Solution Sheet 1

Cryptography and Security 2025

Solution 1 Element order

1,2 Check the document "Prerequisites for Cryptography & Security Course ".

3. Assume that a has order k in G and a^{-1} has order k'. Then we have

$$a^k = e$$

and

$$(a^{-1})^{k'} = e,$$

where e is the neutral element in G.

The inverse of a^k is $(a^k)^{-1} = (a^{-1})^k$. But $a^k = e$ so $(a^{-1})^k = e^{-1} = e$. So k must divide k'. Similarly, the inverse of $(a^{-1})^{k'}$ is $a^{k'}$ and we must have $e = a^{k'}$, so k' divides k. Thus, $k = k'$.

Solution 2 Algebra

1. Check the document "Prerequisites for Cryptography & Security Course."

2. From the Little Fermat theorem we have that $a^{p-1} \equiv 1 \pmod{p}$, for a prime p and a coprime with p. In our case 7 is prime. Also $a^i \equiv (a \bmod p)^i \pmod{p}$. Thus $i^6 \equiv 1 \pmod{7}$ for any i that is not a multiple of 7 and $i^6 \equiv 0 \pmod{7}$ for others. We have $\sum_{i=1}^{100} i^6 \bmod 7 \equiv 86 \bmod 7 \equiv 2 \pmod{7}$, as we have 14 multiples of 7 in the set $\{1, \ldots, 100\}$.

Solution 3 Extended Euclidean Algorithm

Firstly, we can find that 23 divides 1081 and 299. Then, we can rewrite the equation as follows.

$$47x + 13y = 1$$

Then, we can apply the extended Euclidean algorithm as follows.

$$\begin{array}{lcll}
(47,1,0) & - & (13,0,1) & \times\ 3 \\
 & \swarrow & & \\
(13,0,1) & - & (8,1,-3) & \times\ 1 \\
 & \swarrow & & \\
(8,1,-3) & - & (5,-1,4) & \times\ 1 \\
 & \swarrow & & \\
(5,-1,4) & - & (3,2,-7) & \times\ 1 \\
 & \swarrow & & \\
(3,2,-7) & - & (2,-3,11) & \times\ 1 \\
 & \swarrow & & \\
(2,-3,11) & - & (1,5,-18) & \times\ 2 \\
 & \swarrow & & \\
(1,5,-18) & & (0,-13,47) &
\end{array}$$

Hence, we can deduce that $(x, y) = (5, -18)$ satisfies the given equation, and $1081 \times -13 + 299 \times 47 = 0$. Hence, the set of (x, y) solutions is

$$\{(x, y) \in \mathbb{Z} \times \mathbb{Z} \mid x = 5 - 13n \text{ and } y = -18 + 47n, \forall n \in \mathbb{Z}\}.$$

(Alternative solution)
Firstly, we can find that 23 divides 1081 and 299. Then, we can rewrite the equation as follows.

$$47x + 13y = 1$$

Then, the (x, y) pairs for which we are looking is the integer solutions of the equation

$$y = -\frac{47}{13}x + \frac{1}{13}$$

From this equation, we can deduce that if $(x, y) = (x_1, y_1)$ is an integer solution of the given equation, then $(x, y) = (x_1 + 13n, y_1 - 47n)$ is also an integer solution of the given equation for all $n \in \mathbb{Z}$. Now, we need to find an integer solution (x_1, y_1). The given equation can be rewritten as follows.

$$y = -3x - \frac{8x - 1}{13}$$

So, x_1 for which we are looking is an integer such that $8x_1 - 1$ is a multiple of 13. Then, we can find an integer solution $(x_1, y_1) = (5, -18)$. Hence, the set of (x, y) solutions is

$$\{(x, y) \in \mathbb{Z} \times \mathbb{Z} \mid x = 5 + 13n \text{ and } y = -18 - 47n, \forall n \in \mathbb{Z}\}.$$

Solution 4 Random variables

1.

$$\begin{aligned}
E[\sum_{i=1}^{n} iX_i] &= \sum_{i=1}^{n} E[iX_i] \\
&= \sum_{i=1}^{n} i \cdot E[X_i] \\
&= \sum_{i=1}^{n} i \cdot (1 \cdot p + i \cdot (1 - p)) \\
&= p \cdot \sum_{i=1}^{n} i + (1 - p) \cdot \sum_{i=1}^{n} i^2 \\
&= p\frac{n(n+1)}{2} + (1 - p)\frac{n(n+1)(2n+1)}{6}
\end{aligned}$$

2.

$$\begin{aligned}
Var[i \cdot X_i] &= i^2\, Var[X_i] \\
&= i^2(E[X_i^2] - E[X_i]^2) \\
&= i^2\left((1^2 \cdot \frac{1}{2} + i^2\frac{1}{2}) - (\frac{1}{2} + i\frac{1}{2})^2\right) \\
&= i^2(\frac{1}{2} + \frac{i^2}{2} - \frac{1}{4} - \frac{i^2}{4} - \frac{i}{2}) \\
&= i^2(\frac{1}{2} - \frac{i}{2})^2
\end{aligned}$$

Solution 5 Expected complexity

1. We see that in every iteration, the algorithm terminates if $x \in \{5, 6\}$. As x is obtained by a die-roll, this occurs with probability $\frac{2}{6} = \frac{1}{3}$. Since every iteration is independent, the number of iterations r is given by a sequence of $r - 1$ unsuccessful rolls ($x \in \{1, 2, 3, 4\}$) followed by a single successful roll ($x \in \{5, 6\}$). This corresponds to geometric distribution with parameter $p = \frac{1}{3}$, and so $E[r] = 1/(1/3) = 3$.

2. If there were r iterations, N was incremented $r-1$ times. Each time, it was incremented by either 1, or by 2 with equal probability. This gives us

$$\begin{aligned} E[N|\ r \text{ iterations}] &= \sum_{i=1}^{r-1} E[\text{increment in } i^{th} \text{ iteration } |r \text{ iterations}] \\ &= \sum_{i=1}^{r-1} (\frac{1}{2} \cdot 1 + \frac{1}{2} \cdot 2) \\ &= (r-1) \cdot \frac{3}{2} \end{aligned}$$