10-2007

Some Open Questions on Modulo Classes

Frank J. Palladino
University of Rhode Island, fpaladino@mail.uri.edu

SOME OPEN QUESTIONS ON MODULO CLASSES

FRANK J. PALLADINO

FACULTY SPONSOR: LUBOS THOMA

Department of Mathematics,
University of Rhode Island,
Kingston, RI 02881-0816, USA
fpalladino@mail.uri.edu

ABSTRACT. Modular arithmetic is a system of arithmetic for integers which most people use on a daily basis. The 24-hour clock is based off of this system. The study of modular arithmetic is a fundamental area of study in number theory. Many of the important theorems concerning modulo classes have been well understood for centuries, however there still remains a number of difficult open questions concerning various properties of modulo classes. Over the course of this project I have focused on several of these conjectures with the intention of producing original work in the field of number theory.

Although I have yet to fully resolve any of the open questions, I have obtained non-trivial results for certain special cases of the general problems. It is my intention to present several of the more prominent techniques I have used throughout the semester. The focus of this study shall be the following conjectures:

Conjecture 1. *Suppose we have k pairwise disjoint modulo classes $a_i \bmod M_i$ $i = 1, \ldots, k$ then there exists M_l, M_j, $1 \leq j < l \leq k$ such that $gcd(M_l, M_j) \geq k$.*

Conjecture 2. *Given $k > 0$ there exists N_k modulo classes $a_i \bmod M_i$ $i = 1, \ldots, N_k$, such that $M_i \geq k$ for $i = 1, \ldots, N_k$, and these N_k modulo classes cover the integers.*

During the course of this project Conjecture 1 has been established for small finite cases, namely for $k \leq 7$. Furthermore the following theorem, a weakening of Conjecture 1, has been established:

Theorem 1. *Suppose we have k pairwise disjoint modulo classes $a_i \bmod M_i$ $i = 1, \ldots, k$ then there exists M_l, M_j, $1 \leq j < l \leq k$ such that $gcd(M_l, M_j) \geq \sqrt{k}$.*

My goal here is to present an explicit proof for each of the 7 special cases of Conjecture 1 which have been established over the course of this project. With this goal in mind I will first present several techniques which allowed these special cases to be resolved. Once the 7 special cases have been addressed I will present a proof of Theorem 1.

Keywords: congruence class.
AMS Subject Classification: 11A07

1. Introduction

The study of modular arithmetic is a fundamental area of study in number theory. Many of the important theorems concerning modulo classes have been well understood for centuries, however there still remains a number of difficult open questions concerning various properties of modulo classes.

Definition 1. *Given integers a, b, M with $M > 0$. We say that a is congruent to b modulo M, and we write*

$$a \equiv b(modM)\,, \tag{1}$$

if M divides the difference $a - b$. The number M is called the modulus of the congruence. The congruence class $a \bmod M$ is the set of integers C so that

$$a \equiv b(modM)\,, \tag{2}$$

for all $b \in C$.

In this paper I study several conjectures relating to modulo classes. I present this report as a summary of my year-long work and to document my partial findings in support of the general conjectures. The main goal of this work is to demonstrate my insights into the general conjectures and to present relevant background information. In this way I hope to inspire interest regarding these open problems in the mind of the reader. The conjectures studied are the following.

Conjecture 1. *Suppose we have k pairwise disjoint modulo classes $a_i \bmod M_i$ $i = 1, \ldots, k$ then there exists M_l, M_j, $1 \leq j < l \leq k$ such that $gcd(M_l, M_j) \geq k$.*

Conjecture 2. *Given $k > 0$ there exists N_k modulo classes $a_i \bmod M_i$ $i = 1, \ldots, N_k$, such that $M_i \geq k$ for $i = 1, \ldots, N_k$, and these N_k modulo classes cover the integers.*

In this paper I will include a proof of Conjecture 1 for $k \leq 7$. Also a proof of the following theorem, a weakening of Conjecture 1, will be presented.

Theorem 1. *Suppose we have k pairwise disjoint modulo classes $a_i \bmod M_i$ $i = 1, \ldots, k$ then there exists M_l, M_j, $1 \leq j < l \leq k$ such that $gcd(M_l, M_j) \geq \sqrt{k}$.*

It should be noted that these problems are highly non-trivial. In [3] Paul Erdős offers \$ 500.00 for proof or disproof of Conjecture 2. Conjecture 1 is proposed by Sun, cf. [2].

2. Preliminary Observations

Before we attempt to prove the main results of the paper, we will introduce a number of preliminary observations which help to simplify the results presented in the following sections. First we shall present the Chinese remainder theorem. This theorem is a standard textbook result, and shall play an important role in the following obeservations.

Theorem 2. *The Chinese remainder theorem: Assume $m_1, \ldots, m_r$ are positive integers, relatively prime in pairs:*

$$gcd(m_i, m_k) = 1; i \neq k. \tag{3}$$

Let $b_1, \ldots, b_r$ be arbitrary integers. Then the system of congruences

$$x \equiv b_1 \bmod m_1$$
$$\vdots$$
$$x \equiv b_r \bmod m_r \tag{4}$$

has exactly one solution modulo the product $m_1 \ldots m_r$.

Proof. Let $M = m_1 \ldots m_r$ and let $M_k = M/m_k$. Then $gcd(M_k, m_k) = 1$ so each M_k has a unique reciprocal M'_k modulo m_k. Now let

$$x = b_1 M_1 M'_1 + b_2 M_2 M'_2 + \cdots + b_r M_r M'_r. \tag{5}$$

Consider each term in this sum modulo m_k. Since $M_i \equiv 0 \bmod m_k$ if $i \neq k$ we have

$$x \equiv b_k M_k M'_k \equiv b_k \bmod m_k. \tag{6}$$

Hence x satisfies every congruence in the system. But it is easy to show that the system has only one solution mod M. In fact, if x and y are two solutions of the system we have $x \equiv y \bmod m_k$ for each k and, since the m_k are relatively prime in pairs, we also have $x \equiv y \bmod M$. This completes the proof. □

The first observation we shall discuss follows directly from the Chinese remainder theorem.

Observation 1. *Suppose the modulo classes $a_i \bmod M_i$ and $a_j \bmod M_j$ are disjoint, then $gcd(M_i, M_j) \geq 2$.*

Proof. Suppose $gcd(M_i, M_j) < 2$, then $gcd(M_i, M_j) = 1$. Thus M_i and M_j are relatively prime. By the Chinese remainder theorem the system of congruences has exactly one solution modulo the product $M_i M_j$. Thus the modulo classes are not disjoint, however this contradicts our original assumption. □

Notice that by Observation 1 the special case k=2 of Conjecture 1 is established. The following generalization of Observation 1 becomes a vital tool in verifying the further cases of Conjecture 1.

Observation 2. *The modulo classes $a_i \bmod M_i$ and $a_j \bmod M_j$ are not disjoint if and only if $a_i \equiv a_j \bmod gcd(M_i, M_j)$.*

Proof. The modulo classes $a_i \bmod M_i$ and $a_j \bmod M_j$ are not disjoint if and only if there exist integers N_1, N_2 so that $a_i + N_1 M_i = a_j + N_2 M_j$. Which happens if and only if there exist integers N_1, N_2 so that $a_i + \frac{N_1 M_i}{gcd(M_i, M_j)} gcd(M_i, M_j) = a_j + \frac{N_2 M_j}{gcd(M_i, M_j)} gcd(M_i, M_j)$. This is true if and only if there exist integers N_1, N_2 so that $\frac{a_i - a_j}{gcd(M_i, M_j)} = \frac{N_2 M_j - N_1 M_i}{gcd(M_i, M_j)}$. Now we know from the properties of the greatest common divisor, or more specifically from Theorem 1.2 in [1], that $gcd(M_i, M_j) | (N_2 M_j - N_1 M_i)$ this is true if and only if $gcd(M_i, M_j) | (a_i - a_j)$. Thus $a_i \bmod M_i$ and $a_j \bmod M_j$ are not disjoint if and only if $a_i \equiv a_j \bmod gcd(M_i, M_j)$. □

The next two observations follow quickly from the definition of the greatest common divisor, however as they are needed for the proof of Observation 5, which is essential to our study I will state them here.

Observation 3. *Let S be a finite set of natural numbers, and let P(S) be a permutation of S. Then gcd(S)=gcd(P(S)).*

Proof. Obvious from the definition of the greatest common divisor. □

Observation 4. *Let A,B,C be finite sets of natural numbers where $A = B \cup C$, then gcd(A)=gcd(gcd(B),gcd(C)).*

Proof. By the definition of gcd(A), $gcd(A)|gcd(B)$, and $gcd(A)|gcd(C)$, thus $gcd(A)|gcd(gcd(B), gcd(C))$. By definition $gcd(gcd(B), gcd(C))|gcd(B)$, and $gcd(gcd(B), gcd(C))|gcd(C)$. Thus $gcd(gcd(B), gcd(C))|x$ for $x \in B$ and $gcd(gcd(B), gcd(C))|y$ for $y \in C$. Thus for $z \in B \cup C = A$, $gcd(gcd(B), gcd(C))|z$. Therefore $gcd(gcd(B), gcd(C))|gcd(A)$, thus gcd(A)=gcd(gcd(B),gcd(C)). □

Now I will present Observation 5. This observation is useful when attempting a proof by contradiction for sufficiently small special cases of Conjecture 1.

Observation 5. *Suppose we have k pairwise disjoint modulo classes $a_i \bmod M_i$ $i = 1, \ldots, k$ such that for every pair M_l, M_j, $1 \leq j < l \leq k$ $gcd(M_l, M_j) \leq 6$, then $gcd(M_1, \ldots, M_k) \geq 2$.*

Proof. From Observation 1 since the modulo classes are pairwise disjoint we have that for every pair M_l, M_j, $1 \leq j < l \leq k$, $gcd(M_l, M_j) \geq 2$. Suppose there exists $1 \leq j < d < i < l \leq k$ such that $gcd(M_i, M_j, M_l, M_d) = 1$, then by Observations 3 and 4 along with our assumptions, the integers $gcd(M_i, M_j)$,$gcd(M_i, M_d)$,$gcd(M_k, M_j)$,$gcd(M_d, M_k)$,$gcd(M_d, M_j)$, and $gcd(M_i, M_k)$ must all be in the range $2 \leq n \leq 6$ and must be pairwise relatively prime. However this is impossible since there are only 3 primes in this region. Thus for every foursome M_l, M_j, M_i, M_d, $1 \leq j < d < i < l \leq k$, $gcd(M_l, M_j, M_i, M_d) \geq 2$. Now suppose $gcd(M_{j_1}, M_{j_2}, \ldots, M_{j_{L-2}}) \geq 2$, and there exists $1 \leq j_1 < j_2 < \cdots < j_L \leq k$ such that $gcd(M_{j_1}, M_{j_2}, \ldots, M_{j_L}) = 1$, then by Observations 3 and 4 along with our assumptions, the integers $gcd(M_{j_L}, M_{j_{L-1}})$,$gcd(M_{j_L}, M_{j_{L-2}})$,$gcd(M_{j_{L-1}}, M_{j_{L-2}})$, $gcd(M_{j_L}, gcd(M_{j_1}, M_{j_2}, \ldots, M_{j_{L-3}}))$, $gcd(M_{j_{L-1}}, gcd(M_{j_1}, M_{j_2}, \ldots, M_{j_{L-3}}))$, and $gcd(M_{j_{L-2}}, gcd(M_{j_1}, M_{j_2}, \ldots, M_{j_{L-3}}))$ must all be in the range $2 \leq n \leq 6$ and must be pairwise relatively prime. However this is impossible since there are only 3 primes in this interval. Thus by induction for every set $M_{j_1}, M_{j_2}, \ldots, M_{j_L}$, $gcd(M_{j_1}, M_{j_2}, \ldots, M_{j_L}) \geq 2$, thus $gcd(M_1, \ldots, M_k) \geq 2$. □

This concludes the preliminary observations required.

3. Special Cases

Here I will present the explicit proof for each of the special cases of Conjecture 1 where $k \leq 7$.

Special Case k = 1. *Suppose we have a modulo class $a_1 \bmod M_1$ then $gcd(M_1) \geq 1$.*

Proof. Obvious. □

Special Case k = 2. *Suppose the modulo classes* $a_1 \bmod M_1$ *and* $a_2 \bmod M_2$ *are disjoint, then* $gcd(M_1, M_2) \geq 2$.

Proof. Suppose $gcd(M_1, M_2) < 2$, then $gcd(M_1, M_2) = 1$. Thus M_1 and M_2 are relatively prime. By the Chinese remainder theorem the system of congruences has exactly one solution modulo the product $M_1 M_2$. Thus the modulo classes are not disjoint, however this contradicts our original assumption. □

Special Case k = 3. *Suppose we have 3 pairwise disjoint modulo classes* $a_i \bmod M_i$ $i = 1, \ldots, 3$ *then there exists* M_l, M_j, $1 \leq j < l \leq 3$ *such that* $gcd(M_l, M_j) \geq 3$.

Proof. Suppose not, then we have 3 pairwise disjoint modulo classes $a_i \bmod M_i$ $i = 1, \ldots, 3$ such that for every pair M_l, M_j, $1 \leq j < l \leq 3$ $gcd(M_l, M_j) \leq 2$. Also by Observation 1, we have 3 pairwise disjoint modulo classes $a_i \bmod M_i$ $i = 1, \ldots, 3$ such that for every pair M_l, M_j, $1 \leq j < l \leq 3$ $gcd(M_l, M_j) \geq 2$. Thus we have 3 pairwise disjoint modulo classes $a_i \bmod M_i$ $i = 1, \ldots, 3$ such that for every pair M_l, M_j, $1 \leq j < l \leq 3$ $gcd(M_l, M_j) = 2$. This means that by the pidgeon hole principle there exists a_l, a_j, $1 \leq j < l \leq 3$ such that $a_l \equiv a_j \bmod gcd(M_l, M_j)$. Thus by Observation 2 the 3 modulo classes in question are not pairwise disjoint, however this contradicts our original assumptions. □

Special Case k = 4. *Suppose we have 4 pairwise disjoint modulo classes* $a_i \bmod M_i$ $i = 1, \ldots, 4$ *then there exists* M_l, M_j, $1 \leq j < l \leq 4$ *such that* $gcd(M_l, M_j) \geq 4$.

Proof. Suppose not, then we have 4 pairwise disjoint modulo classes $a_i \bmod M_i$ $i = 1, \ldots, 4$ such that for every pair M_l, M_j, $1 \leq j < l \leq 4$ $gcd(M_l, M_j) \leq 3$. By Observation 5, $gcd(M_1, M_2, M_3, M_4) \geq 2$, thus either 2 or 3 divides M_i $i = 1, \ldots, 4$.
Suppose 3 divides M_i $i = 1, \ldots, 4$, then for every pair M_l, M_j, $1 \leq j < l \leq 4$ $gcd(M_l, M_j) = 3$. This means that by the pidgeon hole principle there exists a_l, a_j, $1 \leq j < l \leq 4$ such that $a_l \equiv a_j \bmod gcd(M_l, M_j)$. Thus by Observation 2 the 4 modulo classes in question are not pairwise disjoint, however this contradicts our original assumptions.
Suppose 2 divides M_i $i = 1, \ldots, 4$, then for every pair M_l, M_j, $1 \leq j < l \leq 4$ $gcd(M_l, M_j) = 2$. This means that by the pidgeon hole principle there exists a_l, a_j, $1 \leq j < l \leq 4$ such that $a_l \equiv a_j \bmod gcd(M_l, M_j)$. Thus by Observation 2 the 4 modulo classes in question are not pairwise disjoint, however this contradicts our original assumptions.
Thus in either case we arrive at a contradiction. □

Special Case k = 5. *Suppose we have 5 pairwise disjoint modulo classes* $a_i \bmod M_i$ $i = 1, \ldots, 5$ *then there exists* M_l, M_j, $1 \leq j < l \leq 5$ *such that* $gcd(M_l, M_j) \geq 5$.

Proof. Suppose not, then we have 5 pairwise disjoint modulo classes $a_i \bmod M_i$ $i = 1, \ldots, 5$ such that for every pair M_l, M_j, $1 \leq j < l \leq 5$ $gcd(M_l, M_j) \leq 4$. By Observation 5, $gcd(M_1, M_2, M_3, M_4, M_5) \geq 2$, thus either 2 or 3 divides M_i $i = 1, \ldots, 5$.
Suppose 3 divides M_i $i = 1, \ldots, 5$, then for every pair M_l, M_j, $1 \leq j < l \leq 5$

$gcd(M_l, M_j) = 3$. This means that by the pidgeon hole principle there exists a_l, a_j, $1 \leq j < l \leq 5$ such that $a_l \equiv a_j \bmod gcd(M_l, M_j)$. Thus by Observation 2 the 5 modulo classes in question are not pairwise disjoint, however this contradicts our original assumptions.
Suppose 2 divides M_i $i = 1, \ldots, 5$, then for every pair M_l, M_j, $1 \leq j < l \leq 5$ $gcd(M_l, M_j)|4$. This means that by the pidgeon hole principle there exists a_l, a_j, $1 \leq j < l \leq 5$ such that $a_l \equiv a_j \bmod gcd(M_l, M_j)$. Thus by Observation 2 the 5 modulo classes in question are not pairwise disjoint, however this contradicts our original assumptions. Thus in either case we arrive at a contradiction. □

Special Case k = 6. *Suppose we have 6 pairwise disjoint modulo classes* $a_i \bmod M_i$ $i = 1, \ldots, 6$ *then there exists* M_l, M_j, $1 \leq j < l \leq 6$ *such that* $gcd(M_l, M_j) \geq 6$.

Proof. Suppose not, then we have 6 pairwise disjoint modulo classes $a_i \bmod M_i$ $i = 1, \ldots, 6$ such that for every pair M_l, M_j, $1 \leq j < l \leq 6$ $gcd(M_l, M_j) \leq 5$. By Observation 5, $gcd(M_1, M_2, M_3, M_4, M_5, M_6) \geq 2$, thus either 2, 3, or 5 divides M_i $i = 1, \ldots, 6$.
Suppose 3 divides M_i $i = 1, \ldots, 6$, then for every pair M_l, M_j, $1 \leq j < l \leq 6$ $gcd(M_l, M_j) = 3$. This means that by the pidgeon hole principle there exists a_l, a_j, $1 \leq j < l \leq 6$ such that $a_l \equiv a_j \bmod gcd(M_l, M_j)$. Thus by Observation 2 the 6 modulo classes in question are not pairwise disjoint, however this contradicts our original assumptions.
Suppose 2 divides M_i $i = 1, \ldots, 6$, then for every pair M_l, M_j, $1 \leq j < l \leq 6$ $gcd(M_l, M_j)|4$. This means that by the pidgeon hole principle there exists a_l, a_j, $1 \leq j < l \leq 6$ such that $a_l \equiv a_j \bmod gcd(M_l, M_j)$. Thus by Observation 2 the 6 modulo classes in question are not pairwise disjoint, however this contradicts our original assumptions.
Suppose 5 divides M_i $i = 1, \ldots, 6$, then for every pair M_l, M_j, $1 \leq j < l \leq 6$ $gcd(M_l, M_j) = 5$. This means that by the pidgeon hole principle there exists a_l, a_j, $1 \leq j < l \leq 6$ such that $a_l \equiv a_j \bmod gcd(M_l, M_j)$. Thus by Observation 2 the 6 modulo classes in question are not pairwise disjoint, however this contradicts our original assumptions.
Thus in any of the three cases we arrive at a contradiction. □

Special Case k = 7. *Suppose we have 7 pairwise disjoint modulo classes* $a_i \bmod M_i$ $i = 1, \ldots, 7$ *then there exists* M_l, M_j, $1 \leq j < l \leq 7$ *such that* $gcd(M_l, M_j) \geq 7$.

Proof. Suppose not, then we have 7 pairwise disjoint modulo classes $a_i \bmod M_i$ $i = 1, \ldots, 7$ such that for every pair M_l, M_j, $1 \leq j < l \leq 7$ $gcd(M_l, M_j) \leq 6$. By Observation 5, $gcd(M_1, M_2, M_3, M_4, M_5, M_6, M_7) \geq 2$, thus either 2, 3, or 5 divides M_i $i = 1, \ldots, 7$.
Suppose 5 divides M_i $i = 1, \ldots, 7$, then for every pair M_l, M_j, $1 \leq j < l \leq 7$ $gcd(M_l, M_j) = 5$. This means that by the pidgeon hole principle there exists a_l, a_j, $1 \leq j < l \leq 7$ such that $a_l \equiv a_j \bmod gcd(M_l, M_j)$. Thus by Observation 2 the 7 modulo classes in question are not pairwise disjoint, however this contradicts our original assumptions.
Suppose 3 divides M_i $i = 1, \ldots, 7$, then for every pair M_l, M_j, $1 \leq j < l \leq 7$ $gcd(M_l, M_j)|6$. This means that by the pidgeon hole principle there exists a_l, a_j, $1 \leq j <$

$l \leq 7$ such that $a_l \equiv a_j \bmod gcd(M_l, M_j)$. Thus by Observation 2 the 7 modulo classes in question are not pairwise disjoint, however this contradicts our original assumptions. Suppose 2 divides M_i $i = 1, \ldots, 7$, then we can partition the set M_i $i = 1, \ldots, 7$ in the following way.
$M_i \in A$ if and only if $2|M_i$, but 4 does not divide M_i, and 6 does not divide M_i; $M_i \in B$ if and only if $4|M_i$, but 6 does not divide M_i; $M_i \in C$ if and only if 4 does not divide M_i, and $6|M_i$; and $M_i \in D$ if and only if $12|M_i$.
Notice that taking arbitrary $x \in A$, $y \in B$, and $z \in C$ then $gcd(x, y) = 2$, $gcd(x, z) = 2$, and $gcd(y, z) = 2$, thus the cardinality of $A \cup B \cup C$ is no greater than 3 lest we have a contradiction. Thus the cardinality of D is greater than or equal to 4. However this contradicts our original assumptions.
Hence we arrive at a contradiction in all cases. □

Thus Conjecture 1 has been established for $k \leq 7$.

4. A Weaker Result

Here I will present a proof of Theorem 1, which is similar to Conjecture 1, however rather than proving $gcd(M_l, M_j) \geq k$ we will prove that $gcd(M_l, M_j) \geq \sqrt{k}$.

Theorem 1. *Suppose we have k pairwise disjoint modulo classes* $a_i \bmod M_i$ $i = 1, \ldots, k$ *then there exists* M_l, M_j, $1 \leq j < l \leq k$ *such that* $gcd(M_l, M_j) \geq \sqrt{k}$.

Proof. Suppose not, then we have k pairwise disjoint modulo classes $a_i \bmod M_i$ $i = 1, \ldots, k$ such that for every pair M_l, M_j, $1 \leq j < l \leq k$ $gcd(M_l, M_j) < \sqrt{k}$. Since there are at most $k - 1$ possible distinct modulo classes whose modulus is less than $\sqrt{k}$. We have that by the pidgeon hole principle there exists a_l, a_j, $1 \leq j < l \leq k$ such that $a_l \equiv a_j \bmod gcd(M_l, M_j)$. Thus by Observation 2 the k modulo classes in question are not pairwise disjoint, however this contradicts our original assumptions. Thus the theorem is proved. □

5. Conclusion

To conclude, the field of number theory is a field of mathematics with many rich, diverse, and difficult open problems. These preliminary results barely scratch the surface of what remains to be known regarding modulo classes. I believe that these problems are of paramount importance, and that this area requires further study.

References

[1] T. Apostol, Introduction to Analytic Number Theory. 1976 Springer-Verlag New York, Inc.

[2] K. O'Bryant, On Z-W Sun's Disjoint Congruence Classes Conjecture, *arXiv.math.NT/0604347* .

[3] P. Erdős, Some problems in number theory, in *Computers in Number Theory, Academic Press*, 1971, 405-414; esp. pp. 408-409.