Cryptography and Security 2017

Solution Sheet 1

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 $\{1, \dots, 100\}$.

Solution 3 Fermat numbers

1. $F_m(F_m - 2) = (2^{2^m} + 1)(2^{2^m} - 1) = 2^{2^{m+1}} - 1 = F_{m+1} - 2$. This can be seen as a recurrence relation. We deduce that $F_{m+1} - 2 = F_m(F_m - 2) = F_m F_{m-1}(F_{m-1} - 2) = \ldots = F_m F_{m-1} \cdots F_0$.

2. Assume by contradiction that $\gcd(F_m, F_n) = d$ with $d > 1$. As all the Fermat numbers are odd, d must be odd. Writing the factorization of $d = p_1^{e_1} \cdots p_k^{e_k}$ we can deduce that $p_1 | F_m$ and $p_1 | F_n$. W.l.o.g. we assume that $n < m$. Using the previous results we have that

$$p_1 | F_{m-1} \cdots F_n \cdots F_0 + 2$$

and

$$p_1 | F_n \text{ and thus } p_1 | F_{m-1} \cdots F_n \cdots F_0.$$

This means that $p_1 | 2$. This is a contradiction as d cannot have 2 as a prime factor. Thus, $\gcd(F_m, F_n) = 1$.

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

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