Some parameterizations of rational points on $y^2 = x^n + k$ and related curves

Andrew Bremner (Tempe), Maciej Ulas (Krakow)

$$y^2 = x^n + k,$$

$$y^2 = x(x^n + k),$$

$$y^3 = x^n + k,$$

$$y^3 = x(x^n + k),$$

$$y^m = x^n + k, \; m \geq 4.$$

genus 2: Stoll

The system of equations

$$u_1^2 - A_1T = u_2^2 - A_2T = u_3^2 - A_3T = u_4^2 - A_4T$$

has infinitely many solutions (u_1, u_2, u_3, u_4, T) in the field $\mathbf{Q}(A_1, A_2, A_3, A_4)$.

Proof. The system is equivalent to

$$\frac{u_1^2 - u_2^2}{A_1 - A_2} = \frac{u_2^2 - u_3^2}{A_2 - A_3} = \frac{u_3^2 - u_4^2}{A_3 - A_4} = T,$$

which implies the following equations:

$$\begin{aligned} u_1^2(A_2 - A_3) + u_2^2(A_3 - A_1) &= u_3^2(A_2 - A_1), \\ u_1^2(A_4 - A_2) + u_2^2(A_1 - A_4) &= u_4^2(A_1 - A_2). \end{aligned}$$

In projective space with coordinates u_1, u_2, u_3, u_4 over the field $\mathbf{Q}(A_1, A_2, A_3, A_4)$, we have the intersection of two quadrics, and thus an elliptic curve C since it contains the eight points at $(\pm 1, \pm 1, \pm 1, 1)$.
Specify the origin of the group law to be the point $P_0 = (1, 1, 1, 1)$, and set

$$P_0 = (1,1,1,1), \quad P_1 = (-1,-1,1,1), \quad P_2 = (-1,1,-1,1), \quad P_3 = (1,-1,-1,1),$$

$$P_4 = (1,1,1,-1), \quad P_5 = (1,1,-1,1), \quad P_6 = (1,-1,1,1), \quad P_7 = (-1,1,1,1).$$

Then P_0, P_1, P_2, P_3 are torsion points on C, giving the group $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$; and P_4 is a point of infinite order (with $P_{4+i} = P_4 + P_i$, $i = 1, 2, 3$). We now obtain infinitely many points on C defined over $\mathbf{Q}(A_1, A_2, A_3, A_4)$ by considering multiples of P_4. $\square$

The elliptic curve:

$$u_1^2(A_2 - A_3) + u_2^2(A_3 - A_1) = u_3^2(A_2 - A_1),$$
$$u_1^2(A_4 - A_2) + u_2^2(A_1 - A_4) = u_4^2(A_1 - A_2).$$

has point of infinite order

$$P_4 = (1, 1, 1, -1).$$

The point $2P_4$ corresponds to (u_1, u_2, u_3, u_4) equal to:

$$\begin{aligned}(&-3A_1^2 + 2A_1A_2 + A_2^2 + 2A_1A_3 - 2A_2A_3 + A_3^2 \\ &\qquad + 2A_1A_4 - 2A_2A_4 - 2A_3A_4 + A_4^2, \\ &A_1^2 + 2A_1A_2 - 3A_2^2 - 2A_1A_3 + 2A_2A_3 + A_3^2 \\ &\qquad - 2A_1A_4 + 2A_2A_4 - 2A_3A_4 + A_4^2, \\ &A_1^2 - 2A_1A_2 + A_2^2 + 2A_1A_3 + 2A_2A_3 - 3A_3^2 \\ &\qquad - 2A_1A_4 - 2A_2A_4 + 2A_3A_4 + A_4^2, \\ &A_1^2 - 2A_1A_2 + A_2^2 - 2A_1A_3 - 2A_2A_3 + A_3^2 \\ &\qquad + 2A_1A_4 + 2A_2A_4 + 2A_3A_4 - 3A_4^2),\end{aligned}$$

$$\boxed{y^2 = x^n + k, \quad n \text{ odd}}$$

Set

$$x_i = a_i T, \qquad y_i = u_i T^{\frac{n-1}{2}}$$

giving

$$k/T^{n-1} = u_i^2 - a_i^n T, \qquad i = 1, 2, 3, 4.$$

We deduce the four pairs of points $(x_i, \pm y_i) =$

$$\Big(8a_i(a_1^n + a_2^n - a_3^n - a_4^n)(a_1^n - a_2^n + a_3^n - a_4^n)(a_1^n - a_2^n - a_3^n + a_4^n),$$

$$8^{\frac{n-1}{2}}(a_1^n + a_2^n - a_3^n - a_4^n)^{\frac{n-1}{2}}(a_1^n - a_2^n + a_3^n - a_4^n)^{\frac{n-1}{2}}(a_1^n - a_2^n - a_3^n + a_4^n)^{\frac{n-1}{2}} u_i \Big)$$

where $(u_1, u_2, u_3, u_4) =$

$$\begin{aligned}(&-3a_1^{2n} + 2a_1^n a_2^n + a_2^{2n} + 2a_1^n a_3^n - 2a_2^n a_3^n + a_3^{2n} + 2a_1^n a_4^n - 2a_2^n a_4^n - 2a_3^n a_4^n + a_4^{2n},\\ &a_1^{2n} + 2a_1^n a_2^n - 3a_2^{2n} - 2a_1^n a_3^n + 2a_2^n a_3^n + a_3^{2n} - 2a_1^n a_4^n + 2a_2^n a_4^n - 2a_3^n a_4^n + a_4^{2n},\\ &a_1^{2n} - 2a_1^n a_2^n + a_2^{2n} + 2a_1^n a_3^n + 2a_2^n a_3^n - 3a_3^{2n} - 2a_1^n a_4^n - 2a_2^n a_4^n + 2a_3^n a_4^n + a_4^{2n},\\ &a_1^{2n} - 2a_1^n a_2^n + a_2^{2n} - 2a_1^n a_3^n - 2a_2^n a_3^n + a_3^{2n} + 2a_1^n a_4^n + 2a_2^n a_4^n + 2a_3^n a_4^n - 3a_4^{2n}),\end{aligned}$$

on the curve

$$y^2 = x^n + k,$$

$$k = (8(a_1^n + a_2^n - a_3^n - a_4^n)(a_1^n - a_2^n + a_3^n - a_4^n)(a_1^n - a_2^n - a_3^n + a_4^n))^{n-1} \prod (a_1^{\frac{n}{2}} \pm a_2^{\frac{n}{2}} \pm a_3^{\frac{n}{2}} \pm a_4^{\frac{n}{2}}).$$

Without loss of generality, we may take the parameters a_i to satisfy

$$a_1 > a_2 > a_3 > a_4 > 0,$$

and then can force $k < 0$ by demanding

$$a_2^{\frac{n}{2}} + a_3^{\frac{n}{2}} - a_4^{\frac{n}{2}} \quad < \quad a_1^{\frac{n}{2}} \quad < \quad a_2^{\frac{n}{2}} + a_3^{\frac{n}{2}} + a_4^{\frac{n}{2}}.$$

If we take $(a_1, a_2, a_3, a_4) = (2m+2,\ 2m-2,\ m+1,\ m-1)$, then it is straightforward to check that the above inequality is satisfied for sufficiently large m.

In the case $n = 5$, for example, we require $m \geq 20$, and there results (on removing tenth powers) the curve

$$y^2 = x^5 - k$$

$$k = 2^8 \cdot 3^4 \cdot 11^4 \cdot m^4(m^4 + 10m^2 + 5)^4(128m^{10} - 24665m^8 - 94820m^6 - 106990m^4 - 18580m^2 - 1089),$$

containing the 8 points $(x, \pm y)$:

$$(264m(m \pm 1)(m^4 + 10m^2 + 5),\ 17424m^2(m^4+10m^2+5)^2(64m^5 \pm 165m^4 + 640m^3 \pm 330m^2 + 320m \pm 33)),$$

$$(132m(m \pm 1)(m^4 + 10m^2 + 5),\ 17424m^2(m^4 + 10m^2 + 5)^2(2m^5 \pm 165m^4 + 20m^3 \pm 330m^2 + 10m \pm 33)).$$

Infinitude of points

$$\boxed{y^3 = x^n + k, \qquad (n,3) = 1}$$

Take positive integers α, β, such that

$$n\alpha - 3\beta = 1.$$

Suppose that

$$y_1^3 - x_1^n = y_2^3 - x_2^n = y_3^3 - x_3^n = k,$$

and set

$$x_i = a_i T^\alpha, \qquad y_i = b_i T^\beta, \quad i = 1,2,3.$$

Then

$$b_i^3 - a_i^n T = k/T^{3\beta}, \qquad i = 1,2,3.$$

Now

$$\frac{b_1^3 - b_2^3}{a_1^n - a_2^n} = \frac{b_2^3 - b_3^3}{a_2^n - a_3^n} \quad (= T),$$

so that

$$(a_2^n - a_3^n)b_1^3 + (a_3^n - a_1^n)b_2^3 + (a_1^n - a_2^n)b_3^3 = 0.$$

Set $(a_1, a_2, a_3) = (s^3t^3, t^3r^3, r^3s^3)$. Then this elliptic curve becomes

$$r^{3n}(s^{3n} - t^{3n})b_1^3 + s^{3n}(t^{3n} - r^{3n})b_2^3 + t^{3n}(r^{3n} - s^{3n})b_3^3 = 0,$$

which contains the point

$$(b_1, b_2, b_3) = \left(s^n t^n(-2r^{3n} + s^{3n} + t^{3n}),\ t^n r^n(r^{3n} - 2s^{3n} + t^{3n}),\ r^n s^n(r^{3n} + s^{3n} - 2t^{3n})\right).$$

The corresponding value of T is given by

$$\begin{aligned}
&T = (b_1^3 - b_2^3)/(a_1^n - a_2^n) = \\
&\quad (r^n + s^n + t^n)\cdot \\
&\quad \left(r^{2n} + s^{2n} + t^{2n} - r^n s^n - s^n t^n - t^n r^n\right)\left(r^{2n} + s^{2n} + t^{2n} + 2r^n s^n - s^n t^n - t^n r^n\right)\cdot \\
&\quad \left(r^{2n} + s^{2n} + t^{2n} - r^n s^n + 2s^n t^n - t^n r^n\right)\left(r^{2n} + s^{2n} + t^{2n} - r^n s^n - s^n t^n + 2t^n r^n\right).
\end{aligned}$$

This gives

$$\begin{aligned}
k(r,s,t) &= T^{3\beta}(b_1^3 - a_1^n T) \\
&= -9\,T^{3\beta}\,(rst)^{3n}\,\left(r^{6n} + s^{6n} + t^{6n} - r^{3n}s^{3n} - s^{3n}t^{3n} - t^{3n}r^{3n}\right),
\end{aligned}$$

and we now have the three points

$$(x_i, y_i) = (a_i T^\alpha, b_i T^\beta)$$

(three pairs of points if n even) on the curve $y^3 = x^n + k(r,s,t)$.

$$\boxed{y^3 = x(x^n + k), \qquad n \equiv 2 \bmod 3.}$$

From

$$\frac{y_1^3 - u^{n+1}}{u} = \frac{y_2^3 - v^{n+1}}{v} \; (= k)$$

results

$$vy_1^3 - uy_2^3 = vu^{n+1} - uv^{n+1}.$$

The only obvious point is $(y_1, y_2) = (u^{\frac{n+1}{3}}, v^{\frac{n+1}{3}})$ which we take as zero point, and obtain an elliptic curve with Weierstrass cubic model

$$Y^2 = X^3 - 432u^4v^4(u^n - v^n)^2.$$

This curve possesses a point of infinite order, namely

$$(X, Y) = \left(\frac{4(u^{2n} - u^n v^n + v^{2n})}{(uv)^{\frac{2}{3}(n-2)}}, \frac{4(u^n + v^n)(u^n - 2v^n)(2u^n - v^n)}{(uv)^{n-2}} \right),$$

which corresponds to

$$y_1 = \frac{u^{\frac{n+1}{3}}(u^n - 2v^n)(u^{4n} + 10u^{3n}v^n - 12u^{2n}v^{2n} + 4u^n v^{3n} - 2v^{4n})}{(u^n + v^n)(u^{4n} - 14u^{3n}v^n + 24u^{2n}v^{2n} - 14u^n v^{3n} + v^{4n})},$$

$$y_2 = \frac{v^{\frac{n+1}{3}}(2u^n - v^n)(2u^{4n} - 4u^{3n}v^n + 12u^{2n}v^{2n} - 10u^n v^{3n} - v^{4n})}{(u^n + v^n)(u^{4n} - 14u^{3n}v^n + 24u^{2n}v^{2n} - 14u^n v^{3n} + v^{4n})}.$$

We now deduce

$$
\begin{aligned}
k =& 9u^n v^n (u^{2n} - u^n v^n + v^{2n})(u^{4n} - 5u^{3n}v^n + 15u^{2n}v^{2n} - 5u^n v^{3n} + v^{4n}) \\
& (7u^{4n} - 14u^{3n}v^n + 6u^{2n}v^{2n} + u^n v^{3n} + v^{4n})(u^{4n} + u^{3n}v^n + 6u^{2n}v^{2n} - \\
& 14u^n v^{3n} + 7v^{4n}) / \big((u^n + v^n)(u^{4n} - 14u^{3n}v^n + 24u^{2n}v^{2n} - 14u^n v^{3n} + v^{4n})\big)^3
\end{aligned}
$$

and the curve $y^3 = x(x^n + k)$ has point at $(0, 0)$ together with the two points (two pairs of points if n even) at $(x, y) = (u, y_1)$, (v, y_2).

$$\boxed{y^m = x^n + k,\ m \geq 4.}$$

In the case that $(m, n) = 1$, then we may apply previous arguments to obtain the following Theorem.

There exist infinitely many curves as in the title, $(m, n) = 1$, with at least two finite rational points (four, if m or n is even).

Similarly, we may treat $y^m = x(x^n + k)$ and obtain infinitely many k for which the curve has at least two points.

In the instance that m, n are not coprime, it is difficult to make much progress. We restrict attention to the following case.

Let N be a fixed odd integer. Then there exist infinitely many curves

$$y^4 = x^{2N} + k$$

with at least two quadruples $(\pm x, \pm y)$ of finite rational points.