PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 95, Number 2, October 1985

BIPOWERS IN NUMBER FIELDS

D. K. HARRISON

ABSTRACT. The set of all solutions to the Fermat equation is given a structure. This structure is then characterized up to isomorphism in terms of certain subsets of the integers modulo a prime.

The purpose of this note is to add to the vast literature on Fermat's last theorem the structure (cf. [**1**]) which the set of solutions to that equation has. No claim is made that this structure will help in determining whether nontrivial solutions exist, but finding extra natural structure on an unknown set is a time honored approach in general, which does not seem to have been overly tried for this particular theorem.

Our aim is to axiomatize the rational numbers in such a way that the subset of Fermat solutions satisfies most of the axioms. Of necessity, the axioms will be unusual. To ease the presentation, we give Theorem 1 about "contexts" first, then indicate the proof, and only after this give the definition of what a context actually is. This definition involves some 22 axioms, so the reader will probably want to refer to each axiom only when it is used. The key axiom is (6) which hypothesises an S_3-action. Then with Theorem 2 we show that nothing is lost by our point of view; in other words, the concept of a full context is the same as the concept of a division ring. We omit the obvious extra axioms needed to make a division ring isomorphic to the rational numbers (infinite but no proper full subcontext).

For p an odd positive integer and D a division ring, we say $\alpha \in D$ is a *nontrivial p-bipower* if $\alpha \neq 0,\ \alpha \neq 1,$

$$\alpha = x^p, \quad 1 - \alpha = y^p, \quad x \cdot y = y \cdot x$$

for $x, y \in D$.

THEOREM 1. *Let p be an odd positive integer and D be a division ring. Let $C_p(D)$, or just C, be the set of all nontrivial p-bipowers from D. If $\alpha \in C$, then $t(\alpha) = 1 - \alpha$ is in C, and $s(\alpha) = \alpha^{-1}$ is in C. Let*

$$\Delta = \{(\alpha, \beta, \gamma) | \alpha, \beta, \gamma \in C, \alpha \cdot \beta \cdot \gamma = 1\},$$
$$\Sigma = \{(\alpha, \beta, \gamma) | \alpha, \beta, \gamma \in C, \alpha \cdot \beta \cdot \gamma = 1\}.$$

If either $p = 1$ or D is a field, then a context results. If $p = 1$, it is full. If D is a field, it is abelian.

PROOF. If $\alpha \neq 0,\ \alpha \neq 1,\ \alpha = x^p,\ 1 - \alpha = y^p,\ x \cdot y = y \cdot x$, then one checks $\alpha^{-1} = (x^{-1})^p,\ 1 - \alpha^{-1} = (-y \cdot x^{-1})^p$ and $x^{-1} \cdot (-y \cdot x^{-1}) = (-y \cdot x^{-1}) \cdot x^{-1}$. The rest of the proof consists of a sequence of verifications, each of which is easily made.

Received by the editors September 29, 1983 and, in revised form, October 29, 1984.
1980 *Mathematics Subject Classification.* Primary 10A99; Secondary 10B15, 12C30.

0002-9939/85 $1.00 + $.25 per page

We now define a context to be a tuple $(C, \Delta, \Sigma, s, t)$ where C is a set, Δ and Σ are subsets of C^3, and s and t are maps from C to C, such that

(1) $(\alpha,\beta,\gamma) \in \Delta$ imply (β,γ,α), $(s(\gamma), s(\beta), s(\alpha)) \in \Delta$;
(2) $\alpha, \beta \in C$ implies there exists at most one γ with $(\alpha,\beta,\gamma) \in \Delta$;
(3) (α,β,γ), $(\delta,\lambda,\gamma) \in \Delta$, $(\alpha,\beta,\omega) \in \Sigma$ imply $(\delta,\lambda,\omega) \in \Sigma$;
(4) (α,β,γ), $(s(\gamma),\delta,\lambda)$, $(\beta,\delta,\omega) \in \Delta$ imply $(\alpha, s(\omega), \lambda) \in \Delta$;
(5) $\Delta = \Sigma$ or $\Delta \cap \Sigma = \emptyset$;
(6) $\alpha \in C$ implies $s(s(\alpha)) = \alpha$, $t(t(\alpha)) = \alpha, t(s(t(\alpha))) = s(t(s(\alpha)))$;
(7) $(\alpha, s(\gamma), \gamma)$, $(\beta, s(\delta), \delta) \in \Sigma$ imply $\alpha = \beta$;
(8) $\alpha \in C$ implies $(\alpha, t(s(\alpha)), s(t(\alpha))) \in \Sigma$;
(9) $(\alpha,\beta,\gamma), (s(t(s(\alpha))), t(\beta), \delta) \in \Delta$ imply $(t(\alpha), t(s(\delta)), s(t(s(\gamma)))) \in \Delta$;
(10) $(\alpha,\beta,\gamma) \in \Delta$ implies $s(\alpha) \neq \beta$;
(11) $(\alpha,\beta,\gamma) \in \Delta$ implies there exists δ with $(s(t(s(\alpha))), t(\beta), \delta) \in \Delta$;
(12) (α,β,γ), (α,γ,δ), $(\alpha,t(\beta),\lambda)$, $(\alpha,\lambda,\omega) \in \Delta$ imply $t(\delta) = \omega$;
(13) $(\alpha, s(t(\beta)), \beta) \in \Delta$ implies $(\alpha,\beta,s(t(\beta))) \in \Delta$;

and (1′), (2′), (3′), (4′), (12′), (13′) which are formally identical to (1), (2),...,(13) but with Δ and Σ interchanged.

If, in addition,

(14) $\alpha, \beta \in C$, $s(\alpha) \neq \beta$ imply there exists γ with $(\alpha,\beta,\gamma) \in \Delta$,

then we say the context is *full.* If a context satisfies

(15) $(\alpha,\beta,\gamma) \in \Delta$ implies $(\beta,\alpha,\gamma) \in \Delta$; and
(15′) $(\alpha,\beta,\gamma) \in \Sigma$ implies $(\beta,\alpha,\gamma) \in \Sigma$;

then we say the context is *abelian.* Note then (12), (12′), (13) and (13′) are redundant.

We now give a converse to the $p = 1$ case of Theorem 1.

THEOREM 2. *Let C be a full context (actually, just the unprimed premises and the first half of (1′) suffice). Let D^* be C with a formal symbol 1 adjoined. Define*

$$1 \cdot 1 = 1, \quad s(\alpha) \cdot \alpha = 1, \quad \alpha \cdot 1 = \alpha, \quad 1 \cdot \alpha = \alpha,$$
$$t(1) = 1, \quad s(1) = 1, \quad \alpha \cdot \beta = \gamma \quad \text{if } (\alpha,\beta,s(\gamma)) \in \Delta$$

for all $\alpha, \beta, \gamma \in C$. Then there exists a unique $e \in D^*$ with $\alpha \cdot e = t(\alpha) \cdot s(t(s(\alpha)))$ for all $\alpha \in C$. Let D be D^* with a formal symbol 0 adjoined. Define

$$0 \cdot a = 0, \quad a \cdot 0 = 0, \quad 0 \cdot 0 = 0,$$
$$0 + a = a, \quad a + 0 = a, \quad 0 + 0 = 0, \quad \text{and}$$
$$a + b = a \cdot t(s(a) \cdot b \cdot e) \quad \text{if } s(a) \cdot b \cdot e \neq 1, \quad \text{and}$$
$$a + b = 0 \quad \text{if } s(a) \cdot b \cdot e = 1,$$

for all $a, b \in D^*$. Then a division ring results. Also $C_1(D) = C$.

PROOF. First we show that D^* is a group. Existence of an identity and inverses are quickly checked. Let $a, b, c \in D^*$. We wish to check $(a \cdot b) \cdot c = a \cdot (b \cdot c)$. One checks this when $a = 1$ or $b = 1$ or $c = 1$ so without loss $a = \alpha$, $b = \beta$, $c = \gamma$ are in C.

Case 1. $s(\alpha) = \beta$, $\gamma = \alpha$. Use (6).
Case 2. $s(\alpha) = \beta$, $\gamma \neq \alpha$. Use (6), (14) and (1).
Case 3. $\gamma = s(\beta)$, $\gamma = \alpha$. Use (6).

Case 4. $\gamma = s(\beta)$, $\gamma \neq \alpha$. Use (6), (14) and (1).

Without loss we can assume $\beta \neq s(\alpha)$, $s(\beta) \neq \gamma$. Let $(\alpha, \beta, s(\delta))$, $(\beta, \gamma, s(\lambda)) \in \Delta$. We need to prove $\delta \cdot \gamma = \alpha \cdot \lambda$.

Case 1. $\delta = s(\gamma)$. Use (6), (1) and (2).

Case 2. $\alpha = s(\lambda)$. Use (1), (2) and (6).

Case 3. $\delta \neq s(\gamma)$, $\alpha \neq s(\lambda)$. Use (6), (14), (4) and (2).

We now prove, for $\alpha, \beta \in C$,

$$s(\alpha) \cdot t(\alpha) \cdot s(t(s(\alpha))) = s(\beta) \cdot t(\beta) \cdot s(t(s(\beta))).$$

Case 1. $\alpha \neq t(\alpha)$, $s(\alpha) \cdot t(\alpha) \cdot s(t(s(\alpha))) \neq 1$. By (14), $(s(\alpha), t(\alpha), s(\gamma)) \in \Delta$ for $\gamma \in C$. Write δ for $s(t(s(\alpha)))$. By (6) and (8), $(s(\alpha), t(\alpha), \delta) \in \Sigma$. Since $s(\alpha) \cdot t(\alpha) \cdot \delta \neq s(\delta)$, $\gamma \neq s(\delta)$ so $s(\gamma) = \delta$. By (14), $(\gamma, s(s(\delta)), s(\lambda)) \in \Delta$ for $\lambda \in C$. By (1), $(\lambda, s(\delta), s(\gamma)) \in \Delta$. By (3),

$$(s(\alpha) \cdot t(\alpha) \cdot s(t(s(\alpha))), s(\delta), \delta) \in \Sigma.$$

If $\beta \neq t(\beta)$, $s(\beta) \cdot t(\beta) \cdot s(t(s(\beta))) \neq 1$, the same argument on β with (7) yields our result. If $\beta \neq t(\beta)$, $s(\beta) \cdot t(\beta) \cdot s(t(s(\beta))) = 1$, then $s(\beta) \cdot t(\beta) = t(s(\beta))$, so

$$(s(\beta), t(\beta), s(t(s(\beta)))) \in \Delta,$$

so by (8) and (5), $\Delta = \Sigma$, which with (8) contradicts $s(\alpha) \cdot t(\alpha) \cdot s(t(s(\alpha))) \neq 1$. If $\beta = t(\beta)$, by (8) and (1), $(s(t(s(\beta))), s(\beta), \beta) \in \Sigma$ so (7) yields

$$s(t(s(\beta))) = s(\alpha) \cdot t(\alpha) \cdot s(t(s(\alpha)))$$

which with $s(\beta) \cdot t(\beta) = 1$ gives our result.

Case 2. $s(\alpha) \cdot t(\alpha) \cdot s(t(s(\alpha))) = 1$. One checks

$$(s(\alpha), t(\alpha), s(t(s(\alpha)))) \in \Delta$$

so, with (8) and (5), $\Delta = \Sigma$, so by (8)

$$(s(\beta), t(\beta), s(t(s(\beta)))) \in \Delta,$$

so $s(\beta) \cdot t(\beta) = t(s(\beta))$, so $s(\beta) \cdot t(\beta) \cdot s(t(s(\beta))) = 1$ which is our result.

Case 3. $\beta \neq t(\beta)$. Interchange β and α and proceed as in the last two cases.

Case 4. $\alpha = t(\alpha)$, $\beta = t(\beta)$. By (8),

$$(s(\alpha), \alpha, s(t(s(\alpha)))), (s(\beta), \beta, s(t(s(\beta)))) \in \Sigma,$$

which with (1′), (7) and (6) gives $\alpha = \beta$, which gives our result.

We now prove for $\alpha, \beta \in C$, $s(\alpha) \neq \beta$, that

$$t(\alpha \cdot \beta) = t(\alpha) \cdot t(t(\alpha^{-1})^{-1} \cdot t(\beta)).$$

Write γ for $\alpha \cdot \beta$ and δ for $t(\alpha^{-1})^{-1} \cdot t(\beta)$, which one checks is in C. Then (6) and (9) give $t(\alpha) \cdot t(\delta) = t(\gamma)$, which is what we want.

We prove, for $a, b \in D^*$, that $t(a \cdot b \cdot a^{-1}) = a \cdot t(b) \cdot a^{-1}$. Clearly, without loss $a = \alpha \in C$, $b = \beta \in C$.

Case 1. $s(\alpha) \neq \beta$, $s(\alpha) \neq t(\beta)$. Using (14), there exists γ, $\lambda \in C$ with

$$(\alpha, \beta, s(\gamma)), (\alpha, t(\beta), s(\lambda)) \in \Delta.$$

If $\gamma = \alpha$, we would have $\alpha \cdot \beta = \alpha$ or $\beta = 1$. If $\lambda = \alpha$, we would have $\alpha \cdot t(\beta) = \alpha$ or $r(\beta) = 1$. Hence by (14), there exists $\omega, \pi \in C$ with

$$(\gamma, s(\alpha), s(\omega)), (\lambda, s(\alpha), s(\pi)) \in \Delta.$$

By (1), (6), and (12), $t(\omega) = \pi$, which is our result.

Case 2. $s(\alpha) = \beta$, $s(\alpha) \neq t(\beta)$. As above,

$$(\alpha, t(\beta), s(\lambda)), (\lambda, s(\alpha), s(\pi)) \in \Delta.$$

By (1) and (6),

$$(\lambda, s(t(\beta)), \beta), (\lambda, \beta, s(\pi)) \in \Delta.$$

By (13) and (2), $s(t(\beta)) = s(\pi)$, so $t(\beta) = \pi$ which is our result.

Case 3. $s(\alpha) \in \beta$, $s(\alpha) = t(\beta)$. As in Case 1, $(\alpha, \beta, s(\gamma)), (\gamma, s(\alpha), s(\omega)) \in \Delta$. Using (1) and (6), one checks

$$(s(\gamma), s(t(\beta)), \beta), (\omega, s(t(\beta)), s(\gamma)) \in \Delta.$$

By (13) and (6),

$$(s(\gamma), \beta, s(t(\beta))) \in \Delta,$$

$$(s(t(\beta)), s(\gamma), \beta), (s(t(\beta)), s(\gamma), \omega) \in \Delta,$$

so by (2), $\beta = \omega$ which is our result.

Case 4. $s(\alpha) = \beta$, $s(\alpha) = t(\beta)$. By (6), $t(s(\alpha)) = s(\alpha)$, which is our result.

Employing Theorem 3.3 of [**1**], Theorem 1 is now proved.

By a *number context* we mean a $C_p(F)$ where p is an odd prime and F is a number field. Such is abelian and finite (by the recent positive solution to the Mordell conjecture; see [**2**]). By a *subcontext* of a context C we mean a subset S of C such that

$$\alpha \in S \text{ implies } s(\alpha),\ t(\alpha) \in S;$$

and

$$\alpha, \beta, \gamma \in S,\ (\alpha, \beta, \gamma),\ (s(t(s(\alpha))), t(\beta), y) \in \Delta \text{ imply } y \in S.$$

One checks that such is a context in its own right, with the intersection of Δ and Σ to S^3 and with the restriction of s and t to S.

We will now prove that any number context is isomorphic to a subcontext of a finite full abelian context; actually, we prove a stronger general representation theorem. By a *spread of classes* we mean a pair (S, p) where p is a prime number, and S is a subset of Z_p such that $0 \notin S$, $1 \notin S$;

$$\alpha \in S \text{ implies } \alpha^{-1} \text{ and } 1 - \alpha \text{ are in } S;$$

and

$$\alpha, \beta \in S,\ \alpha \in \beta \cdot S \text{ imply } (1 - \alpha) \in (1 - \beta) \cdot S.$$

Each such is a subcontext of $C_1(Z_p)$ and thus is a context.

THEOREM 3. *Let S be a number context. Then S is isomorphic to a spread of classes.*

PROOF. One checks that a subcontext of a subcontext is a subcontext. One checks, if K is a field extension of a field F, then $C_p(F)$ is a subcontext of $C_p(K)$. Let F be a number field and p be an odd prime, with $S = C_p(F)$. Let K be the normal closure of F. S is a subcontext of $C_p(K) = T$. By the Tchebotarev density theorem (see p. 169 of [**3**]), K has infinitely many valuations of degree one. But for all but finitely many valuations v of K,

$$v(\alpha) = 0, \quad v(t(\alpha)) = 0, \quad v(t(\beta \cdot \gamma)) = 0,$$

$$v(t(\delta \cdot \lambda \cdot \omega)) = 0, \quad v(t(-\mu \cdot \pi \cdot \eta)) = 0,$$

for all $\alpha \in T$, all $\beta, \gamma \in T$ with $\beta \cdot \gamma \neq 1$, all $\delta, \lambda, \omega \in T$ with $\delta \cdot \lambda \cdot \omega \neq 1$ and all $\mu, \pi, \eta \in T$ with $-\mu \cdot \pi \cdot \eta \neq 1$. Hence such a v exists of degree one. Let A, P, k be the valuation ring, maximal ideal, and residue class field, respectively, of v. Let $\phi: T \to C_1(k)$ be the well-defined map $\alpha \mapsto \alpha + P$, for $\alpha \in T$. One checks that ϕ is injective. One checks that ϕ commutes with s and t. One checks that

$$(\phi(\alpha), \phi(\beta), \phi(\gamma)) \in \Delta \quad \text{(respectively} \in \Sigma)$$

if and only if $(\alpha, \beta, \gamma) \in \Delta$ (respectively $\in \Sigma$). Finally, one checks the last condition for being a subcontext.

Using Theorem 2 one gets (since a number field has no subfield of p-powers)

THEOREM 4. *A number context is itself full if and only if it is empty.*

REFERENCES

1. D. K. Harrison, *On ordered groups, division rings and fields*, Comm. Algebra **12** (1984).
2. G. Faltings, *Endlichkeitssatze fur Abelsche Varietaten über Zahlkorpern*, Invent Math. **73** (1983), 349–366.
3. L. J. Goldstein, *Analytic number theory*, Prentice-Hall, Englewood Cliffs, N.J., 1971.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF OREGON, EUGENE, OREGON 97403

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF ARIZON, TUCSON, ARIZONA 85721