Math 30810 Honors Algebra 3
Homework 6

Andrei Jorza

Due Thursday, October 6

Do any 8 of the following questions. Artin a.b.c means chapter a, section b, exercise c.

1. Explicit Chinese Remainder Theorem.

   (a) Let m and n be coprime integers and let u and v be integers such that $mu+nv=1$ (from Bézout's relation). Show that the system of equations

   $$\begin{cases} x \equiv a \pmod{m} \\ x \equiv b \pmod{n} \end{cases}$$

   has the unique solution $x \equiv anv + bmu \pmod{mn}$.

   (b) Compute

   $$12^{34^{56^{78}}} \pmod{90}$$

   [Hint: Use the Chinese Remainder Theorem.] (A bit on notation: the exponent of 56 is 78, the exponent of 34 is 56^{78}, the exponent of 12 is $34^{56^{78}}$. In particular, this is NOT $((12^{34})^{56})^{78}$.)

Proof. (a) That the solution is unique follows from the bijectivity of $x \mod mn \mapsto (x \mod m, x \mod n)$. Finally, $mu \equiv 1 \pmod{n}$ and $nv \equiv 1 \pmod{n}$ and so $x = anv + bmu \equiv a \pmod{m}$ and $\equiv b \pmod{n}$ as desired.

(b) It suffices to find the residue mod 9, 2 and 5. First, since 12 is even the giant number is also even so $S \equiv 0 \pmod{2}$. Next, $3 \mid 12$ so certainly $9 \mid S$ which means $S \equiv 0 \pmod{9}$. We only need to compute $S \mod 5$. The exponent $34^{56^{78}}$ is certainly a multiple of 4 and so $S \equiv 12^{4k} \equiv (12^4)^k \pmod{5} \equiv 1 \pmod{5}$ because of Fermat's little theorem. So now we know that $S \equiv 0 \pmod{18}$ and $S \equiv 1 \pmod{5}$. Applying part (a) for $5 \cdot 11 - 18cdot3 = 1$ we get $S \equiv 0 \cdot 55 - 1 \cdot 18 \cdot 3 \equiv -54 \equiv 36 \pmod{90}$. ☐

2. Artin 2.9.5 on page 73.

Proof. Let's try to solve the system by hand. From the first equation $y \equiv 2x - 1 \pmod{n}$. Plugging this into the second one we get $10x - 3 \equiv 2 \pmod{n}$ or $10x \equiv 5 \pmod{n}$. Certainly if n is even this cannot be solved as 5 is odd. If n is odd then 2 is invertible mod n so we could even solve $2x \equiv 1 \pmod{n}$ which also satisfies $10x \equiv 5$.

Thus the condition on n is that n be odd. ☐

3. Let p be a prime integer. Show that $(p-1)! \equiv -1 \pmod{p}$. [Hint: There are two ways to do this. Either (a) decompose the polynomial $X^{p-1} - 1 \mod p$ into linear factors or (b) interpret $(p-1)!$ as a product of elements in $(\mathbb{Z}/p\mathbb{Z})^\times$.]

Proof. **Method 1:** From class if $a \in (\mathbb{Z}/p\mathbb{Z})^\times$, $a^{p-1} \equiv 1 \pmod p$ and so every element in $\{1, 2, \dots, p-1\}$ is a root of $X^{p-1} - 1$. Since this is a polynomial of degree $p-1$ these are all the roots and so $X^{p-1} - 1 \equiv (X-1)(X-2)\dots(X-(p-1)) \pmod p$. Subbing $X = 0$ we get $-1 \equiv (-1)(-2)\dots(-(p-1)) = (-1)^{p-1}(p-1)! \pmod p$ which gives $(p-1)! \equiv (-1)^p \pmod p$. This is -1 if p is odd. When $p = 2$ this is 1 but then $1 \equiv -1$ anyway.

Method 2: Note that $x^2 \equiv 1 \pmod p$ is the same as $p \mid x^2 - 1 = (x-1)(x+1)$ so has solutions ± 1. Now $(\mathbb{Z}/p\mathbb{Z})^\times = \{1, 2, \dots, p-1\}$ and we can group these elements in pairs (g, g^{-1}) whenever $g \neq g^{-1}$, i.e., for $g \notin \{-1, 1\}$. So

$$(p-1)! = 1 \cdot (-1) \cdot \prod_{\text{pairs } (g, g^{-1})} g \cdot g^{-1} \equiv -1 \pmod p$$

$\square$

4. Artin 2.12.1 on page 74.

Proof. If H is not normal there exists $g \in G$ and $h \in H$ such that $b^{-1}hb \notin H$. But then pick $a = 1$ so $H \cdot bH$ contains $1 \cdot bH$ so if $aHbH$ were a coset it would have to be bH. But it also contains $hb \cdot 1 = hb \notin bH$. $\square$

5. Artin 2.12.2 on page 75.

Proof. We already know that the set B of upper triangular matrices forms a group and that when you multiply two matrices in B, the diagonal elements simply get multiplied in pairs. This implies that H is a subgroup of B.

Write $n(a, b, c) = \begin{pmatrix} 1 & a & b \\ & 1 & c \\ & & 1 \end{pmatrix}$. The map $n(a, b, c) \mapsto (a, c) \in \mathbb{R} \times \mathbb{R}$ is a surjective group homomorphism. Indeed, $m(a, b, c)m(a', b', c') = m(a + a', b + b' + ac', c + c')$.

Note that the kernel of this homomorphism is exactly K which will then be a normal subgroup of H. By the first isomorphism theorem, $H/K \cong \mathbb{R} \times \mathbb{R}$.

Suppose $m(a, b, c) \in Z(H)$. Then $m(a, b, c)m(a', b', c') = m(a', b', c')m(a, b, c)$ for all a', b', c'. From the formula above this implies that $ac' = a'c$ for all a' and c' and therefore that $a = c = 0$. Thus $K = Z(H)$. $\square$

6. Let n be a positive integer and $G = \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \mid a \in (\mathbb{Z}/n\mathbb{Z})^\times, b \in \mathbb{Z}/n\mathbb{Z} \right\}$ and $H = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \mid b \in \mathbb{Z}/n\mathbb{Z} \right\}$. Show that G is a group under usual matrix multiplication and H is a normal subgroup of G. (The group G will be a Galois group next semester, so this is a useful problem.)

Proof. Write $m(a, b)$ for the first matrix. Then $m(a, b)^{-1} = m(a^{-1}, -a^{-1}b)$ and $m(a, b)m(a', b') = m(aa', ab' + b)$ so G is a group. Consider the map $f : G \to (\mathbb{Z}/n\mathbb{Z})^\times$ given by $f(m(a, b)) = a$. The multiplication formula implies that f is a group homomorphism. Its kernel is exactly H which is therefore a normal subgroup of G. $\square$

7. Let G be a finite group and $g \in G$ not the identity. Show that g has order m if and only if the following two conditions are satisfied:

   (a) $g^m = e$ and

   (b) for every prime divisor $p \mid m$, $g^{m/p} \neq e$.

Proof. Suppose g has order m. Then $m/p < m$ for every prime divisor p of m so certainly $g^{m/p} \neq e$.

Reciprocally, suppose g satisfies the two properties. Then $\operatorname{ord}(g) \mid m$ from the first property. Suppose $\operatorname{ord}(g) < m$. Let p be a prime divisor of $m/\operatorname{ord}(g)$. Then $g^{m/p} = g^{\operatorname{ord}(g)\frac{m}{\operatorname{ord}(g)p}} = e^{\frac{m}{\operatorname{ord}(g)p}} = e$ contradicting the second property. Therefore $\operatorname{ord}(g) = m$. □

8. (We will use this exercise in class so try to do it) Suppose G is an abelian group containing an element g of order p^{k+1} where p is a prime and an element h of order $p^k m$ where $p \nmid m$. Show that $p^{k+1}m \mid \operatorname{ord}(gh)$.

   Proof. Let d be the order of gh. Then $(gh)^d = 1$ implies that $g^d = h^{-d}$ and so from class we deduce that
   $$\frac{p^{k+1}}{(p^{k+1}, d)} = \operatorname{ord}(g^d) = \operatorname{ord}(h^{-d}) = \frac{p^k m}{(p^k m, d)}$$
   Write $d = p^s t$ where $p \nmid t$. If $t \leq k$ then $(p^{k+1}, d) = p^s$ while $(p^k m, d) = p^s(m, t)$. Comparing the two sides we get
   $$p^{k+1-s} = p^{k-s} m/(m, t)$$
   which is impossible as $p \nmid m$. We deduce that $s \geq k+1$ so $(p^{k+1}, d) = p^{k+1}$ and $(p^k m, d) = p^k(m, t)$. Comparing the two sides again we deduce that $1 = m/(m, t)$ so $m \mid t$. This implies that $p^{k+1}m \mid d = \operatorname{ord}(gh)$ as desired. □

9-10 (Counts as two problems) Consider the permutations $a_1 = (12)(34)$, $a_2 = (13)(24)$ and $a_3 = (14)(23)$ in S_4. Let $X = \{a_1, a_2, a_3\}$.

   (a) If $\sigma \in S_4$ show that the inner automorphism $\phi_\sigma(x) = \sigma x \sigma^{-1}$ of S_4 yields a bijective function $\phi_\sigma|_X : X \to X$. I.e., you need to check that ϕ_σ takes X to X and that it is a bijection on X.

   (b) For $\sigma \in S_4$ define the permutation $c_\sigma \in S_3$ such that $\phi_\sigma(a_1) = a_{c_\sigma(1)}$, $\phi_\sigma(a_2) = a_{c_\sigma(2)}$ and $\phi_\sigma(a_3) = a_{c_\sigma(3)}$. Show that the map $q : S_4 \to S_3$ defined by $q(\sigma) = c_\sigma$ is a group homomorphism.

   (c) Show that q is surjective. [Hint: It suffices to show that the image of q contains a transposition and a 3-cycle as we showed in class that S_3 is generated by two such elements.]

   (d) Show that $\ker q = X \cup \{e\}$. [Hint: show that $\ker q$ contains $X \cup \{e\}$ and then use the first isomorphism theorem.]

   (e) Conclude that $\ker q$ is a normal subgroup of order 4 of the alternating group A_4.

   Proof. (a): If σ is a permutation and $c_1 = (i_{1,1}, \ldots, i_{1,k_1})$, ..., $c_r = (i_{r,1}, \ldots, i_{r,k_r})$ are disjoint cycles then
   $$\sigma c_1 \cdots c_r \sigma^{-1} = \prod \sigma c_j \sigma^{-1}$$
   where $\sigma c_j \sigma^{-1} = c_j^\sigma := (\sigma(i_{j,1}), \ldots, \sigma(i_{j,k_j}))$, these conjugate cycles being again disjoint. Indeed, we only need to check that $\sigma c_j = c_j^\sigma \sigma$ take $i_{u,v}$ to the same value. If $u = j$ then $\sigma c_j(i_{j,v}) = \sigma(i_{j,v+1})$ and $c_j^\sigma \sigma(i_{j,v}) = \sigma(i_{j,v+1})$ by definition. If $u \neq j$ then $\sigma c_j(i_{u,v}) = \sigma(i_{u,v})$ whereas $c_j^\sigma \sigma(i_{u,v}) = \sigma(i_{u,v})$ as c_j^σ doesn't do anything to $\sigma(i_{u,v})$ when $u \neq v$.

   So this means that ϕ_σ takes a product of transpositions again to a product of transpositions and therefore ϕ_σ restricts to a function $X \to X$ as desired. Since ϕ_σ is an inner automorphism it is bijective and therefore $\phi_\sigma|_X$ is injective on a set of 3 elements which implies it is also bijective.

   (b): We need to check that $q(\sigma\tau) = q(\sigma)q(\tau)$, i.e., that $c_{\sigma\tau} = c_\sigma c_\tau$. We need therefore show that $a_{c_{\sigma\tau}(i)} = a_{c_\sigma c_\tau(i)}$. But the LHS is simply $\phi_{\sigma\tau}(a_i)$ while the RHS is $\phi_\sigma\phi_\tau(a_i)$ and the equality follows from the fact that $\sigma \mapsto \phi_\sigma$ is a homomorphism from homework 4.

   (c): If $\sigma = (23)$ then from the solution to part (a) we deduce that $\sigma a_1 \sigma^{-1} = a_2$, $\sigma a_2 \sigma^{-1} = a_1$ and $\sigma a_3 \sigma^{-1} = a_3$. Thus $q(\sigma) = (12)$. If $\tau = (123)$ then again we see that ϕ_τ takes a_1 to a_3, a_3 to a_2 and a_2 to a_1 and so $q(\tau) = (132)$. Since $\operatorname{Im} q \subset S_3$ contains (12) and (132) it must contain all of S_3.

(d): By the first isomorphism theorem $|S_4|/|\ker q| = |S_3|$ and so $|\ker q| = 4$. The recipe from the proof of part (a) clearly shows that if $\sigma \in X \cup \{e\}$ then $\phi_\sigma(a_i) = a_i$ and so $X \cup \{e\} \subset \ker q$. Comparing sizes we get that $\ker q$ is exactly $X \cup \{e\}$.

(e): $\ker q$ is normal in S_4 as any kernel is. Moreover, by inspection $\ker q \subset A_4$ as any product of two transpositions is even. Since $\ker q$ is normal in S_4 it is also normal in A_4 (fewer conditions to check). $\square$