CORRIGENDUM FOR “RATIONAL AND INTEGRAL POINTS ON QUADRATIC TWISTS OF A GIVEN HYPERELLIPTIC CURVE”

Andrew Granville

Abstract. We correct an error in the proofs of two of our theorems in [2].

The *abc*-conjecture. *If a, b, c are coprime positive integers satisfying $a+b=c$ then*

$$c \ll N(abc)^{1+o(1)},$$

where $N(m)$ is the product of the distinct primes dividing m

With this one can prove the following result:

Theorem 8.1 of [2] (corrected). *Assume the abc-conjecture. Let $f(x) \in \mathbb{Z}[x]$ have degree n and no repeated roots. Suppose that there exists a polynomial $h(x) \in \mathbb{Z}[x]$ of degree $\ell < n$ with no roots in common with $f(x)$, such that $g(x) := f(x) - h(x)$ has μ distinct roots and*

$$n > \frac{5+\sqrt{17}}{10}\,(4\ell + 5\mu).$$

For all sufficiently large squarefree integers d for which there is more than one non-trivial integer solution to $f(x) = d\,y^2$, say $f(x_1) = d\,y_1^2$ and $f(x_2) = d\,y_2^2$ with $x_1, x_2 \in \mathbb{Z}$, we have $h(x_1)/f(x_1) = h(x_2)/f(x_2)$.

In the proof of Theorem 8.1 in [2] we implicitly assumed that each of a, b, c were non-zero in our application of the *abc*-conjecture, which is not true in one particular case. This gives rise to the possibility that we have two solutions as given in the corrected statement above.

Similarly we assumed the following:

The *abcd*-conjecture. *If a, b, c and d are integers for which $a+b+c+d=0$, where no subsum vanishes and* $\gcd(a,b,c,d)=1$*, then*

$$|a|, |b|, |c|, |d| \ll \ N(abcd)^{3+o(1)}.$$

With this we claimed to have proved the following strengthening:

We thank Maciej Ulas for highlighting this error with his interesting example.

Typeset by $\mathcal{A}\mathcal{M}\mathcal{S}$-TEX

Theorem 8.3 of [2] (corrected). *Assume the abc-conjecture and abcd-conjecture. Let $f(x) \in \mathbb{Z}[x]$ have degree n and no repeated roots. Suppose that there exists a polynomial $h(x) \in \mathbb{Z}[x]$ with no roots in common with $f(x)$, such that $h(x)(f(x)-h(x))$ has $< n/10$ distinct roots. For all sufficiently large squarefree integers d for which there is more than one non-trivial rational solution to $f(x) = dy^2$, say $f(x_1) = dy_1^2$ and $f(x_2) = dy_2^2$ where $x_1, x_2 \in \mathbb{Q}$, we have $h(x_1)/f(x_1) = h(x_2)/f(x_2)$ or $h(x_1)/f(x_1) + h(x_2)/f(x_2) = 1$.*

In the proof of Theorem 8.3 in [2] we implicitly assumed that no subsum vanished in our application of the *abcd*-conjecture, which is not true in two particular cases. These gives rise to the two possibilities for two solutions as given in the corrected statement above.

This issue was brought to my attention by Maciej Ulas who noted that for any integers a, b, there are two points $(g(t), 1)$ and $(t^2 g(t), t^n)$ on the twist $dy^2 = x^n + ax + b$ where $d = g^n + ag + b$ and $g(t) = -\frac{b}{a}\frac{t^{2n}-1}{t^{2n}-t^2}$. Choosing n large enough and t arbitrary large contradicted our original Theorem 8.3 (taking $h(x) = ax + b$), but is now covered by the corrected version: To see this first note that $at^2 g + b = t^{2n}(ag + b)$ by the definition of g. Hence

$$\frac{h(t^2 g(t))}{f(t^2 g(t))} = \frac{at^2 g + b}{(t^{2n} g^n + at^2 g + b)} = \frac{t^{2n}(ag + b)}{(t^{2n} g^n + t^{2n}(ag + b))} = \frac{ag + b}{g^n + ag + b} = \frac{h(g(t))}{f(g(t))}.$$

The proof of Theorem 8.3 in [2] is easier to understand if one remembers to replace $|r|$ by $\max\{|j|, |k|\}$ where $r = j/k$ with j and k coprime integers.

It would be interesting to classify all rational functions $\phi(x) = h(x)/f(x)$ for which some component curve of $(\phi(x_1) - \phi(x_2))/(x_1 - x_2)$ or of $\phi(x_1) + \phi(x_2) = 1$ has genus ≤ 1, particularly with $f(x_1)f(x_2) = z^2$. (Avanzi and Zannier [1] classified all genus 0 components of $(\phi(x_1) - \phi(x_2))/(x_1 - x_2)$ when ϕ is a polynomial but our question seems to be open.)

References

[1] Roberto M. Avanzi and Umberto M. Zannier, *The equation $f(X) = f(Y)$ in rational functions $X = X(t)$, $Y = Y(t)$.*, Compositio Math. **139** (2003), 263–295.

[2] Andrew Granville, *Rational and integral points on quadratic twists of a given hyperelliptic curve*, International Mathematics Research Notices **27(8)** (2007), 1-25.

[3] Maciej Ulas, *Rational points on certain hyperelliptic curves over finite fields*, Bull. Polish Acad. Sci. Math **55** (2007), 97–104.

Département de Mathématiques et statistique, Université de Montréal, CP 6128 succ. Centre-Ville, Montréal QC H3C 3J7, Canada

E-mail address: andrew@dms.umontreal.ca