, 0)$ and $(0, 1)$. Any point of $\mathbb{R}^2$ modulo Λ may be represented in a fundamental domain

$$D_\Lambda = \{(s, t) \mid 0 \leq s < 1 \text{ and } 0 \leq t < 1\}.$$

Similarly, let Γ be the lattice with generators (c, d) and $(14d, c)$ and fundamental domain

$$D_\Gamma = \{s(c, d) + t(14d, c) \mid 0 \leq s < 1 \text{ and } 0 \leq t < 1\}.$$

Then Λ represents the whole ring $\mathbb{Z}[\sqrt{14}]$, but Γ represents the ideal generated by $c + d\sqrt{14}$. To adapt lemma 2 which applies to the case of arithmetic modulo

Λ to the case of arithmetic modulo Γ we map $(x, y) \in D_\Lambda$ to $(x', y') \in D_\Gamma$ by the linear transformation

$$(x', y') = (cx + 14dy, dx + cy).$$

Then the quadratic form $F(x, y) = x^2 - 14y^2$ at (x', y') becomes

$$F(x', y') = (c^2 - 14d^2)(x^2 - 14y^2) = (c^2 - 14d^2)F(x, y).$$

Thus, the linear transformation has simply rescaled $F(x, y)$. The 'exceptional' point $(1/2, 1/2) \in D_\Lambda$ maps to the new 'exceptional' point $(c/2+7d, d/2+c/2) \in D_\Gamma$. Hence, if $(1/2, 1/2) \neq (x, y) \in D_\Lambda$, then

$$M_\Gamma(x', y') = |c^2 - 14d^2|\, M_\Lambda(x, y) < |c^2 - 14d^2|$$

whereas

$$M_\Gamma(c/2 + 7d, d/2 + c/2) = |c^2 - 14d^2|\, M_\Lambda(1/2, 1/2) = \frac{5}{4}|c^2 - 14d^2|.$$

This proves the lemma. ∎

Proposition 1 is an immediate consequence of lemma 3. If $1/2$ is adjoined to $\mathbb{Z}[\sqrt{14}]$ then the elements 2 and $\eta = 4 + \sqrt{14}$ become units in $\mathbb{Z}[\sqrt{14}, 1/2]$. The ordinary prime 2 ramifies in $\mathbb{Z}[\sqrt{14}]$ and the prime above it is η. Define a completely multiplicative function ϕ on $\mathbb{Z}[\sqrt{14}, 1/2]$ by

$$\phi(x) = |\mathrm{Norm}(x')|$$

where $\mathrm{Norm}(a + b\sqrt{14}) = a^2 - 14b^2$ denotes the norm of an element in $\mathbb{Q}(\sqrt{14})$ and x is written as $x = x'\eta^\alpha$ such that x' contains no power of η. By inverting 2 we eliminate the difficulty caused by the evenness of c and d in the second part of lemma 3. Thus given any $a, b \in \mathbb{Z}[\sqrt{14}, 1/2]$ with $b \neq 0$ there exist q and r such that $a = bq + r$ and $\phi(r) < \phi(b)$. This completes the proof of proposition 1.

ACKNOWLEDGMENT. I would like to thank David Clark for introducing me to the problem of Euclidean number fields during a brief visit to Brigham Young University in 1995, and I wish to thank Ram Murty of Queen's University for several useful conversations. The referee made several suggestions which improved this paper. Also, the papers of Hartman [6] and Elsner [4] influenced my thinking as I studied this problem.

REFERENCES

[1] E.S. Barnes and H.P.F. Swinnerton-Dyer, *The inhomogeneous minima of binary quadratic forms (I).* Acta Mathematica **87** (1952), 259–323.

[2] Edmondo Bedocchi, *L'anneau* $\mathbb{Z}[\sqrt{14}]$ *et l'algorithme Euclidien.* Manuscripta Mathematica **53** (1985), 199–216.

[3] David A. Clark, *A quadratic field which is Euclidean but not norm-Euclidean.* Manuscripta Mathematica **83** (1994), 327–330.
[4] C. Elsner, *On the approximation of irrational numbers with rationals restricted by congruence relations.* Fibonacci Quarterly, Vol. 34, No. 1, (1996), 18–29.
[5] Malcolm Harper, McGill University Ph.D. Thesis, (1997).
[6] S. Hartman, *Sur une condition supplémentaire dans les approximations diophantiques.* Colloquium Mathematicum, Vol. 2, (1951), 48–51.
[7] Joseph Heinhold, *Verallgemeinerung und Verschärfung eines Minkowskischen Satzes.* Mathematische Zeitschrift **44** (1938), 659–688.
[8] Franz Lemmermeyer, *The Euclidean algorithm in algebraic number fields.* Expositiones Mathematicae **13** (1995), 385–416.
[9] H.W. Lenstra *On Artin's Conjecture and Euclid's Algorithm in Global Fields.* Inventiones Mathematicae **42** (1977), 201–224.
[10] P. Samuel, *About Euclidean Rings.* Journal of Algebra **19** (1971), 282–301.
[11] Peter J. Weinberger, *On Euclidean rings of algebraic integers.* Analytic Number Theory, Proceedings of Symposia in Pure Mathematics, AMS, Volume XXIV (1972), 321–332.

Department of Mathematics and Statistics
Queen's University
Kingston, Ontario K7L 3N6
email: cardon@mast.queensu.ca