Multiplicative Number Theory

A. Project summary of Kevin Ford's Proposal

This proposal concerns the continuation of three recent projects of the proposer. The first involves extending a famous conjecture of R. L. Graham on the maximum of $a/\gcd(a,b)$ over a, b lying in a finite set of integers. In turn this problem has an application to a combinatorial problem on configurations of intersecting arithmetic progressions, on which the proposer has made substantial recent progress. The second project deals with questions in "comparative prime number theory", the theory of subtle inequities in the distribution of prime numbers in residue classes. The third investigation is an extension of the proposers work on the distribution of "shifted primes" (sets $\{p+a : p \text{ prime}\}$ for fixed $a \neq 0$) and related questions concerning arithmetic functions such as Euler's function $\phi(n)$ and the sum of divisors function $\sigma(n)$.

Section C — Text of the Proposal

C.1. Graham's problem and related questions

In 1970, R. L. Graham [G] made the conjecture that for any set of n positive integers, there are two of them, say a and b, such that $a/(a,b) \geq n$. Here (a,b) means the greatest common divisor of a and b. Graham's conjecture was proved for all large n independently by Zaharescu [Z] and Szegedy [Sz] in the mid-1980s. Introducing several new ideas, and making use of explicit bounds for prime number counting functions, Balasubramanian and Soundararajan [BS] recently proved the conjecture for all n.

For a set $A = \{a_1, \ldots, a_n\}$ of positive integers, let $G(A)$ be the maximum over all i, j of $\frac{a_i}{(a_i, a_j)}$. Define $A^* = \{L/a_1, \ldots, L/a_n\}$, where $L = \mathrm{lcm}[a_1, \ldots, a_n]$. In addition to conjecturing that $G(A) \geq n$ for every set A of n integers, Graham made the stronger conjecture (also proved in [BS] for all n) that if $G(A) = n$ and $n > 4$, then either A or A^* is equal to $\{1, 2, \ldots, n\}$. Balasubramanian and Soundararajan claim that their method could be used to prove an even stronger statement, but gave no details. The gist of the claim is that if A is a set of M positive integers and $G(A) = N$ with N "not too much larger" than M, then either A or A^* lies in $\{1, 2, \ldots, N\}$. To quantify the claim, let $f(N)$ denote the largest number R so that the following holds:

> For every set A of M positive integers with $N - R \leq M \leq N$ and $G(A) \leq N$, either A or A^* lies in $\{1, 2, \ldots, N\}$.

In [BS, p. 3] is the claim that the method yields $f(N) \geq \dfrac{cN}{\log N \log\log N}$ for some $c > 0$, but this appears to be too optimistic.

Problem 1. Develop upper and lower bounds for $f(N)$.

The proposer has already made appropriate generalizations of key lemmas in [BS], and this leads to the lower bound

$$f(N) \geq \frac{cN}{(\log\log N)^{1/2}(\log N)^2} \tag{1}$$

for large N (with an explicit value for c). This is as yet unpublished, and will form the nucleus for the development of further bounds. Work to be done includes developing good explicit lower bounds for $f(N)$ for "small" N (say $N < e^{10000}$), because of an application to a problem of intersecting arithmetic progressions (Problem 2 below). The proposer already has some improvements to lemmas in [BS], which should lead to good explicit bounds and may also lead to order of magnitude improvements over (1).

A simple construction leads to the upper bound

$$f(N) \ll \frac{N}{\log\log N}.$$

The idea is to take A to be $\{1 \leq m \leq H : (m,H) > 1\} \cup \{2H\}$ where H is the product of many small primes. The proposer will investigate more complex constructions, using ideas from [BS], to develop better upper bounds for $f(N)$. It would also be of some interest to determine the true order of magnitude of $f(N)$, even heuristically.

The proposer's work on Problem 1 was motivated by a problem in combinatorial number theory (which in turn was motivated by work of R. Howard, G. Karolyi and L. Szekeley [HKS] on the Erdős-Ko-Rado intersection theorems [EKR]). For integers $t \geq 3$ and $k \geq 2$, let $N_t(k)$ denote the maximum number of k-term arithmetic progressions (APs) of real numbers, in a configuration where any two have t points in common. We call such a configuration of APs *t-intersecting.* Without loss of generality we can assume that the APs consist of integers. The connection to Problem 1 is quite simple: if $\{a, a+d_1, a+2d_1, \ldots, a+(k-1)d_1\}$ and $\{b, b+d_2, \ldots, b+(k-1)d_2\}$ are two APs, their intersection is an AP with elements spaced $d_1/(d_1, d_2)$ apart. Thus, if the two APs have t points in common, then $d_1/(d_1, d_2) \leq \frac{k-1}{t-1}$. A direct application of the Balasubramanian-Soundararajan theorem yields good upper bounds for $N_t(k)$, but still short of the conjectured bounds by a factor of 2 or so. For $t = 2$, the conjectured maximal configuration (modulo translations and dilations) is given by

Example 1. Let C_k be the collection of APs B_{ij} $(1 \leq i < j \leq k)$, whose ith element is 0 and jth element is $k!$.

Recently, the proposer [F4] has shown

Theorem 1. *For prime k and $k \geq 10^{4000}$, the following holds: $N_2(k) = \frac{1}{2}k(k-1)$ and any configuration of $\frac{1}{2}k(k-1)$ k-term 2-intersecting APs is equivalent to C_k.*

The proof for prime k is elementary, but for large non-prime k the proof requires the above mentioned lower bound on $f(N)$ as well as bounds for the gaps between prime numbers (from an explicit version of the Prime Number Theorem, e.g. Theorem 11 of [Sc]). Improvements in the explicit lower bounds for $f(N)$ lead directly to reductions in the 10^{4000}. The proposer also has generalizations of the method to the case $t \geq 3$. These yield non-trivial bounds, but as yet we cannot prove an exact formula for $N_t(k)$, even for large k, for any such t.

Problem 2. Prove the conclusion of Theorem 1 for all k.

Problem 3. Improve the bounds on $N_t(k)$ for $t \geq 3$, with the goal of proving precise values for this function.

For problem 2, the proposer can at this time deduce the conclusion of Theorem 2 in the range $10^{10} \leq k \leq e^{9000}$, provided that in this range there is a prime number in the interval $[k, k + k/(6 \log^3 k)]$ (improved lower bounds for $f(N)$ would weaken this requirement). This is certainly true, but does not follow from bounds in the literature (e.g. Theorem 5.1.1 of [RR]). All known explicit bounds on prime counting functions are based on Rosser-Schoenfeld type arguments, making explicit the classical error term in the Prime Number Theorem and using computations of zeros of the Riemann zeta function $\zeta(s)$. Recently, however, Y. Cheng [Cheng] has proven explicit bounds for $\zeta(s)$ of the Vinogradov-Korobov type (i.e. $|\zeta(1 + it)| \leq c_1 \log^{2/3} t$ with an explicit c_1). This should lead to vastly improved explicit bounds for gaps between primes, but it is unclear if improvements will be made for "small" k $(k \leq 10^{4000})$.

C.2. Comparative Prime Number Theory

Denote by $\pi(x)$ the number of prime numbers $\le x$, and for $q > 2$ and $(a,q) = 1$, let $\pi_{q,a}(x)$ denote the number of primes $\le x$ in the progression $a \pmod q$. Chebyshev [Cheb] observed that there are "more" primes in the progression $3 \mod 4$ than in the progression 1 mod 4 (meaning $\pi_{4,3}(x) \ge \pi_{4,1}(x)$ most of the time). As noted by later authors, for many such triples q, a, b there appears to be a bias in the sign of $\Delta_{q,a,b}(x) := \pi_{q,a}(x) - \pi_{q,b}(x)$. In general, if a is a quadratic non-residue modulo q and b is a quadratic residue, then $\Delta_{q,a,b}(x)$ tends to be more often positive than negative. In some cases, the first sign change is quite large, especially if $q|24$, $b = 1$ and $a \ne 1$. For example, computations by Bays and Hudson ([BH1], [BH2]) have shown that the first sign change in $\Delta_{3,1,2}(x)$ occurs at 608981813029. The biases "against" quadratic residues can be explained analytically via the explicit formulae for $\pi_{q,a}(x)$ in terms of zeros of Dirichlet L-functions (e.g. [RS]), or combinatorially ([H2]). These problems are also closely related to the bias in the sign of $\mathrm{li}(x) - \pi(x)$, where $\mathrm{li}(x) = \text{p.v.} \int_0^x dt/\log t$ is the natural smooth approximation to $\pi(x)$.

On the theoretical side, it is widely believed that for any modulus q and numbers a and b coprime to q, the function $\Delta_{q,a,b}(x)$ changes sign infinitely often. The first such proof was by Littlewood in 1914 [Li] for the cases $q = 3, a = 1, b = 2$ and $q = 4, a = 1, b = 3$, as well as showing that $\mathrm{li}(x) - \pi(x)$ also changes sign infinitely often. An extensive program by Knapowski and Turán in the 1960's ([KT1,KT2]) addressed this question. They established infinitely many sign changes for a wide class of q, a, b, some results of which required the hypothesis that the corresponding L-functions have no real non-trivial zeros (easy to verify for a given modulus q), and some which required that the L-functions have no non-trivial zeros off the critical line up to a certain height T (given as cq^{10} for an unspecified c).

Problem 4. Make explicit the height T required to prove that for a given fixed q, all functions $\Delta_{q,a,b}(x)$ with $(a,q) = (b,q) = 1$ have infinitely many sign changes. Thus reducing the problem for a given q to a finite (and reasonable) computation.

It is also of interest to locate sign changes, or obtain upper bounds on the first sign change. Although Littlewood's proofs provided no particular x for which $\mathrm{li}(x) - \pi(x)$ is negative, Skewes ([Sk1],[Sk2]) in 1955 showed unconditionally that a sign change occurs before $10^{10^{10^{10^3}}}$. A major breakthrough was made in 1966 by R. S. Lehman [Le], who showed that $\mathrm{li}(x) - \pi(x)$ is negative somewhere between 1.53×10^{1165} and 1.65×10^{1165}. His method involved approximating a weighted average of $\mathrm{li}(x) - \pi(x)$ and using the computed values of the first 12,000 zeros of the Riemann zeta function $\zeta(s)$ lying above the real axis. The upper bound has since been lowered twice ([tR], [BH3]) using Lehman's theorem together with more extensive computations of the zeros of $\zeta(s)$.

Problem 5. Locate sign changes of $\pi_{q,a}(x) - \pi_{q,b}(x)$ for large x.

In joint work with R. Hudson [FH], the proposer has successfully generalized Lehman's method to obtain a method of locating sign changes of any $\Delta_{q,a,b}(x)$, provided that sufficiently many small zeros of the corresponding L-functions are known. The zeros ρ with $|\Im\rho| \le 10000$ for many small q have been computed by R. Rumely [Ru], and with these we have shown

Theorem 2. For each $b \in \{3,5,7\}$, $\pi_{8,b}(x) < \pi_{8,1}(x)$ for some $x < 10^{24}$. For each $b \in \{5,7,11\}$, $\pi_{12,b}(x) < \pi_{12,1}(x)$ for some $x < 10^{429}$. For each $b \in \{5,7,11,13,17,19,23\}$, $\pi_{24,b}(x) < \pi_{24,1}(x)$ for some $x < 10^{353}$.

In addition to computed zeros of L-functions, extending Lehman's result to primes in progressions required explicit bounds for the number of zeros to height T given by McCurley [M], plus a small trick to deal with the possibility that an L-function has a very small zero (the smallest zero of $\zeta(s)$ has imaginary part about 14.137). The explicit bounds and tools used to prove Theorem 2 have direct application to Problem 4.

Some of the sign changes indicated by Theorem 2 actually occur in the interval $[10^{15}, 10^{20}]$. In this range it is impractical to search for sign changes by computer using a sieve (e.g. [BH1]), but it is practical using a variant of Meissel's formula given by Hudson [H1]. Together with appropriate modifications of the algorithm of Lagarias, Miller and Odlyzko [LMO] for computing $\pi(x)$, this gives an algorithm for exactly computing $\pi_{q,a}(x)$ with a running time of about $O(x^{2/3})$. The proposer has already written such a program for the special case $q = 8$, in order to test the ideas. One preliminary new discovery is of a specific value of x (near 2×10^{14}) where $\Delta_{8,7,1}(x) < 0$.

Problem 6. Extend the program to compute $\pi_{q,a}(x)$ for any q, a.

In addition to comparing counts of primes in pairs of arithmetic progressions modulo q, one can compare any $m \le \phi(q)$ progressions and ask whether all $m!$ possible orderings occur (or occur for arbitrarily large x). The origin of this type of problem was an observation of Shanks [Sh] that $\pi_{8,1}(x) \le \pi_{8,a}(x)$ ($a = 3,5,7$) for $x < 10^6$. Shanks asked whether $\pi_{8,1}(x)$ is ever the largest of the four functions. Note that 1 is the only quadratic residue modulo 8.

Only recently have any theoretical results been given for the comparison of three or more progressions. Kaczorowski [K1] showed that, assuming the Extended Riemann Hypothesis (ERH) for the Dirichlet L-functions modulo q (all non-trivial zeros have real part $\frac{1}{2}$), that indeed $\pi_{q,1}(x)$ is larger than all the other $\pi_{q,b}(x)$ ($(b,q) = 1$) for a positive proportion of x, and likewise $\pi_{q,1}(x)$ runs behind all the others for a positive proportion of x. In [K2] and [K3] he extends this to other (but not all) orderings.

Based on computations with zeros of L-functions similar to those needed for Theorem 2, it appears that in fact $\pi_{8,1}(x)$ does run ahead of the other three functions $\pi_{8,a}(x)$ for x in the vicinity of e^{383}, but we cannot prove this yet.

Problem 7. Combine the methods of Kaczorowski and Ford-Hudson [FH] to develop a way of showing that a particular ordering of three or more of the functions $\pi_{q,a}(x)$ occurs in the vicinity of a particular (large) x.

Recently, the proposer and S. Konyagin have investigated the necessity of the assumption of the ERH in deducing a particular ordering of functions $\pi_{q,a}(x)$ occurs for arbitrarily large x. We believe that assuming the ERH is absolutely necessary.

Problem 8. Show that for any q and any triple of numbers a, b, c coprime to q, one can deduce that at least one of the orderings of the functions $\pi_{q,a}(x)$, $\pi_{q,b}(x)$, $\pi_{q,c}(x)$ does not occur for large x if the associated L-functions have a certain finite collection of zeros off the critical line.

We have already established this for many many q, a, b, c. Moreover, the set of exceptional zeros can all be taken to be as close to the critical line as desired (i.e. we can take all the exception zeros to have real part $< \frac{1}{2} + \delta$ for any $\delta > 0$). We plan to pursue this further, with the goal of completely solving Problem 8.

Under the assumptions of the Extended Riemann Hypothesis (ERH) and the hypothesis that all the imaginary parts of the zeros of L-functions for the modulus q (those with positive imaginary part) are linearly independent over $\mathbb{Q}$, Rubinstein and Sarnak [RS] have shown that the set of values x for which a certain ordering of the functions $\pi_{q,a_i}(x)$ $(1 \le i \le k)$ occurs has a logarithmic density, and this provides numerical values for the biases [RS, p. 188]. They show that this bias is always positive, and give a method of computing it. For example, the logarithmic density of the set of x giving $\pi(x) - \mathrm{li}(x) < 0$ is about 0.99999973.

For more than two progressions, the procedure becomes quite complex, although G. Martin and A. Feuerverger at the University of Toronto have succeeded in the cases $q = 8, a_1 = 3, a_2 = 5, a_3 = 7$ and $q = 12, a_1 = 5, a_2 = 7, a_3 = 11$. Bays and Hudson have developed a less rigorous, but easier to implement, method of approximating the densities by using a truncated version of explicit formulas for $\pi_{q,a}(x)$.

Using this method, the proposer has computed biases for the six orderings for triples of progressions of quadratic non-residues modulo $q = 8$, $q = 12$ and $q = 24$. In every case there is a significant deviation from 1/6 for the six bias numbers, although the bias when comparing any two of the progressions is exactly $\frac{1}{2}$. While combinatorial arguments can explain the bias against quadratic residues, we as yet do not have a combinatorial explanation (one not using the specific values of zeros of L-functions) to explain this. It is a genuinely new phenomenon, and more work is necessary to understand it.

Problem 9. Gather more data on the biases for triples of progressions, and try to find combinatorial explanations for the deviation from non-biased behavior.

C.3. The distribution of shifted primes and values of arithmetic functions

For fixed nonzero integer a, let P_a denote the set of numbers of the form $p+a$ where p is prime. These are often referred to as sets of "shifted primes". Determining the structure of the sets P_a has been the subject of numerous investigations. In particular, there is a close connection between properties of P_a and properties of certain multiplicative functions, such as Euler's function $\phi(n)$ ($\phi(p) = p - 1$ for primes p) and the sum of divisors function $\sigma(n)$ ($\sigma(p) = p + 1$ for primes p). The structure of P_{-1} also plays a crucial role in the recent proof that there are infinitely many Carmichael numbers [AGP], and in the work by Gupta and Murty [GM] and Heath-Brown [H-B] on Artin's primitive root conjecture.

Let $P_a(x) = P_a \cap [1, x]$. It is expected that in a multiplicative setting, the sets $P_a(x)$ should behave very much like a "random" set of $\pi(x)$ integers $\le x$, where $\pi(x)$ is the number of primes $\le x$. This heuristic of course has limits, for example P_a will have at most one number in each residue class $-a \pmod{p}$ for each prime p. But for many arithmetic functions, such as P^+ (the largest prime factor function), the distribution of $P^+(p+a)$ should correspond roughly to the distribution of $P^+(n)$ over all $n \le x$. Current knowledge for this particular function is scant. For instance, Baker and Harman [BHa] have proved that $P^+(p+a) \gg p^{0.677}$ for infinitely many p, and that $P^+(p+a) \ll p^{0.2961}$ for infinitely many p. These statements are expected to be true with exponents $1-\varepsilon$ and ε, respectively, where $\varepsilon > 0$ is arbitrary.

Denote by $\Omega(n)$ the number of prime factors of n counted with multiplicity (e.g. $\Omega(4) = 2$). It is fairly easy to show by sieve methods (e.g. [E1], [F1,§2]) that the distribution of $\Omega(p+a)$ corresponds to the distributions of $\Omega(n)$ over $n \le x$. This and stronger forms are one key in bounding $R_a(x)$, the number of positive integers $\le x$ which can be written as a product of numbers in P_a. Such bounds in turn provide bounds on $V_f(x)$, the number of values taken by $f(n)$ that are $\le x$, for various multiplicative functions f such as ϕ and σ. Several authors, including Erdős [E1] and recently Maier and Pomerance [MP], have developed bounds for $V_\phi(x)$ (and the methods work to give identical bounds for $R_a(x)$). Still, a sizeable gap remained between upper and lower bounds. Recently, the proposer proved ([F1, Theorems 1,14])

Theorem 3. *For two positive constants c_1 and c_2, depending only on a, we have $c_1 \le R_a(x)/Z(x) \le c_2$, where*

$$Z(x) = \frac{x}{\log x} \exp\{C(\log_3 x - \log_4 x)^2 + D\log_3 x - (D + 1/2 - 2C)\log_4 x\}.$$

Here $C = 0.817\ldots$ and $D = 2.176\ldots$ are specific constants and $\log_k x$ is the kth iterate of the logarithm. Furthermore, for a large class $\mathcal{F}$ of multiplicative functions f with $f(p) = p + a$ for primes p and $f(p^b)$ "not too small" for $b \ge 2$, we have $c_3 \le V_f(x)/Z(x) \le c_4$ for positive constants c_3, c_4 which depend only on f.

The second part holds in particular for $f = \phi$ and $f = \sigma$.

Problem 10. Determine the limit of $R_a(x)/Z(x)$, or at least bound it between two "reasonable" constants.

A line of inquiry closely related to that of bounding $V_f(x)$ is to study the function $A_f(m)$, the number of solutions of $f(x) = m$, also called the "multiplicity" of m. Using the same methods used to determine the order of $R_a(x)$, the proposer has shown [F1,Theorems 2 and 14] that

Theorem 4. *For $f \in \mathcal{F}$ and for each $k \ge 1$, the number of $m \le x$ for which $A_f(m) = k$ is either identically zero or is $\ge c_5 V_f(x)$, where c_5 depends only on f and k.*

Erdős [E2] had previously shown that for each $k \ge 1$, $A_\phi(m) = k$ either has no solutions or infinitely many solutions. Another result from [F1] is that the multiplicity of "most" f-values is bounded, specifically for $N \ge 1$,

$$\frac{|\{m \le x : A_f(m) \ge N\}|}{V_f(x)} \ll N^{-1} \exp\{O(\sqrt{\log N})\}.$$

It is natural to ask what multiplicities are possible for a given f. Carmichael's famous conjecture [C1,C2] states that for $f = \phi$ the multiplicity 1 is not possible. This remains open, although large lower bounds on a possible counterexample are easy to obtain, the latest being $10^{10^{10}}$ [F1,Theorem 6]. There is no analog of Carmichael's Conjecture for $f = \sigma$, since $A_\sigma(1) = 1$.

In the 1950's, Sierpiński conjectured that for $f = \phi$ and $f = \sigma$ that all multiplicities $k \ge 2$ are possible (see [S1] and [E2]). In 1961, Schinzel [S2] deduced this conjecture from his well-known Hypothesis H [SS], which is a generalization to polynomials of arbitrary degree of Dickson's Prime k-tuples Conjecture [D] (itself a generalization of the Twin Prime Conjecture).

Recently, the proposer has proven the Sierpiński conjecture for $\phi(n)$ [F3] and with S. Konyagin [FK] proved the Sierpiński conjecture for $\sigma(n)$. Despite the similarities of the two functions, neither method was applicable to the other conjecture. These results use the modern theory of "almost primes" (non-primes with few prime factors) from sieve theory, in particular the famous theorem of Chen ([Ch1], [Ch2]). We take a number m satisfying $A_\phi(m) = k$ and constructing a number m' so that $A_\phi(mm') = k + 2$ and the proof depends on the identity $\phi(p^2) = p\phi(p)$. More generally, the method gives

Theorem 5 *Suppose $f \in \mathcal{F}$ and $f(p^2) = pf(p)$ for primes p. If $A_f(m) = k$, then there is a number m' such that $A_f(mm') = k + A_f(1)$.*

The proof of the Sierpiński Conjecture for $\sigma(n)$ uses almost primes in a simpler way, depending on the following easy sieve result (see [HR]):

Theorem *For some positive real number c, some integer $n \ge 2$, and x sufficiently large, there are $\gg x/\log^2 x$ primes $s \in (x/2, x]$ for which $(s+1)/2$ has exactly n prime factors, each exceeding x^c.*

The usual goal of lower bound sieve methods is to show that a certain form represents primes infinitely often, but it is critical to this argument that the numbers $(s+1)/2$ have at least two prime factors. This may be the first application of lower bound sieve results where genuine almost primes are desired and primes are not. The basic idea is to take a number m with $A_\sigma(m) = k$ and construct a multiple of m with $A_\sigma(m'm) = rk$ for any integer r. The proof carries over to other $f \in \mathcal{F}$ as well, but only shows that all multiplicities are possible if multiplicity 1 is.

Theorem 6 *Suppose $f \in \mathcal{F}$. If $A_f(m) = k$ and r is any positive integer, there is an m' such that $A_f(mm') = rk$.*

Problem 11. For what $f \in \mathcal{F}_a$ is there an analog of Carmichael's Conjecture? In other words, for what f is multiplicity 1 impossible.

The values taken by $f(n)$ may be classified in two additional ways. If $A_f(m) = k$ and $f(x_i) = m$ with $x_1 < x_2 < \cdots x_k$, write $G_f(m) = \gcd(x_1, \dots, x_k)$ and let $H_f(m)$ be the k-tuple $(x_2/x_1, x_3/x_1, \dots, x_k/x_1)$ of ratios of the pre-images. In the proof of the lower bound of $V_f(x)$ in [F1, Theorems 2,14], it is proven that if $A_f(m) = k \ge 1$ and $f(x_1) = \cdots = f(x_k) = m$, then for $\gg V_f(x)$ square-free numbers u with $(u, m) = 1$, the pre-images of $f(u)m$ are precisely $ux_1, \dots, ux_k$. One corollary is that for every $k \ge 1$, either $k \nmid G_f(m)$ for all m or $k | G_f(m)$ for $\gg V_f(x)$ values of $m \le x$. A second corollary is that for every k-tuple of rationals $\mathbf{y} = (y_1, y_2, \dots, y_k)$ with $1 < y_1 < \cdots y_k$, either $H_f(m) = \mathbf{y}$ for no m or for $\gg V_f(x)$ values of $m \le x$. For $f = \phi$, a short search reveals examples with $G_\phi(m) = k$ for each $k \le 11$ except $k = 6$ and $k = 10$. It appears that there might not be any value of $\phi(n)$, all of whose pre-images are divisible by 6.

Problem 12. Investigate the possible values of $G_f(m)$ and $H_f(m)$, in particular for $f = \phi$ and $f = \sigma$.

The proposer believes that work on Problem 12 will be necessary for any proof of Carmichael's Conjecture. In particular, any totient with a unique pre-image must have that pre-image divisible by 6, so the non-existence of such numbers implies Carmichael's Conjecture. In fact, all the works [F1], [F2], [FK] were motivated by an attempt to settle this long standing conjecture.