MAT 221 exam solutions

David Pierce

January 10, 2013

http://mat.msgsu.edu.tr/~dpierce/

Problem 1. Explain why the following argument is incorrect.

1. All numbers are equal to one another.
2. We shall prove this by showing by induction that, for all positive integers n, for every set of n numbers, those numbers are all equal to one another.
3. This is obviously true when $n = 1$: if a set contains just one number, then all numbers in the set are equal to one another.
4. Suppose the claim is true when $n = k$, so that for every set of k numbers, those numbers are equal to one another.
5. Let A be a set of $k + 1$ numbers.
6. Suppose $b \in A$ and $c \in A$; we shall show $b = c$.
7. Suppose $b \neq c$.
8. Then $c \in A \smallsetminus \{b\}$.
9. By inductive hypothesis, all elements of $A \smallsetminus \{b\}$ are equal to one another.
10. Let $d \in A \smallsetminus \{b\}$.
11. Therefore $c = d$.
12. Similarly $b = d$. (That is, $b \in A \smallsetminus \{c\}$, so if $d \in A \smallsetminus \{c\}$, we have $b = d$.)
13. Therefore $b = c$.
14. Thus all elements of A are equal to one another.
15. By induction, every set of n numbers really contains only one number.

Solution. Step 12 is incorrect. There is no similarity to step 11. The elements b and c of A are not interchangeable with respect to d. By step 10, $d \in A \setminus \{b\}$; but we need not have $d \in A \setminus \{c\}$. In fact $d \notin A \setminus \{c\}$, since $d = c$. (The argument in parentheses in step 12 is correct, but the hypothesis $d \in A \setminus \{c\}$ is false, so the conclusion $b = d$ does not follow.)

Problem 2. The following prime factorizations will be useful:

$$280 = 2^3 \cdot 5 \cdot 7, \qquad\qquad 679 = 7 \cdot 97.$$

(a) If the congruence
$$280x \equiv a \pmod{679}$$
has at least one solution, how many solutions *modulo* 679 does it have?
Solution. Since $\gcd(679, 280) = 7$, there are 7 solutions, if there are any at all.

(b) Find all solutions of the linear congruence $40x \equiv 14 \pmod{97}$. (Do not try to solve by trial and error; there is a clear method available to us.)
Solution. We have $\gcd(40, 14) = 2$ (and $2 \nmid 97$); so we have to solve
$$20x \equiv 7 \pmod{97}.$$
We invert 20 *modulo* 97 by means of the Euclidean algorithm:
$$\begin{aligned} 97 &= 20 \cdot 4 + 17, \\ 20 &= 17 \cdot 1 + 3, \\ 17 &= 3 \cdot 5 + 2, \\ 3 &= 2 \cdot 1 + 1, \end{aligned}$$
and then
$$\begin{aligned} 1 &= 3 - 2 = 3 - (17 - 3 \cdot 5) \\ &= 3 \cdot 6 - 17 = (20 - 17) \cdot 6 - 17 \\ &= 20 \cdot 6 - 17 \cdot 7 = 20 \cdot 6 - (97 - 20 \cdot 4) \cdot 7 \\ &= 20 \cdot 34 - 97 \cdot 7. \end{aligned}$$
Thus
$$x \equiv 34 \cdot 7 = 238 \equiv 44 \pmod{97}.$$

(c) Find all solutions of the linear congruence $280x \equiv 98 \pmod{679}$. (You may express these in terms of a solution to the congruence in part (b).)
Solution. Since $98 = 7 \cdot 14$, the solutions of $280x \equiv 98 \pmod{679}$ are precisely the solutions of $40x \equiv 14 \pmod{97}$; but if b is a solution of the latter, then the solutions of the former are expressed as

$$x \equiv a, a + 97, a + 97 \cdot 2, \ldots, a + 97 \cdot 6 \pmod{679}.$$

In fact the solutions are

$$x \equiv 44, 141, 238, 335, 432, 529, 626 \pmod{679}.$$

Problem 3. The number 2003 is known to be a prime number.

(a) Solve $2x \equiv 1 \pmod{2003}$.
Solution. $x \equiv 1002 \equiv -1001 \pmod{2003}$.

(b) Compute 2000! *modulo* 2003. (We have a named theorem that is useful for this.)
Solution. By Wilson's Theorem,

$$2002! \equiv -1 \pmod{2003},$$

and therefore

$$2000! \equiv \frac{2002!}{2002 \cdot 2001} \equiv \frac{-1}{-1 \cdot -2} \equiv 1001 \pmod{2003}.$$

Problem 4. (a) Show that 3 is a primitive root of 7 by filling out the following table:

k	1	2	3	4	5	6	(mod 6)
3^k							(mod 7)

Solution.

k	1	2	3	4	5	6	(mod 6)
2^k	3	2	-1	-3	-2	1	(mod 7)

(b) Fill out the following table. (Recall that $\mathrm{ord}_p(a)$ is the least non-negative exponent b such that $a^b \equiv 1 \pmod{p}$.)

k							(mod 6)
3^k	1	2	3	4	5	6	(mod 7)
$\mathrm{ord}_7(3^k)$							

Solution.

k	0	2	1	4	5	3	(mod 6)
3^k	1	2	3	4	5	6	(mod 7)
$\mathrm{ord}_7(3^k)$	1	3	6	3	6	2	

(c) Fill out the following table, in which ϕ is Euler's phi-function. (You can use this to check your work in (b), since for every divisor d of 6, the number of elements of $\mathbb{Z}_7{}^\times$ with order d is precisely $\phi(d)$. Alternatively, if you are confident of your solution to (b), you can use that to fill out the table here.)

d	1	2	3	6
$\phi(d)$				

Solution.

d	1	2	3	6
$\phi(d)$	1	1	2	2

(d) Solve the quadratic congruence

$$x^2 + 8x + 5 \equiv 0 \pmod{19}.$$

Again, do not use trial and error; we have a clear method. You may find needed square roots from the following table: and then you should make it clear how you do this.

k	1	2	3	4	5	6	7	8	9	(mod 18)
2^k	2	4	8	-3	-6	7	-5	9	-1	(mod 19)
2^{k+9}	-2	-4	-8	3	6	-7	5	-9	1	(mod 19)

Solution. $x \equiv \dfrac{-8 \pm \sqrt{64-20}}{2} \equiv \dfrac{-8 \pm \sqrt{6}}{2}$. From the table, $6 \equiv 2^{14}$, so $\sqrt{6} \equiv \pm 2^7 \equiv \mp 5$. Therefore $x \equiv -4 \pm 10 \cdot 5 \equiv 46, -54 \equiv 8, 3 \pmod{19}$.

Alternatively, we can complete the square:

$$\begin{aligned} & x^2 + 8x + 5 \equiv 0 \\ \iff\ & x^2 + 8x \equiv -5 \\ \iff\ & x^2 + 8x + 16 \equiv 11 \\ \iff\ & (x+4)^2 \equiv -8. \end{aligned}$$

From the table, $-8 \equiv 2^{12}$, so $\sqrt{-7} \equiv \pm 2^6 \equiv \pm 7$, and therefore $x \equiv -4 \pm 7 \equiv 3, -11 \equiv 3, 8$.