Elliptic Wieferich primes

José Felipe Voloch

Fermat's little theorem states that $a^{p-1} \equiv 1 (\bmod p)$, if p is a prime number and a is an integer coprime with p. The primes for which $a^{p-1} \equiv 1 (\bmod p^2)$ are sometimes called base-a Wieferich primes, or simply Wieferich primes if $a = 2$. This stems from a theorem of Wieferich that asserts that the first case of Fermat's last theorem holds if p is not a Wieferich prime (similar results were obtained for a few other bases). This is of historical interest only now, but Wieferich primes appear in other contexts, most notably they are the primes for which "the derivative of a vanishes", when one pursues a number field-function field analogy, such as in ([Bu],[I],[Sm]). Numerical evidence indicates there are very few Wieferich primes for a given base, for instance $p = 1093, 3511$ are the only (base-2) Wieferich primes less than 10^{12}([CDP]). A naive heuristic argument suggests that there should be about $\log\log x$ Wieferich primes up to x, whereas the analogy with function fields would suggest there are only finitely many Wieferich primes. These two possibilities (and an unlikely third) are contrasted in [I]. However there are very few unconditional results on Wieferich primes. For instance it is not known for any base a if there are infinitely many non-Wieferich primes to base a, although Silverman showed that this follows from the *abc*-conjecture and Johnson [J] showed that Mersenne primes are not (base-2) Wieferich primes. About the only unconditional result is due to Granville [G] and asserts that if a is prime (this condition may be removed, as we shall see) and $a^{p-1} \equiv 1 (\bmod p^2)$ for all sufficiently large primes p, then $a^{p-1} \equiv 1 (\bmod p^3)$ for infinitely many primes. Replacing the multiplicative group by the group of an elliptic curve one obtains an analogous notion of elliptic Wieferich primes, introduced by Silverman [S], where it shown that the *abc*-conjecture implies the existence of infinitely many non-elliptic Wieferich primes for some special elliptic curves.

The purpose of this note is to investigate further the elliptic Wieferich primes, we prove an analogue of Granville's result in the number field case and prove some results in the function field case. We will also discuss Silverman's result. In the process we will also indicate simple proofs in the case of the multiplicative group.

Let K be a global field, that is, a number field or a function field in one variable over a finite field. If v is a non-archimedian place of norm q_v of K and $a \in K$, with $v(a) = 0$ then $v(a^{q_v-1} - 1) \geq 1$. If $v(a^{q_v-1} - 1) > 1$, we call v a Wieferich place for base a. If a is a root of unity, all places will be Wieferich places, we exclude this case in what follows. Similarly, let E/K be an elliptic curve and $P \in E(K)$ a rational point. If v is a non-archimedian place of K for which E has good reduction, let N_v be the number of rational points, over the residue field of v, of the reduction of E at v. Then N_vP belongs to the formal group $\hat{E}$ of E at v, which admits a canonical filtration $\hat{E} = E_1 \supset E_2 \cdots$ (see [S2]). We call v an elliptic Wieferich place for base $P \in E$ if $N_vP \in E_2$. Contrary to the case of the multiplicative group, it can happen that $(q_v, N_v) > 1$, which causes some complication. We will call v a strong elliptic Wieferich place for base $P \in E$ if $n_vP \in E_2$, where n_v is the order of P modulo v. We begin generalizing [G]. We say that an element x of an infinite subset of K is almost an n-th power if there exists $y \in K$ such that xy^{-n} lies on a finite set.

Theorem 1. *Let K be a number field.*

(i) Let $a \in K^*$, not a root of unity. If $v(a^{q_v-1} - 1) \geq 2$ for all but finitely many places of K then $v(a^{q_v-1} - 1) \geq 3$ for infinitely many places of K.

(ii) Let E/K be an elliptic curve and $P \in E(K)$ a rational point of infinite order. If $n_vP \in E_2$ for all but finitely many of the places of K satisfying $(n_v, q_v) = 1$, then $n_vP \in E_3$ for infinitely many places of K satisfying $(n_v, q_v) = 1$.

Proof: (i) Assume that $v(a^{q_v-1} - 1) = 2$ for all but finitely many places of K. If r is a prime number and v a place with $v(a^r - 1) > 0$, but $v(a - 1) = 0$, it follows that $v(a^r - 1) = 2$, unless v is on a fixed finite set. Hence, there exists $b \in K$ such that, for infinitely many $r \equiv 1 (\bmod 5)$, say, we have $a^r - 1 = by^2$, for some $y \in K$. Writing $x = a^{(r-1)/5}$ we thus obtain infinitely many points on the curve $ax^5 - 1 = by^2$, contradicting

Faltings' theorem!

(ii) Assume that $n_vP \in E_2 \setminus E_3$ for all but finitely many places of K satisfying $(n_v, q_v) = 1$. We may assume, enlarging K if necessary, that there exists $Q, R \in E(K), 2Q = P, 2R = 0$. Let x be a function on E with divisor $2(R - 0)$. Then, since the divisor of x is divisible by 2, $x(T)$ is almost a square for $T \in E(K)$. If r is a prime number which splits completely in K and v a place with $v(x(rP)) < 0$ then $rP \in E_1$, then $r = n_v$ and $rP \in E_2 \setminus E_3$, unless v is on a fixed finite set, provided that $(q_v, n_v) = 1$. If this doesn't happen, then $r = n_v | N_v$, but also $2|N_v$, since R is rational. However $q_v = r$ since $(q_v, r) > 1$ and r splits in K, but then $2r \leq N_v \leq r + 1 + 2\sqrt{r}$, which is a contradiction for r large. We conclude then that $v(x(rP)) = -4$ for such r. If v is a place with $v(x(rP)) > 0$ then arguing with $2rP$ instead of rP as above we conclude that $v(x(rP)) = 4$. Therefore, for infinitely many r, $x(rP)$ is almost a 4-th power. We have thus produced infinitely many K-rational points on the cover of E defined by $by^4 = x$, for some $b \in K^*$, again contradicting Faltings' theorem!

One can get by with Siegel's theorem by being more careful. One can also make similar arguments in the function field case but there much more is true. For instance, it is easy to see that there are only finitely many Wieferich places to base $a \in K^*$, a not a p-th power, (p being the characteristic of K). Indeed if $v(a^{q_v - 1} - 1) > 1$, then, applying a non-trivial derivation D of K and using that $q_v = 0 \in K$, we get $v(a^{q_v - 2}Da) > 0$, so $v(aDa) > 0$, which can only be satisfied by finitely many v, unless $Da = 0$, as desired. Note that the heuristic argument that gives infinitely many Wieferich places in the number field case also seem to apply to function fields.

As for the elliptic case, there can be infinitely many v's with p dividing n_v which forces these places to be Wieferich. However we have:

Theorem 2. *Let K be a function field of characteristic p, E/K an elliptic curve, $P \in E(K)$, such that $P \notin pE(K_s)$, where K_s is the separable closure of K. Then there are only finitely many strong elliptic Wieferich places to base P with p not dividing n_v.*

Proof: We will assume $p > 2$ for simplicity but the proof can be modified to handle $p = 2$. Suppose first that E is defined over K^p and choose a Weierstrass equation $y^2 = f(x)$ with coefficients in K^p. The map $\mu : E(K) \to K, (x, y) \mapsto Dx/y$ is a homomorphism with kernel $E(K^p) = E(K) \cap pE(K_s)$, for any non-trivial derivation D of K. This is proved, e.g., in [V]. Then $\mu(P) \neq 0$, so there are only finitely many v with $v(\mu(P)) > 0$. If $n_v P = (x, y) \in E_m \setminus E_{m+1}$, then $v(x) = -2m, v(y) = -3m$ and $v(Dx/y) \geq m - 1$, if v is outside a finite set. However, $Dx/y = \mu(n_v P) = n_v \mu(P)$, and we are done. If E is not defined over K^p, we use the map $\mu : E(K) \to K$, with kernel $pE(K)$ constructed in [V] and a similar argument gives the result.

If E is defined over a finite field k, we can refine further the notion of elliptic Wieferich place, by saying that v is a very strong elliptic Wieferich place to base $P \in E(K)$ if $P - P_v \in E_2$, where P_v is the unique point in $E(\bar{k})$ with $P - P_v \in E_1$. Now it is easy to see there are only finitely many very strong elliptic Wieferich places to base $P \in E(K)$ under the assumption of theorem 2. Indeed, if C/k is a curve with function field K then P corresponds to a map $f : C \to E$ and v is a very strong elliptic Wieferich place if and only if df vanishes at v, so if $df \neq 0$, there are only finitely many such places, as desired.

In the hypotheses of theorem 2, it follows from a result of Scanlon [Sc] that there exists m depending on E, P but not on v with $P \notin E_m$. It can be shown, along the lines of Silverman, that in the number field case there exists m depending on E, P such that $P \notin E_m$ for infinitely many v, assuming the *abc* conjecture. Take $x : E \to \mathbf{P}^1$ ramified only above the 2-torsion $E[2]$ of E. By an argument similar to the proof of theorem 1, it is enough to show that P does not get v-adically close to $E[2]$. Now by Belyi's theorem, there exists $f : \mathbf{P}^1 \to \mathbf{P}^1$ ramified only above $\{0, 1, \infty\}$ with $f(x(E[2])) \subset \{0, 1, \infty\}$. Applying *abc* to $f(x(rP))$ for primes r yields the result. The simple form of Belyi's map f when $j(E) = 0, 1728$ allowed Silverman to get $m = 2$ in those cases.

Acknowledgements: The author would like to thank the TARP (grant ARP-006) and the NSA (grant MDA904-97-1-0037) for financial support.

References.

[B] A. Buium, *Geometry of p-jets*, Duke Math. J., to appear.

[CDP] R. Crandall, K. Dilcher, C. Pomerance,*A search for Wieferich and Wilson primes.* Math. Comp. **66** (1997) 433–449.

[G] A.Granville, *Refining the conditions on the Fermat quotient*, Math. Proc. Cambridge Philos. Soc. **98** (1985) 5–8.

[I] Y. Ihara, *On Fermat quotient and "differentiation of numbers"* RIMS Kokyuroku **810** (1992) 324-341, (In Japanese). English translation by S. Hahn, Univ. of Georgia preprint.

[S] J. Silverman,*Wieferich's criterion and the abc-conjecture*, J. Number Theory **30** (1988), 226–237.

[S2] J. Silverman, *The Arithmetic of Elliptic Curves*, Springer 1987.

[Sc] T. Scanlon, *The abc theorem for commutative algebraic groups in characteristic p*, Intern. Math. Research Notices, (1997), **17** 881-898.

[Sm] A. L. Smirnov, *Hurwitz inequalities for number fields*, St. Petersburg Math. J. **4** (1993) 357-375.

[V] J. F. Voloch, *Explicit p-descent for elliptic curves in characteristic p*, Compositio Math. **74** (1990) 247-258.

Dept. of Mathematics, Univ. of Texas, Austin, TX 78712, USA

e-mail: voloch@math.utexas.edu