

## CLASS NUMBER BOUNDS AND CATALAN'S EQUATION

RAY STEINER

ABSTRACT. We improve a criterion of Inkeri and show that if there is a solution to Catalan's equation

$$(1) \quad x^p - y^q = \pm 1,$$

with  $p$  and  $q$  prime numbers greater than 3 and both congruent to 3 (mod 4), then  $p$  and  $q$  form a double Wieferich pair. Further, we refine a result of Schwarz to obtain similar criteria when only one of the exponents is congruent to 3 (mod 4). Indeed, in light of the results proved here it is reasonable to suppose that if  $q \equiv 3 \pmod{4}$ , then  $p$  and  $q$  form a double Wieferich pair.

### 1. INTRODUCTION

In 1844 Catalan posed the following question: Do there exist any consecutive positive integers other than 8 and 9 which are powers? This question can be reduced to considering Catalan's equation

$$(1) \quad x^p - y^q = \pm 1,$$

where  $p$  and  $q$  are primes greater than 3. Throughout this paper we shall assume that eq. (1) has a nontrivial solution in integers  $x, y$  and that  $p < q$ . We shall also assume that the reader is familiar with Ribenboim's very fine book on Catalan's equation [14]. Our point of departure is the following result of Inkeri ([4]; see also [14], p. 222).

**Lemma 1** ([4]; see also [14], p. 222). *Suppose  $p \equiv q \equiv 3 \pmod{4}$ . Let  $h(\sqrt{-q})$  be the class number of the quadratic field  $Q(\sqrt{-q})$ . If  $p \nmid h(\sqrt{-q})$ , then  $p^{q-1} \equiv 1 \pmod{q^2}$  and  $q^{p-1} \equiv 1 \pmod{p^2}$ .*

This lemma shows that if  $p \nmid h(\sqrt{-q})$  and  $p \equiv q \equiv 3 \pmod{4}$ , then  $p^{q-1} \pmod{q^2}$  and  $q^{p-1} \equiv 1 \pmod{p^2}$ , i.e.,  $p$  and  $q$  form a *double Wieferich pair*. As we shall see, there is a similar class number condition in all other cases. The purpose of this paper is to show that in many cases these class number conditions never hold, and thus  $p$  and  $q$  form a double Wieferich pair. To this end, we first state (with outline of proof) and extend recent results of Mignotte [11], who gave outlines of proof of the following two results:

**Theorem 1.** *If both  $p$  and  $q$  are congruent to 3 (mod 4), then  $p^{q-1} \equiv 1 \pmod{q^2}$  and  $q^{p-1} \equiv 1 \pmod{p^2}$ .*

---

Received by the editor March 17, 1997.

1991 *Mathematics Subject Classification.* Primary 11D41; Secondary 11R29.

*Key words and phrases.* Catalan's equation, class number bounds, algebraic number fields.

**Theorem 2.** *If  $p \equiv 3 \pmod{4}$ , then  $p^{q-1} \equiv 1 \pmod{q^2}$ . If  $q \equiv 3 \pmod{4}$ , then  $q^{p-1} \equiv 1 \pmod{p^2}$ .*

For this purpose, we use an upper bound for class numbers of imaginary quadratic fields due to Louboutin [8].

Theorems 1 and 2 improve results of O’Neil [13], who obtained Theorem 1 only for  $\min(p, q) > 113233$ ,  $\max(p, q) > 284575469$  and Theorem 2 only for  $\min(p, q) > 1780549$ ,  $\max(p, q) > 41605234051$ . Incidentally, O’Neil’s second result is incorrectly stated in [13].

We also investigate the cases  $p \equiv 1 \pmod{4}$  or  $q \equiv 1 \pmod{4}$ . Unfortunately, these cases have turned out to be far more difficult and elusive than the preceding ones.

The first result about these cases was obtained by Inkeri [5], who proved

**Theorem 3.** *Let  $h_p$  be the class number of the cyclotomic field  $Q(\zeta_p)$ . If  $q \nmid h_p$ , then  $p^{q-1} \equiv 1 \pmod{q^2}$ . If  $p \nmid h_q$ , then  $q^{p-1} \equiv 1 \pmod{p^2}$ .*

Unfortunately, this result turned out to be very difficult to use. As is well known,  $h_p$  can be written as  $h_p = h_p^+ \cdot h_p^-$ . While there is a straightforward algorithm for computing  $h_p^-$ ,  $h_p^+$  is very difficult to compute. In fact, its value is only known for a few cases if  $p > 67$ . In 1993 Mignotte [10] improved Theorem 3 as follows:

**Theorem 4.** *Let  $p$  and  $q$  be odd prime numbers. Let  $p - 1 = dk$ , where  $k$  is odd and  $d = 2^t$  for some integer  $t$ . Assume  $k > 1$ . Put  $\zeta = e^{2\pi i/p}$ . Let  $g$  be a primitive root mod  $p$  and  $m = g^d \pmod{p}$ . Let  $K = Q(\xi)$ , where  $\xi = \zeta + \zeta^m + \dots + \zeta^{m^{k-1}}$ . Let  $h_K = h_K(p)$  denote the class number of  $K$ . If  $q \nmid h_K$ , then  $p^{q-1} \equiv 1 \pmod{q^2}$ .*

Note that in this theorem  $p$  and  $q$  may be interchanged.

Unfortunately,  $h_K$ , the class number of  $K$ , can again be written  $h_K = h_K^- \cdot h_K^+$  and while  $h_K^-$  is easy to compute (in fact, Clother [2] and Louboutin [9] have just given very fine algorithms for this purpose),  $h_K^+$  is difficult to compute if  $d$  is large. Finally, Schwarz [15] showed that one need not compute  $h_K^+$  at all.

**Theorem 5.** *Let  $K$  and  $h_K$  be as above. If  $q \nmid h_K^-$ , then  $p^{q-1} \equiv 1 \pmod{q^2}$ .*

As before,  $p$  and  $q$  may be interchanged in this result.

The main theorem of our paper (and the key for the proof of our new results on Catalan’s conjecture) is the following improvement of Schwarz’s result:

**Theorem 6.** *Let the level of  $q$  (denoted by  $\text{lev}(q)$ ) be equal to  $v_2(q-1)$  and let  $d$ ,  $K$  and  $h_K$  be as above. Suppose  $\text{lev}(q) \leq \text{lev}(p)$ . Let  $F$  denote the order of  $q \pmod{d}$ . If  $q^f \nmid h_K^-$ , then  $p^{q-1} \equiv 1 \pmod{q^2}$ .*

Let  $f$  denote the order of  $q \pmod{d}$ . If  $q^f \nmid h_K^-$ , then  $p^{q-1} \equiv 1 \pmod{q^2}$ . Again,  $p$  and  $q$  are interchangeable here.

From this result and a new relative class number bound for imaginary abelian fields of Louboutin [8] we prove

**Theorem 7.** *Suppose  $p \equiv 3 \pmod{4}$  and  $q \equiv 5 \pmod{8}$ . Then  $p$  and  $q$  form a double Wieferich pair.*

We also extend the “Corollaire” of [11] and prove

**Theorem 8.** *If  $p \equiv 5 \pmod{8}$  and  $q \equiv 3 \pmod{4}$ , then  $p$  and  $q$  form a double Wieferich pair.*

These theorems make it clear that the essence of completing a proof of Catalan's conjecture is to find sharp upper bounds on  $p$  and  $q$  by improving the lower bounds for linear forms in logarithms, calculating all relevant double Wieferich pairs below these bounds and then using an idea of Mignotte [10] to complete the remaining cases. At present the provable bound for  $q$  (about  $4 \cdot 10^{17}$ ) may be too large to make the checking of the double Wieferich conditions possible.

Incidentally, we note that there are only six double Wieferich pairs known:  $(p, q) = (2, 1093), (3, 1006003), (5, 1645333507), (83, 4871), (911, 318917)$  and  $(2903, 18787)$ . Very recently, Ernvall and Metsänkylä [3] have shown that there are no further double Wieferich pairs with both  $p$  and  $q$  less than one million. Further, Mignotte [11] has shown that there are no further such pairs if  $p < 10^5$  and  $q < 2.77p \log p (\log q - \log \log p + 2.34)^2$ . Both of these results were obtained after very long computer searches.

Of course  $p$  always divides  $a^p - a$  but it rarely happens that  $p$  also divides the quotient  $(a^p - a)/p$ . Thus there does not seem to be any hope of avoiding the extensive calculation needed to complete the solution of Catalan's conjecture. However, elimination of all the class number conditions from Catalan's conjecture would reduce it to examining very few pairs  $(p, q)$ .

## 2. NECESSARY LEMMAS

We now list some results on eq. (1) relevant to our problem. Some of these can be found in [14].

- Lemma 2.** (i)  $q < 4.13 \cdot 10^{17}$  and  $p < 3.31 \cdot 10^{12}$ .  
(ii) If  $p \equiv 3 \pmod{4}$ , then  $q < 2.16 \cdot 10^{16}$  and  $p < 2.73 \cdot 10^{12}$ .  
(iii)  $p > 100000$  and  $q > 1000000$ .

The first two of these results were obtained by O'Neil [13], who used a new, sharp result on linear forms in logarithms of three positive rational numbers found in [1] and some results of Mignotte and Roy [12]. The last result is due to Mignotte [11].

**Lemma 3** ([11], [12]). (i)

$$(2) \quad q \leq 2.77p \log p (\log q - \log \log p + 2.34)^2 \quad \text{for } p > 10^4.$$

(ii)

$$(3) \quad \text{If } p \equiv 3 \pmod{4}, \text{ then } q \leq 4.51p(\max(17, \log q + 3.5))^2.$$

(iii) If  $p \equiv 5 \pmod{8}$ , then  $q \leq 17.75p(2.5 + \log q)^2$ .

These results were obtained by using very sharp results on linear forms in two logarithms obtained by Laurent, Mignotte and Nesterenko [7].

**Lemma 4** ([8], class number bounds). (a) *The class number of the imaginary quadratic field  $Q(\sqrt{-q})$ ,  $q \equiv 3 \pmod{4}$ , satisfies the inequality*

$$(4) \quad h(\sqrt{-q}) < \frac{\sqrt{q}}{2\pi} (\log q + 2 + \gamma - \log \pi).$$

(b) *Let  $N$  be an imaginary abelian field of degree  $2n \geq 2$ ,  $\omega_N$  the number of roots of unity in  $N$ ,  $h_N^-$  its relative class number and  $Q_N$  its Hasse index (always 1 or*

2: see [16]). Let  $A_N$  be the quotient of the discriminants of  $N$  and its maximal real subfield  $N^+$  (of degree  $n$ ), and  $c_1 = (2 + \gamma - \log \pi)/(4\pi) = 0.1139\dots$ . Then

$$(5) \quad h_N^- \leq Q_N \omega_N \sqrt{A_N} \left( \frac{1}{4\pi n} \log A_N + c_1 \right)^n.$$

### 3. PROOF OF THEOREMS

As we pointed out in the introduction, the proof of Theorem 1 was outlined by Mignotte [11]. We shall give the proof in full for completeness and illustration of the techniques used.

*Proof of Theorem 1.* Let us assume  $p \equiv q \equiv 3 \pmod{4}$  and  $p \mid h(\sqrt{-q})$ . Since  $p > h(\sqrt{-p})$ ,  $q \nmid h(\sqrt{-p})$  so  $p^{q-1} \equiv 1 \pmod{q^2}$ . By Lemma 2, we may also assume that  $q > 1000000$ . First, an application of Lemma 4 (using  $q > 1000000$ ) gives

$$(6) \quad p \leq h(\sqrt{-q}) < 0.17566\sqrt{q} \log q.$$

Also, by (3) we get  $q \leq 4.51p(\log q + 3.5)^2$  which implies

$$q < 7.0846p(\log q)^2.$$

Substituting in (6), we get

$$\frac{\sqrt{q}}{(\log q)^3} < 1.2445.$$

This yields  $q < 47200000$ . Finally, (6) yields  $p \leq h(\sqrt{-q}) < 21325$ . But this contradicts  $p > 100000$  and the result follows.  $\square$

*Proof of Theorem 2.* As in the proof of Theorem 1, we see that if  $p \equiv 3 \pmod{4}$ ,  $q$  does not divide  $h(\sqrt{-p})$  so  $p^{q-1} \equiv 1 \pmod{q^2}$ . To show that  $p \nmid h(\sqrt{-q})$  if  $q \equiv 3 \pmod{4}$ , we note that  $p > 100000$ , and a long computer search shows that if  $q < 2 \cdot 10^9$  there are only 9 cases with  $h(\sqrt{-q}) > 100000$ . These are

$$\begin{aligned} (q, h(\sqrt{-q})) = & (1909754831, 100411), \quad (1912080959, 100057), \\ & (1952812319, 100193), \quad (1959974519, 102551), \\ & (1962039551, 102079), \quad (1963698959, 101741), \\ & (1982662919, 100943), \quad (1992681239, 100393) \quad \text{and} \\ & (1994489111, 100799), \end{aligned}$$

and in each case  $p$  must equal  $h(\sqrt{-q})$ . However, we find that none of these cases satisfy  $p^{q-1} \equiv 1 \pmod{q^2}$  or  $q \mid h_K^-$ . Thus we can assume  $q > 2 \cdot 10^9$ . Then (5) yields

$$(7) \quad p \leq h(\sqrt{-q}) < 0.169801\sqrt{q} \log q.$$

Substituting in (2) and simplifying we get

$$(8) \quad \frac{\sqrt{q}}{(\log q)^4} < 0.302472,$$

which yields  $q < 6.065 \cdot 10^9$  and  $p \leq 297853$ .  $\square$

But using this result, (2), (7) and (8) we reduce the bound to  $q < 5.206 \cdot 10^9$ ,  $p \leq 274103$ . Repeating this eleven more times, we get  $q < 3.946 \cdot 10^9$  and  $p \leq 235679$ . But another long computer search reveals that for  $q$  in this range, in all cases with  $h(\sqrt{-q}) > 100000$ , neither of the conditions  $p^{q-1} \equiv 1 \pmod{q^2}$  or  $q \mid h_K^-$  is satisfied. Thus the result follows.

**Corollary 1.** *If  $q \equiv 3 \pmod{4}$ ,  $p$  cannot divide  $h(\sqrt{-q})$ .*

Now we give the proof of Theorem 6, which is the key to all our new results on Catalan's conjecture. This theorem follows at once from

**Lemma 5.** *Let  $p$  and  $q$  be odd primes and suppose  $\text{lev}(p) = t$ ,  $d = 2^t$ , and  $\text{lev}(q) < \text{lev}(p)$ . If  $q \mid h_K^-$ , then  $q^f \mid h_K^-$ , where  $f$  is the order of  $q \pmod{d}$ .*

*Proof.* Let  $K$  be the subfield of  $Q(\zeta_p)$  of degree  $d$  over  $Q$ . By Theorem 10.4 of [16],  $K$  has odd class number. Let  $\text{lev}(q) < \text{lev}(p)$  and let  $A$  be the subgroup of  $H_K$  consisting of elements of order 1 or  $q$ . Since  $q$  is odd, we can use the ideas of Section 6.3 of [16] to get  $A = A^+ \oplus A^-$ , where  $A^+ = (\frac{1+J}{2})A$ ,  $A^- = (\frac{1-J}{2})A$ , and  $J$  is complex conjugation. Let  $\sigma$  generate  $\text{Gal}(K/Q)$ . Then  $\sigma$  has order  $d$  and  $\sigma^{d/2} = J$ . Let  $v \in A^-$  and suppose that the orbit of  $v$  under the action of  $\text{Gal}(K/Q)$  has fewer than  $d$  elements. Then  $\sigma^i v = v$  for some  $i, i < d, i \mid d$ . In particular,  $-v = Jv = \sigma^{d/2} v = v$ , so  $v = 0$ . Thus every nonzero element of  $A^-$  has  $d$  elements in its orbit, so  $|A^-| \equiv 1 \pmod{d}$ . Thus if  $q \mid h_K^-$ , then  $q^f \mid h_K^-$ . The result follows.  $\square$

*Note.* This result was discovered by the author while experimenting with class numbers of  $K(p)$  for various primes  $p$ . It is a strengthening of Theorem 10.8 of [15] for subfields of  $Q(\zeta_p)$  of degree  $d$ , since the restriction that  $q$  not divide the class number of any intermediate subfield between  $Q$  and  $K(p)$  is unnecessary. The idea of the proof is due to L. C. Washington, who sent the proof for  $d = 8$ .

*Proof of Theorem 7.* We use Lemmas 4(b) and 5. We take  $\zeta = e^{2\pi i/q}$  and  $L = K(q)$ , where  $K(q)$  is the field defined in Theorem 4, and  $K = Q$ . Here  $K(q)$  is a cyclic quartic extension of  $Q$  of degree  $q^3$ , so  $n = 2$ . Some results of Clother [2, Chapter 3] yield  $\omega_N = 2$  and  $Q_N = 1$ . Suppose  $p \mid h_K^-(q)$ . Then by Lemma 5 we get  $p^2 \mid h_K^-(q)$  and eq. (5) yields

$$p^2 < 2q \left( \frac{1}{4\pi} \log q + 0.114 \right)^2,$$

which simplifies to  $p < 0.12421\sqrt{q} \log q$ . Substituting into (3), we get

$$\frac{\sqrt{q}}{(\log q)^3} < 0.87998,$$

which yields  $q < 16210000$  and  $p < 8302$ . This contradicts  $p > 100000$ .  $\square$

*Proof of Theorem 8.* By Corollary 1,  $p \nmid h(\sqrt{-q})$ , so all we need do is show  $q \nmid h_K^-(p)$ . We take  $\zeta = e^{2\pi i/(p)}$  and  $L = K(p)$ ,  $K = Q$ . Suppose  $q \mid h_K^-(p)$ . Then by Lemma 5, we get  $q^2 \mid h_K^-(p)$  and, by eq. (5),

$$q^2 < 2p \left( \frac{1}{4\pi} \log p + 0.114 \right)^2,$$

which simplifies to

$$q < 0.1266\sqrt{p} \log p,$$

but this is always less than  $p$ , contradiction.  $\square$

## 4. CONCLUDING REMARKS

The theorems of this paper show that in many cases of Catalan's equation we can eliminate the class number conditions completely. In view of Theorems 7 and 8, the following conjecture seems likely:

*Conjecture.* If  $q \equiv 3 \pmod{4}$ , then  $p$  and  $q$  form a double Wieferich pair.

We shall return to this conjecture in a future paper.

## ACKNOWLEDGMENTS

The author is deeply grateful to S. Louboutin for sending him reprints of his papers on class number bounds of imaginary abelian number fields and pointing out an error in the main result of [6], which was used in an earlier version of this paper. The author is also deeply grateful to Duncan Buell of the Center for Computing Sciences for doing a duplicate run of the long computer searches used in the proof of Theorem 2 and to L. C. Washington for sending the proof of Lemma 5 for  $d = 8$ .

## REFERENCES

1. C. Bennet, J. Blass, A. M. W. Glass, D. Meronk and R. Steiner, *Linear forms in the logarithms of three positive rational numbers*, Journal Théorie des Nombres Bordeaux **9** (1997), 97–136.
2. D. R. Clother, *Eliminating possible counterexamples to Catalan's conjecture by computation of class numbers of  $M^2$ -fields*, Master's thesis, Bowling Green State University, 1995.
3. R. Ernvall and T. Metsänkylä, *On the  $p$ -divisibility of Fermat quotients*, Math. Comp. **66** (1997), 1353–1365. MR **97i**:11003
4. K. Inkeri, *On Catalan's problem*, Acta Arith. **9** (1964), 285–290. MR **29**:5780
5. ———, *On Catalan's conjecture*, J. Number Theory **34** (1990), 142–152. MR **91e**:11030
6. A. F. Lavrik, *A remark on the Siegel-Brauer theorem concerning the parameters of algebraic number fields*, Mat. Zametki **8** (1970), 259–263; English Transl. in Math Notes **8** (1970), 615–617. MR **45**:219
7. M. Laurent, M. Mignotte and Y. V. Nesterenko, *Formes linéaires en deux logarithmes et déterminants d'interpolation*, J. Number Theory **55** (1995), 285–321. MR **96h**:11073
8. S. Louboutin, *Majorations explicites de  $|L(1, \chi)|$  (Suite)*, C. R. Acad. Sci. Paris **323** (1996), 443–446. MR **93m**:11084
9. S. Louboutin, *Computation of relative class numbers of imaginary abelian number fields* (to appear).
10. M. Mignotte, *A criterion on Catalan's equation*, J. Number Theory **52** (1995), 280–283. MR **96b**:11042
11. M. Mignotte and Y. Roy, *Minorations pour l'équation de Catalan*, C. R. Acad. Sci. Paris Sér. I Math. **324** (1997), 377–380. CMP 97:10
12. ———, *Catalan's equation has no new solution with either exponent less than 10651*, Experiment. Math. **4** (1995), 259–268. MR **97g**:11030
13. T. O'Neil, *Improved upper bounds on the exponents in Catalan's equation*, manuscript, 1995.
14. P. Ribenboim, *Catalan's conjecture. Are 8 and 9 the only consecutive powers?*, Academic Press, New York, 1994. MR **95a**:11029
15. W. Schwarz, *A note on Catalan's equation*, Acta Arith. **72** (1995), 277–279. MR **96f**:11048
16. L. C. Washington, *Introduction to cyclotomic fields*, Springer-Verlag, New York, 1982. MR **85g**:11001

DEPARTMENT OF MATHEMATICS, BOWLING GREEN STATE UNIVERSITY, BOWLING GREEN, OHIO 43403

*E-mail address:* steiner@math.bgsu.edu