Hang Lung Mathematics Awards
Vol. 7 (2016)

Hang Lung Mathematics Awards 2016

Honorable Mention

Congruences of Solutions of the Pell's Equation

Team member: Man Yi Kwok
Teacher: Mr. Kim Fung Lee
School: Baptist Lui Ming Choi Secondary School

Hang Lung Mathematics Awards
Vol. 7 (2016), pp. 77–85

CONGRUENCES OF SOLUTIONS OF THE PELL'S EQUATION

TEAM MEMBER
Man Yi Kwok

TEACHER
Mr. Kim Fung Lee

SCHOOL
Baptist Lui Ming Choi Secondary School

Abstract. In this research, we are interested in how the solutions of the famous Pell's equation look like. It is well known that the solutions of the Pell's equation are generated by the fundamental solution of the equation, which could be represented by a set of recursive equations. Therefore, we would like to explore the characteristics of such recurrence sequences and tell the relationship between the cycle length of the congruence modulo a number and divisibility of the terms.

1. Introduction

Recursive sequences has been extensively studied by mathematicians. Among linear homogeneous recurrence sequences of order 2, divisibilities of some famous sequences such as the Fibonacci sequence and the Lucas sequence have been studied well. This paper would concentrate on a certain type of recurrence relations, namely, those which could generate solutions of the Pell's equation, and investigate the divisibilities of the terms.

The research explored the possible cycle length of the congruences of the recurrence relation generated by the Pell's equation $x^2 - Dy^2 = 1$. In the first place, we found the general formulation of the solutions of the Pell's equation by a recurrence relation, namely, the n-th large solution of the Pell's equation, (x_n, y_n), could be represented by $\left(\frac{1}{2}(\alpha^n + \beta^n), \frac{1}{2\sqrt{D}}(\alpha^n - \beta^n)\right)$. We then explore what would happen when the recurrence is put under modulo a prime and find that the minimum cycle $m(p)$ is exactly the multiplicative order of the two roots of the characteristic equation of the recurrence sequence. [See reviewer's comment (2) and (3)] We further find that if $4 \mid m(p)$, then $x_{\frac{m(p)}{4}}$ would be the minimum term divisible by p, and $p \mid x_n$ if and only if $n \equiv \frac{m(p)}{4} \pmod{\frac{m(p)}{2}}$, and this result could be generalised to any odd number k instead of a prime p. Finally, if the least multiple of two odd

numbers among the sequence are the same, then their multiples in the sequence are precisely the same.
I would like to thank my teacher Mr. Lee Kim Fung and my friend Ching Tak Wing for inspirations of this paper.

2. The Pell's equation

For any positive integer D which is not a square, there are infinitely many pairs of integral solution of the Pell's equation $x^2 - Dy^2 = 1$, given by $x_n + y_n\sqrt{D} = \left(x_1 + y_1\sqrt{D}\right)^n$, where (x_1, y_1) is the minimal non-trivial solution of the equation (which exists)[1]. From $x_{n+1} + y_{n+1}\sqrt{D} = \left(x_1 + y_1\sqrt{D}\right)\left(x_n + y_n\sqrt{D}\right) = (x_1x_n + Dy_1y_n) + (y_1x_n + x_1y_n)\sqrt{D}$ we have the following recurrence relations: [See reviewer's comment (4)]

$$x_{n+1} = x_1x_n + Dy_1y_n \tag{1}$$

$$y_{n+1} = y_1x_n + x_1y_n \tag{2}$$

Therefore, by substituting (1) into (2), we obtain $x_{n+2} - x_1x_{n+1} = Dy_1^2x_n + x_1(x_{n+1} - x_1x_n)$, so $x_{n+2} = 2x_1x_{n+1} + (Dy_1^2 - x_1^2)x_n$, and finally, [See reviewer's comment (5)]

$$x_{n+2} = 2x_1x_{n+1} - x_n \tag{*}$$

which is a linear homogeneous recurrence relation of order 2 with initial conditions $(x_0, y_0) = (1, 0)$, x_1 and y_1. Therefore, if $\alpha > \beta$ (as $x_1 \neq 1, \alpha \neq \beta$) are the roots of the characteristic equation $t^2 - 2x_1t + 1 = 0$, the general solution of x_n would be $A\alpha^n + B\beta^n$ for some number A and B such that $A + B = 1$ and $A\alpha + B\beta = x_1$.[4] From $\alpha + \beta = 2x_1$ and the above equations we have $A = B = \frac{1}{2}$. Therefore,

$$x_n = \frac{1}{2}(\alpha^n + \beta^n)$$

and

$$y_n = \sqrt{\frac{x_n^2 - 1}{D}} = \frac{1}{2\sqrt{D}}(\alpha^n - \beta^n)$$

3. Congruences mod p

We would now consider the equations taken modulo an odd prime p. This gives rise to a problem: could α and β exist mod p? Consider the characteristic equation $t^2 - 2x_1t + 1 \equiv 0 \pmod p \iff (t - x_1)^2 \equiv x_1^2 - 1 \equiv Dy_1^2 \pmod p$. Therefore, the quadratic equation has roots in $\mathbb{F}_p$ if and only if Dy_1^2 is a quadratic residue mod p. We would separate the cases of whether p divides y_1 or not.
If $p \mid Dy_1^2$, that means this equation has a double root in $\mathbb{F}_p$, namely $t \equiv x_1 \pmod p$, where $x_1 \equiv 1$ or -1 (mod p). Hence $x_n \equiv x_1^n(A + Bn) \pmod p$. After solving

$1 \equiv x_0 \equiv A \pmod{p}$ and $x_1 \equiv x_1(A+B) \pmod{p}$, this gives $A \equiv 1 \pmod{p}$, $B \equiv 0 \pmod{p}$, and

$$x_n \equiv x_1^n \pmod{p}.$$

If not (as what would actually happen in general), then there are solutions in $\mathbb{F}_p$ if and only if D is a quadratic residue mod p. [See reviewer's comment (6)] If D is not a quadratic residue mod p, we could actually consider a *field extension* of $\mathbb{F}_p$[2]:

Lemma 1. *There exist elements α, β in the field $\mathbb{F}_{p^2}$ such that they are the solutions of*

$$t^2 - 2x_1 t + 1 \equiv 0 \pmod{p}.$$

Proof. Since $t^2 - 2x_1 t + 1 \equiv 0 \pmod{p} \iff (t - x_1)^2 \equiv x_1^2 - 1 \equiv Dy_1^2 \pmod{p}$, we only need to show that there exists some element $i \in \mathbb{F}_{p^2}$ such that $i^2 \equiv D \pmod{p}$ as α and β would then be given by some linear combination of elements in $\mathbb{F}_{p^2}$. We have $i^{p^2} \equiv i^{p^2-1} i \equiv (i^2)^{(p-1)(\frac{p+1}{2})} i \equiv (D^{p-1})^{\frac{p+1}{2}} i \equiv i$, the statement is true since $x \in \mathbb{F}_{p^2} \iff x^{p^2} - x \equiv 0 \pmod{p}$. □

Hence, we know that for the recurrence relation, we would have the following:

Proposition 2. *If $x_{n+2} = 2x_1 x_{n+1} - x_n$, then for any prime p, if $x_1^2 \not\equiv 1 \pmod{p}$, we have*

$$x_n \equiv A\alpha^n + B\beta^n \pmod{p}$$

for $A, B, \alpha, \beta \in \mathbb{F}_{p^2}$ such that $\alpha + \beta \equiv 2x_1 \pmod{p}$ and $\alpha\beta \equiv 1 \pmod{p}$.

[See reviewer's comment (7)]

Proof. Since α and β are well defined and we could see division as taking the multiplicative inverse mod p, the same formula of the general solution of the original recurrence relations could be still applicable when considering modulo p. □

By solving $A + B \equiv x_0 \equiv 1 \pmod{p}$ and $A\alpha + B\beta \equiv x_1$, we find that $A \equiv B \equiv \frac{1}{2} \pmod{p}$ (here $\frac{1}{2}$ represents the multiplicative inverse of 2 mod p). Therefore,

Corollary 3. *If $x_{n+2} = 2x_1 x_{n+1} - x_n$, then for any prime p, we have*

$$x_n \equiv \frac{1}{2}(\alpha^n + \beta^n) \pmod{p}$$

for some distinct α and β satisfying $t^2 - 2x_1 t + 1 \equiv 0 \pmod{p}$.

4. The Cycle

For every odd prime p, since there are only finitely many possible pairs of (x_n, x_{n+1}) mod p (namely, at most p^2 pairs), so there must exist some $i < j$ such that $x_i \equiv x_j \pmod p$ and $x_{i+1} \equiv x_{j+1} \pmod p$. Therefore, since each term is recursively defined solely by the previous two terms, we could conclude that $x_{i+n} \equiv x_{j+n} \pmod p$ for every positive n. Moreover, since we could determine the previous terms from the recurrence relations too, $x_{i-n} \equiv x_{j-n} \pmod p$ for every positive n. So we finally have the following: [See reviewer's comment (8)]

Lemma 4. *For any prime p, there exists a positive integer d such that*

$$x_0 \equiv x_d \pmod p \text{ and } x_1 \equiv x_{d+1} \pmod p$$

Definition 5. *Let $m(p)$ be the minimum number satisfying $x_0 \equiv x_{m(p)} \pmod p$ and $x_1 \equiv x_{m(p)+1} \pmod p$. [See reviewer's comment (9)]*

Proposition 6. *For all positive integers d satisfying $x_0 \equiv x_d \pmod p$ and $x_1 \equiv x_{d+1} \pmod p$, we have $m(p) \mid d$.*

Proof. If not, by the division algorithm, we may let $d = m(p)q + r$ for some integers q and r such that $0 \leq r \leq m(p) - 1$. Then $x_{m(p)q} \equiv x_d \pmod p$ and $x_{m(p)q+1} \equiv x_{d+1} \pmod p$. Subtracting $m(p)q$ in the subscripts implies $x_0 \equiv x_r \pmod p$ and $x_1 \equiv x_{r+1} \pmod p$, contradicting to the minimality of $m(p)$.[3] □

Corollary 7. *For any positive integer i and j, $x_i \equiv x_j \pmod p$ and $x_{i+1} \equiv x_{j+1} \pmod p$ are both satisfied if and only if $i \equiv j \pmod{m(p)}$.*

If $x_1 \equiv 1 \pmod p$, then $x_n \equiv 1^n \equiv 1 \pmod p$ for all n; if $x_1 \equiv 1 \pmod p$, then $x_{2n} \equiv 1^n \equiv 1 \pmod p$ for all n, i.e. $x_n \equiv 1 \pmod p$ if and only if n is even. If $x_1^2 \not\equiv 1 \pmod p$, then $\alpha \not\equiv \beta \pmod p$. From the general formula, we obtain $1 \equiv \frac{1}{2}(\alpha^{m(p)} + \beta^{m(p)}) \pmod p \iff 1 - \alpha^{m(p)} \equiv \beta^{m(p)} - 1 \pmod p \iff \alpha(1 - \alpha^{m(p)}) \equiv \alpha(\beta^{m(p)} - 1) \pmod p$ and $\frac{1}{2}(\alpha + \beta) \equiv \frac{1}{2}(\alpha^{m(p)+1} + \beta^{m(p)+1}) \pmod p \iff \alpha(1 - \alpha^{m(p)}) \equiv \beta(\beta^{m(p)} - 1) \pmod p$. Combining the two congruences we necessarily have $\beta^{m(p)} \equiv 1 \pmod p$. Since α is the multiplicative inverse of β, we also have $\alpha^{m(p)} \equiv 1 \pmod p$. On the other hand, if $\beta^d \equiv 1 \pmod p$ for some positive integer d, we have $\alpha^d \equiv 1$, so $1 \equiv \frac{1}{2}(\alpha^d + \beta^d) \pmod p$ and $\frac{1}{2}(\alpha + \beta) \equiv \frac{1}{2}(\alpha^{d+1} + \beta^{d+1}) \pmod p$, so $m(p) \mid d$. Therefore, we know that $m(p)$ is the *minimum* positive integer such that $\alpha^{m(p)} \equiv \beta^{m(p)} \equiv 1 \pmod p$. [See reviewer's comment (10)]

Proposition 8. *The minimum length of the congruence cycle of the recurrence relation is the multiplicative order of α and β mod p.*

From the fact that $\alpha \in \mathbb{F}_{p^2}$, we know $\alpha^{p^2-1} \equiv 1 \pmod p$. Therefore, we van conclude that

$$m(p) \mid p^2 - 1.$$

In the above arguments, we omitted the prime 2. In fact, we can take $A = B = \frac{1}{2}$ in the general solution of recurrence sequences because we are considering an odd modulo. Modulo 2 gives $x_{n+2} \equiv x_n \pmod 2$ for all non-negative integer n. Therefore, the parity of the solutions of x_i only depends on the parity of i, in particular, for all even i, we have $x_i \equiv x_0 \equiv 1 \pmod 2$. Therefore, we have

$$2 \nmid x_{2n}$$

for all non-negative integer n. What it remains would be the terms x_i that i is odd. If D is even, by considering the parity of the original equation $x^2 - Dy^2 = 1$, we have $x_n \equiv 1 \pmod 2$ for all n. However, if x_1 is even, then for all odd n, $2 \mid x_n$.

5. How if ... not a prime?

If we are considering the modulo of a prime power, or even an arbitrary positive integer, we also have a similar conclusion: if we consider the roots of the characteristic equation mod p^m, we have $t^2 - 2x_1 t \equiv 0 \pmod{p^m} \iff (t - x_1)^2 \equiv x_1^2 - 1 \equiv Dy_1^2 \pmod{p^m}$. [See reviewer's comment (11)] We need the following lemma first:

Lemma 9. *If there exists some $k \in \mathbb{F}_{p^2}$ such that $D \equiv k^2 \pmod p$, and $p \nmid Dy_1^2$, for all positive integer n, we have $D \equiv k_n^2 \pmod{p^n}$ for some k_n in the extension of the reduced residue class modulo p^n. (This implies that D is a quadratic residue mod p^n if and only if it is a residue mod p.)*

Proof. We would proceed by mathematical induction. When $n = 1$, the statement is trivial. Assume that $D \equiv k_r^2 \pmod{p^r}$ for some r, and assume $k_r^2 \equiv sp^r + D \pmod{p^{r+1}}$ for some integer $0 \le s \le p - 1$. Since there exist a number t such that $s \equiv -2k_r t \pmod p$ (by considering the multiplicative inverse of $-2k_r \bmod p$, which is in the field $\mathbb{F}_{p^2}$), we have $(k_r + tp^r)^2 \equiv k_r^2 + 2tk_r p^r \equiv (s + 2tk_r)p^r + D \equiv D \pmod{p^{r+1}}$ as desired. □

Therefore, since the powers of the roots α and β still have a limited possible congruences mod p^n, there must still exist distinct positive integers $i < j$ such that $\alpha^i \equiv \alpha^j \pmod{p^n}$, which means there exist some d such that $\alpha^d \equiv 1 \pmod{p^n}$. For an arbitrary positive integer n, by the (extended) Chinese remainder theorem, we would still have a proper definition of α and β, and there exists a positive integer d such that $\alpha^d \equiv 1 \pmod n$ if and only if Dy_1^2 and n are co-prime. Therefore, we can extend the definition of $m(p)$ to positive integers:

Definition 10. *$m(n)$ is the least positive integer such that $x_0 \equiv x_{m(n)} \pmod n$ and $x_1 \equiv x_{m(n)+1} \pmod n$.*

If so, we would also have a similar conclusion alike proposition 6: For all positive integer d satisfying $x_0 \equiv x_d \pmod n$ and $x_1 \equiv x_{d+1} \pmod n$, we have $m(n) \mid d$. Otherwise, we could find a smaller number that satisfies the condition by the division algorithm, hence a contradiction. Since there exists a number, namely $4d$,

that makes $\beta^{4d} \equiv 1 \pmod{n}$, we can conclude that *for all odd divisor n of x_d for any d*, $\gcd(n, Dy_1^2) = 1$. Moreover, we have a similar conclusion of the divisibility of the terms in the recurrence sequence:

Lemma 11. *If a term x_d has an odd divisor n, then*

$$n \mid x_{(2m+1)d}$$

for all non-negative integer m.

6. Divisibility

Now consider an arbitrary odd number n such that there exists some positive integer d such that $n \mid x_d$ and $\gcd(n, Dy_1^2) = 1$, we have $0 \equiv \frac{1}{2}(\alpha^d + \beta^d) \pmod{n} \iff -\alpha^d \equiv \beta^d \pmod{n}$. Therefore we have $\beta^{2d} \equiv -1 \pmod{n}$ and $\beta^{4d} \equiv 1 \pmod{n}$. Hence, we must have

$$m(n) \mid 4d \text{ and } m(n) \nmid 2d.$$

From this we have $4 \mid m(n)$. On the other hand, for any odd number n such that $4 \mid m(n)$, since $\left(\beta^{\frac{m(n)}{2}}\right)^2 \equiv 1 \pmod{n}$, we have $\left(\beta^{\frac{m(n)}{2}} - 1\right)\left(\beta^{\frac{m(n)}{2}} + 1\right) \equiv 0 \pmod{n}$. From the minimality of $m(n)$ tells us that $\beta^{\frac{m(n)}{2}} - 1 \not\equiv 0 \pmod{n}$. This gives $\beta^{\frac{m(n)}{2}} \equiv -1 \pmod{n}$ and $\beta^{\frac{m(n)}{4}} \equiv \alpha^{\frac{m(n)}{4}} \beta^{\frac{m(n)}{2}} \equiv -\alpha^{\frac{m(n)}{4}}$. As a result, we have the following:

Proposition 12. *For any odd n which is co-prime with Dy_1^2, there exits a positive integer d such that $n \mid x_d$ if and only if $4 \mid m(n)$. Moreover, for all positive integer k, $p \mid x_n$ if and only if $\frac{m(n)}{4} \mid k$ and $\frac{m(n)}{2} \nmid k$.*

Corollary 13. *If $4 \mid m(k)$ for some odd k, $p \mid x_n$ if and only if $n \equiv \frac{m(k)}{4}$ (mod $\frac{m(k)}{2}$).*

How if $\gcd(n, Dy_1^2)$ is not 1? We discussed the situation that for a prime p such that $p \mid Dy_1^2$, we have $x_n \equiv x_1^n \pmod{p}$. Therefore, the terms in the sequence $\{x_n\}$ are never divisible by p, and hence not divisible by n. By these, we have the lemma here:

Lemma 14. *If a term x_d has an odd divisor n, then*

$$n \mid x_{(2m+1)d}$$

for all non-negative integer m.

This means if there exists two odd numbers i and j such that they divides x_d for some d, then $4d$ is a common cycle when the recurrence equation is in modulo i and j. Therefore, $4d$ is divisible by both $m(i)$ and $m(j)$. Moreover, if $m(i) = m(j)$, we have

$$i \mid x_n \iff j \mid x_n.$$

Corollary 15. *If the least multiples of two odd positive integers i and j among the sequence $\{x_n\}$ are the same, then the recurrence sequence have the same cycle modulo i and j, and $i \mid x_n \iff j \mid x_n$.*

7. General Recurrence Relations

From this, what we actually did is studying the solutions of the linear homogeneous recurrence relations of order 2 when the constant term in the characteristic equation is 1. In general, if product of the roots of the characteristic equation does not equal to 1, then there will still be cycles when we take mod due to the limited number of possible congruences, and the minimum cycle is still the multiplicative order of the two roots (!), as $A + B \equiv A\alpha^{m(p)} + B\beta^{m(p)} \pmod{p} \iff A\alpha(1 - \alpha^{m(p)}) \equiv -B\alpha(1 - \beta^{m(p)}) \pmod{p}$ and $A\alpha + B\beta \equiv A\alpha^{m(p)+1} + B\beta^{m(p)+1} \pmod{p} \iff A\alpha(1 - \alpha^{m(p)}) \equiv -B\beta(1 - \beta^{m(p)}) \pmod{p}$, which tells us that either $B \equiv 0 \pmod{p}$ (which means $A \equiv A\alpha^{m(p)} \pmod{p}$), $1 - \beta^{m(p)} \equiv 0 \pmod{p}$ or $\alpha \equiv \beta \pmod{p}$ (which means $A + B \equiv \alpha^{m(p)}(A + B) \pmod{p}$. In all the cases, we still have $m(p)$ would be the multiplicative order of at least one of α and β, and from $A + B \equiv A\alpha^{m(p)} + B\beta^{m(p)} \pmod{p}$ we know that $m(p)$ would be the multiplicative order of *both* α and β, even if they are not the multiplicative inverse of each other. However, when we study the divisibility of the terms of the sequence, the nice relationship between the minimum cycle and least multiple of p among the sequence could not hold.

8. Application and Conclusion

In this research, we find that the recurrence sequence that forms solutions for the Pell's equation is rather special that the cycle and the divisibility of the terms when modulo a certain number could be related in a simple way. Moreover, if a term has two co-prime odd divisors, we could determine that they have a common cycle when we take mod with respect to these two odd divisors. This new exploration could be applied to solve a group of Diophantine equations when they could be reduced to the Pell's equation. For example, for the Diophantine equation $a^{2x} = by^2 + 1$ with fixed a and b, we could consider the equations mod powers of a. When the power increases, we could know that, for sufficiently large k such that $a^m \mid x_k$ for some m, x_k would have another odd divisor d, and hence we obtain that $a^m \mid x_n \iff d \mid x_n$. This shows that this Diophantine equation has only a finite number of solutions.

While the solutions of Pell's equation $x^2 - Dy^2 = 1$ could be nicely represented by recurrence relations, the solutions of the generalisation, $x^2 - Dy^2 = n$, has a less neat formula and need to be represented by continuous fractions[1]. However, since the solutions of the Pell's equation is just the terms of a certain type of recurrence relations, the findings could be applicable to the divisibilities of recurrence relations

of type $x_n = Rx_{n-1} - x_{n-2}$. Nevertheless, knowing the divisibility and cycles of the solutions of the Pell's equation could be very useful.

REFERENCES

[1] Edward J. Barbeau, *Pell's Equation*, Springer-Verlag, New York, 2003.
[2] *Field Extension*, http://www.math.uiuc.edu/r-ash/Algebra/Chapter3.pdf
[3] Paul Erdős, János Surányi, *Topics in the Theory of Numbers*, Springer-Verlag, New York, 2003.
[4] Titu Andreescu, *Essential Linear Algebra with Applications*, Birkhäuser Basel, 2014.

Reviewer's Comments

Grammatical mistakes and typos

1. The reviewer has comments on the wordings, which have been amended in this paper.
2. a prime $\to$ an odd prime p
3. the multiplicative order $\to$ the least common multiple of the orders
4. integral solutions (x_n, y_n) of
5. (1) into (2) $\to$ (2) into (1)
6. If not (as what would actually happen in general), then there are solutions $\to$ If $p \nmid Dy_1^2$, then the quadratic equation has solutions
7. any prime $\to$ any odd prime
8. (namely, p^2 pairs)
9. minimum positive number
10. (The second one) if $x_1 \equiv 1 \pmod{p} \to x_1 \equiv -1 \pmod{p}$
11. odd prime power, or even an arbitrary odd positive integer

Comments

The author studied the solutions of the Pell's equation $x^2 - Dy^2 = 1$. He considered a recursive sequence arising from the equation and investigated its properties modulo an odd prime p. Some interesting results on the cycle length and divisibility properties were obtained. The author also tried to extend the results from p to an arbitrary odd number in general.

It is nice to see that tools from both number theory and algebra, such as field extension, were used. I would suggest going further in this direction. For example, the author studied the recursive sequence and the roots of its characteristic polynomial both integrally and modulo n. The relationship between the two cases would be made more transparent by regarding the numbers as elements of different rings and considering homomorphism between these rings.

Expressing the results using the language of algebra may also increase clarity. For instance, the mod p notation can be confusing. In the equation $\alpha^i \equiv \alpha^j \pmod{p^n}$, the two sides may not be integers or elements of $\mathbb{Z}/p^n$. A better way is to write the two sides as elements of some ring containing $\mathbb{Z}/p^n$.

Careful treatment should be given for the case when n is not a prime, since $\mathbb{Z}/n$ is no longer an integral domain. In other words, two elements a, b with product $ab = 0$ does not imply $a = 0$ or $b = 0$. More details should be provided for this part.

Finally I recommend the author to improve the readability of the article by numbering important equations for later referencing.