DISCRETE MATH 37181 TUTORIAL WORKSHEET 9

INSTRUCTIONS. Complete these problems in groups of 3-4 at the whiteboard. Partial solutions at the end of the PDF.

1. An old woman goes to market and a horse steps on her basket and crushes her eggs. The rider offers to pay for the damage and asks her how many eggs she had brought. She does not remember the exact number, but when she had taken them out two at a time, there was one egg left. The same happened when she picked them out three, four, five and six at a time, but when she took them out seven at a time they came out even (no eggs left). What is the smallest number of eggs she could have had? [1]

2. (a) State Euler's theorem.

   (b) Give an example of its use.

   (c) Find the remainder of 7^{16} upon division by 40 (that is, compute $[7^{16}]_{40}$]). Can anyone do this in one second?

   (d) Compute $\varphi(40) = \varphi(2.2.2.5)$ using the Lemmas in Lecture 16: $\varphi(p^n) =?$ when p is prime and $\varphi(ab) =?$ when a, b are relatively prime.

   (e) What is the size of the set $\mathbb{Z}_{40}^*$?

   (f) Demonstrate (by example) that multiplying every element of $\mathbb{Z}_{40}^*$ by $a \in \mathbb{Z}_{40}^*$ simply *permutes* the elements around, by checking $a = 3$.

3. (a) Without using a computer, find the final digit of 43^{68}. [2]

   (b) Without using a computer, what is the value of $[43^{68}]_{18}$?

4. Prove that every $n \in \mathbb{N}, n > 1$ can be written as a product of primes.
   That is, there exist $p_1, \ldots, p_r$ distinct primes and $i_1, \ldots i_r \in \mathbb{N}_+$ so that $n = p_1^{i_1} p_2^{i_2} \ldots p_r^{i_r}$. [3] [4]

5. Prove that if $x, y \in \mathbb{Z}_n^*$ (that is, x, y are relatively prime to n) then so is $[xy]_n$. [5]

Date: Week 9 workshop (Wednesday 27, Thursday 28, Friday 29 April).

[1] From: Number Theory and Its History (Dover Books on Mathematics) Oystein Ore, 1948

[2] Hint: mod 10 will give the final digit. Repeated squaring, or can you use Euler's theorem?

[3] Hint: strong induction

[4] Actually, you can prove that *up to reordering* the product of primes is unique. Proving uniqueness: suppose $n = p_1^{i_1} p_2^{i_2} \ldots p_r^{i_r} = q_1^{i_1} q_2^{i_2} \ldots q_s^{i_s}$, where without loss of generality we can assume the primes are written in increasing size order. Then $r = s$ and $p_i = q_i$. If you like doing these proofs, maybe you like doing pure mathematics.

[5] Therefore, when we multiply elements of $\mathbb{Z}_n^*$ together they *stay* inside $\mathbb{Z}_n^*$.

6. Let G be a set, and $* : G \times G \to G$ a function. [6] We call $(G, *)$ a *group* if the following three conditions are satisfied:

   1 $*$ is associative. [7]

   2 there exists an element $e \in G$ so that for all $x \in G$ we have $*(x, e) = x = *(e, x)$.

   3 for each $x \in G$ there exists $y \in G$ so that $*(x, y) = e = *(y, x)$.

   Discuss with your teammates whether each of the following examples is a group: [8].

   (a) $G = \mathbb{Z}_n^*, *(a, b) = [ab]_n$

   (b) $G = \mathbb{Z}$, $*(a, b) = a + b$.

   (c) $G = \mathbb{Z}$, $*(a, b) = ab$ (a multiplied by b).

   (d) $G = \mathbb{Z}$, $*(a, b) = \dfrac{a}{b}$ (a divided by b).

   (e) $G =$ the set of all 2×2 matrices with real number entries and determinant 1, $*(A, B) = AB$ (matrix multiplication) [9]

7. Find the 2018 final exam from the UTS Library website [10], and do questions 19, 20, 23.

END OF TUTORIAL WORKSHEET 9

[6] For example, $G = \mathbb{Z}_n^*, *(x, y) = [xy]_n$ (you just proved that $[xy]_n$ lands back inside G).

[7] that is, $*(x, *(y, z)) = *(*(x, y), z)$ for all $x, y, z \in G$. To save time, you don't have to *prove* this, just decide between your teammates if you all agree its true or false.

[8] if Yes, what is the element e? Given x, what is the element y in the last condition?

[9] We assume at least one person in each team has done Maths 1, LDS, or otherwise knows about matrices

[10] UTS no longer provides copies of past exams since COVID. Why not? You should ask the Library and Exams branch. Instead we have posted this under the Final Exam tab in Canvas.

Brief solutions:

1. We have a number x with $[x]_2 = 1, [x]_3 = 1, [x]_4 = 1, [x]_5 = 1, [x]_6 = 1, [x]_7 = 0$. Find the smallest x that satisfies all those conditions. To brute-force it I would just start at $x = 7, 14, 21, \ldots$ and check the remainders mod $2, 3, 4, 5, 6$ and stop the first time I find the remainders are all 1. Alternatively, since $x = 2p + 1$, and $x = 3q + 1, \ldots$, we need $x = 2.3.2.5k + 1$ (note I don't need to put $4, 6$ since I already have some of their factors - for 4 I just need an extra 2.) This is $60k + 1$, so I am looking for the smallest k so that $60k + 1$ is divisible by 7. Answer: 301.

   So many additional questions, why did the old woman take them out and back so many times previously? Was the horse black?

2. $\varphi(40) = \varphi(8)\varphi(5) = (8 - 4)(4) = 16$ so $7^{16} \mod 40 \equiv 1$ by Euler's theorem.

$$\mathbb{Z}_{40}^* = \{1, 3, 7, 9, 11, 13, 17, 19, 21, 23, 27, 29, 31, 33, 37, 39\}$$

   (good, there are 16 elements here) and

$$3\mathbb{Z}_{40}^* = \{3, 9, 21, 27, 33, 39, 3.17, 3.19, 3.21, 3.23, 3.27, 3.29, 3.31, 3.33, 3.37, 3.39\}$$

   (multiply and reduce those last ones mod 40, and it should check out.)

3. (a) mod 10 will give the final digit. Try the *repeated squaring* method to do this quickly:

   $43 \equiv 3 \mod 10$ so we need $3^2 = 9, 3^4 = 9.9 = 81 \equiv 1, 3^8 = 3^4.3^4 = 1.1$, will be 1 from now on, so

$$43^{68} \equiv 3^{68} = 3^{64+4} = 3^{64}.3^4 = 1.1 \equiv 1$$

   But even quicker is to use Euler's theorem: $\varphi(10) = (5 - 1)(2 - 1) = 4$ so

$$43^{68} = (43^4)^{17} \equiv 1^{17} = 1$$

   by Euler's theorem.

   (b) $\varphi(18) = \varphi(9)\varphi(2) = 6$ so by Euler's theorem $a^6 \equiv 1 \mod 18$ when a is relatively prime to 18.

   $68 = 66 + 2$ so $a^{68} = a^{66}a^2 = (a^6)^{11}a^2 \equiv 1.a^2$ when a is relatively prime to 18 .

   We have $\gcd(43, 18) = 1$ so we can use this, we get $43 \equiv 7$ and $43^{68} \equiv 43^2 \equiv 7^2 = 49 \equiv 13$

   If you didn't see Euler's theorem, you can do the whole thing with repeated squaring: $43 \equiv 7$, $7^2 = 49 \equiv 13, 7^4 \equiv 7, 7^8 \equiv 13$ alternates between 13 and 7. Then $7^{68} = 7^{64}.7^4 \equiv 7.7 \equiv 13$.

4. Proof: Either n is prime (and we are done), or not. If not, by definition of *not* being prime, $n = ab$ where

$$a, b, \in \mathbb{Z}, \quad 1 < a, b < n$$

   by definition (negation of being prime). By strong induction, $a = p_1^{i_1} p_2^{i_2} \ldots p_r^{i_r}$ and $b = q_1^{i_1} q_2^{i_2} \ldots q_s^{i_s}$.

   Okay, so that is the idea, now we need to start the proof again from the start. Let $P(n)$ be the statement .... Base case $n = 2$ is true. Etc.

5. $\gcd(n, x) = 1$ means $1 = ax + bn$; $\gcd(n, y) = 1$ means $1 = cy + dn$; multiply together to get
$$1 = (ax + bn)(cy + dn) = acxy + n(\dots)$$
If $p \mid xy$ and $p \mid n$ then $p \mid 1$ according to the above equation, so that means p must be equal to 1, and $\gcd(xy, n) = 1$.

6. (a) By question 7, $*$ is a map from $G \times G$ back inside G. Multiplication is associative (annoying to *prove* this, but I think we can all agree). The element e in this case is 1. For each $x \in G$, since $\gcd(x, n) = 1$ (relatively prime), it has a multiplicative inverse (Euclidean algorithm backwards). So all the conditions check out, and this is a group.

   Note this is a *finite group*, it has size $\varphi(n)$.

   Also note this fact: if G is a group and $a \in G$ then multiplying (applying $*$) every element of G by a of the left is a bijection from G to G (simply permutes the elements around). Proof: First let me write $a * b$ instead of $*(a, b)$ to make life easier.

   To prove one-to-one: for $x, y \in G$, if $a * x = a * y$, then multiplying (applying $*$) both sides of the left by the inverse of a and applying the rules gives $x = y$. This shows multiplication by a on the left is one-to-one.

   To show onto: since $a \in G$ it has an inverse element, which we can call $a^{-1} \in G$. That is, $a * a^{-1} = e$. For each $x \in G$ there is an element $(a^{-1} * x) \in G$ so that $a * (a^{-1} * x) = x$, so the map is onto.

   This question is leading us to an advanced topic beyond the scope of 37181, but actually what we proved in the lecture about $\mathbb{Z}_n^*$ is much more general.

   (b) Yes (c) No (d) No

   (e) Yes, this is a group, since $\det(AB) = \det(A)\det(B)$ is a thing (proved? in Maths 1 or at least stated.) Using this, if $\det(A) = 1$ and $\det(B) = 1$ then $\det(AB) = 1$ so $*(A, B)$ lands back inside G. The element e in this case is the identity matrix $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. Since $\det = 1$, every element of G has a matrix inverse, so the last rule checks out.