The Number of Different Maximal Product-Free Subsets of a Group

Keith Neu
Science and Mathematics Division, Angelina College,
3500 South First Street, Lufkin, TX 75904, USA
kneu@angelina.edu

Abstract

Let $\alpha(G)$ represent the maximal size of any product-free subset of a finite abelian group G. It is well known that $\alpha(G) = \frac{|G|}{3}\left(1+\frac{1}{p}\right)$ if $|G|$ is divisible by a prime $p \equiv 2 (\mathrm{mod}\ 3)$ and p is the smallest such prime, $\alpha(G) = \frac{|G|}{3}$ if $|G|$ is not divisible by a prime $p \equiv 2 (\mathrm{mod}\ 3)$ but 3 divides $|G|$, and $\alpha(G) = \frac{|G|}{3}\left(1-\frac{1}{m}\right)$ if $|G|$ is divisible only by primes $\equiv 1 (\mathrm{mod}\ 3)$ and m is the exponent of $|G|$. In this paper we use only basic group theory and number theory to derive exact expressions for the number of *different* maximal product-free subsets of G in the first two cases. The formulas are given in terms of the sizes of the subgroups of G.

Let S be a subset of a finite abelian group G. If the product of every pair of elements in S is not in S, then S is said to be *product-free*. A well-known theorem states that if $|G|$ is divisible by a prime congruent to 2(mod 3), and if p is the smallest such prime, then the largest possible product-free subset of G has order $\frac{|G|(p+1)}{3p}$. If $|G|$ is not divisible by a prime congruent to 2(mod 3) but 3 divides $|G|$, then the largest product-free subset of G has order $\frac{|G|}{3}$. A product-free set of maximum size is called a *maximal* product-free set. (See [2] and [4].) In [3] and [4], Street considered the problem of determining the number of different non-isomorphic maximal product-free subsets in these first two cases, and in [1], Green and Ruzsa counted the total number of arbitrary product-free subsets of finite abelian groups using asymptotic expressions. In this paper we derive exact expressions for the number of different maximal product-free subsets for the above two cases in terms of the subgroups of the group, using only basic number theory. We also prove a few related results. Even though the more general results that follow apply to abelian multiplicative groups, we will prove a few results for $\mathbf{Z}_n$, an additive group, to help us with the more general proofs.

Case 1. First we assume there exists a $p \equiv 2 (\mathrm{mod}\ 3)$ such that p divides $|G|$.

Lemma 1.1 Let p be a prime satisfying $p \equiv 2(\text{mod } 3)$. If p is odd, then there are exactly $\frac{p-1}{2}$ different maximal sum-free subsets in $\mathbf{Z}_p$. If $p = 2$, then there is exactly one.

Proof. Let $p \equiv 2(\text{mod } 3)$, and assume p is odd. (If p is even, then there are only two elements in the group, and so $\{1\}$ is the only maximal sum-free subset.) Then $p = 3k - 1$ for some k, and $\{k, k+1, k+2, \cdots, 2k-1\}$ is a maximal sum-free subset of $\mathbf{Z}_p$. By [4], any maximal sum-free subset in $\mathbf{Z}_p$ is in arithmetic progression and so we can write $S = \{a + id | i = 0, 1, 2, \cdots, k-1\}$ for integers a and d. We claim that $S = \{d(k+i) | i = 0, 1, \cdots, k-1\}$. It suffices to show $a = kd$. First let i, j be integers satisfying $0 \leq i, j \leq k-1$. Then $-2k + 2 \leq j - 2i \leq k - 1$. Since $-2k + 2 \equiv k + 1$ and $k - 1 \equiv 4k - 2$, the only value that $j - 2i$ does not take (mod p) is k. Now consider the congruence $dx \equiv a(\text{mod} p)$. We know there exists a solution since $(d, p) = 1$. Let s be the solution and assume $s \neq k$. Then from the preceeding remarks we know there exist i, j satisfying $s = j - 2i$ and $0 \leq i, j \leq k-1$, so $d(j - 2i) \equiv a(\text{mod } p)$ which implies $(a + id) + (a + id) \equiv a + jd(\text{mod } p)$. This contradicts that S is sum-free. Thus $a \equiv kd(\text{mod } p)$ and so $S = \{d(k+i) | i = 0, 1, 2, \cdots, k-1\}$.

Now let $S_d = \{d(k+i) | i = 0, 1, 2, \cdots, k-1\}$, where $d \in D := \{1, 2, ..., \frac{p-1}{2}\}$. We claim that if $d_1 \neq d_2$, then $S_{d_1} \neq S_{d_2}$. Assume not. Then we have $\prod_{i=0}^{k-1} d_1(k+i) \equiv \prod_{i=0}^{k-1} d_2(k+i)(\text{mod } p)$ which implies $d_1^k \equiv d_2^k(\text{mod } p)$ and so $d_1^{(p+1)/3} \equiv d_2^{(p+1)/3}(\text{mod } p)$ which implies $d_1^{p+1} \equiv d_2^{p+1}(\text{mod } p)$ or $d_1^2 \equiv d_2^2(\text{mod } p)$ by Fermat's Theorem. But this means $d_1 + d_2 \equiv 0(\text{mod } p)$, since $d_1 \neq d_2$ by assumption. This is a contradiction because $d_1, d_2 \in D \Rightarrow 2 \leq d_1 + d_2 \leq 2\left(\frac{p-1}{2}\right) = p - 1$.

Thus we have proven that there are at least $\frac{p-1}{2}$ different sum-free subsets of $\mathbf{Z}_p$. To show there are no more, it is enough to show for any $d \in \mathbf{Z}_p$, $S_d = S_{-d}$. This is true because $S_{-d} = \{-d(k+i) | i = 0, 1, 2, \cdots, k-1\} = \{d(2k-1-i) | i = 0, 1, 2, \cdots, k-1\} = \{d(k+i) | i = 0, 1, 2, \cdots, k-1\} = S_d$. This completes the proof. □

The following lemma will be used to prove the more general result.

Lemma 1.2 Let G be a finite abelian group divisible by a prime congruent to 2(mod 3); let p be the smallest such prime. Let $S = \bigcup_{i=1}^{m} a_i H$ be a maximal product-free subset of G, where $m = \frac{p+1}{3}$ and H is a subgroup of G of order $\frac{|G|}{p}$. Then if $x \in G \setminus H$, $< x >$ contains exactly $\frac{p+1}{3p}|x|$ elements of S, where $|x|$ is the order of x. *Proof.* We first note that by [4], S can be written in the form given above. Since $x \in G \setminus H$, xH generates G/H. Also, we know that p divides $|x|$ because if not, then $x^{|x|}H \neq H$, which implies that $x^{|x|} \notin H$. Now, let $E = \{a | x^a H \in S/H, 0 < a < p\}$ and let $R = \{x^{np+a} | n = 0, 1, 2, \cdots, \frac{|x|}{p} - 1; a \in E\}$. Clearly R contains exactly $\frac{|x|}{p}|E|$ different elements, and clearly $|E| = \frac{p+1}{3}$

because $|E|$ is the number of cosets of S/H. To complete the proof, we have to show that $R \subset S$. Let $x^{np+a} \in R$. Then $x^{np+a} \in x^{np+a}H = ((x^n)^p H)(x^a H) = H(x^a H) = x^a H \in S/H$, since $a \in E$. □

We now use Lemma 1 and Lemma 2 to prove the general theorem.

Theorem 1.3 Let G be described as above. If N is the number of subgroups of order $\frac{|G|}{p}$, then there are exactly $\frac{p-1}{2}N$ different maximal product-free subsets of G if p is odd, and N if $p = 2$.

Proof. If $p = 2$ then the result is obvious, so assume p is odd. We first note that if $S = \bigcup_{i=1}^{m} x^{a_i}H$, then the set of integers $\{a_i\}$ is sum-free (mod p). (If not, then there exist a_1, a_2, and a_3 such that $a_1 + a_2 = a_3 (\text{mod } p)$ which implies $x^{a_1+a_2}H = x^{a_3}H$ and so $(x^{a_1}H)(x^{a_2}H) = x^{a_3}H$. This is a contradiction since S is product-free.) But by Lemma 1 we know there are exactly $\frac{p-1}{2}$ different maximal sum-free subsets of $\mathbf{Z}_p$ and each one will generate a different S for a fixed x and a fixed subgroup H of size $\frac{|G|}{p}$. To complete the proof we only need show that $H_1 \neq H_2 \Rightarrow S_1 \neq S_2$, where $S_1 = \bigcup_{i=1}^{m} x^{a_i}H_1$ and $S_2 = \bigcup_{i=1}^{m} y^{b_i}H_2$. Let $z \in H_1/H_2$. By Lemma 2, $< z > \subset H_1$ contains exactly $\frac{p+1}{3p} < z >$ elements of S_2. But $H_1 \bigcap S_1 = \emptyset$ since S_1 is product-free. We conclude that $S_1 \neq S_2$. □

Corollary 1.4 If $p|n$ for some $p \equiv 2 (\text{mod } 3)$, then $\mathbf{Z}_n$ contains exactly $\frac{p-1}{2}$ maximal sum-free subsets if p is odd, and one if $p = 2$.

Proof. $\mathbf{Z}_n$ contains only one subgroup of order n/p.

We will now use the fact that the sum of all of the elements of a maximal sum-free subset of $\mathbf{Z}_p$ is $\equiv 0 (\text{mod } p)$ if p is odd, to prove that the product of all the elements of a maximal product-free subset in this first case is the identity in G.

Theorem 1.5 Let G be described as above and let P be a maximal product-free subset of G. If the smallest prime congruent to 2(mod 3) dividing $|G|$ is odd, then $\prod_{t \in P} t = e$, where e is the identity of G. If $p = 2$, then $\prod_{t \in P} t^2 = e$.

Proof. First assume p is odd and let $S = \bigcup_{i=1}^{m} x^{a_i}H$, $H' = \{h \in H | h \neq h^{-1}\}$, and $H'' = \{h \in H | h = h^{-1}\}$ so that $H = H' \biguplus H''$. Clearly, $\prod_{h \in H'} h = e$. Also, $H'' = \emptyset$ since there is no element in G of order 2. Therefore, we have

$$\begin{aligned}
\prod_{t \in P} t &= \left(\prod_{h \in H} x^{a_1} h\right)\left(\prod_{h \in H} x^{a_2} h\right) \cdots \left(\prod_{h \in H} x^{a_{\frac{p+1}{3}}} h\right) \\
&= x^{|H| \sum a_i} \left(\prod_{h \in H} h\right)\left(\prod_{h \in H} h\right) \cdots \left(\prod_{h \in H} h\right), \\
&= x^{|H| \sum a_i}
\end{aligned}$$

$$
\begin{aligned}
&= x^{|H|\sum_{i=1}^{\frac{p+1}{3}} a_i} \\
&= x^{d|H|\frac{p+1}{6}p} \\
&= x^{|G|d\frac{p+1}{6}} \\
&= e.
\end{aligned}
$$

If $p = 2$ the proof is similar except that H might contain elements of order 2. Squaring each $t \in P$ will allow us to use $\prod_{h \in H''} h^2 = e$. We also need to cancel a 2 out of the exponent of x near the end of the proof. □

Case 2. We now move on to the case where $|G|$ is not divisible by a prime congruent to 2(mod 3) but 3 divides $|G|$. We will try to extend the above results to this second case.

Lemma 2.1 Let k be an integer not divisible by a prime congruent to 2(mod 3). Then the number of maximal sum-free subsets in arithmetic progression in $\mathbf{Z}_{3k}$ is $\phi(3k) + 2$, where ϕ represents the totient function.

Proof. Let S be a maximal sum-free subset so that $S = \{a+id | i = 0, 1, 2, \cdots, k-1\}$ for some $a, d \in \mathbf{Z}_{3k}$. Consider $dx \equiv a (\text{mod } 3k)$. In order for a solution to exist, we must have $(3k, d)|a$. Cleary $(3k, d) > 3$ is impossible because then $|S| < \frac{|G|}{3}$. If $(3k, d) = 3$, then $d = 3t$ for some $(t, 3k) = 1$. This implies that S is a coset of the subgroup $\{3i | i = 0, 1, 2, \cdots, k-1\}$. The two cosets are $\{1 + 3i | i = 0, 1, 2, \cdots, k-1\}$ and $\{2 + 3i | i = 0, 1, 2, \cdots, k-1\}$ and clearly each one is sum-free and maximal. Hence we have two so far. Now consider when $(3k, d) = 1$. In this case the congruence $dx \equiv a (\text{mod } 3k)$ certainly has a solution. As in the proof of Lemma 1.1, let i, j satisfy $0 \leq i, j \leq k-1$ so that $-2k + 2 \leq j - 2i \leq k - 1$, or $k + 2 \leq j - 2i + 3k \leq 4k - 1$. This suggests that $j - 2i$ can take on all values (mod $3k$) except k and $k+1$. If $x \neq k$ or if $x \neq k+1$ then it can be shown (as before) that S is not sum-free. Also, it is easy to verify that $\{d(k+1+i) | i = 0, 1, 2, \cdots, k-1\} = \{-d(k+i) | i = 0, 1, 2, \cdots, k-1\}$. This suggests that $S = \{d(k+i) | i = 0, 1, 2, \cdots, k-1\}$ for some d, $(3k, d) = 1$. Since $\{k+i | i = 0, 1, 2, \cdots, k-1\}$ is clearly sum-free and maximal, to finish the proof we need to show that $\{d_1(k+i) | i = 0, 1, 2, \cdots, k-1\} = \{d_2(k+i) | i = 0, 1, 2, \cdots, k-1\}$ implies $d_1 = d_2$ for any pair d_1, d_2 satisfying $(3k, d_1) = (3k, d_2) = 1$. It is enough to show that $\{d(k+i) | i = 0, 1, 2, \cdots, k-1\} = \{k+i | i = 0, 1, 2, \cdots, k-1\}$ implies that $d \equiv 1 (\text{mod } p)$. To do this, again assume $0 \leq i, j \leq k-1$ so that $2k \leq (k+i) + (k+j) \leq 4k - 2$. This suggests that the sum of any two elements in $\{k+i\}$ is never congruent to $k-1$, as well as any member of the set $\{k+i\}$. Now consider the congruence $dx \equiv k - 1 (\text{mod } 3k)$. Since $(3k, d) = 1$, this congruence has a solution. Clearly, $x \neq k + i, i = 0, 1, 2, \cdots, k-1$, since $\{d(k+i)\} = \{k+i\}$. But $(k+i)+(k+j)$ takes on all values outside $\{k+i\}$ except $k-1$, so if $x \neq k-1$, then $d((k+i)+(k+j)) \equiv k - 1 (\text{mod } 3k)$, which implies $d(k+i) + d(k+j) \equiv k - 1 (\text{mod } 3k)$ and so $(k+i') + (k+j') \equiv k - 1 (\text{mod } 3k)$

for some $0 \leq i, j, i', j' \leq k-1$. This is impossible because the sum of any two elements in $\{k+i\}$ is never $k-1$. Thus it must be that $x \equiv k-1 (\text{mod } 3k)$ so that $d(k-1) \equiv k-1 (\text{mod } 3k)$ which implies $d(k-1) \equiv k-1 (\text{mod } k)$ and so $d \equiv 1 (\text{mod } k)$. If $d \equiv 2 (\text{mod } 3)$, then $dk \equiv 2k (\text{mod } 3k)$, so $2k \in \{d(k+i)\} = \{k+i\}$, a contradiction. Thus $d \equiv 1 (\text{mod } 3)$ and the lemma is proven. □

We now go to the general case.

Theorem 2.2 Let G be described as above. For each divisor d of $\frac{|G|}{3}$, let $N(d)$ be the number of subgroups H of G of order d, such that G/H is cyclic. Then the number of different maximal product-free subsets of G is $\sum_{d|\frac{|G|}{3}} N(d)\phi\left(\frac{|G|}{d}\right)$, where ϕ is the totient function.

Proof. By [4], any maximal product-free subset S is a union of cosets of some subgroup H satisfying $|H| = \frac{|G|}{3m}$ for some m, where G/H is cyclic and S/H is in arithmetic progression. Furthermore, any subgroup H satisfying $|H| = d$, $d|\frac{|G|}{3}$ and G/H cyclic will generate $\phi(3k)+2$ different maximal product-free subsets of G, where $k = \frac{|G|}{3d}$. This is because G/H cyclic $\Rightarrow G/H = \bigcup_{i=0}^{3k-1} x^i H$ for some $x \notin H$. Clearly then $\mathbf{Z}_{3k}$ is isomorphic to G/H and using Lemma 2.1 gives us the $\phi(3k)+2$.

Hence every subgroup H described above will generate maximal product-free subsets and all of the maximal product-free subsets will be counted this way, but we need to make sure we do not count any twice. First observe that for any H described above, the two maximal product-free subsets generated by the cosets of $\{3i|i = 0, 1, 2, \cdots, k-1\}$ in $\mathbf{Z}_{3k}$ are already counted by a subgroup of order $\frac{|G|}{3}$. To see why, let $G/H = \bigcup_{i=0}^{3k-1} x^i H$ and $S_1/H = \bigcup_{i=0}^{k-1} x^{3i+1} H$. If $\pi : G \to G/H$ is the canonical homomorphism, then clearly $S_1 = \pi^{-1}(S_1/H)$ is a maximal sum-free subset generated by a coset of $\{3i|i = 0, 1, 2, \cdots, k-1\}$. But $S_1 = \{x^{3i+1}h | h \in H, 0 \leq i \leq k-1\} = x\{x^{3i}h | h \in H, 0 \leq i \leq k-1\}$, and since $\{x^{3i}h | h \in H, 0 \leq i \leq k-1\}$ is a subgroup of G of order $\frac{|G|}{3}$, S_1 is a coset of this subgroup. We can make a similar argument about the subset generated by the other coset of $\{3i|i = 0, 1, 2, \cdots, k-1\}$. So for each H described above, it is enough to consider only the maximal product-free subsets of the form $S = \pi^{-1}(S/H)$, where $S/H = \bigcup_{i=0}^{k-1} x^{t(k+i)} H$ and $(3k, t) = 1$. To finish the proof we must show that if H_1 and H_2 are two subgroups satisfying the above conditions, where $|H_1| = d_1, |H_2| = d_2, k_1 = \frac{|G|}{3d_1}$ and $k_2 = \frac{|G|}{3d_2}$, then $S_1 = S_2 \Rightarrow H_1 = H_2$, where $S_1/H_1 = \bigcup_{i=0}^{k_1-1} x_1^{t_1(k_1+i)} H_1, (3k_1, t_1) = 1$, and $S_2/H_2 = \bigcup_{j=0}^{k_2-1} x_2^{t_2(k_2+j)} H_2, (3k_2, t_2) = 1$. We know from the proof of Lemma 2.1 that $\{(k+i)+(k+j)|i = 0, 1, 2, \cdots, k-1\}$ contains all elements outside $\{k+i|i = 0, 1, 2, \cdots, k-1\}$ except $k-1$. This means in general that the set $\overline{SS} \setminus S$ consists of elements only from the coset $x^{t(k-1)}H$. Since $S_1 = S_2$, $\overline{S_1 S_1} \setminus S_1 = \overline{S_2 S_2} \setminus S_2$, which implies $x_1^{t_1(k_1-1)} H_1 = x_2^{t_2(k_2-1)} H_2$ and so $H_1 =$

$x_1^{-t_1(k_1-1)}x_2^{t_2(k_2-1)}H_2$. Since H_1 is a subgroup, so is $x_1^{-t_1(k_1-1)}x_2^{t_2(k_2-1)}H_2$, meaning $x_1^{-t_1(k_1-1)}x_2^{t_2(k_2-1)} \in H_2$, which implies $H_1 = H_2$. □

Corollary 2.3 If no prime congruent to 2(mod 3) divides n but $3|n$, then $\mathbf{Z}_n$ contains exactly $\sum_{d|\frac{n}{3}} \phi\left(\frac{n}{d}\right)$ different maximal sum-free subsets.

Proof. For every divisor of $\frac{n}{3}$, there exists one subgroup of that order and since $\mathbf{Z}_n$ is cyclic, so are all the quotient groups.

For completeness, we now state a lemma similar to Lemma 1.2 but for groups of the second type.

Lemma 2.4 Let G be a group described as in Case 2 and let $S = \pi^{-1}(S/H)$ be a maximal product-free subset of G, where $S/H = \bigcup_{i=1}^{m} a_i H$. If $x \in G \setminus H$, then $< x >$ contains exactly $\frac{|x|}{3}$ elements of S, where $|x|$ is the order of x.

Proof. First observe that G/H is cyclic and so xH generates G/H. Set $E = \{a|x^a H \in S/H, 0 < a < 3m\}$ and $R = \{x^{n(3m)+a}|n = 0, 1, 2, \cdots, \frac{|x|}{3m} - 1; a \in E\}$; the proof is similar to the proof of Lemma 1.2.

We now extend Theorem 1.5 to Case 2.

Theorem 2.5 Let G be a group whose order is divisible by 3 but not by any primes congruent to 2(mod 3), and let P be a maximal product-free subset of G. Then $\prod_{t \in P} t^3 = e$, where e is the identity in G.

Proof. The proof is similar to the proof of Theorem 1.5 except that $\sum_{i=0}^{k-1} d(k+i) = \frac{k}{2}(3k-1)$ means we need an extra factor of 3 to make the exponent of x a multiple of $3k$.

We should mention that some of the above results for $\mathbf{Z}_n$ can also be proven using a theorem in [4] (Lemma 6.11), which says that if $G = \mathbf{Z}_m$, $(d, m) = 1$, and $1 \leq s \leq m-3$, then $\{a + id|i = 0, 1, \cdots, s\} = \{b + ie|i = 0, 1, \cdots, s\} \Rightarrow d \equiv \pm e (\text{mod } m)$.

References

[1] B. Green and I. Z. Ruzsa, Sum-free sets in abelian groups. *Israel J. Math.* 247(2005), 157-188.

[2] K. S. Kedlaya, Product-free subsets of groups. *Amer. Math. Monthly* 105 (1998), no. 10, 900-906.

[3] A. P. Street, Counting non-isomorphic sum-free sets, in *Proceedings of the First Australian Conference on Combinatorial Mathematics (Univ. Newcas-*

tle, Newcastle, 1972), 141–143, Univ. of Newcastle Res. Associates, Newcastle.

[4] W. D. Wallis, A. P. Street and J. S. Wallis, *Combinatorics: Room squares, sum-free sets, Hadamard matrices*, Lecture Notes in Math., 292, Springer, Berlin, 1972.