Solutions for AS3

February 24, 2010

Problem 1
$[81x]_{43} = [81]_{43} \cdot [x]_{43} = [38]_{43} \cdot [x]_{43} = [1]_{43}$
As (38,43)=1 $\exists x, k, \quad 38x + 43k = 1$.
Using the extended Euclidean algorithm you can solve for x and k to get, x=17, $k = -15$.
It follows that x=17 is the correct value.

Problem 2
In Z_{11}:
inverse of [2]: [6]
inverse of [4]: [3]
inverse of [5]: [9]
inverse of [7]: [8]

Problem 3
In Z_{14}: $ab \equiv 1 \,(mod\, 14)$ and $gcd(a, 14) = 1$
Numbers could have inverse are: 1, 3, 5, 9, 11, 13
[1] has inverse [1]
[3] has inverse [5], so [5] has inverse [3],
[9] has inverse [11], so [11] has inverse [9],
[13] has inverse [13]

Problem 4
Given a, b, k and n we can use the division algorithm to divide the integer $a - b$ by nk to obtain integers k_1 and c with $a - b = k_1nk + c$, where $0 \leq c < nk$.
Then $a\, mod\, n = (k_1nk + b + c)\, mod\, n = (b + c)\, mod\, n$, because $a \equiv b\,(mod\, n)$, we have $n|c$.
Similarly, $a\, mod\, k = (k_1nk + b + c)\, mod\, k = (b + c)\, mod\, k$, because $a \equiv b\,(mod\, k)$, we have $k|c$.
Since $gcd(n, k) = 1$ it must be the case that $nk|c$, as n and k have no common factors. But as $0 \leq c < nk$, it must be the case that $c = 0$, and so $a = k_1nk + b$, or $a \equiv b\,(mod\, nk)$.

Problem 5

$x^2 \equiv 1\ (mod\, p) \Rightarrow (x^2 - 1) \equiv 0\ (mod\, p) \Rightarrow (x+1)(x-1) \equiv 0\ (mod\, p)$

Hence we have $(x+1) \equiv 0\ (mod\, p)$ or $(x-1) \equiv 0\ (mod\, p)$, since p is prime.

That is $x \equiv -1\ (mod\, p)$ or $x \equiv 1\ (mod\, p)$.

Problem 6

We are given that $gcd(a, m) = d > 1$, and so $a = k_a d$ and $m = k_m d$, for some integers $k - a$ and k_m.

Now assume that $a^x \equiv 1$ (mod m) is solvable for some x > 0, and we will derive a contradiction.

$a^x \equiv 1$ (mod m) yields $a^x \equiv (k_a d)^x \equiv 1\ (mod\, m)$.

But then this tells us $(k_a d)^x - 1 = k_m dk'$ for some k', which implies $(k_a d)^x - k_m dk' = 1$, and as d divides the left hand side of this equation we must have d divides 1. This can only happen if d = 1 which contradicts our assumption that d>1.

Hence $a^x \equiv 1 (modm)$ must not have a solution.

Problem 7

For any integer x, we can always write $x = 2w$ if x is even, or $x = 2w + 1$ if x is odd.

When x is even, $x^2 \equiv (2w)^2 \equiv 4w^2 \equiv 0\ (mod\, 4)$.

When x is odd, $x^2 \equiv (2w+1)^2 \equiv 4w^2 + 4w + 1 \equiv 1\ (mod\, 4)$.

But $4z - 1 \equiv -1\ (mod\, 4)$. So $x^2 = 4z - 1$ has no integer solution.

Problem 8

First, to see that there is a solution, it is a good idea to try a smaller example.

For example take the order sizes to be 3 and 7 instead of 9 and 20.

Here it is pretty easy to see that any number of wings bigger than 11 can be ordered exactly. WHY?? Because you can order 12 wings (12=3+3+3+3), 13 wings (13=7+3+3) and 14 wings (14=7+7) exactly, and then just adding 3 to each of these gives 15, 16 and 17 wings, and 3 to each of these, etc. Finally, it is easy to see you cannot order 11 wings using 3's and 7's. So 11 is the largest number of chicken wings you cannot order exactly.

Now, how about 9 and 20 ? Well, this is harder. But the right answer is 151, as you can check that the 9 numbers from 152 to 160 can all be obtained exactly using wing orders of size 9 and 20, and then any order of size greater than 160 can be obtained by adding some number of orders of size 9 to the orders between 152 and 160. Finally, you need to check you cannot order 151 wings exactly, a fact that takes some time to check. How do you arrive at 151 as the answer ? Well, this is a bit harder, but start with the fact that (9,20)=1 and use Bezout's Identity.

In fact, the result is for any order of size a and b, when (a,b) = 1 then there is a largest number of wings you cannot order. However, when (a,b) > 1 then there is no such largest number. Try, for example, orders of size 4 and 6. Then any order composed from these has even size, so no odd sized orders can be exactly obtained.

Problem 9
Primitive element of Z_{11}: 2
$\{0, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1024\} \equiv \{0, 2, 4, 8, 5, 10, 9, 7, 3, 6, 1\}(mod 11)$.

Problem 10
Let S be a complete set of representatives for Z_m, say $S = \{s_0, s_1, s_2, ..., s_{m-1}\}$. Then by definition of complete set of representatives for Z_m, each of the s_i's is different (mod m).

Now $aS = \{as_0, as_1, as_2, ..., as_{m-1}\}$, and we need to prove that each of the as_i's in aS is different (mod m).

We will assume this is false and get a contradiction. So assume there are two different elements as_i and as_j is aS with $as_i \equiv as_j$ (mod m). Now we use the given assumption that (a,m)=1. From this we know that in Z_m a has a multiplicative inverse. That is, there is a number b in Z_m such that $ba \equiv 1$ (mod n).

Now have $as_i \equiv as_j$ (mod m). Multiply both sides of this equation by b obtaining, $bas_i \equiv bas_j$ (mod m). Since $ba \equiv 1$ (mod n) this gives $s_i \equiv s_j$ (mod m), contradicting the fast that each of the s_i's is different (mod m) and proving our claim.