A DIOPHANTINE EQUATION ASSOCIATED TO $X_0(5)$

IMIN CHEN

Abstract. Several classes of Fermat type diophantine equations have been successfully resolved using the method of galois representations and modularity. In each case, it is possible to view the proper solutions to the diophantine equation in question as corresponding to suitably defined integral points on a modular curve of level divisible by 2 or 3. Motivated by this point of view, we discuss an example of a diophantine equation associated to the modular curve $X_0(5)$. The diophantine equation has four terms rather than the usual three terms characteristic of generalized Fermat equations.

1. Introduction

A solution $(a, b, c) \in \mathbb{Z}^3$ to an integer coefficient polynomial diophantine equation in three variables is said to be proper if $(a, b, c) = 1$. Several classes of Fermat type diophantine equations have been successfully resolved using the method of galois representations and modularity. In each case, it is possible to view the proper solutions to the diophantine equation in question as corresponding to suitably defined integral points on a modular curve of level divisible by 2 or 3 [4]. Motivated by this point of view, we discuss an example of a diophantine equation associated to the modular curve $X_0(5)$.

Theorem 1. *Let $p > 7$ be a prime and suppose $(r, x, y) \in \mathbb{Z}^3$ is a proper solution to*

$$x^{2p} + 22x^p y^p + 125y^{2p} = r^2.$$

Date: 1 October 2004.

1991 *Mathematics Subject Classification.* Primary: 11G05, Secondary: 14G05.

Research supported by NSERC.

Then $y = 0$.

2. Diophantine equations attached to families of elliptic curves

Proposition 2. *Let A be an integral domain with field of fractions K. Let $P, Q \in A[S,T]$ be polynomials and let $R = P - 1728Q$. Write $P = P_0^3 P_1$ and $R = R_0^2 R_1$ where $P_0, R_0 \in A[S,T]$. Suppose that $s, t, \alpha, \beta \in A$ satisfy*

$$P_1(s,t) = \alpha^3$$

$$R_1(s,t) = \beta^2.$$

Then the elliptic curve

$$Y^2 = X^3 - 3P_0(s,t)\alpha X + 2R_0(s,t)\beta$$

has j-invariant $j = P(s,t)/Q(s,t)$ and discriminant $\Delta = 12^6 Q(s,t)$.

Proof. Let $u = P(s,t) = (P_0(s,t)\alpha)^3 = a^3$, $v = Q(s,t)$, $u - 1728v = (R_0(s,t)\beta)^2 = b^2$. The elliptic curve

$$\begin{aligned} Y^2 &= X^3 - 3aX + 2b \\ &= X^3 - 3P_0(s,t)\alpha X + 2R_0(s,t)\beta \end{aligned}$$

over K has j-invariant $j = u/v = P(s,t)/Q(s,t)$ and discriminant $\Delta = 12^6 v = 12^6 Q(s,t)$ using standard formulae. □

3. The diophantine equation associated to $X_0(5)$

Let $P(S,T) = (S^2 + 250ST + 3125T^2)^3, Q(S,T) = S^5 T \in \mathbb{Z}[S,T]$. Elliptic curves over $\mathbb{Q}$ with j-invariants of the form $P(s,t)/Q(s,t)$ where $s,t \in \mathbb{Z}$ correspond to elliptic curves over $\mathbb{Q}$ with a 5-isogeny over $\mathbb{Q}$. For lack of better of reference, we refer to [3] where this parametrization of the modular curve $X_0(5)$ is given.

For non-zero $a, d \in \mathbb{Z}$, let $\mathrm{Rad}_d(a)$ be the product of primes dividing a but not d, and $\mathrm{Sup}_d(a)$ be the largest positive divisor of a coprime to d. For a prime q, let $v_q : \mathbb{Z} \to \mathbb{Z}$ denote the valuation associated to q.

Proposition 3. *Suppose* $(s,t,r) \in \mathbb{Z}^3$ *is a proper solution to the equation*

$$s^2 + 22st + 125t^2 = r^2$$

where $t \neq 0$. *Then there exists an elliptic curve* $E_{(r,s,t)}$ *over* $\mathbb{Q}$ *with* j*-invariant* $P(s,t)/Q(s,t)$, *conductor* $N = 2^a \cdot 3^b \cdot 5^c \cdot \mathrm{Rad}_{30}(s^5 t)$ *with* $a \in \{0,4\}$, $b \in \{0,1\}$, $c \in \{0,1,2\}$, *and discriminant* Δ *satisfying* $\mathrm{Sup}_{30}(\Delta) = \mathrm{Sup}_{30}(s^5 t)$. *Furthermore, the case* $c = 2$ *happens only if* $v_5(s) = 2, 3$.

Proof. Suppose that $(r,s,t) \in \mathbb{Z}^3$ is a proper solution to

$$s^2 + 22st + 125t^2 = r^2$$

where $t \neq 0$. Then $P(s,t) = (s^2 + 250st + 3125t^2)^3$, $R(s,t) = P(s,t) - 12^3 Q(s,t) = (s^2 - 500st - 15625t^2)^2 (s^2 + 22st + 125t^2) = ((s^2 - 500st - 15625t^2)r)^2$. By Proposition 2, the elliptic curve E over $\mathbb{Q}$ given by

$$\begin{aligned} Y^2 &= X^3 - 3 \cdot (s^2 + 250st + 3125t^2)X + 2 \cdot (s^2 - 500st - 15625t^2)r \\ &= X^3 + a_4 X + a_6 \end{aligned} \tag{1}$$

has j-invariant $j = P(s,t)/Q(s,t)$ and this model has discriminant $\Delta = 2^{12} 3^6 s^5 t$.

Since the invariant c_4 of model (1) is given by $c_4 = 144(s^2 + 250st + 3125t^2)$, we have that $v_2(c_4) \geq 4$. If $v_2(c_4) > 4$, then $s^2 + 250st + 3125t^2 \equiv 0 \pmod 2$. Now, $s^2 + 250st + 3125t^2 \equiv s^2 + 22st + 125t^2 \pmod 4$ so since $s^2 + 22st + 125t^2 = r^2$, in fact we have that $s^2 + 250st + 3125t^2 \equiv 0 \pmod 4$. If $s^2 + 250st + 3125t^2 \equiv 0 \pmod 4$ and $s^2 + 22st + 125t^2$ is a square modulo 16, then in fact $s^2 + 250st + 3125t^2 \equiv 0 \pmod{16}$. Hence, we conclude that either $v_2(c_4) = 4$ or $v_2(c_4) \geq 8$. Also, $s^2 + 250st + 3125t^2 \equiv (s+t)^2 \pmod 2$ so $s \equiv t \equiv 1 \pmod 2$. Since $\Delta = 2^{12} 3^6 s^5 t$, we have that $v_2(\Delta) = 12$. By Tableau IV in [7], $v_2(N) = 4$ unless $v_2(c_4) \geq 8$ and model (1) is not minimal (we note in some of the scanned electronic versions of [7] from the publisher, the rightmost columns in the Tableaux are missing). If model (1) is not minimal, a change of variables gives a model with good reduction modulo 2 so $v_2(N) = 0$.

Replacing X by $X+r$ in model (1) yields the model

$$Y^2 = X^3 + 3rX^2 + 3(r^2 - s^2 - 250st - 3125t^2)X$$
$$+ r(r^2 - s^2 - 1750st - 40625t^2).$$

Note that $s^2+250st+3125t^2 \equiv s^2+22st+125t^2 \pmod 3$, and $s^2+1750st+40625t^2 \equiv s^2+22st+125t^2 \pmod{27}$. Replacing X by $3X$, Y by $\sqrt{27}Y$, and dividing by 27 yields the model of a twist of the elliptic curve given by (1). The invariant $c_4 = s^2+250st+3125t^2$ of this twisted model satisfies $v_3(c_4) = 0$. By Tableau II in [7], we have that $v_3(N) = 0, 1$ for this twist.

If $c_4 = 144(s^2+250st+3125t^2) \equiv 0 \pmod 5$, then $s \equiv 0 \pmod 5$. Hence, if $s \not\equiv 0 \pmod 5$, then $c_4 \not\equiv 0 \pmod 5$. By Tableau I in [7], we have that $v_5(N) = 0, 1$. Suppose now that $s \equiv 0 \pmod 5$. Using the equation $s^2+22st+125t^2 = r^2$ and properness of $(r,s,t) \in \mathbb{Z}^3$, we deduce that $v_5(s) = 2, 3$.

Suppose that $q \neq 2, 3, 5$. The elliptic curve associated to model (1) has additive bad reduction modulo q only if model (1) has cuspidal reduction modulo q with the cusp being $(0,0)$. This occurs only if both $d_4 \equiv 0 \pmod q$ and $d_6 \equiv 0 \pmod q$ and hence only if $s^2+250st+3125t^2 \equiv 0 \pmod q$ and either $s^2-500st-15625t^2 \equiv 0 \pmod q$ or $r^2 = s^2+22st+125t^2 \equiv 0 \pmod q$. This happens only if $q = 2, 3, 5$ or $s \equiv t \equiv 0 \pmod q$, a fact which can be verified by equating the roots of the corresponding inhomogenous quadratic polynomials and squaring successively, or directly by using resultants. The latter case is not possible since $(r,s,t) \in \mathbb{Z}^3$ is a proper solution to $s^2+22st+125t^2 = r^2$. The former case is not possible as we are assuming $q \neq 2, 3, 5$. We conclude therefore that $v_q(N) = 0, 1$. □

We remark that a proper solution $r, s, t \in \mathbb{Z}^3$ to $s^2+22st+125t^2 = r^2$ gives rise to a solution $(\alpha, \beta, t) \in \mathbb{Z}^3$ to $\alpha^3 - 1728t = \beta^2$ as the construction of the elliptic curve $E_{(r,s,t)}$ goes through Proposition 2. However, this solution may not be proper and so it seems necessary to perform Tate's algorithm on specifically on $E_{(r,s,t)}$ rather than the more general elliptic curve $Y^2 = X^3 - 3\alpha X + 2\beta$.

The above proposition allows us to invoke the machinery of galois representations and modular forms to establish Theorem 1.

Proof of Theorem 1. Suppose $(r, x, y) \in \mathbb{Z}^3$ is a proper solution to $x^{2p} + 22x^p y^p + 125y^{2p} = r^2$ where $y \neq 0$. Let $E = E_{(r,s,t)}$ be the elliptic curve over $\mathbb{Q}$ associated to $(r, s, t) = (r, x^p, y^p)$ satisfying $s^2 + 22st + 125t^2 = r^2$ as given by Proposition 3.

The elliptic curve E has conductor $N = 2^a \cdot 3^b \cdot 5^c \cdot \mathrm{Rad}_{30}(s^5 t)$ where $a \in \{0, 4\}$, $b \in \{0, 1\}$, $c \in \{0, 1, 2\}$. By the proof of Proposition 3, case $c = 2$ only occurs if $v_5(s) = 2, 3$. Since s is a p-th power where $p > 7$, this case does not arise and so in fact $c \in \{0, 1\}$.

Since $p > 7$, $\rho_{E,p}$ is irreducible by [6]. More precisely, E must have at least one odd prime of multiplicative reduction or else E has conductor 2^a, which is not possible as there are no elliptic curves over $\mathbb{Q}$ with this conductor. By Corollary 4.4 in [6], it follows that $p = 2, 3, 5, 7, 13$. On the other hand, $X_0(65)$ has no non-cuspidal rational points [5] so the case $p = 13$ cannot occur as E would give rise to such a point.

The discriminant Δ of E satisfies $\mathrm{Sup}_{30}(\Delta) = \mathrm{Sup}_{30}(s^5 t) = \mathrm{Sup}_{30}(x^{5p} y^p)$. By modularity of E [2], $\rho_{E,p} \cong \rho_{f,p}$ for a weight 2 newform f on $\Gamma_0(N)$. Since $v_q(\Delta) \equiv 0 \pmod p$ for $q \neq 2, 3, 5$, $\rho_{E,p}$ is unramified at $q \neq 2, 3, 5, p$ and flat at $q = p$. By level lowering [8], $\rho_{E,p} \cong \rho_{g,p}$ for a weight 2 newform g on $\Gamma_0(M)$ where $M = 2^a \cdot 3^b \cdot 5^c$.

A computation in MAGMA [1] reveals that there are no elliptic curves over $\mathbb{Q}$ possessing a 5-isogeny over $\mathbb{Q}$ of conductor $M = 2^a \cdot 3^b \cdot 5^c$ with $a \in \{0, 4\}$, $b \in \{0, 1\}$, $c \in \{0, 1\}$. This allows us to show that $p = 2, 3, 5, 7$ in the following manner, contradicting the assumption that $p > 7$.

If $q \neq 2, 3$, then E either has multiplication or good reduction modulo q. In the former case, $\mathrm{tr}\, \rho_{E,p}(\mathrm{Frob}_q) = \pm(q + 1)$. In the latter case, we note that since E has a 5-isogeny defined over $\mathbb{Q}$, there is an extension $L \mid \mathbb{Q}$ of degree ≤ 4 such that $E(L)$ has a point of order 5. Let $\mathfrak{q}$ be a prime ideal of the ring of integers $\mathcal{O}_L$ of L which lies over the prime ideal $q\mathbb{Z}$ of $\mathbb{Z}$. Let r be the degree of $\mathcal{O}_L/\mathfrak{q} \cong \mathbb{F}_{q^r}$ over $\mathbb{Z}/q\mathbb{Z} \cong \mathbb{F}_q$. It follows that $|E(\mathbb{F}_{q^r})|$ is divisible by 5 for some $r \mid 4$.

Recall that g is a weight 2 newform on $\Gamma_0(M)$ where $M = 2^a \cdot 3^b \cdot 5^c$ and $a \in \{0, 4\}$, $b \in \{0, 1\}$, $c \in \{0, 1\}$. By a computation in MAGMA [1], there are 8 possibilities for g and all of them have rational fourier coefficients. Let F be the elliptic curve over $\mathbb{Q}$ attached to the newform g so that $\rho_{g,p} \cong \rho_{F,p}$ and $a_q(g) = a_q(F)$.

For each of the 8 possibilities for g and its associated F, we determine a set of primes $q \neq 2, 3, 5, p$ such that $|F(\mathbb{F}_{q^r})|$ is not divisible by 5 for all $r \mid 4$. If E has good reduction modulo q, then $a_q(E) \neq a_q(F)$, for if $a_q(E) = a_q(F)$, then $|E(\mathbb{F}_{q^r})| = |F(\mathbb{F}_{q^r})|$ for all $r \geq 1$, contradicting the fact noted above. If E has multiplicative reduction modulo q, then $a_q(F) \pm (q + 1) \neq 0$ by Hasse's bound. Since $\rho_{E,p} \cong \rho_{F,p}$ it follows that $\operatorname{tr} \rho_{E,p}(\mathrm{Frob}_q) = \operatorname{tr} \rho_{F,p}(\mathrm{Frob}_q)$. Hence, either $p \mid a_q(E) - a_q(F)$ or $a_q(F) \pm (q + 1)$. Together with the fact that $|a_q(E)| < 2\sqrt{q}$, the desired constraint $p = 2, 3, 5, 7$ can be obtained.

The above verification can be separated into two cases:

(a) $p = 11$ or $p \geq 17$
(b) $p = 13$.

Table 1 and Table 2 give a list of $a_q(F)$ and $|F(\mathbb{F}_{q^r})|$, respectively, for each possible F and $2 \leq q \leq 41$, as computed by MAGMA [1]. In case (a), we have chosen a prime q for each F so that $|F(\mathbb{F}_{q^r})|$ is not divisible by 5 for $r \mid 4$. The corresponding entries in Table 2 have been boxed. For the column corresponding to the same q, the entry $a_q(F)$ in Table 1 is also boxed. From this, one can easily verify that the constraint $p = 2, 3, 5, 7$ is obtained as described above.

For case (b), a bit more work is necessary. For each F, we choose three q's so that $|F(\mathbb{F}_{q^r})|$ is not divisible by 5 for $r \mid 4$. The corresponding entries in Table 2 are in bold face. For the column corresponding to the same q's, the entries for $a_q(F)$ in Table 1 are also in bold face. From this, it can be verified that $p = 2, 3, 5, 7$ by simultaneously using the constraints imposed by all three primes. □

Table 1. Table of $a_q(F)$

Label	2	3	5	7	11	13	17	19	23	29	31	37	41
15 : 1	−1	∗	∗	$\boxed{\mathbf{0}}$	**−4**	−2	2	4	**0**	−2	0	−10	10
48 : 1	∗	∗	−2	$\boxed{\mathbf{0}}$	**−4**	−2	2	4	**8**	6	−8	6	−6
80 : 1	∗	0	∗	$\boxed{\mathbf{4}}$	**−4**	−2	2	−4	−4	**−2**	8	6	−6
80 : 2	∗	2	∗	−2	0	$\boxed{2}$	**−6**	4	−6	6	**4**	2	**6**
240 : 1	∗	∗	∗	$\boxed{\mathbf{0}}$	**4**	6	**−6**	4	0	−2	8	−2	−6
240 : 2	∗	∗	∗	$\boxed{\mathbf{4}}$	0	2	**6**	4	**0**	−6	−8	2	−6
240 : 3	∗	∗	∗	$\boxed{\mathbf{-4}}$	0	−6	−2	−4	**8**	−6	0	**−6**	10
240 : 4	∗	∗	∗	$\boxed{\mathbf{0}}$	**4**	−2	2	−4	**0**	−2	0	−10	10

4. Acknowledgements

I would like to thank M. Bennett for discussions which led to the topics considered in this paper.

References

[1] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system. I. The user language. Computational algebra and number theory (London, 1993). *J. Symbolic Comput.*, 24(3-4):235–265, 1997.

[2] C. Breuil, B. Conrad, F. Diamond, and R. Taylor. Modularity of elliptic curves over Q: wild 3-adic exercises. *Journal of the American Mathematical Society*, 14(4):843–939, 2001.

[3] I. Chen and N. Yui. Singular values of Thompson series. In *Groups, Difference sets, and the Monster (Columbus, OH, 1993)*, volume 4 of *Ohio State University Mathematics Research Institute Publications*, pages 255–326. De Gruyter, Berlin, 1996.

[4] H. Darmon. Faltings plus epsilon, Wiles plus epsilon, and the generalized Fermat equation. *C.R. Math. Rep. Acad. Sci. Canada*, 19(1):2–14, 1997.

[5] M.A. Kenku. The modular curves $X_0(65)$ and $X_0(91)$ and rational isogeny. *Math. Proc. Cambridge Philos. Soc.*, 87:15–20, 1980.

TABLE 2. Table of $|F(\mathbb{F}_{q^r})|$

Label	r	2	3	5	7	11	13	17	19	23	29	31	37	41
15 : 1	1	4	*	*	**8**	**16**	16	16	16	**24**	32	32	48	32
	2	8	*	*	**64**	**128**	192	320	384	**576**	896	1024	1344	1664
	4	16	*	*	**2304**	**14848**	28416	83200	130560	**278784**	706048	921600	1876224	2828800
48 : 1	1	*	*	8	**8**	**16**	16	16	16	**16**	24	40	32	48
	2	*	*	32	**64**	**128**	192	320	384	**512**	864	960	1408	1728
	4	*	*	640	**2304**	**14848**	28416	83200	130560	**280576**	708480	925440	1875456	2827008
80 : 1	1	*	4	*	**4**	**16**	16	16	24	28	**32**	24	32	48
	2	*	16	*	**48**	**128**	192	320	384	560	**896**	960	1408	1728
	4	*	64	*	**2496**	**14848**	28416	83200	130560	280000	**706048**	925440	1875456	2827008
80 : 2	1	*	2	*	10	12	12	**24**	16	30	24	**28**	36	**36**
	2	*	12	*	60	144	192	**288**	384	540	864	**1008**	1440	**1728**
	4	*	96	*	2400	14400	28416	**84096**	130560	280800	708480	**923328**	1872000	**2827008**
240 : 1	1	*	*	*	**8**	**8**	8	**24**	16	24	32	24	40	48
	2	*	*	*	**64**	**128**	160	**288**	384	576	896	960	1440	1728
	4	*	*	*	**2304**	**14848**	28800	**84096**	130560	278784	706048	925440	1872000	2827008
240 : 2	1	*	*	*	**4**	12	12	**12**	16	**24**	36	40	36	48
	2	*	*	*	**48**	144	192	**288**	384	**576**	864	960	1440	1728
	4	*	*	*	**2496**	14400	28416	**84096**	130560	**278784**	708480	925440	1872000	2827008
240 : 3	1	*	*	*	**12**	12	20	20	24	**16**	36	32	**44**	32
	2	*	*	*	**48**	144	160	320	384	**512**	864	1024	**1408**	1664
	4	*	*	*	**2496**	14400	28800	83200	130560	**280576**	708480	921600	**1875456**	2828800
240 : 4	1	*	*	*	**8**	**8**	16	16	24	**24**	32	32	48	32
	2	*	*	*	**64**	**128**	192	320	384	**576**	896	1024	1344	1664
	3	*	*	*	**2304**	**14848**	28416	83200	130560	**278784**	706048	921600	1876224	2828800

[6] B. Mazur. Rational isogenies of prime degree. *Inventiones Mathematicae*, 44:129–162, 1978.

[7] I. Papadopoulos. Sur la classification de Néron des courbes elliptiques en caractéristique résiduelle 2 et 3. *Journal of Number Theory*, 44:119–152, 1993.

[8] K. Ribet. On modular representations of $\mathrm{Gal}(\overline{\mathbb{Q}} \mid \mathbb{Q})$ arising from modular forms. *Inventiones Mathematicae*, 100:431–476, 1990.