Melbourne High School
Maths Extension Group 2023
Term 1 Week 10 Handout Solutions

§1. Problems relating to combinatorial games

§2. Modular arithmetic and congruences

§2.1 Theory and notation

§2.2 Exercises

1. If $a \equiv b \pmod{m}$ then $a-b = km$ for some integer k. Then $b-a = -km$, and hence $b \equiv a$.
   If $b \equiv c$ then let $b-c = mt$ for some integer t. Then $a-c = a-(b-mt) = km+mt = m(k+t)$. Hence $a \equiv c$.

2. A number n in decimal with digits $a_0, a_1, \ldots, a_n$ can be written as
   $$n = a_0 + a_1 10 + \cdots + a_n 10^n.$$
   Since $10 \equiv 1$ modulo 3 and 9,
   $$n \equiv a_0 + a_1 + \cdots + a_n$$
   and hence $n \equiv 0$ if and only if its digit sum is also congruent to 0 modulo 3 or 9.

3. This proof is much the same as the preceding one except that we have
   $$10^n \equiv \begin{cases} 1 & \text{if } n \text{ is even} \\ -1 & \text{if } n \text{ is odd} \end{cases} \pmod{11}$$
   Therefore
   $$n \equiv a_0 - a_1 + a_2 - a_3 + \cdots + (-1)^n a_n.$$
   That is, a number is divisible by 11 if the difference between the sum of all the digits in the even places and the digits in the odd places is divisible by 11. (This is the same thing as saying that divisibility depends on the alternating sum of the digits.)

4. Let $a - b = 2tm$ for some integer t. Then
   $$a^2 = b^2 + 4btm + 4t^2m^2$$
   which implies
   $$a^2 - b^2 = 4m(bt + t^2m).$$
   Therefore $a^2 \equiv b^2 \pmod{4m}$.

   The more general result requires the binomial theorem. Again let $a = tkm + b$ for some integer t. Then by the binomial theorem
   $$\begin{aligned} a^k &= \sum_{i=0}^{k} b^{k-i}(tkm)^i. \\ &= b^k + \binom{k}{1} b^{k-1}(tkm) + \binom{k}{2} b^{k-2}(tkm)^2 + \cdots + (tkm)^k. \\ &= b^k + b^{k-1}(tk^2m) + \binom{k}{2} b^{k-2}(tkm)^2 + \cdots + (tkm)^k. \end{aligned}$$

Hence

$$a^k - b^k = b^{k-1}(tk^2m) + \binom{k}{2} b^{k-2}(tkm)^2 + \cdots + (tkm)^k.$$

Each term on the RHS is clearly divisible by k^2m. This completes the proof.

§2.3 Linear congruences

§2.4 Problems

1. If the cupcake vendor only sells in batches of 97, I need to order $97x$ cupcakes, for some positive integer x. There are only 105 people at my party, and the remainder after everyone eats the same amount needs to be 13. Therefore the linear congruence to solve is

   $$97x \equiv 13 \pmod{105}.$$

   We find that the solution is $x \equiv 64$, which is greater than 50. Therefore I cannot satisfy the needs of my party.

2. Finding the multiplicative inverse a^{-1} is really the same as solving the congruence

   $$ax \equiv 1 \pmod{m},$$

   which has 1 solution when a and m are coprime.

3. From the preceding problem, every number in the list

   $$1, 2, 3, ..., (p-1)$$

   has exactly one multiplicative inverse in the same list. It is clear that apart from 1 and $(p-1)$, each number will not be paired with itself. Hence taking the product of $2, 3, \ldots, (p-2)$ is the same as taking the product of pairs that all are congruent to 1 modulo p; hence

   $$2 \cdot 3 \cdot 4 \cdots (p-2) \equiv 1 \pmod{p}.$$

   Multiplying both sides by $p-1$ yields the desired result.

4. Both sets have m numbers, so we only need to show that none of the numbers in the first set are congruent. If $ia \equiv ja \pmod{m}$ for $0 \leq i, j < m$, by the cancellation law we have $i \equiv j \pmod{m}$. But since $0 \leq i, j < m$, we must have $i = j$, and therefore no two numbers in the first set are congruent. This completes the proof.

   Now for the linear congruence. We may assume that b is already a least residue; that is, $0 \leq b < m - 1$. We have already shown that the numbers

   $$0, a, 2a, \ldots, (m-1)a$$

   run through a complete set of least residues, which must include b. Therefore one of those numbers is congruent to b, say $ka \equiv b \pmod{m}$, and this number k is the solution we are looking for.