C.R. Math. Rep. Acad. Sci. Canada - Vol. V, No.4, August 1983 aout

---

C.R. Math. Rep. Acad. Sci. Canada - Vol. V, No.4, August 1983 aout

A NOTE ON THE BERNOULLI NUMBERS AND THE CLASS NUMBER OF REAL QUADRATIC FIELDS

by

T. AGOH (at Chiba)

Presented by P. Ribenboim, F.R.S.C.

1. The Bernoulli numbers are defined by the formal power series expansion

$$\frac{x}{e^x - 1} = \sum_{n=0}^{\infty} B_n \frac{x^n}{n!}.$$

If n is odd, $n > 3$, then $B_n = 0$. Let p be an odd prime and $\pi = (p - 1)/2$. A pair $(p, 2k)$ is called irregular if $B_{2k} \equiv 0 \pmod p$, k being an integer such that $1 \leq k \leq \pi - 1$.

The question of whether (p, π) can be irregular for $p \equiv 1 \pmod 4$ is very interesting and important in connection with the problem of the fundamental unit in the real quadratic field $Q(\sqrt{p})$. Namely, Ankeny, Artin and Chowla [3] showed that if $p \equiv 1 \pmod 4$ and $\varepsilon = (t + u\sqrt{p})/2$, $u > 0$, is the fundamental unit of $Q(\sqrt{p})$, then

$$u \equiv 0 \pmod p \tag{1}$$

if and only if

$$(p, \pi) \text{ is an irregular pair.} \tag{2}$$

This statement has been given by proving the congruence as follows (cf. also [2] and [4]):

(I) $$\frac{hu}{t} \equiv B_\pi \pmod p,$$

where h is the class number of $Q(\sqrt{p})$.

If we assume (I), then the following congruences can be proved:

(II) $$4\frac{hu}{t} \equiv -\sum_{r=1}^{\pi/2} (r|p)\frac{1}{r} \pmod p \quad (p \equiv 5 \pmod 8),$$

(III) $$2\frac{hu}{t} \equiv \frac{A + B}{p} \pmod p,$$

where $(r|p)$ is the Legendre symbol, A is the product of quadratic residue of p between 0 and p, and B is the product of the nonresidue of p between 0 and p.

The proofs of (II) and (III) can be found in Carlitz [5].

In the present note we shall prove that if we assume (1), then the following congruences hold:

(IV) $$E\frac{hu}{t} \equiv \sum_{p/6<r<p/4} (r|p)\frac{1}{r} \pmod p$$
$$(p \not\equiv 1 \pmod{24}),$$

(V) $$2\frac{hu}{t} \equiv \frac{1}{p}(2A+1) - B_{p-1} + 1$$
$$\equiv \frac{1}{p}(2B-1) + B_{p-1} - 1 \pmod p,$$

(VI) $$4\frac{hu}{t} \equiv \sum_{r=1}^{p-1} (r|p)\, c_r$$
$$\equiv \frac{1}{p}\sum_{r=1}^{p} (r|p)(2rd_r - p(r+d_r)) \pmod p,$$

where

$$E = 6 \text{ if } p \equiv 5 \pmod{24},$$
$$= -12 \text{ if } p \equiv 13 \pmod{24},$$
$$= -6 \text{ if } p \equiv 17 \pmod{24}$$

and c_r, d_r are the smallest integers satisfying

$$pc_r = 1 + rd_r,\ 1 \le c_r \le r,\ 1 \le d_r \le p-1. \qquad (3)$$

2. In this section we shall give the proofs of the congruences (IV), (V) and (VI).

Proof of (IV). By making use of Voronoi's congruence

$$(a^{2k}-1)\frac{B_{2k}}{2k} \equiv a^{2k-1}\sum_{r=1}^{p-1}\left[\frac{ar}{p}\right]r^{2k-1} \pmod p$$
$$(p-1\nmid 2k,\ p\nmid a,\ a>0),$$

Vandiver ([7], [8]) proved

$$(4^{p-2k}+3^{p-2k}-6^{p-2k}-1)\frac{B_{2k}}{4k}$$
$$\equiv \sum_{p/6<r<p/4} r^{2k-1} \pmod p,$$

where $[ar/p]$ means the greatest integer in ar/p. Taking $2k = u$ for $p \equiv 1 \pmod 4$, we have

$$EB_u \equiv \sum_{p/6<r<p/4} (r|p)\frac{1}{r} \pmod p,$$

where

$$E = -4(2|p)^2 - 3(3|p) + 6(2|p)(3|p) + 1.$$

Since

$$(2|p) = 1 \text{ if } p \equiv 1 \pmod 8,$$
$$= -1 \text{ if } p \equiv 5 \pmod 8$$

and

$$(3|p) = 1 \text{ if } p \equiv 1 \pmod 3,$$
$$= -1 \text{ if } p \equiv 2 \pmod 3,$$

the possibilities for the value of E are

$$E_1 = 0 \text{ if } p \equiv 1 \pmod{24},$$
$$E_2 = 6 \text{ if } p \equiv 5 \pmod{24},$$
$$E_3 = -12 \text{ if } p \equiv 13 \pmod{24},$$
$$E_4 = -6 \text{ if } p \equiv 17 \pmod{24}.$$

Consequently, if $p \not\equiv 1 \pmod{24}$, then $E \not\equiv 0 \pmod{p}$. In view of (I) we can give our assertion.

We note that the congruence (IV) is more useful than (II) to test for the question of whether (1) or (2) holds, because the right hand side of (IV) contains only $([p/4] - [p/6])$ terms.

Proof of (V). If $p \equiv 1 \pmod{4}$, then

$$A \equiv (\pm 1)^2 \equiv (-1)^{\frac{p-1}{2}}(p-1)! \equiv -1 \pmod{p},$$

hence we have

$$B \equiv \frac{(p-1)!}{A} \equiv 1 \pmod{p}.$$

That is, there exist integers Ω_p and Ω_p' such that

$$A = -1 + p\Omega_p, \quad B = 1 - p\Omega_p'.$$

Since

$$(p-1)! + AB = (-1 + p\Omega_p)(1 - p\Omega_p')$$
$$\equiv -1 + p(\Omega_p + \Omega_p') \pmod{p^2},$$

it follows that

$$W_p \equiv \Omega_p + \Omega_p' \pmod{p}, \tag{4}$$

where $W_p = ((p-1)! + 1)/p$ is the Wilson quotient.

On the other hand, Carlitz states in [5] that

$$\Omega_p - \Omega_p' \equiv 2B_{\frac{p-1}{2}} \pmod{p}. \tag{5}$$

From (4) and (5) we have

$$2\Omega_p \equiv 2B_{\frac{p-1}{2}} + W_p \pmod{p},$$
$$2\Omega_p' \equiv -2B_{\frac{p-1}{2}} + W_p \pmod{p},$$

which show that (V) holds by using the relation (see e.g. [10])

$$W_p \equiv B_{p-1} + \frac{1}{p} - 1 \pmod{p}.$$

Proof of (VI). Let r be a positive integer. And, put

$$\lambda(r, i) = 0 \text{ if } r = 1,$$
$$= \sum_{\zeta}{}' \frac{\zeta^i - 1}{\zeta^p - 1} \text{ if } r \neq 1,$$

where Σ' ranges over all r-th roots ζ ($\neq 1$) of unity. Vandiver ([9], [10]) gave the congruence involving in general two Bernoulli numbers as follows: If $1 \le k < p-1$, then

$$i\frac{B_k}{k} + i^{k+1}\frac{B_{p-1-k}}{p-1-k} \equiv \sum_{r=1}^{p-1} r^k \lambda(r, i) \pmod{p}, \tag{6}$$

where i is any integer such that $1 \le i \le p-1$.

On the other hand, let $c_{r,i}$ and $d_{r,i}$ be the smallest integers satisfying

$$pc_{r,i} = i + rd_{r,i},\ 1 \le c_{r,i} \le r,\ 1 \le d_{r,i} \le p - 1.$$

If $2 \le r \le p - 1$, then

$$\lambda(r, i) = \sum{}' \frac{\zeta^{pc_{r,i}} - 1}{\zeta^p - 1} = \sum{}' \frac{\zeta^{c_{r,i}} - 1}{\zeta - 1} = r - c_{r,i}, \tag{7}$$

which contains the special case for $i \equiv 0 \pmod r$.

Setting $i = 1$ and $k = n$ in (6), it follows from (7) that if $c_r = c_{r,1}$ and $d_r = d_{r,1}$,

$$2\frac{B_n}{n} \equiv \sum_{r=1}^{p-1} r^n\lambda(r, 1) \equiv \sum_{r=1}^{p-1} r^{n+1} - \sum_{r=1}^{p-1} r^n c_r \equiv -\sum_{r=1}^{p-1} (r|p)c_r \equiv -\frac{1}{p}\sum_{r=1}^{p-1} (r|p)rd_r \pmod p,$$

since $\sum_{r=1}^{p-1} r^{n+1} \equiv 0 \pmod p$ and $\sum_{r=1}^{p-1} (r|p) = 0$. Here, if $p \equiv 1 \pmod 4$, then $(r|p) = (p - r|p)$ for $r = 1, 2, \dots, n$. Also, we have $p(c_r - c_{p-r}) = -pd_{p-r} + r(d_r + d_{p-r})$, which shows that $d_r + d_{p-r} \equiv 0 \pmod p$. On the other hand, $d_r \ne d_{r'}$ if $r \ne r'$, so that $3 \le d_r + d_{p-r} \le 2p - 3$. Hence, we have $d_r + d_{p-r} = p$ for $r = 1, 2, \dots, n$. From this fact it follows that

$$\sum_{r=1}^{p-1} (r|p)rd_r \equiv \sum_{r=1}^{n} (r|p)(2rd_r - p(r + d_r)) \pmod{p^2},$$

which completes the proof of (VI).

The integers c_r ($r = 1, 2, \dots, p - 1$) in (3) may be also obtained from the congruence

$$W_p \equiv c_r \pmod r,\quad 1 \le c_r \le r,$$

or

$$-q_p(r) \equiv c_r \pmod r,\quad 1 < c_r < r,$$

where $q_p(r) = (r^{p-1} - 1)/p$ is the Fermat's quotient. Here, if $r = 1$, we should take $c_r = 1$. The first twenty values of $A_p = \sum_{r=1}^{p-1} (r|p)c_r$ for $p \equiv 1 \pmod 4$ are

$A_5 = -1$, $A_{13} = -3$, $A_{17} = 1$, $A_{29} = -5$, $A_{37} = 13$, $A_{41} = 57$, $A_{53} = -7$, $A_{61} = 49$, $A_{73} = 141$, $A_{89} = -1$, $A_{97} = 311$, $A_{101} = 61$, $A_{109} = 233$, $A_{113} = 425$, $A_{137} = 269$, $A_{149} = 297$, $A_{157} = 461$, $A_{173} = -13$, $A_{181} = 115$, $A_{193} = 365$.

In consequence of (IV), (V) and (VI), we can deduce the equivalent statements to (1) or (2), i.e., the right hand sides of (IV), (V), (VI) are congruent to 0 modulo p. In 1978 Wagstaff [11] showed with a computer that (p, n) is not irregular for all primes $p \equiv 1 \pmod 4$, $p < 125000$. But, the question of whether one of these statements holds or not for primes $p \equiv 1 \pmod 4$, $p > 125000$, is still unsettled (cf. [6]).

In connection with Fermat's last theorem, the question is raised in [1] whether there exist a prime p and a positive integer k such that (p, 2k) and (p, p - 1 - 2k) both are irregular.

REFERENCES

[1] T. Agoh, On Fermat's last theorem and the Bernoulli numbers, J. of Number Theory, 15(1982), 414-422.

[2] N. C. Ankeny, E. Artin and S. Chowla, The class-number of real quadratic fields, Proc. Nat. Acad. Sci. U.S.A., 37(1951), 524-525.

[3] N. C. Ankeny, E. Artin and S. Chowla, The class-number of real quadratic fields, Ann. of Math., 56(1952), 479-493.

[4] N. C. Ankeny and S. Chowla, A further note on the class number of real quadratic fields, Acta Arith., 7(1962), 271-272.

[5] L. Carlitz, Note on the class number of real quadratic fields, Proc. A. M. S., 4(1953), 535-537.

[6] P. Chowla and S. Chowla, A note on Bernoulli numbers, J. of Number Theory, 12(1980), 445-446.

[7] H. S. Vandiver, Symmetric functions formed by systems of elements of a finite algebra and their connection with Fermat's quotient and Bernoulli numbers, Ann. of Math., 18(1917), 105-114.

[8] H. S. Vandiver, On Bernoulli numbers and Fermat's last theorem, Duke Math. J., 3(1937), 569-584.

[9] H. S. Vandiver, On congruences which relate the Fermat and Wilson quotients to the Bernoulli numbers, Proc. Nat. Acad. Sci. U.S.A., 35(1949), 332-337.

[10] H. S. Vandiver, On developments in an arithmetic theory of the Bernoulli and allied numbers, Scripta Math., 25 (1961), 273-303.

[11] S. S. Wagstaff, The irregular primes to 125000, Math. Comp., 32(1978), 583-591.

T.AGOH
Department of Mathematics
Science University of Tokyo
Noda, Chiba 278
JAPAN

Received April 15, 1983

A SHORT PROOF OF THE JACOBIAN CONJECTURE IN CASE OF DEGREE ≤ 2

Susumu Oda and Ken-ichi Yoshida

Presented by P. Ribenboim, F.R.S.C.

Let $X_1,\ldots,X_n$ be indeterminates over a field k and let $f_1,\ldots,f_n$ be polynomials in $X_1,\ldots,X_n$ with coefficients in k. Let A_k^n denote an affine space of dimension n over k. Then we have a morphism $f : A_k^n \longrightarrow A_k^n$ which maps a point $x = (x_1,\ldots,x_n)$ to $(f_1(x),\ldots,f_n(x))$. If f has an inverse morphism then the Jacobian determinant $\left| \frac{\partial f_i}{\partial X_j} \right|$ is a non-zero constant by the chain rule.

The Jacobian conjecture asks if the converse is true. Note that if the characteristic of k is $p \neq 0$ and $f(X) = X + X^p$, then $f'(X) = 1$ but X is not a polynomial in f. Let $A = k[X_1,\ldots,X_n]$ and $R = k[f_1,\ldots,f_n]$. Then the Jacobian conjecture is equivalent to asking about the validity of $A = R$ when the Jacobian determinant $\left| \frac{\partial f_i}{\partial X_j} \right|$ is a non-zero constant of a field k of characteristic zero.

In the paper of H. Bass, E.H. Connell and D. Wright, they showed that it suffices to prove the Jacobian conjecture under the assumption of $\deg f_i \leq 3$ for all $i = 1,\ldots,n$. On the other hand, S. Wang showed that the Jacobian conjecture holds if the degree of each $f_i \leq 2$ and the characteristic of $k \neq 2$.

The purpose of this paper is to give a short proof of

Grant-in-Aid for Scientific Research

Wang's theorem which is stated as follows :

Theorem. Let k be a field of characteristic $\neq 2$ and let $A = k[X_1,\ldots,X_n]$ be a polynomial ring. Let $f_1,\ldots,f_n$ be elements of A and put $R = k[f_1,\ldots,f_n]$. If the Jacobian matrix $(\frac{\partial f_i}{\partial X_j})$ is invertible and the total degree of $f_i \leq 2$ for all i, then we have $A = R$.

Proof. Let $\bar{k}$ be the algebraic closure of k. Since the function $\otimes_k \bar{k}$ is faithfully flat, it suffices to show our assertion in the case $k = \bar{k}$. Considering the differential modules $\Omega_k(A) = AdX_1 \oplus \cdots \oplus AdX_n$ and $\Omega_k(R) \otimes_R A = Adf_1 \oplus \cdots \oplus Adf_n$, the canonical homomorphism $\Omega_k(R) \otimes_R A \longrightarrow \Omega_k(A)$ is an isomorphism because the Jacobian matrix is invertible. Hence we have $\Omega_R(A) = (0)$, that is, A is unramified over R. So the quotient field $K(A)$ is a separable algebraic extension over $K(R)$. Since $\mathrm{trans.deg}_k K(R) = n$, R is a polynomial ring in n indeterminates $f_1,\ldots,f_n$ over k.

Next we show that the canonical morphism $f : \mathrm{Spec}\ A \longrightarrow \mathrm{Spec}\ R$ is injective on closed points of $\mathrm{Spec}\ A$, or, equivalently it is sufficient to prove that the hypersurfaces $V(f_i - a_i)$ $(i = 1,\ldots,n,\ a_i \in k)$ meet at only one point in the affine space A^n_k. Replacing f_i by $f_i - a_i$ for some $a_i \in k$, we may suppose $f_i(0,\ldots,0) = 0$ for all $i = 1,\ldots,n$. Now suppose that there exists $b_1,\ldots,b_n \in k$ such that $b = (b_1,\ldots,b_n) \neq (0,\ldots,0)$ and $f_i(b) = 0$ for all i. Let t be an indeterminate over A and put $f_i^*(t) = f_i(b_1 t,\ldots,b_n t) \in k[t]$. It is clear that $f_i^*(0) =$

$f_i^*(1) = 0$, hence $f_i^*(t) \in t(t-1)k[t]$. By the hypothesis that $\deg f_i \leq 2$ and the characteristic of $k \neq 2$, we have $f_i^*(t) = c_i t(t-1)$ for some $c_i \in k$. Therefore $\frac{df_i^*}{dt}(\frac{1}{2}) = 0$ for $i = 1,\ldots,n$. Since $\frac{df_i^*}{dt}(\frac{1}{2}) = \frac{\partial f_i}{\partial X_1}(e)b_1 + \cdots + \frac{\partial f_i}{\partial x_n}(e)b_n$, where $e = (\frac{b_1}{2},\ldots,\frac{b_n}{2})$, we see that

$$\left(\frac{\partial f_i}{\partial X_j}(e)\right)\begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}.$$

But the matrix $(\frac{\partial f_i}{\partial X_j}(e))$ is invertible, this is a contradiction. Thus the morphism f is birational, since $K(A)$ is a separable algebraic extension over $K(R)$.

From the result written in the text book of Hartshorne ((10.4), Ch.III), A is flat over R, for both R and A are polynomial domains over k and $\Omega_R(A) = (0)$. Therefore the morphism f is birational and flat.

At last, we show that there does not exist a prime ideal P of height one in $\operatorname{Spec} R$ such that $PA = A$. Suppose that, for a prime ideal $P \in \operatorname{Spec} R$ of height one, $PA = A$. Since R is a polynomial domain, R is a UFD, so there exists an element p of R such that $P = pR$. Then we have $pA = A$, that is, p is an invertible element of A. But invertible elements of A are contained in k, a contradiction. Therefore the canonical morphism f is an isomorphism (see Yoshida, Lemma (1,1), (1,2) and (1,3)).

References

H. Bass, E.H. Connell and D. Wright, The Jacobian conjecture: reduction of degree and formal extension of the inverse, Bull. Amer. Math. Soc. (N.S) 7 (1982),no 2, 287-330.

R. Hartshorne, Algebraic geometry, G.T.M. 52 (1977), Springer-Verlag.

S. Wang, A Jacobian criterion for separability, J. Alg. 65 (1980), 453-494.

D. Wright, On the Jacobian conjecture, Illinois J. Math. 25 (1981), 423-440.

K. Yoshida, On flat over-ring of a Krull domain, J. Math. Soc. Japan, 27 (1975), 258-263.

Ujiyamada High School
3-13-1 Uraguchi Ise-city
Mie-prefecture Japan

Department of Mathematics
Faculty of Science
Osaka University
Toyonaka Osaka Japan

Received May 2, 1983

A NEW PROOF OF BURGESS' THEOREM ON CHARACTER SUMS

J.H.H. Chalk, F.R.S.C.

1. If $k = p^{\alpha}$, where $\alpha \geq 2$ and p is prime and χ is a primitive character mod k, D.A. Burgess [1] has proved that the inequality

$$\sum_{x=1}^{k} \left| \sum_{y=N+1}^{N+h} \chi(x+y) \right|^{2r} \ll kh^r + k^{\frac{1}{2}+\epsilon} h^{2r}$$

holds for the case $r = 2$ and has recently informed me that it holds for certain special cases (with $\alpha \leq 6$) for $r = 3$. Here, the Vinogradov symbol " $\ll$ " depends at most on $\epsilon > 0$ and r. From such an inequality one can deduce (by another argument due to Burgess, *loc. cit.*) an estimate, for an incomplete character sum, of the form

$$\left| \sum_{x=N+1}^{N+h} \chi(x) \right| \ll h^{r/(r+1)} k^{(\frac{1}{4r})+\epsilon}.$$

As it seems difficult to make much further progress for $r \geq 3$ along present lines, I have designed an entirely different proof for the case $r = 2$ (which, incidentally, provides a more explicit form to the result). For α *even*, the proof is quite short but even so there still remain considerable difficulties in extending it to the case $r = 3$.

2. THEOREM. Let $k = p^{\alpha}$, where $\alpha \geq 2$ and p is prime, let $h \in \mathbb{N}$, $N \in \mathbb{Z}$ and let χ denote a primitive character mod k. Then

$$(1) \qquad \sum_{x=1}^{k} \left| \sum_{y=N+1}^{N+h} \chi(x+y) \right|^{4} \leq 108\, h^2 k, \quad \text{if } 1 \leq h \leq k^{\frac{1}{4}}.$$

Proof: There is no loss of generality in taking $N = 0$, since x runs through a complete set of residues mod k. Then the sum S

say on the left of (1) may be expressed as

$$(2) \qquad S = S(h, p^{\alpha}) = \sum_{x=1}^{k} \sum_{m_1=1}^{h} \cdots \sum_{m_4=1}^{h} \chi(f(x))\bar{\chi}(g(x))$$

where

$$f(X) = \prod_{i=1,2} (X-m_i) = X^2 - 2a_1X + a_2 ,$$

$$g(X) = \prod_{i=3,4} (X-m_i) = X^2 - 2b_1X + b_2 .$$

Let

$$B = \{\underline{m} = (m_1, \ldots, m_4) : 1 \le m_i \le h\}$$

and put

$$(3) \qquad \sigma(p^{\alpha}) = \sigma(\underline{m}, p^{\alpha}) = \sum_{x=1}^{p^{\alpha}} \chi(f(x))\bar{\chi}(g(x)) .$$

Then, for $\beta \ge \frac{1}{2}\alpha$,

$$(4) \qquad \sigma(p^{\alpha}) = p^{\alpha-\beta} \sum_{\substack{x=1 \\ fg'-f'g \equiv 0 (\mathrm{mod}\ p^{\alpha-\beta}) \\ fg \not\equiv 0 (\mathrm{mod}\ p)}}^{p^{\beta}} \chi(f(x)/g(x))$$

on putting $x = y + p^{\beta}z$ say (cf., [1], Lemma 2). We write

$$n = [\tfrac{1}{2}\alpha] \quad , \quad \nu = \nu(n) = [\tfrac{1}{2}(n+1)]$$

for convenience and choose $\beta = \alpha - n$. Then

$$|\sigma(p^{\alpha})| = p^n \left| \sum_{\substack{x=1 \\ fg'-fg' \equiv 0 (\mathrm{mod}\ p^n) \\ fg \not\equiv 0 (\mathrm{mod}\ p)}}^{p^{\alpha-n}} \chi(f(x)/g(x)) \right|$$

$$(5) \qquad \le p^n \sum_{\substack{x=1 \\ fg'-f'g \equiv 0 (\mathrm{mod}\ p^n) \\ fg \not\equiv 0 (\mathrm{mod}\ p)}}^{p^{\alpha-n}} 1 \le p^{\alpha-n} \sum_{\substack{x=1 \\ fg'-f'g \equiv 0 (\mathrm{mod}\ p^n) \\ fg \not\equiv 0 (\mathrm{mod}\ p)}}^{p^n} 1 .$$

If the sum N_n say, on the right of (5) is empty, there is nothing to prove. Otherwise, there is an integer λ, with $(\lambda,p) = 1$,

$1 \le \lambda < p^n$, and a $t = t(\lambda)$ such that

$$f(t) + \lambda g(t) \equiv 0 (\mathrm{mod}\ p^n)$$

$$f'(t) + \lambda g'(t) \equiv 0 (\mathrm{mod}\ p^n)$$

since $f(t)g(t) \not\equiv 0(p)$. Hence, on writing

$$F_\lambda(X) = f(X) + \lambda g(X),$$

we have

$$F_\lambda(X) \equiv (1+\lambda)(X-t)^2 \bmod p^n, \tag{6}$$

identically in X, since in general

$$F_\lambda(X) = F_\lambda(x_0) + (X-x_0)F_\lambda'(x_0) + \frac{(X-x_0)^2 F_\lambda''(x_0)}{2} + \cdots .$$

We now fix λ and t, once and for all. Then

$$\begin{aligned} f(X)g'(X) - f'(X)g(X) &= F_\lambda(X)g'(X) - F_\lambda'(X)g(X) \\ &\equiv (1+\lambda)(X-t)[(X-t)g'(X) - 2g(X)] \bmod p^n . \end{aligned} \tag{7}$$

The polynomial in X on the right of (7) has degree ≤ 2. If this degree $= 2$ then the discriminant D_t is given by

$$D_t = [2g(t)]^2(1+\lambda)^2$$

and so

$$\mathrm{ord}_p D_t = 2s$$

where

$$s = \mathrm{ord}_p(1+\lambda), \qquad 0 \le s \le n,$$

since $g(t) \not\equiv 0(\mathrm{mod}\ p)$. If it is linear, then $t = b_1$ and it takes the form $2(1+\lambda)\{-g(t)\}(X-t)$ and if constant, $1 + \lambda \equiv 0(\mathrm{mod}\ p^n)$ i.e. $s = n$. In the first case, $D_t \neq 0$ and so, by the Sándor estimate ([2], [3]), we have

$$N_n \le 2p^s, \tag{8}$$

since $g(t) \not\equiv 0(\mathrm{mod}\ p)$. The trivial estimate for the other cases suffices to show that N_n satisfies (8) without the factor 2.

We now estimate the number of sets $\underline{m} \in B$ which satisfy (6), (for fixed λ and t).

By means of the translation $X \mapsto X+t$, we may suppose that $t = 0$ at the expense of locating the zeros $\underline{m}$ of $f(X)$ and $g(X)$ in the translated 'box'

$$B_t = \{\underline{m} : t+1 \le m_i \le t+h\} . \tag{9}$$

Then, by (6) with $t = 0$

$$a_1 + \lambda b_1 \equiv 0 \ , \ a_2 + \lambda b_2 \equiv 0 \mod p^n . \tag{10}$$

Now, fix one of the pairs (m_3 , m_4) ; there being at most h^2 of them. As λ is fixed and $|a_1 - b_1| < 2h$, by (9), there are

$$\le \frac{2h}{p^n} + 1 \le 3 \tag{$(10)_1$}$$

values for $a_1 = m_1 + m_2$, by $(10)_1$ and

$$h \le [p^{\alpha/4}] \le p^{\alpha/4} \le p^{[2\alpha/4]} = p^n . \tag{11}$$

By (10)

$$(m_1-m_2)^2 = 4a_1^2 - 4a_2 \equiv 4\lambda^2 b_1^2 + 4\lambda b_2 \bmod p^n , \tag{12}$$

where $|m_1-m_2| < h$, by (9). Now, in general, the number of solutions X of the congruence

$$X^2 \equiv A \pmod{p^n}$$

in the interval $H+1 \le X < H+K$ cannot exceed $2(Kp^{-\nu}+1)$. Hence there are at most $2(2hp^{-\nu}+1)$ values for $m_1 - m_2$ and so at most $6h^2(2hp^{-\nu}+1)$ sets (m_1 , m_2 , m_3 , m_4). Then, by (2), (3), (4), (5) and (8),

$$S \le 6h^2(2hp^{-\nu}+1)p^{\alpha-n}\cdot 2p^s$$

$$\le \begin{cases} 36h^2\, p^{\alpha-n+s} & , \quad \text{if } h < p^\nu \\ 36h^2\cdot hp^{-\nu}\, p^{\alpha-n+s} & , \quad \text{if } h \ge p^\nu . \end{cases}$$

By inspection, we see that $S \le 36\, h^2 p^\alpha$, (using the bound $h^4 p^{\frac{1}{2}\alpha} < h^2 p^\alpha$), when α is even or when $s < n$ or even when $s = n$ and n is odd. Thus it remains to consider the case

$$\alpha \text{ odd}, \quad n \text{ even} \quad \text{and} \quad s = n .$$

Then

$$\lambda \equiv -l , \quad a_1 \equiv b_1 , \quad a_2 \equiv b_2 \mod p^n \tag{13}$$

and (12) reduces to

$$(m_1 - m_2)^2 \equiv (b_1^2 - 4b_2) = (m_3 - m_4)^2 \mod p^n .$$

Since $|m_3 - m_4| < h$, by (9), there are now at most $h\cdot 2(2hp^{-\nu}+1)$ pairs (m_3 , m_4). But, as

$$|a_1 - b_1| = |(m_1 + m_2) - (m_3 + m_4)| < 2h \le 2p^n \tag{14}$$

by (11), there are, for each such pair (m_3 , m_4), at most $3\cdot 2(2hp^{-\nu}+1)$ pairs $(m_1 + m_2 , m_1 - m_2)$, by $(13)_2$ and (14). Thus, there are not more than $12h(2hp^{-\nu}+1)^2$ sets (m_1 , m_2 , m_3 , m_4), and so

$$S \le 12h(2hp^{-\nu}+1)^2 p^{\alpha-n}\cdot p^n$$

$$\le \begin{cases} 108\, hp^\alpha & , \quad \text{if } h \le p^\nu \\ 108\, h^3 p^{\alpha-n+n-2\nu} & , \quad \text{if } h > p^\nu \end{cases}$$

where, for $h > p^\nu$

$$h^3 p^{\alpha-n+n-2\nu} < h^4 p^{\alpha-3\nu} < h^4 p^{\alpha/2},$$

since $n = [\frac{1}{2}\alpha] \geq 1$.

REFERENCES

1. D.A. Burgess, "On Character Sums and L-series", Proc. London Math. Soc., (3) 12 (1962), 193-206.

2. J.H.H. Chalk and R.A. Smith, "Sándor's Theorem on Polynomial Congruences and Hensel's Lemma", C.R. Math. Rep. Acad. Sci. Canada, IV (1982), No. 1, 49-54.

3. G. Sándor, "Uber die Anzahl der Lösungen einer Kongruenz", Acta Math., 87 (1952), 13-17.

Department of Mathematics
University of Toronto
Toronto, Canada
M5S 1A1.

Received May 21, 1983

SMOOTHNESS IN DISJOINT GROUPS OF REAL FUNCTIONS UNDER COMPOSITION

G. Blanton
Presented by J. Aczél, F.R.S.C.

Let I be a non-empty open interval in $\mathbb{R}$ and let G be a group (under composition) of homeomorphisms on I. Suppose further that G is a disjoint collection (identifying homeomorphisms on I with their graphs). The union, $\cup G$, of the collection G (the set of all points on graphs of elements of G) is a subset of $I\times I$. The group G is dense if $\cup G$ is dense in $I\times I$, and G is complete if $\cup G = I\times I$.

Given a bijection $\phi: I \to \mathbb{R}$ of I onto $\mathbb{R}$, for each $\alpha \in \mathbb{R}$ we define $\phi_\alpha: I \to I$ by $\phi_\alpha(x) = \phi^{-1}(\alpha+\phi(x))$ for each $x \in I$. We call $F[\phi] = \{\phi_\alpha: \alpha \in \mathbb{R}\}$ the iteration group generated by ϕ.

It is easy to see that under these circumstances $F[\phi]$ is a complete disjoint group of homeomorphisms on I. The converse is also true [1]: If G is a complete disjoint group of homeomorphisms on I, then $G = F[\phi]$ is an iteration group for some homeomorphism $\phi: I \to \mathbb{R}$.

We have found that the logarithm of iteration, ϕ, necessarily has the same order of differentiability as do the functions in G. This is related to the so called difference property investigated by N.G. de Bruijn in [3]. Also every dense disjoint group of homeomorphisms on I has a unique extension to a complete disjoint group of homeomorphisms on I, the smoothness may differ however in a group and its completion. For instance a dense group G may consist entirely of C^∞ functions, but its

completion may contain functions which are not even once continuously differentiable.

The main result concerning complete groups is the following.

Theorem 1. For $n \geq 0$, G is a complete disjoint group of C^n bijections on I iff $G = F[\phi]$ for some C^n diffeomorphism ϕ mapping I onto $\mathbb{R}$.

The case $n = 0$, as mentioned earlier, is essentially due to Aczél. This author proved, by a direct argument, the case $n = 1$. Baker [2] extended the result to all $n \geq 0$ by using the following result of [3] concerning the difference property. If all the differences of a function ψ, $(x \mapsto \psi(x+\alpha) - \psi(x), \alpha \in \mathbb{R})$ are C^n then $\psi = A+\phi$ where A is additive and ϕ is C^n. We can reformulate Theorem 1 as an analogue to the de Bruijn result:

Theorem 2. For $n \geq 0$, if $\psi: I \to \mathbb{R}$ is a bijection such that, for all $\alpha \in \mathbb{R}$, the mapping $x \mapsto \psi^{-1}(\alpha+\psi(x))$ is n times continuously differentiable, then there is an increasing C^n bijection $\phi: I \to \mathbb{R}$ and an additive bijection $A: \mathbb{R} \to \mathbb{R}$ such that $\psi(x) = A(\phi(x))$ for all $x \in I$.

We now turn to the problem of completing dense groups.

Proposition 3. Let G be a disjoint group of homeomorphisms on I.

(a) If G is dense, then $\{f(\theta): f \in G\}$ is dense in I for each $\theta \in I$.

(b) If $\{f(\theta): f \in G\}$ is dense in I for some $\theta \in I$, then G is dense.

The basic result on completions is the following.

Theorem 4. If G is a dense disjoint group of homeomorphisms on I, then there is a homeomorphism $\phi: I \to \mathbb{R}$ such that G is a subgroup of $F[\phi]$. Further, $F[\phi]$ is the unique complete group of homeomorphisms which contains G.

Theorem 4 does not generalize to higher orders of smoothness:

Theorem 5. There is a (finitely generated) dense disjoint group of C^∞ bijections on I which is not a subgroup of any complete disjoint group of C^1 bijections on I.

It is easier to show that such an infinitely generated group exists (isomorphic to a subgroup of the rationals). To do this, pick $\theta \in I$, (assume WLOG that I is finite), and start with any C^∞ function g_0. Then construct compositional roots $g_1^{n_1} = g_0, g_2^{n_2} = g_1, \ldots$ successively so that each g_i is C^∞ and so that $g_i'(\theta) = 2$, and $|g_i(x)-x| < \frac{1}{2^i}$ for $x \in I$. The last condition insures that G, the group generated by $g_0, g_1, \ldots$ will be dense, while $g_i'(\theta) = 2$ for $i = 1,2,\ldots$ insures that G will not have a C^1 completion.

To show that such a group can be finitely generated, the following result is useful.

Theorem 6. Let $n \geq 1$ be an integer. Let $(f_i)_{i=1}^\infty$ be a sequence of C^n functions mapping I into I. Let $h_i = f_i \circ \ldots \circ f_2 \circ f_1$ for each $i \geq 1$. Suppose that $h: I \to I$ is a continuous function such that $h_i \to h$ uniformly on compact

subsets of I and

$$\sum_{i=1}^{\infty} \sup_{x \in J} |f_i^{(k)}(x) - i^{(k)}(x)| < \infty$$

for every compact $J \subseteq I$ and $1 \leq k \leq n$. Then h is C^n and $h_i^{(k)} \to h^{(k)}$ uniformly on compact subsets of I $(k=1,2,\ldots,n)$.

Now the proof of this stronger version of Theorem 5 is similar in spirit to the sketch given above. Again a sequence of compositional powers is constructed for a given C^∞ function f_0: $f_0 = g_0^2$, $g_0 = f_1^{n_1}$, $f_1 = g_1^2$, ... where we insist again that $g_1'(\theta) = 2$, but also that $(n_i)_{i=1}^{\infty}$ be a strictly increasing sequence of powers of two. Also the f_i are chosen in accordance with Theorem 6, so that $f_i \circ \ldots \circ f_2 \circ f_1 \to h$ as $i \to \infty$ for some C^∞ function h. Then the group H generated by h and f will be a dense group of C^∞ functions whose completion has some functions which are not C^1.

REFERENCES

[1] Aczél, J., Funtionskomposition, Iterationsgruppen und Gewebe. Arch. Math. (Basel) 17 (1966), 469-475.

[2] Blanton, G. and Baker, John A., Iteration groups generated by C^n functions. To appear in Archivum Mathematicum.

[3] de Bruijn, N.G., Functions whose differences belong to a given class. Nieuw Arch. Wisk. 23 (1951), 194-218.

Pure Mathematics Department
University of Waterloo
Waterloo, Ontario
N2L 3G1
Canada

Received June 6, 1983

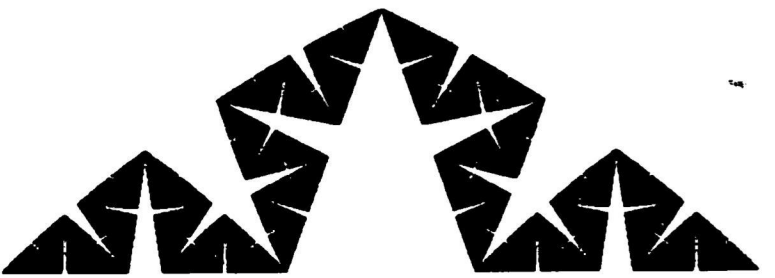
C.R. Math. Rep. Acad. Sci. Canada - Vol. V, No.4, August 1983 aout

COURBES DE VON KOCH ET COURBES D'OSGOOD

SERGE DUBUC

Presented by H. Schwerdtfeger, F.R.S.C.

Une courbe d'Osgood est un arc simple continu du plan dont l'aire est positive. Une telle courbe est paradoxale, mais Osgood [3] a bien montré que de telles courbes existent. Mandelbrot [2], pp.148-149, et moi-même [1], p.106, avons introduit très simplement des courbes d'Osgood en modifiant une construction de von Koch [4]. Par cette note, je justifie les résultats annoncés par l'un et l'autre et je donne sur le champ une réalisation graphique à haute définition d'une de ces courbes d'Osgood.



La construction élémentaire de von Koch consiste à remplacer un segment P_0,P_1 par 4 segments consécutifs Q_0,Q_1,Q_2,Q_3,Q_4 déterminés par un paramètre c ($1/4 < c < 1/2$). Q_0 est confondu avec P_0, Q_4 est confondu avec P_1; Q_1 et Q_3 sont portés par le segment P_0,P_1 en divisant ce segment en trois parties selon les rapports c, 1-2c et c: $Q_1 = (1-c)P_0 + cP_1$, $Q_3 = cP_0 + (1-c)P_1$. Le point Q_2 est tel que chacun des triangles Q_0,Q_1,Q_2 et Q_2,Q_3,Q_4 est isocèle. Il y a deux candidats possibles pour Q_2. On convient de choisir le point qui donne un triangle orienté positivement

pour Q_0,Q_1,Q_2. Par construction, les quatre segments de la ligne Q_0,Q_1,Q_2,Q_3,Q_4 sont de même longueur, égale à $c.||P_1-P_0||$.

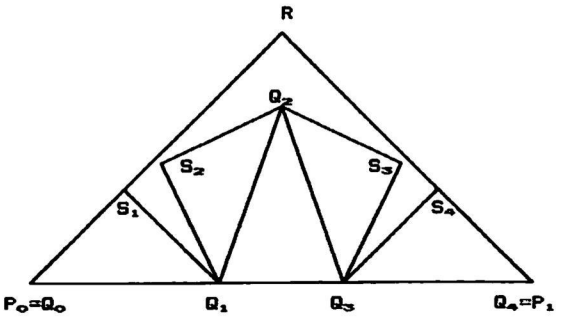
Pour créer une courbe simple sans tangente en chacun de ses points, von Koch a suggéré de considérer une suite infinie de lignes polygonales $L_0,L_1,L_2,\ldots$ où L_0 est un segment P_0,P_1, L_1 est la ligne Q_0,Q_1,Q_2,Q_3,Q_4, L_2 est la ligne polygonale de seize segments obtenue en remplacant chacun des segments de L_1 selon la construction élémentaire décrite ci-dessus. Par récurrence, L_n engendre L_{n+1}. Cependant la construction de la ligne polygonale de la n ème génération dépend du paramètre c que nous ferons varier d'une génération à l'autre, c'est en cela que nous nous écartons de von Koch. Soit c_n le paramètre utilisé à la n ème génération, nous maintenons la restriction que $1/4 < c_n < 1/2$. Nous verrons que les sommets des lignes polygonales $L_0,L_1,L_2,\ldots$ font partie d'un arc simple continu en y étant denses et que l'aire plane de cet arc est égale à $||P_1-P_0||^2/4$ fois le carré du produit infini des nombres $2c_n$.

Comparons les sommets des lignes polygonales de deux générations successives. Si S est un sommet de la n ème génération, S sera un sommet pour les générations suivantes. Si l'on accorde à S son rang naturel dans la n ème génération, ce rang j est un entier compris entre 0 et 4^n tandis que son rang naturel dans la génération suivante sera 4j. Cette remarque permet de définir une fonction V(t) à valeurs dans le plan pour les fractions t de l'intervalle-unité qui sont de la forme $t = j/4^n$: si t est cette fraction, si S est le sommet de rang j de la ligne polygonale L_n, on pose $V(t) = S$.

Théorème: La fonction V est uniformément continue sur son domaine de définition. Plus précisément, si $|t_2-t_1| < 1/4^n$, alors la distance de $V(t_2)$ à $V(t_1)$ ne dépasse pas $2||P_1-P_0||/2^n$.

L'arc généralisé de von Koch est le prolongement par continuité de la fonction V à tout l'intervalle-unité. Avant d'établir ce théorème, nous revenons à la construction élémentaire de von Koch en prêtant attention à la ligne polygonale L_1 issue de L_0. Il est fort commode d'associer à L_0 et à L_1 divers triangles rectangles isocèles. Soit R le point du plan qui assure que le triangle R,P_0,P_1 est un triangle rectangle isocèle orienté positivement, dont l'angle droit est situé en R, on désignera par T ce triangle de la première génération. De même, soient U_1,U_2,U_3,U_4 les quatre triangles rectangles isocèles dont les hypothénuses sont respectivement les segments consécutifs de la ligne polygonale Q_0,Q_1,Q_2,Q_3,Q_4. Il s'agira des triangles de la seconde génération.

Lemme: Les triangles de la seconde génération U_1, U_2, U_3 et U_4 sont disjoints deux à deux sauf peut-être pour leurs sommets et sont tous contenus dans le triangle T de la première génération.



Démonstration: Le point Q_2 est situé sur le segment $(P_0+P_1)/2,R$, car $Q_2 = (1-d)(P_0+P_1)/2 + dR$ ou d est la racine carrée de 4c-1. On voit que le point Q_2 est dans le triangle T. Soient S_1,S_2,S_3 et S_4 les sommets où les triangles U_1,U_2,U_3 et U_4 sont droits, S_1 et S_4 sont portés par les côtés du triangle T. S_2 est à l'intérieur du triangle T, car la distance de Q_1 à S_2 est égale à la distance de Q_1 au segment R,P_0; S_3 est aussi à l'intérieur du même triangle. Les quatre triangles rectangles sont donc tous contenus dans le triangle T. D'autre part, on peut remarquer que ces quatre triangles rectangles sont disjoints deux à deux si l'on exclut les trois points Q_1,Q_2,Q_3: ceci vient du fait que l'angle Q_0,Q_1,Q_2 est obtus et que les deux angles Q_0,Q_1,S_1 et S_2,Q_1,Q_2 sont de 45 degrés. Q.E.D.

Revenons à la démonstration du théorème. Si t_1 et t_2 sont deux fractions distinctes dont leur dénominateur est une puissance de 4 et si $|t_2-t_1| < 1/4^n$, quitte à échanger t_1 et t_2 entre eux, on peut supposer que: $t_1 < t_2 < t_1 + 1/4^n$. Soit j la partie entière de $t_1.4^n$, on pose $t=j/4^n$. Deux cas peuvent se présenter. a) Si t minore t_1, alors les points $V(t_1)$ et $V(t_2)$ sont des sommets éventuels dans la construction de von Koch appliquée à partir du segment initial $R_0,R_1 = V(t),V(t+1/4^n)$. Le lemme affirme que $V(t_1)$ et $V(t_2)$ appartiennent au triangle rectangle isocèle T dont l'hypothénuse est R_0,R_1. La distance de $V(t_1)$ à $V(t_2)$ ne peut pas dépasser le diamètre de T . Or le diamètre de T ne dépasse pas $1/2^n$ fois la distance de P_0 a P_1. b) Si $t_1 < t$, le raisonnement donné en a) permet de majorer la distance de $V(t_1)$ à $V(t)$ et de $V(t_2)$ à $V(t)$: en effet $V(t_1)$ est un sommet éventuel dans la construction de von Koch appliquée sur le segment initial

$V(t-1/4^n)$, $V(t)$ tandis que $V(t_2)$ est un sommet éventuel relativement au segment initial $V(t),V(t+1/4^n)$. Selon l'inégalité triangulaire, la distance de $V(t_1)$ à $V(t_2)$ est majorée par la somme des distances de $V(t)$ à $V(t_1)$ et à $V(t_2)$. D'où la majoration de $||V(t_2)-V(t_1)||$ par le nombre $2||P_1-P_0||/2^n$.

Vérifions maintenant que l'arc de von Koch est simple. Si t_1 et t_2 sont deux nombres distincts de $[0,1]$, $t_1<t_2$, on peut choisir deux entiers j et n tels que $t_1 < j/4^n$ et $(j+1)/4^n < t_2$. Or les deux triangles rectangles isocèles dont les hypothénuses sont les segments de rang j et $j+2$ de la ligne polygonale L_n sont disjoints et contiennent respectivement $V(t_1)$ et $V(t_2)$. Ces deux points sont donc distincts. Déterminons enfin l'aire de la courbe généralisée de von Koch.

Théorème: L'aire de la courbe est $||P_1-P_0||^2$ / 4 fois le carré du produit infini des nombres $2c_n$.

Démonstration. Soit W_n la réunion des triangles rectangles isocèles du lemme, les W_n forment des ensembles emboîtés dont l'intersection est l'adhérence de la courbe de von Koch. En effet chacun des triangles dont est formé W_n rencontre cette courbe et est de diamètre qui tend vers zéro à mesure que n augmente. Comme la courbe de von Koch est compacte, l'intersection des W_n coincide donc avec la courbe. L'aire de celle-ci est donc la limite de l'aire de W_n. Il y a 4^n triangles dans W_n et l'aire de chacun des triangles de la n ème génération est $||P_1-P_0||^2$ / 4 fois le carré du produit de 1 à n des c_k. Q.E.D.

La figure du début du texte est la courbe généralisée de von Koch dont les paramètres c_n sont successivement 3/8, 7/16, ..., $(1 - 1/2^{n+1})/2$, ... Elle a été réalisée avec un microprocesseur APPLE III de 128 K et une imprimante EPSON MX-80F/T muni de GRAFTRAX ^{PLUS}. Il s'agit d'un graphique à haute définition, 120 points au pouce à l'horizontale et 216 points au pouce à la verticale. Peut-on croire qu'il s'agit de l'image d'une courbe simple? Pourtant ce que l'oeil ne voit pas, l'esprit peut l'appréhender.

Bibliographie

[1] S. Dubuc, Une foire de courbes sans tangentes. Actualités mathématiques. Actes du VI ème Congrès du GMEL. Gauthier-Villars. Paris, 1982.

[2] B.B. Mandelbrot, The Fractal Geometry of Nature. W.H.Freeman. San Francisco, 1982.

[3] W.F. Osgood, A Jordan curve of positive area. Trans. Amer. Soc. 4 (1903), 107-112.

[4] H. von Koch, Sur une courbe continue sans tangente obtenue par une construction géometrique élémentaire. Arkiv for Matematik, Astronomie och Fysik 1 (1904), 681-704.

Département de mathématiques et de statistique
Université de Montréal
C.P. 6128
Montréal, Qué. Canada H3C 3J7

Received June 8, 1983

APPROXIMATION OF DIFFERENTIABLE FUNCTIONS ON A HILBERT SPACE

M. P. Heble

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

§ 1. Introduction. The objective of this paper is to prove the following theorem.

Thm. 1. Let Ω be an open set in a separable finite- or infinite-dimensional real Hilbert space $\mathcal{H}$, F a real Banach space, and $f:\Omega \to F$ a C^k-smooth mapping in the Fréchet sense. We shall denote by $D^j\varphi$ the j^{th} successive Fréchet derivative of φ (if it exists). Further let $\epsilon(.)$ be a positive continuous function on Ω. Then there exists mapping $g:\Omega \to F$ which is C^∞-smooth in the Fréchet sense, and satisfies: $\forall$ integers j s $0 \le j \le k$, $\| D^j g(x) - D^j f(x) \| < \epsilon(x)$ $\forall\, x \in \Omega$. In other words, C^∞-smooth mappings from Ω to F form a dense subclass in the class of C^k-smooth mappings from Ω to F with the C^k-fine topology. k here is a given integer ≥ 0. A similar result is true for ℓ^p-spaces ($p \ge 1$ an integer) after re-equipment with an equivalent C^∞-smooth norm away from the origin (cf. [1]

Such results are important in "global analysis" (cf. [2] -[9]). In [6] Moulis proved that a C^{2k-1} mapping $\Omega \to F$ can be approximated in C^k_{2k-1} by a C^∞-mapping. Our present result in this paper is new, as far as I am aware, and improves the result of [6] just mentioned, but depends partly on some of the techniques of [6]. I am indebted to S. Kakutani and K. Sundaresan for valuable discussions and to the referee for suggesting improvements.

In [6] the local C^∞- approximation in C^k_{2k-1} was very complicated, and was shown as a composite $\mathcal{H} \to \mathcal{H}^\infty \to F, \mathcal{H}^\infty$ being a subspace of $\mathcal{H}$ (not closed). We have been able to replace this cumbersome method by a rather simple one; this has resulted in improving the local approximation itself. Further, the technique of putting together the various local C^∞-approximations, although following [6], has been considerably streamlined, so that calculations have been simplified. (See [4] for a partial improvement of [6] .)

Partitions of unity were used effectively in [3] (on C^∞-approximation in C^0). It may bepossible in the near future to use partitions of unity (or something related) for the problem of our paper and/or avoid dependence on [6] ; however, our paper gives detailed information about the C^k-approximating C^∞ function (Lemmas 3 - 6); this can be useful for other questions e.g. whether the approximation can be more special, etc.

In § 2 we establish (Thm.2) at each point x of $\mathcal{M}$ a C^∞-function $\tilde{f} = \tilde{f}_x$ such that $\tilde{f}$ and its k successive derivatives approximate f and its respective k successive derivatives, locally uniformly. In § 3 we put together these various local approximations to prove Thm. 1. More details will be published elsewhere.

§ 2. Local C^∞-approximation. The following theorem is true even if $\mathcal{M}$ is non-separable.

Thm.2. Let $x \in \mathcal{M}$, and $\varepsilon > 0$. Then $\exists\ \tilde{f} = \tilde{f}_x : \mathcal{M} \to P \ni \tilde{f} \in C^\infty$ on $\mathcal{M}$ and in a suitable neighbourhood $U = U(x, \varepsilon, f)$ of x, $\tilde{f}$ satisfies: $\forall$ integers $j \ni 0 \le j \le k, \| D^j\tilde{f}(y) - D^j f(y)\| < \varepsilon\ \forall y \in U$.

Proof of Thm. 2. Define $\tilde{f} = \tilde{f}_x$ by: $\tilde{f}(y) = f(x) + Df(x).(y-x) + \frac{D^2 f(x)}{2!}.(y-x)^{(2)} + \ldots + \frac{D^k f(x)}{k!}.(y-x)^{(k)}$. Then clearly $\tilde{f} \in C^\infty$ on $\mathcal{M}$, and $\exists\ \delta = \delta(x, \varepsilon, f) > 0$ $\ni \|y-x\| < \delta \Rightarrow \forall$ integers $j \ni 0 \le j \le k, \| D^j\tilde{f}(y) - D^j f(y)\| < \varepsilon$. So we let $U = [y \mid \|y-x\| < \delta]$. (Here " $(w)^{(j)}$ " means the j-tuple "$(w,\ldots,w)$" , $w \in \mathcal{M}$.)

§ 3. Proof of Thm.1. Let $a_1, a_2, \ldots$ be the points of a countable dense set X in $\mathcal{M}$. The proof of the next Lemma follows by Thm.2 in § 2, and by a repetition of the arguments of [6] pp. 301-302.

Lemma 1. (i) For each of the points $a_1, a_2, \ldots$ of the countable dense set X, $\exists$ sphere B_n' with centre a_n and radius $\varrho_n' > 0$ $\ni$ on B_n' the following hold:

(a) $$\sup_{y,y' \in B_n'} |\varepsilon(y) - \varepsilon(y')| < \inf_{z \in B_n'} \frac{\varepsilon(z)}{2} ;$$

(b) $\exists$ $\tilde{f}_n \in C^\infty$ on $\mathcal{S}_\alpha \to P$ $\ni$ for each integer j with $0 \le j \le k$,

$$\sup_{y \in B_n'} \|D^j \tilde{f}_n(y) - D^j f(y)\| < \frac{\varepsilon_n}{2^{n+3}} \text{ with } \varepsilon_n = \varepsilon(a_n).$$

(ii) For any $z \in \mathcal{S}-X$ $\exists$ sphere $B_z' \subset \mathcal{S}$ with centre z and radius $\varrho_z' > 0$ with the following property:

(a') $$\sup_{y,y' \in B_n'} |\varepsilon(y) - \varepsilon(y')| < \inf_{y \in B_z'} \frac{\varepsilon(y)}{2} .$$

(iii) The two systems of spheres $\mathcal{B}_1 = \{B_n'\}_{n=1}^{\infty}$, the B_n' satisfying (i), and $\mathcal{B}_2 = \{B_z'\}_{z \in \mathcal{S}-X}$, the B_z' satisfying (ii), can be further chosen to satisfy the following: if B_λ' belongs to either $\mathcal{B}_1$ or $\mathcal{B}_2$, and B_μ' likewise belongs to either $\mathcal{B}_1$ or $\mathcal{B}_2$, and if $B_\lambda' \cap B_\mu' \neq \phi$, then

(c) $$\frac{1}{4} < \frac{\varrho_\lambda'}{\varrho_\mu'} < 4.$$

From now on let $\mathcal{B}_1 = \{B_n'\}_{n=1}^{\infty}$ and $\mathcal{B} = \{B_z'\}_{z \in \mathcal{S}-X}$ be two systems of spheres in $\mathcal{S}$ satisfying the properties asserted in Lemma 1. We now set $\varrho_n = \frac{1}{2}\varrho_n'$, $n = 1,2,\ldots$ and let B_n be the open sphere concentric with B_n' and radius ϱ_n. Let $E = \bigcup_{n=1}^{\infty} B_n$.

The next Lemma is required to prove Lemmas 5 and 6.

Lemma.2. If B_p', $B_n' \in \mathcal{B}_1$ and $B_p' \cap B_n' \neq \phi$, then $\varepsilon_p < 2^2 \varepsilon_n$.

Henceforth we shall denote by $\varphi(.)$ a function on $\mathbb{R}^1 \to \mathbb{R}^1$ with the following properties: $\varphi \in C^\infty$ on $\mathbb{R}^1$, $\varphi(t) = 1$ for $|t| \leq \frac{1}{2}$, $\varphi(t) = 0$ for $|t| \geq 1$, $\varphi(t) \nearrow$ on $\langle -1, -\frac{1}{2} \rangle$, and $\varphi(t) \searrow$ on $\langle \frac{1}{2}, 1 \rangle$. Next, for each $n = 1, 2, \ldots$ we define φ_n on $\mathcal{U}$ by: $\varphi_n(z) = \varphi\left(\frac{1}{2\delta_n} \|z - a_n\|\right)$. Then $\varphi_n \in C^\infty$ on $\mathcal{U}$, $\varphi_n = 1$ on B_n, $\varphi_n = 0$ outside B_n'. By Lemma 1(i)(b), $\exists\ \tilde{f}_n \in C^\infty$ on $\mathcal{U} \ni$ for $0 \leq j \leq k$, $\sup_{z \in B_n'} \|D^j \tilde{f}_n(z) - D^j f(z)\| < \frac{\varepsilon_n}{2^{n+1}}$. Next define for each $n = 1, 2, \ldots$, $g_n : \mathcal{U} \longrightarrow F$ by:

$$g_n = f + \varphi_1(\tilde{f}_1 - f) + \varphi_2(1 - \varphi_1)(\tilde{f}_2 - f) + \ldots + \varphi_n(1 - \varphi_{n-1}) \ldots (1 - \varphi_1)(\tilde{f}_n - f).$$

This sequence has the properties listed in Lemmas 3-6 below.

Lemma 3. If $z \in B_p$, then for $n \geq p$, $g_n(z) = g_p(z)$.

The proofs of the next Lemmas follow the lines of the corresponding arguments in [6].

Lemma 4. On each B_n, g_n is C^∞.

Lemma 5. $\exists$ constant λ_0 independent of $n \ni \sup_{z \in B_n} \|g_n(z) - f(z)\| < \lambda_0 \varepsilon_n$.

Lemma 6. $\exists$ constants $\lambda_1, \ldots, \lambda_k$ independent of $n \ni$ for each j with $1 \leq j \leq k$:

$$\sup_{z \in B_n} \|D^j g_n(z) - D^j f(z)\| < \lambda_j \varepsilon_n.$$

Next for each $z \in E$, set $n_z = \inf\{n : z \in B_n\}$. Then n_z is constant on a neighbourhood $V_z \subset B_{n_z}$.

Finally we show that $E = \mathcal{U}$. Let $x \in \mathcal{U}$, and $\rho'_x > 0$ be the radius of the sphere B'_x associated with x by Lemma 1. Since X is dense in $\mathcal{U}$, $\exists\ a_N \in X \ni \|x - a_N\| < \frac{\rho'_x}{8}$. But by Lemma 1(iii), $\frac{\rho'_x}{4} < \rho'_N$, and hence $\|x - a_N\| < \frac{\rho'_N}{2}$, and therefore $x \in B_N$. Hence $E = \mathcal{U}$.

This completes the proof of Thm.1.

REFERENCES

1. Bonic,R. and Frampton,J.: Smooth functions on Banach manifolds. J. Math. Mech. 15 (1966), 877-898.
2. Eells,J.: A setting for global analysis. B.A.M.S. 1966.
3. Eells,J. and McAlpin,J.: An approximate Morse-Sard Theorem. J.Math. Mech. 17,1967;1055-1064.
4. Heble,M. P. : Lie theory and application to entropy and approximation. Proc. 1977 Canad. Math.Congress Annual Seminar on " Lie theories and their application ". pp. 439-470.
5. Lang,S.: Differential manifolds. Addison-Wesley. Rev. ed. 1972.
6. Moulis-Desolneux,N.: Approximation de fonctions differentiables sur certains espaces de Banach. Grenoble. Ann. Inst. Fourier. 21,4 (1971),293-345.
7. Palais,R.S.: Foundations of global analysis. W.A.Benjamin,Inc.
8. Sundaresan,K.: Geometry and non-linear analysis in Banach spaces. Pacific J. of Math. Vol. 162, no.1,1982.
9. Wells,J.: Differentiable functions in c_0. B.A.M.S. 75 (1969).

Department of Mathematics
University of Toronto
Toronto, Canada M5S 1A1.

Received June 21, 1983

MAILING ADDRESSES

1. T. Agoh
   Dept. of Mathematics
   Science University of Tokyo
   Noda, Chiba 278, Japan

2. G. Blanton
   Dept. of Pure Mathematics
   University of Waterloo
   Waterloo, Ontario, Canada N2L 3G1

3. J.H.H. Chalk
   Dept. of Mathematics
   University of Toronto
   Toronto, Ontario, Canada M5S 1A1

4. S. Dubuc
   Dépt. de mathématiques et de statistique
   Université de Montréal, C.P. 6128
   Montréal, Québec, Canada H3C 3J7

5. M.P. Heble
   Dept. of Mathematics
   University of Toronto
   Toronto, Ontario, Canada M5S 1A1

6. S. Oda
   Ujiyamada High School
   3-13-1 Uraguchi Ise-city
   Mie-prefecture, Japan

7. Ken-ichi Yoshida
   Dept. of Mathematics
   Faculty of Science
   Osaka University
   Toyonaka, Osaka, Japan