

# On a conjecture concerning non-intersecting congruence classes

Robert Hines

September 7, 2004

Here is the conjecture that is the subject of this paper.

**Conjecture.** *Given  $k$  non-intersecting congruence classes  $a_1 \pmod{q_1}, \dots, a_k \pmod{q_j}$ ,  $\exists i, j$  such that  $(q_i, q_j) \geq k$*

The first step towards proving or disproving this conjecture is discovering what it means for two congruence classes to intersect.

**Theorem 1.** *Two congruence classes,  $a_i \pmod{q_i}$  and  $a_j \pmod{q_j}$  intersect if and only if  $a_i \equiv a_j \pmod{(q_i, q_j)}$*

*Proof.*  $\{a_i + q_i\mathbb{Z}\} \cap \{a_j + q_j\mathbb{Z}\} \neq \emptyset \iff$   
 $a_i + xq_i = a_j + yq_j$  has solutions  $(x, y) \in \mathbb{Z}^2 \iff$   
 $a_i - a_j = (q_i, q_j)(y \frac{q_j}{(q_i, q_j)} - x \frac{q_i}{(q_i, q_j)})$  has solutions  $\iff$   
 $a_i \equiv a_j \pmod{(q_i, q_j)}$  □

The next step is to show that, given  $k$ , the solution can be found with a finite number of calculations. Since the intersection/non-intersection of the congruence classes depends only on the pairwise gcds of the moduli, the moduli of any set of congruence classes can be reduced by removing extraneous factors, i.e. those factors not involved in any pairwise gcd. With the added restriction that every pairwise gcd be less than  $k$ , an upper bound on the set of moduli that need be considered can be established.

**Theorem 2.** *The preceding conjecture is true, given  $k > 1$ , if there exist no non-intersecting congruence classes such that  $\forall q_i, q_i | M, q_i \neq 1, M$ . Here  $M = p_1^{e_1} \dots p_n^{e_n}$  where  $p_1, \dots, p_n$  are the primes less than  $k$  and  $p_i^{e_i} < k \leq p_i^{e_i+1}$ .*

*Proof.* Assume that more than one of the moduli share a prime factor greater than or equal to  $k$ . Then they have a gcd greater than or equal to  $k$ . So only one of the moduli has a prime factor greater than or equal to  $k$ . This factor then does not affect the pairwise gcd's of the system and does not affect whether or not any of them intersect by theorem 1. Now assume that more than one of the moduli is divisible by  $p^a$  such that  $p < k$  and  $p^a \geq k$ . Then there would exist a pairwise gcd greater than or equal to  $k$ . So only one of the moduli

have such a factor. However, only the factor of  $p^b$ , where  $b$  is the next highest power of  $p$  in any of the moduli, affects the pairwise gcds of the moduli, and of course  $p^b < k$ . So each moduli must divide  $M$ . No moduli is equal to one (else that class would necessarily intersect any other class) and none of the moduli can equal  $M$  else there would be a gcd greater than or equal  $k$ . (To see this, let  $l$  be the lcd of the  $q_i$ 's. For each congruence class, there are  $\frac{l}{q_i}$  corresponding classes (mod  $l$ ). Summing over  $i$  we have  $\sum_{i=1}^k \frac{l}{q_i} \leq l$ . Dividing by  $l$ ,  $\sum_{i=1}^k \frac{1}{q_i} \leq 1$ . Now assume that  $q_1 \geq k$  and for all other  $q_i$ ,  $q_i < k$ . Then  $1 \geq \sum_{i=1}^k \frac{1}{q_i} \geq \frac{1}{q_1} + \sum_{i=2}^k \frac{1}{k-1} = \frac{1}{q_1} + \frac{k-1}{k-1} > 1$ , a contradiction. Therefore, at least two of the  $q_i$  must be greater than or equal  $k$ . But if one of the  $q_i = M$  then another moduli must necessarily be greater than or equal  $k$  and there will be a gcd greater than or equal  $k$  since every possible moduli divides  $M$ .)  $\square$

Here is a result that will reduce the number of possible moduli to be considered in the cases of the conjecture to be considered later.

**Theorem 3.** *Let  $\frac{k}{n+1} \leq d < \frac{k}{n}$  such that  $\forall i, d|q_i$ . Then if the conjecture is true for  $n+1$ , the classes intersect.*

*Proof.* Because there are  $k$  objects and only  $d$  classes modulo  $d$ , for at least  $n+1$  of the  $q_i$ ,  $a_i \equiv c \pmod{d}$  for some constant  $c$ . Let  $n+1$  of these classes be denoted by  $c + b_0d \pmod{r_0d}$ ,  $\dots$ ,  $c + b_nd \pmod{r_nd}$ . Assume these classes do not intersect. Then  $\forall i, j$ , with  $i \neq j$ , we have  $c + b_id \not\equiv c + b_jd \pmod{(r_i, r_j)d}$  by theorem 1. This implies that  $(b_i - b_j) \not\equiv m(r_i, r_j) \forall m \in \mathbb{Z}$ . This last statement implies that  $b_i \not\equiv b_j \pmod{(r_i, r_j)}$ . Because  $(r_i, r_j)d < k$ ,  $(r_i, r_j) < \frac{k}{d} \leq n+1$ , the last implication of the previous sentence would imply the existence of a non-intersecting system of  $n+1$  congruences with a maximum gcd less than  $n+1$ . But the conjecture was assumed true for  $n+1$  and so we have a contradiction.  $\square$

This last theorem rules out the possibility of having prime power moduli since if  $q_1 = p^a$ , then  $\forall i, p|q_i$  so that all gcds are  $\geq 1$ . With these tools in hand, we are now ready to prove the conjecture for some small values of  $k$ .

**Theorem 4.** *The conjecture is true for  $k \leq 10$ .*

*Proof.*  $k = 2$ : Since both pairwise gcds must be one, the classes intersect by theorem 1.

$k = 3$ : All pairwise gcds must be two (or one, but we see that causes intersection above). So  $\forall i, 2|q_i$  and the classes intersect by theorem 3.

$k = 4$ : Here,  $M = 2 \cdot 3$  and the possible moduli are 2 and 3. Both of these, however, are ruled out by theorem 3.

$k = 5$ : Here,  $M = 2^2 \cdot 3$  and the possible moduli are 2, 3,  $2^2$ , and 6. But 2, 3, and  $2^2$  are impossible by theorem 3 and 6 can only be used once else there would be a gcd greater than or equal  $k = 5$ . So no  $k$ -tuple of moduli can even be created.

$k = 6$ : In this case,  $M = 2^2 \cdot 3 \cdot 5$  and the possible moduli (ruling out prime powers) are 6, 10, 12, 15, 20, and 30. However, since the gcd of 30 and

every number on the list is greater than or equal  $k = 6$ , 30 is not a candidate. Now we have only five possible moduli, none of which can be repeated without there being a gcd greater than or equal  $k = 6$ . So no  $k$ -tuple can be constructed.

Here I will interject a brief fact. If  $k = n$  and the conjecture is true for  $n - 1$ , then there must be two moduli with factors of  $n - 1$  else there would be a system of  $n - 1$  classes with maximum gcd of less than  $n - 1$ .

$k = 7$ : As in the previous case,  $M = 2^2 \cdot 3 \cdot 5$  and the possible moduli are 6, 10, 12, 15, 20, and 30. Two of the moduli must be divisible by 5, but since 30 has a gcd greater than or equal  $k = 7$  with every other possible moduli that is divisible by 5, it can be dismissed. All of this reduces to two possible  $k$ -tuples: (15, 10 or 20 but not both, 12, 6, 6, 6, 6) and (15, 10 or 20 but not both, 6, 6, 6, 6, 6). Now to show that any system with these moduli will intersect. Because  $(10, 6) = (20, 6) = 2$ , and because any four classes modulo 6 must represent both classes modulo 2, any system with these moduli must intersect by theorem 1.

The proof for  $k = 8$  is much longer than the previous cases but it sets the stage for the proofs of  $k = 9, 10$  since they are all very similar.

$k = 8$ :  $M = 2^2 \cdot 3 \cdot 5 \cdot 7$ . Two of the moduli must be divisible by 7 and not equal to 7 by theorem 3, and at most three (since there are only three other primes dividing  $M$  and if two moduli were divisible by 7 and another prime, they would have a gcd greater than or equal  $k = 8$ ).

Assume three of the moduli are divisible by 7. Then these moduli must be  $(2 \cdot 7, 3 \cdot 7, 5 \cdot 7)$  or  $(2^2 \cdot 7, 3 \cdot 7, 5 \cdot 7)$ . Both of these, however, are impossible since it implies that  $2 \cdot 3 \cdot 5$  divides all of the other possible moduli implying a gcd greater than or equal  $k = 8$ . So there are only two moduli such that  $7|q_i$ .

One of the moduli divisible by 7 must be divisible by 3, because if it were not, every other moduli would have to be divisible by 10 ( $\text{gcd} \geq 8$ ). Also, one of the moduli divisible by 7 must be divisible by 2, because if it were not, every other moduli would have to be divisible by 15 ( $\text{gcd} \geq 8$ ). Finally, neither of the moduli divisible by 7 is divisible by 6, otherwise every other moduli would have to be divisible by 10 or 15 and that would mean that no more than four moduli could be put together without having a  $\text{gcd} \geq k = 8$ .

So we have  $2^{(2)} \cdot 5 \cdot 7, 3 \cdot 7$  and  $2^{(2)} \cdot 7, 3 \cdot 5$  as our possible pairs of moduli that are divisible by 7, where the parentheses around the exponent imply that it is optional (actually that there are more cases, one for 2 and  $2^2$ , but they can be treated together). For the first pair, all other moduli are divisible by either  $3 \cdot 5$  or  $2 \cdot 3$  and for the second pair all other moduli are divisible by either  $2 \cdot 5$  or  $2 \cdot 3$ . In the first case, all but one of the moduli in the system is divisible by 3 and in the second case, all but one is divisible by 2.

These situations are analogous to that of theorem 3. In the first case, there must be three of the seven congruence classes whose moduli are divisible by 3 that are all congruent to  $c \pmod{3}$  for some constant  $c$  and in the second case, there must be four of the seven whose moduli are divisible by 2 that are

congruent to  $d \pmod{2}$  for some constant  $d$ . So by the same reasoning as in theorem 3 and the fact that the conjecture is true for  $k = 3, 4$ , the classes must intersect in both cases.

$k = 9$ :  $M = 2^3 \cdot 3 \cdot 5 \cdot 7$ . Two of the moduli must be divisible by  $2^3$  and at most three since there are only three other prime factors of  $M$  (if they shared a factor other than  $2^3$ , there would be a  $\gcd \geq k = 9$ ) and none of the moduli can be  $2^3$  by theorem 3. If three of the moduli were divisible by  $2^3$  and more than one of the other moduli were not divisible by 2, then  $3 \cdot 5 \cdot 7$  would divide both of them, with  $\gcds \geq k = 9$ . So in that case only one of the moduli is not divisible by 2.

Now assume that exactly two of the moduli are divisible by  $2^3$  so we have the pairs  $(2^3 \cdot 3, 2^3 \cdot 5)$ ,  $(2^3 \cdot 3, 2^3 \cdot 7)$ ,  $(2^3 \cdot 5, 2^3 \cdot 7)$ ,  $(2^3 \cdot 3 \cdot 5, 2^3 \cdot 7)$ ,  $(2^3 \cdot 5 \cdot 7, 2^3 \cdot 3)$  and  $(2^3 \cdot 3 \cdot 7, 2^3 \cdot 5)$ . In the first three cases, only one of the possible moduli could be not divisible by 2, and in the last three cases, only two of the possible moduli could be not divisible by 2. So, overall, at most two and at least one of the moduli must be not divisible by 2.

In any case, four of the classes must be congruent to  $c \pmod{2}$  for some constant  $c$ . In a situation analagous to theorem 3 and  $k = 8$ , if these classes were non-intersecting, it would imply the existence of a system of four non-intersecting congruence classes with  $\gcd \leq 4$ . While this doesn't directly contradict the case for  $k = 4$ , it is easy to show that if a reduced (in the sense implied by theorem 2) system of four congruence classes is non-intersecting with  $\gcd \leq 4$  then all four of the moduli must be 4. But in our cases above, at most three of the moduli were divisible by  $2^3$  and so, once divided by 2, at most three of them can have factors of 4, so we have a contradiction and the classes intersect.

$k = 10$ :  $M = 2^3 \cdot 3^2 \cdot 5 \cdot 7$ . Two of the moduli must be divisible by  $3^2$  and at most three since there are only 3 other prime factors of  $M$  (if they shared a factor other than  $3^2$ , there would be a  $\gcd \geq k = 10$ ) and none of the moduli can be  $3^2$  by theorem 3. If three of the moduli were divisible by  $3^2$  and more than one of the other moduli was not divisible by 3, then  $2 \cdot 5 \cdot 7$  would divide them, with  $\gcds \geq k = 10$ . So in this case, only one of the moduli can be not divisible by 3.

Now assume that exactly two of the moduli are divisible by  $3^2$  so we have the pairs  $(3^2 \cdot 2^n, 3^2 \cdot 5)$ ,  $(3^2 \cdot 2^n, 3^2 \cdot 7)$ ,  $(3^2 \cdot 5, 3^2 \cdot 7)$ ,  $(3^2 \cdot 2^n \cdot 5, 3^2 \cdot 7)$ ,  $(3^2 \cdot 5 \cdot 7, 3^2 \cdot 2^n)$  and  $(3^2 \cdot 2^n \cdot 7, 3^2 \cdot 5)$  where  $n = 1, 2, 3$ . In the first three cases, only one of the possible moduli could be not divisible by 3, and in the last three cases, only two of the possible moduli could be not divisible by 3. So, overall, at most two and at least one of the moduli must be not divisible by 3.

We can treat all of the cases where only two of the moduli are divisible by  $3^2$  just as we did with  $k = 9$ . At least three of the classes must be congruent to  $c \pmod{3}$ , and this implies a non-intersecting system with  $\gcd \leq 3$ . It is easy to show that if a reduced (in the sense implied by theorem 2) system of three congruence classes is non-intersecting with  $\gcd \leq 3$  then all three of the moduli must be 3. But in these cases, at most two of the moduli were divisible by  $3^2$  and so, once divided by 3, at most two of them can have factors of 3, so we have a contradiction and the classes intersect.

Finally, we must consider the cases where three of the moduli are divisible by  $3^2$ . This is relatively easy to do, since all of the cases are equivalent as far as the system's, gcds are concerned. The only possibilities are:

$3^2 \cdot 2^3$ or $3^2 \cdot 2^2$	$3^2 \cdot 2$	$3^2 \cdot 2$
$3^2 \cdot 5$	$3^2 \cdot 5$	$3^2 \cdot 5$
$3^2 \cdot 7$	$3^2 \cdot 7$	$3^2 \cdot 7$
$2 \cdot 5 \cdot 7$	$2 \cdot 5 \cdot 7$	$2 \cdot 5 \cdot 7$ or $2^2 \cdot 5 \cdot 7$ or $2^3 \cdot 5 \cdot 7$
$2 \cdot 3$	$2 \cdot 3$ or $2^2 \cdot 3$ or $2^3 \cdot 3$	$2 \cdot 3$
$2 \cdot 3$	$2 \cdot 3$	$2 \cdot 3$
$2 \cdot 3$	$2 \cdot 3$	$2 \cdot 3$
$2 \cdot 3$	$2 \cdot 3$	$2 \cdot 3$
$2 \cdot 3$	$2 \cdot 3$	$2 \cdot 3$
$2 \cdot 3$	$2 \cdot 3$	$2 \cdot 3$

All of these obviously intersect, (seven classes with pairwise gcds all equal to 6 for instance). □