# Some results on counting roots of polynomials and the Sylvester resultant.

Michael Monagan and Baris Tuncer

*Department of Mathematics, Simon Fraser University, Burnaby, B.C., V5A 1S6, CANADA.*

**Abstract.** We present two results, the first on the distribution of the roots of a polynomial over the ring of integers modulo $n$ and the second on the distribution of the roots of the Sylvester resultant of two multivariate polynomials. The second result has application to polynomial GCD computation and solving polynomial diophantine equations.

**Résumé.** Nous présentons deux résultats: le premier concerne la distribution des racines d'un polynôme sur l'anneau des entiers modulo $n$ et le deuxième concerne la distribution des racines du déterminant de Sylvester de deux polynômes multivariés. Ceci est utile pour le calcul de PGCD et la résolution des équations diophantiennes poly-nomiales.

**Keywords.** roots of polynomials, finite fields, the Sylvester resultant, unlucky evaluation points

## 1   Introduction

Let $\mathbb{F}_q$ denote the finite field with $q$ elements and let $\mathbb{Z}_n$ denote the ring of integers modulo $n$. Let $\mathrm{E}[X]$ denote the expected value of a random variable $X$ and let $\mathrm{Var}[X]$ denote the variance of $X$.

Let $f$ be a polynomial in $\mathbb{F}_q[x]$ of a given degree $d > 0$ and let $X$ be the number of distinct roots of $f$. Schmidt proves in Ch. 4 of [9] that $\mathrm{E}[X] = 1$ and for $d > 1$, $\mathrm{Var}[X] = 1 - 1/q$. This result has been generalized by Knopfmacher and Knopfmacher in [5] who count distinct irreducible factors of a given degree of $f$. The two main results presented in this paper are Theorems 1 and 2 below.

**Theorem 1** *Let $\phi(n) = |\{\, 1 \leq i \leq n : \gcd(i,n) = 1\}|$ denote Euler's totient function. Let $X$ be a random variable which counts the number of distinct roots of a monic polynomial in $\mathbb{Z}_n[x]$ of degree $m > 0$. Then*
  (a) $\mathrm{E}[X] = 1$ *and*
  (b) *if $m = 1$ then $\mathrm{Var}[X] = 0$, otherwise $\mathrm{Var}[X] = \sum_{d|n,d\neq n} \frac{d}{n}\phi(\frac{n}{d}) = \sum_{d|n} \frac{d-1}{n}\phi(\frac{n}{d})$.*
      *In particular, if $n = p^k$ where $p$ is a prime number and $k \geq 1$, $\mathrm{Var}[X] = k(1 - 1/p)$.*

**Theorem 2** *Let $f, g$ be polynomials in $\mathbb{F}_q[x,y]$ of the form $f = c_n x^n + \sum_{i=0}^{n-1}\sum_{j=0}^{n-i} c_{ij}x^i y^j$ and $g = d_m x^m + \sum_{i=0}^{m-1}\sum_{j=0}^{m-i} d_{ij}x^i y^j$ with $c_n \neq 0$ and $d_m \neq 0$, thus of total degree $n$ and $m$ respectively. Let $X$ be a random variable that counts the number of $\gamma \in \mathbb{F}_q$ such that $\gcd(f(x,\gamma), g(x,\gamma)) \neq 1$. If $n > 0$ and $m > 0$ then*
  (a) $\mathrm{E}[X] = 1$ *and*
  (b) $\mathrm{Var}[X] = 1 - 1/q$.

Theorems 1 and 2 were found by computation. We give some details on our computations later in the paper. To prove the results we use a generalization of the Inclusion Exclusion principle (Proposition 1) which allows us to determine $E[X]$ and $Var[X]$ without having explicit formulas for $Prob[X = k]$. Before proving these results we connect Theorem 2 with the Sylvester resultant and with polynomial GCD computation and with solving polynomial diophantine equations.

Let $F$ be a field and let $A$ and $B$ be polynomials in $F[x_0, x_1, \ldots, x_n]$ with positive degree in $x_0$. The Sylvester resultant of $A$ and $B$ in $x_0$, denoted $\mathrm{res}_{x_0}(A, B)$, is the determinant of Sylvester's matrix. We gather the following facts about it into Lemma 1 below. Proofs may be found in Ch. 3 of [3]. Note, in the Lemma $\deg A$ denotes the total degree of $A$.

**Lemma 1** *Let $R = \mathrm{res}_{x_0}(A, B)$*

> *(i) $R$ is a polynomial in $F[x_1, \ldots, x_n]$ ($x_0$ is eliminated),*
> *(ii) $\deg R \leq \deg A \deg B$ (Bezout bound).*
>
> *For $A$ and $B$ monic in $x_0$ and $\alpha \in F^n$*
>
> *(iii) $\gcd(A(x_0, \alpha), B(x_0, \alpha)) \neq 1 \iff \mathrm{res}_{x_0}(A(x_0, \alpha), B(x_0, \alpha)) = 0$ and*
> *(iv) $\mathrm{res}_{x_0}(A(x_0, \alpha), B(x_0, \alpha)) = R(\alpha)$.*

Properties (iii) and (iv) connect the roots of the resultant with Theorem 2 and 3.

## 1.1 Polynomial GCD computation and polynomial diophantine equations.

Our motivation comes from the following problems in computer algebra. Let $A, B$ be polynomials in $\mathbb{Z}[x_0, x_1, \ldots, x_n]$ and $G = \gcd(A, B)$. Thus $A = G\widehat{A}$ and $B = G\widehat{B}$ for some polynomials $\widehat{A}$ and $\widehat{B}$ called the cofactors of $A$ and $B$. Modular GCD algorithms compute $G$ modulo a sequence of primes $p_1, p_2, p_3, \ldots$ and recover the integer coefficients of $G$ using Chinese remaindering. The fastest algorithms for computing $G$ modulo a prime $p$ interpolate $G$ from univariate images. Maple, Magma and Mathematica all currently use Zippel's algorithm (see [11, 4]). Let us write

$$A = \sum_{i=0}^{k} a_i x_0^i, \;\; B = \sum_{i=0}^{l} b_i x_0^i, \;\; \text{and} \;\; G = \sum_{i=0}^{m} c_i x_0^i$$

where the coefficients $a_i, b_i, c_i \in \mathbb{F}_p[x_1, \ldots, x_n]$. Zippel's algorithm picks points $\alpha_i \in \mathbb{F}_p^n$, computes monic univariate images of $G$

$$g_i = \gcd(A(x_0, \alpha_i), B(x_0, \alpha_i)),$$

scales them (details omitted), then interpolates the coefficients $c_i(x_1, \ldots, x_n)$ of $G$ from the coefficients of these (scaled) images.

What if $\gcd(\widehat{A}(x_0, \alpha_j), \widehat{B}(x_0, \alpha_j)) \neq 1$ for some $j$? For example, if $\widehat{A} = x_0^2 + x_2$ and $\widehat{B} = x_0^2 + x_2 + (x_1 - 1)$ then $\gcd(\widehat{A}, \widehat{B}) = 1$ but $\gcd(\widehat{A}(x_0, 1, \beta), \widehat{B}(x_0, 1, \beta)) \neq 1$ for all $\beta \in \mathbb{F}_p$. The evaluation points $(1, \beta)$ are said to be *unlucky*. We cannot use the images $\gcd(A(x_0, 1, \beta), B(x_0, 1, \beta))$ to interpolate $G$. The same issue of unlucky evaluation points arises in our current work in [6] where, given polynomials $a, b, c \in \mathbb{Z}[x_0, x_1, \ldots, x_n]$ with $\gcd(a, b) = 1$ we want to solve the diophantine equation $\sigma a + \tau b = c$ for $\sigma$ and $\tau$ in $\mathbb{Z}[x_0, x_1, \ldots, x_n]$ by interpolating $\sigma$ and $\tau$ modulo a prime $p$ from univariate images.

What is the maximum number of unlucky evaluation points that can occur? And what is the expected number of unlucky evaluation points? We answer the first question for $A$ and $B$ monic in $x_0$. Lemma 1

implies $\alpha_j$ is unlucky if and only if $R(\alpha_j) = 0$ where $R = \operatorname{res}_{x_0}(\widehat{A}, \widehat{B}) \in \mathbb{F}_p[x_1, \ldots, x_n]$. If $\alpha_j$ is chosen at random from $\mathbb{F}_p^n$ then applying the Schwarz-Zippel lemma (see [10]) we have

$$\operatorname{Prob}[R(\alpha_j) = 0] \le \frac{\deg R}{p}.$$

Applying Lemma 1(ii) we have $\deg R \le \deg \widehat{A} \deg \widehat{B} \le \deg A \deg B$. So if the algorithm needs, say, $t$ images to interpolate $G$ modulo $p$, then we can avoid unlucky evaluation points with high probability if we pick $p \gg t \deg A \deg B$.

But this is an upper bound – a worst case bound for the GCD algorithm. Researchers in computer algebra have observed that unlucky evaluation points are rare in practice and that we "never see them" when testing algorithms on random inputs. Theorems 2 and 3 give first results on the distribution of unlucky evaluation points. In particular, for coprime $\widehat{A}$ and $\widehat{B}$ of positive degree, Theorem 3 (page 11) implies $\operatorname{Prob}[\alpha_j \text{ is unlucky}] < 1/p$.

## 2 Results and Proofs

Given a set $U$ and the finite collection of sets $\Gamma = \{A_i, i = 0, \ldots, n-1\}$ where each $A_i \subseteq U$, let us define $C_0 = U$, $C_{n+1} := \emptyset$ and, for $1 \le k \le n$,

$$C_k := \bigcup_{i_1 < \cdots < i_k} (A_{i_1} \cap A_{i_2} \cdots \cap A_{i_k}).$$

Then for $1 \le k \le n$, $C_k$ is the union of all possible intersections of the $k-$subsets of the collection $\Gamma$. In particular $C_1 = A_0 \cup A_1 \cup \cdots \cup A_{n-1}$ and $C_n = A_0 \cap A_1 \cap \cdots \cap A_{n-1}$. Let $B_k := C_k - C_{k+1}$ for $0 \le k \le n$. Observe that $C_k \supseteq C_{k+1}$, so $|B_k| = |C_k| - |C_{k+1}|$. Let us also define

$$b_k := |B_k| \text{ and } t_k := \sum_{i_1 < \cdots < i_k} |A_{i_1} \cap A_{i_2} \cdots \cap A_{i_k}|.$$

We have $t_1 = \sum_{i=0}^{n-1} |A_i|$ and $t_2 = \sum_{0 \le i < j < n} |A_i \cap A_j|$. We also have $b_n = t_n$ and $b_{n-1} = t_{n-1} - \binom{n}{1} b_n$. Now $A_0 \cap A_1 \cap \cdots \cap A_{n-1}$ is a subset of $\binom{n}{n-2} = \binom{n}{2}$ sets of the form $A_{i_1} \cap A_{i_2} \cap \cdots \cap A_{i_{n-2}}$ and each $(n-1)$-section $A_{i_1} \cap A_{i_2} \cap \cdots \cap A_{i_{n-1}}$ is a subset of $\binom{n-1}{n-2} = \binom{n-1}{1}$ sets of the form $A_{i_1} \cap A_{i_2} \cap \cdots \cap A_{i_{n-2}}$ with $i_1 < i_2 < \cdots < i_{n-2}$. Therefore $b_{n-2} = t_{n-2} - \binom{n-1}{1} b_{n-1} - \binom{n}{2} b_n$.

Similarly, since each $(n - k + i)$-section is a subset of $\binom{n-k+i}{i}$ intersections of $(n - k)$ sets for $i = 1, \ldots, k$, we have the recursive formula

$$b_{n-k} = t_{n-k} - \sum_{i=1}^{k} \binom{n-k+i}{i} b_{n-k+i} \text{ for } k = 0, \ldots, n. \tag{1}$$

**Lemma 2** *Following the notation introduced above*

$$b_{n-k} = \sum_{i=0}^{k} (-1)^i \binom{n-k+i}{i} t_{n-k+i} \text{ for } k = 0, \ldots, n. \tag{2}$$

**Proof:** We will prove the claim by strong induction on $k$. For $k = 0$ we have $b_n = t_n$. Now assume that the claim is true for any integer $i \leq k$ in place of $k$.

By the recursive formula (1) we have

$$b_{n-(k+1)} = t_{n-(k+1)} - \binom{n-k}{1}b_{n-k} - \binom{n-k+1}{2}b_{n-k+1} - \cdots - \binom{n}{k+1}b_n.$$

On the other hand by induction we have the following equations

$$
\begin{aligned}
b_n &= t_n \\
b_{n-1} &= t_{n-1} - \binom{n}{1}t_n \\
b_{n-2} &= t_{n-2} - \binom{n-1}{1}t_{n-1} + \binom{n}{2}t_n \\
&\;\;\vdots \\
b_{n-k} &= t_{n-k} - \binom{n-k+1}{1}t_{n-k+1} + \cdots + (-1)^k\binom{n}{k}t_n.
\end{aligned}
$$

It follows that

$$
\begin{aligned}
-\binom{n}{k+1}b_n &= -\binom{n}{k+1}t_n \\
-\binom{n-1}{k}b_{n-1} &= -\binom{n-1}{k}t_{n-1} + \binom{n-1}{k}\binom{n}{1}t_n \\
-\binom{n-2}{k-1}b_{n-2} &= -\binom{n-2}{k-1}t_{n-2} + \binom{n-2}{k-1}\binom{n-1}{1}t_{n-1} - \binom{n-2}{k-1}\binom{n}{2}t_n \\
&\;\;\vdots \\
-\binom{n-k}{1}b_{n-k} &= -\binom{n-k}{1}t_{n-k} + \binom{n-k}{1}\binom{n-k+1}{1}t_{n-k+1} - \cdots (-1)^{k+1}\binom{n-k}{1}\binom{n}{k}t_n.
\end{aligned}
$$

If we sum all these equalities, then on the right hand side the coefficient of $t_n$ is

$c(t_n) = \sum_{i=0}^{k}(-1)^{k-i+1}\binom{n-k+i}{i+1}\binom{n}{k-i}$. For $d \leq k$ one has

$\binom{n-d}{k-d+1}\binom{n}{d} = \frac{(n-d)!}{(n-k-1)!(k-d+1)!}\frac{n!}{(n-d)!d!} = \frac{n!}{(k+1)!(n-k-1)!}\frac{(k+1)!}{d!(k-d+1)!} = \binom{n}{k+1}\binom{k+1}{d}$.

Then $c(t_n) = \binom{n}{k+1}\sum_{i=0}^{k}(-1)^{k-i+1}\binom{k+1}{k-i} = -\binom{n}{k+1}(-1)^k = (-1)^{k+1}\binom{n}{k+1}$,

where the last equality follows from the fact that

$\binom{k+1}{0} - \binom{k+1}{1} + \binom{k+1}{2} + \cdots + (-1)^k\binom{k+1}{k} = -(-1)^{k+1} = (-1)^k$.

Similarly for $s = 1, \ldots, k$ we have $c(t_{n-s}) = \sum_{i=0}^{k-s}(-1)^{k-s-i+1}\binom{n-s-k+i}{i+1}\binom{n}{k-s-i}$

$= \binom{n-s}{k-s+1}\sum_{i=0}^{k-s}(-1)^{k-s-i+1}\binom{n}{k-s-i} = (-1)^{k-s+1}\binom{n-s}{k-s+1}$.

Now plugging $s = k - i$ in the formula above we get

$b_{n-(k+1)} = \sum_{i=0}^{k}(-1)^{i+1}\binom{n-k+i}{i+1}t_{n-k+i}$.                                    □

**Proposition 1** *Following the same notation one has for $1 \leq k \leq n$,*
$\sum_{i=0}^{n} i^k b_i = \sum_{i=1}^{k} i^k\left[\sum_{j=i}^{k}(-1)^{j-i}\binom{j}{j-i}t_j\right]$, *In particular:*

(a) $\sum_{i=0}^{n} i b_i = t_1 = \sum_{i=0}^{n-1} |A_i|$ *(Inclusion Exclusion Principle) and*

(b) $\sum_{i=0}^{n} i^2 b_i = t_1 + 2 t_2 = \sum_{i=0}^{n-1} |A_i| + 2 \sum_{i<j} |A_i \cap A_j|$.

**Proof:** According to Lemma 2 we have

$$b_n = t_n$$
$$b_{n-1} = t_{n-1} - \binom{n}{1} t_n$$
$$b_{n-2} = t_{n-2} - \binom{n-1}{1} t_{n-1} + \binom{n}{2} t_n$$
$$\vdots$$
$$b_2 = t_2 - \binom{3}{1} t_3 + \binom{4}{2} t_4 + \cdots + (-1)^{n-3} \binom{n-1}{n-3} t_{n-1} + (-1)^{n-2} \binom{n}{n-2} t_n$$
$$b_1 = t_1 - \binom{2}{1} t_2 + \binom{3}{2} t_3 + \binom{4}{3} t_4 + \cdots + (-1)^{n-2} \binom{n-1}{n-2} t_{n-1} + (-1)^{n-1} \binom{n}{n-1} t_n$$

If we sum $\sum_{i=1}^{n} i^k b_i$, then for $1 \leq s \leq n$, the coefficient of $t_s$ on the right hand side is

$$c(t_s) = \sum_{i=1}^{s} i^k \binom{s}{s-i} (-1)^{s-i}.$$

We claim that $c(t_s) = 0$ for $k < s \leq n$. We prove this by strong induction on $k$. For $k = 1$ we have

$$c(t_s) = \sum_{i=1}^{s} i \binom{s}{s-i} (-1)^{s-i} = \sum_{i=1}^{s} i \binom{s}{i} (-1)^{s-i} = \sum_{i=1}^{s} s \binom{s-1}{i-1} (-1)^{s-i}$$

Since $s \geq 2$, by substituting $m = s - 1 \geq 1$ and $j = i - 1$

$$c(t_s) = s \sum_{j=0}^{m} \binom{m}{j} (-1)^{m-j} = s(1-1)^m = 0.$$

Now assume $\sum_{i=1}^{s} i^l \binom{s}{s-i} (-1)^{s-i} = 0$ for any $1 \leq l \leq k$ and $l + 1 \leq s \leq n$. Then

$$c(t_s) = \sum_{i=1}^{s} i^{k+1} \binom{s}{s-i} (-1)^{s-i} = \sum_{i=1}^{s} i^{k+1} \binom{s}{i} (-1)^{s-i} = \sum_{i=1}^{s} s i^k \binom{s-1}{i-1} (-1)^{s-i}.$$

Substituting $m = s - 1 \geq l \geq 1$ and $j = i - 1$ we obtain

$$c(t_s) = s \sum_{j=0}^{m} (j+1)^k \binom{m}{j} (-1)^{m-j} = s \sum_{j=0}^{m} \sum_{l=0}^{k} \binom{k}{l} j^l \binom{m}{j} (-1)^{m-j}$$

$$= s \sum_{l=0}^{k} \binom{k}{l} \sum_{j=0}^{m} j^l \binom{m}{j} (-1)^{m-j}.$$

Since $m = s - 1 \geq l$, we have $m \geq l + 1$ and by induction hypothesis each summand

$$\sum_{j=0}^{m} j^l \binom{m}{j} (-1)^{m-j} = \sum_{j=1}^{m} j^l \binom{m}{m-j} (-1)^{m-j} = 0.$$

Hence $c(t_s) = 0$. On the other hand for $1 \leq s \leq k$ the coefficient of each $i^s$ on the right hand side is $\sum_{j=i}^{k} (-1)^{j-i} \binom{j}{j-i} t_j$. Hence we have the result. In particular, for $k = 2$ the non-zero terms on the right-hand-side are $t_1 - \binom{2}{1} t_2 + 2^2 t_2 = t_1 + 2 t_2$. $\square$

**Theorem 1** *Let* $\phi(n) = |\{\, 1 \le i \le n : \gcd(i,n) = 1 \}|$ *denote Euler's totient function. Let $X$ be a random variable which counts the number of distinct roots of a monic polynomial in $\mathbb{Z}_n[x]$ of degree $m > 0$. Then*

*(a)* $\mathrm{E}[X] = 1$ *and*

*(b) if $m = 1$ then $\mathrm{Var}[X] = 0$, otherwise $\mathrm{Var}[X] = \sum_{d|n, d \ne n} \frac{d}{n} \phi(\frac{n}{d}) = \sum_{d|n} \frac{d-1}{n} \phi(\frac{n}{d})$.
In particular, if $n = p^k$ where $p$ is a prime number and $k \ge 1$, $\mathrm{Var}[X] = k(1 - 1/p)$.*

**Remark 1.** We found this result by direct computation and using the Online Encyclopedia of Integer Sequences (OEIS) see [7]. For polynomials of degree 2,3,4,5 in $\mathbb{Z}_n[x]$ we computed $\mathrm{E}[X]$ and $\mathrm{Var}[X]$ for $n = 2, 3, 4, \ldots, 20$ using Maple and found that $\mathrm{E}[X] = 1$ in all cases. Values for the variance are given in the table below.

| $n$ | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $\mathrm{Var}[X]$ | $\frac{1}{2}$ | $\frac{2}{3}$ | 1 | $\frac{4}{5}$ | $\frac{3}{2}$ | $\frac{6}{7}$ | $\frac{3}{2}$ | $\frac{4}{3}$ | $\frac{17}{10}$ | $\frac{10}{11}$ | $\frac{7}{3}$ | $\frac{12}{13}$ | $\frac{25}{14}$ | 2 | 2 |
| $a(n)$ | 1 | 2 | 4 | 4 | 9 | 6 | 12 | 12 | 17 | 10 | 28 | 12 | 25 | 30 | 32 |

When we first computed $\mathrm{Var}[X]$ we did not recognize the numbers. Writing $\mathrm{Var}[X] = a(n)/n$ we computed the sequence for $a(n)$ (see the table) and looked it up in the OEIS. We found it is sequence A006579 and that $a(n) = \sum_{k=1}^{n-1} \gcd(n,k)$. The OEIS also has the formula $a(n) = \sum_{d|n} (d-1)\phi(\frac{n}{d})$.

**Proof:** Let $A_i$ be the set of all monic univariate polynomials of degree $m > 0$ which have a root at $\alpha_i \in \mathbb{Z}_n$. Then since $x - \alpha_i$ is monic, for any $f \in A_i$ we have $f = (x - \alpha_i)q$ for a unique $q \in \mathbb{Z}_n[x]$ and we have $n^{m-1}$ choices for such an $f$. Hence $|A_i| = n^{m-1}$.

Let $x_i := \mathrm{Prob}[X = i]$. This is the probability that $f$ has exactly $i$ distinct roots, i.e. $f \in B_i$ in the notation introduced in section 1 considering the finite collection of sets $\Gamma = \{A_i, i = 0, \ldots, n-1\}$. Since we have $n^{m-1}$ choices for a monic polynomial of degree $m$ in $\mathbb{Z}_n[x]$ we have $x_i = \frac{b_i}{n^{m-1}}$. Then by Proposition 1

$$\mathrm{E}[X] = \sum_{i=0}^{n} i x_i = \sum_{i=0}^{n} i \frac{b_i}{n^m} = \frac{\sum_{i=0}^{n} i b_i}{n^m} = \frac{\sum_{i=0}^{n-1} |A_i|}{n^m} = \frac{\sum_{i=0}^{n-1} n^{m-1}}{n^m} = \frac{n n^{m-1}}{n^m} = 1$$

To prove (b), if $m = 1$ then $f = x - \alpha$ for some $\alpha \in \mathbb{Z}_n$ and hence $X = 1$ and $\mathrm{Var}[X] = 0$. For $m > 1$ and $\alpha \in \mathbb{Z}_n^*$, our first aim is to find $|A_0 \cap A_\alpha|$. Let $f \in A_0 \cap A_\alpha$. It may not be the case that $f = x(x - \alpha)q$ for a unique $q \in \mathbb{Z}_n[x]$, since $\mathbb{Z}_n[x]$ is not a unique factorization domain in general. However $f = xq_1 = (x - \alpha)q_2$ for unique $q_1, q_2 \in \mathbb{Z}_n[x]$. It follows that $\alpha q_2(0) = 0 \bmod n$. If $\gcd(\alpha, n) = d$ then $\gcd(\frac{\alpha}{d}, \frac{n}{d}) = 1$ and hence $q_2(0) = 0 \bmod \frac{n}{d}$. The general form of $q_2 = x^{m-1} + a_{m-2}x^{m-2} + \cdots + a_0$ where $a_i \in \mathbb{Z}_n$ for $i = 0, \ldots, m-2$. Since $q_2(0) = a_0 \bmod \frac{n}{d}$, there are $d$ choices for $a_0$ and hence there are $dn^{m-2}$ choices for $q_2$. Therefore $|A_0 \cap A_\alpha| = dn^{m-2}$.

For a given pair $(\gamma, \beta)$ with $\beta > \gamma$, to compute $|A_\gamma \cap A_\beta|$, define $\alpha := \beta - \gamma$ and consider $A_0 \cap A_\alpha$. If $f \in A_\gamma \cap A_\beta$, then we have $f(x) = (x - \gamma)q_3(x) = (x - \beta)q_4(x)$ for unique $q_3, q_4 \in \mathbb{Z}_n[x]$. By the coordinate translation $x \mapsto x + \gamma$ we have $f(x + \gamma) \in A_0 \cap A_\alpha$, since $f(x + \gamma) = xq_3(x + \gamma) = (x - \alpha)q_4(x + \gamma)$ where $f(x + \gamma), q_3(x + \gamma), q_4(x + \gamma)$ are monic and with the same degree before the translation. This correspondence is bijective and it follows that $|A_\gamma \cap A_\beta| = |A_0 \cap A_\alpha| = dn^{m-2}$.

Let $d = \gcd(\alpha, n)$. There are $k = \phi(\frac{n}{d})$ elements $\beta_1, \ldots, \beta_k$ in $\mathbb{Z}_{\frac{n}{d}}$ such that $\gcd(\beta_j, \frac{n}{d}) = 1$. If we define $\alpha_j := d\beta_j \in \mathbb{Z}_n$ then $\gcd(\alpha_j, n) = d$. For, if $s = \gcd(\alpha_j, n)$ and $d|s$ then $s|\alpha_j \Rightarrow s|d\beta_j \Rightarrow \frac{s}{d}|\beta_j$

and $\frac{s}{d}|\frac{n}{d} \Rightarrow \frac{s}{d}|\gcd(\beta_j, \frac{n}{d}) \Rightarrow \frac{s}{d}|1 \Rightarrow s = d$. Now, for each $j$ consider the $n - \alpha_j$ pairs of the form $(i, i + \alpha_j)$ where $i = 0, \ldots, n - \alpha_j - 1$. We have $|A_i \cap A_{i+\alpha_j}| = |A_0 \cap A_{\alpha_j}|$ and

$$\sum_{\beta > \gamma, d = \gcd(\beta - \gamma, n)} |A_\gamma \cap A_\beta| = \sum_{j=1}^{k}(n - \alpha_j)|A_0 \cap A_{\alpha_j}| = \sum_{j=1}^{k}(n - \alpha_j)dn^{m-2} = dn^{m-2}\sum_{j=1}^{k} n - \alpha_j$$

where $d = \gcd(\alpha_j, n)$ and $k = \phi(\frac{n}{d})$. Since $\gcd(n, \alpha_j) = d \iff \gcd(n, n - \alpha_j) = d$ we have $\sum_{j=1}^{k} n - \alpha_j = \sum_{j=1}^{k} \alpha_j$. Then

$$2\sum_{j=1}^{k}\alpha_j = \sum_{j=1}^{k}\alpha_j + \sum_{j=1}^{k} n - \alpha_j = \sum_{j=1}^{k} n = kn = \phi(\frac{n}{d})n \implies \sum_{j=1}^{k}\alpha_j = \frac{n}{2}\phi(\frac{n}{d}).$$

It follows that

$$\sum_{\beta > \gamma, d = \gcd(\beta - \gamma, n)} |A_\gamma \cap A_\beta| = dn^{m-2}\sum_{j=1}^{k} n - \alpha_j = dn^{m-2}\sum_{j=1}^{k} \alpha_j = \frac{n}{2}\phi(\frac{n}{d})dn^{m-2}.$$

Then by Proposition 1 it follows that

$$\begin{aligned}
\mathrm{Var}[X] &= \mathrm{E}[X^2] - \mathrm{E}[X]^2 = -1^2 + \mathrm{E}[X^2] \\
&= -1 + \sum_{i=0}^{n} i^2 x_i = -1 + \sum_{i=0}^{n} i^2 \frac{b_i}{n^m} = -1 + \frac{\sum_{i=0}^{n} i^2 b_i}{n^m} \\
&= -1 + \frac{\sum_{i=0}^{n-1}|A_i| + 2\sum_{i<j}|A_i \cap A_j|}{n^m} \\
&= -1 + \frac{nn^{m-1}}{n^m} + \frac{2\sum_{d|n\, d\neq n}\frac{n}{2}\phi(\frac{n}{d})dn^{m-2}}{n^m} \\
&= 2\sum_{d|n\, d\neq n}\frac{n}{2}\phi(\frac{n}{d})dn^{-2} = \sum_{d|n\, d\neq n}\frac{d}{n}\phi(\frac{n}{d}).
\end{aligned}$$

Also, since by Gauss' Lemma $\sum_{d|n}\phi(\frac{n}{d}) = n$ we have

$$\begin{aligned}
\sum_{d|n}\frac{d-1}{n}\phi(\frac{n}{d}) &= \sum_{d|n}\frac{d}{n}\phi(\frac{n}{d}) - \frac{1}{n}\sum_{d|n}\phi(\frac{n}{d}) \\
&= \phi(1) + \sum_{d|n, d\neq n}\frac{d}{n}\phi(\frac{n}{d}) - \frac{1}{n}n = \sum_{d|n, d\neq n}\frac{d}{n}\phi(\frac{n}{d}).
\end{aligned}$$

To prove the last claim, let $n = p^k$ where $p$ is a prime number and $k \geq 1$. Then

$$\sum_{d|n, d\neq n}\frac{d}{n}\phi(\frac{n}{d}) = \sum_{s=0}^{k-1}\frac{p^s}{p^k}\phi(\frac{p^k}{p^s}) = \sum_{s=0}^{k-1}p^{s-k}p^{k-s-1}(p-1) = k(1 - 1/p).$$

$\square$

**Theorem 2** *Let $f, g$ be polynomials in $\mathbb{F}_q[x, y]$ of the form $f = c_n x^n + \sum_{i=0}^{n-1} \sum_{j=0}^{n-i} c_{ij} x^i y^j$ and $g = d_m x^m + \sum_{i=0}^{m-1} \sum_{j=0}^{m-i} d_{ij} x^i y^j$ with $c_n \neq 0$ and $d_m \neq 0$, thus of total degree $n$ and $m$ respectively. Let $X$ be a random variable that counts the number of $\gamma \in \mathbb{F}_q$ such that $\gcd(f(x, \gamma), g(x, \gamma)) \neq 1$. If $n > 0$ and $m > 0$ then*

   *(a)* $\mathrm{E}[X] = 1$ *and*
   *(b)* $\mathrm{Var}[X] = 1 - 1/q$.

**Remark 2.** We found this result by computation. For quadratic polynomials $f, g$ of the form $f = x^2 + (a_1 y + a_2)x + a_3 y^2 + a_4 y + a_5$ and $g = x^2 + (b_1 y + b_2)x + b_3 y^2 + b_4 y + b_5$ over finite fields of size $q = 2, 3, 4, 5, 8, 9, 11$ we generated all $q^{10}$ pairs and computed $X = |\{\alpha \in \mathbb{F}_q : \gcd(f(x, \alpha), g(x, \alpha)) \neq 1\}|$. Magma code for $\mathbb{F}_4$ is given in Appendix A. We repeated this for cubic polynomials and some higher degree bivariate polynomials for $q = 2, 3$ to verify that $\mathrm{E}[X] = 1$ and $\mathrm{Var}[X] = 1 - 1/q$ holds more generally. For yet higher degree polynomials we used random samples. That $\mathrm{E}[X] = 1$ independent of the degrees of $f$ and $g$ was a surprise to us. We had expected a logarithmic dependence on the degrees of $f$ and $g$.

**Proof:** Without loss of generality we may assume $f$ and $g$ are monic in $x$ because $\gcd(f(x, \gamma), g(x, \gamma)) = 1 \iff \gcd(c_n^{-1} f(x, \gamma), d_m^{-1} g(x, \gamma)) = 1$. For $\gamma \in \mathbb{F}_q$, let us define $A_\gamma$ as the set of polynomial pairs $(f, g) \in \mathbb{F}_q[x, y]^2$ where $f, g$ are monic in $x$ with total degrees, $\deg(f) = n > 0$ and $\deg(g) = m > 0$ such that $\gcd(f(x, \gamma), g(x, \gamma)) \neq 1$. Our first aim is to compute $|A_0|$.

Let $(f, g) \in A_0$. Since $f$ and $g$ are monic in $x$, $f(x, 0), g(x, 0)$ are monic polynomials of degree $n$ and $m$ respectively in $\mathbb{F}_q[x]$. We have finitely many choices, say $s$, for non-relatively prime monic polynomial pairs $(h_i(x), l_i(x))$ with $\deg(h_i) = n$ and $\deg(l_i) = m$ with $i = 1, \dots, s$ in $\mathbb{F}_q[x]^2$. Let $(f(x, 0), g(x, 0)) = (h_i(x), l_i(x))$ for some fixed $i$ where $1 \leq i \leq s$. In fact $s = (q^n q^m)/q = q^{n+m-1}$, since there are $q^n q^m$ possible choices for monic polynomial pairs $(h, l)$ in $\mathbb{F}_q[x]$ with $\deg(h) = n$, $\deg(l) = m$ and the probability of a given monic pair is non-relatively prime over $\mathbb{F}_q[x]$ is $1/q$ (see [8, 2] and also [1] for an accessible proof).

Let $f(x, y) = x^n + c_{n-1}(y)x^{n-1} + \cdots + c_1(y)x + c_0(y)$ where $c_d(y) \in \mathbb{F}_q[y]$ of total degree $\deg(c_{n-d}(y)) \leq d$ and let $c_{n-d}(y) = a_d^{(n-d)} y^d + \cdots + a_0^{(n-d)}$ where $a_i^{(n-d)} \in \mathbb{F}_q$.

Let $h_i(x) = x^n + \alpha_{n-1}^{(i)} x^{n-1} + \cdots + \alpha_0^{(i)}$ with $\alpha_v^{(i)} \in \mathbb{F}_q$ for $0 \leq v \leq n - 1$. Then for $1 \leq d \leq n$, we have $c_{n-d}(0) = a_0^{(n-d)} = \alpha_{n-d}^{(i)}$. It follows that there are $q^d$ choices for such $c_{n-d}(y)$ and hence there are $q^1 q^2 \cdots q^n = q^{n(n+1)/2}$ choices for such $f(x, y)$. Similarly there are $q^{m(m+1)/2}$ choices for $g(x, y)$. Let us denote these numbers as $D = q^{n(n+1)/2}$ and $R = q^{m(m+1)/2}$. Since we have $s$ choices for $i$, $|A_0| = sDR$.

On the other hand for a given $\gamma \in \mathbb{F}_q$ if $(f(x, y), g(x, y)) \in A_0$ then $(f(x, y - \gamma), g(x, y - \gamma)) \in A_\gamma$, since $f(x, y - \gamma)$ is again a bivariate polynomial which is a monic polynomial in $x$ of total degree $n$ and $g(x, y - \gamma)$ is again a bivariate polynomial which is monic polynomial in $x$ of total degree $m$. This correspondence (coordinate transformation) is bijective. Hence for any $\gamma \in \mathbb{F}_q$, one has $|A_\gamma| = sDR$.

For a general polynomial $f(x, y) \in \mathbb{F}_q[x, y]$ which is monic in $x$ and of total degree $n > 0$, one has $q^2 q^3 \cdots q^{n+1} = q^n D$ choices. Similarly for a general polynomial $g(x, y) \in \mathbb{F}_q[x, y]$ which is monic in $x$ and of total degree $m > 0$, one has $q^2 q^3 \cdots q^{m+1} = q^m R$ choices and therefore there are $q^{n+m} DR$ pairs $(f, g)$ which are monic in $x$ with total degrees $\deg(f) = n$ and $\deg(g) = m$.

Let $x_i := \mathrm{Prob}[X = i]$. This is the probability that $\gcd(f(x, \gamma), g(x, \gamma)) \neq 1$ for exactly $i$ different $\gamma$'s in $\mathbb{F}_q$, i.e. the probability that $(f, g) \in B_i$ in the notation introduced in section 1 considering the finite

collection of sets $\Gamma = \{A_\gamma, \gamma \in \mathbb{F}_q\}$. Hence $x_i = \frac{b_i}{q^{n+m}DR}$. Then by Proposition 1

$$
\begin{aligned}
\mathrm{E}[X] &= \sum_{i=0}^q ix_i = \sum_{i=0}^q i\frac{b_i}{q^{n+m}DR} = \frac{\sum_{i=0}^q ib_i}{q^{n+m}DR} \\
&= \frac{\sum_{i=0}^{q-1} |A_i|}{q^{n+m}DR} = \frac{\sum_{i=0}^{q-1} sDR}{q^{n+m}DR} = \frac{qsDR}{q^{n+m}DR} = \frac{qq^{n+m-1}}{q^{n+m}} = 1.
\end{aligned}
$$

To determine the variance of $X$, our proof assumes a set ordering of the elements of $\mathbb{F}_q$. For this purpose let us fix a generator $\alpha$ of $\mathbb{F}_q^*$ and use the ordering $0 < 1 < \alpha < \alpha^2 < \cdots < \alpha^{q-2}$.

For $(\gamma, \theta) \in \mathbb{F}_q^2$ with $\gamma < \theta$, let us define $A_{\gamma,\theta}$ as the set of bivariate polynomial pairs $(f, g)$ with $f, g$ are monic in $x$ with total degrees, $\deg(f) = n > 0$ and $\deg(g) = m > 0$ such that $\gcd(f(x, \gamma), g(x, \gamma)) \neq 1$ and $\gcd(f(x, \theta), g(x, \theta)) \neq 1$. Our first aim is to compute $|A_{0,1}|$.

Let $f, g \in A_{0,1}$. Since $f$ and $g$ are monic in $x$, $f(x, 0), f(x, 1)$ are monic polynomials of degree $n$ and $g(x, 0), g(x, 1)$ are monic polynomials of degree $m$ in $\mathbb{F}_q[x]$. We have finitely many choices for non-relatively prime monic polynomial pairs $(h_i(x), l_i(x))$ with $\deg(h_i) = n$ and $\deg(l_i) = m$ with $i = 1, \ldots, s$ in $\mathbb{F}_q[x]^2$.

Let $(f(x, 0), g(x, 0)) = (h_i(x), l_i(x))$ and $(f(x, 1), g(x, 1)) = (h_j(x), l_j(x))$ for some fixed pair $(i, j)$ where $1 \leq i, j \leq s$.

Let $f(x, y) = x^n + c_{n-1}(y)x^{n-1} + \cdots + c_1(y)x + c_0(y)$ where $c_d(y) \in \mathbb{F}_q[y]$ of total degree $\deg(c_{n-d}(y)) \leq d$ and let $c_{n-d}(y) = a_d^{(n-d)}y^d + \cdots + a_0^{(n-d)}$ where $a_i^{(n-d)} \in \mathbb{F}_q$.

Let $h_i(x) = x^n + \alpha_{n-1}^{(i)}x^{n-1} + \cdots + \alpha_0^{(i)}$ and $h_j(x) = x^n + \beta_{n-1}^{(j)}x^{n-1} + \cdots + \beta_0^{(j)}$ with $\alpha_v^{(i)}, \beta_w^{(j)} \in \mathbb{F}_q$ for $0 \leq v, w \leq n - 1$. Then for $1 \leq d \leq n$, we have

$$
c_{n-d}(0) = a_0^{(n-d)} = \alpha_{n-d}^{(i)} \text{ and } c_{n-d}(1) = a_d^{(n-d)} + \cdots + a_1^{(n-d)} + a_0^{(n-d)} = \beta_{n-d}^{(j)}.
$$

It follows that there are $q^{d-1}$ choices for such $c_{n-d}(y)$ and hence there are $q^0q^1 \cdots q^{n-1} = q^{n(n-1)/2}$ choices for such $f(x, y)$. Similarly there are $q^{m(m-1)/2}$ choices for $g(x, y)$. Let us call these numbers as $D_1 = q^{n(n-1)/2}$ and $R_1 = q^{m(m-1)/2}$. Since we have $s^2$ choices for $(i, j)$ ($i$ and $j$ are need not be different), $|A_{0,1}| = s^2D_1R_1$.

On the other hand if $(f(x, y), g(x, y)) \in A_{0,1}$ then for $\gamma, \theta \in \mathbb{F}_q$ with $\gamma < \theta$, $(f(x, \frac{y-\gamma}{\theta-\gamma}), g(x, \frac{y-\gamma}{\theta-\gamma})) \in A_{\gamma,\theta}$, since $f(x, \frac{y-\gamma}{\theta-\gamma})$ is again a monic polynomial in $x$ of total degree $n$ and $g(x, \frac{y-\gamma}{\theta-\gamma})$ is again a monic polynomial in $x$ of total degree $m$. This correspondence (coordinate transformation) is bijective and preserves relative primeness. Hence for a given $\gamma, \theta \in \mathbb{F}_q$ with $\gamma < \theta$, one has $|A_{\gamma,\theta}| = s^2D_1R_1$.

For a general bivariate polynomial $f(x, y) \in \mathbb{F}_q[x, y]$ which is monic in $x$ and of total degree $n$, one has $q^2q^3 \cdots q^{n+1} = q^{2n}D_1$ choices. Similarly for a general bivariate polynomial $g(x, y) \in \mathbb{F}_q[x, y]$ which is monic in $x$ and of total degree $m$, one has $q^2q^3 \cdots q^{m+1} = q^{2m}R_1$ choices and therefore the number of bivariate polynomial pairs in $(f, g)$ which are monic in $x$ with total degrees, $\deg(f) = n$ and $\deg(g) = m$ is $q^{2n+2m}D_1R_1$. Then with this notation we have $x_i = \frac{b_i}{q^{2n+2m}D_1R_1}$.

Since we have $\binom{q}{2}$ choices for $(\gamma, \theta)$ with $\gamma < \theta$, $|A_{\gamma,\theta}| = s^2D_1R_1$ for all $(\gamma, \theta)$ with $\gamma < \theta$ and $\mathrm{E}[X] = 1$, by Proposition 1 we have

$$
\begin{aligned}
\mathrm{Var}[X] &= \mathrm{E}[X^2] - \mathrm{E}[X]^2 = \mathrm{E}[X^2] - 1^2 = -1 + \sum_{i=0}^{q} i^2 x_i \\
&= -1 + \sum_{i=0}^{q} i^2 \frac{b_i}{q^{2n+2m} D_1 R_1} = -1 + \frac{\sum_{i=0}^{q} i^2 b_i}{q^{2n+2m} D_1 R_1} \\
&= -1 + \frac{\sum_{i=0}^{q-1} |A_i| + 2 \sum_{i<j} |A_i \cap A_j|}{q^{2n+2m} D_1 R_1} = -1 + \frac{\sum_{i=0}^{q-1} |A_i|}{q^{2n+2m} D_1 R_1} + \frac{2 \sum_{i<j} s^2 D_1 R_1}{q^{2n+2m} D_1 R_1} \\
&= -1 + \frac{\sum_{i=0}^{q} i b_i}{q^{2n+2m} D_1 R_1} + \frac{2 \sum_{i<j} s^2 D_1 R_1}{q^{2n+2m} D_1 R_1} = -1 + \sum_{i=0}^{q} i \frac{b_i}{q^{2n+2m} D_1 R_1} + \frac{2 \sum_{i<j} s^2 D_1 R_1}{q^{2n+2m} D_1 R_1} \\
&= -1 + \sum_{i=0}^{q} i x_i + \frac{2 \sum_{i<j} s^2 D_1 R_1}{q^{2n+2m} D_1 R_1} = -1 + \mathrm{E}[X] + \frac{2 \sum_{i<j} s^2 D_1 R_1}{q^{2n+2m} D_1 R_1} \\
&= -1 + 1 + \frac{2 \sum_{i<j} s^2 D_1 R_1}{q^{2n+2m} D_1 R_1} = \frac{2 \binom{q}{2} s^2 D_1 R_1}{q^{2n} q^{2m} D_1 R_1} = \frac{q(q-1) q^{2n+2m-2}}{q^{2n+2m}} \\
&= \frac{q(q-1)}{q^2} = 1 - \frac{1}{q}. \qquad \square
\end{aligned}
$$

**Theorem 3** *Let $f, g \in \mathbb{F}_q[x_1, x_2, \ldots, x_n]$ be of the form $f = c_l x_1^l + \sum_{i=0}^{l-1} c_{l-i}(x_2, \ldots, x_n) x^i$ and $g = d_m x_1^m + \sum_{i=0}^{m-1} d_{m-i}(x_2, \ldots, x_n) x^i$ where $c_l \neq 0$, $d_m \neq 0$, $\deg c_{l-i} \leq l-i$, and $\deg d_{m-i} \leq m-i$, thus $f$ and $g$ have total degree $l$ and $m$ respectively. Let $X$ be a random variable which counts the number of $\gamma = (\gamma_2, \ldots, \gamma_n) \in \mathbb{F}_q^{n-1}$ such that $\gcd(f(x_1, \gamma_2, \ldots, \gamma_n), g(x_1, \gamma_2, \ldots, \gamma_n)) \neq 1$.*
*If $n > 1$, $l > 0$ and $m > 0$ then*
   *(a) $\mathrm{E}[X] = q^{n-2}$ and*
   *(b) $\mathrm{Var}[X] = q^{n-2}(1 - 1/q)$.*

It follows from (a) that if $\gamma$ is chosen at random from $\mathbb{F}_q^{n-1}$ then

$$
\mathrm{Prob}[\gcd(f(x_1, \gamma_2, \ldots, \gamma_n), g(x_2, \gamma_2, \ldots, \gamma_n) \neq 1] = \frac{q^{n-2}}{q^{n-1}} = \frac{1}{q}.
$$

**Proof:** A version of the paper with the proof which runs about 3 pages may be found at
`http://www.cecm.sfu.ca/~mmonagan/papers/FPSAC16.pdf`

## 2.1 A comparison with the binomial distribution.

Let $Y$ be a random variable from a binomial distribution $B(n, p)$ with $n$ trials and probability $p$. So $0 \leq Y \leq n$, $\mathrm{Prob}[Y = k] = \binom{n}{k} p^k (1-p)^{n-k}$, $E[Y] = np$ and $\mathrm{Var}[Y] = np(1-p)$. We noticed that the mean and variance of $X$ in Theorem 2 is the same as the mean and variance of the binomial distribution $B(n, p)$ with $n = q$ trials and probability $p = 1/q$. In Table 1 below we compare the two distributions for

$$
\begin{aligned}
f &= x^2 + (a_1 y + a_2) x + (a_3 y^2 + a_4 y + a_5) \text{ and} \\
g &= x^2 + (b_1 y + b_2) x + (b_3 y^2 + b_4 y + b_5)
\end{aligned}
$$

in $\mathbb{F}_q[x, y]$ with $q = 7$. Note that there are $7^{10}$ pairs for $f, g$. In Table 1 $F_k$ is the number of pairs for which $\gcd(f(x, \alpha), g(x, \alpha)) \neq 1$ for exactly $k$ values for $\alpha \in \mathbb{F}_7$. We computed $F_k$ by computing this gcd for all distinct pairs using Maple. The values for $B_k$ come from $B(7, 1/7)$. They are given by $B_k = 7^{10} \mathrm{Prob}[Y = k]$.

| $k$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|---|
| $F_k$ | 96606636 | 110666892 | 56053746 | 17287200 | 1728720 | 0 | 0 | 132055 |
| $B_k$ | 96018048 | 112021056 | 56010528 | 15558480 | 2593080 | 259308 | 14406 | 343 |

**Table 1:** Data for quadratic $(f, g)$ in $\mathbb{F}_7[x, y]$

The two zeros $F_5$ and $F_6$ can be explained as follows. Let $R(y)$ be the Sylvester resultant of $f$ and $g$. Then applying Lemma 1 we have $R(\alpha) = 0 \iff \gcd(f(x, \alpha), g(x, \alpha)) \neq 1$ for $\alpha \in \mathbb{F}_q$. For our quadratic polynomials $f$ and $g$, Lemma 1(ii) implies $\deg R \leq \deg f \deg g = 4$. Hence $R(y)$ can have at most 4 distinct roots unless $f$ and $g$ are not coprime in $\mathbb{F}_7[x, y]$ in which case $R(y) = 0$ and it has 7 roots. Therefore $F_5 = 0$, $F_6 = 0$ and $F_7 = 132055$ is the number pairs $f, g$ which are not coprime in $\mathbb{F}_7[x, y]$.

# References

[1] Arthur Benjamin and Curtis Bennett. The Probability of Relatively Prime Polynomials. *Mathematics Magazine* **80** (3), 197–202, 2007.

[2] Erwin Berlekamp. *Algebraic Coding Theory*, McGraw-Hill, 1968.

[3] David Cox, John Little and Donal O'Shea. *Ideals, Varieties and Algorithms*. Springer-Verlag, 3rd ed., 2007.

[4] J. de Kleine, M. B. Monagan, A. D. Wittkopf. Algorithms for the Non-monic case of the Sparse Modular GCD Algorithm. *Proc. ISSAC '05*, ACM Press, (2005), 124–131.

[5] Arnold Knopfmacher and John Knopfmacher. Counting irreducible factors of polynomials over finite fields. *Discrete Mathematics* **112** (1993) 103–118.

[6] Michael Monagan and Baris Tuncer. Using Sparse Interpolation to Solve Multivariate Diophantine Equations. *Communications in Computer Algebra 49:3*, Issue 193, pp. 94−97, September 2015.

[7] Sequence http://oeis.org/A006579 in *The On-Line Encyclopedia of Integer Sequences*, published electronically at http://oeis.org, 2010.

[8] Gary Mullen and Daniel Panario. 11.2.3.4 Greatest common divisors of polynomials. *Handbook of Finite Fields.* CRC Press, 2013.

[9] Wolfgang Schmidt. *Equations over Finite Fields: An Elementary Approach.* Springer-Verlag LNCS **536** (1976) Ch 4 pp. 157–159.

[10] Jack Scwartz, Fast probabilistic algorithms for verification of polynomial identities. *J. ACM* **27** 701–717, 1980. See also https://en.wikipedia.org/wiki/Schwartz%E2%80%93Zippel_lemma .

[11] Richard. Zippel. Probabilistic Algorithms for Sparse Polynomials, *Proc. EUROSAM '79*, Springer-Verlag LNCS, **2**, 216–226, 1979.

## Appendix A

Below is Magma code for quadratic polynomials over $\mathbb{F}_4$. For each pair of quadratic polynomials $F, G \in \mathbb{F}_4[x,y]$ we compute $X = |\{\alpha \in \mathbb{F}_4 : \gcd(F(x,\alpha), G(x,\alpha) \neq 1\}|$. The code counts $A_k$ the number of pairs $(F, G)$ with $k = X$ and computes $\mathrm{E}[X]$ and $\mathrm{Var}[X]$.

```
q := 4;
Fq<z> := FiniteField(q);
P<x,y> := PolynomialRing(Fq,2);
N := 0; // counter
M := 0; // mean
V := 0; // variance
A := AssociativeArray(); // frequencies

for X in [0..q] do A[X] := 0; end for;

for a in Fq do for b in Fq do
for c in Fq do for d in Fq do for e in Fq do
for r in Fq do for s in Fq do
for t in Fq do for u in Fq do for v in Fq do

if not ( [a,b,c,d,e] gt [r,s,t,u,v] ) then
    X := 0;
    for y in Fq do
        F := x^2+(a*y+b)*x+(c*y^2+d*y+e);
        G := x^2+(r*y+s)*x+(t*y^2+u*y+v);
        if Gcd(F,G) ne 1 then X := X+1; end if;
    end for;
    if [a,b,c,d,e] eq [r,s,t,u,v] then
        N := N+1; A[X]  := A[X]+1;
        M := M+X; V := V+(X-1)*(X-1);
    else
        N := N+2;   A[X]  := A[X]+2;
        M := M+2*X; V := V+2*(X-1)*(X-1);
    end if;
end if;
end if;

end for; end for; end for; end for; end for;
end for; end for; end for; end for; end for;

"field size", q;
"N", N, q^10;
"frequencies", A[0],A[1],A[2],A[3],A[4];
"mean", 1.0*M/q^10;
"variance", 1.0*V/q^10;
```