PACIFIC JOURNAL OF MATHEMATICS
Vol. 173, No. 2, 1996

GROUP STRUCTURE AND MAXIMAL DIVISION FOR CUBIC RECURSIONS WITH A DOUBLE ROOT

Christian Ballot

An equivalence relation is defined on the set of recurring sequences with given cubic characteristic polynomial $f(X) = (X - \theta_1)^2(X - \theta_2) \in \mathbb{Z}[X]$ so that sequences in a class share the same maximal prime divisors. The set $G(f)$ of equivalence classes is shown to form a group structure by exhibiting an isomorphism φ between $G(f)$ and the Laxton group $G(f_1)$, where $f_1(X) = (X - \theta_1)(X - \theta_2)$ is the squarefree part of $f(X)$. The map φ has the additional property that the maximal prime divisors of a $\mathcal{U} \in G(f)$ are the prime divisors of $\varphi(\mathcal{U}) \in G(f_1)$.

§1. Introduction.

Laxton considered the set $F(f)$ of linear recurring sequences with terms in $\mathbb{Z}$ which have the same quadratic characteristic polynomial $f(X) \in \mathbb{Z}[X]$ (see [**Lax**]). If this polynomial is *non-degenerate*, that is, if the ratio of its two roots is not a root of unity, then Laxton defines a product of two sequences in $F(f)$, which makes $F(f)$ a semi-group with identity. The product is defined in such a way that if a prime p divides two sequences U and V, it also divides the product sequence $U \cdot V$. Here division by p of a sequence $U = \{u_n\}_{n=0}^{+\infty}$ means that there exists an n such that $p \mid u_n$, but $p \nmid u_{n+1}$. This type of division is called *proper* division. Laxton then defines an equivalence relation on the set $F(f)$. In words, two sequences which are rational multiples of one another or are merely shifts of each other are said to be equivalent. The product $\cdot$ defined on $F(f)$ is well-defined on the set $G(f)$ of equivalence classes. One can extend the notion of a prime p being a proper divisor of a sequence to a class of sequences in $G(f)$. The set $G(f)$ together with the binary operation $\cdot$ forms a group which preserves proper division by a prime p. In fact, Laxton shows that the subset $G(f, p)$ of classes that have p as a proper divisor forms a subgroup of $G(f)$.

In [**Ba**], all the results stated above are generalized to non-degenerate characteristic polynomials $f(X) \in \mathbb{Z}[X]$ of arbitrary degree $m \geq 2$ where proper division by a prime p becomes *maximal* division by a prime p. A prime p is a maximal divisor of an m^{th} order recurring sequence U if there exist m consecutive terms of U such that the first $m - 1$ are divisible by p, but the m^{th} one is not. The definition of maximal division was first proposed by Ward [**Wal**].

Certain classes of sequences in $G(f)$ have a set of maximal divisors having a natural density. Using a result of Schinzel [**Schi**], Somer [**So**] showed that the identity class in $G(f)$, which is the class of the sequence starting with $m-1$ zeros and a one, is the only class with density of maximal divisors equal to 1. In [**Ba**], results about the natural density of prime maximal divisors of sequences that have order two (in the group $G(f)$) are demonstrated.

The work [**Ba**] quoted above only dealt with non-degenerate characteristic polynomials. In this paper, we treat the simplest case of degeneracy, namely polynomials of the type

$$f(X) = (X - \theta_1)^2 g(X), \tag{1}$$

when the squarefree part $f_1(X) = (X - \theta_1)g(X)$ is non-degenerate.

The motivation came from a remarkable property of the Cullen numbers, which are the terms of the sequence

$$\{n\,2^n + 1\}_{n=0}^{\infty}. \tag{2}$$

Cullen numbers have been studied because their terms have an unusually large number of prime divisors (see [**Cu & Wo**] and [**Ro**]). Also, Hooley proved that almost all Cullen numbers are composite (see [**Hoo**]). But here we first observe that sequence (2) is a cubic recurring sequence with degenerate characteristic polynomial

$$f(X) = (X-2)^2(X-1) = X^3 - 5X^2 + 8X - 4. \tag{3}$$

To us, the remarkable property of the Cullen numbers $c_n = n\,2^n + 1$ is that every odd prime p is a maximal divisor of C. Indeed :

$$\begin{aligned} c_{p-2} &= (p-2)2^{p-2} + 1 \equiv -2^{p-1} + 1 \equiv 0 \mod p,\\ c_{p-1} &= (p-1)2^{p-1} + 1 \equiv -2^{p-1} + 1 \equiv 0 \mod p,\\ \text{but} \quad c_p &= p2^p + 1 \equiv 1 \not\equiv 0 \mod p. \end{aligned} \tag{4}$$

This property implies that the density of prime maximal divisors of the Cullen numbers is equal to 1. However, no Cullen number is equal to zero, so that sequence (2) is not equivalent in the sense of Laxton (see (6) below) to the identity sequence $[0,0,1]_f$. Hence, there are at least two non-equivalent sequences whose density of divisors is equal to one. This is unlike the non-degenerate cubic recursions, which we studied in [**Ba**, Chapter 4].

This observation prompted us to introduce an appropriate notion of equivalence, called weak equivalence (see (12), Section 3), for sequences whose characteristic polynomial is of type (1). As in the non-degenerate case, we are able to construct a group structure on the set $G(f)$ of weak equivalence classes, which preserves maximal division in the usual way. In fact, it then remains true that only sequences in the class of the identity $[0,0,1]$ have a set of maximal divisors of density one. In particular, the Cullen number sequence is weakly equivalent to the sequence $[0,0,1]$.

Moreover, in Section 3, we describe an isomorphism φ between the groups $G(f)$ and $G(f_1)$, which has the property that the maximal divisors of the class $Cl(U)$ of a sequence U in $F(f)$ correspond to the maximal divisors of the image class $\varphi(Cl(U))$. This correspondence enables us to obtain density results about sequences having degenerate characteristic polynomials $f(X)$ from the existing density results about sequences in $F(f_1)$. Some of these results are given in Section 4.

Section 5 is devoted exclusively to the Law of Apparition of maximal prime divisors in sequences which belong to the identity weak equivalence class. Note that Ward [**Wa2**] wrote about the laws of apparition and repetition in a cubic recurrence. However, his study was not confined to maximal division and dealt with rules having distinct roots.

Throughout the paper, our theorems are proved in the particular case of a cubic recursion $f(X) = (X - \theta_1)^2(X - \theta_2) \in \mathbb{Z}[X]$, but, in Section 6, we briefly state more general results that apply to an arbitrary characteristic polynomial $f(X) = (X - \theta_1)^2 g(X) \in \mathbb{Z}[X]$.

This article is merely a beginning of this subject, since we have studied only the simplest family of degenerate recursions, namely those with exactly one double root.

§2. Preliminaries.

Let us introduce some notation and recall some facts that will be of use here.

If $U = \{u_n\}_{n=0}^{\infty}$ is a recurring sequence with characteristic polynomial (or *rule*) in $\mathbb{Z}[X]$ of degree $m \geq 2$, then a prime p is said to be a *maximal divisor* of U at n (we will often write $p \mid_{max} U$ at n) if and only if

$$p \mid u_{n+i} \text{ for } 0 \leq i \leq m-2, \text{ but } p \nmid u_{n+m-1}. \tag{5}$$

In this article, we will only consider maximal prime divisors. Hence, saying that p is a *divisor* of U will mean that it is a maximal divisor of U. The set of divisors of a sequence U is denoted by $P(U)$ (or sometimes by $P_{max}(U)$ to emphasize the fact that the divisors are maximal). The *natural density* of this set, denoted by $\delta(U)$, is defined to be

$$\delta(U) = \lim_{X \to +\infty} \frac{|\{p \in P(U),\ p \leq X\}|}{\Pi(X)}, \text{ if it exists,}$$

where $\Pi(X) = |\{p \in \mathcal{P},\ p \leq X\}| \sim X/\log X$ and $\mathcal{P}$ is the set of all primes. Two sets of primes S and T are said to be *essentially the same* if and only if their symmetric difference $(S\backslash T) \cup (T\backslash S)$ is finite. We denote this by $S \approxeq T$. Note that if $S \approxeq T$, then their natural densities $\delta(S)$ and $\delta(T)$ are the same.

Since a recurring sequence U belonging to a rule $f(X)$ of degree m is entirely determined by its first m terms $u_0, u_1, \dots, u_{m-1}$, we will sometimes write

$$U = [u_0, u_1, \dots, u_{m-1}]_f = [u_0, u_1, \dots, u_{m-1}].$$

We now wish to be slightly more precise about the work of Laxton on quadratic rules than we were in the introduction. So let us assume that $f_1(X) = (X - \theta_1)(X - \theta_2) = X^2 - PX + Q \in \mathbb{Z}[X]$, where $Q \neq 0$ and f_1 is non-degenerate. A recurring sequence U with rule f_1 has the general term $u_n = \alpha\theta_1^n + \beta\theta_2^n$, where α and β are constants depending on u_0 and u_1. Laxton defined the set $F(f_1)$ to be the set of recurring sequences U with rule f_1 and terms in $\mathbb{Z}$ such that if we write $u_n = \alpha\theta_1^n + \beta\theta_2^n$, $\forall n \geq 0$, then $\alpha\beta \neq 0$. The n^{th} term u_n can also be written in the form

$$u_n = \frac{A\theta_1^n - B\theta_2^n}{\theta_1 - \theta_2}, \quad \forall n \in \mathbb{N},$$

where

$$\begin{cases} A = u_1 - u_0\theta_2, \\ B = u_1 - u_0\theta_1. \end{cases}$$

This gives us another way of denoting the sequence U, namely $U = \langle A, B\rangle$, which we call the *standard notation* for U.

Two sequences U and V in $F(f_1)$ are said to be *equivalent* (we write $U \sim V$) if and only if

$$\exists\lambda,\ \mu \in \mathbb{Z},\ \exists s \in \mathbb{Z},\ \forall n \in \mathbb{N}:\ \lambda u_{n+s} = \mu v_n, \tag{6}$$

that is, U and V are rational multiples of each other, or subscript shifts of one another. Laxton observed that the relation $\sim$ is an equivalence relation. The class of a sequence $U = \langle A, B\rangle = [u_0, u_1]$ is denoted by $\mathcal{U}$, or $Cl\,\langle A, B\rangle$ or $Cl\,[u_0, u_1]$. Laxton [**Lax**] showed that the set $G(f_1)$ of equivalence classes forms a group. If $U = \langle A_1, B_1\rangle$ and $V = \langle A_2, B_2\rangle$, then the group law is defined by

$$Cl\,\langle A_1, B_1\rangle \cdot Cl\,\langle A_2, B_2\rangle = Cl\,\langle A_1A_2, B_1B_2\rangle.$$

Clearly, the identity class is $Cl\,\langle 1, 1\rangle = Cl\,[0, 1]$, which is the famous Lucas sequence $L(\theta_1, \theta_2)(n) = (\theta_1^n - \theta_2^n)/(\theta_1 - \theta_2)$. Two equivalent sequences U and U' satisfy $P(U) \approxeq P(U')$. A prime p is said to be a *divisor* of the class $\mathcal{U}$ in

$G(f)$ if there exists a sequence U in the class $\mathcal{U}$ such that p is a divisor of U. The set of divisors of a class $\mathcal{U}$ is denoted by $P(\mathcal{U})$; in fact, for all sequences U in $\mathcal{U}$, we have $P(U) \approxeq P(\mathcal{U})$ (see Remark 4.4.3 in [**Ba**]).

Remark 1. We may and will assume that Laxton's set $F(f_1)$ includes sequences with terms in $\mathbb{Q}$ rather than in $\mathbb{Z}$. This will have no effect on group or density results in $G(f_1)$, if we agree that $p \mid a/b$, $a, b \in \mathbb{Z}$ and $(a,b) = 1$ when $p \mid a$, but $p \nmid b$. Indeed, note that for every sequence $[q_0, q_1]$, there exists a sequence $[z_0, z_1]$, where $z_0, z_1 \in \mathbb{Z}$ such that $[z_0, z_1] = N \cdot [q_0, q_1]$, where $N \in \mathbb{Z}$ is the least common multiple of the denominators of q_0, q_1, and so $[z_0, z_1] \sim [q_0, q_1]$.

§3. Cubic Recurrences with a Double Root : Group Structure.

Let

$$(7)\quad f(X) = (X-\theta_1)^2(X-\theta_2) = X^3 - PX^2 + QX - R \in \mathbb{Z}[X], \quad R \neq 0,$$

and note that reducibility necessarily implies that the roots θ_1, θ_2 are integers. We suppose $\theta_1 \neq \pm\theta_2$. Thus, the associated characteristic polynomial (or *rule*, to follow the terminology used in [**Ba**])

$$f_1(X) = (X-\theta_1)(X-\theta_2),$$

is non-degenerate.

Actually, for every rule of the type (7), there exists a recurring sequence satisfying a property analogous to (4). To find this sequence, we set

$$u_n = (\alpha n + \alpha')\theta_1^n + \beta\theta_2^n,$$

and solve the system of linear equations

$$\begin{cases} u_{p-2} \equiv 0 \mod p, \\ u_{p-1} \equiv 0 \mod p, \end{cases}$$

for α, α' and β, and for an arbitrary prime p. A solution of this system, which we will refer to as the *generalized Cullen sequence*, namely the sequence

$$(8)\qquad c_n = \left(\frac{n}{\theta_1-\theta_2} - \frac{2\theta_2-\theta_1}{(\theta_1-\theta_2)^2}\right)\theta_1^n + \frac{\theta_2}{(\theta_1-\theta_2)^2}\theta_2^n,$$

has the property that for all primes $p \nmid \theta_1\theta_2(\theta_1-\theta_2)$, we have

$$c_{p-2} \equiv c_{p-1} \equiv 0 \mod p, \text{ but } c_p \equiv 1 \not\equiv 0 \mod p.$$

As mentioned in the introduction, we will show how to define a group structure on the set $G(f)$ of equivalence classes of sequences that share the same cubic rule f. However, with the definition of equivalence that we will set, the sequences $\{c_n\}$ and $[0,0,1]_f$ will turn out to be in the same class. In fact, it will remain true that only sequences from the identity class have a density of divisors equal to one.

If we compute the closed form of the n^{th} term of the sequence $[0,0,1]_f$, we find that it is equal to

$$\left(\frac{n}{\theta_1(\theta_1-\theta_2)}-\frac{1}{(\theta_1-\theta_2)^2}\right)\theta_1^n+\frac{\theta_2^n}{(\theta_1-\theta_2)^2}.$$

Hence, we will say that a sequence U with rule f is in standard form when it is written as

$$\left(\frac{An}{\theta_1(\theta_1-\theta_2)}-\frac{A'}{(\theta_1-\theta_2)^2}\right)\theta_1^n+\frac{B\theta_2^n}{(\theta_1-\theta_2)^2}, \tag{9}$$

where the numbers A, A' and B depend on the initial values of U in the following way

$$\begin{bmatrix} A \\ A' \\ B \end{bmatrix} = \begin{bmatrix} \theta_1\theta_2 & -(\theta_1+\theta_2) & 1 \\ \theta_2(2\theta_1-\theta_2) & -2\theta_1 & 1 \\ \theta_1^2 & -2\theta_1 & 1 \end{bmatrix} \begin{bmatrix} u_0 \\ u_1 \\ u_2 \end{bmatrix}. \tag{10}$$

The matrix has determinant $(\theta_1-\theta_2)^3$. Since $\theta_1, \theta_2 \in \mathbb{Z}$ it follows that

$$A, A', B \in \mathbb{Q} \iff u_0, u_1, u_2 \in \mathbb{Q}.$$

For the sake of brevity we will write $U = \langle A, A', B\rangle$ instead of (9).

Definition. Let $F(f)$ be the set of sequences $U = \langle A, A', B\rangle$ with $A, A', B \in \mathbb{Q}$ such that the product $A \cdot B \neq 0$.

Theorem 2. *Let $U = \langle A, A', B\rangle \in F(f)$ and p be a prime. If $p \nmid AB\theta_1\theta_2(\theta_1-\theta_2)$, then we have*

$$\text{(11)} \quad p \textit{ is a maximal divisor of } U \iff \exists n \in \mathbb{N} : A\theta_1^n \equiv B\theta_2^n \mod p.$$

No prime divisor of $AB\theta_1\theta_2(\theta_1-\theta_2)$ divides U maximally.

Proof. Assume $\forall n \in \mathbb{N} : u_n = (\alpha n + \alpha')\theta_1^n + \beta\theta_2^n$. Hence, by (9) we have that

$$\alpha = \frac{A}{\theta_1(\theta_1-\theta_2)} \quad \text{and} \quad \beta = \frac{B}{(\theta_1-\theta_2)^2}.$$

First we prove statement (11).

$\Longrightarrow$)

$$\begin{aligned} p \,|_{max}\, U \text{ at } n &\Longleftrightarrow p \mid u_n,\ u_{n+1}, \text{ but not } u_{n+2}, \\ &\Longrightarrow u_n\theta_1 - u_{n+1} \equiv 0 \mod p. \end{aligned}$$

$$\begin{aligned} \text{But, } u_n\theta_1 - u_{n+1} \equiv 0 \mod p &\Longleftrightarrow \alpha\,\theta_1^{n+1} + \beta\,(\theta_2 - \theta_1)\,\theta_2^n \equiv 0 \mod p \\ &\Longleftrightarrow \frac{A}{\theta_1 - \theta_2}\,\theta_1^n \equiv \frac{B}{\theta_1 - \theta_2}\,\theta_2^n \mod p, \\ &\Longleftrightarrow A\,\theta_1^n \equiv B\,\theta_2^n \mod p. \end{aligned}$$

$\Longleftarrow$) Conversely, assume $\exists n \in \mathbb{N} :\ A\,\theta_1^n \equiv B\,\theta_2^n \mod p$. Then we have $\forall\lambda \in \mathbb{Z}$

$$l = n + \lambda(p-1) \Longrightarrow A\,\theta_1^l \equiv B\,\theta_2^l \mod p.$$

But, by the proof of $\Longrightarrow$), $A\,\theta_1^l \equiv B\,\theta_2^l$ is equivalent to $u_l\theta_1 - u_{l+1} \equiv 0 \mod p$. And so, to prove that p divides u_l and u_{l+1}, it is sufficient to show that $p \mid u_l = (\alpha l + \alpha')\,\theta_1^l + \beta\,\theta_2^l$.

Now, since $p \nmid \theta_1 - \theta_2$,

$$\begin{aligned} A\theta_1^n \equiv B\theta_2^n &\Longrightarrow \frac{\alpha\theta_1}{\theta_1 - \theta_2}\theta_1^n \equiv \beta\theta_2^n \\ &\Longrightarrow \frac{\alpha\theta_1}{\theta_1 - \theta_2}\theta_1^l \equiv \beta\theta_2^l, \text{ for any } l \text{ of the form } n + \lambda(p-1). \end{aligned}$$

$$\begin{aligned} \text{Hence, } p \mid u_l &\Longleftrightarrow p \mid (\alpha l + \alpha')\theta_1^l + \frac{\alpha\theta_1}{\theta_1 - \theta_2}\theta_1^l, \\ &\Longleftrightarrow p \mid (\alpha l + \alpha') + \frac{\alpha\theta_1}{\theta_1 - \theta_2} \quad \text{, since } p \nmid \theta_1. \end{aligned}$$

But $p \nmid A \Longrightarrow p \nmid \alpha$, so α has an inverse α^{-1} modulo p. And with $\gamma \equiv \alpha' + \dfrac{\alpha\theta_1}{\theta_1 - \theta_2} \mod p$, the integer l must satisfy

$$\begin{cases} l \equiv n \mod (p-1), \\ l \equiv -\gamma\alpha^{-1} \mod p. \end{cases}$$

Since p and $p - 1$ are coprime, the Chinese Remainder Theorem gives the existence of such an l.

Hence, we have shown that $\exists\, l \in \mathbb{N} :\ p \mid u_l,\ u_{l+1}$.

We have yet to prove that $p \nmid u_{l+2}$. Let us proceed by contradiction and assume that $p \mid u_{l+2}$. Then $p \mid u_{l+1},\ u_{l+2}$, which by the proof of $\Longrightarrow$), implies that $A\theta_1^{l+1} \equiv B\theta_2^{l+1}$. But since $A\theta_1^l \equiv B\theta_2^l$ and since $p \nmid AB\theta_1\theta_2$, it follows that $\theta_1 \equiv \theta_2 \mod p$, contradicting $p \nmid \theta_1 - \theta_2$.

So now let us assume that $p \mid AB\theta_1\theta_2(\theta_1 - \theta_2)$ and show that p cannot be a maximal divisor of U.

If $p \mid \theta_1$, then $\forall n \geq 0,\ u_n \equiv v_n \mod p$, where the terms $v_n = B\theta_2^n/(\theta_1 - \theta_2)^2$ form a geometric sequence. But p cannot divide two consecutive terms of $\{v_n\}$ without dividing the third consecutive one.

If $p \mid AB\theta_2(\theta_1 - \theta_2)$, then $\forall n \geq 0$, we have $u_n \equiv v_n \mod p$, where

$$\begin{cases} v_n = \dfrac{B\theta_2^n - A'\theta_1^n}{(\theta_1 - \theta_2)^2}, & \text{if } p \mid A, \\ v_n = \left(\dfrac{An}{\theta_1(\theta_1 - \theta_2)} - \dfrac{A'}{(\theta_1 - \theta_2)^2}\right)\theta_1^n, & \text{if } p \mid B\theta_2, \\ v_n = \left(\dfrac{An}{\theta_1(\theta_1 - \theta_2)} - \dfrac{B - A'}{(\theta_1 - \theta_2)^2}\right)\theta_1^n, & \text{if } p \mid (\theta_1 - \theta_2). \end{cases}$$

In each of the three cases above, $\{v_n\}$ is a recurring sequence of order two (with rule $f_1(X)$ in the first case, and rule $(X - \theta_1)^2$ in the second and third cases), so that if p divided two consecutive terms of $\{v_n\}$, then it would also divide all subsequent terms. This prevents p from being a maximal divisor of U. □

Remark. We have actually proved more than what Theorem 2 states. Indeed, if $p \mid_{max} U$ at n, then $A\theta_1^n \equiv B\theta_2^n \mod p$ (for the same n). For the converse, we only have :

$$A\theta_1^n \equiv B\theta_2^n \Longrightarrow \exists l = n + \lambda(p-1), \text{ for some } \lambda \in \mathbb{Z} \text{ such that } p \mid_{max} U \text{ at } l.$$

Let $U = \langle A, A', B\rangle \in F(f)$. As was shown when f is non-degenerate [**Ba**, Remark 4.4.3 & Prop. 5.4.4], sequences which are shifts or rational multiples of each other share essentially the same divisors. In fact, the same result holds true when f is degenerate. But for f of type (7) and $U = \langle A, A', B\rangle$ in $F(f)$, Theorem 2 also shows that the value of the number A' does not affect the set of divisors. This suggests a modified definition of equivalence, which not only allows shifting or multiplying by a rational scalar, but also changing the value of A'.

Definition. We will say that the sequences $U = \langle A, A', B\rangle$ and $V = \langle C, C', D\rangle$ are *weakly equivalent* (and write $U \sim V$) if and only if

$$\exists q \in \mathbb{Q},\ \exists s \in \mathbb{Z} \ : \quad \begin{cases} qA = C\theta_1^s, \\ qB = D\theta_2^s. \end{cases} \tag{12}$$

The relation $\sim$ is an equivalence relation on $F(f)$. The set of equivalence classes is denoted by $G(f)$. It is easy to check that the binary operation defined on $G(f)$ by :

$$\mathcal{U} \cdot \mathcal{V} = Cl\,\langle A, A', B\rangle \cdot Cl\,\langle C, C', D\rangle = Cl\,\langle AC, A'C', BD\rangle,$$

is well-defined.

Definition 3. Let us introduce the *projection map* $\varphi : G(f) \longrightarrow G(f_1)$ defined by $\varphi(Cl\,\langle A, A', B\rangle) = Cl\,\langle A, B\rangle$. First, observe that there exists $[u_0, u_1] = \langle A, B\rangle \in F(f_1)$. Indeed, A and B are in $\mathbb{Q}$, so that there exist u_0, $u_1 \in \mathbb{Q}$ satisfying

$$\begin{cases} A = u_1 - u_0\theta_2, \\ B = u_1 - u_0\theta_1, \end{cases}$$

since the determinant of the above system is $\theta_2 - \theta_1 \neq 0$. Now, note that φ is a well-defined map, since a shift of $\langle A, A', B\rangle$ is of the form $\langle A\theta_1^k, A'', B\theta_2^k\rangle$ for some $A'' \in \mathbb{Q}$ and $\langle A\theta_1^k, B\theta_2^k\rangle \sim \langle A, B\rangle$ in $F(f_1)$. A rational multiple of $\langle A, A', B\rangle$ is of the form $\langle \lambda A, \lambda A', \lambda B\rangle$ for some $\lambda \in \mathbb{Q}$, but $\langle \lambda A, \lambda B\rangle \sim \langle A, B\rangle$ in $F(f_1)$. Finally, the value of A' clearly does not affect the value of the image.

Theorem 4. *The projection map φ is an isomorphism from $(G(f), \cdot)$ onto $(G(f_1), \cdot)$.*

Proof. Since Definition 3 shows welldefinedness of φ, to show surjectivity, given $\langle A, B\rangle$ in $F(f_1)$, pick any A' in $\mathbb{Q}$ and note that

$$\varphi(Cl\langle A, A', B\rangle) = Cl\langle A, B\rangle.$$

Secondly φ is injective. If $\varphi(Cl\,\langle A, A', B\rangle) = \varphi(Cl\,\langle A_1, A_1', B_1\rangle)$, then

$$\begin{cases} A = \lambda A_1\theta_1^k, \\ B = \lambda B_1\theta_2^k, \end{cases}$$

where $\lambda \in \mathbb{Q}$ and $k \in \mathbb{Z}$. But by (12), this means that $\langle A, A', B\rangle \sim \langle A_1, A_1', B_1\rangle$, which implies that $Cl\,\langle A, A', B\rangle = Cl\,\langle A_1, A_1', B_1\rangle$.

Finally, φ is a homomorphism, since if $U = \langle A, A', B\rangle$ and $V = \langle A_1, A_1', B_1\rangle$, then $\varphi(Cl\,U \cdot Cl\,V) = \varphi(Cl\,\langle AA_1, A'A_1', BB_1\rangle) = Cl\,\langle AA_1, BB_1\rangle = Cl\,\langle A, B\rangle \cdot Cl\,\langle A_1, B_1\rangle = \varphi(Cl\,U) \cdot \varphi(Cl\,V)$. □

Corollary 5. *$(G(f), \cdot)$ is an abelian group.*

Proof. This follows from the fact that $(G(f_1), \cdot)$ is an abelian group (the Laxton group) and Theorem 4. □

Lemma 6. *Let $V = \langle A, B\rangle \in F(f_1)$ and p be a prime. Then*

$$p \text{ is a maximal divisor of } V \implies p \nmid AB\theta_1\theta_2(\theta_1 - \theta_2).$$

Proof. If $p \mid AB\theta_1\theta_2(\theta_1 - \theta_2)$, then modulo p the sequence V with terms $v_n = (A\theta_1^n - B\theta_2^n)/(\theta_1 - \theta_2)$ is a geometric sequence of the type $\{\alpha\theta^n\}_{n\geq 0}$, and hence we cannot have, for any $n \geq 0$, $v_n \equiv 0$ and $v_{n+1} \not\equiv 0 \mod p$. □

Lemma 7. *Let $U = \langle A, A', B\rangle \in F(f)$ and $V = \langle A, B\rangle \in F(f_1)$ and p be a prime. Then*

$$p \text{ is a maximal divisor of } U \iff p \text{ is a maximal divisor of } V.$$

Proof. $\implies$) If $p \in P(U)$, then, by Theorem 2, $A\theta_1^n \equiv B\theta_2^n \mod p$, for some n, and p does not divide $AB\theta_1\theta_2(\theta_1 - \theta_2)$. But $A\theta_1^n \equiv B\theta_2^n \mod p$ and $p \nmid (\theta_1 - \theta_2) \implies p \mid v_n$. Now if p also divided v_{n+1}, then the second congruence $A\theta_1^{n+1} \equiv B\theta_2^{n+1} \mod p$ would hold, which combined with the first one would imply, since $p \nmid AB\theta_1\theta_2$, that $\theta_1 \equiv \theta_2 \mod p$, a contradiction.

$\impliedby$) Use Lemma 6 and Theorem 2. □

As Laxton did for $G(f_1,p)$ (see Introduction above), we define $G(f,p)$ to be the set of weak equivalence classes having p as a divisor (i.e. the classes which have a representative having p as a divisor).

Theorem 8. *Let p be a prime. Then*

$$\varphi(G(f,p)) = G(f_1,p),$$

where φ is the projection map between $G(f)$ and $G(f_1)$.

Proof. Let $\mathcal{U} \in G(f,p)$. We must show that

$$\mathcal{U} \in G(f,p) \iff \varphi(\mathcal{U}) \in G(f_1,p).$$

But, $\mathcal{U} \in G(f,p) \iff p \in P(\mathcal{U}) \iff \exists U = \langle A, A', B\rangle \in \mathcal{U} : p \in P(U)$, which means that p is a maximal divisor of U. However, by Lemma 7, this says that p is a maximal divisor of $V = \langle A, B\rangle \in F(f_1)$, i.e. $p \in P(V) \iff p \in P(Cl\, V) = P(\varphi(Cl\, U)) = P(\varphi(\mathcal{U}))$. But,

$$p \in P(\varphi(\mathcal{U})) \iff \varphi(\mathcal{U}) \in G(f_1,p).$$ □

Remark. It is remarkable that Theorem 8 holds without any exceptional primes.

Corollary 9. *Let p be a prime number. Then $G(f,p)$ is a subgroup of $G(f)$.*

Proof. This follows immediately from the facts that φ is an isomorphism and $G(f_1,p)$ a subgroup of $G(f_1)$. □

Corollary 10.

$$P(\mathcal{U}) = P(\varphi(\mathcal{U})),\ \forall \mathcal{U} \in G(f).$$

Proof. This is a direct consequence of Lemma 7. □

§4. Application to Density Results.

Letting $h(X)$ be the cubic rule $(X-\theta_1)(X-\theta_2)^2$, where θ_2 is the double root and not θ_1, Theorem 4 says that $G(h)$ is isomorphic to $G(f_1)$. Hence, $G(f) \simeq G(f_1) \simeq G(h)$. In [**Ba**, Chap. 3, Theorem 3.1.3], the density of divisors of the Companion Lucas sequence $C_2(\theta_1,\theta_2) = \{\theta_1^n + \theta_2^n\}_{n=0}^{+\infty}$ was computed for any non-degenerate rule $f_1(X) = (X-\theta_1)(X-\theta_2)$, where θ_1, $\theta_2 \in \mathbb{Z}$. For instance, $\delta(3^n+5^n) = 2/3$. Now letting $U = C_2(\theta_1,\theta_2) = \langle A, B\rangle$, we have $U = \{3^n+5^n\} = [2,8]$, so that

$$\begin{cases} A = u_1 - u_0\theta_2 = 8 - 10 = -2, \\ B = u_1 - u_0\theta_1 = 8 - 6 = 2. \end{cases}$$

Hence, in $F(f)$, where $f(X) = (X-3)^2(X-5)$, the sequence $\langle -2, 0, 2\rangle$, which is in the class of the pre-image of U, has the closed form

$$\begin{aligned}\left\{\frac{-2n}{3(5-3)}3^n + \frac{2}{(5-3)^2}5^n\right\} &\sim \{4n3^{n-1} - 5^n\}, \text{ multiplying by } -2,\\ &\sim \{4(n+1)3^n - 5^{n+1}\}, \text{ shifting once to the right,}\\ &\sim \{4n3^n - 5\cdot 5^n\}, \text{ changing the } A' \text{ coefficient.}\end{aligned}$$

Hence, $\{4n3^n - 5\cdot 5^n\}$ has a 2/3 density of maximal divisors. So does the sequence $\langle -2, 0, 2\rangle$ in $F(h)$, where $h(X) = (X-3)(X-5)^2$. In closed form this sequence is

$$\begin{aligned}\left\{\frac{-2n}{5(3-5)}5^n + \frac{2}{(-2)^2}3^n\right\} &\sim \{2n5^{n-1} + 3^n\}\\ &\sim \{2(n+1)5^n + 3^{n+1}\} \sim \{2n5^n + 3\cdot 3^n\}.\end{aligned}$$

Hence,

$$(13) \qquad P\left(\{3^n+5^n\}\right) \approxeq P_{max}\left(\{4n3^n-5^{n+1}\}\right) \approxeq P_{max}\left(\{2n5^n+3^{n+1}\}\right);$$

these three sets of primes having a 2/3 natural density (we may not have strict equalities in (13), since we took sequences that are equivalent to $\langle -2,0,2\rangle$).

In general, the sequence

$$(14) \qquad \{(\theta_1-\theta_2)n\theta_1^n-\theta_2^{n+1}\}$$

is in the class of the pre-image through the isomorphism φ of the class of the Companion Lucas sequence $\{\theta_1^n+\theta_2^n\}$ in $F(f_1)$. Thus, for rule (3), this sequence is $\{n2^n-1\}$ and it has a 17/24 density of maximal prime divisors, since $\delta(2^n+1)=17/24$ (see Lagarias' paper [**Lag**], or [**Ba**, Theorem 3.1.3]).

Let us return to the Cullen numbers. The sequence $\{n\,2^n+1\}$ belongs to the rule $f(X)=(X-2)^2(X-1)$, which in turn is related to the quadratic rule $f_1(X)=(X-2)(X-1)$. Since it is known that the only sequences in $F(f_1)$, whose density of prime divisors is one, are in the class of the Lucas sequence (the identity in $G(f_1)$), Corollary 10 tells us that any sequence with a density of maximal divisors equal to one in $F(f)$ must be in the weak equivalence class of the identity $\langle 1,1,1\rangle$.

But we saw that every odd prime is a maximal divisor of $\{n\,2^n+1\}$. Hence, $\delta_{max}(n2^n+1)=1$. Thus, we must have $\{n2^n+1\}\sim\langle 1,1,1\rangle$. This fact can be verified directly :

$$\begin{aligned}\langle 1,1,1\rangle &= \left\{\left(\frac{n}{2}-1\right)2^n+1\right\} = \{(n-2)\,2^{n-1}+1\}\\ &\sim \{(n-1)\,2^n+1\} \text{ shifting once to the right, i.e. replacing } n-1 \text{ by } n\\ &\sim \{n\,2^n+1\} \text{ replacing } A'=1 \text{ by } 0.\end{aligned}$$

§5. Law of Apparition of Prime Maximal Divisors.

Every odd prime is a maximal divisor of the Cullen numbers at $p-2$. The results of this Section will show that, in fact, for any sequence in the class of the identity, one can compute the exact term numbers at which a prime p appears as a maximal divisor.

But first, let us mention results about ranks and periods of division by a prime p.

Recall that for the Lucas sequence $L(\theta_1,\theta_2)=[0,1]_{f_1}=\{(\theta_1^n-\theta_2^n)/(\theta_1-\theta_2)\}$, the first positive term number r for which a prime p divides $L(\theta_1,\theta_2)(r)$, if it exists, is called the *rank* of p. This rank will be denoted by $r=rk_{f_1}(p)$.

The next proposition due to Lucas expresses the fact that prime division in $L(\theta_1, \theta_2)$ is periodic of period r. Note that this proposition is valid whether $f_1(X) \in \mathbb{Z}[X]$ has integral roots or not.

Proposition 11 (Lucas' Law of Apparition). *If $p \nmid \theta_1\theta_2$, then $\exists r \in \mathbb{Z}^+$ such that*

$$p \mid L(\theta_1, \theta_2)(n) \iff r \mid n.$$

Moreover if $p \nmid 2\theta_1\theta_2$, then $r \mid p - \left(\frac{\Delta}{p}\right)$, where $\left(\frac{*}{*}\right)$ is the Legendre symbol and $\Delta = (\theta_1 - \theta_2)^2$.

Proof. See Lucas' memoir [**Lu**], Sections 24 and 25, pp. 287-297. □

Remark. If a prime $p \nmid \theta_1\theta_2$ is a divisor of some sequence $U \in F(f_1)$, then the period with which it divides U is equal to its rank r.

Definition. Let f be a cubic rule and p be a prime. The *rank of maximal division $\rho = rk_f(p)$* of p is the least $\rho > 0$ such that p is a maximal divisor of $[0, 0, 1]_f$ at ρ (if it exists).

Remark 12. If $V \in F(f)$ and p is a maximal divisor of V not dividing the product of the roots of f, then maximal division of V by p occurs periodically with period $\rho = rk_f(p)$. In particular, if $V = [0, 0, 1]_f$, then

$$p \mid_{max} V \text{ at } n \iff \rho \mid n.$$

In fact, if the roots of f are integral and distinct in absolute value, then, using Theorem 4.4.1 of [**Ba**], we see that ρ is the least common multiple of the ranks of p in the Lucas sequences $L(\theta_1, \theta_2)$, $L(\theta_1, \theta_3)$ and $L(\theta_2, \theta_3)$.

We proceed to establish a law of apparition for cubic rules of the type $f(X) = (X - \theta_1)^2(X - \theta_2) \in \mathbb{Z}[X]$.

Theorem 13 (Law of Apparition for cubic rules with a double root). *Let p be a prime. If $p \nmid 2\theta_1\theta_2(\theta_1 - \theta_2)$, then*

$$p \mid_{max} [0, 0, 1]_f \text{ at } n \iff \rho = pr \mid n,$$

where r is the rank of p in $L(\theta_1, \theta_2) = [0, 1]_{f_1}$.

Proof. According to Remark 12 we only need to show that ρ, the rank of maximal division of p, equals pr, i.e. $rk_f(p) = p \cdot rk_{f_1}(p)$.

By the Remark following Theorem 2, if p is a maximal divisor of $U = [0, 0, 1]_f = \langle 1, 1, 1 \rangle$ at n, then $\theta_1^n \equiv \theta_2^n \mod p$. But $p \nmid (\theta_1 - \theta_2)$ and

$\theta_1^n \equiv \theta_2^n \mod p \implies p \mid L(\theta_1,\theta_2)(n)$, which implies that $r \mid n$ (note that the rank r is well-defined since $p \nmid \theta_1\theta_2$). Hence, $r \mid \rho$. Now by (9)

(15)
$$u_\rho = \left[\frac{\rho}{\theta_1(\theta_1-\theta_2)} - \frac{1}{(\theta_1-\theta_2)^2}\right]\theta_1^\rho + \frac{\theta_2^\rho}{(\theta_1-\theta_2)^2} \equiv \frac{\rho}{\theta_1(\theta_1-\theta_2)}\cdot\theta_1^\rho \equiv 0 \mod p,$$

since ρ being a multiple of r, we have $\theta_1^\rho \equiv \theta_2^\rho \mod p$.

But $p \nmid \theta_1(\theta_1-\theta_2)$, so that $\rho \equiv 0 \mod p$. Hence, $p \mid \rho$.

Since $p \nmid 2\theta_1\theta_2$ and $\theta_1, \theta_2 \in \mathbb{Z}$, we have by Proposition 11 $2 \le r \le p-1$, which implies $(p,r) = 1$ and therefore $pr \mid \rho$.

It remains to see that $p \mid u_{pr}$, u_{pr+1}, but not u_{pr+2}. We already can check that $p \mid u_{pr}$ by replacing ρ by pr in (15); the two other divisibility conditions can be checked just as readily. □

Consequence. Let q be a prime. Then, $\forall p$ prime, $p \nmid 2q\theta_1\theta_2(\theta_1-\theta_2)$, we have
$$q \mid rk_f(p) \iff q \mid rk_{f_1}(p).$$

This is an immediate consequence of Theorem 13. It is of interest since the density of primes whose rank is a multiple of a given prime q is known in the case of a quadratic rule with integer roots (see [**Ba**], Proposition 2.1.3 and Theorem 3.2.3). In particular, it is well known that the prime divisors of the Companion Lucas sequence $C_2(\theta_1,\theta_2)$ are essentially these primes whose rank in $[0,1]_{f_1}$ is a multiple of two. Hence, sequence (14) has the property that its divisors are the primes of even rank in $[0,0,1]_f$.

We prove an analogue of Theorem 13 for general sequences in the identity class. But we first need a lemma.

Lemma 14. *Let p be a prime $\nmid 2\theta_1\theta_2$, with rank r in $L(\theta_1,\theta_2)$ and ρ_0 be an integer satisfying $0 \le \rho_0 \le p-1$. Then*
$$\exists i \ge 0 : \ r \mid \rho_0 + ip \quad \textit{and} \quad \rho_0 + ip < pr.$$

Proof. Consider the numbers $\rho_0 + ip$, $0 \le i \le r-1$. These r numbers form a complete residue system modulo r, since
$$\theta_1,\ \theta_2 \in \mathbb{Z} \implies \Delta \in \mathbb{Z}^2 \implies \left(\frac{\Delta}{p}\right) = 1 \implies r \nmid p, \quad \text{and so}$$
$$i \ne j \implies (\rho_0 + ip) - (\rho_0 + jp) = (i-j)p \not\equiv 0 \mod r.$$

Hence, $\exists i$, $0 \le i \le r-1$, such that $r \mid \rho_0 + ip$.

But, $\rho_0 + ip < p + (r-1)p < rp$. □

Theorem 15. *Let $U = \langle A, A', A\rangle \in F(f)$ and p be a prime not dividing $2A\theta_1\theta_2(\theta_1 - \theta_2)$. Then*

$$p \mid {}_{max}\langle A, A', A\rangle \text{ at } n \iff n = n_0 + \lambda pr,\ \lambda \geq 0,$$

where r is the rank of p in the Lucas sequence $L(\theta_1, \theta_2)$ and n_0 is the smallest non-negative integer divisible by r with

$$n_0 \equiv \theta_1/(\theta_1 - \theta_2) \cdot (A' - A)/A \mod p.$$

Proof. Let ρ_0 be an integer such that $\rho_0 \equiv \theta_1/(\theta_1 - \theta_2) \cdot (A' - A)/A \mod p$ and $0 \leq \rho_0 \leq p-1$. Then, by Lemma 14, we know that $\exists n_0 = \rho_0 + ip$, $i \geq 0$, such that $r \mid n_0$ and $n_0 < pr$. Note that $n_0 \equiv \rho_0 \equiv \theta_1/(\theta_1 - \theta_2) \cdot (A' - A)/A \mod p$.

We can directly check that p is a divisor of U at n_0, i.e. that

$$\begin{cases} u_{n_0} \equiv u_{n_0+1} \equiv 0 \mod p, \\ u_{n_0+2} \equiv A\theta_1^{n_0} \not\equiv 0 \mod p. \end{cases}$$

We will only check here that $u_{n_0} \equiv 0 \mod p$.

Thus,

$$u_{n_0} = \left(\frac{An_0}{\theta_1(\theta_1 - \theta_2)} - \frac{A'}{(\theta_1 - \theta_2)^2}\right)\theta_1^{n_0} + \frac{A}{(\theta_1 - \theta_2)^2}\theta_2^{n_0},$$

and since $r \mid n_0$, we have $\theta_1^{n_0} \equiv \theta_2^{n_0} \mod p$. Hence,

$$u_{n_0} \equiv \left[\left(\frac{An_0}{\theta_1(\theta_1 - \theta_2)} - \frac{A'}{(\theta_1 - \theta_2)^2}\right) + \frac{A}{(\theta_1 - \theta_2)^2}\right]\theta_1^{n_0} \mod p,$$

but $n_0 \equiv \theta_1/(\theta_1 - \theta_2) \cdot (A' - A)/A \mod p$, so

$$\begin{aligned} u_{n_0} &\equiv \left(\frac{A}{\theta_1(\theta_1 - \theta_2)} \cdot \frac{\theta_1}{\theta_1 - \theta_2} \cdot \frac{A' - A}{A} - \frac{A'}{(\theta_1 - \theta_2)^2} + \frac{A}{(\theta_1 - \theta_2)^2}\right)\theta_1^{n_0} \mod p, \\ &\equiv \left(\frac{A' - A}{(\theta_1 - \theta_2)^2} + \frac{A - A'}{(\theta_1 - \theta_2)^2}\right)\theta_1^{n_0} \equiv 0 \mod p. \end{aligned}$$

Now, since by Remark 12, division is periodic with period pr and the number n_0 is less than pr, it follows that n_0 is the first term at which maximal division occurs. Hence the theorem follows. □

The most general sequence V in the class of the identity $\langle 1, 1, 1\rangle$ is of the form $V = \langle A_V, A'_V, B_V\rangle = \langle A\theta_1^k, A'_k, A\theta_2^k\rangle$, where k is some integer. That is $V = \{v_n = u_{n+k}\}$ is a shift of the sequence $U = \langle A, A', A\rangle$ by k places. One can compute, by induction, the relationship between A'_k and A', since for $k = 1$ and $k = -1$ we have respectively $A'_1 = A'\theta_1 + A(\theta_1 - \theta_2)$ and $A'_{-1} = A'\theta_1^{-1} - A\theta_1^{-2}(\theta_2 - \theta_1)$, and obtain

$$A'_k = A'\theta_1^k + kA\theta_1^{k-1}(\theta_2 - \theta_1),\ \forall k \in \mathbb{Z}. \tag{16}$$

To find exactly where maximal division occurs in a given sequence in the identity class, one may use the following theorem.

Theorem 16. *Let* $V = \langle A_V, A'_V, B_V\rangle = \langle A\theta_1^k, A'_k, A\theta_2^k\rangle \in F(f)$, *where* $k \in \mathbb{Z}$ *and* $A'_k = A'\theta_1^k + kA\theta_1^{k-1}(\theta_2 - \theta_1)$. *Let p be a prime not dividing* $2A\theta_1\theta_2(\theta_1 - \theta_2)$. *Then*

$$p \mid_{max} V \text{ at } n \iff n = n'_0 + \lambda pr,\ \lambda \geq 0,$$

where r is the rank of p in the Lucas sequence $L(\theta_1, \theta_2)$ and n'_0 is the smallest non-negative integer such that $n'_0 + k$ is divisible by r and

$$n'_0 \equiv \theta_1/(\theta_1 - \theta_2) \cdot (A'_V - A_V)/A_V \mod p.$$

Proof. First observe that

$$\begin{aligned} n'_0 \equiv \frac{\theta_1}{\theta_1 - \theta_2} \cdot \frac{A'_k - A\theta_1^k}{A\theta_1^k} &\equiv \frac{\theta_1}{\theta_1 - \theta_2} \cdot \frac{[A'\theta_1^k + kA\theta_1^{k-1}(\theta_2 - \theta_1)] - A\theta_1^k}{A\theta_1^k} \\ &= \frac{\theta_1}{\theta_1 - \theta_2} \cdot \left[\frac{(A' - A)\theta_1^k}{A\theta_1^k} + k \cdot \frac{\theta_2 - \theta_1}{\theta_1}\right] \\ &\equiv n_0 - k \mod p, \end{aligned}$$

where n_0 is the smallest non-negative number divisible by r and congruent to $\theta_1/(\theta_1 - \theta_2) \cdot (A' - A)/A \mod p$.

Now, by (16) we know that V is a shift of $U = \langle A, A', A\rangle$ by k places. So we know by Theorem 15 that maximal division of U by p occurs at every $n_0 + \lambda pr$, $\lambda \geq 0$. Hence, maximal division of V by p must occur at every $(n_0 - k) + \lambda pr$, so that n'_0 must be the first non-negative subscript of the form $(n_0 - k) + \lambda pr$, $\lambda \in \mathbb{Z}$.

But since

$$n'_0 = (n_0 - k) + \lambda pr \iff \begin{cases} n'_0 \equiv n_0 - k \mod p, \\ r \mid n'_0 + k, \end{cases} \tag{17}$$

the theorem follows. To see that (17) holds, note that the direct implication $\Longrightarrow$) is clear and that if $n'_0 \equiv n_0 - k \mod p$, then $n'_0 = (n_0 - k) + \mu p$, for some integer μ, i.e. $n_0' + k = n_0 + \mu p$. But,

$$\left.\begin{array}{l} r \mid n_0 \\ r \mid n_0' + k \end{array}\right\} \implies r \mid \mu p \implies r \mid \mu.$$

Hence, n_0' is of the form $(n_0 - k) + \lambda pr$. □

Application. We use Theorem 16 to check maximal division of the generalized Cullen sequence at $p-2$. Indeed, from (8) we have

$$c_n = \left(\frac{n}{\theta_1 - \theta_2} - \frac{2\theta_2 - \theta_1}{(\theta_1 - \theta_2)^2}\right) + \frac{\theta_2 \cdot \theta_2^n}{(\theta_1 - \theta_2)^2},$$

so that $C = \langle \theta_1, 2\theta_2 - \theta_1, \theta_2 \rangle$ and $k = 1$. Now,

$$n_0' \equiv \frac{\theta_1}{\theta_1 - \theta_2} \cdot \frac{(2\theta_2 - \theta_1) - \theta_1}{\theta_1} = -2 \mod p.$$

Hence, maximal division occurs at the smallest n_0' of the form $-2+\mu p$, $\mu \geq 1$ such that $n_0' + k = n_0' + 1 = \mu p - 1$ is divisible by r. But if $\mu = 1$, then $n_0' + 1 = p - 1$ which is a multiple of the rank r. Hence, $n_0' = p - 2$.

§6. Generalizations.

The results of this paper readily generalize to the situation where

$$f(X) = (X - \theta_1)^2 g(X) \text{ and } f_1(X) = (X - \theta_1) g(X),$$

and $f_1(X)$ is a non-degenerate monic polynomial in $\mathbb{Z}[X]$ with roots

$$\theta_1, \theta_2, \ldots, \theta_m.$$

We state some of the analogous results below without proof.

If the sequence $[0, 0, \ldots, 0, 1]_f$ has the closed form

$$(\gamma_1 n + \gamma_1')\theta_1^n + \gamma_2\theta_2^n + \ldots + \gamma_m\theta_m^n,$$

then one defines a *standard form* for a sequence $U \in F(f)$ as

$$(A_1\gamma_1 n + A_1'\gamma_1')\theta_1^n + A_2\gamma_2\theta_2^n + \ldots + A_m\gamma_m\theta_m^n.$$

We write $U = \langle A_1, A_1', A_2, \ldots, A_m \rangle$. *Weak equivalence* of two sequences is defined via shifting of the subscript, multiplication by a rational scalar and change of the number A_1'. The *product* of two sequences

$$U = \langle A_1, A_1', A_2, \ldots, A_m \rangle \quad \text{and} \quad V = \langle B_1, B_1', B_2, \ldots, B_m \rangle$$

is defined to be the sequence

$$U \cdot V = \langle A_1B_1, A_1'B_1', A_2B_2, \ldots, A_mB_m \rangle.$$

Theorem 2 generalizes as follows.

Theorem 17. *Let $U = \langle A_1, A_1', A_2, \ldots, A_m \rangle \in F(f)$. Let p be a prime not dividing $\delta^2 \cdot \prod_{i=1}^m A_i\theta_i$, where $\delta = \prod_{1\le i<j\le m}(\theta_j - \theta_i)$. Then :*

$$p \in P_{max}(U) \iff \exists n \in \mathbb{N} : A_i\theta_i^n \equiv A_j\theta_j^n \mod (p),\ \forall i, j \in \{1, 2, \ldots, m\},$$

where (p) is the ideal generated by p in the root field $\mathbb{Q}(\theta_2, \ldots, \theta_m)$.

Defining the *projection map* $\varphi : G(f) \longrightarrow G(f_1)$ by

$$\varphi(Cl\,\langle A_1, A_1', A_2, \ldots, A_m\rangle) = Cl\,\langle A_1, A_2, \ldots, A_m\rangle,$$

we have a generalization of Theorem 4 in the following statement.

Theorem 18. *The projection map φ is an isomorphism from $(G(f), \cdot)$ onto the group $(G(f_1), \cdot)$ which preserves maximal division by any prime p.*

Example. If $f(X) = (X-3)^2(X-2)(X-1)$, then the identity sequence $[0,0,0,1]_f = \langle 1,1,1,1\rangle$ is the sequence

$$\left\{\left(\frac{n}{6} - \frac{3}{4}\right)3^n + 2^n - \frac{1}{4}\right\}.$$

In [**Ba**, Proposition 4.6.6] the sequence $\langle -1,1,1\rangle$ in $F(f_1)$ was shown to have a density of maximal divisors equal to 65/224. But $\varphi^{-1}(Cl\,\langle -1,1,1\rangle) = Cl\,\langle -1,0,1,1\rangle$ and the sequence $\langle -1,0,1,1\rangle$ is weakly equivalent to

$$\langle -4,0,4,4\rangle = \left\{-\frac{2n}{3}3^n + 2^{n+2} - 1\right\} \sim \{2n\,3^n - 2^{n+3} + 1\}.$$

(Multiplying by -1, shifting once to the right and putting $A_1' = 0$.)

Therefore, $\delta(2n\,3^n - 2^{n+3} + 1) = 65/224$, i.e. about 29% of the primes divide three consecutive terms of the sequence.

Acknowledgment. The author wishes to thank John Brillhart, who showed me the special divisibility property that the Cullen numbers satisfy and for his friendly presence while I was at Arizona, but also to thank the Referee for his suggestions and his interest.

References

[Ba] C. Ballot, *Density of prime divisors of linear recurrences*, Memoirs of the A.M.S., **115**, Nu. 551, May 1995.

[Cu & Wo] A.J.C. Cunningham and H.J. Woodall, *Factorisation of $Q = (2^q \pm q)$ and $(q2^q \pm 1)$*, Messenger of Mathematics, **47** (1917), 1-38.

[Hoo] C. Hooley, *Application of Sieve Methods to the Theory of Numbers*, Cambridge U. Press 1976, Chapter 7, Section 3.

[Lag] J.C. Lagarias, *The set of primes dividing the Lucas Numbers has density* 2/3, Pacific J. Math., **118(2)** (1985), 449-461 and "Errata", **162** (1994), 393-396.

[Lax] R.R. Laxton, *On groups of linear recurrences* I, Duke Math., **26** (1969), 721-736.

[Lu] E. Lucas, *Théorie des fonctions numériques simplement périodiques*, Amer. J. Math., **1** (1878), 184-240, 289-321.

[Ro] R.M. Robinson, *A report on primes of the form $k\,2^n + 1$ and on factors of Fermat numbers*, Proc. AMS, **9**, 1958.

[Schi] A. Schinzel, *On power residues and exponential congruences*, Acta Arithmetica, **27** (1975), 397-420.

[So] L. Somer, *Linear recurrences having almost all primes as maximal divisors*, Fibonacci Numbers and Their Applications, A. N. Philippou, G. E. Horodam (Eds.), D. Reidel Pub. Co.: Dordrecht, The Netherlands, 1986, 257-272.

[Wal] M. Ward, *The maximal prime divisors of linear recurrences*, Canad. J. Math., **6** (1954), 455-462.

[Wa2] ———, *The laws of apparition and repetition of primes in a cubic recurrence*, Trans. Amer. Math. Soc., **79** (1955), 72-90.

Received November 12, 1993.

Université de Caen
Caen 14032, France
E-mail address: ballot@math.unicaen.fr