Algebra I
Homework 1

Nutan Nepal

September 19, 2022

(1.3 - 13) Show that an element has order 2 in S_n if and only if its cycle decomposition is a product of commuting 2-cycles.

($\Longrightarrow$) Let $x \in S_n,\ n > 1$ be an element that has order 2. If $x(i) = j$ for some i, $j \in \{1, \ldots, n\}$. then since $x^2 = 1$ and we have $x(j) = i$. We see that $(i\ j)$ is a cycle in the cycle decomposition of the permutation x and we can do the same for every other elements of $\{1, \ldots, n\}$. Then the cycle decomposition of x is a product of disjoint 2-cycles. Since the disjoint cycles are also commuting, we have our proof.

($\Longleftarrow$) Let $x = \sigma_1 \cdot \sigma_2 \cdots \sigma_k \in S_n$ where each σ_i is a commuting 2-cycle. Then

$$x^2 = (\sigma_1 \cdot \sigma_2 \cdots \sigma_k)^2 = \sigma_1^2 \cdot \sigma_2^2 \cdots \sigma_k^2 = 1 \cdots 1 = 1$$

Hence x has order 2 in S_n.

(1.4 - 11) Let $H(F) = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \ :\ a, b, c \in F \right\}$ be called the Heisenberg group over F. Let $X = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}$ and $Y = \begin{pmatrix} 1 & d & e \\ 0 & 1 & f \\ 0 & 0 & 1 \end{pmatrix}$ be elements of $H(F)$.

(a) Compute the matrix product XY and deduce that $H(F)$ is closed under matrix multiplication. Exhibit explicit matrices such that $XY \neq YX$ (so that $H(F)$ is always non-abelian).

$XY = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & d & e \\ 0 & 1 & f \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a+d & e+af+b \\ 0 & 1 & f+c \\ 0 & 0 & 1 \end{pmatrix}$. Hence $H(F)$ is closed under matrix multiplication.

Let $X = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ and $Y = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$. Then $XY = \begin{pmatrix} 1 & 1 & 3 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix}$ and $YX = \begin{pmatrix} 1 & 1 & 2 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$. Hence we see that $XY \neq YX$.

(b) Find an explicit formula for the matrix inverse X^{-1} and deduce that $H(F)$ is closed under inverses.

Let Y be the inverse of X with their respective entries from previous exercise. Then

$$a + d = 0,\ f + c = 0,\ e + af + b = 0$$

Solving these equations gives us

$$X^{-1} = \begin{pmatrix} 1 & -a & ac - b \\ 0 & 1 & -c \\ 0 & 0 & 1 \end{pmatrix}$$

Since X^{-1} is also an upper triangular matrix, $H(F)$ is closed under inverses.

(c) Prove the associative law for $H(F)$ and deduce that $H(F)$ is a group of order $|F|^3$. (Do not assume that matrix multiplication is associative.)

Let $Z = \begin{pmatrix} 1 & g & h \\ 0 & 1 & i \\ 0 & 0 & 1 \end{pmatrix}$. Then

$$\begin{aligned}
(XY)Z &= \left[\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & d & e \\ 0 & 1 & f \\ 0 & 0 & 1 \end{pmatrix}\right] \cdot \begin{pmatrix} 1 & g & h \\ 0 & 1 & i \\ 0 & 0 & 1 \end{pmatrix} \\
&= \begin{pmatrix} 1 & a+d & e+af+b \\ 0 & 1 & f+c \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & g & h \\ 0 & 1 & i \\ 0 & 0 & 1 \end{pmatrix} \\
&= \begin{pmatrix} 1 & a+d+g & h+ai+di+e+af+b \\ 0 & 1 & c+f+i \\ 0 & 0 & 1 \end{pmatrix}
\end{aligned}$$

and

$$
\begin{aligned}
X(YZ) &= \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \cdot \left[\begin{pmatrix} 1 & d & e \\ 0 & 1 & f \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & g & h \\ 0 & 1 & i \\ 0 & 0 & 1 \end{pmatrix} \right] \\
&= \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & d+g & h+di+e \\ 0 & 1 & f+i \\ 0 & 0 & 1 \end{pmatrix} \\
&= \begin{pmatrix} 1 & a+d+g & h+ai+di+e+af+b \\ 0 & 1 & c+f+i \\ 0 & 0 & 1 \end{pmatrix}.
\end{aligned}
$$

Hence, $H(F)$ is associative and is a subgroup of $GL_3(F)$. If the order of F is finite. Then for $X \in H(F)$ each $a,\ b,\ c$ has $|F|$ choices. So, $|H(F)| = |F|^3$.

(d) Find the order of each element of the finite group $H(\mathbb{Z}/2\mathbb{Z})$.

There are $2^3 = 8$ elements in the group $H(\mathbb{Z}/2\mathbb{Z})$ which are given below with their orders:

$$e = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad |e| = 1$$

$$x_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}, \quad x_1^2 = e \Longrightarrow |x_1| = 2$$

$$x_2 = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad x_2^2 = e \Longrightarrow |x_2| = 2$$

$$x_3 = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad x_3^2 = e \Longrightarrow |x_3| = 2$$

$$x_4 = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad x_4^2 = e \Longrightarrow |x_4| = 2$$

$$x_5 = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}, \quad x_5^2 = e \Longrightarrow |x_5| = 2$$

$$x_6 = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}, \quad x_6^4 = e \Longrightarrow |x_6| = 4$$

$$x_7 = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}, \quad x_7^4 = e \Longrightarrow |x_7| = 4$$

(e) Prove that every nonidentity element of the group $H(\mathbb{R})$ has infinite order.

First, we show that any n-*th* power of an element in $H(\mathbb{R})$ is given by

$$X^n = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}^n = \begin{pmatrix} 1 & na & \frac{n(n-1)}{2}ac + nb \\ 0 & 1 & nc \\ 0 & 0 & 1 \end{pmatrix}$$

We can prove this by mathematical induction. The statement

$$S(k): \; X^k = \begin{pmatrix} 1 & ka & \frac{k(k-1)}{2}ac + kb \\ 0 & 1 & kc \\ 0 & 0 & 1 \end{pmatrix}$$

is trivial for the base case $k = 1$. Let $S(k)$ be true for some positive integer > 1. Then

$$\begin{aligned} S(k+1): \; X^{k+1} &= \begin{pmatrix} 1 & ka & \frac{k(k-1)}{2}ac + kb \\ 0 & 1 & kc \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & ka + a & b + kac + \frac{k(k-1)}{2}ac + kb \\ 0 & 1 & c + kc \\ 0 & 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & (k+1)a & \frac{k(k+1)}{2}ac + (k+1)b \\ 0 & 1 & (k+1)c \\ 0 & 0 & 1 \end{pmatrix} \end{aligned}$$

Since $S(k) \implies S(k+1)$, the statement $S(k)$ is true for all positive integers.

If $a, \; b, \; c \in \mathbb{R}$ are not all zero then X^n cannot be the identity matrix for any n. Hence every nonidentity element of the group $H(\mathbb{R})$ has infinite order.

(2.1 - 12) Let A be an abelian group and fix some $n \in \mathbb{Z}$. Prove that the following sets are subgroups of A:

(a) $S_1 = \{a^n : \; a \in A\}$

We can prove that $S_1 \neq \phi$ and if $x, y \in S_1$ then $xy^{-1} \in S_1$.

Clearly, $S_1 \neq \phi$ since $1^n = 1 \in S_1$. Let $x = a^n$ and $y = b^n$ are in S_1 for some $a, \; b \in A$. We have $y^{-1} = (b^n)^{-1} = (b^{-1})^n$. Then since A is an abelian group, $xy^{-1} = a^n(b^{-1})^n = (ab^{-1})^n$. The last step here is justified by A being an abelian group. Hence $xy^{-1} \in S_1$ and S_1 is a subgroup of A.

(b) $S_2 = \{a \in A : \ a^n = 1\}$

Clearly $S_2 \neq \phi$ since $1 \in S_2$. If x, $y \in S_2$, then

$$\begin{aligned} (xy^{-1})^n =& x^n \cdot (y^{-1})^n && (1)\\ =& x^n \cdot (y^n)^{-1} && (2)\\ =& 1 \cdot 1 = 1 && (3) \end{aligned}$$

Line 1 here is justified by the fact that A is an abelian group. Hence $xy^{-1} \in S_2$ and S_2 is subgroup.

(2.2 - 10) Let H be a subgroup of order 2 in G. Show that $N_G(H) = C_G(H)$. Deduce that if $N_G(H) = G$ then $H \leq Z(G)$.

Let $H = \{1, x\}$ is a subgroup of order 2 in G. Then for any $g \in N_G(H)$, $gH = Hg$ by definition. Since $gH = \{g, gx\}$ and $Hg = \{g, xg\}$, we must have $xg = gx$ for all $g \in N_G(H)$. So $N_G(H) \subset C_G(H)$. Now, suppose $g \in C_G(H)$, then $g1g^{-1} = 1$ and $gx = xg \implies gxg^{-1} = x$. So $C_G(H) \subset N_G(H)$. Hence $N_G(H) = C_G(H)$.

If $N_G(H) = G$ then $C_G(H) = G$ which means that that every elements of G commutes with the elements of H. Hence $H \leq Z(G)$.

(2.3 - 16) Assume $|x| = n$ and $|y| = m$. Suppose that x and y commute: $xy = yx$. Prove that $|xy|$ divides the least common multiple of m and n. Need this be true if x and y do not commute? Give an example of commuting elements x, y such that the order of xy is not equal to the least common multiple of $|x|$ and $|y|$.

Let p be the least common multiple of m and n. Then

$$\begin{aligned} (xy)^p &= x^p \cdot y^p \quad (\text{since } xy = yx)\\ &= 1 \cdot 1 \quad (\text{since } m,\ n \text{ both divide } p)\\ &= 1 \end{aligned}$$

So the order of xy must divide the lease common multiple p.

This need not be true if x and y do not commute. In S_3, we see that the order of $(1\ 2)$ and $(2\ 3)$ are 2. But $(1\ 2)(2\ 3) = (1\ 2\ 3)$ has order 3 which is not the l.c.m of 2 and 2.

In the abelian group $\mathbb{Z}_{12}$, the order of 2 is 6 and the order of 3 is 4. Here l.c.m of 4 and 6 is 12 but the order of the product $2 \cdot 3 = 6$ is just 2.

(2.3 - 23) Show that $(\mathbb{Z}/2^n\mathbb{Z})^\times$ is not cyclic for any $n \geq 3$. [Find two distinct subgroups of order 2.]

If we show that there exists two distinct subgroups of $(\mathbb{Z}/2^n\mathbb{Z})^\times$ of order 2, then it is enough to prove that $(\mathbb{Z}/2^n\mathbb{Z})^\times$ is not cyclic.

First, we note that in a group $(\mathbb{Z}/2^n\mathbb{Z})^\times$ where $n \geq 3$, $2^n - 1$ and $2^{n-1} - 1$ are distinct elements. Then

$$(2^n - 1)^2 = 2^{2n} - 2 \cdot 2^n + 1 \equiv 1 \mod 2^n$$

and

$$\left(2^{n-1} - 1\right)^2 = 2^{2n-2} - 2 \cdot 2^{n-1} + 1 \equiv 1 \mod 2^n$$

So we see that $2^n - 1$ and $2^{n-1} - 1$ both have order two in $(\mathbb{Z}/2^n\mathbb{Z})^\times$ and $\{1, 2^{n-1} - 1\}$ and $\{1, 2^n - 1\}$ are two distinct subgroups of $(\mathbb{Z}/2^n\mathbb{Z})^\times$. Hence the group $(\mathbb{Z}/2^n\mathbb{Z})^\times$ is not cyclic.

(2.4 - 9) Prove that $SL_2(\mathbb{F}_3)$ is the subgroup of $GL_2(\mathbb{F}_3)$ generated by $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$. [Recall from Exercise 9 of Section 1 that $SL_2(\mathbb{F}_3)$ is the subgroup of matrices of determinant 1. You may assume this subgroup has order 24 - this will be an exercise in Section 3.2.]

We need to show that the subgroup generated by $X = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $Y = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ is equal to the subgroup $SL_2(\mathbb{F}_3)$ of $GL_2(\mathbb{F}_3)$. Clearly, X, $Y \in SL_2(\mathbb{F}_3)$, so $\langle X, Y \rangle \leq SL_2(\mathbb{F}_3)$. Since we can assume that the order of $SL_2(\mathbb{F}_3)$ is 24, we need to only show that $\langle X, Y \rangle$ has more than 12 distinct elements as this would prove that the order of $\langle X, Y \rangle$ is 24 by Lagrange's theorem. We list 13 distinct elements of $\langle X, Y \rangle$ below:

$$X = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad Y = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \quad X^2 = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \quad Y^2 = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$$

$$XY = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} \quad YX = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \quad XYX = \begin{pmatrix} 2 & 0 \\ 1 & 2 \end{pmatrix} \quad YXY = \begin{pmatrix} 2 & 1 \\ 0 & 2 \end{pmatrix}$$

$$(XY)^2 = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} \quad (XY)^3 = \begin{pmatrix} 1 & 2 \\ 2 & 2 \end{pmatrix} \quad X^2Y^2 = \begin{pmatrix} 2 & 2 \\ 2 & 1 \end{pmatrix} \quad X^2Y = \begin{pmatrix} 0 & 2 \\ 1 & 1 \end{pmatrix}$$

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Hence $\langle X, Y \rangle = SL_2(\mathbb{F}_3)$.

(3.1 - 17) Let G be the dihedral group of order 16 (whose lattice appears in Section 2.5):

$$G = \langle r, s : \ r^8 = s^2 = 1, rs = sr^{-1} \rangle$$

and let $\overline{G} = G \backslash \langle r^4 \rangle$ be the quotient of G by the subgroup generated by $\langle r^4 \rangle$ (this subgroup is the center of G, hence is normal).

(a) Show that the order of $\overline{G}$ is 8.

Since $\langle r^4 \rangle = \{1, r^4\}$, $|\langle r^4 \rangle| = 2$. Then by Lagrange's theorem,

$$|\overline{G}| = \frac{|G|}{|\langle r^4 \rangle|} = 8.$$

(b) Exhibit each element of $\overline{G}$ in the form $\overline{s}^a \overline{r}^b$, for some integers a and b.

The elements of $\overline{G}$ are $\overline{1}$, $\overline{r}$, $\overline{r}^2$, $\overline{r}^3$, $\overline{s}$, $\overline{s}\overline{r}$, $\overline{s}\overline{r}^2$, $\overline{s}\overline{r}^3$.

(c) Find the order of each of the elements of $\overline{G}$ exhibited in (b).

$|\overline{1}| = 1$, $|\overline{r}| = 4$, $|\overline{r}^2| = 2$, $|\overline{r}^3| = 4$, $|\overline{s}| = 2$, $|\overline{s}\overline{r}| = 2$, $|\overline{s}\overline{r}^2| = 2$, $|\overline{s}\overline{r}^3| = 2$

(d) Write each of the following elements of $\overline{G}$ in the form $\overline{s}^a \overline{r}^b$, for some integers a and b as in (b): $\overline{rs}$, $\overline{sr^{-2}s}$, $\overline{s^{-1}r^{-1}sr}$.

i. $\overline{rs} = \overline{sr^{-1}} = \overline{sr^7} = \overline{sr^3}$
ii. $\overline{sr^{-2}s} = \overline{ss(r^{-2})^{-1}} = \overline{s^2r^2} = \overline{r^2}$
iii. $\overline{s^{-1}r^{-1}sr} = \overline{ssrr} = \overline{r^2}$.

(e) Prove that $\overline{H} = \langle \overline{s}, \overline{r}^2 \rangle$ is a normal subgroup of $\overline{G}$ and $\overline{H}$ is isomorphic to the Klein 4-group. Describe the isomorphism type of the complete preimage of $\overline{H}$ in G.

Since $\overline{H}$ is generated by the elements of $\overline{G}$, it is a subgroup of $\overline{G}$. We show that, for any $g \in \overline{G}$, $g\overline{H}g^{-1} \subset H$ to prove that $\overline{H}$ is a normal subgroup of $\overline{G}$. It is enough to show that the conjugate of the generators $\{\overline{s}, \overline{r^2}\}$ belong to $\overline{H}$. If $g = \overline{r^k} \in \overline{G}$ for some integer $0 \leq k \leq 3$ then

$$g\overline{s}g^{-1} = \overline{r^k s r^{-k}} = \overline{r^{2k}s} = \overline{(r^2)^k s} \in \overline{H}$$

and

$$g\overline{r^2}g^{-1} = \overline{r^k r^2 r^{-k}} = \overline{r^2} \in \overline{H}.$$

and if $g = \overline{sr^k}$ then

$$g\overline{s}g^{-1} = \overline{sr^k s(sr^k)^{-1}} = \overline{s^2 r^{-k} r^{-k} s^{-1}} = \overline{(r^2)^{-k}s} \in \overline{H}$$

and

$$g\overline{r^2}g^{-1} = \overline{sr^k r^2 (sr^k)^{-1}} = \overline{sr^k r^2 r^{-k} s^{-1}} = \overline{1} \in \overline{H}.$$

Hence $\overline{H}$ is a normal subgroup.

We see that all nonidentity elements of $\overline{H} = \{\overline{1}, \overline{r^2}, \overline{s}, \overline{sr^2}\}$ have order 2. The Klein 4-group is given by

$$V_4 = \langle a, b : \ a^2 = b^2 = (ab)^2 = 1 \rangle.$$

We define a homeomorphism $\varphi : \overline{H} \to V_4$ by $\varphi(\overline{s}) = a$ and $\varphi(\overline{r^2}) = b$. Then we see that φ is an isomorphism.

The complete preimage of $\overline{H}$ are

$$P = \{1, r^2, r^4, r^6, r^8, s, sr^2, sr^4, sr^8\}$$

If we define a homeomorphism $\varphi : P \to D_8$ by $\varphi(r^2) = r$ and $\varphi(s) = s$, we see that it is bijective and hence an isomorphism.

(f) Find the center of $\overline{G}$ and describe the isomorphism type of $\overline{G}/Z(\overline{G})$.

The only element that commutes with $\overline{s}$ is $\overline{r^2}$. We see that $\overline{r^2}$ also commutes with all other elements of $\overline{G}$. So $Z(\overline{G}) = \{1, \overline{r^2}\}$.

The elements of $\overline{G}/Z(\overline{G})$ are $\{\overline{1}, \overline{\overline{r}}, \overline{\overline{s}}, \overline{\overline{sr}}\}$. We see that all the nonidentity elements have order 2 and $|\overline{G}/Z(\overline{G})| = 4$. Hence, $\overline{G}/Z(\overline{G})$ is isomorphic to the Klein 4-group.

(3.2 - 4) Show that if $|G| = pq$ for some primes p and q (not necessarily distinct) then either G is abelian or $Z(G) = 1$. [See Exercise 36 in Section 1.]

If G is abelian, we are done. Suppose that G is not abelian. Since $Z(G)$ is a subgroup and G is not abelian, the order of $Z(G)$ must be either 1, p or q.

We assume that $|Z(G| \neq 1$ and prove that this contradicts with our assumption. Suppose that the order of the center is p. Then since $Z(G)$ is normal, we take $G/Z(G)$ that has the order $|G|/|Z(G)| = pq/p = q$ which is prime. So, $G/Z(G)$ is cyclic.

Let $gZ(G)$ be a generator of the group $G/Z(G)$. Then every coset of $Z(G)$ can be written in the form $g^kZ(G)$ for some integer k. We know that every element of G belongs to some coset of $Z(G)$. Let x, $y \in G$ be written as g^iz_1 and g^jz_2 for z_1, $z_2 \in Z(G)$. Then $xy = g^iz_1g^jz_2 = g^jz_1g^iz_1 = yx$. This shows that G is an abelian group which contradicts our initial assumption. Hence G is abelian or $Z(G) = 1$.

(3.2 - 16) Use Lagrange's Theorem in the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^\times$ to prove Fermat's Little Theorem: if p is a prime then $a^p \equiv a \mod p$ for all $a \in \mathbb{Z}$.

We first note that $|(\mathbb{Z}/p\mathbb{Z})^\times| = p - 1$ by Euler's totient function. Let $p \nmid a$ then $\overline{a} \in (\mathbb{Z}/p\mathbb{Z})^\times$ and by Lagrange's theorem, $|\overline{a}|^{p-1} = 0$. So,

$$a^{p-1} \equiv 0 \mod p.$$

Multiplying both sides by a gives us the desired result. Now, if $p|a$ then $\overline{a} = 0$ and $\overline{a}^p = 0$. So again,

$$a^p \equiv 0 \equiv a \mod p.$$