# The minimum size of complete caps in $(\mathbb{Z}/n\mathbb{Z})^2$

Jack Huizenga
Department of Mathematics
University of Chicago
Chicago, IL 60637 USA
huizenga@uchicago.edu

Submitted: Oct 19, 2005; Accepted: Jul 12, 2006; Published: Jul 28, 2006
Mathematics Subject Classification: 51E22

**Abstract**

A *line* in $(\mathbb{Z}/n\mathbb{Z})^2$ is any translate of a cyclic subgroup of order $n$. A subset $X \subset (\mathbb{Z}/n\mathbb{Z})^2$ is a *cap* if no three of its points are collinear, and $X$ is *complete* if it is not properly contained in another cap. We determine bounds on $\Phi(n)$, the minimum size of a complete cap in $(\mathbb{Z}/n\mathbb{Z})^2$. The other natural extremal question of determining the maximum size of a cap in $(\mathbb{Z}/n\mathbb{Z})^2$ is considered in [8]. These questions are closely related to well-studied questions in finite affine and projective geometry. If $p$ is the smallest prime divisor of $n$, we prove that

$$\max\{4, \sqrt{2p} + \frac{1}{2}\} \leq \Phi(n) \leq \max\{4, p+1\}.$$

We conclude the paper with a large number of open problems in this area.

## 1 Introduction

A $k$-*cap* in $\mathrm{AG}(n,q)$ (affine $n$-space over $\mathbb{F}_q$) is a subset $X \subset \mathrm{AG}(n,q)$ of size $k$, no three of whose points are collinear. When a $k$-cap is not contained in any $(k+1)$-cap, it is said to be *complete*. The same definitions may be made for $\mathrm{PG}(n,q)$ (projective $n$-space over $\mathbb{F}_q$). There are two very natural extremal questions in the study of caps. First, what is the maximum size of a cap in $\mathrm{AG}(n,q)$ or $\mathrm{PG}(n,q)$? This question is of great importance in coding theory, and relates to the existence of certain $q$-ary codes. A nice survey of this question is provided in [4].

On the other hand, we could try to determine the minimum number of points in a complete cap. This question was originally posed by B. Segre ([16, 17]) in the late 1950's in the special case of finite projective planes of order $q$. Most work in this field has concerned the two-dimensional case, so we will restrict our attention to $n = 2$. An essentially trivial lower bound for the minimum number of points in a complete cap in $\mathrm{PG}(2,q)$ is given by $\sqrt{2q}$, and the best known lower bound to date is roughly $\sqrt{3q}$, which holds when $q$ is prime or the square of a prime (see [1, 2]).

Regarding upper bounds, Kim and Vu ([10]) recently made a major breakthrough in this field, using a variant of the probabilistic method known as Rödl's nibble to prove that if $q$ is sufficiently large then there is a complete cap in $\mathrm{PG}(2,q)$ containing at most $\sqrt{q}(\ln q)^{10}$ points. A similar bound holds for the minimum size of a complete cap in $\mathrm{AG}(2,q)$ since we can obtain $\mathrm{AG}(2,q)$ from $\mathrm{PG}(2,q)$ by removing a line at infinity.

We can ask the same questions in a slightly different setting. Suppose that we have an $n \times n$ grid on the torus. We can naturally identify this grid with the abelian group $(\mathbb{Z}/n\mathbb{Z})^2$. Under this identification, lines in the $n \times n$ grid are sent to translates of cyclic subgroups of $(\mathbb{Z}/n\mathbb{Z})^2$. It is not difficult to show that any cyclic subgroup of $(\mathbb{Z}/n\mathbb{Z})^2$ is contained in some cyclic subgroup of order $n$. Since we are only concerned with the collinearity relations which lines impose, we therefore define a *line* in $(\mathbb{Z}/n\mathbb{Z})^2$ to be any translate of a cyclic subgroup of order $n$. An equivalent definition is that a line in $(\mathbb{Z}/n\mathbb{Z})^2$ is a subset of $(\mathbb{Z}/n\mathbb{Z})^2$ of the form

$$\{(x,y) : ax + by = c\},$$

where $\gcd(a,b,n) = 1$. Of course when $n = p$ is prime, the resulting space is just $\mathrm{AG}(2,p)$.

We will call $X \subset (\mathbb{Z}/n\mathbb{Z})^2$ a *cap* if it contains no collinear triple, and we will call $X$ *complete* if it is maximal with respect to set-theoretic inclusion. With these definitions, we may then ask the exact same questions for $(\mathbb{Z}/n\mathbb{Z})^2$ that were considered for $\mathrm{AG}(2,q)$. In [8], we address the first question: what is the maximum possible size of a cap in $(\mathbb{Z}/n\mathbb{Z})^2$? This article will be concerned with exploring the second question. That is, what is the minimum size $\Phi(n)$ of a complete cap in $(\mathbb{Z}/n\mathbb{Z})^2$?

Our main results are summarized in the following theorem.

**Theorem 1.1.** *Let $p$ be the smallest prime divisor of $n$. Then*

$$\max\{4, \sqrt{2p} + \frac{1}{2}\} \leq \Phi(n) \leq \max\{4, p+1\}.$$

We will prove the lower bounds first, in Section 2.

The proof of the upper bound is far more difficult than the proof of the lower bound, and will occupy Sections 3 and 4. Our first result in Section 3 will show that

$$\Phi(nm) \leq \min\{\Phi(n), \Phi(m)\}$$

when $n$ and $m$ are coprime. For this reason, we will concentrate primarily on determining an upper bound for $\Phi(p^a)$.

To find an upper bound for $\Phi(p^a)$, we introduce the notion of a *diverse* cap in $(\mathbb{Z}/p\mathbb{Z})^2$. A cap $X \subset (\mathbb{Z}/p\mathbb{Z})^2$ is said to be *diverse* if it contains pairs of points of every slope (the slope between two points of $(\mathbb{Z}/p\mathbb{Z})^2$ is defined by the usual formula). We prove that $\Phi(p^a)$ is no larger than the size of the smallest complete diverse cap in $(\mathbb{Z}/p\mathbb{Z})^2$, and we also assert the existence of a complete diverse cap in $(\mathbb{Z}/p\mathbb{Z})^2$ with no more than $p+1$ points when $p$ is odd. This implies the above displayed upper bound for $\Phi(n)$.

While the upper bound is more difficult to prove than the lower bound, we also suspect that it is less tight. Following the proof of the upper bound for $\Phi(n)$, we give computational evidence supporting this view.

We conclude the paper with a large number of open questions.

# 2 A Pair of Lower Bounds for $\Phi(n)$

Our goal in this section is to prove the lower bound

$$\Phi(n) \geq \max\{4, \sqrt{2p} + \frac{1}{2}\},$$

where $p$ is the smallest prime divisor of $n$. Both estimates will follow without too much difficulty from Lemma 2.2, which gives an upper bound for the number of points which can lie on lines between a pair of two points. Before the proof of the lemma, we will demonstrate a basic result concerning the structure of $(\mathbb{Z}/n\mathbb{Z})^2$. For the basic definitions of group theory that we make use of in the rest of this article, we refer the reader to Lang [12].

**Lemma 2.1.** *Let $x, y \in (\mathbb{Z}/n\mathbb{Z})^2$ be two points of order $d$. Then there exists an automorphism of $(\mathbb{Z}/n\mathbb{Z})^2$ which takes $x$ to $y$.*

*Proof.* Write $x = (x_1, x_2)$. It suffices to show that there exists an automorphism of $(\mathbb{Z}/n\mathbb{Z})^2$ which takes $(n/d, 0)$ to $x$. It is a simple exercise in the Chinese remainder theorem to prove that any cyclic subgroup of $(\mathbb{Z}/n\mathbb{Z})^2$ is contained in a cyclic subgroup of order $n$ (this was the motivation for our definition of lines in $(\mathbb{Z}/n\mathbb{Z})^2$). It follows that we can find some $x' = (x'_1, x'_2)$ of order $n$ such that $\frac{n}{d} \cdot x' = x$. Since the order of $x'$ is $n$, we deduce that $g = \gcd(x'_1, x'_2)$ is a unit in $\mathbb{Z}/n\mathbb{Z}$. Now we may find $a, b \in \mathbb{Z}/n\mathbb{Z}$ such that $ax'_1 + bx'_2 = g$. It therefore follows that the matrix

$$\begin{pmatrix} x'_1 & -b \\ x'_2 & a \end{pmatrix}$$

is in $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$, and the corresponding automorphism of $(\mathbb{Z}/n\mathbb{Z})^2$ takes $(n/d, 0)$ to $x$. $\square$

With the aid of Lemma 2.1, we can give an elementary upper bound for the number of points which lie on lines between two given points.

**Lemma 2.2.** *If $x \in (\mathbb{Z}/n\mathbb{Z})^2$ is a point of order $d$, then there are at most $n^2/d$ points on lines through $0$ and $x$.*

*Proof.* By Lemma 2.1, we may assume that $x = (n/d, 0)$. Let $S$ be the set of points on lines through $0$ and $x$. It suffices to show that

$$S \subset \{(y, y') : y' \equiv 0 \pmod{d}\}.$$

Suppose that $(y, y') \in S$. Then there are $a$, $b \in \mathbb{Z}/n\mathbb{Z}$ with $\gcd(a, b, n) = 1$ such that

$$\begin{aligned} ay + by' &= 0 \\ an/d &= 0. \end{aligned}$$

The second equation implies that $a \equiv 0 \pmod{d}$. Therefore $by' \equiv 0 \pmod{d}$. But $b$ is a unit mod $d$, for if $\gcd(b, d) = g$, then $g$ is a common divisor of $a$, $b$, and $n$ since $d \mid a$ and $d \mid n$. Therefore $y' \equiv 0 \pmod{d}$. $\square$

A simple counting argument now gives the first of our lower bounds for $\Phi(n)$.

**Proposition 2.3.** *Let $p$ be the smallest prime divisor of $n$. Then*

$$\Phi(n) > \sqrt{2p} + \frac{1}{2}.$$

*Proof.* Suppose that $X$ is a complete cap. If $x$ and $y$ are distinct points of $X$, then the order of $x - y$ is at least $p$. By Lemma 2.2, the number of points on lines between $x$ and $y$ is at most $n^2/p$. It follows from the completeness of $X$ that there must be at least $p$ pairs of points in $X$. Therefore

$$\frac{1}{2} \cdot \left(|X| - \frac{1}{2}\right)^2 > \binom{|X|}{2} \geq p,$$

from which the bound follows. $\square$

Another application of Lemma 2.2 is the following proposition, which gives our second lower bound for $\Phi(n)$.

**Proposition 2.4.** *If $n > 1$, then $\Phi(n) \geq 4$.*

*Proof.* From Lemma 2.2, it is clear that $\Phi(n) \geq 3$. So suppose that some complete cap $X$ has only three points. By Lemma 2.1, we may assume that the three points are 0, $(n/d, 0)$, and $x$, where $d \mid n$. Additionally, we may assume that there are at least as many points on lines between 0 and $(n/d, 0)$ as there are on lines between the other two pairs of points of $X$. Now there are at most $n^2/d$ points between 0 and $(n/d, 0)$, from which it follows that $d \leq 3$. If it were the case that $d = 3$, then it would be necessary for the set of points on lines between $x$ and 0 to be disjoint from the set of points on lines between 0 and $(n/d, 0)$, which is impossible as each set contains 0. We conclude that $d = 2$.

If the order of $x$ is 2, then either $x = (0, n/2)$ or $(n/2, n/2)$. In the first case, the point $(n/2, n/2)$ lies on no line, and in the second case the point $(0, n/2)$ lies on no line. Thus the order of $x$ is at least 3. If the order of $x$ is 3, then the order of $x - (n/2, 0)$ must be 6. The number of points on lines through $x$ and 0 is at most $n^2/3$, and the number of points on lines through $x$ and $(n/2, 0)$ is at most $n^2/6$, so the number of points on lines through two points of $X$, one of which is $x$, is at most $-1 + n^2/2$. As there are at most $n^2/2$ points on lines through 0 and $(n/2, 0)$, there must be some point of $(\mathbb{Z}/n\mathbb{Z})^2$ which is on no line through two points of $X$. If instead the order of $x$ is 4 or 6 then a contradiction is obtained in the same manner. When the order of $x$ is 5 or at least 7, then the order of $x - (n/2, 0)$ is at least 5, so since $2/5 < 1/2$ we once again obtain a contradiction. Therefore no such $X$ exists, and we deduce that $\Phi(n) \geq 4$ whenever $n > 1$. $\square$

## 3 An Upper Bound for $\Phi(n)$

In this section, we will prove the upper bound

$$\Phi(n) \leq \max\{4, p+1\}, \tag{1}$$

where $p$ is the smallest prime divisor of $n$. Our first step will be to show that if $n$ and $m$ are coprime, then

$$\Phi(nm) \leq \min\{\Phi(n), \Phi(m)\}. \tag{2}$$

From this result, we see that to establish inequality (1) it will suffice to prove that $\Phi(2^a) = 4$ and $\Phi(p^a) \leq p+1$ for every odd prime power $p^a$. Before proving inequality (2), we need a simple lemma which relates the structure of collinear triples in $(\mathbb{Z}/nm\mathbb{Z})^2$ with the structure of collinear triples in $(\mathbb{Z}/n\mathbb{Z})^2$ and $(\mathbb{Z}/m\mathbb{Z})^2$.

**Lemma 3.1.** *Let $n$ and $m$ be coprime integers. Then points $x, y, z \in (\mathbb{Z}/nm\mathbb{Z})^2$ are collinear if and only if their residues modulo $n$ and their residues modulo $m$ are collinear.*

*Proof.* Apply the Chinese remainder theorem to the coefficients $a$,$b$, and $c$ of a line passing through $x$, $y$, and $z$. It is worth mentioning that if the congruence $x \equiv y \pmod{n}$ holds coordinatewise, then the residues modulo $n$ of $x$, $y$, and $z$ are automatically collinear. $\square$

**Proposition 3.2.** *If $n$ and $m$ are coprime integers with $n, m > 1$, then*

$$\Phi(nm) \leq \min\{\Phi(n), \Phi(m)\}.$$

*Proof.* We prove $\Phi(nm) \leq \Phi(n)$. Let $X \subset (\mathbb{Z}/n\mathbb{Z})^2$ be a complete cap with $|X| = \Phi(n)$. Consider the subset $X \times \{0\} \subset (\mathbb{Z}/n\mathbb{Z})^2 \times (\mathbb{Z}/m\mathbb{Z})^2$, realized as a subset of $(\mathbb{Z}/nm\mathbb{Z})^2$ under the isomorphism of the Chinese remainder theorem. This subset has no collinear triples modulo $n$, so by Lemma 3.1 it follows that $X \times \{0\}$ is a cap. Now suppose that $x \in (\mathbb{Z}/nm\mathbb{Z})^2$. By the completeness of $X$, there are points $y, z \in X$ such that the residue of $x$ modulo $n$ is collinear with $y$ and $z$ in $(\mathbb{Z}/n\mathbb{Z})^2$. This is to say that the residue of $x$ modulo $n$ is collinear with the residues of $(y, 0)$ and $(z, 0)$ modulo $n$. But the residue of $x$ modulo $m$ is clearly collinear with two copies of 0 in $(\mathbb{Z}/m\mathbb{Z})^2$, so $\{x, (y, 0), (z, 0)\}$ is a collinear triple by Lemma 3.1. Therefore $X \times \{0\}$ is complete, and $\Phi(nm) \leq \Phi(n)$. $\square$

In light of Proposition 3.2, we will concentrate on finding upper bounds for $\Phi(p^a)$, where $p$ is prime. Our main approach will be to examine the following construction: suppose we are given a cap $X$ in $(\mathbb{Z}/p\mathbb{Z})^2$, and let $n$ be a positive integer. Consider the subset $p^{a-1} * X \subset (\mathbb{Z}/p^a\mathbb{Z})^2$ which is intuitively defined by viewing $X$ as a subset of $(\mathbb{Z}/p^a\mathbb{Z})^2$ and multiplying the coordinates of each element of $X$ by $p^{a-1}$ (this definition will be made more rigorous in Section 4). We will show in Section 4 that $p^{a-1} * X$ is a cap. We would like to be able to conclude that $p^{a-1} * X$ is complete whenever $X$ is; unfortunately, this is not generally true. For instance, if $f\colon \mathbb{Z}/5\mathbb{Z} \to \mathbb{Z}/5\mathbb{Z}$ is the function given by $f(x) = x^2$, then the graph of $f$,

$$\Gamma_f = \{(x, x^2) : x \in \mathbb{Z}/5\mathbb{Z}\} \subset (\mathbb{Z}/5\mathbb{Z})^2,$$

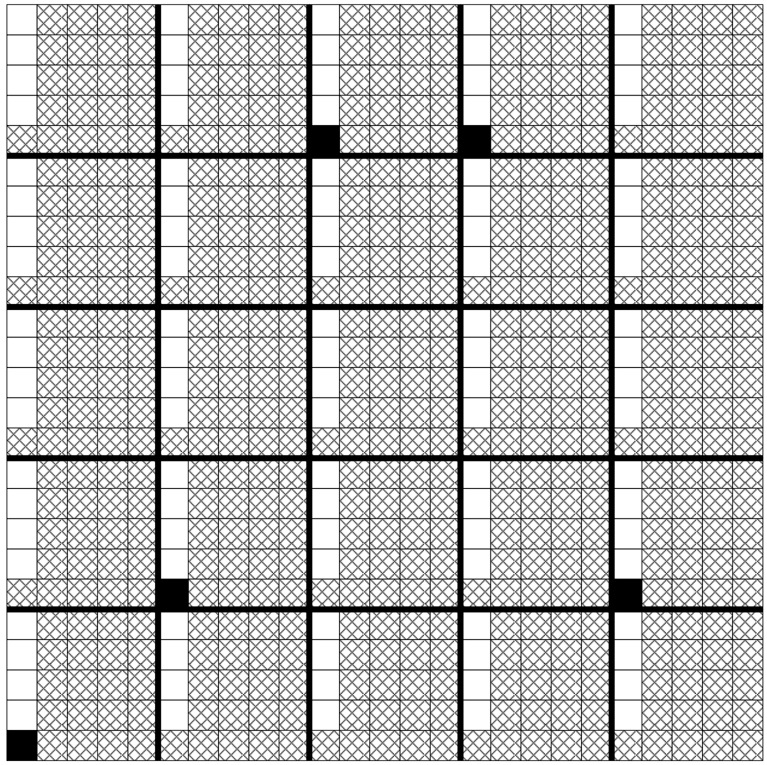


Figure 1: This illustrates the set of points which lie on lines through pairs of points of $5 * \Gamma_f = \{(5x, 5x^2) : 0 \leq x \leq 4\} \subset (\mathbb{Z}/25\mathbb{Z})^2$. Black squares represent points of $5 * \Gamma_f$, while shaded squares represent points lying on lines through pairs of points of $5 * \Gamma_f$. Note that the white squares are exactly those points of order 25 whose residues modulo 5 lie on the line of slope $\infty$ through 0 in $(\mathbb{Z}/5\mathbb{Z})^2$.

is a complete cap such that $5 * \Gamma_f \subset (\mathbb{Z}/25\mathbb{Z})^2$ is not a complete cap (see Figure 1).

For distinct points $x = (x_1, x_2)$ and $y = (y_1, y_2)$ in $(\mathbb{Z}/p\mathbb{Z})^2$, define the *slope* $t$ between $x$ and $y$ by the usual formula

$$t = \frac{y_2 - x_2}{y_1 - x_1},$$

putting $t = \infty$ when $y_1 = x_1$ so that $t \in \mathbb{Z}/p\mathbb{Z} \cup \{\infty\}$. As just shown, the cap $5 * \Gamma_f$ fails to be complete. However, the next theorem (whose proof is delayed until later) characterizes exactly why $5 * \Gamma_f$ fails to be complete: there is no pair of points in $\Gamma_f$ whose slope is infinite. If a subset of $(\mathbb{Z}/p\mathbb{Z})^2$ contains pairs of points of every slope, we will call it *diverse*.

**Theorem 3.3.** *Let $X \subset (\mathbb{Z}/p\mathbb{Z})^2$ be a complete cap. The following are equivalent:*

1. *$X$ is diverse.*

2. *$p * X \subset (\mathbb{Z}/p^2\mathbb{Z})^2$ is a complete cap.*

*3.* $p^{a-1} * X \subset (\mathbb{Z}/p^a\mathbb{Z})^2$ *is a complete cap for every* $a \geq 1$.

*Proof.* See Section 4. □

In Theorem 3.5, we will show that there is a complete diverse cap in $(\mathbb{Z}/p\mathbb{Z})^2$ for every odd prime $p$. As the maximum size of a cap in $(\mathbb{Z}/p\mathbb{Z})^2 = \mathrm{AG}(2,p)$ is $p+1$ (see [3]), it will therefore follow that $\Phi(p^a) \leq p+1$ for every odd prime $p$. In order to prove the diversity of our construction, we will need an analogue of the Cauchy-Davenport theorem from additive number theory (see [14, p. 43]). The proof is simple, so we include it here for the sake of completeness.

**Lemma 3.4.** *Let* $S \subset \mathbb{Z}/p\mathbb{Z}$ *with* $|S| \geq (p+3)/2$*, where* $p$ *is an odd prime. Put*

$$S \dot{+} S = \{s_1 + s_2 : s_i \in S \text{ and } s_1 \neq s_2\}.$$

*Then* $S \dot{+} S = \mathbb{Z}/p\mathbb{Z}$.

*Proof.* Fix some $x \in \mathbb{Z}/p\mathbb{Z}$, and consider the sets $S$ and $x - S$. Since $|S| \geq (p+3)/2$, the set $S \cap (x - S)$ has at least 3 elements. However, there is at most one way to write $x = 2s$ for some $s \in S$ since $p$ is odd. Therefore there are distinct $s_1, s_2 \in S$ such that $s_1 = x - s_2$. We conclude that $x = s_1 + s_2 \in S \dot{+} S$. □

**Theorem 3.5.** *Let* $p$ *be an odd prime. There exists a complete diverse cap* $X \subset (\mathbb{Z}/p\mathbb{Z})^2$.

*Proof.* See Figure 2 for an example of the construction when $p = 13$. Define an equivalence relation $\sim$ on $\mathbb{Z}/p\mathbb{Z}$ by declaring $x \sim y$ iff $x = y$ or $x = y^{-1}$, placing 0 in its own equivalence class. Let $S$ be a set of equivalence class representatives for $\sim$. The elements 0, 1, and $-1$ are each unique in their equivalence classes, while all other classes have size 2, so

$$|S| = 3 + \frac{p-3}{2} = \frac{p+3}{2}.$$

Define a function $f\colon S \to \mathbb{Z}/p\mathbb{Z}$ by $f(x) = x^2$, and consider the graph of $f$,

$$\Gamma_f = \{(x, x^2) : x \in S\} \subset (\mathbb{Z}/p\mathbb{Z})^2.$$

First we must show that $\Gamma_f$ contains no collinear triple. If it were the case that $(x, x^2)$, $(y, y^2)$, and $(z, z^2)$ were collinear for distinct $x$, $y$, and $z$, then we would have

$$y + x = \frac{y^2 - x^2}{y - x} = \frac{y^2 - z^2}{y - z} = y + z,$$

which forces $x = z$, a contradiction. Moreover, it is also the case that $\Gamma_f \cup \{(0, -1)\}$ contains no collinear triple. For if $(0, -1)$ were contained in some collinear triple, there would be distinct nonzero $x, y \in S$ such that $(0, -1)$, $(x, x^2)$, and $(y, y^2)$ are collinear. This requires

$$y + x = \frac{y^2 - x^2}{y - x} = \frac{y^2 + 1}{y - 0} = y + y^{-1},$$

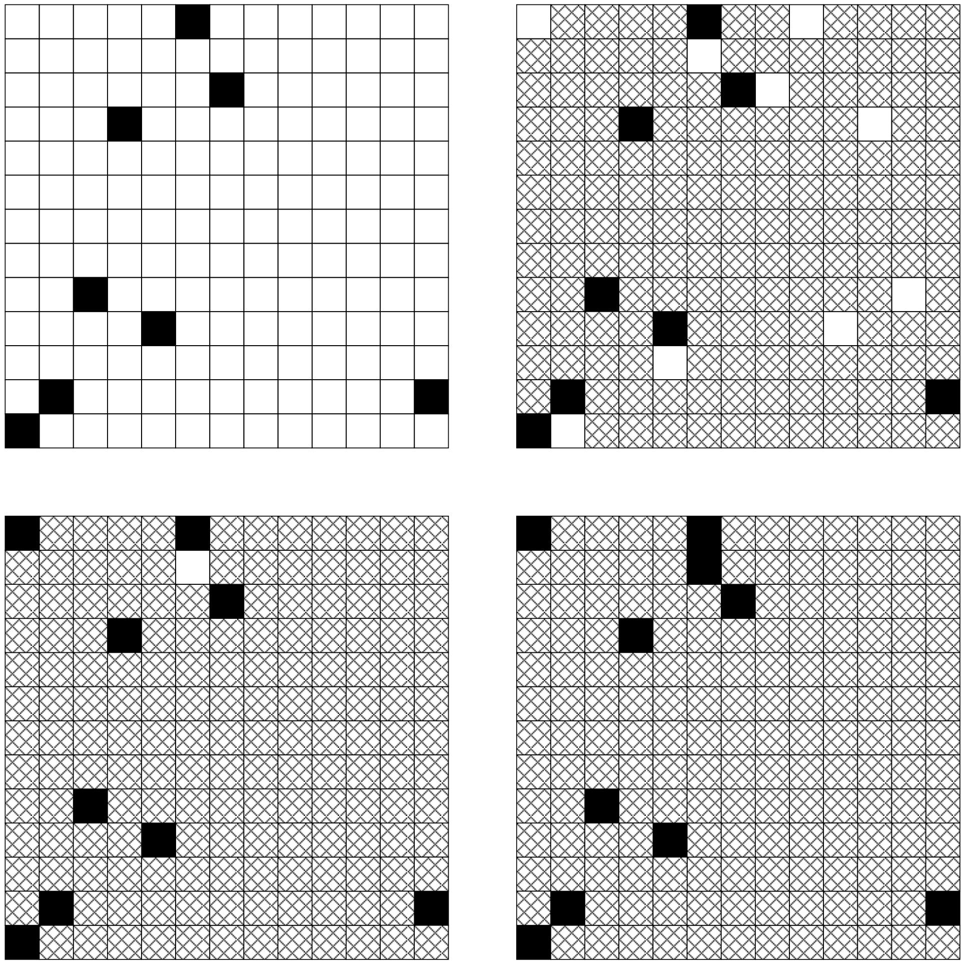


Figure 2: The four figures above demonstrate the steps of the construction in Theorem 3.5 when $p = 13$. Let $S = \{0, 1, 2, 3, 4, 5, 6, 12\} \subset \mathbb{Z}/13\mathbb{Z}$. Then $S$ is a set of equivalence class representatives for the relation $\sim$ defined in the proof of Theorem 3.5. The top left grid is the graph $\Gamma_f$ of the function $f\colon S \to \mathbb{Z}/13\mathbb{Z}$ defined by $x \mapsto x^2$. Observe that for every finite slope $t \in \mathbb{Z}/13\mathbb{Z}$, there is a pair of points in the graph of $f$ whose slope is $t$. The top right grid is the set of points which lie on lines through pairs of points in the graph of $f$. Note that $(0, 12)$ lies on no line through a pair of two points of $\Gamma_f$. The bottom left grid is the set of points which lie on lines between pairs of points of $\Gamma_f \cup \{(0, 12)\}$. In the bottom right grid, we add the point $(5, 11)$ to $\Gamma_f \cup \{(0, 12)\}$ to obtain a complete cap of size 10 which contains pairs of points of every slope. From Theorem 3.3 it follows that $\Phi(13^a) \leq 10$ for every $a \geq 1$.

from which we deduce that $x = y^{-1}$. But since $x \neq y$ and $x, y \in S$, this is impossible.

Finally, we claim that $\Gamma_f \cup \{(0,-1)\}$ is diverse. The slope between $(0,0)$ and $(0,-1)$ is $\infty$, so it suffices to show that $\Gamma_f$ contains pairs of points of every finite slope. So let $t \in \mathbb{Z}/p\mathbb{Z}$. By Lemma 3.4, there are distinct $x, y \in S$ such that $t = x + y$. Then the slope between $(x, x^2)$ and $(y, y^2)$ is

$$\frac{y^2 - x^2}{y - x} = x + y = t.$$

Hence $\Gamma_f \cup \{(0,-1)\}$ is a diverse cap in $(\mathbb{Z}/p\mathbb{Z})^2$. We can now add points to $\Gamma_f \cup \{(0,-1)\}$ to make it complete. □

**Theorem 3.6.** *For each odd prime power* $p^a$*,*

$$\Phi(p^a) \leq p + 1.$$

*Additionally,* $\Phi(2^a) \leq 4$.

*Proof.* When $p$ is odd, this is an immediate consequence of Theorems 3.3 and 3.5, together with the fact that the maximum size of a cap in $(\mathbb{Z}/p\mathbb{Z})^2$ is $p+1$. When $p = 2$, simply observe that the cap $X = (\mathbb{Z}/2\mathbb{Z})^2$ is diverse, and apply Theorem 3.3. □

**Corollary 3.7.** *If* $n$ *is even, then* $\Phi(n) = 4$*. Otherwise, if* $p$ *is the smallest prime dividing* $n$*, then* $\Phi(n) \leq p + 1$.

*Proof.* Combine Propositions 2.4 and 3.2 with Theorem 3.6. □

We do not expect that our upper bound is close to being tight. The main reason for this is that we have merely asserted the existence of complete diverse caps in $(\mathbb{Z}/p\mathbb{Z})^2$; ideally one would show that there are actually *small* complete diverse caps in $(\mathbb{Z}/p\mathbb{Z})^2$ to obtain a better upper bound. We expect that the smallest complete diverse caps are roughly the same size as the smallest complete caps. This suspicion is based on computer trials which suggest that a very large portion of complete caps are also diverse. For $11 \leq p \leq 31$, we generated 1000 random complete caps by the following algorithm: let $X_0 = \emptyset \subset (\mathbb{Z}/p\mathbb{Z})^2$. Given $X_n$, construct $X_{n+1}$ by selecting a point of $(\mathbb{Z}/p\mathbb{Z})^2$ which lies on no line between pairs of points of $X_n$, and adding this point to $X_n$. This process stops when the resulting cap is complete. The following table displays what percentage of these 1000 complete caps were diverse for each prime $p$.

| $p$ | Percentage of random complete caps which were diverse |
|---|---|
| 11 | 96.3 % |
| 13 | 96.2 % |
| 17 | 96.8 % |
| 19 | 96.0 % |
| 23 | 97.3 % |
| 29 | 97.4 % |
| 31 | 96.8 % |

In light of this data, we would not be surprised if the probabilistic methods of Kim and Vu used in [10] could be applied to this problem to produce small complete diverse caps in $(\mathbb{Z}/p\mathbb{Z})^2$. This could potentially improve the upper bound to something closer to $\sqrt{p} \cdot (\ln p)^{10}$.

Using our upper bound, we are also able to calculate $\Phi(n)$ exactly for many small values of $n$. We include a table of small values of $\Phi(n)$ here. We omit cases where $n$ is divisible by 2 or 3, as $\Phi(n) = 4$ in these cases. When the answer is not exactly known, we provide the range of possible values known to us through the lower bounds of Section 2 and computer trials which generated random complete and complete diverse caps. Particularly when $n$ is prime, there may be sharper known values existing in the literature.

| $n$ | $\Phi(n)$ |
|---|---|
| 5 | 5 |
| 7 | 6 |
| 11 | $6 \leq \Phi(11) \leq 7$ |
| 13 | $6 \leq \Phi(13) \leq 8$ |
| 17 | $7 \leq \Phi(17) \leq 10$ |
| 19 | $7 \leq \Phi(19) \leq 11$ |
| 23 | $8 \leq \Phi(23) \leq 12$ |
| 25 | $4 \leq \Phi(25) \leq 6$ |

When $p$ is a prime between 7 and 23, the size of the smallest known complete diverse cap is identical to the upper bound given for $\Phi(p)$ in the above table. For $p = 5$, the smallest complete diverse cap has 6 elements, hence the upper bound for $\Phi(25)$.

# 4 Conditions equivalent to diversity

To complete the proof of our upper bound, we must complete the proof of Theorem 3.3, whose statement we recall here.

**Theorem 3.3.** *Let $X \subset (\mathbb{Z}/p\mathbb{Z})^2$ be a complete cap. The following are equivalent:*

1. *$X$ is diverse.*

2. *$p * X \subset (\mathbb{Z}/p^2\mathbb{Z})^2$ is a complete cap.*

3. *$p^{a-1} * X \subset (\mathbb{Z}/p^a\mathbb{Z})^2$ is a complete cap for every $a \geq 1$.*

The proof of this theorem will comprise this section. Before proceeding, we must introduce some notation to eliminate confusion. For a prime $p$, let $M_p$ be the monoid whose underlying set is $\{p^a : a \geq 0\}$, with multiplication of integers as the binary operation. Define a left monoid action $*$ of $M_p$ on the disjoint union

$$\coprod_{i=1}^{\infty} (\mathbb{Z}/p^i\mathbb{Z})^2$$

as follows: if $x \in (\mathbb{Z}/p^a\mathbb{Z})^2$, then pick any element $\overline{x}$ of $(\mathbb{Z}/p^{a+1}\mathbb{Z})^2$ whose reduction modulo $p^a$ equals $x$, and define $p * x = p \cdot \overline{x} \in (\mathbb{Z}/p^{a+1}\mathbb{Z})^2$. This action is clearly well-defined. Since $M_p$ is a cyclic monoid, we can extend this definition to all of $M_p$ uniquely by demanding that $*$ be a monoid action. Our earlier "intuitive" definition of $p * X$ obviously coincides with the notion that $p * X$ is the image of $X$ under the map $p*$. The necessity of this rigorous definition of $*$ will become apparent in the following proofs, as we frequently need to distinguish between the multiplication of the usual $\mathbb{Z}$-module structure on $(\mathbb{Z}/p^a\mathbb{Z})^2$ and our $*$-multiplication which changes the ground ring of the element being acted upon.

We will need the following basic properties relating the $\mathbb{Z}$-module structure and the $*$-multiplication.

1. $*$ commutes with ordinary multiplication: if $x \in (\mathbb{Z}/p^a\mathbb{Z})^2$, $b \geq 0$, and $k \in \mathbb{Z}$, then
$$p^b * (kx) = k(p^b * x).$$
2. $*$ distributes over addition: if $x, y \in (\mathbb{Z}/p^a\mathbb{Z})^2$ and $b \geq 0$, then
$$p^b * (x + y) = p^b * x + p^b * y.$$
3. $*$ is order-preserving: if $x \in (\mathbb{Z}/p^a\mathbb{Z})^2$ has order $p^c$ and $b \geq 0$, then the order of $p^b * x$ is $p^c$.

The proofs of these statements are immediate from the definition of $*$. These properties will be used implicitly in the proofs which follow. One last useful property of $*$ is that $p^{a-1}* : (\mathbb{Z}/p\mathbb{Z})^2 \to (\mathbb{Z}/p^a\mathbb{Z})^2$ maps $(\mathbb{Z}/p\mathbb{Z})^2$ bijectively onto the elements of order at most $p$ in $(\mathbb{Z}/p^a\mathbb{Z})^2$.

With this notational framework out of the way, we are ready proceed with the proof of Theorem 3.3. As a preliminary step, we prove that the action of $*$ actually preserves caps. For an element $x$ of a group $G$, we denote by $\langle x \rangle$ the cyclic subgroup generated by $x$. With this notation, lines in $(\mathbb{Z}/n\mathbb{Z})^2$ are exactly the subsets of the form $y + \langle x \rangle$, where $x, y \in (\mathbb{Z}/n\mathbb{Z})^2$ and $x$ is an element of order $n$.

**Proposition 4.1.** *Let $X \subset (\mathbb{Z}/p\mathbb{Z})^2$ be a cap. Then $p^{a-1} * X \subset (\mathbb{Z}/p^a\mathbb{Z})^2$ is also a cap.*

*Proof.* By way of contradiction, assume that $\{x, x', x''\}$ is a triple in $X$ such that $\{p^{a-1} * x, p^{a-1} * x', p^{a-1} * x''\}$ is collinear in $(\mathbb{Z}/p^a\mathbb{Z})^2$. Without loss of generality, we may take $x'' = 0$. Fix a line containing $\{p^{a-1} * x, p^{a-1} * x', 0\}$. This line is actually a cyclic subgroup of $(\mathbb{Z}/p^a\mathbb{Z})^2$ of order $p^a$. Let $y$ be a generator of this subgroup. Then $p^{a-1}y$ is an element of order $p$ in $(\mathbb{Z}/p^a\mathbb{Z})^2$, and we can find some $z \in (\mathbb{Z}/p\mathbb{Z})^2$ with $p^{a-1} * z = p^{a-1}y$. Now $z$ is an element of order $p$ in $(\mathbb{Z}/p\mathbb{Z})^2$, so $\langle z \rangle$ is a line in $(\mathbb{Z}/p\mathbb{Z})^2$.

We claim that $\langle z \rangle$ contains $x$ and $x'$. Since $y$ has order $p^a$ and $p^{a-1} * x$ has order $p$, we see that there is some $k$ coprime to $p$ such that $p^{a-1} * x = kp^{a-1}y$. Now
$$p^{a-1} * (kz) = k(p^{a-1} * z) = kp^{a-1}y = p^{a-1} * x.$$
But $*$ is faithful, so $kz = x$ and $x \in \langle z \rangle$. Similarly $x' \in \langle z \rangle$, which violates our assumption that $X$ is a cap. ◻

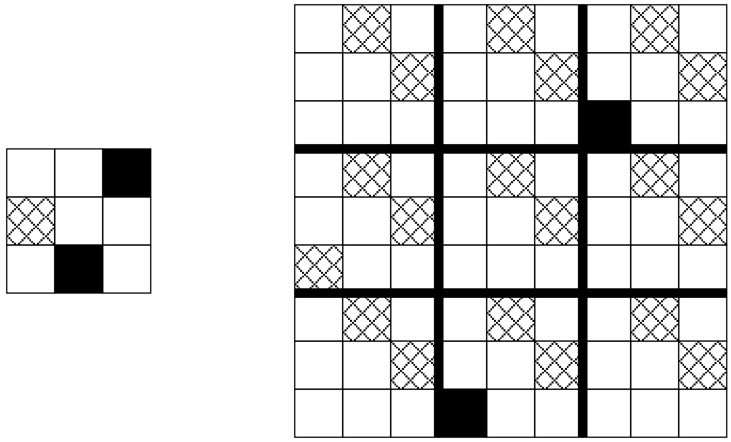


Figure 3: The set of points lying on lines through $(3,0)$ and $(6,6)$ in $(\mathbb{Z}/9\mathbb{Z})^2$ is equal to the set of points of order 9 whose residues modulo 3 lie on the line of slope 2 through 0 in $(\mathbb{Z}/3\mathbb{Z})^2$, together with the points of order 3 such that dividing each coordinate by 3 gives a point of $(\mathbb{Z}/3\mathbb{Z})^2$ which lies on the line through $(1,0)$ and $(2,2)$. When we put $x = (1,0) \in (\mathbb{Z}/3\mathbb{Z})^2$ and $x' = (2,2) \in (\mathbb{Z}/3\mathbb{Z})^2$, this is a consequence of the proof of Proposition 4.2.

We now begin the proof of Theorem 3.3. In the following proposition, we prove the implication (1) $\Rightarrow$ (2).

**Proposition 4.2.** *Let $X \subset (\mathbb{Z}/p\mathbb{Z})^2$ be a complete diverse cap. Then $p * X \subset (\mathbb{Z}/p^2\mathbb{Z})^2$ is a complete cap.*

*Proof.* See Figure 3. Since $X$ is a cap, it is clear that $p * X$ is a cap. Additionally, since $X$ is complete, it follows that every element of $(\mathbb{Z}/p^2\mathbb{Z})^2$ which has order at most $p$ lies on some line between two points of $p * X$. So suppose that $z \in (\mathbb{Z}/p^2\mathbb{Z})^2$ has order $p^2$, and let $t$ be the slope between 0 and the residue of $z$ modulo $p$ in $(\mathbb{Z}/p\mathbb{Z})^2$. Assume that $t \neq \infty$; the analysis in this case is similar. It follows that we can find a point $y$ in $(\mathbb{Z}/p\mathbb{Z})^2$ and some $i \in (\mathbb{Z}/p^2\mathbb{Z})^\times$ such that

$$z = p * y + i(1, \bar{t}),$$

where $\bar{t}$ denotes one of the lifts of $t$ to an element of $\mathbb{Z}/p^2\mathbb{Z}$ under the reduction map $\mathbb{Z}/p^2\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$. Let $x$ and $x'$ be points of $X$ such that the slope between $x$ and $x'$ is $t$. Consider the line

$$p * x + \langle (1, \bar{t}) + i^{-1}(p * (y - x)) \rangle \subset (\mathbb{Z}/p^2\mathbb{Z})^2. \tag{3}$$

The line between $x$ and $x'$ in $(\mathbb{Z}/p\mathbb{Z})^2$ is given by

$$x + \langle (1, t) \rangle,$$

so any line in $(\mathbb{Z}/p^2\mathbb{Z})^2$ which contains

$$p * x + \langle p * (1, t) \rangle$$

will contain both $p * x$ and $p * x'$. But the line (3) contains the above set since $p(1, \overline{t}) = p * (1, t)$ and $p(p * (y - x)) = 0$, so it must contain $p * x$ and $p * x'$. However, this line also contains $z$ since

$$p * x + i((1, \overline{t}) + i^{-1}(p * (y - x))) = p * y + i(1, \overline{t}) = z.$$

Therefore $z$ lies on a line between two points of $p * X$. As this holds for any $z$, we conclude that $p * X$ is complete. $\square$

Before proving the implication (2) $\Rightarrow$ (3) of Theorem 3.3, we must establish a technical lemma.

**Lemma 4.3.** *Let $y, y' \in (\mathbb{Z}/p\mathbb{Z})^2$, and let $a \geq 3$. Suppose that $x \in (\mathbb{Z}/p^{a-1}\mathbb{Z})^2$ has order $p^{a-1}$, and assume that $x$ lies on some line containing $p^{a-2} * y$ and $p^{a-2} * y'$. If the order of $z \in (\mathbb{Z}/p^a\mathbb{Z})^2$ is $p^a$ and $z$ lies on a line through $0$ and $p * x$, then $z$ lies on a line through $p^{a-1} * y$ and $p^{a-1} * y'$.*

*Proof.* See Figure 4 for an example of the hypotheses in this lemma. Since $z$ lies on a line through 0 and $p * x$, the order of $p * x$ in $(\mathbb{Z}/p^a\mathbb{Z})^2$ is $p^{a-1}$, and the order of $z$ in $(\mathbb{Z}/p^a\mathbb{Z})^2$ is $p^a$, it follows that there is some $k$ prime to $p$ such that $kpz = p * x$ (note that the multiplication on the left is the usual multiplication in $\mathbb{Z}/p^a\mathbb{Z}$). As $\{x, p^{a-2} * y, p^{a-2} * y'\}$ is a collinear triple in $(\mathbb{Z}/p^{a-1}\mathbb{Z})^2$ and $x$ and $x - p^{a-2} * y$ have order $p^{a-1}$, we see that

$$p^{a-2} * y' \in \langle x - p^{a-2} * y \rangle + p^{a-2} * y.$$

From this it follows that $\{p * x, p^{a-1} * y, p^{a-1} * y'\}$ is a collinear triple in $(\mathbb{Z}/p^a\mathbb{Z})^2$ which lies in the subset

$$\langle p * x - p^{a-1} * y \rangle + p^{a-1} * y \subset (\mathbb{Z}/p^a\mathbb{Z})^2.$$

Since the order of $p * x$ in $(\mathbb{Z}/p^a\mathbb{Z})^2$ is $p^{a-1} > p$, the order of $p^{a-1} * y'$ in $(\mathbb{Z}/p^a\mathbb{Z})^2$ is at most $p$, and the order of $p^{a-1} * y$ in $(\mathbb{Z}/p^a\mathbb{Z})^2$ is at most $p$, we deduce that there is some $j$ coprime to $p$ such that

$$\begin{aligned} p^{a-1} * y' &= jp^{a-2}(p * x - p^{a-1} * y) + p^{a-1} * y \\ &= jp^{a-2}(p * x) - jp^{a-2}(p^{a-1} * y) + p^{a-1} * y \\ &= jp^{a-2}(p * x) + p^{a-1} * y, \end{aligned}$$

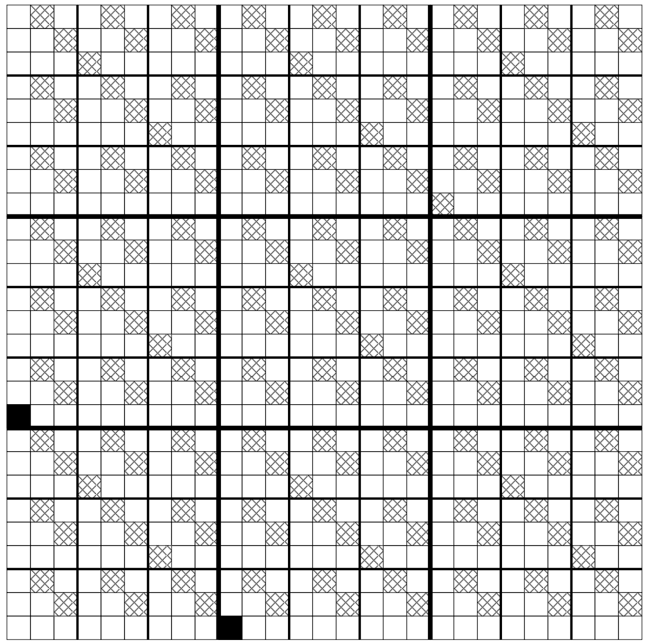
where the last equality holds since $p^{a-1} * y$ has order at most $p$ and $a \geq 3$. Then

$$\begin{aligned} jkp^{a-1}(z - p^{a-1} * y) + p^{a-1} * y &= jp^{a-2}(kpz) + p^{a-1} * y \\ &= jp^{a-2}(p * x) + p^{a-1} * y \\ &= p^{a-1} * y', \end{aligned}$$

so that

$$p^{a-1} * y' \in \langle z - p^{a-1} * y \rangle + p^{a-1} * y.$$

Clearly $z$ and $p^{a-1} * y$ lie on the above line, so we are done. $\square$



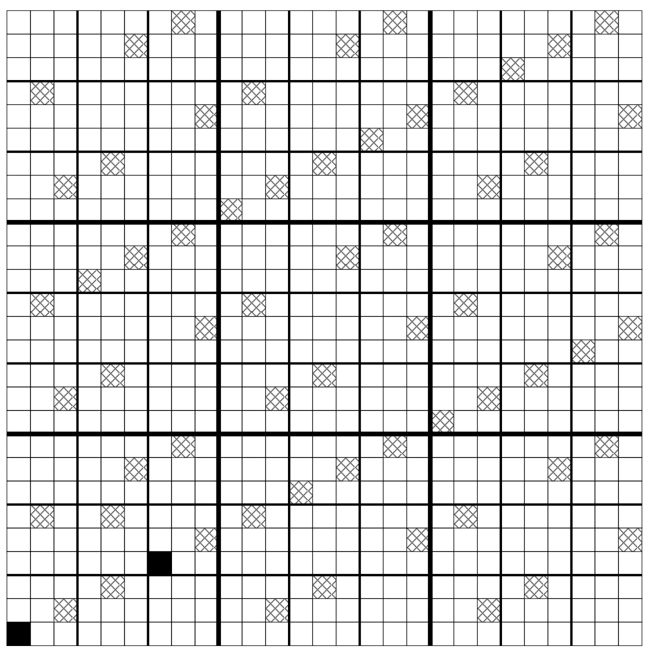


Figure 4: The top grid shows the set of points on lines through $(9, 0)$ and $(0, 9)$ in $(\mathbb{Z}/27\mathbb{Z})^2$, while the bottom grid shows the set of points on lines through $(0, 0)$ and $(6, 3)$. Notice that the points of order 27 which lie on lines through $(0, 0)$ and $(6, 3)$ also lie on lines through $(9, 0)$ and $(0, 9)$. This is a consequence of Lemma 4.3 with $y = (1, 0) \in (\mathbb{Z}/3\mathbb{Z})^2$, $y' = (0, 1) \in (\mathbb{Z}/3\mathbb{Z})^2$, $x = (2, 1) \in (\mathbb{Z}/9\mathbb{Z})^2$, and $a = 3$.

**Proposition 4.4.** *If $X \subset (\mathbb{Z}/p\mathbb{Z})^2$ is such that $p * X \subset (\mathbb{Z}/p^2\mathbb{Z})^2$ is a complete cap, then $p^{a-1} * X \subset (\mathbb{Z}/p^a\mathbb{Z})^2$ is a complete cap for every $a \geq 1$.*

*Proof.* We prove this by induction on $a$. Clearly if $p * X$ is a complete cap then $X$ is a complete cap as well, so the cases $a = 1$ and $a = 2$ are done. So suppose that $p^{a-2} * X \subset (\mathbb{Z}/p^{a-1}\mathbb{Z})^2$ is a complete cap, where $a \geq 3$. As a consequence, we are given that every point in $(\mathbb{Z}/p^a\mathbb{Z})^2$ of order at most $p^{a-1}$ lies on some line between two points of $p^{a-1} * X$. So suppose that $z \in (\mathbb{Z}/p^a\mathbb{Z})^2$ has order $p^a$, and let $\overline{z}$ be the image of $z$ under the reduction $(\mathbb{Z}/p^a\mathbb{Z})^2 \to (\mathbb{Z}/p^{a-1}\mathbb{Z})^2$. Now $\overline{z}$ lies on a line through $p^{a-2} * y$ and $p^{a-2} * y'$ for some $y, y' \in X$, the order of $\overline{z}$ is $p^{a-1}$, and $z$ lies on the line $\langle z \rangle$ which contains 0 and $p * \overline{z}$ since $p * \overline{z} = pz$, so Lemma 4.3 (with $x = \overline{z}$) implies that $z$ lies on a line through $p^{a-1} * y$ and $p^{a-1} * y'$. Therefore $p^{a-1} * X \subset (\mathbb{Z}/p^a\mathbb{Z})^2$ is complete, and the induction may proceed. $\square$

At this point, we have proven enough of Theorem 3.3 that our arguments in Section 3 are valid. Since the implication (3) $\Rightarrow$ (2) of Theorem 3.3 is trivial, all that is left to complete our classification is to prove the implication (2) $\Rightarrow$ (1).

**Proposition 4.5.** *Suppose that $X \subset (\mathbb{Z}/p\mathbb{Z})^2$ is a complete cap such that $p*X \subset (\mathbb{Z}/p^2\mathbb{Z})^2$ is a complete cap. Then $X$ is diverse.*

*Proof.* Let $t \in \mathbb{Z}/p\mathbb{Z}$ be a finite slope; once again the analysis when $t = \infty$ is similar. Since $p * X \subset (\mathbb{Z}/p^2\mathbb{Z})^2$ is complete, there exist $x, y \in X$ such that $\{(1, \overline{t}), p * x, p * y\}$ is a collinear triple in $(\mathbb{Z}/p^2\mathbb{Z})^2$, where $\overline{t}$ is any lift of $t$ to $\mathbb{Z}/p^2\mathbb{Z}$ under the reduction map $\mathbb{Z}/p^2\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$. As the order of $(1, \overline{t}) - p * x$ is $p^2$, it follows easily that

$$p * y \in \langle (1, \overline{t}) - p * x \rangle + p * x.$$

Then by order considerations there must be some $j$ coprime to $p$ such that

$$p * y = jp((1, \overline{t}) - p * x) + p * x = p * (j(1, t) + x).$$

Since our map $p*\colon (\mathbb{Z}/p\mathbb{Z})^2 \to (\mathbb{Z}/p^2\mathbb{Z})^2$ is injective, we deduce that $y = j(1, t) + x$, from which it immediately follows that the slope between $x$ and $y$ is $t$. Therefore $X$ is diverse. $\square$

This completes the proof of Theorem 3.3.

# 5 Open Questions

## 5.1 Higher dimensions and general groups

In this article, we have concerned ourselves entirely with determining the minimum size of a complete cap in $(\mathbb{Z}/n\mathbb{Z})^2$. The same question for $(\mathbb{Z}/n\mathbb{Z})^s$ is just as natural, although it seems much more difficult. The question when $n$ is a prime is the question of determining the minimum size of a complete cap in $\mathrm{AG}(s, p)$, which is already known to be difficult.

At the very least, it would be interesting to obtain bounds on the minimum size of a complete cap in $(\mathbb{Z}/n\mathbb{Z})^s$.

On the other hand, we could approach this question from the group-theoretic standpoint, and consider a similar question for arbitrary (or just abelian) finite groups. The abelian case is surely simpler, and perhaps more interesting since it has a natural geometric structure induced by the structure of the torus. Of course the order constraint on the definition of a line should be removed; the most natural definition is probably to declare a line to be any translate of a maximal cyclic subgroup.

**Problem 5.1.** *What is the minimum number of points in a complete cap in some finite groups?*

## 5.2 Improving Proposition 3.2

An obvious question to ask regarding Proposition 3.2 is whether equality always holds. If it does always hold, then this would mean that a complete cap of minimum size in $(\mathbb{Z}/nm\mathbb{Z})^2$ can always be obtained from a complete cap in $(\mathbb{Z}/n\mathbb{Z})^2$ or a complete cap in $(\mathbb{Z}/m\mathbb{Z})^2$ whenever $n$ and $m$ are coprime. We believe that this is always the case.

**Conjecture 5.2.** *If $n$ and $m$ are coprime integers which are at least 2, then*

$$\Phi(nm) = \min\{\Phi(n), \Phi(m)\}.$$

This conjecture is true for all factorizations of numbers smaller than 35 since all composite integers $n$ smaller than 35 with at least 2 prime divisors satisfy $\Phi(n) = 4$. Of course, if this conjecture is true, then the computation of $\Phi(n)$ would be entirely reduced to the computation of $\Phi(p^a)$ for prime powers $p^a$.

## 5.3 Are diverse constructions best possible?

For a prime number $p$, denote by $\Phi'(p)$ the minimum size of a complete diverse cap in $(\mathbb{Z}/p\mathbb{Z})^2$ (we know that such a cap exists by Theorem 3.5). There are many interesting questions relating $\Phi$ to $\Phi'$. First, are there complete caps of minimum size in $(\mathbb{Z}/p\mathbb{Z})^2$ which are also diverse? We conjecture that if $p$ is large enough, then the answer is yes.

**Conjecture 5.3.** *For all sufficiently large primes $p$, we have $\Phi(p) = \Phi'(p)$.*

Without the "sufficiently large" hypothesis, the conjecture fails for $p = 5$. This conjecture is based on our computational evidence which suggests that almost all complete caps are diverse for large enough values of $p$.

Another natural question is whether we can always obtain a complete cap of minimal size in $(\mathbb{Z}/p^a\mathbb{Z})^2$ from a complete diverse cap in $(\mathbb{Z}/p\mathbb{Z})^2$ by multiplying all points by $p^{a-1}$. This is equivalent to the following question.

**Problem 5.4.** *Does $\Phi'(p) = \Phi(p^a)$ for each $a > 1$?*

A weaker statement is the following conjecture, which already seems to be difficult.

**Conjecture 5.5.** *If $a \leq b$, then $\Phi(p^a) \leq \Phi(p^b)$.*

Although this seems intuitively obvious, we have no idea how to prove it.

## 5.4 Improving Theorem 3.5

We use the same notation as in the proof of Theorem 3.5. It appears that the cap $\Gamma_f \cup \{(0,-1)\}$ may actually be very close to being complete. It is easy to show that all points of the curve $y = x^2$ lie on a line between two points of $\Gamma_f \cup \{(0,-1)\}$. So let $(j,k)$ be a point of $(\mathbb{Z}/p\mathbb{Z})^2$ with $k \neq j^2$. It is not difficult to show that $(j,k)$ lies on no line between two points of $\Gamma_f$ if and only if

1. $j \in S$,
2. the function $g$ defined on $(\mathbb{Z}/p\mathbb{Z}) \setminus \{j\}$ by
$$x \mapsto \frac{jx-k}{x-j}$$
has exactly two fixed points, both of which are in $S$, and
3. $|g(S) \cap S| = 2$.

Note that the map $g$ is injective and $g = g^{-1}$ (ignoring the behavior at poles). It seems like all three of these conditions can be met only very rarely, so that very few points of $(\mathbb{Z}/p\mathbb{Z})^2$ fail to lie on a line between two points of $\Gamma_f \cup \{(0,-1)\}$. It would even be interesting to show that at most $o(p)$ points satisfy all three of the above conditions, as this would yield a construction of a complete diverse cap containing $p/2 + o(p)$ points, improving our upper bound for $\Phi(p^a)$ greatly.

## 5.5 A coloring question for $\mathbb{Z}/p\mathbb{Z}$

In our proof of Theorem 3.5, we selected a subset $S$ of $(p+3)/2$ points from $\mathbb{Z}/p\mathbb{Z}$ in order to ensure that the graph of the function $f\colon S \to \mathbb{Z}/p\mathbb{Z}$ defined by $f(x) = x^2$ contained pairs of points of every slope. If we were able to pick the points of $S$ more explicitly, however, we might be able to make the size of $S$ much smaller.

Let us outline a possible approach for picking such a set $S$. Assume that there exists a coloring of $\mathbb{Z}/p\mathbb{Z}$ using the colors red and blue with the following properties:

1. The points $0, 1, 2, \ldots, \lfloor\sqrt{p}\rfloor, p-1$ are all red.
2. If $x \neq 0, 1, p-1$ and $x$ is red, then $x^{-1}$ is blue.
3. For each $s \in \mathbb{Z}/p\mathbb{Z}$, the elements $s, s+1, s+2, \ldots, s+\lfloor\sqrt{p}\rfloor$ are not all blue.

Also, pick this coloring so that there are few red points as possible. Now let $S \subset \mathbb{Z}/p\mathbb{Z}$ be the set of all red points, and consider $\Gamma_f$, where $f$ is the same function as before, defined on $S$. By the second condition above, we see that $\Gamma_f \cup \{(0, -1)\}$ is a cap. The first and third conditions together imply that $\Gamma_f$ contains pairs of points of every finite slope, so $\Gamma_f \cup \{(0, -1)\}$ is diverse. The set $S$ appears to have many fewer than $(p+3)/2$ points; in fact we believe that the size of $S$ is roughly $2\sqrt{p}$ provided that a coloring with the above properties exists.

**Problem 5.6.** *Does a coloring of $\mathbb{Z}/p\mathbb{Z}$ with properties* (1)–(3) *always exist?*

Unfortunately, we cannot immediately say anything interesting about the size of a complete cap $X$ obtained from $\Gamma_f \cup \{(0, -1)\}$ since the completion process may add a large number of points, but it seems reasonable to expect that if we can start with a cap which contains a small number of points then it might be possible to complete the cap more efficiently–that is, we may be able to add fewer points to complete the cap.

**Problem 5.7.** *Given any cap $X \subset (\mathbb{Z}/p\mathbb{Z})^2$ with $o(p)$ points, can we find a cap $Y$ containing $X$ which has, say, $p/2 + o(p)$ points?*

## 5.6 Saturated sets

A subset $X \subset (\mathbb{Z}/n\mathbb{Z})^2$ is said to be *saturated* if every point in $(\mathbb{Z}/n\mathbb{Z})^2$ lies on a line between two points of $X$. In the context of $\mathrm{PG}(2, q)$, saturated sets have been studied fairly thoroughly; as far as we are aware there are no results on saturated sets in $(\mathbb{Z}/n\mathbb{Z})^2$. Theorem 3.3 actually shows that any diverse saturated set in $(\mathbb{Z}/p\mathbb{Z})^2$ gives rise to a diverse saturated set in $(\mathbb{Z}/p^a\mathbb{Z})^2$ for every $a$. This fact could prove to be very useful in studying the following question.

**Problem 5.8.** *What is the minimum size of a saturated subset of $(\mathbb{Z}/n\mathbb{Z})^2$?*

# 6 Acknowledgements

I would like to thank Reid Barton, David Arthur, and Joseph Gallian for comments which greatly improved the presentation of this paper. This research was conducted in Duluth, Minnesota at Joseph Gallian's REU program under grants from the National Science Foundation (DMS-0137611) and the National Security Agency (H-98230-04-1-0050).

# References

[1] S. Ball, On small complete arcs in a finite plane, Discrete Math. 174 (1997) 29-34.

[2] A. Blokhuis, Polynomials in finite geometry and combinatorics: Survey in Combinatorics, Cambridge Univ. Press, Cambridge (1993), 35-52.

[3] J. Bierbrauer and Y. Edel, Bounds on affine caps, Journal of Combinatorial Designs. 10 (2002) 111-115.

[4] J. Bierbrauer, Large Caps, J. Geom. 76 (2003) 16-51.

[5] J. Cooper and J. Solymosi, Collinear points in permutations, Ann. Combin. 9 (2005) 169-175.

[6] A. Davydov and P. Östergård, Recursive constructions of complete caps, J. Statist. Plann. Inference. 95 (2001) 167-173.

[7] J.W.P. Hirschfeld, Projective Geometries over Finite Fields, Clarendon Press, Oxford, 1979.

[8] J. Huizenga, The maximum size of caps in $(\mathbb{Z}/n\mathbb{Z})^2$, Preprint.

[9] F. Kárteszi, Introduction to Finite Geometries, Akadémiai Kiadó, Budapest, 1976.

[10] J.H. Kim and V.H. Vu, Small complete arcs in projective planes, Combinatorica 23 (2003) 311-363.

[11] G. Korchmáros, New examples of complete $k$-arcs in $\mathrm{PG}(2,q)$, European J. Combin. 4 (1983) 329-334.

[12] S. Lang, Algebra, rev. 3rd Edition, Springer Verlag, 2002.

[13] C.C. Lindner and C.A. Rodger, Design Theory, CRC Press, New York, 1997.

[14] R. Meshulam, On subsets of finite abelian groups with no 3-term arithmetic progressions, J. Combin. Theory Ser. A. 71 (1995) 168-172.

[15] M. B. Nathanson, Additive Number Theory: Inverse Problems and the Geometry of Sumsets, Springer, New York, 1996.

[16] B. Segre, Le geometrie di Galois, Ann. Mat. Pura Appl. 48 (1959) 1-97.

[17] B. Segre, Introduction to Galois Geometries, J.W.P. Hirschfeld, ed., Mem. Accad. Naz. Lincei (8) Vol. VIII 5 (1967).

[18] T. Szőnyi, Small complete arcs in Galois planes, Geom. Dedicata 18 (1985) 161-172.

[19] T. Szőnyi, Note on the order of magnitude of $k$ for complete $k$-arcs in $\mathrm{PG}(2,q)$, Discrete Math. 66 (1987) 279-282.