The Mathematics Enthusiast

Volume 18
Number 1 *Numbers 1 & 2*

Article 2

1-2021

When is Freshman's Dream Actually True?

Michael P. Abramson

When is Freshman's Dream Actually True?

Michael P. Abramson
National Security Agency

ABSTRACT: We address the problem of determining what points in a field satisfy Freshman's Dream, or equivalently, when a monomial behaves additively. It is conjectured that the only additive points over the rational numbers are trivial. In the case of finite fields, we generalize well-known results about univariate polynomials to bivariate homogeneous polynomials in order to count the number of additive points.

Keywords: Freshman's Dream, finite fields, additivity, nonlinearity, cyclotomic cosets, homogeneous polynomial

The Mathematics Enthusiast, **ISSN 1551-3440, vol. 18, nos. 1-2**, pp. 3–9

Freshman's Dream

The well-known *Freshman's Dream* is the statement that for all x, y in a field F

$$(x+y)^n = x^n + y^n. \tag{1}$$

This statement is of course false in general (a common student error), but is true in special cases, for example, if the characteristic of F is a prime number p and $n = p$. Recall that the *characteristic* of a field F is the smallest number of a's, for any $a \in F$, which sum to zero. But if (1) is false, are there points $(x, y) \in F^2$ that still satisfy (1)? Such points are equivalent to points for which the monomial x^n is additive. Additivity is a relaxation of the definition of linearity, but is the same as linearity when the field has characteristic 2. Thus we will call a point $(x, y) \in F^2$ an *additive point* of x^n if it satisfies (1). Clearly, if $x = 0$, $y = 0$, or if n is odd and $x = -y$, (1) is satisfied. Hence, we will call an additive point (x, y) *trivial* if $xy(x + y) = 0$, and *nontrivial* otherwise.

Our general strategy will be to expand the bivariate polynomial

$$g_n(x,y) = (x+y)^n - x^n - y^n$$

using the Binomial Theorem, cancel the x^n and y^n terms, and then factor what is left. Therefore, (x, y) is an additive point if and only if

$$g_n(x,y) = \sum_{i=1}^{n-1} \binom{n}{i} x^{n-i} y^i = 0.$$

Freshman's Dream Over the Rational Numbers

In this section, we work toward a conjecture that there are no nontrivial values that satisfy Freshman's Dream over the rationals $\mathbb{Q}$. We begin by computing the first few $g_n(x, y)$ factored over the rational numbers. Note that all of the factors are symmetric.

n	$g_n(x,y)$
2	$2xy$
3	$3xy(x+y)$
4	$2xy(2x^2+3xy+2y^2)$
5	$5xy(x+y)(x^2+xy+y^2)$
6	$xy(6x^4+15x^3y+20x^2y^2+15xy^3+6y^4)$
7	$7xy(x+y)(x^2+xy+y^2)^2$
8	$2xy(4x^6+14x^5y+28x^4y^2+35x^3y^3+28x^2y^4+14xy^5+4y^6)$
9	$3xy(x+y)(3x^6+9x^5y+19x^4y^2+23x^3y^3+19x^2y^4+9xy^5+3y^6)$
10	$xy(10x^8+45x^7y+120x^6y^2+210x^5y^3+252x^4y^4+\ldots)$
11	$11xy(x+y)(x^2+xy+y^2)(x^6+3x^5y+7x^4y^2+9x^3y^3+\ldots)$
12	$xy(12x^{10}+66x^9y+220x^8y^2+495x^7y^3+792x^6y^4+924x^5y^5+\ldots)$
13	$13xy(x+y)(x^2+xy+y^2)^2(x^6+3x^5y+8x^4y^2+11x^3y^3+\ldots)$

Patterns in the table allow us to state and prove the following partial factorization of $g_n(x, y)$.

Theorem 1. *$g_n(x,y) = Cxy(x+y)^{n \ mod \ 2}(x^2+xy+y^2)^{s(n)}h_n(x,y)$ for some $h_n(x,y)$, where $C = p$ if n is a power of a prime p and 1 otherwise, and*

$$s(n) = \begin{cases} 2 & \text{if } n \equiv 1 \bmod 6 \\ 1 & \text{if } n \equiv 5 \bmod 6 \\ 0 & \text{otherwise.} \end{cases}$$

Proof. The constant C was derived in 1909 [Ram] and will not be derived again here because we are only interested in the roots of $g_n(x, y)$. We have already accounted for $xy(x + y)$, so it suffices to determine precisely when $(x^2+xy+y^2)^{s(n)}$ is a factor of $g_n(x,y)$. The nontrivial roots of x^2+xy+y^2 are $(x,\omega x)$ and $(x,\omega^2 x)$, where $x \neq 0$ and ω and ω^2 are the complex (conjugate) cube roots of 1. Setting $g_n(x,\omega x) = 0$ and relying on $x \neq 0$ and the identity $\omega^2+\omega+1 = 0$,

$$0 = g_n(x,\omega x) = (x+\omega x)^n - x^n - (\omega x)^n = (-1)^n \omega^{2n} - 1 - \omega^n.$$

If $n \equiv 0 \bmod 3$, then $(-1)^n - 2 = 0$, a contradiction. If $n \equiv 1 \bmod 3$, then $(-1)^n\omega^{2n} - 1 - \omega^n = (-1)^n\omega^2 - 1 - \omega = 0$ if and only if n is also odd. If $n \equiv 2 \bmod 3$, then $(-1)^n\omega^{2n} - 1 - \omega^n = (-1)^n\omega - 1 - \omega^2 = 0$ if and only if n is also odd. Then by the Chinese Remainder Theorem, $(x,\omega x)$ is a nontrivial root of $g_n(x,y)$, and in particular $s(n) > 0$, if and only if $n \equiv \pm 1 \bmod 6$.

To distinguish between $s(n)$ being 1 or 2, we must determine when the derivatives are also zero. More specifically, $(x,\omega x)$ is a double root of $g_n(x,y)$ if and only if $(x,\omega x)$ is also a root of $\frac{\partial g_n}{\partial x}$ and $\frac{\partial g_n}{\partial y}$. So we compute

$$\begin{aligned} 0 &= \frac{\partial g_n}{\partial x}(x,\omega x) = n(x+\omega x)^{n-1} - nx^{n-1} &&= (-1)^{n-1}\omega^{2(n-1)} - 1. \\ 0 &= \frac{\partial g_n}{\partial y}(x,\omega x) = n(x+\omega x)^{n-1} - n(\omega x)^{n-1} &&= (-1)^{n-1}\omega^{2(n-1)} - \omega^{n-1}. \end{aligned}$$

Both derivatives are zero if and only if $n-1$ is even and $n-1 \equiv 0 \bmod 3$, or equivalently $n-1 \equiv 0 \bmod 6$ by the Chinese Remainder Theorem. □

Computer experiments in Magma [C] show that the factor $h_n(x,y)$ of $g_n(x,y)$ is irreducible over $\mathbb{Q}$ for all $n \leq 2000$. If $h_n(x,y)$ is actually irreducible for all n, then the following conjecture is true, implying that there are no nontrivial rational values satisfying Freshman's Dream.

Conjecture. *x^n has no nontrivial additive points in $\mathbb{Q}$.*

Review of Finite Fields

Before we address the problem of Freshmen's Dream over finite fields, we include here a short review of finite fields. A reader who is already familiar with finite fields may skip this section without missing anything. The concepts discussed in this section can be found in any text on finite fields. The most readable accounts of finite fields are often individual chapters on finite fields within texts on the the theory of error correcting codes, such as [MS].

Recall that a *field* is just a set of numbers in which all four of the operations of addition, subtraction, multiplication, and division are well-defined in the usual way with which we are familiar. The usual examples are the rational numbers $\mathbb{Q}$, the real numbers $\mathbb{R}$, and the complex numbers $\mathbb{C}$. The integers $\mathbb{F}_p = \{0, 1, \ldots, p-1\}$, in which p is prime, and addition and multiplication are done modulo p also form a field. In addition to these basic fields, we can *extend* these fields by adjoining numbers that are not in the set. For example, $\mathbb{Q}(\sqrt{3}) = \{a + b\sqrt{3} : a, b \in \mathbb{Q}\}$ is also a field.

Finite field extensions could be constructed in a similar way, but they are normally derived using quotients of polynomial rings by maximal ideals. A well-known result from ring theory states that a ring modulo a maximal ideal is a field. We mimic this construction by noting that an ideal in $F[x]$ generated by an irreducible polynomial $f(x)$ is maximal, so we form the quotient ring $F[x]/\langle f\rangle$ which is a field. The complex numbers $\mathbb{C}$ can be viewed this way because x^2+1 is irreducible over $\mathbb{R}$, so $\mathbb{C} \cong \mathbb{R}/\langle x^2+1\rangle$.

Example 1. Let $f(x) = x^2+x+1 \in \mathbb{F}_2[x]$. Since the degree of f is only 2 and neither 0 nor 1 is a root of f, $f(x)$ is irreducible over $\mathbb{F}_2$. Then $\mathbb{F}_2[x]/\langle f\rangle$ is a field whose elements are $\langle f\rangle, 1+\langle f\rangle, x+\langle f\rangle, 1+x+\langle f\rangle$, which we abbreviate as $0, 1, x, 1+x$. Thus this field has four elements instead of two, and their addition and multiplication tables are given by

$+$	0	1	x	$1+x$
0	0	1	x	$1+x$
1	1	0	$1+x$	x
x	x	$1+x$	0	1
$1+x$	$1+x$	x	1	0

$\times$	0	1	x	$1+x$
0	0	0	0	0
1	0	1	x	$1+x$
x	0	x	$1+x$	1
$1+x$	0	$1+x$	1	x

The fact that this field has size $4 = 2^2$ is no coincidence. If the degree of our irreducible polynomial $f(x) \in \mathbb{F}_p[x]$ is k, we get a field of size p^k, which we denote by $\mathbb{F}_{p^k}$. The main reason for constructing finite fields using irreducible polynomials is to prove the following theorem which makes the notation $\mathbb{F}_{p^k}$ well-defined.

Theorem 2. *There exists a field $\mathbb{F}_{p^k}$ for every prime p and every positive integer k, and all fields of size p^k are isomorphic.*

Existence can be proved by showing that there exist irreducible polynomials of every degree over $\mathbb{F}_p$. Uniqueness is shown by exhibiting an isomorphism between the roots of irreducible polynomials of the same degree that leave $\mathbb{F}_p$ fixed. The proof is both significant and instructive, but too long for this summary, so the interested reader should consult the literature.

If we throw out the row and column of zeros in the multiplication table, we get the group table for the cyclic group of three elements. This is true more generally.

Theorem 3. *The set of nonzero elements of a field $\mathbb{F}_{p^k}$ forms a cyclic group of size $p^k - 1$.*

The next result is often referred to as the Fundamental Theorem of Finite Fields.

Theorem 4. *$x^{p^k} - x$ is the product of all monic irreducible polynomials over $\mathbb{F}_{p^k}$ whose degree divides k.*

The product of these polynomials enables us to partition the elements of $\mathbb{F}_{p^k}$ according to the polynomials for which they are roots. This partitioning is done using cyclotomic cosets. A *cyclotomic coset* C_s of an integer s, $0 \leq s \leq p^m$, is the set of integers $\{s, ps, \ldots, p^r s\}$, where each $p^i s$ is computed modulo $p^m - 1$. For example, the cyclotomic coset of 3 modulo $2^4 - 1$ is $\{3, 6, 12, 9\}$. When expressed as powers of a generator ζ (which exists by Theorem 3), the roots of any irreducible polynomial $f(x) \in \mathbb{F}_p[x]$ have exponents that lie in the same cyclotomic coset modulo $p^k - 1$, which we denote by C_f.

Theorem 5. *Let $f(x) \in \mathbb{F}_p[x]$ be irreducible and ζ a generator of the multiplicative group of $\mathbb{F}_{p^k}$. Then*

$$f(x) = \prod_{t \in C_f} \left(x - \zeta^t\right).$$

For example, if we multiply out $\left(x - \zeta^3\right)\left(x - \zeta^6\right)\left(x - \zeta^{12}\right)\left(x - \zeta^9\right)$, where ζ generates the nonzero elements of $\mathbb{F}_{2^4}$ and the exponents come from the same cyclotomic coset $\{3, 6, 12, 9\}$, the result is an irreducible polynomial in $\mathbb{F}_2[x]$. There are three irreducible polynomials of degree 4 over $\mathbb{F}_2$ and the specific polynomial we get will depend on our choice of ζ.

Freshman's Dream over Finite Fields

In this section, we wish to determine the additive points of x^n that lie in $\mathbb{F}_{p^k}$. As in the first section $g_n(x, y)$ will be defined as $g_n(x, y) = (x + y)^n - x^n - y^n$, but this time with coefficients in $\mathbb{F}_p$. It is well-known that if $n = p^j$ and j divides k, then $g_n(x, y)$ is identically zero, implying that all points of $\mathbb{F}_{p^k}^2$ are roots of $g_n(x, y)$ (this result is, in fact, called *Freshman's Dream*).

In studying g_n, we won't really care about the multiplicity of roots, just the roots themselves, so let $m_n(x, y)$ be the product of the irreducible factors of $g_n(x, y)$ without multiplicity. We call m_n the *minimal additivity polynomial* of x^n since it has the same roots as g_n but with minimal degree.

A polynomial f is *homogeneous* if all its terms have the same (total) degree. A univariate polynomial $f(x)$ can be turned into a bivariate homogeneous polynomial by forming $f^h(x, y) = y^{\deg(f)} f(x/y)$. This process is called *homogenization.* The inverse process, *dehomogenization*, is given by $f(x) = f^h(x, 1)$. For example, if $f(x) = x^3 + x + 1$, it's homogenization is $f^h(x, y) = x^3 + xy^2 + y^3$, and we see immediately that $f^h(x, 1) = f(x)$. Homogenization and dehomogenization commute with polynomial multiplication and preserve degrees. Note that $g_n(x, y)$ and $m_n(x, y)$ are both homogeneous. Here is a homogeneous version of Theorem 4:

Theorem 6. *$x^{p^k} y - x y^{p^k}$ is the product of all monic irreducible homogeneous polynomials in $\mathbb{F}_p[x, y]$ whose degree divides k.*

Proof. Let $f(x,y)$ be a monic irreducible homogeneous polynomial whose degree divides k. Then $f(x,1)$ is a monic irreducible polynomial whose degree divides k. So $f(x,1)$ divides $x^{p^k}-x$. Then there exists a polynomial $r(x)\in\mathbb{F}_2[x]$ such that $f(x,1)r(x)=x^{p^k}-x$. Homogenizing, we get $f(x,y)r^h(x,y)=x^{p^k}-xy^{p^{k-1}}$. Hence, $f(x,y)$ divides $x^{p^k}y-xy^{p^k}$. Conversely, suppose $f(x,y)$ is a factor of $x^{p^k}y-xy^{p^k}$. Then $f(x,1)$ divides $x^{p^k}-x$, and by Theorem 4, $f(x,1)$ is a product of monic irreducible polynomials whose degrees divide k. Therefore, $f(x,y)$ is a product of monic irreducible homogeneous polynomials over $\mathbb{F}_2$ whose degrees divide k. □

The next theorem will enable us to count the number of roots of the minimum additivity polynomial $m_n(x,y)$ in $\mathbb{F}_{p^k}$. For $f\in\mathbb{F}_p[x,y]$, let $d=\deg(f)$ and $N_{p^k}(f)$ denote the number of roots of f in $\mathbb{F}_{p^k}^2$ (without multiplicity).

Theorem 7. *$N_{p^k}(f)=d(p^k-1)+1$ if $d\mid k$, and $N_{p^k}(f)=0$ if $d\nmid k$.*

Proof. Let $f(x,y)=f_1(x,y)\cdots f_r(x,y)$, where each $f_i(x,y)\in\mathbb{F}_2[x,y]$ is a monic irreducible homogeneous polynomial of degree d_i. By irreducibility, the only root common to all the f_i is $(0,0)$. Thus to compute $N_{p^k}(f)$, we simply total the number of nonzero roots of each f_i and add 1 at the end. Thus

$$N_{p^k}(f)=1+\sum_{i=1}^{r}\left[N_{p^k}(f_i)-1\right]=1-r+\sum_{i=1}^{r}N_{p^k}(f_i). \tag{2}$$

Formula (2) can be used to compute $N_{p^k}(f)$, provided we know its monic irreducible homogeneous factors, which we can derive using cyclotomic cosets.

Now suppose $f(x,y)\in\mathbb{F}_p[x,y]$ is a monic irreducible homogeneous polynomial of degree $d>1$. If d does not divide k, then by Theorem 6, $f(x,y)$ does not divide $x^{p^k}y-xy^{p^k}$, which means that f has no roots in $\mathbb{F}_{p^k}$. Thus $N_{p_k}(f)=0$. Conversely, suppose d divides k. Then by Theorem 5, $f(x,1)=\prod_{i\in C_f}(x-\zeta^i)$, so $f(x,y)=\prod_{i\in C_f}(x-\zeta^i y)$. Excluding the case $x=y=0$, we note that $x-\zeta^i y=0$ has exactly p^k-1 nonzero solutions for any fixed i and that no pair of these $x-\zeta^i y$ are simultaneously zero for two different i (as can be verified by routine computation). Thus $f(x,y)$ has $d(p^k-1)+1$ roots in $\mathbb{F}_{p^k}^2$. □

Computing Minimal Additivity Polynomials

We can now compute m_n and $N_{p^k}(m_n)$ for any n,p,k using Theorems 6 and 7.

Algorithm. *The following steps compute $m_n(x,y)$ and $N_{p^k}(m_n)$ in $\mathbb{F}_{p^k}[x,y]$:*

1. *Factor $(x+y)^n-x^n-y^n$ as $g_n(x,y):=f_1(x,y)^{e_1}\cdots f_s(x,y)^{e_s}$.*
2. *Compute $m_n(x,y):=f_{i_1}(x,y)\cdots f_{i_r}(x,y)$, where each $\deg\left(f_{i_j}\right)$ divides k.*
3. *Compute $N_{p^k}(f_{i_j}):=\deg(f_{i_j})(p^k-1)+1$ for $j=1,\dots,r$ (using Theorem 7).*
4. *Compute $N_{p^k}(m_n):=N_{p^k}(f_{i_1})+\ldots+N_{p^k}(f_{i_r})-r+1$ using* (2)

Step 1 can be accomplished using a fast method for polynomial factorization plus homogenization, (see [GG]). Step 2 is necessary to throw out extraneous factors, i.e. factors whose roots do not lie $\mathbb{F}_{p^k}^2$.

By earlier remarks, xy divides g_n and hence m_n. Similarly, $x+y$ divides m_n if n is odd. If $p=2$, addition and subtraction are the same, so (α,α) is a root of $(x+y)^n+x^n+y^n$ for all $\alpha\in\mathbb{F}_{p^k}$. Thus (α,α) is a root of m_n for all $\alpha\in\mathbb{F}_{2^k}$. But every root of $x+y$ has the form (α,α) where $\alpha\in\mathbb{F}_{2^k}$. Thus every root of $x+y$ is a root of m_n. Then since $\deg(x+y)=1$, $x+y$ divides m_n. Thus we have shown that $m_n(x,y)$ is always divisible by xy, and is divisible by $x+y$ whenever n is odd or $p=2$.

In some special cases, which we consider below, we can compute m_n without using the algorithm, thus speeding up computation. In principle, similar computations could be carried out for any monomial, but this becomes impractical as n and k get larger.

Example 2. If $n=p^i$ for some i, this is the usual Freshman's Dream, so (1) always holds. Thus every element of $\mathbb{F}_{p^k}^2$ is a root of m_n, so $m_n=x^{p^k}y-xy^{p^k}$.

Example 3. Suppose $n = p^k - 1$. For $xy(x+y) \neq 0$,

$$(x+y)^{p^k-1} - x^{p^k-1} - y^{p^k-1} = 1 - 1 - 1 = -1 \neq 0.$$

This means that m_{p^k-1} divides $xy(x+y)$. Clearly, xy divides m_{p^k-1}. Now suppose, $x+y=0$ but $x \neq 0$ and $y \neq 0$. Then $(x+y)^{p^k-1} - x^{p^k-1} - y^{p^k-1} = 0 - 1 - 1 = -2 = 0$ if and only if $p = 2$. So $x+y$ divides m_{p^k-1} if and only if $p = 2$. Thus $m_n = xy(x+y)$ if $p = 2$ and $m_n(x,y) = xy$ if $p > 2$.

Example 4. For $n = 3, 5, 7$, $(x+y)^n - x^n - y^n = nxy(x+y)(x^2+xy+y^2)^{\frac{n-3}{2}}$ by direct computation. Now $x^3 - y^3 = (x-y)(x^2+xy+y^2)$ is the homogenization of $x^3 - 1 = (x-1)(x^2+x+1)$, whose roots are $1, \omega, \omega^2$, where ω is a primitive cube root of unity (in $\overline{\mathbb{F}}_p$). Thus x^2+x+1, and therefore x^2+xy+y^2, has its roots in $\mathbb{F}_{p^k}$ if and only if $\omega \in \mathbb{F}_{p^k}$. But the roots of x^2+x+1 lie in $\mathbb{F}_{p^k}^2$ if and only if $p^k \equiv 1 \bmod 3$ (because if $x^3 - 1$ divides $x^{p^{k-1}} - 1$, then 3 divides $p^k - 1$). Thus if $n \in C_r$ for $r \in \{3,5,7\}$ and $p \neq r$ (so that we are not in Example 1),

$$m_n(x,y) = \begin{cases} xy(x+y)(x^2+xy+y^2), & \text{if } p^k \equiv 1 \bmod 3 \\ xy(x+y), & \text{if } p^k \not\equiv 1 \bmod 3. \end{cases} \tag{3}$$

Example 5. Suppose $n \in C_{p^k-2}$. Since $p \neq 2$ implies $p^k - 2$ is odd, $xy(x+y)$ divides m_n. So we may assume that $xy(x+y) \neq 0$. Then

$$\begin{aligned} 0 &= (x+y)^{p^k-2} - x^{p^k-2} + y^{p^k-2} \\ &= xy(x+y)^{p^k-1} - xy(x+y)\left(x^{p^k-2} + y^{p^k-2}\right) \quad = \quad xy - (x+y)^2 \\ &= x^2+xy+y^2, \text{ thus (3) holds in this case also.} \end{aligned}$$

Example 6. Suppose $p = 2$ and $n \in C_{p^k-3}$. Then $xy(x+y)$ divides m_n, so we may assume that $xy(x+y) \neq 0$. Then

$$\begin{aligned} 0 &= (x+y)^{p^k-3} - x^{p^k-3} + y^{p^k-3} \\ &= (xy)^2(x+y)^{p^k-1} - (xy)^2(x+y)^2\left(x^{p^k-3} + y^{p^k-3}\right) \\ &= (xy)^2 - (x+y)^2(x^2+y^2) \quad = \quad (xy)^2 - (x^2+y^2)^2 \quad = \quad (x^2+xy+y^2)^2 \\ &= x^2+xy+y^2, \text{ thus (3) holds yet again.} \end{aligned}$$

A Full Example

We conclude with the example $F = \mathbb{F}_{2^6} = \mathbb{F}_{64}$. In addition to $xy(x+y)$, the irreducible factors of $x^{64}y - xy^{64}$ are given by

$$\begin{aligned} g_2 &= x^2+xy+y^2 & \qquad g_{61} &= x^6+x^3y^3+y^6 \\ g_{31} &= x^3+x^2y+y^3 & g_{62} &= x^6+x^5y+x^3y^3+x^2y^4+y^6 \\ g_{32} &= x^3+xy^2+y^3 & g_{63} &= x^6+x^4y^2+x^3y^3+xy^5+y^6, \end{aligned}$$

which were obtained by factoring $x^{64} - x$ and homogenizing the resulting irreducible polynomial factors. The table below lists the nontrivial factors of m_n for each $n = 1, \ldots, 63$, grouped by cyclotomic coset $C_n = C_{x^n}$, which were computed using the algorithm or the special cases. Also listed for each cyclotomic coset are the number $N_{64}(x^n)$ of roots in F^2 computed using Theorem 4, as well as the percent of additive points, which is computed by dividing $N_{64}(x^n)$ by $|F^2| = 64^2 = 4096$.

C_n	$m_n(x,y)/[xy(x+y)]$	$N_{64}(x^n)$	% additive
$\{1,2,4,8,16,32\}$	$g_2g_{31}g_{32}g_{61}g_{62}g_{63}$	4096	100.00
$\{3,6,12,24,48,33\}$	1	190	4.64
$\{5,10,20,40,17,34\}$	g_2	316	7.71
$\{7,14,28,56,49,35\}$	g_2	316	7.71
$\{9,18,36\}$	$g_{31}g_{32}$	568	13.87
$\{11,22,44,25,50,37\}$	$g_2g_{31}g_{32}$	694	16.94
$\{13,26,52,41,19,38\}$	g_2	316	7.71
$\{15,30,60,57,51,39\}$	$g_{31}g_{32}$	568	13.87
$\{21,42\}$	$g_{61}g_{62}g_{63}$	1324	32.32
$\{23,46,29,58,53,43\}$	$g_2g_{31}g_{32}$	694	16.94
$\{27,54,45\}$	1	190	4.64
$\{31,62,61,59,55,47\}$	g_2	316	6.71

The methods described here can be used to compute all points in $\mathbb{F}_{p^k}$ that satisfy Freshman's Dream for any exponent n. The speed of the algorithm is only limited by the speed of the polynomial factorization algorithm.

References

[C] Cannon, J. et al. (2019). *Magma Computer Algebra System.* Retrieved 15 February 2019. `magma.maths.usyd.edu.au/magma/`.

[GG] Gathen, J von zur & Gerhard, J. (1999). *Factoring Polynomials Over Finite Fields.* Chapter 14 in *Modern Computer Algebra.* Cambridge, UK: Cambridge University Press.

[MS] MacWilliams, F. J. & Sloane, N. J. A. (1983). *Finite Fields.* Chapter 4 in *The Theory of Error-Correcting Codes.* Mathematical Library 16, Amsterdam: North-Holland Publishing Company.

[Ram] Ram, B. (1909). Common Factors of $\frac{n!}{m!(n-m)!}$, $(m = 1,2,\ldots,n-1)$. *Journal of the Indian Mathematics Club (Madras)*, 1, 39-43.

National Security Agency, Fort Meade, MD 20755, USA
Email address: `mpabram@nsa.gov`