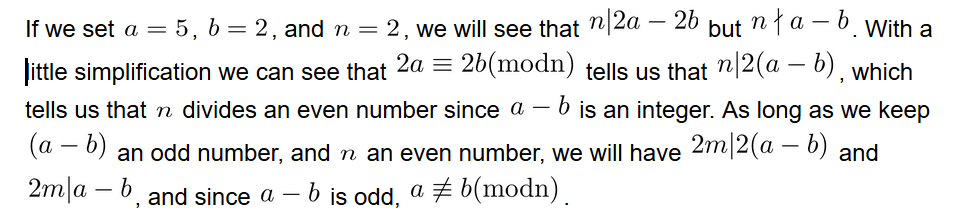
**Homework 5 Solution**

1. Find an example of numbers *a, b* and *n* such that but

If we think about the definition of equivalence, we want an example of numbers so that *n* does not divide but divides Say, Divide both sides by 2, we get If we cannot factor out *n* from the right hand side (because is not divisible by *n*), that means 2 divides *n* but not *k,* so and *k* is odd. If we choose both to be from the least complete residue system, we then have So given for some *m* and for any *b*, if we let the statement will be satisfied.



1. Suppose that where Show that if and only if and

* If then and
  + by the definition of congruence.
  + Since then and .
  + Thus, by the definition of congruence, and .
* If and then .
  + and by the definition of congruence. So and .
  + Thus, is a common multiple of and and so .
  + Since and we know that then .
  + So and by the definition of congruence.

Assume By definition n|(a-b), so there exists some integer k such that a-b = k\*n. Using the fact that n = n\_1\*n\_2 we will show—without loss of generality—that n\_1 divides a-b.

a-b = k\*n\_1\*n\_2 = n\_1(kn\_2).

So, by definition n\_1 divides a-b and n\_2 divides a-b.

We will now show that the reverse direction is true. That is, we assume a ≡ b (mod n\_1) and a≡ b (mod n\_2) and we will show that a≡b (mod n).

We know that gcds(n\_1,n\_2) = 1, which means that there exist integers x, y such that

n\_1x + n\_2y = 1.

Using this fact, and multiplying both sides of the equation by (a-b) we see that

n\_1x(a-b) + n\_2y(a-b) = a-b.

Further, by assumption, there exists integers j and p such that a-b = n\_2\*p and a-b = n\_1\*j.

We substitute these into the equation and see that

(n\_1)(x)(n\_2)(p) + (n\_2)(y)(n\_1)(j) = a-b

(n\_1\*n\_2)(xp + yj) = a-b.

From this we see that n\_1\*n\_2 = n divides a-b. We have shown that a≡ b (mod n).

Here’s another proof for the backwards direction: Assume and and we will show From the first part of the assumption, . We know that from the second part of the assumption. Since by Theorem 5 of Week 2 activity, i.e. Hence, and so

1. Find a complete residue system modulo 5 composed entirely of multiples of 9.

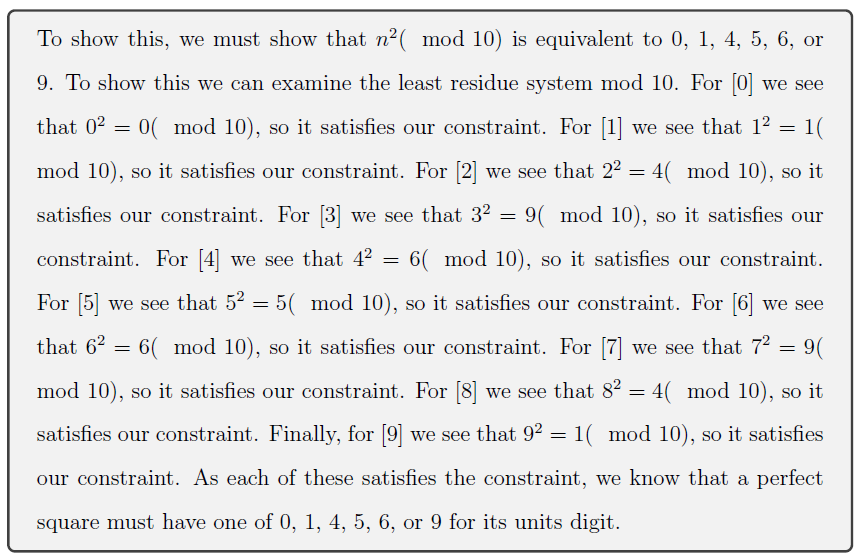
**Claim:** Given any complete residue system modulo *n*, and *a* satisfying then is also a complete residue system.

**Proof:** Note that there are *n* elements in the complete residue system candidate. If we show that no two elements are in the same residue class, we will be done because there are *n* residue classes modulo *n.* Assume two are in the same residue class, i.e.

This means Since by Theorem 5 of Week 2 class activity, this means But is a complete residue system, so and all of ’s give rise to different residue classes, forming a complete residue system.

Using the claim, we know that is a complete residue system.

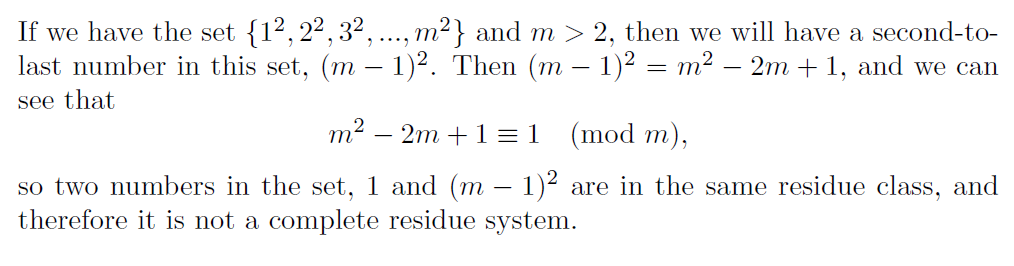
1. Show that a perfect square must have one of 0, 1, 4, 5, 6, or 9 for its units digit.



1. Show that any *n* consecutive integers form a complete residue system modulo *n*.

Suppose are *n* consecutive integers. To show that they form a complete residue system modulo *n,* it is enough to show that no two are congruent modulo *n* since there are exactly *n* integers in the list. Suppose Then which is a contradiction since form a complete residue system modulo *n.*

1. Show that is not a complete residue system modulo *m* if



1. Prove that 17 does not divide for any *n.*

* Every can be represented as for .
* Thus, every perfect square can be represented as for .
* So the possible residues of modulo 17 are exactly the squares of the possible residues of modulo 17.
* Squaring each entry of and reducing mod 17 yields
* We only needed to check half of this list because the entries will repeat after the ninth entry for the reason presented at the end of problem 6. But I calculated all squares anyway.
* Removing repeated entries tells us that the possible residues of modulo 17 are .
* Multiplying each of these entries by 5, adding 15, then reducing modulo 17 yields .
* The fact that this list does not contain a 0 means that is never congruent to 0 modulo 17. Thus 17 does not divide for any

I'm going choose to solve this as a modular question

5n^2 +15 == 0 mod 17 5n^2 == 2 mod 17

5n^2 == 70 mod 17 n^2 == 14 mod 17

At this point we check if any of the x mod 17 number types give us a remainder of 14

If you go through and check we see

1, 4, 9, 16, 8, 2, 15, 13, 13, 15, 2, 8, 16, 9, 4, 1, 0