Generalized Base Representations

Daniel M. Kane

December 31, 2005

Abstract

Let $B \in \mathbb{Z}[x]$ be a polynomial with $b = B(0)$. Let S be a complete residue class modulo b containing 0. We attempt to classify the polynomials B and residue classes S so that for every polynomial $P \in \mathbb{Z}[x]$ there exists a polynomial Q with coefficients in S such that $P \equiv Q \pmod{B}$.

1 Introduction

It is well known that any integer n can be written uniquely in base $-k$ where $k \in \mathbb{Z}$ and $k > 1$. Such a representation is a sequence of the form $d_m d_{m-1} \dots d_0$ so that $n = \sum_{i=0}^{m} d_i(-k)^i$ and every $d_i \in \{0, 1, \dots, k-1\}$. Problem 3 of the 1997 USA Mathematical Olympiad was to prove that for any integer n there exists a polynomial Q with coefficients in $\{0, 1, \dots, 9\}$ so that $Q(-2) = Q(-5) = n$. One way to prove this is by proving the stronger statement that if $n, m \in \mathbb{Z}$ and $n \equiv m \pmod 3$ then there exists such a polynomial Q so that $Q(-2) = n$ and $Q(-5) = m$. This states that if $n \equiv m \pmod 3$ then there exists a base representation (using the digits $0, 1, \dots, 9$) that is equal to n in base -2 and m in base -5. More generally, we are looking for a polynomial that has coefficients in $\{0, 1, ..., 9\}$ that is congruent to $\frac{(x+2)(m-n)}{-3} + n \bmod (x+2)(x+5)$. In this paper, we look at more general circumstances in which this happens.

Definition. *Let $B \in \mathbb{Z}[x]$ be a polynomial with $b = B(0)$. Let S be a complete residue system modulo b so that $0 \in S$. Given polynomials $P, Q \in \mathbb{Z}[x]$ where Q has coefficients in S, we say that Q* represents *P over (B, S) if $P \equiv Q \pmod{B}$. We say that (B, S) is a* complete base *if for any $P \in \mathbb{Z}[x]$ there exists a $Q \in \mathbb{Z}[x]$ so that Q represents P over (B, S).*

Notice that if such a polynomial Q exists, it is unique, for if $Q_1 \equiv P \equiv Q_2 \pmod{B}$ then B divides $Q_1 - Q_2$. This implies that the coefficient of the lowest degree non-zero term of $Q_1 - Q_2$ is a multiple of b. But if Q_1 and Q_2 have coefficients in S, the only coefficients of their difference that are divisible by b are 0. Hence $Q_1 = Q_2$.

The problem of classifying the pairs of (B, S) that form complete bases has already been extensively studied in the quadratic case ([2] and [3]). This statement of the problem for general polynomials was studied by Kiran Kedlaya [**?**].

From now on B will always be taken to be a monic polynomial with integer coefficients and $B(0) = b$. The set S will be taken to be a complete residue class modulo b containing 0.

In this paper we consider the question of which pairs of (B, S) constitute complete bases. In Section 2, we derive some necessary conditions involving the locations of the roots of B. In Section 3, we derive an alternative criterion for (B, S) to be a complete base. In Section 4, we use these criteria to prove that for a large class of polynomials with distinct integer roots, B, (B, S) form a complete base when $S = \{0, 1, \ldots, b-1\}$.

2 Preliminaries

Here are some preliminary theorems proven by Kiran Kedlaya that provide necessary conditions for (B, S) to be a complete base.

Proposition 1. *Let $\mathbb{Z}_0^+$ denote the non-negative integers. If $S \subseteq \mathbb{Z}_0^+$ and B has a root r in $\mathbb{R}^+$, then (B, S) does not form a complete base.*

Proof. Let $P(x) = -1$. Suppose for the sake of contradiction that Q is a polynomial which represents P over (B, S). Then $-1 = P(r) = Q(r) \geq 0$. Hence (B, S) does not form a complete base. □

Proposition 2. *If B has a root r in the open unit disk, then (B, S) does not form a complete base.*

Proof. Let $M = \max_{s \in S} |s|$. Let $P(x) = \lceil \frac{M}{1-|r|} \rceil + 1 = C$. Suppose for the sake of contradiction that Q is a polynomial which represents P over (B, S). Then $|C| = |P(r)| = |Q(r)| \leq \sum_{n=0}^{\infty} M|r|^n = \frac{M}{1-|r|}$. Hence P is not representable in this way, so (B, S) does not form a complete base. □

Proposition 3. *If B has a root r on the unit circle, then (B, S) does not form a complete base.*

Proof. Let $C(x)$ be the minimal polynomial of r. Since r has a multiplicative inverse, namely $\bar{r}$, that is a root of C, the multiplicative inverses of all roots of C are also roots. Hence $C(0) = \pm 1$. Let $B = C \cdot D$. Let $P = D$. Suppose for sake of contradiction that Q is a polynomial with coefficients in S so that $P \equiv Q \pmod{B}$. Then since B does not divide P, we know that $Q \neq 0$. Also since D divides B and P, it follows that D divides Q. Therefore, the smallest non-zero coefficient of Q must be a multiple of the units term of D. Hence, some coefficient of Q is a non-zero multiple of b. However, no such number is in S. Therefore, (B, S) does not form a complete base. □

3 An Equivalent Criterion

In this section, we prove the following theorem which gives us a criterion equivalent to (B, S) constituting a complete base.

Theorem 4. *(B, S) forms a complete base if and only if B has no roots on the closed unit disk and there exists no polynomial $T \in \mathbb{Z}[x]$ and natural number n so that when $B \cdot T$ is reduced modulo $1 - x^n$ to a polynomial of degree at most $n - 1$ it is a non-zero polynomial with coefficients in S.*

Before proving Theorem 4 we must develop the necessary machinery.

Definition. *Given $P \in \mathbb{Z}[x]$, let $R_n(x) \in \mathbb{Z}[x]$ be defined by $R_0(x) = P(x)$ and $R_{n+1}(x) = \frac{1}{x}(R_n(x) - s_n - a_n B(x))$, where s_n and a_n are the unique integers so that $s_n \in S$ and $s_n + b \cdot a_n = R_n(0)$.*

Let $f : \mathbb{Z}[x] \to \mathbb{Z}[x]$ be the map that takes $R_n(x)$ to $R_{n+1}(x)$.

Let $Q_n(x) = s_0 + s_1 x + \cdots + s_{n-1}x^{n-1} + x^n R_n(x)$.

Lemma 5. *The unique polynomial whose coefficients up to degree $n - 1$ are in S that is equal to $P + B \cdot M_n$ for some polynomial M_n with $\deg M_n \leq n - 1$ is Q_n (we use the convention that $\deg 0 = -1$).*

Proof. We proceed by induction on n. When $n = 0$, $\deg M_0 \leq -1$, so $M_0 = 0$. Hence the only such polynomial is $P = R_0 = Q_0$.

Assume that the $n - 1$ case of the lemma is true. Let Q be a polynomial so that $Q = P + B \cdot M_n$ where $\deg M_n \leq n - 1$ and the first $n - 1$ coefficients of Q are in S. Let s be the coefficient of x^{n-1} of Q. Write $M_n = M - ax^{n-1}$ where $\deg M \leq n-2$. Then $Q = P + B \cdot M - ax^{n-1}B$. Since the first $n-2$ coefficients of Q are in S, the first $n-2$ coefficients of $P + B \cdot M$ are also in S. Therefore, by the inductive hypothesis, $P + B \cdot M = Q_{n-1}$. Hence, $Q = Q_{n-1} - ax^{n-1}B$. Since the x^{n-1} coefficient of Q is in S and the x^{n-1} coefficient of Q_{n-1} is $R_{n-1}(0)$, we must have that $a = a_{n-1}$. Therefore,

$$\begin{aligned}
Q(x) &= Q_{n-1}(x) - a_{n-1}x^{n-1}B(x) \\
&= s_0 + \cdots + s_{n-2}x^{n-2} + x^{n-1}R_{n-1}(x) - a_{n-1}x^{n-1}B(x) \\
&= s_0 + \cdots + s_{n-1}x^{n-1} + x^n\left(\frac{1}{x}(R_{n-1}(x) - s_{n-1} - a_{n-1}B(x))\right) \\
&= s_0 + \cdots + s_{n-1}x^{n-1} + x^n R_n(x) \\
&= Q_n(x).
\end{aligned}$$

Thus, $Q_n(x)$ is the unique such polynomial. Conversely, if we let $M_n = M_{n-1} - a_{n-1}x^{n-1}$ we get that $Q_n = P + B \cdot M_n$, proving that Q_n is such a polynomial. □

Corollary 6. *There exists a polynomial Q with coefficients in S so that $P \equiv Q \pmod{B}$ if and only if $R_n(x)$ is identically 0 for some n.*

Proof. If $R_n(x) = 0$, then Q_n suffices by Lemma 5. If $P \equiv Q \pmod{B}$ then $Q = P + M \cdot B$ for some M. If $n = \max(\deg(M) + 1, \deg(Q) + 1)$, then by Lemma 1, Q must equal Q_n which implies that $R_n(x) = 0$. □

Lemma 7. *$\deg R_n < \deg B$ for all sufficiently large n.*

Proof. By the definition, $\deg R_{n+1} = \deg(R_n - s_n - a_n B(x)) - 1$. Suppose $\deg R_j \leq \deg R_n$ for all n. Then $\deg R_j < \deg B$ because $\deg R_j \leq \deg R_{j+1}$. Therefore, $\deg R_n < \deg B$ for all $n \geq j$. □

Proposition 8. *If B has no roots in the closed unit disk, then there exists some finite set $C \subset \mathbb{Z}[x]$ so that for any P, $R_n(x) \in C$ for all sufficiently large n.*

Proof. Let $B(x) = \prod (x - r_i)^{p_i}$. Let $M = \max_{s \in S} |s|$. By Lemma 5, $R_n(x)x^n + s_{n-1}x^{n-1} + \cdots + s_0 \equiv P(x) \pmod{B}$. Therefore,

$$R_n(x) \equiv -s_{n-1}x^{-1} - \cdots - s_0 x^{-n} + P(x)x^{-n} \pmod{B}.$$

If $k < p_i$ is a natural number, then

$$\left[\frac{d^k}{dx^k} R_n(x)\right]_{x=r_i} = \left[\frac{d^k}{dx^k}(s_{n-1}x^{-1} + \cdots + s_0 x^{-n} + P(x)x^{-n})\right]_{x=r_i}.$$

Therefore, we have that

$$\begin{aligned}
\left|\frac{d^k}{dx^k} R_n(x)\right|_{x=r_i} &\leq |s_{n-1}| \left|\frac{d^k}{dx^k} x^{-1}\right|_{x=r_i} + \cdots + |s_0| \left|\frac{d^k}{dx^k} x^{-n}\right|_{x=r_i} \\
&+ \left|\frac{d^k}{dx^k} P(x)x^{-n}\right|_{x=r_i} \\
&\leq M\left(\sum_{i=1}^{\infty} \left|\frac{d^k}{dx^k} x^{-i}\right|_{x=r_i}\right) + O(n^k |r_i|^{-n}) \\
&\leq M \left|\frac{d^k}{dx^k} \frac{1}{1-x}\right|_{x=|r_i|} + 1 \\
&\leq \frac{M \cdot k!}{(|r_i| - 1)^k} + 1
\end{aligned}$$

for all sufficiently large n. Since Lemma 7 implies that $\deg R_n < \deg B$ for all sufficiently large n, we have, by Lagrange Interpolation, that R_n is some fixed linear function of values in these ranges. Therefore, for all sufficiently large n, R_n lies in some linear transformation of a product of closed disks. Since R_n only has integer coefficients, R_n lies in the intersection of a compact set with a discrete set for all sufficiently large n. Hence, there is a finite set C so that $R_n \in C$ for all sufficiently large n independently of P. □

Notice that this implies that we can determine whether (B, S) is a complete base by a finite computation. We only need to check that B has no roots in the closed unit disk and that for any $R \in C$, $f^{(n)}(R)$ is eventually 0.

Corollary 9. *(B, S) forms a complete base if and only if B has no roots in the closed unit disk and there is no $R \in \mathbb{Z}[x]$ where $R \neq 0$ and $n \in \mathbb{N}$ so that $f^{(n)}(R) = R$ (R is fixed under n iterations of f).*

Proof. If B has no roots in the closed unit disk, then by Proposition 4, there exists an N so that $R_n \in C$ for all $n > N$. Therefore, by the pigeon-hole principle, $R_{N+1}, R_{N+2}, \cdots, R_{N+|C|+1}$ are not all distinct. Therefore, two of them, which we call R_n and R_m, are the same. Hence $f^{(m-n)}R_n = R_n$. Therefore, if iterations of f have no fixed point other than 0, this implies that $R_n = 0$, which by Corollary 6 implies that any P has a representation and that (B, S) forms a complete base.

If B has a root in the closed unit disk, then (B, S) does not form a complete base by Propositions 2 and 3.

If some iteration of f has a fixed point other than 0, there is some P such that $R_n = f^{(n)}(P) \neq 0$ for every n (since $f(0) = 0$). Therefore, by Corollary 6, P does not have a representation, so (B, S) does not form a complete base. □

Proof of Theorem 4. By Corollary 9, it is enough to show that if B has no roots in the closed unit disk, then some iteration of f has a non-zero fixed point if and only if some multiple of B is congruent modulo $1 - x^n$ to a non-zero polynomial of degree at most $n - 1$ with coefficients in S.

Suppose that $f^{(n)}R = R$ where $R \neq 0$. Let $P = R$. By Lemma 5,

$$\begin{aligned} P &\equiv R_0 \equiv s_0 + s_1 x + \cdots + s_{n-1}x^{n-1} + R_n x^n \\ &\equiv s_0 + \cdots + s_{n-1}x^{n-1} + R_0 x^n \pmod{B}. \end{aligned}$$

Therefore, B divides

$$(x^n - 1)R_0 + (s_0 + \cdots + s_{n-1}x^{n-1}).$$

Hence some multiple of B is congruent modulo $1 - x^n$ to some polynomial of degree at most $n - 1$ with coefficients in S. Furthermore, this polynomial is not 0 because then we would have B divides $(1 - x^n)R_0$ or R_0 (because B has no roots in the closed unit disk). Since R_0 is fixed by some iteration of f, Lemma 7 implies that $\deg R_0 < \deg B$. Therefore, if B divides R_0, then R_0 must be 0, which it is not.

Now suppose that some multiple of B is $T + R(x^n - 1)$ where T has degree less than n, is non-zero, and has coefficients in S. Then

$$R \equiv T + x^n R \equiv \cdots \equiv T + x^n T + \cdots + x^{(k-1)n}T + x^{kn}R \pmod{B}$$

for every k. Suppose that $R \equiv Q \pmod{B}$ where Q has coefficients in S. Choose k so that $(k - 2)n > \deg Q$. We have that B divides $x^{kn}R + (T + \cdots + Tx^{(k-1)n} - Q)$. Notice that since T is not identically 0, the first non-zero coefficient of this polynomial is the difference of two members of S. But this would imply that the first non-zero coefficient of some multiple of B is not a multiple of b which leads to a contradiction. Therefore (B, S) does not form a complete base if there is a multiple of B that yields a non-zero polynomial with coefficients in S when reduced modulo $1 - x^n$. □

4 Polynomials with distinct integer roots

We will use a series of technical lemmas to prove the following theorem which provides a sufficient condition on B and S for (B, S) to form a complete base.

Theorem 10. *If B is a polynomial whose roots are k distinct integers less than -1, if $k \leq 4$, and $S = \{0, 1, \cdots, b-1\}$, then (B, S) forms a complete base.*

Notice that the bounds on the roots are necessary because of Propositions 1, 2, and 3.

Lemma 11. *If B has non-negative coefficients, $2B(0) > B(1)$, and $S = \{0, 1, \ldots, b-1\}$, then (B, S) forms a complete base.*

Proof. Let $b_0 = b$. Let $B(x) = b_0 + b_1 x + \cdots + b_m x^m$. It is clear that $b_0 > b_1 + b_2 + \cdots + b_m$ and that $b_i \geq 0$. This implies that B has no roots in the closed unit disk. By Theorem 4, we just have to prove that there can be no polynomial $T \in \mathbb{Z}[x]$ of degree less than n so that when $B \cdot T$ is reduced modulo $1 - x^n$ the result has coefficients in S. Suppose that such a T does exist. Let $T = t_0 + t_1 x + \cdots + t_{n-1} x^{n-1}$. Let t_k be a coefficient of T that has the largest absolute value of any coefficient of T and is negative if the largest absolute value is attained by a negative coefficient. Without loss of generality, $k = m$ (where the indices of the t_i are taken modulo n). The coefficient of x^k in $T \cdot B$ when reduced modulo $x^n - 1$ is $b_0 t_m + b_1 t_{m-1} + \cdots + b_m t_0$.
Case 1: t_m is negative.
Note that $b_0 t_m + b_1 t_{m-1} + \cdots + b_m t_0 \geq 0$. Therefore, $b_1 t_{m-1} + \cdots + b_m t_0 \geq b_0(-t_m)$. But since t_m has the largest absolute value of any t, we know $b_1 t_{m-1} + \cdots + b_m t_0 \leq (-t_m)(b_1 + b_2 + \cdots + b_m) < b_0(-t_m)$. This is a contradiction.
Case 2: t_m is positive.
Then $b_0 t_m + b_1 t_{m-1} + \cdots + b_m t_0 < b_0$. Therefore, $b_1(-t_{m-1}) + \cdots + b_m(-t_0) > b_0(t_m - 1)$. But since t_m has the largest absolute value of any t, and because the largest absolute value is only obtained by positive t, we have that $-t_i < t_m - 1$. Therefore, $b_1(-t_{m-1}) + \cdots + b_m(-t_0) \leq (t_m - 1)(b_1 + \cdots + b_m) < b_0(t_m - 1)$. This is a contradiction. □

Proof of Theorem 10 when $k = 1$ or 2. All cases except for $B(x) = (x+2)(x+3)$ follow immediately from Lemma 11. This last case is easily checked by hand. □

Lemma 12. *If B has only negative integer roots other than -1 and $T \in \mathbb{Z}[x]$ has degree less than n so that $B(x)T(x) \equiv U(x) \pmod{1 - x^n}$ where $U(x)$ has degree less than n and coefficients in $\{0, 1, \ldots, b-1\}$, then all of the coefficients of T are in $\left[\frac{b-1}{2}\left(-\frac{1}{B(-1)} + \frac{1}{B(1)}\right), \frac{b-1}{2}\left(\frac{1}{B(-1)} + \frac{1}{B(1)}\right)\right]$.*

Proof. Since B has only negative real roots, $\frac{1}{B(x)}$ is a product of terms of the form $\frac{1}{(x-r)}$. Therefore, the power series of $\frac{1}{B(x)}$ has every other term positive. Thus, the endpoints of this interval are $b-1$ times the sum of the negative and positive coefficients respectively of $\frac{1}{B(x)}$. Hence the endpoints are bounds on the

coefficients of the power series of $\frac{U(x)}{B(x)(1-x^n)}$. Since $\frac{U(x)}{B(x)(1-x^n)} - \frac{T(x)}{1-x^n}$ is some polynomial divided by $B(x)$, its coefficients go to 0 because the coefficients of $\frac{1}{B(x)}$ go to 0. Therefore, the coefficients of $T(x)$ are arbitrarily close to numbers in $\left[\frac{b-1}{2}\left(-\frac{1}{B(-1)}+\frac{1}{B(1)}\right), \frac{b-1}{2}\left(\frac{1}{B(-1)}+\frac{1}{B(1)}\right)\right]$. Hence, all coefficients of $T(x)$ are in the specified range. □

Lemma 13. *If $\alpha, \beta, \gamma \geq 2$ are distinct integers, and if $(x+\alpha)(x+\beta)(x+\gamma) = x^3 + \rho_1 x^2 + \rho_2 x + \rho_3$, then the following inequalities hold:*

1. $\rho_3 + \rho_1 > \rho_2 + 1$,
2. $\rho_3 > 2\rho_1 + 2$,
3. $\rho_2 > \rho_1$,
4. $\rho_1 > 1$.

Proof. These are all easily verified. □

Proof of Theorem 10 for $k = 3$. Suppose for the sake of contradiction that (B, S) does not form a complete base. Since B has no roots in the unit disk, by Theorem 4, there must exist $T \in \mathbb{Z}[x]$ of degree less than n so that $B \cdot T$ yields a non-zero polynomial with coefficients in S when reduced modulo $x^n - 1$. By Lemma 12, the coefficients of T are in $\{-1, 0, 1, 2\}$. Since $T \cdot B$ has some positive coefficients and all non-negative coefficients mod $x^n - 1$, we have that $T(1) > 0$. This means that there exists some string of non-negative coefficients of T whose sum exceeds the absolute value of the preceding string of non-positive coefficients. Therefore, T must contain one of the following strings of coefficients which do not work for the given reasons (a/b denotes either a or b):

Case	Coefficient String	Reason
1	0,-1,+2	Lemma 13.2
2	+1/+2,-1 ,+2	Lemma 13.1
3	0,+2	Lemma 13.2
4	+1,+1	Lemma 13.3
5	+1,0,+1	Lemma 13.4

Thus we have a contradiction, and (B, S) form a complete base □

Lemma 14. *If $\alpha, \beta, \gamma, \delta \geq 2$ are distinct integers, and if $(x+\alpha)(x+\beta)(x+\gamma)(x+\delta) = x^4 + \rho_1 x^3 + \rho_2 x^2 + \rho_3 x + \rho_4$, then the following inequalities hold:*

1. $\rho_3 + \rho_4 > 2\rho_2 + 2\rho_1 + 2$,
2. $\rho_3 > 2\rho_2$,
3. $\rho_4 > \rho_2$,
4. $\rho_4 + \rho_2 > \rho_3 + 2\rho_1$,
5. $2\rho_4 > \rho_3$,

6. $\rho_2 > \rho_1$,

7. $2\rho_4 + \rho_2 > 2\rho_3 + 1$,

8. $\rho_1 > 1$.

Proof. These are all easily verified. □

Proof of Theorem 10 for $k = 4$. Suppose for the sake of contradiction that (B, S) does not form a complete base. Since B has no roots in the unit disk, by Theorem 4, there must exist a $T \in \mathbb{Z}[x]$ of degree less than n so that $B \cdot T$ yields a non-zero polynomial with coefficients in S when reduced modulo $1 - x^n$. By Lemma 12, the coefficients of T are in $\{-2, -1, 0, 1, 2\}$. The following sequences of coefficients cannot appear in T for the given reasons:

Case	Coefficient String	Reason
1	-1/-2,-1/-2	Lemma 14.1
2	1/+2,+1/+2	Lemma 14.2 and Case 1
3	0/-1,0,+2	Lemma 14.3 and Case 1
4	-2,0,+2	Lemma 14.2
5	0,+2	Cases 3 and 4
6	0/+1,0,-1/-2	Lemma 14.3 and Case 2
7	+2,0,-1/-2	Lemma 14.2, Cases 1 and 2
8	0,-1/-2	Cases 6 and 7
9	-2,+2,-2	Lemma 14.4
10	+1/+2,-1,+2,-2	Lemma 14.4
11	0,-1,+2,-2	Lemma 14.7
12	+2,-2	Cases 2, 5, 9, 10, and 11
13	+1,-2	Lemma 14.5 and Case 2
14	-2	Cases 1, 8, 12, and 13
15	+1/+2,-1,+2	Lemma 14.4
16	+2	Cases 2, 5, 14, 15, and 8
17	+1,0,+1	Lemma 14.6, Cases 14 and 1
18	+1,0,0,+1	Lemma 14.8 and Case 14
19	0/+1,0,0,0,+1	$\rho_4 > \rho_4 - 1$

Since $T \cdot B$ has some positive coefficients and all non-negative coefficients modulo $1 - x^n$, we have that $T(1) > 0$. This means that there exists some string of non-negative coefficients of T whose sum exceeds the absolute value of the preceding string of non-positive coefficients. This is impossible because of Cases 16, 2, 17, 18, and 19 from above. Therefore, (B, S) forms a complete base. □

5 Conclusions

Theorem 10 does not hold for arbitrary k. The smallest degree known counterexample is $B(x) = (x+2)(x+3)(x+4)(x+5)(x+6)(x+7)(x+8)(x+9)(x+10)$ and $P(x) = 8881893+8976926x+4566033x^2+1382656x^3+264947x^4+32503x^5+2478x^6 + 107x^7 + 2x^8$. Any further necessary or sufficient conditions on when

(B, S) form a complete base would be of interest. A complete classification seems difficult to obtain.

6 Acknowledgements

I would like to thank Kiran Kedlaya who gave me this problem to work on as well as proving some of the initial results. I would also like to thank Joe Gallian, who heads the University of Minnesota Duluth REU at which this research took place. This research was partially supported by NSF grant DMS-9820438.

References

[1] D.E. Knuth, *The Art of Computer Programming Vol 2: Seminumerical Algorithms* 2^{nd} Edition, Wesley, 1998.

[2] I. Kátai and B. Kovács, *Canonical number systems in imaginary quadratic fields*, Akta Math. Acad. Sci. Hungar. 37 (1981), 159-164.

[3] I. Kátai and J. Szabo, *Canonical number systems for complex integers*, Akta Sci. Math. (Szeged) 37 (1975), 255-260.

[4] K. Kedlaya, personal communication.