Arithmetic Progressions of Length Three in Multiplicative Subgroups of $\mathbb{F}_p$

Jeremy F. Alm

January 2018

Abstract

In this paper, we give an algorithm for detecting non-trivial 3-APs in multiplicative subgroups of $\mathbb{F}_p^\times$ that is substantially more efficient than the naive approach. It follows that certain Var der Waerden-like numbers can be computed in polynomial time.

1 Introduction

Additive structures inside multiplicative subgroups of $\mathbb{F}_p^\times$ have recently received attention. Alon and Bourgain [1] study solutions to $x + y = z$ in $H < \mathbb{F}_p^\times$, and Chang [2] studies arithmetic progressions in $H < \mathbb{F}_p^\times$. In this paper, we define a Van der Waerden-like number for $H < \mathbb{F}_p^\times$ of index n, and give a polynomial-time algorithm for determining such numbers.

Definition 1. *Let $VW_3^\times(n)$ denote the least prime $q \equiv 1 \pmod{n}$ such that for all primes $p \equiv 1 \pmod{n}$ with $p \geq q$, the multiplicative subgroup of $\mathbb{F}_p^\times$ of index n contains a mod-p arithmetic progression of length three.*

Our main results are the following two theorems:

Theorem 2. *$VW_3^\times(n) \leq (1+\varepsilon)n^4$ for all sufficiently large n (depending on ε). In particular, $VW_3^\times(n) \leq 1.001n^4$ for all $n \geq 45$.*

Theorem 3. *$VW_3^\times(n)$ can be determined by an algorithm that runs in $\mathcal{O}(\frac{n^8}{\log n})$ time.*

Chang [2] proves that if $H < \mathbb{F}_p^\times$ and $|H| > cp^{3/4}$, then H contains nontrivial 3-progressions. This implies our Theorem 2 with $(1+\varepsilon)n^4$ replaced by cn^4. We prove our Theorem 2 because we need to make the constant explicit.

2 Proof of Theorem 2

Proof. We use one of the basic ideas of the proof of Roth's Theorem on 3-progressions [3]. Let $A \subseteq \mathbb{F}_p$ with $|A| = \delta p$. Note that a 3-progression is a solution inside A to the equation $x + y = 2z$. Let $\mathcal{N}$ be the number of (possibly trivial) solutions to $x + y = 2z$ inside A. We have that

$$\frac{1}{p}\sum_{k=0}^{p-1} e^{\frac{-2\pi ik}{p}x} = \begin{cases} 1, & \text{if } x \equiv 0 \pmod{p}; \\ 0, & \text{if } x \not\equiv 0 \pmod{p}. \end{cases} \tag{1}$$

Because of (1), we have

$$\mathcal{N} = \sum_{x\in A}\sum_{y\in A}\sum_{z\in A}\frac{1}{p}\sum_{k=0}^{p-1} e^{\frac{-2\pi ik}{p}(x+y-2z)} \tag{2}$$

Rearranging (2), we get

$$\begin{aligned}
&\frac{1}{p}\sum_{k=0}^{p-1}\sum_{x\in A}\sum_{y\in A}\sum_{z\in A} e^{\frac{-2\pi ik}{p}x}\cdot e^{\frac{-2\pi ik}{p}y}\cdot e^{\frac{2\pi ik}{p}z} \\
&= \frac{1}{p}\sum_{k=0}^{p-1}\left[\sum_{x\in A} e^{\frac{-2\pi ik}{p}x} \cdot \sum_{y\in A} e^{\frac{-2\pi ik}{p}y} \cdot \sum_{z\in A} e^{\frac{2\pi ik}{p}2z}\right] \\
&= \frac{1}{p}\sum_{k=0}^{p-1}\left[\sum_{x\in\mathbb{F}_p} \mathrm{Ch}_A(x)e^{\frac{-2\pi ik}{p}x} \cdot \sum_{y\in\mathbb{F}_p} \mathrm{Ch}_A(y)e^{\frac{-2\pi ik}{p}y} \cdot \sum_{z\in\mathbb{F}_p} \mathrm{Ch}_A(-2z)e^{\frac{2\pi ik}{p}z}\right] \\
&= \frac{1}{p}\sum_{k=0}^{p-1} \hat{\mathrm{Ch}}_A(k)^2\cdot\hat{\mathrm{Ch}}_A(-2k),
\end{aligned} \tag{3}$$

where Ch_A denotes the characteristic function of A, and $\hat{f}$ denotes the Fourier transform of f,

$$\hat{f}(x) = \sum_{k=0}^{p-1} f(k) e^{\frac{-2\pi i k}{p} x}.$$

Now we can pull out the $k = 0$ term from (3):

$$\begin{aligned}
(3) &= \frac{1}{p}\hat{\mathrm{Ch}}(0)^3 + \frac{1}{p}\sum_{k=1}^{p-1} \hat{\mathrm{Ch}}_A(k)^2 \cdot \hat{\mathrm{Ch}}_A(-2k) \\
&= \frac{|A|^3}{p} + \frac{1}{p}\sum_{k=1}^{p-1} \hat{\mathrm{Ch}}_A(k)^2 \cdot \hat{\mathrm{Ch}}_A(-2k) \\
&= \delta^3 p^2 + \frac{1}{p}\sum_{k=1}^{p-1} \hat{\mathrm{Ch}}_A(k)^2 \cdot \hat{\mathrm{Ch}}_A(-2k).
\end{aligned}$$

Let's call $\delta^3 p^2$ the *main term*, and $\frac{1}{p}\sum_{k=1}^{p-1} \hat{\mathrm{Ch}}_A(k)^2 \cdot \hat{\mathrm{Ch}}_A(-k)$ the *error term*. We now bound this error term.

Suppose $0 < \alpha < 1$ and $|\hat{\mathrm{Ch}}_A(k)| \leq \alpha p$ for all $0 \neq k \in \mathbb{F}_p$. In this case, we say that A is *α-uniform*. Then

$$\begin{aligned}
\left| \frac{1}{p}\sum_{k=1}^{p-1} \hat{\mathrm{Ch}}_A(k)^2 \cdot \hat{\mathrm{Ch}}_A(-2k) \right| &\leq \frac{1}{p} \max |\hat{\mathrm{Ch}}_A(k)| \cdot \left| \sum_{k=1}^{p-1} \hat{\mathrm{Ch}}_A(k)^2 \right| \\
&\leq \alpha \left| \sum_{k=1}^{p-1} \hat{\mathrm{Ch}}_A(k)^2 \right| \\
&\leq \alpha p \left| \sum_{k=1}^{p-1} \mathrm{Ch}_A(k)^2 \right| \\
&\leq \alpha \delta p^2.
\end{aligned}$$

Therefore $\mathcal{N} \geq \delta^3 p^2 - \alpha \delta p^2$. Subtracting off the trivial solutions gives $\mathcal{N} - \delta p \geq \delta^3 p^2 - \delta p - \alpha \delta p^2$. Hence there is at least one non-trivial solution if

$$\delta^3 p^2 > \delta p + \alpha \delta p^2.$$

Let $A = H$ be a multiplicative subgroup of $\mathbb{F}_p$ of index n. As is well-known (see for example [4, Corollary 2.5]), if H is a multiplicative subgroup of $\mathbb{F}_p^\times$, then H is α-uniform for $\alpha \leq p^{-1/2}$. Thus it suffices to have

$$\begin{aligned} \delta^3 p^2 \geq \delta p + p^{-1/2}\delta p^2 &\iff \delta^3 p^2 \geq \delta p + \delta p^{3/2} && (4)\\ &\iff \delta^2 p \geq 1 + p^{1/2} && (5)\\ &\iff (p-1)^2 \geq n^2 p(1+p^{1/2}) && (6)\end{aligned}$$

where the last line follows from $\delta = (p-1)/(np)$. It is straightforward to check that (6) is satisfied by $p = (1+\varepsilon)n^4$ for sufficiently large n.

□

The data gathered for $VW_3^\times(n)$, $n \leq 100$, suggest that the exponent of 4 on n is too large; see Figure 1. These data are available at `www.oeis.org`, sequence number A298566.

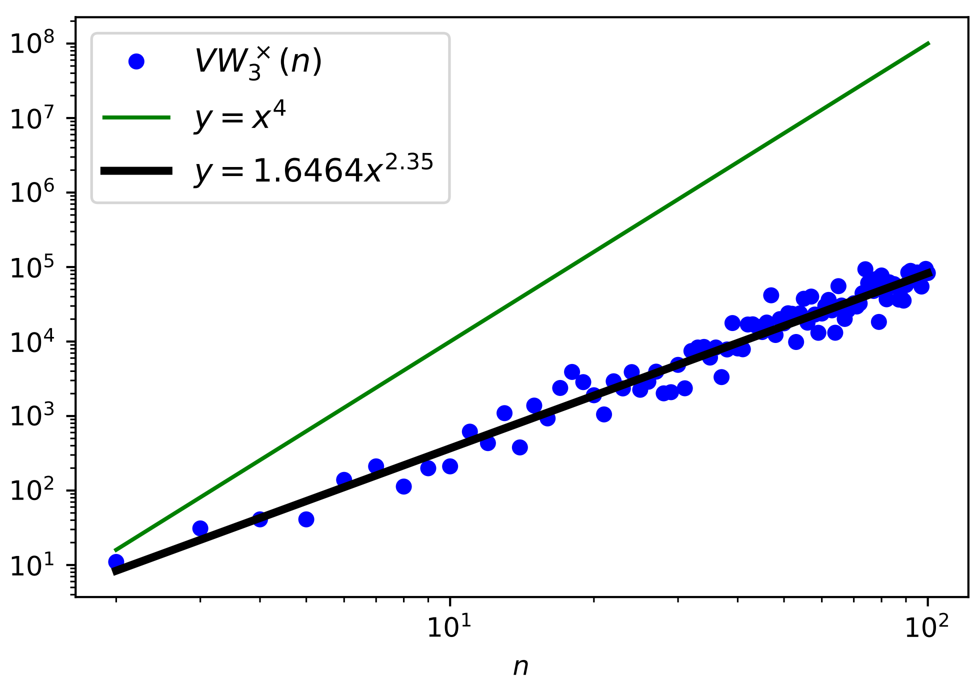

Figure 1: $VW_3^\times(n)$ for $n \leq 100$

3 A More General Framework

Before we establish our algorithm, it will helpful to generalize to arbitrary linear equations in three variables over $\mathbb{F}_p$. Suppose we're looking for solutions to $ax + by = cz$ in $H < \mathbb{F}_p^\times$, for fixed $a, b, c \in \mathbb{F}_p^\times$. There is a solution just in case $(aH + bH) \cap cH$ is nonempty.

The following result affords an algorithmic speedup in counting solutions to $ax + by = cz$ inside H:

Lemma 4. *For a, b, $c \in \mathbb{F}_p^\times$ and $H < \mathbb{F}_p^\times$,*

$$(aH + bH) \cap cH \neq \varnothing \textit{ if and only if } (c - aH) \cap bH \neq \varnothing.$$

Notice that while the implied computation on the left side of the biconditional is $\mathcal{O}(p^2)$, the one on the right is $\mathcal{O}(p)$, since we compute $|H|$ subtractions and $|H|$ comparisons. (We consider the index n fixed.)

Proof. Let $H = \{g^{kn} : 0 \leq k < (p-1)/n\}$, where n is the index of H and g is a primitive root modulo p. Fix $a, b, c \in \mathbb{F}_p$.

For the forward direction, suppose $(aH + bH) \cap cH \neq \varnothing$, so there are $x, y, z \in H$ such that $ax + by = cz$. Then $by = cz - ax$. Multiplying by $z^{-1} \in H$ yields $b(yz^{-1}) = c - a(xz^{-1})$. Therefore $(c - aH) \cap bH \neq \varnothing$. The other direction is similar. $\square$

Lemma 4 allows us to detect solutions to linear equations in linear time. The caveat for the case $a = b = 1$, $c = 2$ is that $H + H$ *always* contains $2H$, since $h + h = 2h$ for all $h \in H$; these solutions correspond to the trivial 3-APs h, h, h. (Similarly, $(2 - H) \cap H$ is always nonempty, since $1 \in H$ and $2 - 1 = 1$.) To account for this, we simply consider $H' = H \setminus \{1\}$, and calculate $(2 - H') \cap H'$ instead.

4 Proof of Theorem 3

Proof. Here is the algorithm.

Data: An integer $n > 1$
Result: The value of $VW_3^\times(n)$
Let $\mathcal{P} = \{p \text{ prime} : p \leq (1+\varepsilon)n^4,\ p \equiv 1 \pmod{n}\}$.
Set $p_0 = 1$.
Set Prev_boolean = False and Current_boolean = True.
for $p \in \mathcal{P}$ **do**
    Let H be the subgroup of $\mathbb{F}_p^\times$ of index n.
    Set Current_boolean to True if $(2 - H') \cap H'$ is non-empty, and False otherwise.
    if *Current_boolean is True and Prev_boolean is False* **then**
        set $p_0 = p$.
    end
    Set Prev_boolean to the value of Current_boolean.
end
Return p_0

Algorithm 1: Algorithm for determining $VW_3^\times(n)$

We now argue that Algorithm 1 runs in $\mathcal{O}\left(\frac{n^8}{\log n}\right)$ time. Since calculating $(2 - H') \cap H'$ is $\mathcal{O}(p)$ for each prime p, our runtime is bounded by

$$\sum_{\substack{p \leq (1+\varepsilon)n^4 \\ p \equiv 1 \pmod{n}}} \mathcal{O}(p) = \mathcal{O}\left(\sum_{\substack{p \leq (1+\varepsilon)n^4 \\ p \equiv 1 \pmod{n}}} p \right).$$

A standard estimate on the prime sum

$$\sum_{\substack{p \leq x \\ p \equiv 1 \pmod{n}}} p$$

is asymptotically $\frac{x^2}{\varphi(n) \log x}$, giving

$$
\mathcal{O}\left(\sum_{\substack{p\le(1+\varepsilon)n^4 \\ p\equiv 1 \pmod n}} p\right) = \mathcal{O}\left(\frac{n^8}{\varphi(n)\log(n^4)}\right)
$$

$$
= \mathcal{O}\left(\frac{n^8}{\log(n)}\right)
$$

as desired. □

Our timing data suggest that the correct runtime might be more like $\mathcal{O}(n^6)$; see Figure 2.

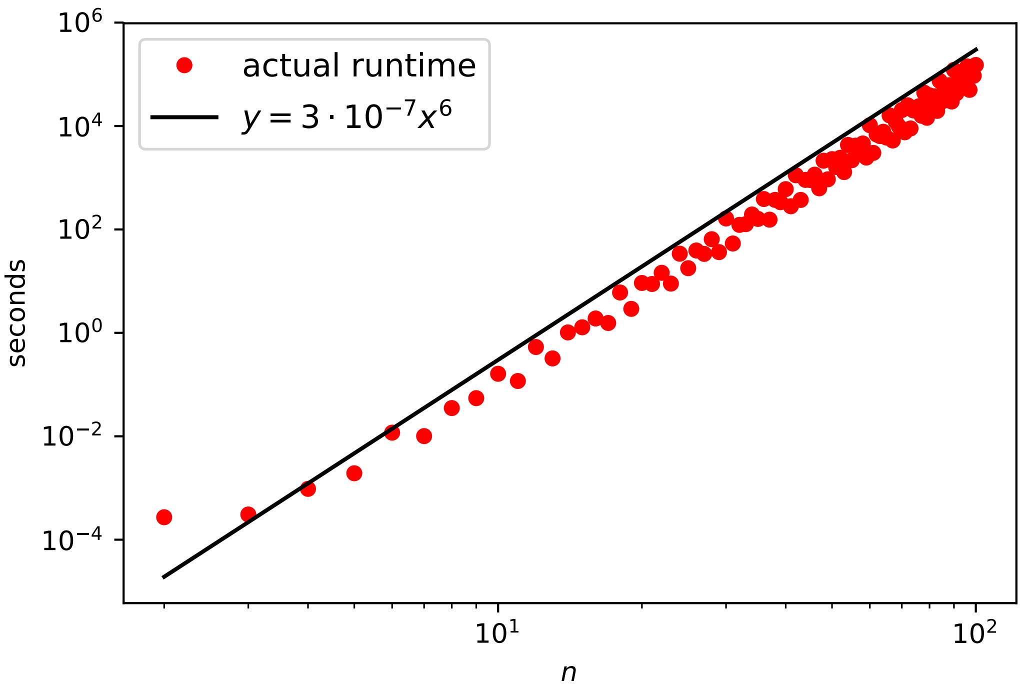

Figure 2: Runtime in seconds to determine $VW_3^\times(n)$

5 Further Directions

For any $a, b, c \in \mathbb{Z}^+$, we can define an analog to $VW_3^\times(n)$ by considering the equation $ax + by = cz$ instead of $x + y = 2z$. (Assume p is greater than a, b, and c.) The bound from Theorem 2 stays the same if $a + b = c$ and goes down to $n^4 + 5$ otherwise. But as suggested by the data in Figure 1, these bounds are not tight. How does the choice of a, b, and c affect the growth rate of the corresponding Van der Waerden-like number? Clearly $VW_3^\times(n)$ is not monotonic, but it appears to bounce above and below some "average" polynomial growth rate. Will that growth rate vary with the choice of a, b, and c? Does it depend on whether $a + b = c$ only?

6 Acknowledgements

The author wishes to thank Andrew Shallue and Valentin Andreev for many productive conversations.

References

[1] Noga Alon and Jean Bourgain. Additive patterns in multiplicative subgroups. *Geom. Funct. Anal.*, 24(3):721–739, 2014.

[2] Mei-Chu Chang. Arithmetic progressions in multiplicative groups of finite fields. *Israel J. Math.*, 222(2):631–643, 2017.

[3] K. F. Roth. On certain sets of integers. *J. London Math. Soc.*, 28:104–109, 1953.

[4] Tomasz Schoen and Ilya D. Shkredov. Additive properties of multiplicative subgroups of $\mathbb{F}_p$. *Q. J. Math.*, 63(3):713–722, 2012.