Solutions for Exercises for TATA55, batch 1, 2019

October 10, 2019

1. (3p) Assuming Bezout (the gcd is a integral linear combination of its arguments) show that a prime dividing a product divides one of the factors.

   Solution:

   Suppose that $p \mid ab$ but $p \nmid a$. Then $\gcd(p, a) = 1$, since p prime, so by Bezout $1 = px + ay$. Thus $b = pbx + aby$. Since $p \mid ab$, we have that $p \mid \mathrm{RHS}$, thus $p \mid b$.

2. (3p) Find all solutions to
$$3x + 5y = 999, \qquad x, y \in \mathbb{Z}$$
   with y positive and x even.

   Solution: Since $3*2+5*(-1) = 1$, a particular solution to the unrestricted Diophantine eqn is $(x_p, y_p) = (2*999, -1*999) = (1998, -999)$. The homogeneous soln is $(x_h, y_h) = n(-5, 3)$, $n \in \mathbb{Z}$, and thus the general solution is
$$x = 1998 - 5n$$
$$y = -999 + 3n$$
   For x to be even, n has got to be even. For y to be positive we must have that
$$y = -999 + 3n > 0,$$
   thus $n > \frac{999}{3} = 333$.

3. (3p) Solve (by hand, though you may check your answer using machines)
$$x \equiv 57 \mod 96$$
$$x \equiv 95 \mod 98$$

   Solution:

   The first equation gives $x = 57 + 96y$. Inserted into the second, this gives
$$57 + 96y \equiv 95 \mod 98$$
$$96y \equiv 38 \mod 98$$
$$48y \equiv 19 \mod 49$$
$$-y \equiv 19 \mod 49$$
$$y \equiv -19 \mod 49$$
$$y \equiv 30 \mod 49$$

So $y = 30 + 49n$, and $x = 57 + 96y = 57 + 96(30 + 49n) = 2937 + 4704n$, i.e.,

$$x \equiv 2937 \mod 4704$$

4. (1p+2p) Let X be a finite set, and let $\sim$ be an equivalence relation on X. Let $T = \{x_1, \ldots, x_n\}$ be a transversal, i.e., a choice of exactly one element from each equivalence class.

   (a) Define a map $N : X \to X$ such that

      i. $N \circ N = N$, and

      ii. $x \sim y$ iff $N(x) = N(y)$, and

      iii. $N(X) = T$.

   (b) If $N : X \to X$ satisfies the first two of the above conditions, need $N(X)$ be a transversal?

   Solution:

   First, note that the first two conditions imply that

$$N(x) = N(N(x)) \quad \Longrightarrow \quad x \sim N(x).$$

   The second condition shows that all elements of the same equivalence class must map to the same element; that element is an element of $N(X) = T$.

   The only way of defining N is thus $N(u) = x_i$ if $u \sim x_i$.

   If N satisfies just the first two conditions, let $S = N(X)$. If $s_1, s_2 \in S$ then $s_1 = N(t_1)$, $s_2 = N(t_2)$, so $N(s_1) = N(N(t_1)) = N(t_1) = s_1$, and similarly $N(s_2) = s_2$. Hence $s_1 \sim s_2$ iff $s_1 = s_2$, so different s_i belong to different equivalence classes.

   Suppose, towards a contradiction, that there is some class $[u]_\sim$ containing no element from S. Then $N(u) = s_j$, with $[s_j]_\sim \neq [u]$. But $N(N(u)) = N(u) = s_j$ and $N(N(u)) = N(s_j)$, so $N(u) = N(s_j)$ which implies that $u \sim s_j$, a contradiction.

   Thus, S is a transversal.

5. (1p+3p) Let $X = \{a, b\}$, and let X^* denote the monoid of all "words" in the letters in X, including the empty word; the operation is concatenation.

   Suppose that u, v are non-empty words in X^*.

   Show that

$$uv = vu$$

   if and only if u, v are both powers of some common word, i.e. if there exists a non-empty word z, and positive integers k, ℓ, such that

$$u = z^k, \qquad v = z^\ell$$

   As an example, $u = abaaba$ and $v = abaabaaba$ commute.

   Solution: : Proof from "Automatic sequences" by Allouche and Shallit included at the end.

6. (3p) Let M be a monoid, and let $x \in M$. Suppose that there exists positive integers $0 < n < m$ such that $x^n = x^m$. Show that there are positive integers N, s such that, for all non-negative integers a, b, it holds that

$$x^{N+a} = x^{N+b} \quad \iff \quad a \equiv b \mod s$$

((2p) If you can't solve this one, give an example of a monoid M and an element x such that $x^7 = x^{11}$ is the earliest coincidence, and show that for non-negative a, b, $x^{7+a} = x^{7+b}$ if and only if $a \equiv b \mod 4$.)

Solution: We actually don't need M to be a monoid, it is enough that it is a semigroup.

First, put $d = m - n$ and note that since $x^n = x^{n+d}$, $n^{n+1} = x^{n+d+1}$, and so on, $x^{n+d-1} = x^{n+2d-1}$, $x^{n+d} = x^{n+2d}$, et cetera, so every x^ℓ with $\ell \geq m$ is equal to a x^k with $k \leq m - 1$.

Next, let

$$J = \left\{ j \in \mathbb{Z}_+ \middle| x^j \neq x^k \text{ for } k < j \right\},$$

and form a directed graph with vertex set J, and a directed edge $i \to j$ whenever $x^{i+1} = x^j$. Then clearly

(a) J is finite,

(b) There is a directed path from 1 to any $j \in J$,

(c) Each vertex has out-degree one.

But such a digraph looks like follows:

$$\begin{tikzcd}
1 \arrow[r] & 2 \arrow[r] & 3 \arrow[r] & \cdots \arrow[r] & N-1 \arrow[r] & N \arrow[dr, bend left] & \\
& & & & N+s-1 \arrow[ur] & & N+1 \arrow[dl, bend left] \\
& & & & & \cdots \arrow[ul, bend left] &
\end{tikzcd}$$

It follows that

$$x^1, x^2, \ldots, x^{N-1}, x^N$$

are all distinct, and that

$$x^N, x^{N+1}, \ldots,$$

repeat with period s.

See also "Fundamentals of semigroup theory" by Howie.

We now state and prove the second theorem of Lyndon and Schützenberger.

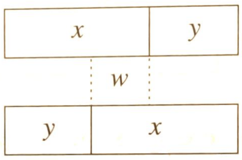
Theorem 1.5.3 *Let $x, y \in \Sigma^+$. Then the following three conditions are equivalent:*

(1) $xy = yx$.
(2) There exist integers $i, j > 0$ such that $x^i = y^j$.
(3) There exist $z \in \Sigma^+$ and integers $k, l > 0$ such that $x = z^k$ and $y = z^l$.

Proof. We show that (1) $\Longrightarrow$ (3), (3) $\Longrightarrow$ (2), and (2) $\Longrightarrow$ (1).

(1) $\Longrightarrow$ (3): By induction on $|xy|$. If $|xy| = 2$, then $|x| = |y| = 1$, so $x = y$ and we may take $z = x = y$, $k = l = 1$.

Now assume the implication is true for all x, y with $|xy| < n$. We prove it for $|xy| = n$. Without loss of generality, assume $|x| \geq |y|$. Then we have a situation like the following:



Hence there exists $w \in \Sigma^*$ such that $x = wy = yw$. If $|w| = 0$ then $x = y$ and we can take $z = x = y$, $k = l = 1$.

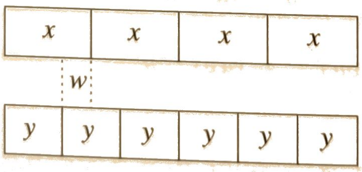
Otherwise $|w| \geq 1$. We have $|wy| = |x| < |xy| = n$, so the induction hypothesis applies, and there exists $z \in \Sigma^+$ and integers $k, l > 0$ such that $w = z^k$, $y = z^l$. It follows that $x = wy = z^{k+l}$.

(3) $\Longrightarrow$ (2): By (3) there exist $z \in \Sigma^+$ and integers $k, l > 0$ such that $x = z^k$ and $y = z^l$. Hence, taking $i = l$, $j = k$, we get

$$x^i = (z^k)^i = z^{kl} = (z^l)^k = (z^l)^j = y^j,$$

as desired.

(2) $\Longrightarrow$ (1): We have $x^i = y^j$. If $|x| = |y|$ then we must have $i = j$ and so $x = y$. Otherwise, without loss of generality assume $|x| > |y|$. Then we have a situation like the following:



That is, there exists $w \in \Sigma^+$ such that $x = yw$. Hence $x^i = (yw)^i = y^j$, and so $y(wy)^{i-1}w = y^j$. Therefore $(wy)^{i-1}w = y^{j-1}$, and so, by multiplying by y on the right, we get $(wy)^i = y^j$. Hence $(yw)^i = (wy)^i$, and hence $yw = wy$. It follows that $x = yw = wy$ and $xy = (yw)y = y(wy) = yx$. ∎

Particular interest attaches to the case where A is finite. If $A = \{a_1, a_2, \ldots, a_n\}$ then we shall write $\langle A \rangle$ as $\langle a_1, a_2, \ldots, a_n \rangle$. Especially interesting is the case where $A = \{a\}$, a singleton set, when

$$\langle a \rangle = \{a, a^2, a^3, \ldots\}.$$

At this point it is worth pausing to note that if S is a monoid then we can equally well talk of the sub*monoid* of S generated by S. This will always contain 1, and in the case of a singleton generator we find that

$$\langle a \rangle = \{1, a, a^2, a^3, \ldots\}.$$

In what follows, however, it will be sufficient to consider the semigroup case.

We refer to $\langle a \rangle$ as the *monogenic* subsemigroup of S generated by the element a. The *order* of the element a is defined, as in group theory, as the order of the subsemigroup $\langle a \rangle$. If S is a semigroup in which there exists an element a such that $S = \langle a \rangle$, then S is said to be a *monogenic* semigroup.

Clifford and Preston (1961) followed the group-theoretic terminology, and referred to semigroups with one generator as 'cyclic'. From what follows, the reader may judge whether monogenic semigroups are 'round' enough to merit the description 'cyclic.'

Let a be an element of a semigroup S, and consider the monogenic subsemigroup

$$\langle a \rangle = \{a, a^2, a^3, \ldots\}$$

generated by a. If there are no repetitions in the list $a, a^2, a^3, \ldots$, that is, if

$$a^m = a^n \;\Rightarrow\; m = n,$$

then evidently $(\langle a \rangle, .)$ is isomorphic to the semigroup $(\mathbf{N}, +)$ of natural numbers with respect to addition. In such a case we say that a is an *infinite* monogenic semigroup, and that a has *infinite order* in S.

Suppose now that there are repetitions among the powers of a. Then the set

$$\{x \in \mathbf{N} : (\exists y \in N)\; a^x = a^y,\; x \neq y\}$$

is non-empty and so has a least element. Let us denote this least element by m and call it the *index* of the element a. Then the set

$$\{x \in \mathbf{N} : a^{m+x} = a^m\}$$

is non-empty, and so it too has a least element r, which we call the *period* of a. We shall also refer to m and r as the index and period, respectively, of the monogenic semigroup $\langle a \rangle$.

Let a be an element with index m and period r. Thus

$$a^m = a^{m+r}. \tag{1.2.1}$$

It follows that

$$a^m = a^{m+r} = a^m a^r = a^{m+r} a^r = a^{m+2r},$$

and, more generally, that

$$(\forall q \in \mathbf{N})\ a^m = a^{m+qr}.$$

By the minimality of m and r in (1.2.1) we may deduce that the powers

$$a, a^2, \ldots, a^m, a^{m+1}, \ldots, a^{m+r-1}$$

are all distinct. For every $s \geq m$ we can, by the division algorithm, write $s = m + qr + u$, where $q \geq 0$ and $0 \leq u \leq r-1$. It then follows that

$$a^s = a^{m+qr} a^u = a^m a^u = a^{m+u};$$

thus

$$\langle a \rangle = \{a, a^2, \ldots, a^{m+r-1}\}, \text{ and } |\langle a \rangle| = m + r - 1.$$

We say that a has *finite order* in this case; the order is given by the rule

$$\text{order of } a = (\text{index of } a) + (\text{period of } a) - 1.$$

The subset $K_a = \{a^m, a^m + 1, \ldots, a^{m+r-1}\}$ of $\langle a \rangle$ is a subsemigroup, indeed an ideal, of $\langle a \rangle$. We call it the *kernel* of $\langle a \rangle$, and we shall see in due course that this use of the word does not conflict with the more general use of 'kernel' in Chapter 3. In fact K_a is a *subgroup* of $\langle a \rangle$, for if a^{m+u} and a^{m+v} are elements of K_a, then we can find an element a^{m+x} in K_a for which

$$a^{m+u} a^{m+x} = a^{m+v}$$

simply by choosing x so that

$$x \equiv v - u - m \pmod r \ \text{ and } \ 0 \leq x \leq r - 1.$$

Indeed K_a is a cyclic group. To see this, notice that the integers

$$m,\ m+1,\ \ldots,\ m+r-1$$

form a complete set of incongruent residues modulo r. (For this and other elementary number-theoretic ideas see, for example, Hardy and Wright (1979).) It follows that there exists g such that

$$0 \leq g \leq r-1 \ \text{ and } \ m + g \equiv 1 \pmod r. \tag{1.2.2}$$

Hence $k(m+g) \equiv k \pmod r$ for every k in $\mathbf{N}$, and so the powers $(a^{m+g})^k$ of a^{m+g}, for $k = 1, 2, \ldots, r$, exhaust K_a. Thus K_a is a cyclic group of order r, generated by the element a^{m+g}.

If we choose z so that

$$0 \leq z \leq r-1 \ \text{ and } \ m + z \equiv 0 \pmod r, \tag{1.2.3}$$

then a^{m+z} is idempotent, and so it is the identity of the group K_a.

Example 1.2.1 Let $X = \{1, 2, \ldots, 7\}$, and consider the element

$$\alpha = \begin{pmatrix} 1\,2\,3\,4\,5\,6\,7 \\ 2\,3\,4\,5\,6\,7\,5 \end{pmatrix}$$

of $\mathcal{T}_X$. (The notation for α is an obvious generalization of the standard notation for permutations: the import is that $1\alpha = 2$, $2\alpha = 3$, …, $6\alpha = 7$, $7\alpha = 5$.) It is easy to calculate that

$$\alpha^2 = \begin{pmatrix} 1\,2\,3\,4\,5\,6\,7 \\ 3\,4\,5\,6\,7\,5\,6 \end{pmatrix}, \quad \alpha^3 = \begin{pmatrix} 1\,2\,3\,4\,5\,6\,7 \\ 4\,5\,6\,7\,5\,6\,7 \end{pmatrix},$$

$$\alpha^4 = \begin{pmatrix} 1\,2\,3\,4\,5\,6\,7 \\ 5\,6\,7\,5\,6\,7\,5 \end{pmatrix}, \quad \alpha^5 = \begin{pmatrix} 1\,2\,3\,4\,5\,6\,7 \\ 6\,7\,5\,6\,7\,5\,6 \end{pmatrix},$$

$$\alpha^6 = \begin{pmatrix} 1\,2\,3\,4\,5\,6\,7 \\ 7\,5\,6\,7\,5\,6\,7 \end{pmatrix}, \quad \alpha^7 = \begin{pmatrix} 1\,2\,3\,4\,5\,6\,7 \\ 5\,6\,7\,5\,6\,7\,5 \end{pmatrix},$$

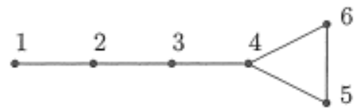
and so α has index 4 and period 3. The kernel K_α is equal to $\{\alpha^4, \alpha^5, \alpha^6\}$, and has Cayley table

	α^4	α^5	α^6
α^4	α^5	α^6	α^4
α^5	α^6	α^4	α^5
α^6	α^4	α^5	α^6

Thus α^6 is the identity of K_a, in accord with formula (1.2.3), since $6 \equiv 0 \pmod 3$. Also, in accord with formula (1.2.2), since $4 \equiv 1 \pmod 3$, a suitable generator of the cyclic group K_a is 4:

$$(\alpha^4)^2 = \alpha^5, \quad (\alpha^4)^3 = \alpha^6.$$

We can visualize $\langle \alpha \rangle$ as



It is useful to summarize the results in a theorem:

Theorem 1.2.2 *Let a be an element of a semigroup S. Then either:*

(1) *all powers of a are distinct, and the monogenic subsemigroup $\langle a \rangle$ of S is isomorphic to the semigroup $(\mathbf{N}, +)$ of natural numbers under addition; or*

(2) *there exist positive integers m (the* index *of a) and r (the* period *of a) with the following properties:*

   (a) $a^m = a^{m+r}$;
   (b) *for all u, v in $\mathbf{N}^0$, $a^{m+u} = a^{m+v}$ if and only if $u \equiv v \pmod{r}$;*
   (c) $\langle a \rangle = \{a, a^2, \ldots, a^{m+r-1}\}$;
   (d) $K_a = \{a^m, a^{m+1}, \ldots, a^{m+r-1}\}$ *is a cyclic subgroup of $\langle a \rangle$.* □

Nothing that we have said so far makes it clear that for every pair (m, r) of positive integers there does in fact exist a semigroup S containing an element a of index m and period r. This, however, is the case: it is a routine matter to verify that the element

$$a = \begin{pmatrix} 1\ 2\ 3 \ldots & m & m+1 \ldots & m+r-1 & m+r \\ 2\ 3\ 4 \ldots & m+1 & m+2 \ldots & m+r & m+1 \end{pmatrix}$$

of the semigroup $\mathcal{T}_{\{1,2,\ldots,m+r\}}$ has index m and period r.

It is easy to see that if a and b are elements of finite order in the same or in different semigroups, then $\langle a \rangle \simeq \langle b \rangle$ if and only if a and b have the same index and period. The conclusion is that for each (m, r) in $\mathbf{N} \times \mathbf{N}$ there is, up to isomorphism, exactly one monogenic semigroup with index m and period r. We shall feel free to talk of *the monogenic semigroup $M(m, r)$* with index m and period r. Notice that $M(1, r)$ is the cyclic group of order r.