

Supplement to NU-CONFIGURATIONS IN TILING THE SQUARE

ANDREW BREMNER AND RICHARD K. GUY

6. Lemmas restricting the rank in specific cases

Although the generic rank of (7) is zero, the rank of the specialized curve, when m and n are given numerical values, is often positive. We obtain arithmetic information about the rank in the manner of §4 of [1]. To make the dependence on m, n more explicit, we introduce some notation and note some congruences which will be useful in the sequel. Write

$$K = m^2 - 2mn - n^2 = (m - n)^2 - 2n^2,$$

$$L = K^2 + 8m^2n^2 = m^4 - 4m^3n + 10m^2n^2 + 4mn^3 + n^4,$$

$$M = K^2 + 16m^2n^2 = m^4 - 4m^3n + 18m^2n^2 + 4mn^3 + n^4,$$

so that $\kappa = K^2/4m^2n^2$, $\kappa^2 + 2 = L/4m^2n^2$, $\kappa^2 + 4 = M/4m^2n^2$. We may take $m \perp n$, so that $K \perp mn$, $L \perp mn$, $M \perp mn$, and

Fact (a) If m, n are of opposite parity, then $K \equiv \pm 1 \pmod{8}$, and each of K^2 , L , and M is congruent to 1 mod 16.

Fact (b) If m, n are both odd, then $K \equiv 2 \pmod{4}$, and $K^2 \equiv 4$, $L \equiv 12$, and $M \equiv 20 \pmod{32}$.

Fact (c) Each odd prime factor of K is congruent to $\pm 1 \pmod{8}$.

Fact (d) Each odd prime factor of M (the sum of two squares) is congruent to 1 mod 4.

We also change the scale, replacing $(4m^2n^2\sigma, 8m^3n^3\tau)$ by (σ, τ) , so that (7), which is

$$64m^6n^6\tau^2 = 4m^2n^2\sigma(16m^4n^4\sigma^2 + L \cdot 4m^2n^2\sigma + 16m^4n^4),$$

becomes

$$\tau^2 = \sigma(\sigma^2 + L\sigma + 16m^4n^4); \tag{19}$$

and replace $(4m^2n^2S, 8m^3n^3T)$ by (S, T) , so that (8), namely

$$64m^6n^6T^2 = 4m^2n^2S(4m^2n^2S - K^2)(4m^2n^2S - M),$$

becomes

$$T^2 = S(S - K^2)(S - M). \tag{20}$$

In (19) we substitute $\sigma = \delta a^2/b^2$, $\tau = \delta ac/b^3$, with $\delta, a, b, c \in \mathbf{Z}$, δ squarefree, $a \perp b$ and $a, b, c \geq 0$, and obtain

$$\delta c^2 = \delta^2 a^4 + L\delta a^2 b^2 + 16m^4 n^4 b^4, \tag{21}$$

and, in (20), substitute $S = \Delta A^2/B^2$, $T = \Delta AC/B^3$ with corresponding conditions on Δ, A, B, C , yielding

$$\Delta C^2 = (\Delta A^2 - K^2 B^2)(\Delta A^2 - MB^2). \quad (22)$$

From (21), $\delta \mid 16m^4n^4$, and, because δ is squarefree, $\delta \mid 2mn$. We have already noted the global solutions $\delta = 1, (a, b, c) = (1, 0, 1)$ and $\delta = -1, (a, b, c) = (2mn, 1, 2mnK)$, where $K = m^2 - 2mn - n^2$, so we only need to seek solutions with $\delta > 1$. See also Lemmas 12 and 13 in §10. Lemmas 1 to 3 concern δ : Lemma 3 refers to the case where m, n are both odd.

Lemma 1. *If an odd prime p divides $M = m^4 - 4m^3n + 18m^2n^2 + 4mn^3 + n^4$, and the Legendre symbol $(\delta|p) = -1$, then (21) has no nontrivial solutions.*

Proof. We may write (21) as

$$(2\delta a^2 + Lb^2)^2 - K^2 M b^4 = 4\delta c^2,$$

so that

$$(2\delta a^2 + Lb^2)^2 \equiv 4\delta c^2 \pmod{p},$$

whereupon $(\delta|p) = -1$ implies that $2\delta a^2 + Lb^2 \equiv 0 \equiv 2c \pmod{p}$, and since $L = M - 8m^2n^2$, we have

$$2\delta a^2 - 8m^2n^2b^2 \equiv 0 \pmod{p}.$$

Again, $(\delta|p) = -1$ implies that $a \equiv 0 \equiv 2mnb \pmod{p}$. Now p odd, $M \perp mn$ and $p \mid M$ imply that $p \mid b$, and $a \equiv 0 \equiv b \pmod{p}$ contradicts $a \perp b$. \square

Lemma 2. *If a prime $p \equiv 1 \pmod{8}$ divides $K = m^2 - 2mn - n^2$, and $(\delta|p) = -1$, then (21) has no nontrivial solutions.*

Proof. As in Lemma 1, $2\delta a^2 + Lb^2 \equiv 0 \pmod{p}$, and since $p \mid K^2$ and $L = K^2 + 8m^2n^2$, $2\delta a^2 + 8m^2n^2b^2 \equiv 0 \pmod{p}$,

$$-6a^2 \equiv (2mntb)^2 \pmod{p}.$$

As before, $p \mid 2mn$, and $a \equiv 0 \equiv b \pmod{p}$ is not permitted, so $(-\delta|p) = -1, (-1|p) = -1, p \equiv 3 \pmod{4}$, contradicting Fact (c) above. \square

Lemma 3. *If m, n are both odd, so is δ .*

Proof. By Fact (b), $L \equiv 12 \pmod{32}$, and (21) gives

$$\delta c^2 \equiv \delta^2 a^4 + 12\delta a^2 b^2 + 16b^4 \pmod{32}.$$

If a is odd, then $\delta c^2 \equiv \delta^2 \pmod{4}$, and $2b$ would imply $2|c, 2^2|c^2$ and $4|\delta$, contradicting δ squarefree. If $2|a$, then b is odd, $b^2 \equiv 1 \pmod{8}$, $\delta c^2 \equiv 16(\delta^2 + 3b^2 + 1) \pmod{32}$, which implies $8|c^2, 16|c^2, \delta \equiv \delta^2 + 3b^2 + 1 \pmod{2}$, and δ odd. If $4|a$, then b is odd, $\delta c^2 \equiv 16 \pmod{32, 8|c^2, 16|c^2}$, and δ odd. \square

From (22), $\Delta \mid K^2 M$, and, because Δ is squarefree, $\Delta \mid KM$. We have noted the global solutions $\Delta = 1, (A, B, C) = (1, 0, 1)$ or $(K, 1, 0)$ and $\Delta = M, (A, B, C) = (1, 1, 0)$ or $(0, -1, K)$, corresponding to the points $(S, T) = \infty, (K^2, 0), (M, 0)$ and $(0, 0)$ on the curve (20). See also Lemmas 14 and 15 in §10. Lemmas 4 to 7 concern Δ : Lemma 7 refers to the case with m and n of opposite parity.

Lemma 4. Δ is positive and odd.

Proof. If Δ were negative, the left side of (22) would be negative, and the right side positive. If $m + n \equiv 1 \pmod{2}$, Fact (a) states that M is odd, so that Δ , which divides MK , is odd. If $m \equiv n \equiv 1 \pmod{2}$, Fact (b) states that $K^2 \equiv 4$ and $M \equiv 20 \pmod{32}$, and (22) gives

$$\Delta C^2 \equiv (\Delta A^2 - 4B^2)(\Delta A^2 - 20B^2) \pmod{32}.$$

If Δ were even, $2 \parallel \Delta$, since it is squarefree; 2^2 divides the right side of (22); $2|C$; 8 divides the left side of (22); 4 divides at least one factor on the right; $2|A; 2 \mid B$; since $A \perp B$; 4 exactly divides each factor on the right of (22), whereas an odd power of 2 exactly divides the left, a contradiction. So Δ is odd. \square

Lemma 5. *If P is an odd prime divisor of m or n , and $(\Delta|P) = -1$, then (22) has no nontrivial solution.*

Proof. We may write (22) as

$$(\Delta A^2 - LB^2)^2 - 64m^4n^4 = \Delta C^2,$$

so that

$$(\Delta A^2 - LB^2)^2 \equiv \Delta C^2 \pmod{P}$$

and $(\Delta|P) = -1$ now implies that $\Delta A^2 - LB^2 \equiv 0 \equiv C \pmod{P}$. Since $P \mid m$ or n , $\Delta A^2 \equiv m^4 B^2$ or $n^4 B^2 \pmod{P}$. But now $(\Delta|P) = -1$ implies that $A \equiv 0 \equiv B \pmod{P}$ in either case, contradicting $A \perp B$. \square

Lemma 6. *Write $\Delta = D_1 D_2$, where $D_1 \mid K = m^2 - 2mn - n^2$, and $D_2 \mid M = m^4 - 4m^3n + 18m^2n^2 + 4mn^3 + n^4$, then every prime factor of D_1 is congruent to $1 \pmod{8}$, and every prime factor of D_2 is congruent to $1 \pmod{4}$.*

Proof. As $\Delta \mid KM$, it is legitimate to write Δ in this way. By Lemma 4, D_1 and D_2 are odd. By Fact (d), the prime factors of D_2 are congruent to 1 mod 4. Let P be a prime which divides D_1 . Then $P \parallel D_1$, because D_1 is squarefree. Moreover, $P \mid K$, so, by Fact (c), $P \equiv \pm 1 \pmod 8$. Suppose $P^2 \parallel K$. From (22),

$$C^2 = \left(D_2 A^2 - \frac{K^2 B^2}{D_1} \right) \left(D_1 A^2 - \frac{M B^2}{D_2} \right), \quad (23)$$

$$C^2 \equiv -M A^2 B^2 \equiv -16m^2 n^2 A^2 B^2 \pmod P.$$

If $P \equiv -1 \pmod 8$, then $C \equiv 0 \pmod{AB \pmod P}$. Suppose first that $C \equiv 0 \pmod A \pmod P$, so that $B \not\equiv 0 \pmod P$. We claim that $C \equiv 0 \pmod A \pmod{P^k}$. To see this, suppose, inductively, that $C \equiv 0 \pmod A \pmod{P^k}$ for some $k \leq \alpha - 1$ (true for $k = 1$), and let $C = P^k C_1, A = P^k A_1$. Then (23) is

$$P^{2k} C_1^2 = \left(D_2 P^{2k} A_1^2 - \frac{K^2}{D_1} B^2 \right) \left(D_1 P^{2k} A_1^2 - \frac{M}{D_2} B^2 \right),$$

where $P^{2\alpha-1}$ divides K^2/D_1 and $2\alpha - 1 \geq 2k + 1$, so that

$$P^{2k} C_1^2 \equiv -P^{2k} M A_1^2 B^2 \pmod{P^{2k+1}},$$

$$C_1^2 \equiv -16m^2 n^2 A_1^2 B^2 \pmod P,$$

$$C_1 \equiv 0 \pmod{A_1 \pmod P},$$

$$C \equiv 0 \pmod A \pmod{P^{k+1}}$$

and, by induction, $C \equiv 0 \pmod A \pmod{P^\alpha}$. So

$$0 \equiv \frac{K^2 B^2}{D_1} B^2 \pmod{P^{2\alpha}}$$

and $0 \equiv B \pmod P$, a contradiction. Suppose second that $C \equiv 0 \pmod B \pmod P$. Then $P \mid A$, since $A \perp B$, and $P \nmid D_2$, since we are still assuming that $P \equiv -1 \pmod 8$. Then P^2 divides the left side of (23), while P does not divide the first factor on the right, and P exactly divides the second factor, again a contradiction. So every prime divisor of D_1 is congruent to 1 mod 8. \square

Lemma 7. *If m, n are of opposite parity, then $\Delta \equiv 1 \pmod 8$.*

Proof. From Lemma 6, $\Delta \equiv D_1 D_2$, where $D_1 \equiv 1 \pmod 8$, and $D_2 \equiv 1 \pmod 4$. We need to show that $D_2 \not\equiv 5 \pmod 8$. Note that D_2 may contain factors congruent to 5 mod 8, but there will always be an even number of them. Suppose $\Delta \equiv 5 \pmod 8$. Then Fact (a) with (22) gives

$$5C^2 \equiv (5A^2 - B^2)^2 \pmod 8,$$

$$C \equiv 0 \equiv 5A^2 - B^2 \pmod 8.$$

Now $A \perp B$ implies $A \equiv B \equiv 1 \pmod 2$, so that Fact (a) gives

$$\Delta A^2 - K^2 B^2 \equiv 4 \equiv \Delta A^2 - MB^2 \pmod 8,$$

and (22) now gives $\Delta C^2 \equiv 16 \pmod{32}$, so that $C \equiv 4 \pmod 8$. But (22) may also be written

$$\Delta C^2 = (\Delta A^2 - LB^2)^2 - 64m^4 n^4 B^4$$

where $\Delta A^2 - LB^2 \equiv 4 \pmod 8$, so that $\Delta C^2 \equiv 16 \pmod{128}$, contradicting $\Delta C^2 \equiv 80 \pmod{128}$. So $\Delta \equiv 1 \pmod 8$. \square

We will use these lemmas in §10 to restrict the numbers of possibilities for δ and Δ , and hence impose bounds on $|\mathbb{G}_\delta^+|$ and $|\mathbb{G}_\delta^-|$, thereby providing an upper bound on the rank of the curves (7) and (8).

We remark that Lemmas 1 to 7 are complete in the sense that if a curve corresponding to a value of δ or Δ cannot be shown by the Lemmas to be locally unsolvable, then the curve actually does have local solutions at all primes. This is made formal for the curve (21) as follows; details for the curve (22) are similar, and may safely be left to the reader.

Observe that if the curve (21) is nonsingular at the prime p , then the Weil estimates [11] show that there is a point on the curve defined over the field with p elements; and then by Hensel's lemma a point defined over \mathbb{Q}_p . It is necessary, therefore, only to consider further those primes for which (21) is singular, namely the primes p with

$$p \mid 2mn(m^2 - 2mn - n^2)(m^4 - 4m^3n + 18m^2n^2 + 4mn^3 + n^4).$$

The greatest common divisor of any pair of the factors

$$2, \quad m, \quad n, \quad m^2 - 2mn - n^2, \quad m^4 - 4m^3n + 18m^2n^2 + 4mn^3 + n^4$$

is at most 2. First, suppose that $p \neq 2$.

1. If $p \mid (m^4 - 4m^3n + 18m^2n^2 + 4mn^3 + n^4)$, then necessarily $\delta \perp p$. The case $(\delta \mid p) = -1$ is covered by Lemma 1; and if $(\delta \mid p) = +1$, then there is a p -adic solution $(a, b, c) = (1, 0, \sqrt{\delta})$.

2. If $p \mid (m^2 - 2mn - n^2)$, then $\delta \perp p$. If $(\delta \mid p) = +1$, then there is a p -adic solution $(a, b, c) = (1, 0, \sqrt{\delta})$. The case $(\delta \mid p) = -1, p \equiv 1 \pmod 8$ is covered by Lemma 2; and if $(\delta \mid p) = -1, p \not\equiv 1 \pmod 8$, then, since $(m - n)^2 - 2n^2 \equiv 0 \pmod p$, it follows that $(2 \mid p) = +1$, so $p \equiv -1 \pmod 8$. Then there is the p -adic solution

$$(a, b, c) = \left(2mn\sqrt{-1/\delta}, 1, 2mn(m^2 - 2mn - n^2)\sqrt{-1/\delta} \right).$$

3. If $p \mid mn$ and $p \mid \delta$, then there is a p -adic solution given by $(a, b) = (1, 1)$. Suppose that $p \mid m$ and $p \nmid \delta$. Let $u, v \in \mathbb{Q}_p$ be a solution of the Pell equation $u^2 - \delta v^2 = 1$ for which $v \not\equiv 0 \pmod p$; then there is a p -adic solution of (21) given by $(a, b) = (n^2 v, 1)$. Similarly for $p \mid n, p \nmid \delta$.

8. A rank-three example considered in detail

In this section we shall examine a specific numerical instance in detail, in order to demonstrate how, for a given slope (m, n) , it is usually possible to determine all the solutions of (3) corresponding to that slope. John Leech observed many solutions containing the slope $(m, n) = (10, 3)$. This corresponds at (7) to the curve

$$r^2 = \sigma(\sigma^2 + 3600\sigma + 1), \tag{24}$$

and this is indeed a curve of rank 3:

Theorem 8. The group of rational points on the elliptic curve (24) has rank 3, and is generated by the points

$$\left(-\frac{3}{5}, -\frac{1}{100}\right), \left(\frac{1}{30}, \frac{341}{1800}\right), \left(\frac{6}{25}, \frac{31}{100}\right)$$

of infinite order, and $(-1, \frac{31}{80})$ of order 4.

In fact, we work with the Néron minimal model of (24), or rather a translation thereof, in order to avoid a rational point with x -coordinate 0. This is necessary in order to apply a technique of Tate.

The curve (24) maps to the following (Figure 6):

$$E: y^2 + xy - 500y = x^3 + 540x^2 - 480000x - 20000000 \tag{25}$$

via the maps

$$(x, y) = (900\sigma + 500, -450\sigma + 27000\sigma),$$

$$(\sigma, \tau) = \left(\frac{x - 500}{900}, \frac{y + \frac{1}{2}x - 250}{27000}\right).$$

We actually prove the following theorem.

Theorem 9. The group of rational points on (25) is generated by $(-40, 0)$, $(530, 5100)$, $(716, 16632)$ of infinite order, and $(-400, 14400)$ of order 4.

355.	40	77	185	18	385	2664	414.	91	60	110	91	132	91
356.	68	11	154	45	29	810	415.	23	130	115	132	260	33
357.	195	44	99	70	275	252	416.	133	22	24	133	264	133
358.	75	104	143	12	13	116	417.	148	7	84	133	111	2002
359.	17	40	79	140	79		418.	42	115	161	40	161	120
360.	100	42	60	79	140	79	419.	120	37	128	57	128	575
361.	79	21	175	22	21	220	420.	85	78	39	176	1105	100
362.	13	110	124	33	1364	195	421.	88	75	141	187	1105	100
363.	38	85	37	153	703	90	422.	91	190	148	137	4635	3068
364.	58	65	40	87	435	104	423.	177	32	128	177	310	231
365.	55	69	115	118	177		424.	81	185	175	34	81	170
366.	3	92	80	143	214	368	425.	133	33	15	224	3040	231
367.	12	110	87	115	115		426.	155	11	18	155	90	341
368.	19	108	112	15	4	513	427.	10	157	117	127	20410	1143
369.	82	104	83	4	2120		428.	104	63	88	117	156	425
370.	26	8	84	3	693		429.	150	17	17	156	425	156
371.	96	28	3	91	495		430.	37	132	132	59	222	59
372.	51	77	88	45	485		431.	60	109	57	115	2180	437
373.	85	44	189	22	2380		432.	84	85	153	80	153	412
374.	5	126	177	7	126		433.	121	48	55	122	1936	215
375.	26	105	91	44	44		434.	135	34	92	153	391	190
376.	63	68	164	63	123		435.	37	115	46	110	146	143
377.	76	55	133	45	693		436.	14	30	59	135	220	21
378.	105	26	87	130	145		437.	13	165	198	13	99	130
379.	110	21	44	135	220		438.	13	165	198	13	99	130
380.	111	20	22	111	111		439.	109	70	120	109	168	109
381.	48	85	131	51	80		440.	140	39	148	45	259	1170
382.	175	58	117	50	145		441.	85	96	165	56	187	224
383.	119	15	203	17	812		442.	125	56	40	183	875	183
384.	118	12	291	17	969		443.	157	24	26	157	312	157
385.	105	31	45	106	371		444.	57	130	209	39	209	390
386.	177	60	175	12	275		445.	59	130	165	26	59	165
387.	19	120	159	40	57		446.	136	53	78	125	7208	4875
388.	54	85	155	32	992		447.	147	44	52	147	286	147
389.	55	84	80	77	77		448.	182	9	8	195	455	282
390.	103	36	44	103	103		449.	141	52	55	156	715	132
391.	104	35	21	176	176		450.	106	91	91	132	391	132
392.	108	31	113	42	3164		451.	14	53	133	56	232	119
393.	1	140	30	119	7		452.	11	136	153	121	740	363
394.	56	85	153	35	280		453.	11	86	78	139	260	139
395.	56	85	153	35	40	2499	454.	139	66	104	133	234	133
396.	56	85	168	37	510		455.	133	72	104	133	234	133
397.	56	85	154	15	72	203	456.	153	52	119	108	238	351
398.	38	105	118	35	177	95	457.	183	26	28	183	364	183
399.	42	53	142	97	174	1239	458.	130	81	81	148	481	180
400.	97	38	126	107	166	963	459.	137	75	91	150	910	411
401.	17	78	126	107	166	963	460.	162	55	41	195	4455	1066
402.	113	133	130	21	570	91	461.	183	38	17	209	3553	366
403.	13	115	130	21	570	91	462.	165	58	137	99	1507	2610
404.	105	41	65	84	195	164	463.	133	94	165	76	420	517
405.	33	115	170	33	115	102	464.	17	212	80	159	255	16
406.	45	104	120	121	484	117	465.	163	66	84	163	308	163
407.	77	72	77	124	279	88	466.	213	16	16	219	584	163
408.	93	56	88	93	154	93	467.	52	183	149	90	9685	2316
409.	105	44	143	53	1092	2915	468.	211	28	30	211	420	211
410.	140	9	9	164	205	42							
411.	15	136	170	13	104	255							
412.	39	112	35	129	1040	129							
413.	46	105	115	61	915	322							

Table 1 (concluded)

The canonical (or Tate) height $\hat{h}(P)$ can be written as a sum of local heights,

$$\hat{h}(P) = \sum_v \hat{h}_v(P),$$

one term for each distinct valuation on \mathbf{Q} , and it is this height which we estimate as follows.

For the archimedean valuation or ordinary absolute value, Tate has given an easily computed power series which allows computation of $\hat{h}_{\infty}(P)$. Specifically, for the curve (25),

$$\hat{h}_{\infty}(P) = \ln |z| + \sum_{n=0}^{\infty} 4^{-n-1} \ln(z_n)$$

with
$$z_n = 1 + \frac{960500}{x_n^2} + \frac{159500000}{x_n^3} + \frac{273725000000}{x_n^4} \quad (n \geq 0)$$

and
$$x_0 = x; \quad x_{n+1} = \frac{x_n^4 + 960500x_n^2 + 159500000x_n + 273725000000}{4x_n^3 + 2161x_n^2 - 1921000x_n - 79750000}.$$

The formula for x_{n+1} corresponds to the duplication formula on (25), so that

$$z_n = x(2^n P), \quad n \geq 0.$$

Note that $2^n P$ for $n \geq 1$ is a point lying in the right-hand branch of the graph of (25). Rewriting (25) in the form

$$\left(y + \frac{1}{2}x - 250\right)^2 = (x - 500)\left(x^2 + \frac{4161}{4}x + 39875\right),$$

we see that for P in the loop of the graph (Figure 6),

$$-1000.390568 \leq x(P) \leq -39.859432,$$

and for P in the right-hand branch,

$$500 \leq x(P).$$

It follows that if P is in the right hand branch, then $x_n \geq 500$ for $n \geq 0$. Since P is nontorsion, then $x_n > 500$ for $n \geq 0$. Hence,

$$1 < z_n \leq 10.497600 \quad (n \geq 0),$$

so that

$$0 < \ln z_n \leq 2.351147 \quad (n \geq 0)$$

and

$$0 < \sum_{n=0}^{\infty} 4^{-n-1} \ln z_n \leq 2.351147 \sum_{n=0}^{\infty} 4^{-n-1} < 0.783716.$$

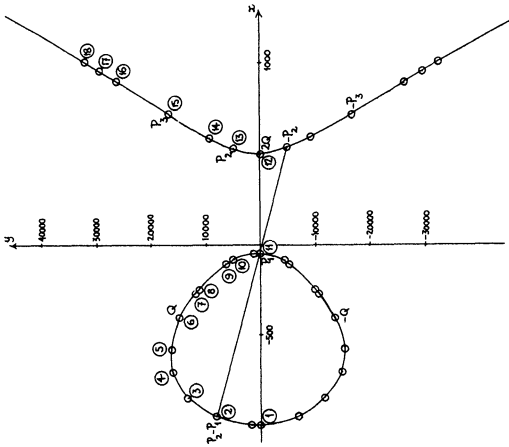


Figure 6. The curve $y^2 + zy - 500y = x^3 + 540x^2 - 480000x - 20000000$. The circled numbers correspond to the line numbers of Table 3.

Proof. The determination of the torsion subgroup is quite straightforward and is left as an exercise for the reader. The group is cyclic of order 4 with generator $Q = (-400, 14400)$. Henceforth, when we indicate a rational point of (25) by P , it will be assumed that P is nontorsion.

Any determination of generators will involve an argument with heights; the proof we present is modelled on that of Buhler, Gross & Zagier [2].

Let $P = (x, y)$ be a point of (25), and write $x = x(P) = a/b$, $a \perp b$, $b > 0$. Then the naive height $h(P)$ is defined by

$$h(P) = \ln \max(|a|, b).$$

Thus, $x > 500$ implies

$$\ln |x| < \hat{h}_\infty(P) < \ln |x| + 0.783716. \tag{26}$$

On the other hand, if P is in the loop of the graph (which is compact), then the maximum and minimum of $(\hat{h}_\infty(P) - \ln |x|)$ can be readily computed, and we find (see Figure 7):

$$\ln |x| + 0.182338 < \hat{h}_\infty(P) < \ln |x| + 2.894039 \tag{26a}$$

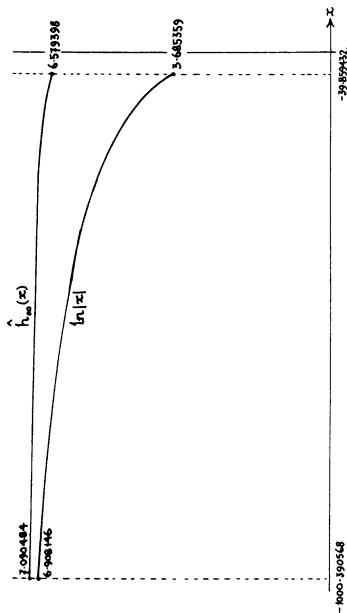


Figure 7. Comparison of archimedean valuation with $\ln |x|$. It remains now to estimate the local component of the canonical height at the prime p . The algorithms of Silverman [9] are useful here; he gives an explicit recipe for computing the p -component.

We summarize the results of the local computation. Recall the notation $x = x(P) = a/b$, $a \perp b$, $b > 0$. Denote the usual p -adic valuation by v_p .

1. If $p|b$, then $\hat{h}_p(P) = \text{ord}_p(b) \cdot \ln p$.
2. If $p \nmid b$, and $p \neq 2, 3, 5$, or 31 , then $\hat{h}_p(P) = 0$. Define c_i as $-7/8, -3/2, -15/8$, or -2 , according as $i = 1, 2, 3$, or $i \geq 4$.
3. If $p = 2, 2 + b$, and $v_2(2y + x - 500) = i$, then $\hat{h}_2(P) = c_i \ln 2$.
4. If $p = 3, 3 + b$, and $x \equiv 1 \pmod 3$, then $\hat{h}_3(P) = 0$, while if $x \not\equiv 1 \pmod 3$ and $v_3(2y + x - 500) = i$, then $\hat{h}_3(P) = c_i \ln 3$.

5. If $p = 5, 5 + b$, and $x \not\equiv 0 \pmod 5$, then $\hat{h}_5(P) = 0$, while if $x \equiv 0 \pmod 5$ and $v_5(2y + x - 500) = i$, then $\hat{h}_5(P) = c_i \ln 5$.

6. If $p = 31$, and $31 + b$, then $\hat{h}_{31}(P) = -\frac{1}{2} \ln 31$ or $\hat{h}_{31}(P) = 0$, according as $x \equiv 3$ or $x \not\equiv 3 \pmod{31}$.

Notice that 1. implies that the sum of all local components for primes dividing b is simply $\ln b$.

The above local factors thus produce the following estimate for the sum over non-archimedean valuations:

$$\ln b - \ln(2^2 \cdot 3^2 \cdot 31^{1/2}) \leq \sum \hat{h}_v(P) \leq \ln b. \tag{27}$$

Combining (26) with (27) we have that for P in the right-hand branch of Figure 6,

$$\ln |a| - 8.519388 < \hat{h}(P) < \ln |a| + 0.783716, \tag{28}$$

and combining (26a) with (27), we have that for P in the loop,

$$\ln |a| - 8.337050 < \hat{h}(P) < \ln |a| + 2.894039. \tag{28a}$$

Since $|a|/b = |x(P)| \geq 39.859$, we can use

$$h(P) = \ln \max(|a|, b) = \ln |a| \ln \min(1, |a|/b) = \ln |a|$$

to rewrite (28) and (28a) in the form

$$-8.519388 < \hat{h}(P) - h(P) < 0.783716 \quad (P \text{ in the right-hand branch}), \tag{29}$$

$$-8.337050 < \hat{h}(P) - h(P) < 2.894039 \quad (P \text{ in the loop}). \tag{29a}$$

It is now straightforward to find all the points P on the curve with given bounded height. For example, to find all points P satisfying $\hat{h}(P) < 2.144204$, we argue as follows.

If P is in the right-hand branch, then (29) implies

$$h(P) < 10.663592, \tag{30}$$

and if P is in the loop, then (29a) implies

$$h(P) < 10.481254. \tag{30a}$$

With $x = a/b$, suppose first $x > 0$. Then (30) holds, and

$$a/b \geq 500.$$

Table 3. Thirty points of the curve (25), with their heights

	x	y	n_0	n_1	n_2	n_3	$\hat{h}(P)$
1.	-1000	0	2	-1	0	0	2,071,634
2.	-953	8262	0	-1	1	0	2,553,675
3.	-850	13500	-1	0	0	-1	1,951,139
4.	-710	15950	0	1	0	1	3,240,451
5.	-580	16200	-1	0	-1	0	2,144,203
6.	-400	14400	1	0	0	0	0
7.	-268	11712	0	1	-1	-1	4,393,466
8.	-250	11250	-1	0	1	0	2,144,203
9.	-100	6000	-1	0	0	1	1,951,139
10.	-88	5376	0	-1	1	-1	4,616,162
11.	-40	0	0	1	0	0	2,071,634
12.	500	0	2	0	0	0	0
13.	530	5100	0	0	1	0	2,144,203
14.	590	9450	-1	-1	0	-1	3,240,451
15.	716	16632	0	0	0	1	1,951,139
16.	892	26096	-1	-1	-1	0	5,878,000
17.	950	29250	-1	1	-1	0	2,553,675
18.	1000	32000	2	0	1	1	3,201,672
19.	1460	59040	1	1	0	0	2,071,634
20.	2120	103680	0	0	-1	-1	3,201,672
21.	2300	117000	-1	-1	1	0	2,553,675
22.	4250	288750	2	0	0	-1	1,951,139
23.	7790	704700	-1	-1	0	1	4,805,095
24.	9500	945000	-1	1	0	1	3,240,451
25.	12020	1339200	0	0	1	-1	4,989,012
26.	27500	4590000	2	0	-1	0	2,144,203
27.	36800	7091700	1	-1	1	1	4,393,466
28.	57632	13870656	1	1	1	1	6,153,146
29.	922100	885254400	0	-2	0	0	8,286,536
30.	1521500	1876329000	1	1	-2	-1	8,270,243

We now have a well-ordering on $E(\mathbb{Q})$ determined by the canonical height. The appropriate quadratic form gives the following lemma.

Thus, $0 < a < e^{10.683892} < 42770$.

Moreover, $b \leq a/500 < 86$ and b has to be a perfect square. It is a small machine search to find all a, b satisfying these conditions; the x -coordinates of the resulting points are displayed on the left of Table 2.

Suppose second $x < 0$. Then (30a) holds and

$$-1000.390568 < \frac{a}{b} < -39.859432.$$

Thus,

$$|a| < e^{10.681254} < 35642,$$

and as above, b is strongly bounded. The x -coordinates of the points resulting from the machine search are displayed on the right of Table 2. The third column of Table 2 expresses the point P in terms of the group law on the curve.

Table 2. All points with $\text{height } \hat{h}(P) < 2.144204$

$x(P)$	$\hat{h}(P)$	$x(P)$	$\hat{h}(P)$	P_1
500	0	-40	2,071,634	P_1
530	2,144,203	-100	1,951,139	$P_3 - Q$
716	1,951,139	-250	2,144,203	$P_2 - Q$
1460	2,071,634	-400	0	Q
4250	1,951,139	-580	2,144,203	$P_1 + Q$
27500	2,144,203	-850	1,951,139	$P_3 + Q$
5375/4	2,071,634	-1000	2,071,634	$P_1 + 2Q$

Now a standard 2-descent on the curve (25) shows that P_1, P_2, P_3 are generators for $E(\mathbb{Q})/2E(\mathbb{Q})$, which is of rank 3 over $\mathbb{Z}/2\mathbb{Z}$. Together with the above computation of all points with small height, it follows immediately that P_1, P_2, P_3 are generators of infinite order for $E(\mathbb{Q})$, as required. \square

The principal theorem is now an immediate corollary.

As an instance of height computations, we list the heights of 30 integer points P of $E(\mathbb{Q})$ in Table 3 together with the representation $P = n_0Q + n_1P_1 + n_2P_2 + n_3P_3$. Some of these are illustrated in Figure 6.

Lemma 10. *The canonical height is given by the quadratic form $\hat{h}(aP_1 + bP_2 + cP_3) = \hat{h}(P_1)a^2 + \hat{h}(P_2)b^2 + \hat{h}(P_3)c^2 + (\hat{h}(P_2 + P_3) - \hat{h}(P_2) - \hat{h}(P_3))bc + (\hat{h}(P_3 + P_1) - \hat{h}(P_3) - \hat{h}(P_1))ca + (\hat{h}(P_1 + P_2) - \hat{h}(P_1) - \hat{h}(P_2))ab$, in which the coefficients $\hat{h}(P_1) \approx 2.071634$, $\hat{h}(P_2) \approx 2.144203$, $\hat{h}(P_3) \approx 1.951139$, $\hat{h}(P_1 + P_2) \approx 3.201672$, $\hat{h}(P_2 + P_1) \approx 3.240451$, $\hat{h}(P_1 + P_3) \approx 5.878000$ can be computed to any desired degree of accuracy.*

Table 4. Points on (25), to within torsion, in order of height, up to height 10

P	x	y	$\hat{h}(P)$
P_3	716	16632	1.951139
P_1	-40	0	2.071634
P_2	530	5100	2.144203
$-P_1 + P_3$	-958	8262	2.553675
$-P_2 - P_3$	2120	103680	3.201672
$P_1 + P_3$	-710	15950	3.240451
$P_1 - P_2 - P_3$	-268	11712	4.393466
$-P_1 + P_2 - P_3$	-88	5376	4.616162
$-Q - P_1 + P_3$	7790	704700	4.805095
$P_2 - P_3$	12020	1339200	4.989012
$-Q - P_1 - P_2$	892	26096	5.878000
$Q + P_1 + P_2 + P_3$	57632	13870656	6.153146
$-Q - 2P_1 + P_2$	-46180/13 ²	26017200/13 ³	7.106415
$Q - P_1 + 2P_2$	-7015/8 ²	-2994975/8 ³	7.324122
$-2P_3$	25496/5 ²	4137516/5 ³	7.804556
$-Q - P_2 - 2P_3$	-103780/11 ²	-15850800/11 ³	8.161419
$Q + P_1 - 2P_2 - P_3$	1521500	1876329000	8.270243
$-2P_1$	922100	885254400	8.286536
$2Q + P_1 + 2P_3$	-70375/16 ²	48670875/16 ³	8.311546
$-2P_1 + P_2 - P_3$	154205/4 ²	61783155/4 ³	8.386580
$2P_2$	817400/11 ²	-768384000/11 ³	8.576812
$Q + 2P_1 + P_3$	-42916/7 ²	-3869424/7 ³	8.673031
$Q + 2P_2 + P_3$	-24946/5 ²	332748/5 ³	8.740611
$P_1 + P_2 - P_3$	-350200/67 ²	1443406500/67 ³	9.505131
$Q + 2P_1 - P_2 - P_3$	-309245/18 ²	49827635/18 ³	9.728526

In Table 4 we list, up to torsion, points on the curve (25) in terms of increasing height, up to height 10.

The maps at (25) which recover the corresponding points on the curve (24) lead to the following formulas for recovery of the r, s, u, v parameters of the geometric

nu-configuration:

$$\frac{r}{s} = \frac{(500 - x)(400 + x)}{30(y - 15x + 7500)}, \quad \frac{u}{v} = \frac{y - 15x + 7500}{30(400 + x)}.$$

Corresponding to the entries of Table 4 we can therefore compute the following parameters for geometric nu-configurations (Table 5).

Table 5. Nu-configurations containing the slope 91/60 ($m = 10, n = 3$)

P	r	s	u	v
P_3	3	-5	2	5
P_1	4	5	3	4
P_2	1	-5	1	6
$-P_1 + P_2$	9	-10	9	-5
$-P_2 - P_3$	12	-7	21	20
$P_1 + P_3$	11	-30	11	-3
$P_1 - P_2 - P_3$	8	55	88	15
$-P_1 + P_2 - P_3$	28	65	91	60
$-Q - P_1 + P_3$	117	-35	63	26
$P_2 - P_3$	184	-45	72	23
$-Q - P_1 - P_2$	238	-285	133	255
$Q + P_1 + P_2 + P_3$	552	-65	299	40
$-Q - 2P_1 + P_2$	154	1105	561	91
$Q - P_1 + 2P_2$	1003	560	357	944
$-2P_3$	1653	-1700	1292	2175
$-Q - P_2 - 2P_3$	5254	-2145	481	-781
$Q + P_1 - 2P_2 - P_3$	3705	-89	2314	57
$-2P_1$	4000	-123	3936	125
$2Q + P_1 + 2P_3$	805	5856	1403	224
$-2P_1 + P_2 - P_3$	2451	-664	4731	1720
$2P_2$	4524	2035	5365	-1716
$Q + 2P_1 + P_3$	7102	-3045	1537	-2345
$Q + 2P_2 + P_3$	4187	-3525	3713	-2650
$P_1 + P_2 - P_3$	6789	14740	6820	4891
$Q + 2P_1 - P_2 - P_3$	5833	-6368	18727	-10280

The eight points $\pm P, \pm P \pm Q, \pm P + 2Q$ each return the same nu-configuration. This is a general phenomenon, illustrated by the pattern on the right of Table 6, and is not restricted to the particular slope $(m, n) = (10, 3)$, nor the particular point $P = P_1$, which corresponds to solution 9. of Table 1, or line 11 (or 1, or 19) of Table 3. We

give the coordinates of the points (x, y) on the curve (25), and also of the corresponding points (σ, τ) on the curve (19), which, for $(m, n) = (10, 3)$, takes the form

$$\tau^2 = \sigma(\sigma^2 + 816\sigma + 60^4). \tag{31}$$

Negation (change of sign of τ in (19) or (31)) corresponds to interchange of (r, s) with (u, v) , and reflexion of Table 6 from top to bottom.

We shall see in the next section that the torsion group of E consists of, or contains as a subgroup, a group isomorphic to $Z/4Z$ and generated by $Q(-4m^2n^2, 4m^2n^2K)$. Addition of Q corresponds to interchange of (r, s) with (u, v) while replacing the latter by $(v, -u)$. The coordinates (x, y) on (25) and (σ, τ) on (31) are related by

$$\sigma = 4(x - 500), \quad \tau = 4(2y + x - 500) \quad \text{or} \quad x = (\sigma + 2000)/4, \quad y = (\tau - \sigma)/8.$$

Table 6. Eight points give a single nu-configuration

	x	y	σ	τ	r	s	u	v
P_1	-40	0	-2160	-2160	4	5	3	4
$P_1 + Q$	1460	59040	3840	476160	4	-3	4	5
$P_1 + 2Q$	-1000	1500	-6000	6000	5	-4	4	-3
$P_1 - Q$	5375/4	-421875/8	3375	-418500	3	4	5	-4
$-P_1 + Q$	5375/4	415125/8	3375	418500	5	-4	3	4
$-P_1 + 2Q$	-1000	0	-6000	-6000	4	-3	5	-4
$-P_1 - Q$	1460	-60000	3840	-476160	4	5	4	-3
$-P_1$	-40	540	-2160	2160	3	4	4	5

Generally, on the curve

$$E : \tau^2 = \sigma(\sigma^2 + L\sigma + 16m^4n^4), \tag{19}$$

the eight points lie one each on the eight arcs of the curve separated by the point at infinity, the three points with $\tau = 0$, and the two pairs of points $(-4m^2n^2, \pm 4m^2n^2K)$ and $(4m^2n^2, \pm 4m^2n^2/M)$, of which the last is not, in general, rational (see Theorem 11 in §10). One could choose a canonical solution from this set of points: for example, that with $0 < \sigma < 4m^2n^2$ and $\tau > 0$.

9. The torsion group

We describe the torsion group, T , of the curve (7), which we recall in the notation of §6 ($L = K^2 + 8m^2n^2, K = m^2 - 2mn - n^2$):

$$E : \tau^2 = \sigma(\sigma^2 + L\sigma + 16m^4n^4). \tag{19}$$

The points $\pm Q(-4m^2n^2, \pm 4m^2n^2K)$ are of order 4, so, by Mazur's theorem [7, 8], the only possibilities for T on E are

$$Z/4Z, \quad Z/8Z, \quad Z/12Z, \quad Z/2Z \times Z/4Z \quad \text{or} \quad Z/2Z \times Z/8Z.$$

Now the doubling law on E gives the σ -coordinate of $2(\sigma, \tau)$ as the perfect square $(16m^4n^4 - s^2)^2/4t^2$, and since the σ -coordinate of Q , namely $-4m^2n^2$, is not a square, the points $\pm Q$ are not divisible by 2, and $T \neq Z/8Z$. A more tedious calculation shows that these points are not divisible by 3.

[From a more sophisticated standpoint, one can argue as follows. The singular fibres of our curve occur at $m = 0, n = 0$, and at the roots of $K = 0$ and $M = 0$. The Kodaira classification of each singular fibre is of Type I_b , where b is in each instance a (small) power of 2. Accordingly the torsion group, being killed by the least common multiple of these orders, is itself of order a power of 2. See §2D of Cox & Zucker [4] for full details.]

So we are left with the possibilities

$$Z/4Z, \quad Z/2Z \times Z/4Z, \quad Z/2Z \times Z/8Z,$$

each of which can occur.

The last two cases each contain three points of order 2, and the quadratic on the right of (19) splits into two linear factors, $(\sigma + r_1)(\sigma + r_2)$. Then $r_1 + r_2 = L, r_1r_2 = 16m^4n^4, (r_1 - r_2)^2 = L^2 - 64m^4n^4 = (L - 8m^2n^2)(L + 8m^2n^2) = K^2M$, so that M is a perfect square, say $z^2 = M = K^2 + 16m^2n^2$, and $(z - 4mn)(z + 4mn) = K^2$. Fact (b) from §6 implies that m, n are of opposite parity, z is odd and $z \perp mn$, and $z - 4mn \perp z + 4mn$ implies that $z \pm 4mn$ are each squares, say w_1^2 and w_2^2 . Also, $r_1 - r_2 = \pm Kz$ and $r_1, r_2 = (L \pm Kz)/2$, and, since $r_1 \perp r_2, r_1r_2 = (2mn)^4, r_1, r_2$ are each fourth powers. The equation

$$M = z^2 = m^4 - 4m^3n + 18m^2n^2 + 4mn^3 + n^4$$

represents an elliptic curve, which maps into $v^2 = u(u^2 + 6u + 4)$, recognizable as the curve (4) of §3, where it arose from symmetrical nu-configurations: its rank is 1, with solutions $(m, n) = (1, 0), (3, 2), (50, 39), (221, 5700), \dots$

The tangents from the origin to the curve (19) have slopes μ , given by repetition of roots in $\mu^2\sigma = \sigma^2 + L\sigma + 16m^4n^4$:

$$(L - \mu^2)^2 = 64m^4n^4, \\ \mu^2 = L \pm 8m^2n^2 = K^2 \quad \text{or} \quad M (= z^2), \\ \mu = \pm K \quad \text{or} \quad \pm z.$$

The four points of contact have order 4, and coordinates $(-4m^2n^2, \pm 4m^2n^2K)$ and $(4m^2n^2, \pm 4m^2n^2z)$.

There will be a point of order 8 just if a tangent from $(4m^2n^2, 4m^2n^2z)$ has a rational point of contact: i.e., if its slope μ is such that the quadratic

$$\sigma^2 + \sigma(L - \mu^2 + 4m^2n^2) + 4m^2n^2(z - \mu)^2 = 0$$

10. Tables of ranks and informations leading to the generation of nu-configurations when the rank is positive

Table 7 ($m+n$ odd; $3 \leq m+n \leq 49$) and Table 8 ($m+n$ even; $4 \leq m+n \leq 50$) give the ranks of the curves (7) and (8) for specific values of m and n .

Columns m and n are clear, while column K lists those factors of $K = m^2 - 2mn - n^2$ which are 1 mod 8. These are factors of potential values of Δ , but, on the other hand, they may, via Lemma 2, restrict the possibilities for δ .

Column M gives the prime factorization of $M = K^2 + 16m^2n^2$. In Table 8, the factor 2^2 is omitted. In Table 7 (but not in 8) the primes congruent to 1 mod 8, are printed in bold: Lemma 7 requires that, if $m+n$ is odd, then $\Delta \equiv 1$ mod 8, so that the other factors of M , congruent to 5 mod 8, must be taken in pairs. Any factor of M may serve, via Lemma 1, to restrict values of δ .

Column $\pm\delta$ contains ω entries, where ω is the number of distinct prime factors of m . There are $2^\omega - 1$ possible values, other than ± 1 , for $\pm\delta$. The entries, in order, are:

1. primes chosen from column M , which successively eliminate, via Lemma 1, $2^{\omega-1}, 2^{\omega-2}, \dots$ of the $2^\omega - 1$ possibilities for δ ;
2. primes from column K , which may continue this elimination process via Lemma 2;
3. solution numbers (in bold, with a period) from Table 1, for as many solutions as are known, whose δ -values are linearly independent;
4. the letter A , repeated if necessary, augmenting the list 3. of solutions by referring to auxiliary Tables 7A or 8A, where further independent values of δ are given, with the relevant solutions (a, b, c) of (21), beyond the range of Table 1;
5. sufficient query marks (?) to make the total number of entries up to ω , indicating (along with similar items in column Δ) the extent of our lack of knowledge of the precise rank.

To calculate solutions corresponding to values of δ not specifically listed in Tables 7A and 8A, use Lemmas 12 and 13:

Lemma 12. *If (δ, a, b, c) satisfies equation (21), then there is a solution $(-\delta, a', b', c')$ with $a' : b' = 2mn(c \pm abK) : \delta a^2 + 4m^2n^2b^2$.*

has equal roots, i.e., just if

$$L - \mu^2 + 4m^2n^2 = \pm 4mn(z - \mu),$$

i.e., just if

$$(L \pm 2mn)^2 = L + 4m^2n^2 + 4m^2n^2 \pm 4mnz = M \pm 4mnz = z(z \pm 4mn). \quad (32)$$

Now $(z + 4mn)(z - 4mn) = M - 16m^2n^2 = K^2$, and $z + 4mn, z - 4mn$ are coprime. Hence $z \pm 4mn = w^2$, so that (32) implies that z is a square, say y^2 . Then $\mu + 2mn = \pm wy$, and the equal roots are $\sigma = 2mn(z - \mu)$, leading to the eight points of order 8:

$$(2mn(2mn + y(\epsilon y \pm w)), \pm 2mnwy(2mn + y(\epsilon y \pm w))),$$

where ϵ is to be read throughout either as + or as -.

Thus the group $T \simeq Z/2Z \times Z/8Z$ occurs only when

$$z^2 = M = m^4 - 4m^3n + 18m^2n^2 + 4mn^3 + n^4 = y^4. \quad (33)$$

The equation (33) represents a curve of genus 3, and by the theorem of Faltings [5], has only finitely many rational solutions. The actual determination of such solutions may be very difficult: we conjecture that the only solutions are afforded by $\pm(m, n) = (0, 1), (1, 0), (3, 2)$ and $(2, -3)$. To sum up:

Theorem 11. (a) $T \simeq Z/4Z$ when $M = m^4 - 4m^3n + 18m^2n^2 + 4mn^3 + n^4 \neq z^2$;
 (b) $T \simeq Z/2Z \times Z/4Z$ when $M = z^2$, but $z \neq y^2$;
 (c) $T \simeq Z/2Z \times Z/8Z$ when $M = y^4$.

Generators in each instance are (a) $(-4m^2n^2, 4m^2n^2K)$; (b) $(-4m^2n^2, 4m^2n^2K)$ and $(-(L + Kz)/2, 0)$; (c) $(2mn2(2mn + y^2 + wy), 2mnwy(2mn + y^2 + wy))$ and $(-(L + Kz)/2, 0)$, where $w = w_+$ in the above notation.

Numerical examples are provided by (a) $(m, n) = (2, 1)$; (b) $(m, n) = (50, 39)$ and $z = 8329$; (c) $(m, n) = (3, 2), y = 5$, and $w = 7$.

In terms of the nu-configurations, (a) returns four degenerate solutions, (b) returns (a) together with four copies of a symmetrical nu-configuration given by

$$\frac{u}{v} = \frac{K + z}{4mn} = -\frac{r}{s},$$

while, if our conjecture is true, (c), with points of order 8, occurs only when $m/n = 3/2$, leading to the exceptional configuration with $r/s = 1/2$ and $u/v = 3/1$, and its permutations.

For the 2-isogenous curve (20) the torsion group is $Z/2Z \times Z/2Z$ in case (a). Otherwise it is $Z/2Z \times Z/4Z$, except for the possibility $Z/2Z \times Z/8Z$ when $M = y^4$ and m and n are both perfect squares, an extremely unlikely situation, given the remark following equation (33).

Lemma 13. If $(\delta_1, a_1, b_1, c_1)$ and $(\delta_2, a_2, b_2, c_2)$ each satisfy equation (21), and the $\gcd(\delta_1, \delta_2) = \delta$, with $\delta_1 = \delta\delta'_1, \delta_2 = \delta\delta'_2$, then there is a solution $(\delta'_1\delta'_2, a', b', c')$, with $a' : b' = a_1b_1c_2 - a_2b_2c_1 : \delta'_1\delta'_2\delta'_1\delta'_2 - \delta'_2\delta'_1\delta'_1\delta'_2$.

Column Δ contains Ω entries, which concern potential values of Δ . These parallel those in column $\pm\delta$, but the situation is more complicated. If there are ω_k entries in column K , and ω_1 and ω_2 distinct prime factors respectively congruent to 1 and 5 mod 8, in column M , then, in Table 7, $\Omega = \omega_k + \omega_1 + \max(\omega_2 - 1, 0) - 1$, while in Table 8, $\Omega = \omega_k + \omega_1 + \omega_2 - 1$. The term $\max(\omega_2 - 1, 0)$ arises from Lemma 7, which requires that, when $m+n$ is odd, the number of factors of Δ which are 5 mod 8 must be even. The final -1 in each formula reflects the fact that possible values of Δ occur in complementary pairs, of which the prototype is 1 and M (more precisely, the squarefree part of M). In fact, if we extend the notation of Lemma 6, a little manipulation leads to the following formula.

Lemma 14. If $K = D_1E_1F_1^2$ and $M = D_2E_2F_2^2$, and there is a solution (A, B, C) of (22) with $\Delta = D_1D_2$, then a complementary solution $(BE_1F_1^2F_2, A, CE_1F_1^2F_2)$ exists with $\Delta = D_1E_2$.

Here we assume that D_1E_1 and D_2E_2 are separately squarefree, but make no other assumptions of coprimality. If it is required that $A \perp B$, then, while removing a common factor from A and B , its square can and must be removed from C . The two pairs of points $(S, \pm T)$ corresponding to this complementary pair of solutions form a quadrangle on the curve (20) whose diagonal point triangle comprises the points $(K^2, 0)$, $(M, 0)$, and the point at infinity, each of finite order. So they are the same, modulo torsion, and yield the same nu-configuration.

For brevity, Tables 7A and 8A list only one solution from each complementary pair, and list only a minimal set of linearly independent values of Δ . Solutions for other possible values of Δ may be constructed by Lemmas 14 and 15.

Lemma 15. If (A_1, B_1, C_1) and (A_2, B_2, C_2) are solutions of (22) with $\Delta = \Delta_1$, and Δ_2 , then (A, B, C) will be a solution, for $\Delta = \Delta_1\Delta_2/(\gcd(\Delta_1, \Delta_2))^2$, where $A : B = A_1B_1C_2 - A_2B_2C_1 : \Delta_1A_1^2B_2 - \Delta_2A_2^2B_1$.

The entries in column Δ are, in order, prime factors of mn which successively eliminate $2^{n-1}, 2^{n-2}, \dots$ of the $2^n - 1$ pairs of possibilities for Δ , other than 1 and M , much as in 1., 2. above, but using Lemma 5 in place of Lemmas 1 and 2, followed by letters A and query marks, as in 4., 5. above.

Column r indicates the rank, either exactly, or in the form $r_1 < r_2$ (meaning $r_1 \leq r \leq r_2$), where r_1 is the total number of solution numbers from column $\pm\delta$ and letters A from columns $\pm\delta$ and Δ , while r_2 is the same total, augmented by the number of query marks in those two columns.

Remark. As observed at the end of §6, if a value of δ (or Δ) is not eliminated by means of Lemmas 1 to 7, then the corresponding curve is actually everywhere locally soluble. In particular, the order of the corresponding Selmer group (see, for example, the Cassels survey article [3]) will be equal to 2^r . The well-known Selmer Conjecture implies that the actual rank satisfies $r \equiv r_2 \pmod 2$. Accordingly, for those rank entries in Tables 7 and 8 such as 0 < 1 and 0 < 3, it seems very likely that they should read 1 and 1 or 3 respectively, indicating the existence of at least one rational solution corresponding to a “?” that lies beyond the bounds of our calculations to date. In fact, this explains many of the larger entries in Tables 7A and 8A, which resulted from searching for precisely such solutions.

Illustrative examples

$(m, n) = (19, 22)$. Prime factors of mn : 2, 11, 19 ($\omega = 3$); $K = -959 = -7 \cdot 137$ ($\omega_k = 1$); $M = 3715265 = 5 \cdot 17 \cdot 109 \cdot 401$ ($\omega_1 = 2, \omega_2 = 3$). Potential values for $\pm\delta$ (other than 1): 2, 11, 22, 19, 39, 209, 418. Of these, $2^{n-1} = 4$, namely 2, 22, 38, 418, are eliminated by Lemma 1 with $p = 5$ (see the table of Legendre symbols at left); $2^{n-2} = 2$ of them (11, 209) by $p = 17$; and finally, $2^{n-3} = 1$ of them, namely 19, is eliminated by $p = 109$, so the $\pm\delta$ column reads: 5 17 109 and there is no positive contribution to the rank. Next, $\Omega = 1+2+(2-1)-1 = 3$, and there are $2^3 - 1 = 7$ pairs of potential values for Δ , other than 1 and M . The $2^{n-1} = 4$ pairs, 17 and $5 \times 109 \times 401$, 5×109 and 17×401 , and 137 times each of these, are all ruled out by Lemma 3 with $P = 11$; and the $2^{n-2} = 2$ pairs 401 and $5 \times 17 \times 109$, 401×137 and $5 \times 17 \times 109 \times 137$ by $P = 19$. There remains the possibility $\Delta = 137$ (or $137 \times M$), so our Δ column entry originally read: 11 19 ? and the rank was listed as 0 < 1. The remark preceding this example induced us to search for, and find, the solution $(A, B, C) = (79247, 407, 35579223616)$ corresponding to $\Delta = 137$.

2	11	19			
-	+	+			
5			+		
17			+		
109			-		
401			+		
137			+		

Prime factors of mn : 2, 3, 5, 7 ($\omega = 4$); $K = -799 = -17 \cdot 47$ ($\omega_k = 1$); $M = 3460801 = 1733 \cdot 1997$ ($\omega_1 = 0, \omega_2 = 2$). Potential values for $\pm\delta$: 2, 3, 6, 5, 10, 15, 30, 7, 14, 21, 42, 35, 70, 105, 210. From the table of Legendre symbols we see that $2^{n-1} = 8$ of these are eliminated by Lemma 1 with $p = 1733$ (or with $p = 1977$), and $2^{n-2} = 4$ more by Lemma 2 with $p = 17$. This leaves $\delta = 15, 42$ and 70, which are represented by solutions 97, 170, and 25. Only two of these are independent, so the entries 1733 17 25. 97. suffice for our $\pm\delta$ column. $\Omega = 1 + 0 + (2 - 1) - 1 = 1$ and the only possible pair of values for Δ , apart from 1 and M , is 17 and 17M, and these are ruled out by Lemma 5 with $P = 3$ (or 5 or 7), so the Δ column reads simply: 3, and the rank is 2.

2	3	5	7		
-	-	-	+		
1733			+		
1977			-		
17			-		

Table 7. Outline of rank calculations, m + n odd

Table with columns: m, n, K, M, ±δ, Δ, r, m, n, K, M, ±δ, Δ, r. Rows 1-14 showing calculations for various ranks.

(m,n)=(31,4). Prime factors of mn: 2, 31 (ω = 2); K = 697 = 17 · 41 (ω_K = 2); M = 731825 = 5^7 · 3 · 401 (ω_M = 2, ω_5 = 1; Ω = 2 + 2 + max(1 - 1, 0) - 1 = 3). Potential values for δ: 2, 31, 62. The first and third fall to Lemma 1 with p = 5, and the second to Lemma 1 with p = 73. The ±δ entry is 5 73. There are, of course, just two independent rows in the table of Legendre symbols. There are 2^0 - 1 = 7 pairs of potential Δ-values, 2^0 - 1 = 4 of which are eliminated by Lemma 5 with P = 31 (the only nontrivial odd divisor of mn). The Δ entry reads 31 A because the solutions (85,1,44880) and (15,1,8680), corresponding to Δ = 41 and Δ = 17 × 73 can be found in Table 7A. This suffices to determine the rank as 2. Lemma 14 enables the complementary solutions, Δ = 41 × 73 × 401 (1,1,526) and Δ = 17 × 401 (41,3,71176) to be found, and Lemma 15 provides the missing Δ = 41 × 17 × 73 (83,1,1551240) and Δ = 41 × 17 × 401 (5,83,7756200).

The numbers of entries of given rank in Tables 7 and 8 are

Table with columns: rank, 0, 0<2, 0<4, 1, 0<1, 0<3, 1<3, 2, 1<2, 2<4, 1<4, 3, 2<3, Total. Rows: Table 7, Table 8, Total.

So, if we assume the truth of the Selmer conjecture, but otherwise take a pessimistic view, the numbers and percentages of various ranks are

Table with columns: rank, 0, 1, 2, 3. Rows: Table 7, Table 8, Total.

It may be of interest to note that the numbers of curves of even rank (396) and of odd rank (376) are roughly equal; further that those of rank 2 or more seem to be at least 0.45 times as numerous as those of rank 0. Compare the concluding remarks of Lecture 1 of Washington [10, esp. pp. 254–256].

Table 7 (continued)

3	20	73	13 24317	13 73 71	5	1	13	14	17	5.136573	5.17 88	11	20	673	97 13133	13 17 5813	13 17 ?	5	0<2	12	23	937	M	$\pm \delta$	Δ	r
4	19		5 ⁵ 13577	5 A	1	14	13	337	643553	5 A	5.17 89,277	5.137 ?	12	22	517 89,277	5.137 ?	5.17 89,277	5.137 ?	3.23	0<1						
5	18		350441	72 ?	1	13	16	11	5.108541	5 A	5.61 115	5.61 115	13	18	89	5 ⁵ 61 829	5.61 115	3 A	0<1	16	19					0
6	17		89 4217	89 73 74	3 A	1<3	16	11	485201	89 ?	7 A ?	7 A ?	13	17	569	5.37 61 109	5.37 ?	7 A ?	1<3	17	18					1
7	16		5.37 2089	37 97 401	3.5	0	19	8	457 809	90 ?	5.37 ?	5.37 ?	15	16	73	89 97 437	89 97 44	3.5 A	0<3	18	17	577			0	
8	15		5.17 269	5.17 76	3	1	22	5	249721	318641	A ?	A ?	16	15	440	401 2801	401 119 120	3 A	3	19	16				1<3	
9	14		17 2273	17 7 ?	5	0<3	23	4	5.48733	5 A	5.121 7 ?	5.121 7 ?	17	14	313	105 993	105 993	3 A	0<3	22	13				0<3	
10	12		13 2137	13 41 53	3.11	0	25	2	13 32857	13 91	13 91	13 91	18	13	313	5.389 457	5.322 123	A	3	24	11	73			3 ?	
11	11		5.89 757	5.89 757	3	11	0	26	5.73 1085	5 73	5.73	5.73	20	11	180	431 1801	421 125 126	5.73	2	27	8				3	
12	10		389 7 ?	389 7 ?	3.7	0	27	17	5.113 1393	5 13	5 13	5 13	21	10	150	13 17 8 128	13 17 8 128	3	2	27	8	233			3 A	
13	8		5.89 613	5.89 137	7	0	3	26	37 22013	37 94	37 94	37 94	22	9	97	283 2141	283 ?	5.97 ?	23	0	31	4	17 41		3 A	
14	9		13 15661	13 17	7	0	24	5	5.33 73	5 ?	5 ?	5 ?	24	7	569	5.97 61 273	5.97 ?	5.97 ?	0<2	29	6	457			0<2	
15	8		5.37 73	5.37 73	3 A	0<3	6	23	769	5.17 9213	5.769 ?	5.769 ?	23	6	17	13 093 313	13 093 313	5 ?	5	0	32	3	953		0<1	
16	7		5.17 237	5.17 237	3 A	1<3	6	24	5.17 9213	5.769 ?	5.769 ?	5.769 ?	26	5	17	4 23 281	17 11 129	5 ?	5	2	34	1	36		1<2	
17	6		5.17 237	5.17 237	3 A	1<3	6	24	5.17 9213	5.769 ?	5.769 ?	5.769 ?	28	3	97	4 33633	61 73	61 73	2	1	36				1	
18	5		5.17 237	5.17 237	3 A	1<3	6	24	5.17 9213	5.769 ?	5.769 ?	5.769 ?	28	3	97	5.96 269	5.132 A	5.132 A	2	2	35	1361			1	
19	4		5.17 237	5.17 237	3 A	1<3	6	24	5.17 9213	5.769 ?	5.769 ?	5.769 ?	28	3	97	5.96 269	5.132 A	5.132 A	2	2	35	1361			1	
20	3		5.17 237	5.17 237	3 A	1<3	6	24	5.17 9213	5.769 ?	5.769 ?	5.769 ?	28	3	97	5.96 269	5.132 A	5.132 A	2	2	35	1361			1	
21	2		5.17 237	5.17 237	3 A	1<3	6	24	5.17 9213	5.769 ?	5.769 ?	5.769 ?	28	3	97	5.96 269	5.132 A	5.132 A	2	2	35	1361			1	
22	1		5.17 237	5.17 237	3 A	1<3	6	24	5.17 9213	5.769 ?	5.769 ?	5.769 ?	28	3	97	5.96 269	5.132 A	5.132 A	2	2	35	1361			1	
23	1		5.17 237	5.17 237	3 A	1<3	6	24	5.17 9213	5.769 ?	5.769 ?	5.769 ?	28	3	97	5.96 269	5.132 A	5.132 A	2	2	35	1361			1	
24	2		5.17 237	5.17 237	3 A	1<3	6	24	5.17 9213	5.769 ?	5.769 ?	5.769 ?	28	3	97	5.96 269	5.132 A	5.132 A	2	2	35	1361			1	
25	1		5.17 237	5.17 237	3 A	1<3	6	24	5.17 9213	5.769 ?	5.769 ?	5.769 ?	28	3	97	5.96 269	5.132 A	5.132 A	2	2	35	1361			1	
26	2		5.17 237	5.17 237	3 A	1<3	6	24	5.17 9213	5.769 ?	5.769 ?	5.769 ?	28	3	97	5.96 269	5.132 A	5.132 A	2	2	35	1361			1	
27	3		5.17 237	5.17 237	3 A	1<3	6	24	5.17 9213	5.769 ?	5.769 ?	5.769 ?	28	3	97	5.96 269	5.132 A	5.132 A	2	2	35	1361			1	
28	4		5.17 237	5.17 237	3 A	1<3	6	24	5.17 9213	5.769 ?	5.769 ?	5.769 ?	28	3	97	5.96 269	5.132 A	5.132 A	2	2	35	1361			1	
29	5		5.17 237	5.17 237	3 A	1<3	6	24	5.17 9213	5.769 ?	5.769 ?	5.769 ?	28	3	97	5.96 269	5.132 A	5.132 A	2	2	35	1361			1	
30	6		5.17 237	5.17 237	3 A	1<3	6	24	5.17 9213	5.769 ?	5.769 ?	5.769 ?	28	3	97	5.96 269	5.132 A	5.132 A	2	2	35	1361			1	
31	7		5.17 237	5.17 237	3 A	1<3	6	24	5.17 9213	5.769 ?	5.769 ?	5.769 ?	28	3	97	5.96 269	5.132 A	5.132 A	2	2	35	1361			1	
32	8		5.17 237	5.17 237	3 A	1<3	6	24	5.17 9213	5.769 ?	5.769 ?	5.769 ?	28	3	97	5.96 269	5.132 A	5.132 A	2	2	35	1361			1	
33	9		5.17 237	5.17 237	3 A	1<3	6	24	5.17 9213	5.769 ?	5.769 ?	5.769 ?	28	3	97	5.96 269	5.132 A	5.132 A	2	2	35	1361			1	
34	10		5.17 237	5.17 237	3 A	1<3	6	24	5.17 9213	5.769 ?	5.769 ?	5.769 ?	28	3	97	5.96 269	5.132 A	5.132 A	2	2	35	1361			1	
35	11		5.17 237	5.17 237	3 A	1<3	6	24	5.17 9213	5.769 ?	5.769 ?	5.769 ?	28	3	97	5.96 269	5.132 A	5.132 A	2	2	35	1361			1	
36	12		5.17 237	5.17 237	3 A	1<3	6	24	5.17 9213	5.769 ?	5.769 ?	5.769 ?	28	3	97	5.96 269	5.132 A	5.132 A	2	2	35	1361			1	
37	13		5.17 237	5.17 237	3 A	1<3	6	24	5.17 9213	5.769 ?	5.769 ?	5.769 ?	28	3	97	5.96 269	5.132 A	5.132 A	2	2	35	1361			1	
38	14		5.17 237	5.17 237	3 A	1<3	6	24	5.17 9213	5.769 ?	5.769 ?	5.769 ?	28	3	97	5.96 269	5.132 A	5.132 A	2	2	35	1361			1	
39	15		5.17 237	5.17 237	3 A	1<3	6	24	5.17 9213	5.769 ?	5.769 ?	5.769 ?	28	3	97	5.96 269	5.132 A	5.132 A	2	2	35	1361			1	
40	16		5.17 237	5.17 237	3 A	1<3	6	24	5.17 9213	5.769 ?	5.769 ?	5.769 ?	28	3	97	5.96 269	5.132 A	5.132 A	2	2	35	1361			1	
41	17		5.17 237	5.17 237	3 A	1<3	6	24	5.17 9213	5.769 ?	5.769 ?	5.769 ?	28	3	97	5.96 269	5.132 A	5.132 A	2	2	35	1361			1	
42	18		5.17 237	5.17 237	3 A	1<3	6	24	5.17 9213	5.769 ?	5.769 ?	5.769 ?	28	3	97	5.96 269	5.132 A	5.132 A	2	2	35	1361			1	
43	19		5.17 237	5.17 237	3 A	1<3	6	24	5.17 9213	5.769 ?	5.769 ?	5.769 ?	28	3	97	5.96 269	5.132 A	5.132 A	2	2	35	1361			1	
44	20		5.17 237	5.17 237	3 A	1<3	6	24	5.17 9213	5.769 ?	5.769 ?	5.769 ?	28	3	97	5.96 269	5.132 A	5.132 A	2	2	35	1361			1	
45	21		5.17 237	5.17 237	3 A	1<3	6	24	5.17 9213	5.769 ?	5.769 ?	5.769 ?	28	3	97	5.96 269	5.132 A	5.132 A	2	2	35	1361			1	
46	22		5.17 237	5.17 237	3 A	1<3	6	24	5.17 9213	5.769 ?	5.769 ?	5.769 ?	28	3	97	5.96 269	5.132 A	5.132 A	2	2	35	1361			1	
47	23		5.17 237	5.17 237	3 A	1<3	6	24	5.17 9213	5.769 ?	5.769 ?	5.769 ?	28	3	97	5.96 269	5.132 A	5.132 A	2	2	35	1361			1	
48	24		5.17 237	5.17 237	3 A	1<3	6	24	5.17 9213	5.769 ?	5.769 ?	5.769 ?	28	3	97	5.96 269	5.132 A	5.132 A	2	2	35	1361			1	
49	25		5.17 237	5.17 237	3 A	1<3	6	24	5.17 9213	5.769 ?	5.769 ?	5.769 ?	28	3	97	5.96 269	5.132 A	5.132 A	2	2	35	1361			1	
50	26		5.17 237	5.17 237	3 A	1<3	6	24	5.17 9213	5.769 ?	5.769 ?	5.769 ?	28	3	97	5.96 269	5.132 A	5.132 A	2	2	35	1361			1	
51	27		5.17 237	5.17 237	3 A	1<3	6	24	5.17 9213	5.769 ?	5.769 ?	5.769 ?	28	3	97	5.96 269	5.132 A	5.132 A	2	2	35	1361			1	
52	28		5.17 237	5.17 237	3 A	1<3	6	24	5.17 9213	5.769 ?	5.769 ?	5.769 ?	28	3	97	5.96 269	5.132 A	5.132 A	2	2	35	1361			1	
53	29		5.17 237	5.17 237	3 A	1<3	6	24	5.17 9213	5.769 ?	5.769 ?	5.769 ?	28	3	97	5.96 269	5.132 A	5.132 A	2	2	35	1361			1	
54	30		5.17 237	5.17 237	3 A	1<3	6	24	5.17 9213	5.769 ?	5.769 ?	5.769 ?	28	3	97	5.96 269	5.132 A	5.132 A	2	2	35	1361			1	
55	31		5.17 237	5.17 237	3 A	1<3	6	24	5.17 9213	5.769 ?	5.769 ?	5.769 ?	28	3	97	5.96 269	5.132 A	5.132 A	2	2	35	1361			1	
56	32		5.17 237	5.17 237	3 A	1<3	6	24	5.17 9213	5.769 ?	5.769 ?	5.769 ?	28	3	97	5.96 269	5.132 A	5.132 A	2	2	35	1361			1	
57	33		5.17 237	5.17 237	3 A	1<3	6	24	5.17 9213	5.769 ?	5.769 ?	5.769 ?	28	3	97	5.96 269	5.132 A									

Table 7 (continued)

Table with columns: m, n, K, M, #Δ, Δ, r, m, n, K, M, #Δ, Δ, r. Rows 33-41.

Table with columns: m, n, K, M, #Δ, Δ, r, m, n, K, M, #Δ, Δ, r. Rows 42-50.

Table with columns: m, n, K, M, #Δ, Δ, r, m, n, K, M, #Δ, Δ, r. Rows 51-59.

Table with columns: m, n, K, M, #Δ, Δ, r, m, n, K, M, #Δ, Δ, r. Rows 60-68.

Table with columns: m, n, K, M, #Δ, Δ, r, m, n, K, M, #Δ, Δ, r. Rows 69-77.

Table with columns: m, n, K, M, #Δ, Δ, r, m, n, K, M, #Δ, Δ, r. Rows 78-86.

Table with columns: m, n, K, M, #Δ, Δ, r, m, n, K, M, #Δ, Δ, r. Rows 87-95.

Table with columns: m, n, K, M, #Δ, Δ, r, m, n, K, M, #Δ, Δ, r. Rows 96-104.

Table with columns: m, n, K, M, #Δ, Δ, r, m, n, K, M, #Δ, Δ, r. Rows 105-113.

Table with columns: m, n, K, M, #Δ, Δ, r, m, n, K, M, #Δ, Δ, r. Rows 114-122.

Table with columns: m, n, K, M, #Δ, Δ, r, m, n, K, M, #Δ, Δ, r. Rows 123-131.

Table with columns: m, n, K, M, #Δ, Δ, r, m, n, K, M, #Δ, Δ, r. Rows 132-140.

Table with columns: m, n, K, M, #Δ, Δ, r, m, n, K, M, #Δ, Δ, r. Rows 141-149.

Table with columns: m, n, K, M, #Δ, Δ, r, m, n, K, M, #Δ, Δ, r. Rows 150-158.

Table with columns: m, n, K, M, #Δ, Δ, r, m, n, K, M, #Δ, Δ, r. Rows 159-167.

Table with columns: m, n, K, M, #Δ, Δ, r, m, n, K, M, #Δ, Δ, r. Rows 168-176.

Table with columns: m, n, K, M, #Δ, Δ, r, m, n, K, M, #Δ, Δ, r. Rows 177-185.

Table with columns: m, n, K, M, #Δ, Δ, r, m, n, K, M, #Δ, Δ, r. Rows 186-194.

Table with columns: m, n, K, M, #Δ, Δ, r, m, n, K, M, #Δ, Δ, r. Rows 195-203.

Table with columns: m, n, K, M, #Δ, Δ, r, m, n, K, M, #Δ, Δ, r. Rows 204-212.

Table with columns: m, n, K, M, #Δ, Δ, r, m, n, K, M, #Δ, Δ, r. Rows 213-221.

Table with columns: m, n, K, M, #Δ, Δ, r, m, n, K, M, #Δ, Δ, r. Rows 222-230.

Table with columns: m, n, K, M, #Δ, Δ, r, m, n, K, M, #Δ, Δ, r. Rows 231-239.

Table with columns: m, n, K, M, #Δ, Δ, r, m, n, K, M, #Δ, Δ, r. Rows 240-248.

Table with columns: m, n, K, M, #Δ, Δ, r, m, n, K, M, #Δ, Δ, r. Rows 249-257.

Table with columns: m, n, K, M, #Δ, Δ, r, m, n, K, M, #Δ, Δ, r. Rows 258-266.

Table with columns: m, n, K, M, #Δ, Δ, r, m, n, K, M, #Δ, Δ, r. Rows 267-275.

Table 7 (concluded)

m	n	K	M	$\pm \delta$	Δ	r	Δ	m	n	δ	Δ	(a,b,c) or (A,B,C)	m	n	δ	Δ	(a,b,c) or (A,B,C)	
15	34		7068001	???	0<4			2	5		41	1,1,360	2	27	1105	25,1,384		
16	33	1889	513149829	513149	311 A	1		1	12	3		312,11,610008	4	25	809	271,4240		
17	32		52316917	5233		0		8	5		41	3,1,928	7	22	14	10612,961,25011213724		
18	31	1753	8054833	1753??	31	0<3		11	2	1241		6,1,1001	9	20	14	3,1,7168		
19	30	73	8017441	73 A??	5	1<3		12	1	1513		3,1,32	11	18	66	7613,3361588		
20	29	1601	53197761	53??	??	0<4		2	13	313		11,1,768	13	16	2	806,1,1117346		
22	27	1433	5153973	51433??	3	0<1		8	7	1649		9,4,295	16	13	26	88,1,85736		
23	26	17	7323313	17??	23	0<2		11	4	1105		7,1,1056	16	13	26	75352,851,573638792		
24	25	1248	1358077	13??	A	1<3		13	2	113		33,2,4277	18	11	2	186,1,16794		
25	24		171492797	17149210	3	1		41	16	41		7231,173,86601600	20	9	2	168,1,131736		
26	23	1049	52375306	51049??	23?	0<2		2	15	23069		11,384	21	6	337	1,1,1344		
29	22	41	561837	56135	3 A	2		13	4	26		13156,1475,3579082964	22	7	14	9460,107,638195892		
30	19	601	6119141	611914	19	2		18	6			138684,2853,174334974546	26	3	6	398,5,186986		
31	18		517371657	517??	A	0<3		8	11	2	17009	9921,1432592	28	1	14	904,1,312892		
32	17	353	5971917	5??	??	0<3		13,17,191600	9	10	30		476,1,1250516	1	30	30	3692,29,17277932	
33	16		4510273	A??	??	0<3		476,1,1250516	2	29	953		21,1,6160	2	29	953	42953,1359,2135624192	
34	15	89	4169521	8948??	3	1<3		318,5,417666	11	8	521		21,1,6160	3	28	7585	1,1,10752	
36	13		57389109	57389	313	0		1459,3,42959000	16	3	6		11,1,480	4	27	3961	73,5,24624	
37	12	337	51350273	513172	3 A	2		1459,3,42959000	4	17	409		23,1,312	5	26	65	28876,1301,40108730756	
38	11		10692837	1069 A	A	2		14,1,4953	8	13	185		14,1,4953	8	23	6	812,5,4464796	
39	10	641	2844481	641212??	3	1<3		47,1,34944	17	4	313		14,1,4953	13	18	27145	49,4,361767	
40	9	17	2712001	172047	3	2		44,1,16084	16	5	5		44,1,16084	14	17	173545	1,1,4056	
41	8		5528973	5??	??	0<1		11,1,1104	17	4	137		11,1,1104	15	16	7081	8,3,1309	
43	6	1297	5215273	5211297 A	3,43	1		24,1,91	16	5	137		24,1,91	16	15	180049	4,1,4725	
44	5		2938241	A??	??	1<3		10127,4029124	19	2	2		10127,4029124	19	12	457	1,1,336	
45	4	1797	3237601	17978	5,3	1		537,17,5325670	1	22	2		537,17,5325670	28	3	21	817,1782152	
46	3		53753373	537 A	3 A	2		35,1,11904	4	19	19		35,1,11904	5	28	2	1900,11,26140100	
47	2	2017	5841933	52017	47	0		1,1,600	6	17	457		1,1,600	8	25	5	35300,167,696137500	
48	1		17288689	17??	3	0<1		5,1,2294	18	5	3961		5,1,2294	10	23	115	2083,3,47096206	
								151,19,127968	22	1	11	5785		151,19,127968	16	17	761	83,1,155040
								1271,17,51696640	1	24				1271,17,51696640	577			55,1,23664
								5388,55,363701148	2	23	10489		5388,55,363701148	23	10	5	16316476,21631,688638413394096	
								2133,102494979	6	19	114		2133,102494979	29	4	593	19,1,9046	
								1394,57,27656	7	18	21		1394,57,27656	29	4	593	7621,29,37162940	
								469,47,23319816	9	16	6		469,47,23319816	32	1	65	7,1,5206	
								35008,50239,32057105403584	12	13	337		35008,50239,32057105403584	8905			16,1,35937	
								3037,4605310	17	8	34		3037,4605310	2	33	26	17482,2893,36504144662	
								294,1,351134	2	20	10		294,1,351134	16	19	19	160,9,7056032	
								1701428,4499,854051125732	7	25	10		1701428,4499,854051125732	18	17	577	163,1,592344	
								1553,13,26600640	10	17	5		1553,13,26600640	18	17	577	2196,1,30152340	
								16236,1,87648752	11	16	185		16236,1,87648752	26	9	39	191,13,559880	
								385,2,474845	16	11	11		385,2,474845	27	8	3961	85,1,44880	
								302,1,178454	20	7	5		302,1,178454	31	4	41	15,1,8680	
								41252,3639,92021083612	22	5	2		41252,3639,92021083612	31	4	41	85,1,44880	
								20,1,3531	23	4	46		20,1,3531	2	35	10	7011674,22809,269371681131806	
								44,7,83121	25	2			44,7,83121	5	32	2	101321920,118801,2216757072348480	
									26	1	6497			13	24	26	67548,1021,125051739852	

Auxiliary Table 8A. Additional solutions of (21) and (22)

m	n	δ	Δ	(a,b,c) or (A,B,C)	m	n	δ	Δ	(a,b,c) or (A,B,C)
7	1	85		8,1,420	45	103,40	237,1	4539836846460	
3	7	205		4,1,420	15	17	5		
1	11	5		821,5568	17	15	17		
1	13	485		1718,61,58412640	25	7	1241		
5	9	949		2,1,960	27	5	3		
7	9	21		135,1,89559	9	25	61		
15	1	1261		4,1,540	13	21	327		
1	17			2911792,284639,2733237019872	15	19	61		
1	19	5		11362900,1951,988436565788	5	31	5		
3	17	51		278290,14687,177241670556	11	25	55		
7	13	91		702,11,5627180	19	17	221		
9	11	1105		14,1,672	19	17	1517		
19	1	5		144,1,68	23	11	5		
3	19	19		1026,1,4616316	1	37	221		
5	17	1165		230,1,1798464	3	35	3		
7	17			4,1,13076	21	17	17		
7	15	21		415,2,821345	23	15	69		
9	13	13		595,41,20136655	27	11	793		
13	9	61		87,1,50683	1	39	157		
17	5	17		584,65,33604236	29	11	319		
21	1	21		185905,5878,39815228385	1	41	5		
1	23	41		2747,1655,2111818049	1	41	5		
5	19	19		213,2,81995	23	19	353		
5	19	305		293,4,1193553	25	17	17		
11	13	95		610,9,3687260	31	11	341		
13	11			1178,7,14376844	5	39	5		
13	11	13		2241070,7357,18816133011884	9	35	21		
17	7	119		583,9,3307843	13	31	13		
19	5	19		5713666,381713,1112713299940284	15	29	145		
1	25	1241		270,1,328420	3	43	17833		
9	17	14065		34,11,131040	7	39	3		
17	9	17		22,3,1704	11	35	77		
23	69			698,1843,359931520	13	33	11		
25	1	41		471,2,1008743	29	17	29		
13	15	39		381,11,182425	55	11	77		
15	13	39		6,1,33690	41	5	5		
17	11	11		1589047,3731,9270354645007	45	1	3		
23	5	5069		138,7,1381280	23	25	5		
25	3	3961		402,7,2394780	29	19	19		
27	1	337		469634,2677,1066684531692	29	19	19		
7	23	26065		324,43,399740	3	47	1105		
11	19	5		6,1,1760	7	43	1201		
29	1	5		14686,311,6532509856	23	27	69		
3	29	29		95,12,673463	27	23	69		
29	1	265		96,1,289852	29	21	109		
3	29	29		340,1,17748	41	9	1105		
				21663,7,2532055221	47	3	337		
				1553,22,7148115					