Two Ways to Count Solutions to Polynomial Equations

Margaret Robinson

Mount Holyoke College

May 24, 2013
Generating functions

A generating function is a clothesline on which we hang up a sequence of numbers for display.—Herbert Wilf

Given a sequence of numbers \( a_0, a_1, a_2, \ldots \) we can form its generating function

\[
f(t) = \sum_{n=0}^{\infty} a_n t^n
\]
Rational Generating Functions

Using formulas like

\[ \sum_{n=0}^{\infty} t^n = \frac{1}{1-t}, \]

\[ \sum_{n=0}^{\infty} (n+1)t^n = \frac{1}{(1-t)^2} \]

and

\[ \sum_{n=0}^{\infty} \left( \frac{(n+1)(n+2)}{2} \right) t^n = \frac{1}{(1-t)^3}, \]

Some generating functions can be seen to be rational functions of \( t \)!
First Generating Function

Consider a prime number $p$ and a polynomial $f(x) = f(x_1, \ldots, x_n)$ in $n$ variables with coefficients in $\mathbb{Z}$ and consider $f$ with coefficients reduced modulo $p$. 
First Generating Function

Consider a prime number $p$ and a polynomial $f(x) = f(x_1, ..., x_n)$ in $n$ variables with coefficients in $\mathbb{Z}$ and consider $f$ with coefficients reduced modulo $p$.

Let

$$|N_e| = \text{Card} \{ x \in \mathbb{F}_{p^e}^{(n)} \mid f(x) = 0 \text{ in } \mathbb{F}_{p^e} \}.$$
First Generating Function
Consider a prime number $p$ and a polynomial $f(x) = f(x_1, \ldots, x_n)$ in $n$ variables with coefficients in $\mathbb{Z}$ and consider $f$ with coefficients reduced modulo $p$.

- Let
  $$|N_e| = \text{Card} \left\{ x \in \mathbb{F}_{p^e}^{(n)} \mid f(x) = 0 \text{ in } \mathbb{F}_{p^e} \right\}.$$  

- Define the **Weil Poincaré Series** as:
  $$P_{Weil}(t) = \sum_{e=0}^{\infty} |N_e| \ t^e$$
  with $|N_0| = 1$ and $|N_e| \leq p^{ne}$. 
Second Generating Function

Consider a prime number $p$ and a polynomial $f(x) = f(x_1, \ldots, x_n)$ in $n$ variables with coefficients in $\mathbb{Z}$ and for $x \in \mathbb{Z}^{(n)}$. 
Second Generating Function
Consider a prime number $p$ and a polynomial $f(x) = f(x_1, \ldots, x_n)$ in $n$ variables with coefficients in $\mathbb{Z}$ and for $x \in \mathbb{Z}^{(n)}$.

Let
\[
|\mathcal{N}_d| = \text{Card} \ \{x \mod p^d \mid f(x) \equiv 0 \mod p^d\}.
\]
Second Generating Function

Consider a prime number $p$ and a polynomial $f(x) = f(x_1, ..., x_n)$ in $n$ variables with coefficients in $\mathbb{Z}$ and for $x \in \mathbb{Z}^{(n)}$.

- Let
  $$|\overline{N_d}| = \text{Card} \{ x \mod p^d \mid f(x) \equiv 0 \mod p^d \}.$$  
- Define the **Igusa Poincaré Series** as:
  $$P_{\text{Igusa}}(t) = \sum_{d=0}^{\infty} |\overline{N_d}| \ t^d$$

with $|\overline{N_0}| = 1$ and $|\overline{N_d}| \leq p^{nd}$.
Both these generating functions are known to be rational functions of $t$. 
Both these generating functions are known to be rational functions of $t$.

- Theorem (Dwork, 1959) $P_{\text{Weil}}(t)$ is a rational function of $t$. $\left| N_e \right| = \sum_{i=1}^{u} \alpha_i^e - \sum_{i=1}^{v} \beta_i^e$

(Special case of the first part of the Weil Conjectures 1949.)
Both these generating functions are known to be rational functions of $t$.

**Theorem (Dwork, 1959)** $P_{\text{Weil}}(t)$ is a rational function of $t$. 
$$|N_e| = \sum_{i=1}^{u} \alpha_i^e - \sum_{i=1}^{v} \beta_i^e$$

(Special case of the first part of the Weil Conjectures 1949.)

**Theorem (Igusa, 1975)** $P_{\text{Igusa}}(t)$ is a rational function of $t$.

(Conjectured in exercises of the 1966 textbook by Borevich and Shafarevich.)
Example 1

Let

\[ f(x) = x \]

Then

\[ |N_e| = |\overline{N_d}| = 1. \]

Hence,
Example 1

Let

\[ f(x) = x \]

Then

\[ |N_e| = |\overline{N}_d| = 1. \]

Hence,

\[ P_{\text{Weil}}(t) = P_{\text{Igusa}}(t) = \sum_{e=0}^{\infty} t^e = \]
Example 1

Let

\[ f(x) = x \]

Then

\[ |N_e| = |\overline{N}_d| = 1. \]

Hence,

\[ P_{\text{Weil}}(t) = P_{\text{Igusa}}(t) = \sum_{e=0}^{\infty} t^e = \frac{1}{(1 - t)} \]
Example 2

Let

\[ f(x, y) = xy \]

Then

\[ |N_e| = 2p^e - 1. \]

Hence,
Example 2

Let

\[ f(x, y) = xy \]

Then

\[ |N_e| = 2p^e - 1. \]

Hence,

\[ P_{\text{Weil}}(t) = \sum_{e=0}^{\infty} (2p^e - 1) t^e = \]
Example 2

Let

\[ f(x, y) = xy \]

Then

\[ |N_e| = 2p^e - 1. \]

Hence,

\[
P_{\text{Weil}}(t) = \sum_{e=0}^{\infty} (2p^e - 1)t^e = \frac{1 + (p - 2)t}{(1 - t)(1 - pt)}
\]
Example 2 (continued)

Counting points solutions of $f(x, y) = xy \mod p^d$ for each $d$, we see that $|\overline{N}_d|$ is more complicated but we find the recursion relation:

$$|\overline{N}_0| = 1$$
Example 2 (continued)
Counting points solutions of \( f(x, y) = xy \mod p^d \) for each \( d \), we see that \( |\overline{N}_d| \) is more complicated but we find the recursion relation:

\[
\begin{align*}
|\overline{N}_0| &= 1 \\
|\overline{N}_1| &= 2p - 1
\end{align*}
\]
Example 2 (continued)

Counting points solutions of \(f(x, y) = xy \mod p^d\) for each \(d\), we see that \(|\overline{N}_d|\) is more complicated but we find the recursion relation:

\[
\begin{align*}
|\overline{N}_0| &= 1 \\
|\overline{N}_1| &= 2p - 1 \\
|\overline{N}_2| &= p(|\overline{N}_1| - 1) + p^2|\overline{N}_0| = 3p^2 - 2p
\end{align*}
\]
Example 2 (continued)

Counting points solutions of \( f(x, y) = xy \mod p^d \) for each \( d \), we see that \( |\overline{N}_d| \) is more complicated but we find the recursion relation:

\[
\begin{align*}
|\overline{N}_0| &= 1 \\
|\overline{N}_1| &= 2p - 1 \\
|\overline{N}_2| &= p(|\overline{N}_1| - 1) + p^2|\overline{N}_0| = 3p^2 - 2p \\
|\overline{N}_d| &= p^{d-1}(|\overline{N}_1| - 1) + p^2|\overline{N}_{d-2}|
\end{align*}
\]

With careful counting and induction we get the closed form expression:
Two Ways to Count Solutions to Polynomial Equations

Margaret Robinson

Example 2 (continued)

Counting points solutions of $f(x, y) = xy \mod p^d$ for each $d$, we see that $|\overline{N}_d|$ is more complicated but we find the recursion relation:

\[
\begin{align*}
|\overline{N}_0| &= 1 \\
|\overline{N}_1| &= 2p - 1 \\
|\overline{N}_2| &= p(|\overline{N}_1| - 1) + p^2|\overline{N}_0| = 3p^2 - 2p \\
|\overline{N}_d| &= p^{d-1}(|\overline{N}_1| - 1) + p^2|\overline{N}_{d-2}|
\end{align*}
\]

With careful counting and induction we get the closed form expression:

\[
|\overline{N}_d| = (d + 1)p^d - dp^{d-1}
\]
Example 2 (continued)
The Igusa Poincaré series for the polynomial $f(x, y) = xy$ is:

$$P_{Igusa}(t) = \sum_{d=0}^{\infty} \left[ (d + 1)p^d - dp^{d-1} \right] t^d$$
Example 2 (continued)
The Igusa Poincaré series for the polynomial \( f(x, y) = xy \) is:

\[
P_{Igusa}(t) = \sum_{d=0}^{\infty} [(d + 1)p^d - dp^{d-1}] t^d
\]

\[
= 1 + \sum_{d=1}^{\infty} (d + 1)(pt)^d - dp^{-1}(pt)^d
\]
Example 2 (continued)
The Igusa Poincaré series for the polynomial $f(x, y) = xy$ is:

$$P_{Igusa}(t) = \sum_{d=0}^{\infty} [(d + 1)p^d - dp^{d-1}]t^d$$

$$= 1 + \sum_{d=1}^{\infty} (d + 1)(pt)^d - dp^{-1}(pt)^d$$

$$= 1 + \sum_{d=1}^{\infty} d(1 - p^{-1})(pt)^d + \sum_{d=1}^{\infty} (pt)^d$$
Example 2 (continued)
The Igusa Poincaré series for the polynomial $f(x, y) = xy$ is:

\[
P_{Igusa}(t) = \sum_{d=0}^{\infty} [(d + 1)p^d - dp^{d-1}] t^d
\]

\[
= 1 + \sum_{d=1}^{\infty} (d + 1)(pt)^d - dp^{-1}(pt)^d
\]

\[
= 1 + \sum_{d=1}^{\infty} d(1 - p^{-1})(pt)^d + \sum_{d=1}^{\infty} (pt)^d
\]

\[
= 1 + \frac{(1 - p^{-1})(pt)}{(1 - pt)^2} + \frac{pt}{(1 - pt)}
\]
Example 2 (continued)

The Igusa Poincaré series for the polynomial \( f(x, y) = xy \) is:

\[
P_{Igusa}(t) = \sum_{d=0}^{\infty} [(d + 1)p^d - dp^{d-1}]t^d
\]

\[
= 1 + \sum_{d=1}^{\infty} (d + 1)(pt)^d - dp^{-1}(pt)^d
\]

\[
= 1 + \sum_{d=1}^{\infty} d(1 - p^{-1})(pt)^d + \sum_{d=1}^{\infty} (pt)^d
\]

\[
= 1 + \frac{(1 - p^{-1})(pt)}{(1 - pt)^2} + \frac{pt}{(1 - pt)}
\]

\[
= \frac{1 - t}{(1 - pt)^2}
\]
Example 3

Let

\[ f(x, y) = y^2 - x^3 \]

\[ P_{Igusa}(p^{-2}t) = \sum_{d=0}^{\infty} |N_d| (p^{-2}t)^d \]
Example 3

Let

\[ f(x, y) = y^2 - x^3 \]

\[
P_{\text{Igusa}}(p^{-2}t) = \sum_{d=0}^{\infty} |N_d| (p^{-2}t)^d
\]

\[
= \frac{(1 + p^{-2}t^2 - p^{-3}t^2 - p^{-6}t^6)}{(1 - p^{-1}t)(1 - p^{-5}t^6)}
\]
Example 3 (continued)

From the Igusa Poincaré series for $f(x, y) = y^2 - x^3$, we get a recursion relation of the form:

$$|\overline{N_0}| = 1$$
Example 3 (continued)

From the Igusa Poincaré series for \( f(x, y) = y^2 - x^3 \), we get a recursion relation of the form:

\[
\begin{align*}
|\bar{N}_0| &= 1 \\
|\bar{N}_1| &= p
\end{align*}
\]
Example 3 (continued)

From the Igusa Poincaré series for $f(x, y) = y^2 - x^3$, we get a recursion relation of the form:

\[
\begin{align*}
|\mathcal{N}_0| &= 1 \\
|\mathcal{N}_1| &= p \\
|\mathcal{N}_d| &= (2p - 1)p^{d-1} \quad \text{for } d = 2, 3, 4, 5
\end{align*}
\]
Example 3 (continued)

From the Igusa Poincaré series for
\[ f(x, y) = y^2 - x^3, \]
we get a recursion relation of the form:

\[
\begin{align*}
|N_0| &= 1 \\
|N_1| &= p \\
|N_d| &= (2p - 1)p^{d-1} \quad \text{for } d = 2, 3, 4, 5 \\
|N_d| &= p^{d-1}(p - 1) + |N_{d-6}|p^7 \quad \text{for } d > 5
\end{align*}
\]
Example 3 (continued)

Using partial fractions on $P_{lgusa}(t)$, we get the following closed form formulas for the $|\overline{N}_d|$: 

$$|\overline{N}_0| = 1 \text{ for } k \geq 0$$
Example 3 (continued)

Using partial fractions on $P_{Igusa}(t)$, we get the following closed form formulas for the $|\overline{N}_d|$:

\[
\begin{align*}
|\overline{N}_0| &= 1 \text{ for } k \geq 0 \\
|\overline{N}_{6k}| &= (p^{k+1} + p^k - 1)p^{6k-1} \\
|\overline{N}_{6k+1}| &= (p^{k+1} + p^k - 1)p^{6k} \\
|\overline{N}_{6k+2}| &= (2p^{k+1} - 1)p^{6k+1} \\
|\overline{N}_{6k+3}| &= (2p^{k+1} - 1)p^{6k+2} \\
|\overline{N}_{6k+4}| &= (2p^{k+1} - 1)p^{6k+3} \\
|\overline{N}_{6k+5}| &= (2p^{k+1} - 1)p^{6k+4}
\end{align*}
\]
Bernstein’s Theorem

Bernstein’s theorem states that for \( f(x) \) a non-zero polynomial in \( \mathbb{Q}[x_1, \ldots, x_n] \), there exists a differential operator \( P \) in \( \mathbb{Q}[s, x_1, \ldots, x_n, \partial/\partial x_1, \ldots, \partial/\partial x_n] \) and a unique, monic polynomial of smallest degree \( b(s) \) in \( \mathbb{Q}[s] \) such that

\[
P \cdot f(x)^{s+1} = b(s)f(x)^s
\]

for \( s \) in \( \mathbb{Z} \).
Bernstein’s Theorem
Bernstein’s theorem states that for $f(x)$ a non-zero polynomial in $\mathbb{Q}[x_1, \ldots, x_n]$, there exists a differential operator $P$ in $\mathbb{Q}[s, x_1, \ldots, x_n, \partial/\partial x_1, \ldots, \partial/\partial x_n]$ and a unique, monic polynomial of smallest degree $b(s)$ in $\mathbb{Q}[s]$ such that

$$P \cdot f(x)^{s+1} = b(s)f(x)^s$$

for $s$ in $\mathbb{Z}$. Conjecture: Zeros of the Bernstein polynomial are related to poles of $P_{\text{Igusa}}(p^{-n}t)$
Example 1

When \( f(x) = x \) the differential operator is \( P = \frac{\partial}{\partial x} \) and the Bernstein polynomial is

\[
    b(s) = (s + 1)
\]

since we have that

\[
    P \cdot x^{s+1} = (s + 1)x^s.
\]
Example 1

When $f(x) = x$ the differential operator is $P = \frac{\partial}{\partial x}$ and the Bernstein polynomial is

$$b(s) = (s + 1)$$

since we have that

$$P \cdot x^{s+1} = (s + 1)x^s.$$

Note that $s = -1$ is the zero of the Bernstein polynomial.
Example 2

When $f(x, y) = xy$ the differential operator is

$$P = \frac{\partial}{\partial x} \left( \frac{\partial}{\partial y} \right)$$

and the Bernstein polynomial is

$$b(s) = (s + 1)^2$$

since we have that

$$P \cdot (xy)^{s+1} = (s + 1)^2(xy)^s.$$
Example 2

When \( f(x, y) = xy \) the differential operator is

\[
P = \frac{\partial}{\partial x} \bigg( \frac{\partial}{\partial y} \bigg)
\]

and the Bernstein polynomial is

\[
b(s) = (s + 1)^2
\]

since we have that

\[
P \cdot (xy)^{s+1} = (s + 1)^2(xy)^s.
\]

Note that \( s = -1 \) is a double root of \( b(s) \).
Example 3

When $f(x, y) = y^2 - x^3$ the differential operator is
Example 3

When \( f(x, y) = y^2 - x^3 \) the differential operator is

\[
P = \frac{1}{27} \frac{\partial^3}{\partial x^3} + \frac{1}{6} x \frac{\partial^3}{\partial x \partial y^2} + \frac{1}{8} y \frac{\partial^3}{\partial y^3} + \frac{3}{8} \frac{\partial^2}{\partial y^2}
\]

and the Bernstein polynomial is
Example 3
When $f(x, y) = y^2 - x^3$ the differential operator is

$$P = \frac{1}{27} \frac{\partial^3}{\partial x^3} + \frac{1}{6} x \frac{\partial^3}{\partial x \partial y^2} + \frac{1}{8} y \frac{\partial^3}{\partial y^3} + \frac{3}{8} \frac{\partial^2}{\partial y^2}$$

and the Bernstein polynomial is

$$b(s) = (s + 1)(s + 5/6)(s + 7/6)$$
Example 3

When $f(x, y) = y^2 - x^3$ the differential operator is

$$P = \frac{1}{27} \frac{\partial^3}{\partial x^3} + \frac{1}{6} x \frac{\partial^3}{\partial x \partial y^2} + \frac{1}{8} y \frac{\partial^3}{\partial y^3} + \frac{3}{8} \frac{\partial^2}{\partial y^2}$$

and the Bernstein polynomial is

$$b(s) = (s + 1)(s + 5/6)(s + 7/6)$$

Note that $s = -1, -5/6, \text{ and } -7/6$ are roots of $b(s)$. 
Mystery

Consider the Igusa Poincaré Series for our three examples:
Consider the Igusa Poincaré Series for our three examples:

\[ P_{\text{Igusa}}(p^{-1}t) = \frac{1}{(1 - p^{-1}t)} \text{ for } f(x) = x \]
Mystery

Consider the Igusa Poincaré Series for our three examples:

\[ P_{\text{Igusa}}(p^{-1}t) = \frac{1}{1 - p^{-1}t} \quad \text{for } f(x) = x \]

\[ P_{\text{Igusa}}(p^{-2}t) = \frac{1 - p^{-2}t}{(1 - p^{-1}t)^2} \quad \text{for } f(x, y) = xy \]
Consider the Igusa Poincaré Series for our three examples:

\[
P_{Igusa}(p^{-1}t) = \frac{1}{(1 - p^{-1}t)} \quad \text{for } f(x) = x
\]

\[
P_{Igusa}(p^{-2}t) = \frac{1 - p^{-2}t}{(1 - p^{-1}t)^2} \quad \text{for } f(x, y) = xy
\]

\[
P_{Igusa}(p^{-2}t) = \frac{1 + p^{-2}t^2 - p^{-3}t^2 - p^{-6}t^6}{(1 - p^{-1}t)(1 - p^{-5}t^6)}
\]
\[
\quad \text{for } f(x, y) = y^2 - x^3
\]
Mystery (continued)

Let $t = p^{-s}$
Mystery (continued)

Let \( t = p^{-s} \)

\[
P_{Igusa}(p^{-1-s}) = \frac{1}{(1 - p^{-1-s})} \text{ for } f(x) = x
\]
Mystery (continued)

Let $t = p^{-s}$

$$P_{Igusa}(p^{-1-s}) = \frac{1}{(1 - p^{-1-s})} \text{ for } f(x) = x$$

$$P_{Igusa}(p^{-2-s}) = \frac{1 - p^{-2-s}}{(1 - p^{-1-s})^2} \text{ for } f(x, y) = xy$$
Mystery (continued)

Let \( t = p^{-s} \)

\[
\text{P}_{Igusa}(p^{-1-s}) = \frac{1}{(1 - p^{-1-s})} \quad \text{for } f(x) = x
\]

\[
\text{P}_{Igusa}(p^{-2-s}) = \frac{1 - p^{-2-s}}{(1 - p^{-1-s})^2} \quad \text{for } f(x, y) = xy
\]

\[
\text{P}_{Igusa}(p^{-2-s}) = \frac{(1 + p^{-2-2s} - p^{-3-2s} - p^{-6-6s})}{(1 - p^{-1-s})(1 - p^{-5-6s})} \quad \text{for } f(x, y) = y^2 - x^3
\]
Let \( t = p^{-s} \)

\[
P_{Igusa}(p^{-1-s}) = \frac{1}{(1 - p^{-1-s})} \quad \text{for } f(x) = x
\]

\[
P_{Igusa}(p^{-2-s}) = \frac{1 - p^{-2-s}}{(1 - p^{-1-s})^2} \quad \text{for } f(x, y) = xy
\]

\[
P_{Igusa}(p^{-2-s}) = \frac{(1 + p^{-2-2s} - p^{-3-2s} - p^{-6-6s})}{(1 - p^{-1-s})(1 - p^{-5-6s})} \quad \text{for } f(x, y) = y^2 - x^3
\]

Conjecture: Real poles of the Poincaré series are all zeros of the Bernstein polynomial. Why??
THANK YOU
I hope there is someone here who gets interested in these questions.

My email: robinson@mtholyoke.edu