CORRECTION TO "JACOBI SUMS, FERMAT JACOBIANS, AND RANKS OF ABELIAN VARIETIES OVER TOWERS OF FUNCTION FIELDS"

DOUGLAS ULMER

1. The problem and a simple correction

There is a gap in the proof of Theorem 5.2 in [Ulm07]. Namely, in the displayed equation in Subsection 5.5, the assertion

$$\sum_{i=0}^{3} \left\langle \frac{a_i'}{d'} \right\rangle = 1$$

assumes that $d' \geq 6$. Thus the theorem should have "$\ell > 3$" replaced with "$\ell > 5$".

The corrected statement is:

1.1. **Theorem.** *Let p be a prime number and let E be the elliptic curve over the rational function field $\mathbb{F}_p(t)$ defined by $y^2 + xy = x^3 - t$. Let S be the set of primes $\ell > 5$ such that $p \equiv 1 \pmod{\ell}$. If d is a product of powers of primes from S, then the rank of $E(\overline{\mathbb{F}}_p(t^{1/d}))$ is zero.*

In the rest of this note we give a counterexample to the original statement and make a few additional comments.

2. A counterexample

Suppose that $d = 5^e$ with $e \geq 1$. Let p be a prime such that 5^{e-1} divides f, the order of p in $(\mathbb{Z}/5^e\mathbb{Z})^\times$. Recall that

$$\mathbf{a} = (a_0, \ldots, a_3) = (1, 2, 3, -6).$$

Since $\{1, 2, 3, -6\}$ is a complete set of representatives of $(\mathbb{Z}/5\mathbb{Z})^\times$, it is clear that for every $s \in (\mathbb{Z}/5^e\mathbb{Z}) \setminus 0$ we have

$$\sum_{i=0}^{3} \sum_{j=0}^{f-1} \left\langle \frac{sp^j a_i}{5^e} \right\rangle = 2f.$$

In other words, $s\mathbf{a}$ is supersingular for all s. As in [Ulm07, Section 5], this shows that the rank of $E(\overline{\mathbb{F}}_p(t^{1/d})$ is $d-1$. Therefore, the restriction $\ell > 5$ in Theorem 1.1 is necessary.

It is a pleasure to thank Georgia Tech undergraduates David Turk and Zach Wilt for producing data leading to this observation.

Date: May 30, 2011.

3. Further comments

In light of the above, the first sentence of [Ulm07, Subsection 5.6] should be be modified to include only primes p such that $p-1$ has a prime divisor $\ell > 5$.

Also, the second paragraph of that same subsection was too optimistic, as the case $d = 5^e$, $p \equiv 6 \pmod{25}$ already shows. Here is another counterexample: Let ℓ be the prime 149 and note that $\phi(\ell) = 4 \cdot 37$. One checks that $\{1, 2, 3, -6\}$ is a set of coset representatives for the subgroup of $(\mathbb{Z}/\ell\mathbb{Z})^\times$ of index 4. Let p be a prime whose order mod ℓ is divisible by 37 and whose order mod ℓ^2 is divisible by 149. Then for $d = \ell^e$ and every $s \in (\mathbb{Z}/d\mathbb{Z}) \setminus 0$ we have

$$\sum_{i=0}^{3} \sum_{j=0}^{f-1} \left\langle \frac{sp^j a_i}{\ell^e} \right\rangle = 2f.$$

This implies that the rank of $E(\overline{\mathbb{F}}_p(t^{1/d})$ is $d-1$. If we further insist that p have odd order mod ℓ, we have another contradiction to the hope expressed in the second paragraph of [Ulm07, 5.6]. Calculations with Sage suggest that there are many other counterexamples of this type.

References

[Ulm07] D. Ulmer, *Jacobi sums, Fermat Jacobians, and ranks of abelian varieties over towers of function fields*, Mathematical Research Letters **14** (2007), 453–467.

School of Mathematics, Georgia Institute of Technology, Atlanta, GA 30332
E-mail address: ulmer@math.gatech.edu