Solutions to Exercises for TATA55, batch 1, 2018

October 18, 2018

1. Determine all positive integer solutions to $5x + 11y = 999$.

   Solution: The extended Euclidean algorithm shows that $\gcd(5, 11) = 1$ and that $1 = 5 * (-2) + 11 * 1$. It follows that $x_p = -2 * 999$, $y_p = 1 * 999$ is one integer solution to the original equation, and that

$$x = -2 * 999 + 11n$$
$$y = 1 * 999 - 5 * n$$

   with $n \in \mathbb{Z}$, constitue all integer solutions.

   Now we want to find the positive integer solutions. Then

$$-2 * 99 + 11n > 0$$
$$1 * 999 - 5n > 0$$

   so
$$\frac{2 * 999}{11} = 181 + \frac{7}{11} < n < \frac{999}{5} = 199 + \frac{4}{5}$$
   whence $182 \leq n \leq 199$.

2. Find all integer x such that $x = 13q_1 + 5 = 17q_2 + 7$, q_1, $q_2 \in \mathbb{Z}$.

   Solution: In other words, we want all x such that

$$x \equiv 5 \mod 13$$
$$x \equiv 7 \mod 17$$

   Since $\gcd(13, 17) = 1$, this is doable, and the solution will be unique mod $13 * 17$. Since
$$x = 13q_1 + 5 \equiv 7 \mod 17$$
   we have that
$$13q_1 \equiv 2 \mod 17$$
   Since
$$1 = \gcd(13, 17) = 13 * 4 + 17 * (-3)$$

we have that

$$13 * 4 \equiv 1 \mod 17,$$

so

$$q_1 \equiv 4 * 2 = 8 \mod 17.$$

Thus

$$x \equiv 13 * 8 + 5 = 109 \mod 13 * 17.$$

3. Let G be a group, and let $H \subseteq G$, such that $e \in H$ and $HH \subseteq H$.

   (a) Show that $HH = H$.

   (b) If $|G| < \infty$, show that $H \leq G$.

   (c) Is it enough that $|H| < \infty$?

   Solution:

   (a) $eh = h$.

   (b) We need only to show that $H^{-1} \subseteq H$. Pick $h \in H$. Consider the map

   $$\phi_h : H \to H$$
   $$\phi_h(x) = hx$$

   This map is injective: if $\phi_h(x) = \phi_h(y)$ then $hx = hy$ so $x = y$ by cancellation. However, since H is finite (beeing a subset of the finite set G), any injective map from H to itself is in fact bijective! Thus, $e \in \phi_h(H)$, that is to say, there is some $x \in h$ with $e = \phi_h(x) = hx$. Thus h has a right inverse x, which, by group laws, is also a left inverse.

   (c) Yes.

4. Let A be a finite set with n elements, and let $f : A \to A$ be a map. Define a digraph G with vertex set A, and with a directed edge $a \to b$ iff $f(a) = b$.

   (a) For $n = 5$, draw the graph associated to

   $$f = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 1 & 1 \end{bmatrix} \quad \text{and} \quad g = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 3 & 3 \end{bmatrix}$$

   (b) Show that every vertex in G has outdegree 1. Show that f is invertible iff every vertex in G has indegree 1.

   (c) Pick $a \in A$. Show that the sequence $f^{(k)}(a)$, $k = 0, 1, 2, \ldots$ is eventually periodic. Is $f^{(k)}$, $k = 0, 1, 2, \ldots$ eventually periodic?

   Solution:

(a)

(b) The vertex a has the unique outgoing arrow $a \to f(a)$. The inverse image $f^{-1}(b)$ of a vertex is the set of all vertices c such that $c \to b$. The map f is invertible iff each such inverse image has cardinality one.

(c) Since A is finite, by the pigeon-hole principle there is some smallest $1 \leq i < j \leq |A| + 1$ such that $f^{(i)}(a) = f^{(j)}(a) =: b$. Then $f^{(i+1)}(a) = f^{(j+1)}(a) = f(b)$, and so on.

Now let $X = A^A$ be the set of all maps from A to A. Given f, define

$$F_f : X \to X$$
$$F_f(g) = f \circ g$$

Since X is finite, we apply our previous result to show that F is eventually periodic.

5. Let T denote the group of complex numbers of unit modulus, under multiplication.

(a) Find all elements of order 2, order 3, and order 4.

(b) Find all elements of finite order n.

(c) Find all finite subgroups of T.

Solution:

(a) The elements that have order dividing n are all roots of the polynomial $z^n - 1$. We see that -1 is the unique element of order 2, that $\pm \exp(\frac{2}{3}\pi i)$ are the ones with order 3, and that $\pm i$ are the ones with order 4.

(b) We can furthermore see that the zeroes of $z^n - 1$ form a cyclic group of order n, with $g = \exp(\frac{2}{n}\pi i)$ as a generator, and all generators given by g^k with $\gcd(k, n) = 1$. These elements have order n. Note that the other solutions to $z^n - 1 = 0$ have order dividing n.

(c) The element $\exp(\frac{a}{b}2\pi i)$, with a, b integers, have finite order (dividing b). The elements $\exp(r2\pi i)$, with r irrational, have infinite order. If H is a finite subgroup, it can thus not contain any $\exp(r2\pi i)$, with r irrational. Hence, $H = \left\{ \exp(\frac{a_j}{b_j}2\pi i) \middle| 1 \leq j \leq N \right\}$. Now note first that we can assume that $\gcd(a_j, b_j) = 1$, and secondly, that if we put $B = \operatorname{lcm}(b_1, \ldots, b_N)$ then $H \leq \left\langle \exp(\frac{1}{B}2\pi i) \right\rangle$. In fact, equality holds!

Thus, all finite subgroups are cyclic, and of the form described in the previous subexercise.

Another proof of this fact goes as follows. Suppose that H is a finite subgroup of the cycle group. Then there is some smallest positive t such that $g = \exp(t2\pi i) \in H$. Clearly, $\langle g \rangle \leq H$. In fact, equality holds: if $w = \exp(s2\pi i) \in H \setminus \langle g \rangle$, then

s is not an integer multiple of t. Write $s = \lfloor s/t \rfloor t + \{s/t\} = mt + \alpha$, using the integer part and the fractional part of s/t. Since $\exp(mt2\pi i) = g^m \in H$, it follows that $\exp(\alpha 2\pi i) \in H$, as well. But $0 < \alpha < t$, a contradiction.

Thus $H = \langle g \rangle$.

6. Find all possible orders of permutations on 5 letters.

   Solution: The order of conjugate elements are the same, thus we check the different cycle types in S_5; these cycle types are represented by numerical partitions of 5.

   - 5=5: 5-cycles have order 5.
   - 5=4+1: 4-cycles have order 4.
   - 5=3+2: $(abc)(de)$ has order $3 * 2 = 6$.
   - 5=3+1+1: 3-cycles have order 3.
   - 5=2+2+1: $(ab)(cd)$ has order 2.
   - 5=2+1+1+1: 2-cycles have order 2.
   - 5=1+1+1+1+1: The identity has order 1.

7. Let $X = \mathbb{Z}$, and let $G = S_X$. Give an explicit element in G with infinite order.

   Solution: The simplest example is probably $x \mapsto x + 1$. Another example is

$$\sigma = (0)(1, -1)(2, -2, 3, -3)(4, -4, 5, -5, 6, -6)(7, -7, 8, -8, 9, -9, 10, -10) \cdots$$

8. Describe the subgroups of S_n generated by the n-cycles.

   Solution: To clarify, for each integer $n \geq 2$, we want the smallest subgroup of S_n the contains all n-cycles.

   We note that

$$(1, 2, 3, 4, \ldots, n)(2, 1, 3, 4, \ldots, n)^{-1} = (1, 3, 2) = (1, 2, 3)^{-1},$$

   and that thus every 3-cycle is a product of two n-cycles. We can thus generate all 3-cycles. The alternating group $A_n \leq S_n$ consisting of the even permutations is generated by 3-cycles (see the textbook) so we can generate at least A_n. If n is odd, all n-cycles are even, and lie in A_n, and generate A_n,thus they generate precisely A_n. If n is even, the subgroup generated by the n-cycles consists of all of A_n, and some more permutations; but since A_n has index 2 in S_n, we must necessarily get all of S_n-

9. Let G be a group, and let $x, y \in G$, with $xy = yx$. Suppose that $o(x) = n < \infty$, $o(y) = m < \infty$. What is $o(xy)$?

   Solution: Since $(xy)^n = x^n y^n$, we have that $o(xy) \,|\mathrm{lcm}(n, m)$. However, taking $n = m$ with $y = x^{-1}$ shows that the order of xy can be much smaller than $\mathrm{lcm}(n, m)$. In the special case that $\langle x \rangle \cap \langle y \rangle = \{1\}$ we can easily see that $o(xy) = \mathrm{lcm}(n, m)$.

10. If G is a group, $A, B \leq G$. Show that $AB \leq G$ iff $AB = BA$.

Solution: Suppose that $AB = BA$. Take $h \in AB$, $h = ab$ with $a \in A$, $b \in B$. Then $\ni h^{-1} = b^{-1}a^{-1} \in BA = AB$. Take furthermore $k = cd$,$c \in A$, $d \in b$. Then $hk = abcd = a(bc)d$. Since $bc \in BA = AB$ there exists $r \in A$, $s \in B$ with $bc = rs$. Thus $hk = a(rs)d = (ar)(sd) \in AB$.

Conversely, suppose that $AB \leq G$. Take $a \in A$, $b \in b$, and put $h = ab$. Then $h^{-1} \in AB$. But $h^{-1} = b^{-1}a^{-1} \in BA$. Since every $k \in AB$ is $(k^{-1})^{-1}$, the result follows.