SEQUENCES OF RATIONAL TORSIONS ON ABELIAN VARIETIES

E. V. Flynn, Mathematical Institute, University of Oxford

Abstract

We address the question of how fast the available rational torsion on abelian varieties over $\mathbb{Q}$ increases with dimension. The emphasis will be on the derivation of sequences of torsion divisors on hyperelliptic curves. Work of Hellegouarch and Lozach (and Klein) may be made explicit to provide sequences of curves with rational torsion divisors of orders increasing linearly with respect to genus. The main results (in §2) are applications of a new technique which provide sequences of hyperelliptic curves for all torsions in an interval $[a_g, a_g + b_g]$ where a_g is quadratic in g and b_g is linear in g. As well as providing an improvement from linear to quadratic, these results provide a wide selection of torsion orders for potential use by those involved in computer integration. We conclude by considering possible techniques for divisors of non-hyperelliptic curves, and for general abelian varieties.

§0. Introduction

Apart from Mazur's result [6] which classifies all possible rational torsions on elliptic curves over $\mathbb{Q}$, there has been virtually no literature which attempts to determine what rational torsions might be available in higher dimension. The lack of a proven upper bound on $\mathbb{Q}$-torsion for any given dimension > 1 (analogous to Mazur's result) is understandable, as the techniques in Mazur's proof use tools which do not yet have analogues in the theory of abelian varieties. From the point of view of searching for rational torsion, most work has concentrated either on elliptic curves over number fields ([3],[5],[8]), or on the point of view of algorithms for determining the rational torsion divisors of a given curve [1]. The latter has largely been motivated by the advent of computer integration programs which exploit the relationship between integrability of algebraic functions and rational torsion

A.M.S. Classifications: 11G, 11Y

divisors. These procedures have in the past had very little opportunity to be tested by curves with large torsion divisors, due to the lack of such explicit curves.

The search for large torsion on abelian varieties cannot merely use a crude analogue of the usual method for elliptic curves (namely, find an explicit model for $X_1(N)$ and search for rational points). The defining equations of the higher dimensional analogues of $X_1(N)$ are far too large, and the techniques for searching for rational points on higher dimensional varieties too slow. It is the purpose of this paper to show how both of these problems may be bypassed if one exploits the availability of special curves of higher genus, which contain a rational divisor D of which a large multiple may easily be described. The derivation of a rational torsion divisor of order approximately the same as this large multiple corresponds [4] to the solubility of a norm form equation with respect to a quadratic extension of $\mathbb{Q}(X)$. Sometimes there is an analogue of a 'fundamental unit' which allows a sequence of torsions, increasing with respect to genus, to be described inductively; an example is given later. The sequences of curves obtained have specialisations which are simple in appearance, and contain rational torsions which increase linearly with respect to genus. A considerable improvement is obtained in §2 by choosing curves for which there are 2 linear conditions on 2 rational points on the curve. This usually provides an easy description of a large multiple of D whose increase divides an amount *quadratic* in the genus, corresponding to the determinant of the matrix of linear conditions. A complete listing of the multiples of D often indicates situations when D has exactly that order. Finally, in §3, we briefly consider divisors on non-hyperelliptic curves, and more general abelian varieties.

§1. Linear Sequences of Torsions

In this section, we make use of an idea of Hellegouarch and Lozach in [4] to provide explicit sequences of hyperelliptic curves with rational torsion divisors of order increasing linearly with respect to genus.

A hyperelliptic curve of genus g may be written in the form

$$Y^2 = Q^\ell(X),\ \ell = 2g+1 \text{ or } 2g+2$$

(discriminant of $Q^\ell(X) \neq 0$), where the notation $P^i(X), Q^i(X), R^i(X)$ or $S^i(X)$ refers to

a polynomial of degree i in X. It will be convenient to use the birationally equivalent form

$$\mathcal{C} : Y^2 + Y \cdot P^k(X) = Q^\ell(X),\ k \leqslant g,\ \ell = 2g+1 \text{ or } 2g+2$$

where the discriminant of $(P^k(X))^2 + 4Q^\ell(X)$ is non-zero.

Each divisor of $\mathcal{C}$ may be represented by an unordered set of g points on the curve, with the group identity $\mathcal{O}$ represented by $g \cdot \omega$, where ω is some fixed rational Weierstrass point, which will always be taken to be ∞ (the point at infinity) when $\ell = 2g+1$. When $\ell = 2g+2$ and g even, we must include ∞^+ and ∞^- (the branches of the singularity at infinity) as separate points on $\mathcal{C}$, and we may take $\mathcal{O} = g/2 \cdot \infty^+ + g/2 \cdot \infty^-$ without reference to a rational Weierstrass point. When $\ell = 2g+2$ and g is odd, then such an $\mathcal{O}$ is not defined over the ground field – however this technicality need not concern us here, as our examples will avoid that situation. Given a point $P = (x, y)$ on $\mathcal{C}$, its *flip* $\overline{P}$ is the unique alternative point on $\mathcal{C}$ with the same x-coordinate, namely $(x, -y - P^k(x))$. The group inverse of a divisor $\{P_1, \ldots, P_g\}$ will then be $\{\overline{P_1}, \ldots, \overline{P_g}\}$. There is a non-uniqueness of codimension 2, characterised by the fact that any subset of the divisor of the form $\{P, \overline{P}\}$ is interchangeable (up to linear equivalence) with any $\{Q, \overline{Q}\}$ (P, Q on $\mathcal{C}$), or, indeed by $\{2 \cdot \omega\}$ where ω is a Weierstrass point. We remove this ambiguity by always denoting such a pair by $\{2 \cdot \infty\}$ when $g = 2\ell + 1$, and by $\{2\,WP\}$ when $g = 2\ell + 2$. In the latter case, if the reader wishes to write a divisor strictly as a set of points on $\mathcal{C}$, then each $\{2\,WP\}$ may be replaced by $\{\infty^+, \infty^-\}$.

Three such divisors D_1, D_2, D_3 sum to $\mathcal{O}$ if there exists a function of the form

$$R^m(X) \cdot Y - S^n(X),\ m \leqslant g/2 - 1, n \leqslant 3g/2$$

whose divisor of zeroes on $\mathcal{C}$ is the union of the supports of D_1, D_2, D_3.

In order to give the explicit sequences of families of curves, we must first define two sequences of polynomials $\theta_i(X), \phi_i(X) \in \mathbb{Z}[X]$ inductively as follows.

$$\theta_1(X) = 1, \phi_1(X) = 1$$

$$\theta_{i+1}(X) = (X+2)\theta_i(X) + 2(X+1)\phi_i(X)$$

$$\phi_{i+1}(X) = 2\theta_i(X) + (X+2)\phi_i(X).$$

It follows that, for any i:

$$\theta_i(X)^2 - (X+1)\phi_i(X)^2 = -X^{2i-1} \tag{1}$$

We observe that (1) may be written as a norm form equation on the quadratic extension $\mathbb{Q}(X)(\sqrt{X+1})/\mathbb{Q}(X)$, namely as:

$$\mathrm{Norm}_{\mathbb{Q}(X)(\sqrt{X+1})/\mathbb{Q}(X)}\big(\theta_i(X) + \phi_i(X)\sqrt{X+1}\big) = -X^{2i-1},$$

and so the above sequence of solutions to (1) may be obtained by setting $\theta_i(X) + \phi_i(X)\sqrt{X+1} = \epsilon^{2i-1}$, where $\epsilon = 1 + \sqrt{X+1}$ has norm $-X$.

We are now in a position to prove:

Result 1. *For any genus g and integer r, $1 \leqslant r \leqslant g/2$,*
(a). The $(g-2r+2)$-parameter family of genus g curves:

$$Y^2 + \big(\phi_r(X)\cdot Y - \theta_r(X)\cdot X^g\big)\cdot \sum_{k=0}^{g-2r+1} w_k X^k = X^{2g+1} + X^{2g}, \quad w_0 \neq 0 \text{ or } -4^{2-r} \tag{2}$$

has the torsion divisor $D = \{(0,0), (g-1)\cdot\infty\}$ of exact order $2g+2r-1$.
(b). The $(g-r+1)$-parameter family of genus g curves:

$$Y^2 = (Y - X^{g+r})(X^{g-r+1} + \sum_{k=0}^{g-r} w_k X^k), \quad w_0 \neq 0 \tag{3}$$

has the torsion divisor $D = \{(0,0), (g-1)\cdot\infty\}$ of exact order $2g+2r$

Proof.
(a). Since ∞ is a Weierstrass point, we have $j\cdot D = \{j\cdot(0,0), (g-j)\cdot\infty\}$ for $j = 1\ldots g$. In particular, $g\cdot D = \{g\cdot(0,0)\}$. Now, from (1) it follows that the function

$$\phi_r(X)\cdot Y - \theta_r(X)\cdot X^g$$

meets (2) at $(0,0)$ with multiplicity $2g+2r-1$, and at no other affine points. Hence $\{(g-2r+1)\cdot\infty, (2r-1)\cdot(0,0)\} + \{g\cdot(0,0)\} + \{g\cdot(0,0)\} = \mathcal{O}$. So $(2r-1)\cdot D + g\cdot D + g\cdot D = \mathcal{O}$, giving that D is $(2g+2r-1)$-torsion. Furthermore, if the exact order of D were a proper factor of $2g+2r-1$, then there would be some $j \leqslant g$ such that either $j\cdot D$ is of order 2

or $j \cdot D = -(j+1) \cdot D$. But $j \cdot D = \{j \cdot (0,0), (g-j) \cdot \infty\}$, so neither of these relations could hold, provided that $(0,0)$ is not a Weierstrass point. The condition $w_0 \neq -4^{2-r}$ guarantees that $Y^2 + (\phi_r(0) \cdot Y - \theta_r(0)) \cdot w_0$ is not the square of a function linear in Y, so that $(0,0)$ cannot be a Weierstrass point.
(b). Here, the function $Y - X^{g+r}$ meets (3) with multiplicity $2g+2r$ at $(0,0)$, and at no other affine points. In a similar manner to (a), this gives that D has order exactly $2g+2r$.

□

Corollary 1. *For any genus g, and any N between $2g$ and $3g$, there is a hyperelliptic curve of genus g over $\mathbb{Q}$ with a rational torsion divisor of order exactly N.*

□

Some specialisations have a particularly simple appearance. For example, the curve:

$$Y^2 + Y = X^{2g+1} + X^{2g} + X^g$$

has the $(2g+1)$-torsion divisor $\{(g-1) \cdot \infty, (0,0)\}$, and the curve:

$$Y^2 + X^g Y + Y = X^{2g+1} + X^{g+1} \tag{4}$$

has the $(2g+2)$-torsion divisor $\{(g-1) \cdot \infty, (0,0)\}$.

§2. Quadratic Sequences of Torsions

In order to derive sequences of intervals of torsions with centres increasing more than linearly in g, one chooses sequences of curves of genus g (with a free parameter r) with rational points $P_1, \ldots, P_n$, so that n different functions meet the curve only at these points. If these functions induce n $\mathbb{Z}[g,r]$-linear conditions given by:

$$A \begin{pmatrix} P_1 \\ \vdots \\ P_n \end{pmatrix} = \begin{pmatrix} \mathcal{O} \\ \vdots \\ \mathcal{O} \end{pmatrix} \tag{5}$$

where $A \in M_n[\mathbb{Z}[g,r]]$, then it is immediate (on multiplying both sides on the left by $\det(A) \cdot A^{-1} \in M_n[\mathbb{Z}[g,r]]$) that

$$\det(A) \begin{pmatrix} P_1 \\ \vdots \\ P_n \end{pmatrix} = \begin{pmatrix} \mathcal{O} \\ \vdots \\ \mathcal{O} \end{pmatrix}$$

so that, for $i = 1, \ldots, n$, $\det(A) \cdot P_i = \mathcal{O}$ (where, as always, everything is up to linear equivalence). This provides a divisor of non-trivial order dividing $\det(A)$.

For the purpose of deriving quadratic sequences, we require only two such points (generally two choices out of: $(0,0)$, $(1,0)$, and $\pm\infty$) and two such functions. A key feature of the following technique is the explicit listing of all multiples of the given divisor D, allowing the exact order of D to be determined. The symbolic algebra package Maple helped to automate this process.

Result 2. *The 1-parameter space of curves of genus g ($t \neq 0$):*

$$\mathcal{C} : Y^2 + \psi(X) \cdot Y = -tX^{g-r}(X-1)^{g+r+1}$$

where $0 \leqslant r \leqslant g-1$, and $\psi(X) = X^{g+1} - t(X-1)^g - X^{g-r}(X-1)^{r+1}$ (degree g in X), has a divisor of positive torsion order dividing: $2g^2+2g+r+1$. In particular, when $r = 0$, the divisor $D = \{(1,0), (g-1)\cdot\infty\}$ has exact order $2g^2+2g+1$.

Proof. Let $D = \{(1,0), (g-1)\cdot\infty\}$. Then $g \cdot D = \{g \cdot (1,0)\}$. Now, the function Y meets $\mathcal{C}$ with multiplicity $g-r$ at $(0,0)$, with multiplicity $g+r+1$ at $(1,0)$, and at no other affine points. So: $(g+1)\cdot D = \{(g-r)\cdot\overline{(0,0)}, r\cdot\overline{(1,0)}\}$, so that $(g+r+1)\cdot D = \{(g-r)\cdot\overline{(0,0)}, r\cdot\infty\}$. (where $\overline{(0,0)} = (0,(-1)^g\cdot t)$ and $\overline{(1,0)} = (1,-1)$). Furthermore, the function $Y - X^{g-r}(X-1)^{r+1}$ meets $\mathcal{C}$ with multiplicity $2g+1-r$ at $(0,0)$, with multiplicity $r+1$ at $(1,0)$, and at no other affine points. It is now immediate that equation (5) is satisfied by taking $P_1 = (0,0)$, $P_2 = (1,0)$ and

$$A = \begin{pmatrix} g-r & g+r+1 \\ 2g+1-r & r+1 \end{pmatrix}$$

so that D has torsion order dividing $\det(A) = 2g^2+2g+r+1$.

In general, this order can be expected to be *exactly* $2g^2+2g+r+1$, unless there is a transparent reason to the contrary. We illustrate this by writing out a complete description of the multiples of D for the case $r = 0$. Namely, the multiple $\big(k(2g+1)+\ell\big)D$ is given

by:

$$\{k\cdot(0,0),\ell\cdot(1,0),(g-k-\ell)\cdot\infty\},\begin{pmatrix}0\leqslant k\leqslant g\\0\leqslant\ell\leqslant g-k\end{pmatrix}$$
$$\{(g-k)\cdot\overline{(0,0)},(g+1-\ell)\cdot\overline{(1,0)},(k+\ell-g-1)\cdot\infty\},\begin{pmatrix}0\leqslant k\leqslant g\\g-k+1\leqslant\ell\leqslant g+1\end{pmatrix}$$
$$\{(g-k)\cdot\overline{(0,0)},(\ell-g-1)\cdot(1,0),(g+k-\ell+1)\cdot\infty\},\begin{pmatrix}0\leqslant k\leqslant g-1\\g+2\leqslant\ell\leqslant g+k+1\end{pmatrix}$$
$$\{(k+1)\cdot(0,0),(2g+1-\ell)\cdot\overline{(1,0)},(\ell-k-g-2)\cdot\infty\},\begin{pmatrix}0\leqslant k\leqslant g-1\\g+k+2\leqslant\ell\leqslant 2g\end{pmatrix}$$

The above describes all multiples of D up to $(2g^2+2g+1)\cdot D$ (corresponding to $k=g,\ell=g+1$), which is $\{g\cdot\infty\}=\mathcal{O}$. Provided that $(0,0),\overline{(0,0)},(1,0),\overline{(1,0)}$ are all distinct points on $\mathcal{C}$ (guaranteed by $t\neq 0$), the above list contains no repetitions, and so D has torsion order exactly $2g^2+2g+1$. □

Similar results may be found for which an explicit description of multiples of D may be written for any value of r. In the following example, this technique allows all torsions to be found in an interval of the form $[a_g,a_g+b_g]$, where a_g is quadratic in g and b_g is linear in g.

Result 3. *In even genus g, there exists $\mathbb{Q}$ rational torsion divisors of all orders in the interval $[g^2+2g+1,g^2+3g+1]$. Explicitly, the 1-parameter space of curves of genus g (g even, $t\neq 0$):*

$$\mathcal{C}:Y^2+t(X-1)Y=\big(\psi(X)\big)^2-t(X^{g+2}+X^{r+1})$$

where $0\leqslant r\leqslant g$, and $\psi(X)=\sum_{i=1}^{g-r+1}X^{r+i}=(X^{g+2}-X^{r+1})/(X-1)$, has a divisor of exact order $g^2+3g+1-r$.

Proof. The function $Y-\psi(X)$ meets $\mathcal{C}$ with multiplicity $g+2$ at $(0,0)$, and with multiplicity g at ∞^+. This is sufficient information to write out all multiples of $D=\{(0,0),\infty^+,(g-2)\cdot WP\}$ up to $\frac{g}{2}(g+2)\cdot D$. Namely, the multiple $\big(k(g+2)+\ell\big)\cdot D$ (for $1\leqslant k\leqslant\frac{g}{2}-1$) is given by:

$$\{\ell\cdot(0,0),(2k+\ell)\cdot\infty^+,(g-2k-2\ell)\cdot WP\},\ 0\leqslant\ell\leqslant\frac{g}{2}-k$$
$$\{(g+2-\ell)\cdot(0,t),(g-2k-\ell)\cdot\infty^-,(2k+2\ell-g-2)\cdot WP\},\ \frac{g}{2}-k+1\leqslant\ell\leqslant g-2k$$
$$\{(g-\ell+2)\cdot(0,t),(2k+\ell-g)\cdot\infty^+,(g-2k-2)\cdot WP\},\ g-2k+1\leqslant\ell\leqslant g+2$$

Now, the function: $Y + t(X-1) - \psi(X)$ meets $\mathcal{C}$ with multiplicity $(r+1)$ at $(0,t)$, and with multiplicity $(2g-r+1)$ at ∞^+, so that equation (5) is satisfied by taking $P_1 = (0,0)$, $P_2 = \infty^+$ and

$$A = \begin{pmatrix} g+2 & g \\ -r-1 & 2g-r+1 \end{pmatrix}$$

Hence D has order dividing $\det(A) = 2(g^2+3g+1-r)$.

Imagine that the order of D were less than $(g^2+3g+1-r)$. Then, it would be at most $\frac{1}{3}\det(A) = \frac{2}{3}(g^2+3g+1-r)$, and so there would exist multiples $\mu_1 \cdot D$, $\mu_2 \cdot D$ with $\mu_1, \mu_2 \leqslant \lfloor \frac{1}{3}(g^2+3g+1-r) \rfloor + 1$, for which $\mu_1 \cdot D = -\mu_2 \cdot D$. But $\lfloor \frac{1}{3}(g^2+3g+1-r) \rfloor + 1 \leqslant \frac{g}{2}(g+2)$, and by inspection the above listing of all multiples of D up to $\frac{g}{2}(g+2) \cdot D$ does not contain such a pair. Hence, the order of D is either $(g^2+3g+1-r)$ or $2(g^2+3g+1-r)$. In the latter case, $2D$ will have the required order. □

A fringe benefit of the care taken to preserve intervals of torsion orders, is that as well as torsions increasing quickly with genus, we also have available many choices of torsion orders for each genus. The user (such as a computer integration programmer [1]) should therefore find a selection of orders of most desired types (such as primes, squares, numbers divisible by a large power of a prime) within the intervals. Furthermore, for a given order (fixing g and r), changing the free parameter t will provide (for generic t) different choices of curves of genus g with that torsion. A example of a function whose integrability depends upon a genus 2 torsion divisor may be found in [2]. We observe that the 13-torsion divisor in genus 2 in [2] is the specialisation of Result 2 to $g = 2, r = 0$. We can construct other examples of similar strength to Results 2 and 3, but do not know how to construct examples that are genuinely more powerful.

§3. Potential Improvements

Having obtained rational torsion divisors on hyperelliptic curves whose orders are quadratic with respect to genus, we now consider potential avenues for improvement. One avenue would be to increase the number of distinguished points on the curve to some $N > 2$, and to restrict the curve so that there are N linear conditions on the N points. In the examples of Section 2, there were 2 linear conditions on 2 distinguished points, and the determinant of the resulting 2 by 2 matrix gave sequences quadratic in g. We might hope that, for example, 3 linear conditions in 3 points might give a sequence of higher

degree in g. Hyperelliptic curves are somewhat constrained in the number of free variables available to satisfy such conditions. One way of increasing the number of free variables is to consider non-hyperelliptic curves. Bryan Birch (personal communication) has observed that an early example of sequences of curves with rational torsion divisors are Klein's 'triangular' curves, given projectively by:

$$\mathcal{C}_{m,a,b,c} : x^{m-c}y^c + y^{m-a}z^a + z^{m-b}x^b + xyz \cdot g(x,y,z)$$

where $m \geqslant 3, 1 \leqslant a,b,c \leqslant m-1$, and g is a form of degree $m-3$. This curve contains the points $P=(1,0,0), Q=(0,1,0), R=(0,0,1)$. Furthermore, the functions x,y,z meet $\mathcal{C}_{m,a,b,c}$ at $a \cdot Q + (m-a) \cdot R, b \cdot R + (m-b) \cdot P, c \cdot P + (m-c) \cdot Q$, respectively. As at the end of section 2, we look at the matrix of linear conditions:

$$\begin{pmatrix} 0 & a & m-a \\ m-b & 0 & b \\ c & m-c & 0 \end{pmatrix}$$

which has determinant $((m-a)(m-b)(m-c)+abc)/m$, providing a divisor with torsion order dividing this quantity. The genus of the curve is at most $\frac{1}{2}(m-1)(m-2)$, and can be expected to be lower than this given the presence of substantial singularities at P,Q,R. There are many ways of choosing a,b,c,m so that the above determinant is prime; for example, if $b=a$, $c=2a$ and $\ell = m-2a$ then $((m-a)(m-b)(m-c)+abc)/m = \ell^2 + a^2$, which will yield every prime congruent to 1 modulo 4. This guarantees a sequence of rational torsion divisors with orders increasing at least linearly with respect to genus.

Bryan Birch has further pointed out that this idea can be extended to 'quadrangular' curves; namely, we construct a curve with the points $P=(1,0,0), Q=(0,1,0), R=(0,0,1), S=(1,1,1)$, which meets the functions $x, y, y-z, x-z$ at $a \cdot R + (m-a) \cdot Q, b \cdot P + (m-b) \cdot R, c \cdot S + (m-c) \cdot P, d \cdot Q + (m-d) \cdot S$. Such a curve is given by:

$$\lambda(z^{m-a-1}y^a(z-x) - y^{m-c}z^{c-1}(z-x) + y^{m-c}(z-x)^c)$$

$$+\mu(x^{m-b}z^{b-1}(z-y) - z^{m-d-1}x^d(z-y) + (z-y)^{m-d}x^d) = xy(x-z)(y-z)\phi$$

where λ, μ are constants, the degree $m \geqslant 4$, ϕ is a form of degree $m-4$ and $1 \leqslant a,b,c,d \leqslant m-1$. The matrix of linear conditions is:

$$\begin{pmatrix} 0 & m-a & a & 0 \\ b & 0 & m-b & 0 \\ m-c & 0 & 0 & c \\ 0 & d & 0 & m-d \end{pmatrix}$$

which has determinant $((m-a)(m-b)(m-c)(m-d)-abcd)/m)$. And so we have a torsion divisor dividing this quantity. We would therefore expect to find sequences of rational torsion divisors on such curves increasing as $(2g)^{3/2}$ – better than the linear sequences of §1, but still worse than the quadratic sequences of §2. However, we might now hope to continue this process to increasing degree, to obtain 5 by 5, 6 by 6 ... matrices of similar type. This might give sequences with a rate of torsion increase which is a higher power of the genus. There are considerable technical difficulties, however. It is not clear when analogues of higher degree exist; for example, the 5 point analogue requires an algebraic extension of $\mathbb{Q}$. There is a $\mathbb{Q}$-rational 6 point example, but the resulting expression (which must be divided by the order of some divisor) is composite, and it is unclear when this maximum is obtained.

More generally, we might search for rational torsion points on sequences of general abelian varieties. One approach which may be inferred directly from the existing literature is first to fix some elliptic curve $\mathcal{E}/\mathbb{Q}$ with complex multiplication and then find the extension field k of smallest degree such that $\mathcal{E}$ has a k-rational m-torsion point. Then $[k:\mathbb{Q}] \leqslant m$, so $N_{k/\mathbb{Q}}\mathcal{E}$ (as defined in [7]) is an abelian variety over $\mathbb{Q}$ of dimension at most m, containing a $\mathbb{Q}$-rational m-torsion point. This crude approach provides sequences of abelian varieties together with torsion orders increasing at least linearly in the dimension. This is slower than the quadratic sequences already found on Jacobians, but the method should be amenable to refinements by taking careful choices of $\mathcal{E}$ for each m (not necessarily with complex multiplication) so as to minimise $[k:\mathbb{Q}]$. In particular, Richard Pinch has pointed out that, since $X_1(11), X_1(13)$ have hyperelliptic models (given in [8]), this process will give abelian varieties over $\mathbb{Q}$ of dimension 2 with $\mathbb{Q}$-rational 11- and 13-torsion points. It would be interesting to compare the resulting varieties with the Jacobians of the genus 2 curves obtained by specialising Results 2 and 3 of §2.

It is also possible to take product varieties of the Jacobians of §2, to get a sequence of abelian varieties with a far more rapidly increasing sequence of torsions.

Corollary 2. *There is a sequence A_n of abelian varieties over $\mathbb{Q}$ of strictly increasing dimensions d_n, each containing a $\mathbb{Q}$-rational torsion point of order r_n, such that r_n increases at least exponentially in $(d_n \log d_n)^{\frac{2}{3}}$. That is to say, there exists a $k > 1$ such that*

$r_n > k^{(d_n \log d_n)^{\frac{2}{3}}}$ *for n sufficiently large.*

Proof. For any m in the interval $[(g+1)^2, (g+1)^2+g]$, g even, let J_m be the Jacobian of a curve of genus g over $\mathbb{Q}$ with a rational m-torsion point (whose existence is guaranteed by Result 3). Let A_n be the product variety of all J_p for primes p in the set $S_n = \bigcup\{[(g+1)^2, (g+1)^2+g] : g \text{ even}, g \leqslant n\}$. It follows from standard results in Analytic Number Theory [9] that the union of all the sets S_n contains the same proportion of the primes as its natural density (namely, $\frac{1}{4}$). That is to say:

$$\big(\text{ Number of primes in } S_n\ \big) \sim \frac{1}{4}\pi\big((n+1)^2+n\big) \sim \frac{1}{4}\pi(n^2) \sim \frac{n^2}{8\log n}.$$

Further, each factor J_p of A_n has dimension at most n, and so A_n has dimension d_n which increases at most as $n^3/(8\log n)$. It follows that, for any $k_1 > \frac{3}{8}$ and n sufficiently large:

$$d_n \log d_n < k_1 n^3.$$

There must be a rational point on A_n with torsion order r_n equal to the product of all primes in S_n. Thus, $\log r_n \sim \frac{1}{4}n^2$, and so for any $k_2 < \frac{1}{4}$ and n sufficiently large:

$$\log r_n > k_2 n^2.$$

Combining the above two inequalities gives that for any choice of $k < \exp\big((\frac{1}{3})^{\frac{2}{3}}\big) \approx 1.617$ and n sufficiently large:

$$r_n > k^{(d_n \log d_n)^{\frac{2}{3}}}$$

as required. □

This result is somewhat artificial, as the torsion orders become heavily composite as the dimension increases, and so there is no indication of whether 'typical' torsion orders exponential in $(d\log d)^{\frac{2}{3}}$ are likely to exist over $\mathbb{Q}$ in dimension d. Note that at the boundary value $k = \exp\big((\frac{1}{3})^{\frac{2}{3}}\big)$, the error terms in the above asymptotic estimates for $\log r_n$ are too large to allow exponentiation. Of course, there is nothing sacred about $\exp\big((\frac{1}{3})^{\frac{2}{3}}\big)$, and it should not be hard to improve this value, either by using an improved alternative to Result 3, or by showing greater finesse in the selection of factors of the product variety. Such finesse as already exists in the above is due to Charles Matthews,

who pointed out that excluding J_m for composite m would improve the exponent of the final result (from $d_n^{\frac{2}{3}}$ to $(d_n \log d_n)^{\frac{2}{3}}$). I am also grateful to both Charles Matthews and Hugh Montgomery, who pointed out that Lemma 5 of [9] (and the standard machinery) implies that the sets S_n contain $\frac{1}{4}$ of the primes.

In the negative direction, it is not known whether there is a global bound on k-rational torsion for any given dimension $d > 1$ and number field k. There is, however, the following result in [10] for abelian varieties of CM-type.

Theorem (Silverberg). *If A is an abelian variety of CM-type and dimension d defined over a number field k, N is the order of a torsion point of $A(k)$, and $\nu(N)$ is the number of distinct primes dividing N, then*

$$\phi(N) \leqslant \begin{cases} [k:\mathbb{Q}](12)^d d! 2^{(d-1)\nu(N)+1} & \text{if } 8|N \\ [k:\mathbb{Q}](12)^d d! 2^{(d-1)\nu(N)} & \text{if } 8 \not| N \end{cases}$$

REFERENCES

[1] Davenport, J. H. *On the Integration of Algebraic Functions*, Springer Lecture Notes in Computer Science, 102, Springer-Verlag (1981).

[2] Flynn, E. V. *Large rational torsion on abelian varieties*, J. Number Theory, **36** (1990), no. 3, 257-265.

[3] Frey, G. *A remark about isogenies of elliptic curves over quadratic fields*, Compositio Math. **58** (1986), no. 1, 133-134.

[4] Hellegouarch, Y., Lozach, M. *Équation Pell et points d'ordre fini*, Analytic and Elementary Number Theory (Marseille, 1983), 72-95, Publ. Math. Orsay, 86-1, Univ. Paris XI, Orsay 1986.

[5] Kamienny, S. *Torsion points on elliptic curves over all quadratic fields*, Duke Math. J., **53** (1988), no. 1, 157-162.

[6] Mazur, B. *Rational points of modular curves*, Modular Functions of One Variable, V, Lecture Notes in Math. **601** (1977), 107-148.

[7] Milne, J. S. *On the arithmetic of abelian varieties*, Invent. Math. **17** (1972), 177-190.

[8] Reichert, M. A. *Explicit determination of non-trivial torsion structures of elliptic curves over quadratic number fields*, Math. Comp. **47** (1986), 637-658.

[9] Saffari, B., Vaughan, R.C. *On the fractional parts of x/n and related sequences, II and III*, Ann. Inst. Fourier, Grenoble, **27**, 2 (1977), 1-36.

[10] Silverberg, A. *Torsion points on abelian varieties of CM-type*, Compositio Math. **68** (1988), 241-149.