#A4 INTEGERS 17 (2017)

A SHORT NOTE ON REDUCED RESIDUES

Pascal Stumpf
Department of Mathematics, University of Würzburg, Germany
littlefriend@mathlino.org

Received: 11/25/14, Revised: 5/31/16, Accepted: 1/26/17, Published: 2/13/17

Abstract

We answer a question due to Bernardo Recamán about the lower bound behavior of the maximum possible length among arithmetic progressions in the least reduced residue system modulo n, as $n \to \infty$. We also provide an upper bound.

1. Introduction

For any positive integer $n > 1$, let

$$\mathcal{A}(n) = \{a \in \mathbf{Z} : 0 < a < n, \, \gcd(a, n) = 1\}$$

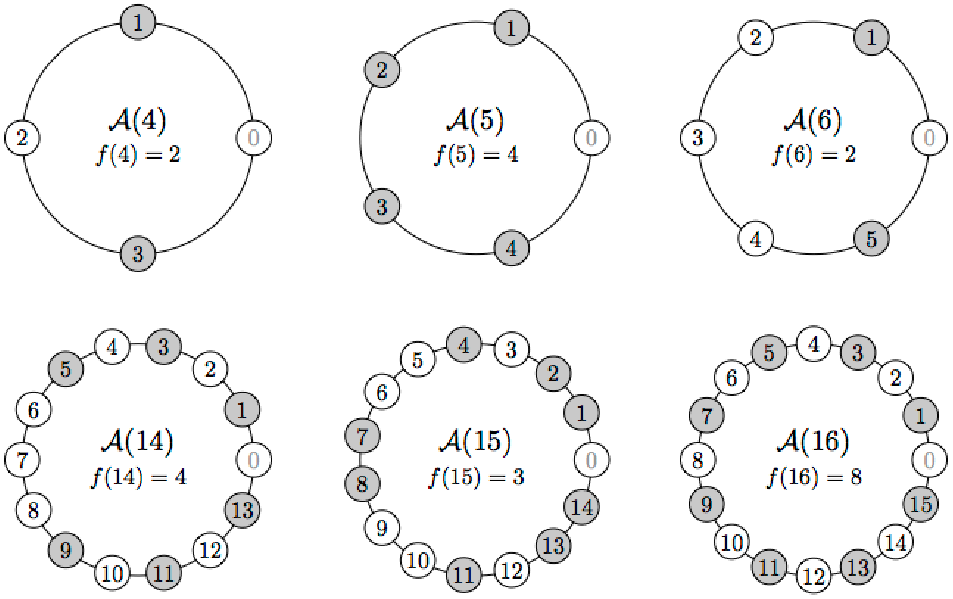
be the (nonempty) set of all smaller positive integers relatively prime to n, or in other words the least reduced residue system modulo n, and let us define $f(n)$ as the maximum possible length among all arithmetic progressions in $\mathcal{A}(n)$.

In a letter from 1995 (see Chapter B40 of [1]) Bernardo Recamán asked if $f(n)$ tends to infinity with n, i.e., if for each $k \in \mathbf{Z}^+$ there exists a constant n_k such that $\mathcal{A}(n)$ contains an arithmetic progression of length k for all $n \geqslant n_k$.

One very nice but deep result coming to mind here is that of Green and Tao [2] telling us about arbitrarily long arithmetic progressions in the primes, and in fact it is a promising indicator for a positive answer to our question, since $\mathcal{A}(n)$ contains all primes less than n except its prime factors. However, it turns out that we can prove the truth of our conjecture by using only elementary methods, and in what follows we present one such solution.

2. Ideas and Proof

Before we start collecting some lower bounds for $f(n)$, let us quickly consider a few examples of $\mathcal{A}(n)$ and $f(n)$ as illustrated in the following figures:



Lemma 1. *For $n > 1$, we have $f(n) \geqslant \max\{(p-1)/2, n/P\}$, where p is the largest prime factor of n and P is the squarefree product of all prime factors of n.*

Proof. According to the prime factorization of n, we build up our proof by working through all of the following possible cases.

First, let us suppose n is prime itself; then exactly all smaller positive integers from 1 up to $n-1$ are relatively prime to n and form an arithmetic progression of length $n-1$ with common difference 1, which means $f(n) = n-1$.

In the more general case $n = p^r$, where p is prime and $r \in \mathbf{Z}^+$, we similarly still have $\{1, \ldots, p-1\} \subset \mathcal{A}(n)$ and so $f(n) \geqslant p-1$. But if $r \geqslant 2$ we can also look at the numbers $1 + m \cdot p$ for $0 \leqslant m < p^{r-1}$. All of them lie in $\mathcal{A}(n)$ since none of them is divisible by p, and they form an arithmetic progression of length p^{r-1} with common difference p, giving us even $f(n) \geqslant p^{r-1} = n/p$ here.

Next, let us consider squarefree numbers $n = p_1 p_2 \ldots p_d$, where $d \geqslant 2$ and $2 \leqslant p_1 < p_2 < \ldots < p_d$ (odd) are prime. Like before, a good idea seems to be looking at numbers of the form $1 + m \cdot q$, now choosing $q = p_1 p_2 \ldots p_{d-1}$ and $0 \leqslant m < p_d$, which ensures us that

$$a_m = 1 + m \cdot q \leqslant 1 + (p_d - 1) \cdot q = 1 + n - q \leqslant 1 + n - 2 < n$$

is already not divisible by any of the primes $p_1, p_2, \ldots, p_{d-1}$, although we are not sure about non-divisibility by p_d yet. However, together $a_0, a_1, \ldots, a_{p_d - 1}$ represent a complete residue system modulo p_d, because if $a_x \equiv a_y \pmod{p_d}$ for some $0 \leqslant x < y < p_d$, then $0 \equiv a_y - a_x = (y-x) \cdot q \pmod{p_d}$ together with $\gcd(q, p_d) = 1$ would imply $y - x \equiv 0 \pmod{p_d}$, or equivalently, $x \equiv y \pmod{p_d}$, in contradiction to our range for x and y. In particular, exactly one member of $a_0, a_1, \ldots, a_{p_d-1}$ is divisible by p_d, say a_m, and so by the box principle we know that

$$a_0, \ldots, a_{m-1} \quad \text{or} \quad a_{m+1}, \ldots, a_{p_d-1}$$

is an arithmetic progression of length at least $(p_d-1)/2$ with common difference q completely contained inside $\mathcal{A}(n)$, which delivers $f(n) \geqslant (p_d-1)/2$.

Finally, let us introduce exponents $r_1, r_2, \ldots, r_d \in \mathbf{Z}^+$ such that we can cover all remaining numbers $n = p_1^{r_1} p_2^{r_2} \ldots p_d^{r_d}$, where $r_1 + r_2 + \ldots + r_d > d$. Because n has the same prime factors as $p_1 p_2 \ldots p_d$, we find $\mathcal{A}(p_1 p_2 \ldots p_d)$ builds a subset of

$$\{a + m \cdot p_1 p_2 \ldots p_d : a \in \mathcal{A}(p_1 p_2 \ldots p_d), 0 \leqslant m < p_1^{r_1-1} p_2^{r_2-1} \ldots p_d^{r_d-1}\} = \mathcal{A}(n).$$

In fact, we have $\gcd(a, n) = 1$ if and only if $\gcd(a, p_1 p_2 \ldots p_d) = 1$, for all integers a, and hence $f(n) \geqslant f(p_1 p_2 \ldots p_d) \geqslant (p_d - 1)/2$. On the other hand, we might again do a bit better by looking at the numbers $1 + m \cdot p_1 p_2 \ldots p_d$ forming an arithmetic progression of length $p_1^{r_1-1} p_2^{r_2-1} \ldots p_d^{r_d-1}$ with common difference $p_1 p_2 \ldots p_d$, and combining both ideas leads us to $f(n) \geqslant \max\{(p_d-1)/2, n/(p_1 p_2 \ldots p_d)\}$. □

Theorem 1. *For each $k \in \mathbf{Z}^+$, there exists a constant n_k such that $\mathcal{A}(n)$ contains an arithmetic progression of length k for all $n \geqslant n_k$.*

Proof. Let P_{2k} be the product of all primes not exceeding $2k$ and put $n_k = k \cdot P_{2k} \geqslant 1 \cdot 2$. Moreover, let us fix some $n \geqslant n_k$, and (as in Lemma 1) denote its largest prime factor by p. If $p \geqslant 2k+1$, we immediately arrive at

$$(p-1)/2 \geqslant ((2k+1)-1)/2 = k.$$

In the other case $p < 2k+1$, we note that all prime factors of n do not exceed $2k$, implying their product P divides P_{2k}, and so in particular

$$n/P \geqslant n_k/P = k \cdot P_{2k}/P \geqslant k \cdot 1.$$

Combining everything we reach $f(n) \geqslant \max\{(p-1)/2, n/P\} \geqslant k$, and our claim follows. □

So far we mainly worked on lower bounds for $f(n)$. As a last step, let us change our point of view and conclude by showing:

Theorem 2. *For $n > 1$, we also have $f(n) \leqslant \max\{(p-1)/1, n/P\}$.*

Proof. Suppose $a_1, a_2, \ldots, a_s$ is an arithmetic progression of length s with common difference q contained in $\mathcal{A}(n)$. Now let us focus a bit more on q.

If $q \geqslant P$, we can only come up to $s \leqslant n/P$, since otherwise $s > n/P$ implies

$$a_s = a_1 + (s-1) \cdot q \geqslant 1 + ((n/P + 1) - 1) \cdot P = n + 1,$$

and our last member would not be in $\mathcal{A}(n)$ anymore. In the other case $q < P$, we know q is missing at least one prime factor p' of the squarefree number P dividing n. But then $\gcd(q, p') = 1$ once again, like in the proof of Lemma 1, can tell us that, whenever $s \geqslant p'$, the first p' members $a_1, a_2, \ldots, a_{p'}$ do represent a complete residue system modulo p'. Therefore one of them, being a multiple of p', could not lie in $\mathcal{A}(n)$ anymore, leaving us only $s \leqslant p' - 1 \leqslant p - 1$ left here. Uniting both cases we reach $f(n) \leqslant \max\{n/P, p-1\}$, as desired. □

3. Future Work

After having established lower and upper bounds for $f(n)$, especially in the case of squarefree numbers n, an interesting question seems to be whether, on average, $f(n)$ is closer to $(p-1)/2$ or $p-1$. Our examples indicate that it can be very near to both thresholds. Another task is to improve on the given border n_k in our main theorem. For both aims one could hope to get better estimates by using more advanced methods.

Acknowledgements. I would like to thank Miriam and her brother Christian Goldschmied for always encouraging me to write things down and making my first paper possible, and the anonymous referee for very useful comments.

References

[1] R. Guy, *Unsolved Problems in Number Theory*, Springer, 2004.

[2] B. Green and T. Tao, The primes contain arbitrarily long arithmetic progressions, *Annals of Mathematics* (2) **167** (2008), 481-547.