401 and beyond: improved bounds and algorithms for the Ramsey algebra search

Jeremy F. Alm
Department of Mathematics
Illinois College
Jacksonville, Il 62650
USA
alm.academic@gmail.com

Abstract

In this paper, we discuss an improvement of an algorithm to search for primes p and coset-partitions of $(\mathbb{Z}/p\mathbb{Z})^\times$ that yield Ramsey algebras over $\mathbb{Z}/p\mathbb{Z}$. We also prove an upper bound on the modulus p in terms of the number of cosets. We have, as a corollary, that there is no prime p for which there exists a partition of $(\mathbb{Z}/p\mathbb{Z})^\times$ into 13 cosets that yields a 13-color Ramsey algebra. Thus A263308(13) = 0.

1 Introduction

In this paper, we continue the project begun in [5] and recently continued in [3, 11] of constructing Ramsey algebras over $\mathbb{Z}/p\mathbb{Z}$ using multiplicative cosets. A *Ramsey algebra in m colors* is a partition of a set $U \times U$ into disjoint binary relations $Id, A_0, \ldots, A_{m-1}$ such that

(I.) $A_i^{-1} = A_i$;

(II.) $A_i \circ A_i = A_i^c$;

(III.) for $i \neq j$, $A_i \circ A_j = Id^c$.

Here, $Id = \{(x, x) : x \in U\}$ is the identity over U, $\circ$ is relational composition, $^{-1}$ is relational inverse, and ^{c} is complementation with respect to $U \times U$.

Ramsey algebras were first defined in [15] (but given no name). With the single exception of an alternate construction of the 3-color algebra (see [13]), all known constructions use the "guess-and-check" finite-field method of Comer, as follows: Fix $m \in \mathbb{Z}^+$, and let $X_0 = H$ be a multiplicative subgroup of $\mathbb{F}_q$of order $(q-1)/m$, where $q \equiv 1 \pmod{2m}$. Let $X_1, \ldots X_{m-1}$ be its cosets; specifically, let $X_i = g^i X_0 = \{g^{am+i} \pmod{p} : a \in \mathbb{Z}^+\}$, where g is a primitive root modulo p. Suppose the following conditions obtain:

(i.) $-X_i = X_i$;

(ii.) $X_i + X_i = \mathbb{F}_q \setminus X_i$,

(iii.) for $i \neq j$, $X_i + X_j = \mathbb{F}_q \setminus \{0\}$.

Then define $A_i = \{(x, y) \in \mathbb{F}_q \times \mathbb{F}_q : x - y \in X_i\}$. It is easy to check that (i.)-(iii.) imply (I.)-(III.), and we get a Ramsey algebra. Condition (ii.) implies that all the X_i's are sum-free. Consequently, the triangle-free Ramsey number $R_m(3)$ is a bound on the size of primes p such that there might be an m-color Ramsey algebra over $\mathbb{Z}/p\mathbb{Z}$.

Comer was able to construct m-color Ramsey algebras for $m = 1, 2, 3, 4, 5$ in 1983 [5]. In 2011, Maddux produced constructions for $m = 6, 7$ using the same method as Comer but with a 2011 computer [14]. Maddux failed to construct a Ramsey algebra for $m = 8$. In 2013, Manske and the author produced constructions over prime fields for all $m \leq 400$, with the exceptions of $m = 8$ and $m = 13$. We were able to rule out $m = 8$ by checking all primes up through the Ramsey bound $R(3, 3, 3, 3, 3, 3, 3, 3)$. Independently around that same time, Kowalski [11] produced constructions for all $m \leq 120$ except for $m = 8$ and $m = 13$, and found some constructions over non-prime fields. He also ruled out $m = 8$ over non-prime fields by checking all prime powers up through the Ramsey bound. The case of $m = 13$ was left open. In the present paper, we give constructions for all $401 \leq m \leq 2000$ using prime fields and prove an upper bound on p in terms of m that is much better than the Ramsey bound, allowing us to rule out $m = 13$ for prime fields.

In Section 2, we state some results we'll be assuming. In Section 3, we give a improvement of the algorithm, using a recent insight. In Section 4, we prove bounds on p in terms of m. The method of proof of the upper bound comes from additive number theory. The first idea is that if a set is "unstructured" with respect to addition, then it should contain a solution to $x + y = z$, and hence not be sum-free. The second idea is that subsets of a field cannot be both additively structured and multiplicatively structured. Since X_0 is a multiplicative subgroup, it is highly structured, so it must be additively unstructured, i.e., its elements are "randomly" distributed. This is an example of a so-called sum-product phenomenon. See [8]. Chung and Graham first studied quasirandom subsets of $\mathbb{Z}/n\mathbb{Z}$ in [4]. They showed that several different measures of quasirandomness were equivalent. The measure that we will use in Section 4 is that of having small nontrivial Fourier coefficients.

For more background on relation algebras, the reader is directed to any of [2, 10, 16].

2 Background from [3]

In order to give a more complete background, we repeat some lemmas from [3], condensed into one. The following lemma shows that, while multiplicative subgroups may appear randomly distributed, they and their cosets have some quite well-behaved sumset properties.

Lemma 1. *Let $m \in \mathbb{Z}^+$ and let $p = mk + 1$ be a prime number, k even, and g a primitive root modulo p. For $i \in \{0, 1, \ldots, m - 1\}$, define*

$$X_i = \left\{g^i, g^{m+i}, g^{2m+i}, \ldots, g^{(k-1)m+i}\right\}.$$

1. *X_0 is sum-free if and only if $1 \notin (X_0 + X_0)$;*

2. *If $X_0 + X_0 = (\mathbb{Z}/p\mathbb{Z}) \setminus X_0$, then $X_i + X_i = (\mathbb{Z}/p\mathbb{Z}) \setminus X_i$ for all $i \in \{1, 2, \ldots, m-1\}$.*

3. *If $X_0 + X_i = (\mathbb{Z}/p\mathbb{Z}) \setminus \{0\}$ for all $i \in \{1, 2, \ldots, m-1\}$, then $\forall i \neq j$, $X_i + X_j = (\mathbb{Z}/p\mathbb{Z}) \setminus \{0\}$.*

Lemma 1 tells us that the sumset structure of the X_i's has "rotational symmetry", which reduces the number of things that must be checked. In particular, it suffices to consider only those set sums involving X_0.

3 Improvement of the algorithm from [3]

The following lemma affords us a way to check, given m and $p \equiv 1 \pmod{2m}$, whether the m cosets of size $\frac{p-1}{m}$ form a Ramsey algebra.

Lemma 2. *Let $m \in \mathbb{Z}^+$ and let $p = mk + 1$ be a prime number, k even, and g a primitive root modulo p. For $i \in \{0, 1, \ldots, m-1\}$, define*

$$X_i = \left\{g^i, g^{m+i}, g^{2m+i}, \ldots, g^{(k-1)m+i}\right\}.$$

Then if $(X_0 + X_0) \cap X_j \neq \emptyset$, then $(X_0 + X_0) \supseteq X_j$.

This lemma is very easy to prove and was apparently known to Comer, but it seems that no one previously saw how to use it to get an algorithmic improvement.. The next corollary justifies the algorithm presented in the psuedocode below it. The algorithm is a special case of a more general one given in [1].

Corollary 3. *Suppose $(X_0 - 1) \cap X_0 = \emptyset$, but for all i, j not both zero, $(X_0 - g^j) \cap X_i \neq \emptyset$. Then the X_i's form a Ramsey algebra.*

```
Data: A prime p, a divisor m of (p − 1)/2, a primitive root g modulo p
Result: A Boolean, telling whether the corresponding cosets structure is a Ramsey
        algebra
Compute X_0 = {g^{am} (mod p) : 0 ≤ a < (p − 1)/m};
Compute g^j − X_0 (mod p) for each 0 ≤ j < m;
if (1 − X_0) ∩ X_0 ≠ ∅ then
 | return False
end
for i ← 1 to m − 1 do
 |  X_i = {g^{am+i} (mod p) : 0 ≤ a < (p − 1)/m}
 |  for j ← i to m − 1 do
 |   |  if (g^j − X_0) ∩ X_i = ∅ then
 |   |   | return False
 |   |  end
 |  end
end
return True
```

Algorithm 1: Fast algorithm for checking for Ramsey algebras

This algorithm is significantly faster. For example, Kowalski's results ($1 \le m \le 120$, skipping 8 and 13) can be reproduced in 59 seconds.

For each m between 1 and 2000, we have found the smallest prime modulus over which Comer's construction yields an m-color Ramsey algebra. The data are available in sequence A263308.

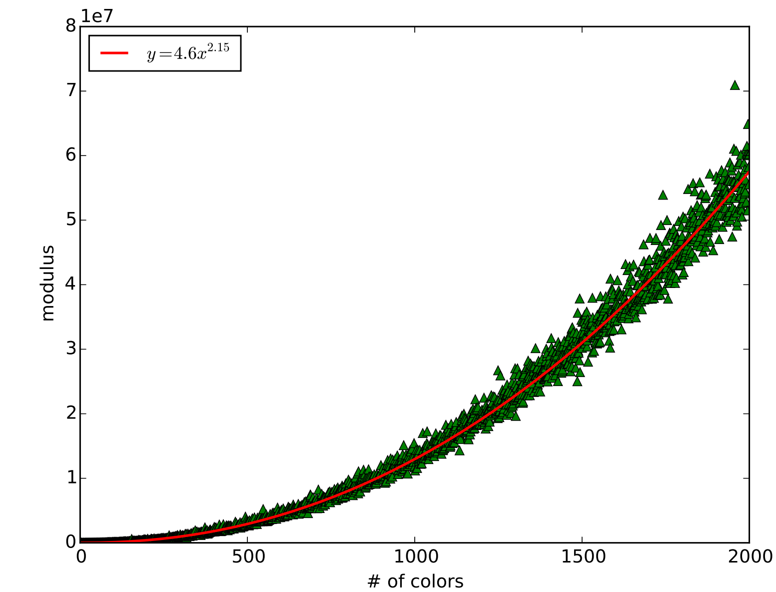


Figure 1: Computational data, with trendline

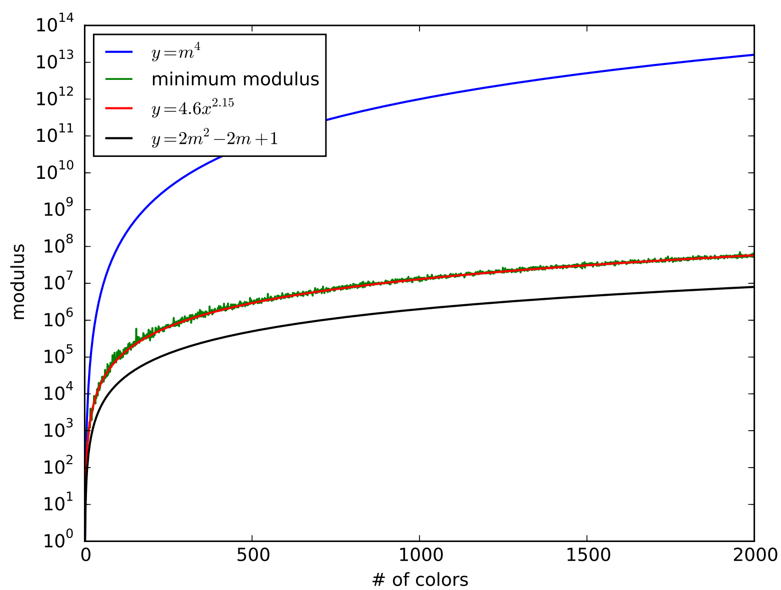


Figure 2: Computational data, with bounds proven in Section 4

4 The Fourier transform, quasirandom sets, and a Ramsey-like bound

Theorem 4. *Let the m-color multiplicative-coset Ramsey algebra be constructible over $\mathbb{Z}/p\mathbb{Z}$. Then for $m > 6$,*

$$2m^2 - 2m + 1 \le p < m^4$$

Proof. First we establish the lower bound by counting formal sums. Suppose $p < 2m^2 - 2m + 1$. Since $(p-1)/2$ must be divisible by m, and $(p-1)/m$ must be even, $p \le 2m^2 - 4m + 1$.

We must have $X_0 + X_0 = (\mathbb{Z}/p\mathbb{Z}) \backslash X_0$, so $|X_0 + X_0| = p - (p-1)/m$; however, counting formal sums we have

$$|X_0 + X_0| \le \binom{\left\lfloor \frac{p-1}{m} \right\rfloor}{2} + \left\lfloor \frac{p-1}{m} \right\rfloor - \frac{1}{2}\left\lfloor \frac{p-1}{m} \right\rfloor + 1 = \frac{\left\lfloor \frac{p-1}{m} \right\rfloor^2}{2} + 1$$

where the binomial coefficient is the number of sums of two distinct elements, $\left\lfloor \frac{p-1}{m} \right\rfloor$ counts the number of self-sums, $\frac{1}{2}\left\lfloor \frac{p-1}{m} \right\rfloor$ is a lower bound on the number of these sums that result in 0, and the 1 adds the identity back to the count.

Thus, it must be the case that

$$\frac{\left\lfloor \frac{p-1}{m} \right\rfloor^2}{2} + 1 \ge p - (p-1)/m. \tag{1}$$

Then one may check that if $p = 2m^2 - 4m + 1$, (1) fails to hold. Certainly, then, no smaller modulus will suffice.

We now turn our attention to the upper bound. It will suffice to show that for $p > m^4$, X_0 is not sum-free. We take as our starting point the ideas of Roth, who first used Fourier-analytic techniques to count the number of solutions to a linear equation inside a set [17]. Fourier analysis in additive number theory has become a subfield in its own right since the seminal work of Gowers [6, 7], now sometimes called quadratic Fourier analysis. We need only the "linear" Fourier analysis of Roth. We follow the development in [12].

Suppose we want to count the solutions to the equation $x + y = z$ inside a set $A \subseteq \mathbb{Z}/p\mathbb{Z}$ with $|A| = \delta p$. Let $\mathcal{N}$ be the number of solutions inside A. We have that

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

Because of (2), we have

$$\mathcal{N} = \sum_{x\in A}\sum_{y\in A}\sum_{z\in A}\frac{1}{p}\sum_{k=0}^{p-1} e^{\frac{-2\pi i k}{p}(x+y-z)} \tag{3}$$

Rearranging (3), we get

$$
\begin{aligned}
&\frac{1}{p}\sum_{k=0}^{p-1}\sum_{x\in A}\sum_{y\in A}\sum_{z\in A} e^{\frac{-2\pi ik}{p}x}\cdot e^{\frac{-2\pi ik}{p}y}\cdot e^{\frac{2\pi ik}{p}z} \\
&= \frac{1}{p}\sum_{k=0}^{p-1}\left[\sum_{x\in A} e^{\frac{-2\pi ik}{p}x} \cdot \sum_{y\in A} e^{\frac{-2\pi ik}{p}y} \cdot \sum_{z\in A} e^{\frac{2\pi ik}{p}z}\right] \\
&= \frac{1}{p}\sum_{k=0}^{p-1}\left[\sum_{x\in\mathbb{Z}/p\mathbb{Z}} Ch_A(x)e^{\frac{-2\pi ik}{p}x} \cdot \sum_{y\in\mathbb{Z}/p\mathbb{Z}} Ch_A(y)e^{\frac{-2\pi ik}{p}y} \cdot \sum_{z\in\mathbb{Z}/p\mathbb{Z}} Ch_A(-z)e^{\frac{2\pi ik}{p}z}\right] \\
&= \frac{1}{p}\sum_{k=0}^{p-1}\widehat{Ch}_A(k)^2\cdot\widehat{Ch}_A(-k), \qquad (4)
\end{aligned}
$$

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

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

Now we can pull out the $k = 0$ term from (4):

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

If we selected elements from $\mathbb{Z}/p\mathbb{Z}$ at random and placed them in A, then we'd expect δ^3p^2 solutions to $x + y - z = 0$ in A. In light of this, we'll call δ^3p^2 the *main term*, and $\frac{1}{p}\sum_{k=1}^{p-1}\widehat{Ch}_A(k)^2\cdot\widehat{Ch}_A(-k)$ the *error term*. The error term will measure how close (or far) A is from being a "random" set. We now bound this error term.

Suppose $0 < \alpha < 1$ and $|\widehat{Ch}_A(k)| \le \alpha p$ for all $0 \ne k \in \mathbb{Z}/p\mathbb{Z}$. In this case, we say that A

is α-*uniform*. Then

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

where the second-to-last line is by Parseval's identity.

Hence $\mathcal{N} \geq \delta^3 p^2 - \alpha\delta p^2$. So we want $\alpha < \delta^2$. By [18, Corollary 2.5], if H is a multiplicative subgroup of $\mathbb{Z}/p\mathbb{Z}$, then H is α-uniform for $\alpha = p^{-1/2}$. It is easy to check that if $p > m^4$, then $p^{-1/2} < \delta^2$. Therefore X_0 is δ^2-uniform, so it contains a solution to $x + y = z$ and hence is not sum-free. □

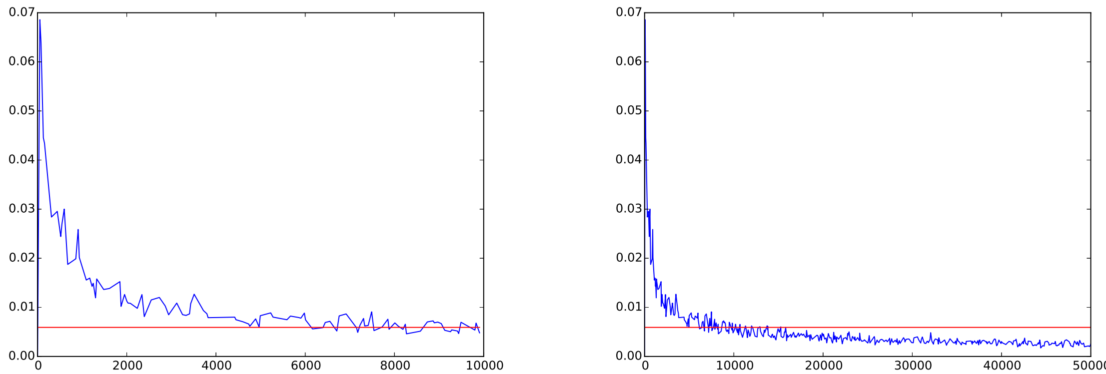
Note that the upper bound given in Theorem 4 is significantly less than what one gets by using the Ramsey number $R_m(3)$, which is at least exponential in m.

Corollary 5. *There is no 13-color multiplicative-coset Ramsey algebra constructible over $\mathbb{Z}/p\mathbb{Z}$ for any prime p. Hence A263308(13) = 0.*

Proof. Let $m = 13$. Then by Theorem 4, $p < 28561$. We have verified that no such prime yields a 13-color multiplicative-coset Ramsey algebra. □

Note that using the upper bound on $R_{13}(3)$ from [9] would have required checking primes up through $1.69 \cdot 10^{10}$.

In Figure 3 below, one can see the maximum modulus of the nontrivial Fourier coefficients of the characteristic function of X_0 over candidate primes p for $m = 13$.



(a) (b)

Figure 3: Normalized maximum modulus of nontrivial Fourier coefficients of $Ch(X_0)$. The red line is $y = 1/\delta^2 = 1/169$.

5 Further directions

While there has been significant computational progress on this problem in the last few years, computation will never get us a proof that Ramsey algebras are constructable for all sufficiently large m. We hope that the ideas in the proof of Theorem 4 are a significant step in this direction. We now collect some open problems whose resolution would contribute to such a proof.

Problem 1. Prove that for all m, there is a prime $p \equiv 1 \pmod{2m}$ between $2m^2$ and m^3.

Problem 2. For certain primes p significantly smaller than m^4, X_0 is not sum-free. Find conditions on p and m that suffice for X_0 to be sum-free.

Problem 3. Improve the Ramsey-like upper bound in Theorem 4. For example, it would seem reasonable to think that one could do better than $1/\sqrt{p}$-uniformity, which holds for *all* subgroups, by taking into account that, for large m, the X_0's are large relative to p.

6 Acknowledgments

I wish to thank Jacob Manske and David Andrews for many useful conversations; Andy Ylvisaker, who made an important observation concerning the algorithm; Illinois College trustee Del Dunham, whose generous donation allowed me to purchase my new compute-server; and Keenan Mack, whose collaboration and friendship kept me sane this past academic year.

References

[1] Jeremy F. Alm. *A fast algorithm for computing the cycle structure of Comer relation algebras over $\mathbb{Z}/p\mathbb{Z}$*. In preparation.

[2] Jeremy F. Alm. *On sets of first-order formulas axiomatizing representable relation algebras*. 2004. Thesis (M.S.)–Iowa State University. arXiv:1604.08227.

[3] Jeremy F. Alm and Jacob Manske. Sum-free cyclic multi-bases and constructions of Ramsey algebras. *Discrete Appl. Math.*, 180:204–212, 2015.

[4] F. R. K. Chung and R. L. Graham. Quasi-random subsets of Z_n. *J. Combin. Theory Ser. A*, 61(1):64–86, 1992.

[5] S. D. Comer. Color schemes forbidding monochrome triangles. In *Proceedings of the fourteenth Southeastern conference on combinatorics, graph theory and computing (Boca Raton, Fla., 1983)*, volume 39, pages 231–236, 1983.

[6] W. T. Gowers. A new proof of Szemerédi's theorem for arithmetic progressions of length four. *Geom. Funct. Anal.*, 8(3):529–551, 1998.

[7] W. T. Gowers. A new proof of Szemerédi's theorem. *Geom. Funct. Anal.*, 11(3):465–588, 2001.

[8] B. Green. Sum-product phenomena in $\mathbb{F}_p$: a brief introduction, 2009. arXiv:0904.2075.

[9] R. E. Greenwood and A. M. Gleason. Combinatorial relations and chromatic graphs. *Canad. J. Math.*, 7:1–7, 1955.

[10] R. Hirsch and I. Hodkinson. *Relation algebras by games*, volume 147 of *Studies in Logic and the Foundations of Mathematics*. North-Holland Publishing Co., Amsterdam, 2002. With a foreword by Wilfrid Hodges.

[11] Tomasz Kowalski. Representability of Ramsey relation algebras. *Algebra Universalis*, 74(3-4):265–275, 2015.

[12] N. Lyall. Roth's theorem: the Fourier-analytic approach. http://math.uga.edu/ lyall/REU/Roth.pdf.

[13] R. Maddux. *The 16*. Unpublished manuscript.

[14] R. Maddux. Do all the Ramsey algebras exist? Presented at the AMS sectional meeting in Iowa City on March 18, 2011.

[15] R. Maddux. Some varieties containing relation algebras. *Trans. Amer. Math. Soc.*, 272(2):501–526, 1982.

[16] R. Maddux. *Relation algebras*, volume 150 of *Studies in Logic and the Foundations of Mathematics*. Elsevier B. V., Amsterdam, 2006.

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

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

2010 *Mathematics Subject Classification*: Primary 11B13, Secondary 11A07, 03G15, 11-04, 11U10, 11Y55.
Keywords:

(Concerned with sequence A263308.)

Received ; revised . Published in *Journal of Integer Sequences*, .

Return to Journal of Integer Sequences home page.