MATH220
Discrete Mathematics and Cryptography

Tutorial 5 **Solutions**

1. (a) (i) Consider the powers of each of the elements of $\mathbb{Z}_{11}^*$.

$$
\begin{aligned}
&1^1 = 1\\
&2^1 = 2,\ 2^2 = 4,\ 2^3 = 8,\ 2^4 = 5,\ 2^5 = 10, \cdots, 2^{10} = 1\\
&3^1 = 3,\ 3^2 = 9,\ 3^3 = 5,\ 3^4 = 4,\ 3^5 = 1\\
&4^1 = 4,\ 4^2 = 5,\ 4^3 = 9,\ 4^4 = 3,\ 4^5 = 1\\
&5^1 = 5,\ 5^2 = 3,\ 5^3 = 4,\ 5^4 = 9,\ 5^5 = 1\\
&6^1 = 6,\ 6^2 = 3,\ 6^3 = 7,\ 6^4 = 9,\ 6^5 = 10, \cdots, 6^{10} = 1\\
&7^1 = 7,\ 7^2 = 5,\ 7^3 = 2,\ 7^4 = 3,\ 7^5 = 10, \cdots, 7^{10} = 1\\
&8^1 = 8,\ 8^2 = 9,\ 8^3 = 6,\ 8^4 = 4,\ 8^5 = 10, \cdots, 8^{10} = 1\\
&9^1 = 9,\ 9^2 = 4,\ 9^3 = 3,\ 9^4 = 5,\ 9^5 = 1\\
&10^1 = 10,\ 10^2 = 1
\end{aligned}
$$

Therefore the order of 1 is 1, the order of 10 is 2, while $3, 4, 5, 9$ each have order 5, and $2, 6, 7, 8$ each have order 10.

Note. Recall that the order of any element divides the number of elements of $\mathbb{Z}_{11}^*$, that is, divides $\phi(11) = 10$. So the possible orders are 1, 2, 5, and 10. It follows that if you have calculated g^1, g^2, g^3, g^4, and g^5 and still have not obtained the value 1, the order must be 10. Knowing this result saves a bit of work!

(ii) The generators of $\mathbb{Z}_{11}^*$ are 2, 6, 7, and 8.

(b)

$$
\begin{aligned}
A &\equiv 2^8 \bmod 11\\
&\equiv 256 \bmod 11\\
&\equiv 3 \bmod 11
\end{aligned}
$$

So Alice sends $A = 3$ to Bob.

(c)

$$
\begin{aligned}
B &\equiv 2^6 \bmod 11\\
&\equiv 64 \bmod 11\\
&\equiv 9 \bmod 11
\end{aligned}
$$

So Bob sends $B = 9$ to Alice.

(d) Alice computes

$$\begin{aligned} K &\equiv B^a \bmod 11 \\ &\equiv 9^8 \bmod 11 \\ &\equiv 3 \bmod 11, \end{aligned}$$

while Bob computes

$$\begin{aligned} K &\equiv A^b \bmod 11 \\ &\equiv 3^6 \bmod 11 \\ &\equiv 3 \bmod 11. \end{aligned}$$

This verifies that their shared key is $K = 3$.

2. (a) Bob enciphers m to

$$\begin{aligned} c &\equiv mK \bmod p \\ &\equiv 5 \times 3 \bmod 11 \\ &\equiv 4 \bmod 11. \end{aligned}$$

So Bob sends $c = 4$.

(b) Alice has to calculate $cK^{-1} \bmod p$, where K^{-1} is the inverse of $K \bmod 11$.

It is clear that with $K = 3$, we have $K^{-1} = 4$ since $3 \times 4 \equiv 1 \bmod 11$. So Alice calculates

$$\begin{aligned} cK^{-1} \bmod p &\equiv 4 \times 4 \bmod 11 \\ &\equiv 5 \bmod 11 \end{aligned}$$

and recovers $m = 5$.

3. (a) $n = 19 \times 13 = 247$

(b) Now $\phi(n) = (19-1)(13-1) = 216$, and so Alice's private key d is the inverse of $e = 5$ in $\mathbb{Z}_{216}$. Using Euclid's Algorithm, we get $d = 173$.

(c) Alice calculates

$$s \equiv 93^{173} \bmod 247.$$

Using fast exponentiation $s = 175$.

4. The easiest way to solve these problems is to run through all possible solutions.

Recall that $x - a$ is a factor of $f(x)$ if and only if $f(a) = 0$ (The Factor Theorem). So run through all values of a in $\{0, 1, 2, \ldots, n-1\}$ to see whether $f(a) = 0$. In this way, we obtain the following:

(a) The roots of $x^2 + 3x + 2$ in $\mathbb{Z}_5[x]$ are 3 and 4. Thus

$$x^2 + 3x + 2 = (x - 3)(x - 4) = (x + 2)(x + 1).$$

(b) The roots of $x^2 + 3x + 2$ in $\mathbb{Z}_7[x]$ are 5 and 6. Thus

$$x^2 + 3x + 2 = (x - 5)(x - 6) = (x + 2)(x + 1).$$

(c) The roots of $x^4 + 4$ in $\mathbb{Z}_5[x]$ are 1, 2, 3, and 4. Thus

$$x^4 + 4 = (x - 1)(x - 2)(x - 3)(x - 4) = (x + 4)(x + 3)(x + 2)(x + 1).$$

5. Putting successively $x = 0, 1, 2, \ldots, 11$, we find that if $x \in \{2, 7, 10, 11\}$, then $f(x) = 0$ but, if $x \in \{0, 1, 3, 4, 5, 6, 8, 9\}$, then $f(x) \neq 0$. So the roots of $f(x)$ in $\mathbb{Z}_{12}[x]$ are 2, 7, 10, 11. This gives two distinct factorisations:

$$f(x) = (x - 2)(x - 7) = (x + 10)(x + 3)$$

and

$$f(x) = (x - 10)(x - 11) = (x + 2)(x + 1).$$

By Corollary 6.7, if p is prime, then a polynomial of degree two in $\mathbb{Z}_p[x]$ has at most two roots, and thus a unique factorisation. But if m is composite, then a polynomial of degree two in $\mathbb{Z}_m[x]$ may have more than two roots and thus more than one factorisation.