# Arithmetic relations between the coefficients of integer polynomials caused by the fixed divisor

Jose **Brox**

**Centre for Mathematics of the University of Coimbra**

17/04/19

## Fixed divisor

- Consider a univariate integer polynomial $f \in \mathbb{Z}[X]$ of degree $d$,

$$f = \sum_{i=0}^{d} a_i X^i$$

- Its *content* is the gcd of its coefficients,

$$c(f) = \gcd_{0 \leq i \leq d} (a_i)$$

- Its *(fixed) divisor* is the gcd of its integral images,

$$d(f) = \gcd_{z \in \mathbb{Z}} (f(z))$$

## Fixed divisor

**Examples:**

- $2X + 2$ has content 2 and divisor 2 ($f(0) = 2$)
- The content always divides the divisor, $c(f)|d(f)$
- It is not true that $c(f) = d(f)$:

$$X^2 - X = X(X - 1)$$

has $c(f) = 1$, $d(f) = 2$
(the product of two consecutive integers is always even and $f(2) = 2$)

## Motivation

- The very important **Bouniakowsky's conjecture** claims that an irreducible integer polynomial with trivial fixed divisor should produce an infinite number of primes.
- Only the $\deg f = 1$ case is proven. This is Dirichlet's theorem on arithmetic progressions:

$$aX + b$$

produces an infinite number of primes iff $\gcd(a, b) = 1$ iff

$$c(f) = d(f) = 1$$

## Basic results

- **Hensel's theorem** (1896) gives the simplest way of computing the fixed divisor:

$$\boxed{d(f) = \gcd(f(0), \ldots, f(d))}$$

- **Pólya's theorem:** (1915) If $f$ is primitive then $d(f)|d!$
- **Well known to É. Borel:** (1900) Let $p$ be a prime in the divisor which is greater than the degree of $f$. Then $p$ is in the content

$$\boxed{p > d,\ p|d(f) \text{ implies } p|c(f)}$$

## Basic questions

### Amazing!

$$\boxed{\text{If } p|d(f) \text{ and } p > d \text{ then } p|a_0, a_1, \ldots, a_d}$$

### Questions

- How can this be proved in a simple way?
- What happens if $p \leq d$? Is there some arithmetic relation between the coefficients of $f$ which is a multiple of $p$, caused by $p|d(f)$?

## Basic answers

- The standard basis
$$X^0, X^1, X^2, \dots$$
is badly suited for relating $d(f)$ to the coefficients. Change to the combinatorial basis
$$1, X, X(X-1), X(X-1)(X-2), \dots$$
Call the basis elements $\Pi(0), \Pi(1), \Pi(2), \dots$
- Observe that $d(\Pi(i)) = i!$

## Basic answers

- Let $f = \sum_{i=0}^{d} c_i \Pi(i)$. Then it is not difficult to prove

$$\boxed{d(f) = \gcd(c_i \cdot i!)}$$

- In particular, if $p|d(f)$ then $p|c_i$ or $p|i!$. If $p > i$ then $p \not| i!$, hence $p|c_i$. If $p > d$ then $p|c_i$ for all $i$
- Since the $a_i$ are linear combinations of the $c_i$, $p|a_i$ for all $i$
- If $p \leq d$, $p|c_i$ for some $i$ gives some relations for the $a_i$, starring the Stirling numbers of the second kind

**Not the best way to proceed!**

## Basic answers

- Actually, it is better to stick with the canonical basis, and use Hensel's theorem and linear algebra
- $p | d(f)$ iff $f(x) = 0 \pmod{p}$ for all $x = 0, \ldots, d$. Write this as the linear system $V(d) \cdot a = 0$ in $\mathbb{Z}_p$,

$$\begin{pmatrix} 0^0 & 0^1 & \ldots & 0^d \\ 1^0 & 1^1 & \ldots & 1^d \\ \vdots & \ddots & \ddots & \vdots \\ d^0 & d^1 & \ldots & d^d \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_d \end{pmatrix} = 0,$$

where $V(d)$ is a Vandermonde matrix

## Basic answers

$$\begin{pmatrix} 0^0 & 0^1 & \dots & 0^d \\ 1^0 & 1^1 & \dots & 1^d \\ \vdots & \ddots & \ddots & \vdots \\ d^0 & d^1 & \dots & d^d \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_d \end{pmatrix} = 0$$

- $\det(V(d))$ is the product of the differences $i - j$ for $0 \leq j < i \leq d$
- Hence, if $d < p$, then $p \not| \det(V(d))$, so $V(d)$ is invertible in $\mathbb{Z}_p$
- The only solution is $a_0, \dots, a_d = 0$ in $\mathbb{Z}_p$

## Basic answers

$$\begin{pmatrix} 0^0 & 0^1 & \dots & 0^d \\ 1^0 & 1^1 & \dots & 1^d \\ \vdots & \ddots & \ddots & \vdots \\ d^0 & d^1 & \dots & d^d \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_d \end{pmatrix} = 0$$

- Now suppose $p \leq d$. Then $p | \det(V(d))$
- Use Fermat's little theorem,

$$x^p = x \text{ for all } x \in \mathbb{Z}_p$$

and hence group $x$ together with $x^p, x^{p+p-1}, \dots,$
$x^2$ together with $x^{p+2}, x^{p+2+p-1}$, and so on

## Basic answers

- We get new variables $s_1 = a_1 + a_p + a_{2p-1} + \cdots$, $s_2 = a_2 + a_{p+1} + a_{2p} + \cdots$,

$$s_i = \sum_{j \equiv i \pmod{p-1}} a_i, \; i = 1, \ldots, p-1$$

- The new system is

$$\begin{pmatrix} 0^0 & 0^1 & \ldots & 0^{p-1} \\ 1^0 & 1^1 & \ldots & 1^{p-1} \\ \vdots & \ddots & \ddots & \vdots \\ (p-1)^0 & (p-1)^1 & \ldots & (p-1)^{p-1} \end{pmatrix} \begin{pmatrix} a_0 \\ s_1 \\ \vdots \\ s_{p-1} \end{pmatrix} = 0$$

## Basic answers

$$\begin{pmatrix} 0^0 & 0^1 & \dots & 0^{p-1} \\ 1^0 & 1^1 & \dots & 1^{p-1} \\ \vdots & \ddots & \ddots & \vdots \\ (p-1)^0 & (p-1)^1 & \dots & (p-1)^{p-1} \end{pmatrix} \begin{pmatrix} a_0 \\ s_1 \\ \vdots \\ s_{p-1} \end{pmatrix} = 0$$

- Now the matrix of the system is $V(p-1)$, invertible in $\mathbb{Z}_p$
- The only solution is $a_0, s_1, \dots, s_{p-1} = 0$ in $\mathbb{Z}_p$

$$\boxed{p|d(f) \text{ iff } p|a_0, \sum_k a_{1+k(p-1)}, \dots, \sum_k a_{p-1+k(p-1)}}$$

**Example:** $3|d\left(\sum_{i=0}^{6} a_i X^i\right)$ iff $3|a_0, a_1 + a_3 + a_5, a_2 + a_4 + a_6$

Relations between coefficients

Brox



## Generalization

- Given $n \in \mathbb{N}$, the polynomials $f \in \mathbb{Z}[X]$ such that $n | d(f)$ form an ideal $I_n$
- $I_n$ has been studied before, and described by sets of generators
- **Goal:** To describe $I_n$ in terms of a smallest set of **implicit relations** for the coefficients of $f$
- This is **doable**: By Hensel's theorem, we get the relations in form of a Vandermonde system of linear equations (over the commutative ring $\mathbb{Z}_n$), with noninvertible matrix $V(d)$ in general. Then...

## Generalization

...we can do an approximation of **Gaussian elimination**:

1. Over $\mathbb{Z}$ we have the **Hermite normal form** $H$ of $V(d)$, which is upper triangular (with some other properties) and so that there exists a unimodular $U$ such that

$$UV(d) = H$$

2. Since $U$ is **unimodular**, the Hermite normal form projects well to $\mathbb{Z}_n$. So we can equivalently put $V(d)$ in triangular form in $\mathbb{Z}_n$
3. We can further simplify $H$ by multiplying pivots by the units in $\mathbb{Z}_n^*$

This way we get a minimum system of implicit equations

## Generalization

**Question:** Is this good enough?

- The computation of the Hermite normal form runs in polynomial time, but the matrix is of order $n$, while the cardinal of the minimal system could be much smaller
- An specific Hermite plus pivots algorithm over $\mathbb{Z}_n$ needs to be implemented (also, in $\mathbb{Z}$ the entries of $H$ grow fast)

**Question:** Can we do better?

- In the prime case we used Fermat's theorem to reduce the system to its minimal expression
- Let's try something similar

## Bumpy road Fermat's little theorem

- Euler's theorem on $\phi(n)$ is of no use to us, it justs ignores the bad elements
- We need a result for all $x \in \mathbb{Z}_n$
- The **Lucas-Bachmann-Singmaster theorem** (1966):

$$x^{\lambda(n)+m(n)} \equiv x^{m(n)} \pmod{n},$$

  and this is the smallest identity of its kind
- $\lambda(n)$ is **Carmichael's function** (an improvement on $\phi(n)$)
- $m(n)$ is the **highest exponent** in the prime decomposition of $n$

## Bumpy road Fermat's little theorem

**Pros:**

- With this trick we reduce the problem to

$$V(\lambda(n) + m(n) - 1)$$

- The reduction is the simplest possible: just group coefficients in sums as before

**Cons:**

- We need the factorization of $n$
- $\lambda(n)$ is quite large most of the time, probably not the best possible reduction

## Bumpy road Fermat's little theorem

| $n$ | $\lambda(n)$ | $m(n)$ | $\lambda(n)+m(n)-1$ |
|---|---|---|---|
| 2 | 1 | 1 | 1 |
| 3 | 2 | 1 | 2 |
| 4 | 2 | 2 | 3 |
| 5 | 4 | 1 | 4 |
| 6 | 2 | 1 | 2 |
| 7 | 6 | 1 | 6 |
| 8 | 2 | 3 | 4 |
| 9 | 6 | 2 | 7 |
| 10 | 4 | 1 | 4 |
| 12 | 2 | 2 | 3 |
| 14 | 6 | 1 | 6 |
| 15 | 4 | 1 | 4 |
| 16 | 4 | 4 | 7 |

## Kempner to the rescue

**Question:** How can we do better?

- We are actually looking at $\mathbb{Z}_n$ as a polynomial identity ring
- We need not the simplest, but a **smallest degree** polynomial identity of $\mathbb{Z}_n$ in one variable
- We also need it to be primitive (monic)
- That identity is given precisely by a smallest degree polynomial inside $I_n$, the ideal of integer polynomials whose fixed divisor contains $n$
- The best description of $I_n$ in terms of generators was given by Kempner (1918)

## Kempner to the rescue

- Recall that $\Pi(i) = X(X-1)\cdots(X-i+1)$
- **Kempner's theorem:** For any $n \in \mathbb{N}$, the ideal of integer polynomials whose fixed divisor contains $n$ is generated by all the polynomials of the form

$$\frac{n}{k}\Pi(\mu(k)),$$

where $k$ is a divisor of $n$ and $\mu$ is the **Kempner function**

## Kempner to the rescue

- The **Kempner function** $\mu(n)$ returns the smallest $m$ such that $n|m!$
- Example: $\mu(6) = 3$ since $6|3!$, $6 \not| 2!$
- For a prime $p$, $\mu(p) = p$ and $\mu(p^k) = kp$ while $k \leq p$, but $\mu(p^{p+1}) = \mu(p^p) = p^2$
- **Why does this matter?** Because $n$ already divides the product of $\mu(n)$ consecutive numbers, and perhaps $\mu(n) < n$.

## Kempner to the rescue

- **Corollary 1:** The smallest monic identity of $\mathbb{Z}_n$ in one variable has degree $\mu(n)$
- **Corollary 2:** If $n$ is in the fixed divisor of a polynomial of degree less than $\mu(n)$ then $f$ is not primitive, it has a divisor of $n$ in its content

## Kempner to the rescue

| $n$ | $\mu(n) - 1$ | $\lambda(n) + \mu(n) - 1$ |
|---|---|---|
| 4 | 3 | 3 |
| 6 | 2 | 2 |
| 8 | 3 | 4 |
| 9 | 5 | 7 |
| 10 | 4 | 4 |
| 15 | 4 | 4 |
| 16 | 5 | 7 |
| 25 | 9 | 21 |
| 27 | 8 | 20 |
| 81 | 8 | 57 |

# Algorithm

**To compute a minimal system of implicit relations for $I_n$:**

1. **Find** some $g \in I_n$ monic **of minimal degree** $\mu(n)$, for example $\Pi(\mu(n))$, and compute it in $\mathbb{Z}_n$
2. This gives a relation $x^{\mu(n)} = \sum_{i=1}^{\mu(n)-1} \alpha_i x^i$ or all $x \in \mathbb{Z}_n$
3. **Reduce all powers** $x^i$ with $i \geq \mu(n)$ with that relation. This can be done in closed form, since it amounts to solving a linear homogeneous recurrence relation (kudos to Stephan Pfannerer for the help!)
4. The evaluation of a generic polynomial $f$ is reduced to an expression of the form $\sum_{i=1}^{\mu(n)-1} S_i x^i + a_0$
5. Carry the Vandermonde matrix $V(\mu(n)-1)$ to triangular form $H$
6. Solve $HS = 0$, where $S = [S_{\mu-1}, \ldots, S_1, a_0]^T$

## Algorithm

**Example:** Implicit relations for $I_9$

- $\mu(9) = 6$
- Pick $g = (X^3 - X)^2$
  (it works since $3 | x^3 - x$ for all $x \in \mathbb{Z}$).
  This is $X^6 - 2X^4 + 2X^2$ in $\mathbb{Z}_9$
- Hence $x^6 = 2(x^4 - x^2)$ for all $x \in \mathbb{Z}_9$
- If $i \geq 6$,

$$x^i = 2(2i+1)x^2 + 2(4-2i)x^4 \text{ if } i \text{ even,}$$
$$x^i = 2(2i-1)x^3 + 2(6-2i)x^5 \text{ if } i \text{ odd}$$

# Algorithm

**Example:** Implicit relations for $I_9$

- Now any $f$ evaluates as $Ax^5 + Bx^4 + Cx^3 + Dx^2 + Ex + a_0$ for $x \in \mathbb{Z}_9$
- Triangularize $V(\mu(9) - 1) = V(5)$ in $\mathbb{Z}_9$ (we skip the 0 row):

$$\begin{pmatrix} 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 3 & 0 & 0 \\ 0 & 0 & 0 & 3 & 0 \\ 0 & 0 & 0 & 0 & 3 \end{pmatrix}$$

**Example:** Implicit relations for $I_9$

- Solve

$$\begin{pmatrix} 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 3 & 0 & 0 \\ 0 & 0 & 0 & 3 & 0 \\ 0 & 0 & 0 & 0 & 3 \end{pmatrix} \begin{pmatrix} A \\ B \\ C \\ D \\ E \end{pmatrix} = 0$$

- The equations are

$$A + C + E = 0, B + D = 0$$
$$3C = 0, 3D = 0, 3E = 0$$

- For deg $f = 13$ this gives

$$a_0 = 0,\ a_3 + a_5 + \cdots + a_{13} = 0,\ a_2 + a_4 + \cdots + a_{12} = 0$$
$$3a_1 = 0, 6(a_{13} + a_7) + 3(a_9 + a_3) = 0, 6(a_{12} + a_6) + 3(a_8 + a_2) = 0$$

# Algorithm

**Question:** Can we give a closed form for the reduction of $V(\mu(n)-1)$ in $\mathbb{Z}_n$, if the factorization of $n$ is known?

- This way we could give a formula instead of an algorithm

$$V(\mu(20)-1) \rightsquigarrow \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 2 & 0 & 2 \\ 0 & 0 & 4 & 2 \\ 0 & 0 & 0 & 4 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 4 & 0 \\ 0 & 0 & 0 & 2 \end{pmatrix}$$

## Multivariate case

- Implicit equations are well carried to the multivariate case by induction
- If $f(x) = 0$ for all $x \in \mathbb{Z}$ implies

$$\sum_{i \in A} \alpha_i a_i = 0$$

with $f = \sum_i a_i X^i$, then $g(x, y) = 0$ for all $x, y \in \mathbb{Z}$ implies

$$\sum_{i,j \in A} \alpha_i \alpha_j a_{ij} = 0$$

for $g = \sum_{i,j} a_{ij} X^i Y^j$, and so on.