数理解析研究所講究録
1097 巻 1999 年 108-112

On a density of the set of primes dividing generalized Lucas sequences

By

Yoshifumi KOHNO and Bo Myoung OK

1. Introduction

In [3], J. C. Lagarias showed that the set of primes dividing certain second-order linear recurrences has positive density. A method of Hasse is used for his proof. In this note, we will reserch similar phenomena for the Pell sequence. Our result is a special case which was not treated in [2]. We need some preliminaries. Any irreducible second-order recurrence $\{U_n\}$ whose terms U_n are rational numbers can be expressed in the form $U_n = \alpha\theta^n + \bar{\alpha}\bar{\theta}^n$, where α and θ are in the quadratic field K generated by a root of characteristic polynomial of $\{U_n\}$, and $\bar{\xi}$ denotes the algebraic conjugate of a number ξ in K. Hasse's conditions are as followes;

(1) $\theta/\bar{\theta} = \pm\phi^k$, where $k = \pm 1$ or ± 2 for some ϕ in K,

(2) $\bar{\alpha}/\alpha = \pm\zeta\phi^j$, where ζ is a root of unity in K and j is an integer.

We put

$$\boldsymbol{P} = \{p; \text{all the prime numbers}\}, \qquad P_x = \{p; p \in \boldsymbol{P},\ p \leq x\},$$

$$S_U = \{p; p \in \boldsymbol{P},\ p|U_n \text{ for some } n\}, \qquad S_{U,x} = \{p; p \in S_U,\ p \leq x\}.$$

These particular recurrences $\{U_n\}$, which satisfy the above conditions (1) and (2), have a specific property which enables us to decompose S_U into disjoint countable union of Chebotarev sets of primes.

Definition 1. A set Σ of primes is a Chebotarev set if there is some finite normal extension L of the rationals $\boldsymbol{Q}$ such that a prime p is in Σ if and only if the Artin symbol $\left[\frac{L/\boldsymbol{Q}}{(p)}\right]$ is in specified conjugacy classes of the Galois group $Gal(L/Q)$.

Then we can define the density $d(S_U)$ as follows.

Definition 2. The density $d(S_U)$ is defined

$$d(S_U) = \lim_{x\to\infty} \frac{\sharp S_{U,x}}{\sharp P_x}, \quad \text{where } \sharp P_x \sim \frac{x}{\log x}.$$

If a sequence $\{U_n\}$ is defined by $U_0 = 2, U_1 = m$ and $U_n = mU_{n-1} + U_{n-2}$ $(n \geq 2)$, then $\{U_n\}$ is called a generalized Lucas sequence. In this case, the characteristic polynomial is $x^2 - mx - 1 = 0$.

2. Main Results

Theorem 1[2]. Let $D = m^2 + 4$ be an odd prime discriminant of $\boldsymbol{Q}(\sqrt{D})$. Then for the sequence $\{U_n\}$ $(U_0 = 2, U_1 = m,\ U_n = mU_{n-1} + U_{n-2})$, the set S_U of primes has density $d(S_U) = \frac{2}{3}$.

Theorem 2. For the Pell sequence $\{P_n\}$ $(P_0 = 1, P_1 = 1,\ P_n = 2P_{n-1} + P_{n-2})$, the set S_P of primes has density $d(S_P) = \frac{17}{24}$.

For the proof, we can use the same Hasse's method based on the Frobenius density theorem as in the case of Theorem 1.

Proof. The Pell sequences $\{P_n\}$ satisfies

$$P_n = \frac{1}{2}\{\varepsilon^n + \bar{\varepsilon}^n\},$$

where $\varepsilon = 1 + \sqrt{2}$. In this case Hasse's method is useful. Hence

$$p|P_n \ \Leftrightarrow\ \varepsilon^n + \bar{\varepsilon}^n \equiv 0 \pmod{p} \ \Leftrightarrow\ \theta^n \equiv -1 \pmod{p},$$

where $\theta = -\varepsilon^2$ and the congruences are in the ring $\boldsymbol{Z}[\sqrt{2}]$ of algebraic integers in $\boldsymbol{Q}(\sqrt{2})$. Thus S_P is just the following set of primes

$$S_P = \{p; \exists x \in \boldsymbol{Z} \text{ such that } \theta^x \equiv -1 \pmod{(p)}\}.$$

If $p \equiv \pm 1 \pmod 8$, then (p) splits into two conjugate degree 1 prime ideals in $\boldsymbol{Q}(\sqrt{2})$, while if $p \equiv \pm 3 \pmod 8$, then (p) is a degree 2 prime ideal in $\boldsymbol{Q}(\sqrt{2})$.

Let $S_P = S_A \bigcup S_B$, where

$$S_A = \{p; p \equiv \pm 1 \pmod 8 \text{ and } p \in S_P\}$$

and

$$S_B = \{p; p \equiv \pm 3 \pmod 8 \text{ and } p \in S_P\}.$$

Case 1. The primes in S_A are separated into the following disjoint sets.

$$S_A = S_{Aa}^{(1)} \cup \bigcup_{j\geq 3} S_A^{(j)},$$

where

$$S_{Aa}^{(1)} = \{p; p \equiv -1 \pmod 8 \text{ and } p \in S_P\}$$

$$S_A^{(j)} = \left\{p; p \equiv 1 + 2^j \pmod{2^{j+1}} \text{ and } p \in S_U\right\} \text{ for } j \geq 1.$$

We consider the associate Kummer extensions over $\boldsymbol{Q}$;

$$K_j = \boldsymbol{Q}\left(\sqrt[2^j]{1}, \sqrt{2}, \sqrt[2^j]{\theta}\right), \quad L_j = \boldsymbol{Q}\left(\sqrt[2^{j+1}]{1}, \sqrt{2}, \sqrt[2^j]{\theta}\right).$$

Then $K_j = C_j(\sqrt[2^j]{\theta})$ for $C_j = \boldsymbol{Q}(\sqrt[2^j]{1})$ and we get for $j \geq 3$

$$[K_j : \boldsymbol{Q}] = \left[C_j(\sqrt[2^j]{\theta}) : \boldsymbol{Q}\right] = 2^{2j-2}, \quad [L_j : \boldsymbol{Q}] = 2^{2j-1}.$$

Let $P^{(j)} = \left\{p; p \equiv 1 + 2^j \pmod{2^{j+1}} \text{ and } p \in \boldsymbol{P}\right\}$ and $\overline{S_A^{(j)}} = P^{(j)} \setminus S_A^{(j)}$, then the primes in $\overline{S_A^{(j)}}$ are exactly the primes that split completely in K_j but not in L_j. Then the density of $\bigcup_{j\geq 3} S_A^{(j)}$ is $\sum_{j\geq 3}\left(\frac{1}{2^j} - \left(\frac{1}{[K_j : \boldsymbol{Q}]} - \frac{1}{[L_j : \boldsymbol{Q}]}\right)\right) = \frac{5}{24}$. Moreover the density of $S_{Aa}^{(1)}$ is $\frac{1}{4}$.

Case 2. Put $S_{Ab}^{(1)} = S_A^{(1)} \setminus S_{Aa}^{(1)}$. Then S_B is composed of $S_B^{(1)} \cup S_B^{(2)}$,

where

$$S_B^{(1)} = \{p; p \equiv -3 \pmod 8 \text{ and } p \in S_B\} = S_A^{(2)},$$

and

$$S_B^{(2)} = \left\{p; p \equiv -1 + 2^2 \pmod{2^3} \text{ and } p \in S_B\right\} = S_{Ab}^{(1)}.$$

Then the set $S_B^{(1)}$ is empty and the density of $S_B^{(2)}$ is $\frac{1}{4}$. From both cases we have the result.

Remark. We can compare with the density by the statistics computed on the 2400 prime numbers. Recently we were noticed that P. Moree and P. Stevenhagen obtained the same results as ours in [4].

Acknowledgments. The authors would like to express their sincere thanks to Mr. R. Takeuchi at Tokyo Metropolitan University for reference [4].

References

[1] B. J. BIRCH, *Cyclotomic Fields and Kummer Extensions*, Algebraic Number Fields (J. W. S. Cassels and A. Fröhlich, Eds.), Academic Press, London 1967, 85-93.

[2] Y. KOHNO, T. NAKAHARA and B. OK, *On a density of the set of primes dividing the generalized Fibonacci numbers*, Number theory and its Applications, Kyoto Univ., RIMS Kokyuroku **1060** (1998), 172-175.

[3] J. C. LAGARIAS, *The set of primes dividing the Lucas numbers has density* 2/3, Pacific J. Math. **118** (1985), 449-461; Errata: ibid. **162**(1994), 393-397.

[4] P. MOREE and P. STEVENHAGEN *Prime divisors of Lucas sequences*, Acta Arith. **82**, 1997, 403–410.

In the following table, D, I, N, and V denote a prime number for $\boldsymbol{Q}\left(\sqrt{D}\right)$, the length of the period of (resp. the suffix i of the first term $P_i \equiv 0 (\mathrm{mod}\ D)$ in) the Pell sequence $\{P_n\}$ modulo D for $P(3) \neq 0$ (resp. $P(3) = 0$), $\sharp S_{P,\ D}$, and $\sharp P_D$ respectively. Here $P(1)$, $P(2)$, $P(3)$, denote three consequtive terms in the Pell sequence $\{P_n\}$ modulo D.

We show several experimental data on Theorem 2 by Fortran 77.

Experiments by Fortran 77 for the sequence $\{P_n\}$ ($P_n = 2P_{n-1} + P_{n-2}$, $P_0 = 1$, $P_1 = 1$).

```
D=      2   P(3)= 1   I=      1   P(1)=      1   P(2)=      1   N=    0   V=      1
D=      3   P(3)= 0   I=      2   P(1)=      1   P(2)=      1   N=    1   V=      2
D=      5   P(3)= 3   I=     12   P(1)=      1   P(2)=      1   N=    1   V=      3
D=      7   P(3)= 0   I=      3   P(1)=      1   P(2)=      3   N=    2   V=      4
D=     11   P(3)= 0   I=      6   P(1)=      6   P(2)=      8   N=    3   V=      5
D=     13   P(3)= 3   I=     28   P(1)=      1   P(2)=      1   N=    3   V=      6
D=     17   P(3)= 0   I=      4   P(1)=      3   P(2)=      7   N=    4   V=      7
D=     19   P(3)= 0   I=     10   P(1)=      7   P(2)=      6   N=    5   V=      8
D=     23   P(3)= 0   I=     11   P(1)=     13   P(2)=      5   N=    6   V=      9
D=     29   P(3)= 3   I=     20   P(1)=      1   P(2)=      1   N=    6   V=     10
D=     31   P(3)= 0   I=     15   P(1)=     15   P(2)=      8   N=    7   V=     11
D=     37   P(3)= 3   I=     76   P(1)=      1   P(2)=      1   N=    7   V=     12
D=     41   P(3)= 0   I=      5   P(1)=      7   P(2)=     17   N=    8   V=     13
D=     43   P(3)= 0   I=     22   P(1)=     32   P(2)=     27   N=    9   V=     14
D=     47   P(3)= 0   I=     23   P(1)=     33   P(2)=      7   N=   10   V=     15
D=     53   P(3)= 3   I=    108   P(1)=      1   P(2)=      1   N=   10   V=     16
D=     59   P(3)= 0   I=     10   P(1)=     46   P(2)=     36   N=   11   V=     17
D=     61   P(3)= 3   I=    124   P(1)=      1   P(2)=      1   N=   11   V=     18
D=     67   P(3)= 0   I=     34   P(1)=     40   P(2)=     47   N=   12   V=     19
D=     71   P(3)= 0   I=     35   P(1)=     24   P(2)=     59   N=   13   V=     20
D=     73   P(3)= 0   I=     18   P(1)=     24   P(2)=     61   N=   14   V=     21
D=     79   P(3)= 0   I=     13   P(1)=     61   P(2)=      9   N=   15   V=     22
D=     83   P(3)= 0   I=     42   P(1)=     65   P(2)=      9   N=   16   V=     23
D=     89   P(3)= 0   I=     22   P(1)=      9   P(2)=     40   N=   17   V=     24

... ... 200 prime numbers are omitted ... ...

D=   1427   P(3)= 0   I=    714   P(1)=    434   P(2)=   1210   N=  159   V=    225
D=   1429   P(3)= 3   I=   2860   P(1)=      1   P(2)=      1   N=  159   V=    226
D=   1433   P(3)= 0   I=    358   P(1)=   1103   P(2)=    165   N=  160   V=    227
D=   1439   P(3)= 0   I=    719   P(1)=   1054   P(2)=    912   N=  161   V=    228
D=   1447   P(3)= 0   I=    241   P(1)=    931   P(2)=    258   N=  162   V=    229
D=   1451   P(3)= 0   I=    242   P(1)=   1072   P(2)=    915   N=  163   V=    230
D=   1453   P(3)= 3   I=   2908   P(1)=      1   P(2)=      1   N=  163   V=    231
D=   1459   P(3)= 0   I=    146   P(1)=   1351   P(2)=     54   N=  164   V=    232
D=   1471   P(3)= 0   I=     49   P(1)=    867   P(2)=    302   N=  165   V=    233
D=   1481   P(3)= 0   I=     74   P(1)=    630   P(2)=   1166   N=  166   V=    234
D=   1483   P(3)= 0   I=    742   P(1)=    275   P(2)=    604   N=  167   V=    235
D=   1487   P(3)= 0   I=    743   P(1)=    318   P(2)=   1328   N=  168   V=    236
D=   1489   P(3)= 0   I=    124   P(1)=    665   P(2)=    412   N=  169   V=    237
D=   1493   P(3)= 3   I=    996   P(1)=      1   P(2)=      1   N=  169   V=    238
D=   1499   P(3)= 0   I=    750   P(1)=     67   P(2)=    716   N=  170   V=    239
D=   1511   P(3)= 0   I=    755   P(1)=    807   P(2)=    352   N=  171   V=    240

... ... 2150 prime numbers are omitted ... ...

D=  21283   P(3)= 0   I= 10642   P(1)=   8815   P(2)=   6234   N= 1699   V=   2391
D=  21313   P(3)= 0   I=   296   P(1)=  17785   P(2)=   1764   N= 1700   V=   2392
D=  21317   P(3)= 3   I= 14212   P(1)=      1   P(2)=      1   N= 1700   V=   2393
D=  21319   P(3)= 0   I= 10659   P(1)=   1001   P(2)=  10159   N= 1701   V=   2394
D=  21323   P(3)= 0   I=  3554   P(1)=   7731   P(2)=   6796   N= 1702   V=   2395
D=  21341   P(3)= 3   I= 42684   P(1)=      1   P(2)=      1   N= 1702   V=   2396
D=  21347   P(3)= 0   I= 10674   P(1)=  10800   P(2)=  15947   N= 1703   V=   2397
D=  21377   P(3)= 0   I=  5344   P(1)=   6210   P(2)=  18272   N= 1704   V=   2398
D=  21379   P(3)= 0   I= 10690   P(1)=  15971   P(2)=   2704   N= 1705   V=   2399
D=  21383   P(3)= 0   I= 10691   P(1)=  18156   P(2)=  12305   N= 1706   V=   2400
9.45u 0.14s 0:43.77 21.9%
ultra:/work/home/nakahara%
```