On two questions of Ono

By Qiang Lin[*)] and Takashi Ono[**)]

(Communicated by Shokichi Iyanaga, M. J. A., Dec. 12, 2002)

Abstract: We answer two questions on Pell's equations and periods of quadratic irrationals raised by the second author while computing some cohomology groups.

Key words: Pell's equation; continued fraction.

1. Question one on fundamental unit.

In [4, §5], Ono compared certain non-abelian cohomology groups of congruence group $\Gamma_0(\ell)$ with that of $\Gamma_1(\ell)$, where ℓ is a prime $\equiv 3 \bmod 4$. During the investigation, he suspected that $\mathcal{U}(\Gamma_0(\ell)) = \mathcal{U}(\Gamma_1(\ell))$, which is, if stated in plainer language and more completely,

Theorem. *Let (x_0, y_0) be the fundamental solution to the Pell's equation*:

$$x^2 - y^2\ell = 1, \tag{1}$$

where ℓ is a prime number. Then $x_0 \equiv 1 \bmod \ell \Leftrightarrow \ell = 2$ or $\ell \equiv 7 \bmod 8$.

Note that since $x^2 - 1 \equiv 0 \bmod \ell$, we have $x \equiv \pm 1 \bmod \ell$. It turns out that the above beautiful theorem has been discovered before. See for example, [8]. Here we present an elementary proof:

Without loss of generality, the values of variables and each component of solutions we will refer to are positive integers.

"$\Leftarrow$": The case when $\ell = 2$ is trivial. Now we will prove for any $\ell \equiv 7 \bmod 8$, not necessarily prime, (1) has no solution with $x \equiv -1 \bmod \ell$. Suppose otherwise that we have $x = m\ell - 1$ for some (positive) integer m. Upon substitution we have

$$y^2 = m(m\ell - 2). \tag{2}$$

There are two cases.

Case one: m is odd. Then $(m, m\ell - 2) = 1$, which implies both m and $m\ell - 2$ are squares. Then $m \equiv 1 \bmod 8$ and hence, $m\ell - 2 \equiv 5 \bmod 8$, which is impossible as $m\ell - 2$ is a square.

Case two: $m = 2n$ for some integer n. Upon substitution, we have $y^2 = 4n(n\ell - 1)$. Since $(n, n\ell - 1) = 1$, both n and $n\ell - 1$ are squares. Then $n \equiv 0, 1, 4 \bmod 8$ and hence, $n\ell - 1 \equiv -1, 6, 3 \bmod 8$, which is again impossible as $n\ell - 1$ is a square. Thus we complete the "if" part.

"$\Rightarrow$": An inspection on the multiplicative group structure of solutions of the Pell's equation tells that if $x_0 \equiv 1 \bmod \ell$, so are all other solutions. So it suffices to show that there exists at least one (positive) solution to (1) with $x \equiv -1 \bmod \ell$ when $\ell \neq 2$ and $\ell \not\equiv 7 \bmod 8$.

There are two cases.

Case one: $\ell \equiv 1 \bmod 4$. Let (a, b) be such that $a^2 - b^2\ell = -1$. For example, by the elementary theory of continued fractions, (a, b) can be the $(k-1)$-th convergent of the continued fraction of $\sqrt{\ell}$, where k is the period of that continued fraction. Setting $m = 2b^2$, $y = 2ba$, we obtain a solution to (2) and hence also a desired solution to (1).

Case two: $\ell \equiv 3 \bmod 8$. Note that

$$(x_0 + 1)(x_0 - 1) = y_0^2\ell.$$

We claim that x_0 is an even number. Otherwise suppose x_0 is odd. Then $(x_0 + 1, x_0 - 1) = 2$ and hence, $x_0 \pm 1 = 2a^2\ell$ and $x_0 \mp 1 = 2b^2$ for some a, b. The upper signs can not hold as it would imply $b^2 \equiv -1 \bmod \ell$, a contradiction to $\ell \equiv 3 \bmod 8$ by reciprocity law. As for the lower signs, we would find $b^2 - a^2\ell = 1$, i.e., a solution (a, b) that is smaller than (x_0, y_0), which is impossible as (x_0, y_0) is the smallest solution.

Now that x_0 is an even number, $(x_0 + 1, x_0 - 1) = 1$. So $x_0 \pm 1 = a^2\ell$ and $x_0 \mp 1 = b^2$ for some a, b. The lower signs can not hold as it would imply $b^2 \equiv 2 \bmod \ell$, again a contradiction to $\ell \equiv 3 \bmod 8$ by reciprocity law. So the upper signs must hold. That is to say, $b^2 - a^2\ell = -2$. We then obtain a

2000 Mathematics Subject Classification. Primary 11D09, 11A55.

[*)] Department of Mathematics, California Institute of Technology, Pasadena, CA 91125, U. S. A.

[**)] Department of Mathematics, The Johns Hopkins University, Baltimore, Maryland 21218-2689, U. S. A.

Dedicated to Professor H. Stark on his 63rd birthday.

solution to (2), namely, $m = a^2$, $y = ab$, and hence also a desired solution to (1). This completes the "only if" part.

2. Question two on period length of continued fraction. The (simple) continued fraction of an irrational number is (eventually) periodic if and only if that number is a quadratic irrational, i.e., an irrational number in a real quadratic extension of **Q** (Lagrange, 1770). Ono was initially interested in the length $k = k(\ell)$ of the (shortest) periods of the continued fraction of $\sqrt{\ell}$, where ℓ is a prime number. In [5] he suggested that

$$k \equiv 0 \bmod 4 \ \text{ if } \ \ell \equiv 7 \bmod 8,$$
$$k \equiv 2 \bmod 4 \ \text{ if } \ \ell \equiv 3 \bmod 8.$$

In fact, the following is already proved by Lagrange (1770).

$$k \text{ is odd if } \ell = 2 \text{ or } \ell \equiv 1 \bmod 4.$$

As we expected this basic result was not news. See [2, Corollary 1] or [1]. However, we would like to present a proof that suggests a little more in this case.

Let k be even so $k = 2n + 2$ for some $n \geq 0$. By [6, Problem 7.20], we can write

$$\text{(3)} \qquad \sqrt{\ell} = \left[q_0; q_1, \ldots, q_n, q_{n+1}, q_n, \ldots, q_1, q_0, \frac{1}{\sqrt{\ell}}\right].$$

Note that throughout this article partial quotients of a continued fraction is indexed beginning with 0 which signifies the integral part of it.

Suppose $n = 0$, i.e., $\sqrt{\ell} = [q_0; \overline{r, 2q_0}]$, where $q_0 = \lfloor\sqrt{\ell}\rfloor$, then $\ell = q_0^2 + 2q_0/r$. So $r \mid 2q_0$. Since $k \neq 1$, $r \neq 2q_0$. Since ℓ is prime, $(q_0, 2q_0/r) = 1$ and hence $q_0 = r$. Being an odd number, $\ell = q_0^2 + 2 \equiv 3 \bmod 8$.

Now let $n > 0$. Let $[q_0, q_1, \ldots, q_n] = a_n/b_n$, $[q_0, q_1, \ldots, q_{n-1}] = a_{n-1}/b_{n-1}$. It is well-known that:

$$\text{(4)} \qquad a_n b_{n-1} - b_n a_{n-1} = (-1)^{n+1}.$$

We also know by [6, Problem 7.7] that $[q_n, \ldots, q_1, q_0] = a_n/a_{n-1}$, $[q_n, \ldots, q_1] = b_n/b_{n-1}$. So,

$$\left[q_n, \ldots, q_1, q_0, \frac{1}{\sqrt{\ell}}\right] = \frac{\frac{1}{\sqrt{\ell}}a_n + b_n}{\frac{1}{\sqrt{\ell}}a_{n-1} + b_{n-1}}.$$

The right hand side of equality (3) becomes

$$\frac{\left(\frac{1}{\sqrt{\ell}}a_n + b_n\right)\left(q_{n+1}a_n + a_{n-1}\right) + \left(\frac{1}{\sqrt{\ell}}a_{n-1} + b_{n-1}\right)a_n}{\left(\frac{1}{\sqrt{\ell}}a_n + b_n\right)\left(q_{n+1}b_n + b_{n-1}\right) + \left(\frac{1}{\sqrt{\ell}}a_{n-1} + b_{n-1}\right)b_n}.$$

Hence (3) implies two equalities, one being trivial and the other one being:

$$\text{(5)} \quad a_n(q_{n+1}a_n + 2a_{n-1}) = \ell b_n(q_{n+1}b_n + 2b_{n-1}).$$

Suppose $\ell \mid a_n$. As $(a_n, q_n a_n + 2a_{n-1}) = (a_n, 2) \mid 2$, we know $\ell \nmid q_{n+1}a_n + 2a_n$. Since $b_n(q_{n+1}a_n + 2a_{n-1}) - a_n(q_{n+1}b_n + 2b_{n-1}) = 2(b_n a_{n-1} - a_n b_{n-1}) = 2(-1)^n$, we know $(q_{n+1}a_n + 2a_{n-1}, q_{n+1}b_n + 2b_{n-1}) \mid 2$. Hence, from (5), we have

$$q_{n+1}a_n + 2a_{n-1} \mid 2b_n.$$

Then $a_n/b_n < 2$. However, a_n/b_n is a best approximation to $\sqrt{\ell}$. Hence, $\sqrt{\ell} < 2$. That is, $\ell = 2$ or 3 which is impossible as $k(2) = 1$ and $k(3) = 2$. So $\ell \nmid a_n$.

We know that $(a_n, b_n) = 1$. So from (5), we have

$$a_n \mid q_{n+1}b_n + 2b_{n-1}.$$

By [6, Problem 7.20], $q_{n+1} < \sqrt{\ell}$. Furthermore, $a_n > \sqrt{\ell}b_n - 1$ as a_n/b_n is a best approximation to $\sqrt{\ell}$. So if $\ell > 16$, we must have $2a_n > q_{n+1}b_n + 2b_{n-1}$ and hence from the divisibility above:

$$\text{(6)} \qquad a_n = q_{n+1}b_n + 2b_{n-1},$$

which can be easily verified for $\ell < 16$. Then combining with (5), we also have:

$$\text{(7)} \qquad \ell b_n = q_{n+1}a_n + 2a_{n-1}.$$

Hence,

$$\text{(8)} \quad a_n^2 - \ell b_n^2 = 2(a_n b_{n-1} - b_n a_{n-1}) = 2(-1)^{n+1}.$$

We know $\ell \neq 2$. If n is even, then $(-2/\ell) = 1$ and hence $\ell \equiv 1, 3 \bmod 8$ by reciprocity law. Checking (8) module 8, we see $\ell \equiv 1 \bmod 8$ is not possible. Hence, $\ell \equiv 3 \bmod 8$. Likewise, $\ell \equiv 7 \bmod 8$ if n is odd. This concludes our proof.

Readers may note that for $\ell \equiv 3 \bmod 8$, the pair (a_n, b_n) here is the same as the (a, b) in the last paragraph of the proof of the previous theorem.

We see that the equations (6) and (7) lead to (8), whose right hand side is determined by the class of $k \bmod 4$. In fact, there are stronger links among them as reflected by part of the following theorem. To set up, let ℓ be a non-square (positive) integer, not necessarily prime. $\sqrt{\ell} = [q_0, q_1, \ldots] = [q_0, \overline{q_1, \ldots, q_k}]$, where $q_0 = \lfloor\sqrt{\ell}\rfloor$ and $q_1, \ldots, q_k$ is the first (shortest) period. Let a_i/b_i be its i-th convergent, $i \geq 0$. Set $a_{-1} = 1$ and $b_{-1} = 0$. Then they satisfy (4) for $n \geq 0$ and

$$a_i = q_i a_{i-1} + a_{i-2} \quad \text{and} \quad b_i = q_i b_{i-1} + b_{i-2},$$

for $i > 0$. More over, a_i/b_i is a best approximation to $\sqrt{\ell}$ for $i \geq 0$.

The following theorem can be viewed as a variant of the celebrated theorem of Lagrange on the solution of $x^2 - y^2\ell = \pm 1$.

Theorem. *The following statements are equivalent for* $\ell \neq 2$.

(A) $x^2 - y^2\ell = \pm 2$ *is solvable.*

(B) $a_n^2 - b_n^2\ell = \pm 2$ *for some* n.

(C) k *is even and* $(a_n, \ell) = 1$ *where* $n = k/2 - 1 + tk$ *for some* $t \geq 0$.

(D) $a_n = q_{n+1}b_n + 2b_{n-1} = b_{n+1} + b_{n-1}$ *for some* $n \geq 0$.

(E) $\ell b_n = q_{n+1}a_n + 2a_{n-1} = a_{n+1} + a_{n-1}$ *for some* $n \geq 0$.

(F) $b_n \mid a_n - 2b_{n-1}$ *for some* $n > \frac{\log(5\ell)}{2\log((1+\sqrt{5})/2)} + 1$.

(G) $a_n \mid \ell b_n - 2a_{n-1}$ *for some* $n > 0$.

(H) $b_{n-1} \mid a_n - b_{n+1}$ *for some* $n > \frac{\log(5\ell)}{2\log((1+\sqrt{5})/2)} + 1$ *and* $1 < q_{n+1} \neq 2q_0$ *if* $\ell \neq 3, 7$.

(I) $a_{n-1} \mid \ell b_n - a_{n+1}$ *for some* $n > 0$ *and* $1 < q_{n+1} \neq 2q_0$ *if* $\ell \neq 3, 7$.

(J) *there is* $2\sqrt{\ell}/3 < q_{n+1} \neq 2q_0$ *for some* $n \geq 0$ *or* $\ell = 3, 7, 14, 23$.

Proof. To prepare for the proof, we recall the continued fraction algorithm applied to $\sqrt{\ell}$: Let $P_0 = 0$, $Q_0 = 1$ and recursively compute for $i \geq 0$:

$$q_i = \lfloor (P_i + \sqrt{\ell}\,)/Q_i \rfloor, \tag{9}$$

$$P_{i+1} = q_iQ_i - P_i, \tag{10}$$

$$Q_{i+1} = (\ell - P_{i+1}^2)/Q_i. \tag{11}$$

Then P_i, Q_i, q_i are positive integers except for P_0 and, moreover, the values of q_i's are actually the same as before. These three sequences are pure periodic with period length k if we ignore P_0 and q_0. $Q_i = 1$ if and only if $i = tk$ for some integer t, which in turn, if and only if $i = 0$ or $q_i = 2q_0$, which is the largest value of q_i's. We know $a_i^2 - b_i^2\ell = (-1)^{i+1}Q_{i+1}$ for all i and:

$$\max(0, \sqrt{\ell} - Q_i) < P_i < \sqrt{\ell} \quad \text{for} \quad i > 0. \tag{12}$$

Note that (12) and (9) implies that:

$$-2 < q_i - 2\sqrt{\ell}/Q_i < 0. \tag{13}$$

We also have the following two equalities that are fundamental to our proof.

$$a_i = P_{i+1}b_i + Q_{i+1}b_{i-1} \quad \text{for} \quad i \geq 0, \tag{14}$$

$$\ell b_i = P_{i+1}a_i + Q_{i+1}a_{i-1} \quad \text{for} \quad i \geq 0. \tag{15}$$

All above can be found in [3, §2.1]. In particular, (14) and (15) are special cases of [3, Exer. 2.1.2 (g)]. To facilitate the proof, we introduce two more conditions (K) and (L):

(K) $Q_{n+1} = 2$ for some $n \geq 0$.

(L) $P_{n+1} = q_{n+1}$ for some n and it is greater than 1 if $\ell \neq 3, 7$.

(A)⇔(B): If $\ell > 4$, this is an application of the often-called Legendre's theorem [3, Exer. 2.1.10 (b)]. Check directly for $\ell = 3$ using $1^2 - 1^2 \cdot 3 = -2$ and $2^2 - 1^2 \cdot 3 = 1$.

(B)⇔(K): because $a_i^2 - b_i^2\ell = (-1)^{i+1}Q_{i+1}$.

(B)⇔(C): The "⇐" part is the essence of what we have proved as above with n replaced by $a_{k/2-1+tk}$. The "⇒" part is a special case of [3, Thm. 6.1.4, p. 193] and in fact, $|a_{k/2-1+tk}^2 - b_{k/2-1+tk}^2\ell| = 2$ for all $t \geq 0$. Also see [7, §4 Lemma 1].

(K)⇒(J): By (13), $q_{n+1} > \sqrt{\ell} - 2$, which is greater than $2\sqrt{\ell}/3$ if $\ell > 36$. Check directly for $\ell < 36$.

(J)⇒(K): Check directly for $\ell = 3, 7, 14, 23$. Now assume $2\sqrt{\ell}/3 < q_{n+1} \neq 2q_0$. The last inequality implies $Q_{n+1} \neq 1$. By (13), $Q_{n+1} < 2\sqrt{\ell}/q_{n+1} < 3$. So $Q_{n+1} = 2$.

(K)⇒(L): (12) becomes $-2 < P_{n+1} - \sqrt{\ell} < 0$. Hence by (9), $q_{n+1} = P_{n+1}$. Verify that if $\ell < 9$, then $\ell = 2, 3, 5, 7$ and $Q_{n+1} = q_{n+1} = 2$ for even n if $\ell = 6$. Furthermore, by (13), $q_{n+1} > \sqrt{\ell} - 2 > 1$ for $\ell > 9$.

(L)⇒(K): $Q_1, Q_3 = 2$ for $\ell = 3, 7$, respectively. Now we assume $P_{n+1} = q_{n+1} > 1$. By (12), $\sqrt{\ell} = P_{n+1} + cQ_{n+1}$ for some $0 < c < 1$. By (9),

$$P_{n+1} < 2P_{n+1}/Q_{n+1} + c < P_{n+1} + 1.$$

Hence, $1 < Q_{n+1} < 4$. If $Q_{n+1} = 2$, we are done. Now assume $Q_{n+1} = 3$. Then $P_{n+1}/3 < c < 1$. Hence, $P_{n+1} = 2$. By (10), $P_{n+2} = 4$. By (11), $\ell = P_{n+2}^2 + Q_{n+1}Q_{n+2} = 16 + 3Q_{n+2}$. On the other hand, $\ell < (P_{n+1} + Q_{n+1})^2 = 25$. So $\ell = 19, 22$. For $\ell = 19, 22$, $Q_3 = 2$.

(K)⇒(D), (E), (F), (G), (H), (I): By the periodicity of P's and q's, we can assume n is sufficiently large and hence we are done as we have (14) and (15).

(F)⇒(K): By induction, $b_i \geq F_i$ for $i > 0$, where F_i is the Fibonacci numbers. The condition on n is to ensure that $F_{n-1} \geq \lfloor \sqrt{\ell} \rfloor$. So $b_{n-1} \geq \lfloor \sqrt{\ell} \rfloor$. Note that b_n and b_{n-1} are coprime as we have (4). So the Diophantine equation

$$a_n = xb_n + yb_{n-1} \tag{16}$$

has only one solution such that $0 < x < \sqrt{\ell}$.

Since $n > 2$, $b_n > b_{n-1}$. Hence (F) and (14) implies that $Q_{n+1} \neq 1$. So (14) shows that $a_n - 2b_{n-1} > 0$, i.e., the assumption (F) provides one such solution. Since we also have (14), $Q_{n+1} = 2$.

(G)⇒(K): Note that $a_{n-1} \geq a_0 = \lfloor\sqrt{\ell}\rfloor$. The rest is similar to that of (F)⇒(K).

(H), (I)⇒(K): Note that $a_{n+1} = q_{n+1}a_n + a_{n-1}$, $b_{n+1} = q_{n+1}b_n + b_{n-1}$. We obtain (L) by argument similar to the previous ones. Hence (K).

(D)⇒(K): Check directly for $n = 0$. Now let $n > 0$. $q_{n+1} < (a_n - 1)/b_n < \sqrt{\ell} < 2q_0$. The middle inequality holds as a_n/b_n is a best approximation to $\sqrt{\ell}$. If $n = 1$, $q_{n+1} + 2 \geq a_n/b_n > \sqrt{\ell}$; if $n > 1$, $q_{n+1} + 2 > a_n/b_n$ and again $q_{n+1} + 2 > \sqrt{\ell}$. Hence $q_{n+1} > 2\sqrt{\ell}/3$ for $\ell > 36$, which implies (K) through (J). For $\ell < 36$, it suffices to check for $n \leq 6$ by (F).

(E)⇒(K): Check directly if $n = 0$. If $n > 0$, then (E)⇒(G)⇒(K).

This concludes the proof of the theorem. Readers could try finding another two equivalent conditions similar to (H) and (I).

Note that the extra conditions to exclude small n can not be discarded. For example, let $\ell = 29$. Then we have $b_3 \mid a_3 - 2b_2$ however $x^2 - y^2 \cdot 29 = \pm 2$ is not solvable.

Also note the dummy index n throughout the statements and proof of the theorem is meant to be the same except for the extra conditions. For example, the proof of $(B) \Rightarrow (C)$ actually shows that if $a_n^2 - b_n^2\ell = \pm 2$ for some n, then k is even and the same $n = k/2 - 1 + tk$ for some $t \geq 0$. Since $a_i/b_i < \sqrt{\ell}$ for even i and $a_i/b_i > \sqrt{\ell}$ for odd i, we have the following link alluded before: if $x^2 - y^2\ell = \epsilon \cdot 2$ is solvable, then $k \equiv \epsilon - 1 \bmod 4$, where $\ell \neq 2$ and $\epsilon = \pm 1$.

The general picture of our theorem is that when we have (A) for $\ell \neq 2$, then k is even and if $n = k/2 - 1 + tk$ for some $t \geq 0$, then we have (B), (D), (E), (K) and $P_{n+1} = P_{n+2} = q_{n+1}$ = the largest integer less than $\sqrt{\ell}$ and having the same parity as ℓ. The last equality can be observed, say, from [6, Table 3, p. 339] and its proof is left to the readers. Among the many families of ℓ's that (A) holds, we list here four: $m^2 - 2$ for $m \geq 2$, $m^2 + 2$ for $m \geq 1$, $2p^i$ and p^{2i-1} for prime $p \equiv 3 \bmod 4$ and positive i. □

A similar theorem can be established for a non-square even $\ell \neq 12$ such that $x^2 - y^2\ell = \pm 4$ has a primitive solution, i.e., y is odd. We exclude odd ℓ to make sure that k is even. For $\ell = 12$, there is a solution $x = 4$, $y = 1$ that is not a convergent of the continued fraction of $\sqrt{12}$. Note that the above condition for ℓ is satisfied if $4 \mid \ell$ and $x^2 - y^2\ell/4 = -1$ has a solution. Among the many families of such ℓ's, we list here two: $m^2 - 4$ for even $m \geq 3$, $4p^{2i-1}$ for prime p and positive i.

References

[1] Friesen, C.: Legendre symbols and continued fractions. Acta Arith., **59** (4), 365–379 (1991).

[2] Halter-Koch, F.: Über Pellsche Gleichungen und Kettenbrüche. Arch. Math. (Basel), **49** (1), 29–37 (1987).

[3] Mollin, R. A.: Quadratics. CRC Press, Boca Raton-New York-London-Tokyo (1996).

[4] Ono, T.: On certain exact sequences for $\Gamma_0(m)$. Proc. Japan Acad., **78A**, 83–86 (2002).

[5] Ono, T.: An email to H. Stark. August 10 (2002).

[6] Rose, H. E.: A Course in Number Theory. Oxford Univ. Press, Oxford (1988).

[7] Williams, H. C.: Some results concerning the nearest integer continued fraction expansion of $\sqrt{D}$. J. Reine Angew. Math., **315**, 1–15 (1980).

[8] Yamamoto, Y.: On the class number problem of quadratic fields. Sugaku, **40**, 167–174 (1988). (In Japanese).