Problem 1. Euler's totient

1. For any prime p, in $G = \mathbb{Z}/p^n\mathbb{Z}$, there are p^{k-1} elements non-invertible, that is, $p, 2p, ..., p^{k-1}p$. All the other elements are cannot be the factor of prime p, since there are p^k elements in the group, we have $\varphi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1)$

2. Given coprime m, n, we have a ring isomorphism derived from CRT.

$$\mathbb{Z}/n\mathbb{Z} \approx \prod_i \mathbb{Z}/p_i^{e_i}\mathbb{Z}$$

$$\mathrm{U}(\mathbb{Z}/mn\mathbb{Z}) \approx \mathrm{U}(\mathbb{Z}/m\mathbb{Z})\mathrm{U}(\mathbb{Z}/n\mathbb{Z})$$

   We know that $\mathrm{U}(\mathbb{Z}/mn\mathbb{Z})$ is bijective toward $\mathrm{U}(\mathbb{Z}/m\mathbb{Z})\mathrm{U}(\mathbb{Z}/n\mathbb{Z})$ due to the linearity. Since $\phi(n)$ represents the number of invertible elements, which is $|U|$, we can conclude that $\varphi(mn) = \varphi(m)\varphi(n)$.

3. Let $p|n$, let $n = p_1^{e_1}p_2^{e_2}\cdots p_k^{e_k}$ where p_i is the prime factor of p. Then we have

$$\begin{aligned}
\varphi(n) &= \varphi(p_1^{e_1})\varphi(p_2^{e_2})\cdots\varphi(p_k^{e_k}) \\
&= p_1^{e_1-1}(p_1-1)p_2^{e_2-1}(p_2-1)\cdots p_k^{e_k-1}(p_k-1) \\
&= p_1^{e_1}p_2^{e_2}\cdots p_k^{e_k}\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_k}\right) \\
&= n\prod_{p|n}\left(1-\frac{1}{p}\right)
\end{aligned}$$

4. To get the last three digits, we apply mod 1000 to 7^{803}

$$\begin{aligned}
7^{803} \bmod 1000 &= 7^{803 \bmod \varphi(1000)} \bmod 1000 \\
&= t^{803 \bmod 1000\left(1-\frac{1}{2}\right)\left(1-\frac{1}{5}\right)} \bmod 1000 \\
&= 7^{803 \bmod 400} \bmod 1000 \\
&= 7^3 \bmod 1000 \\
&= 343
\end{aligned}$$

Problem 2. AES

1. In round 1, we will use K(4) to K(7).
   $K(4) = K(0) \oplus T(K(3))$, we will calculate the transformation T(K(3)). First we have $r(4) = (00000001)$, then we apply cyclical top shift by 1, which have no effect on 11111111. After that, we apply subByte layer. By looking up S-box we have key become 00010110. Thus we have

$$\begin{aligned}
T(K(3)) &= (00010110 \oplus 00000001, 00010110, 00010110, 00010110) \\
&= (00010111, 00010110, 00010110, 00010110) \\
&= (a, b, c, d)
\end{aligned}$$

And finally we have

$$K(4) = (11101000, 11101001, 11101001, 11101001)$$

For $K(5)$ to $K(7)$, it's simple to find out.

$$K(5) = K(1) \oplus K(4) = (00010111, 00010110, 00010110, 00010110)$$
$$K(6) = K(2) \oplus K(5) = (11101000, 11101001, 11101001, 11101001)$$
$$K(7) = K(3) \oplus K(6) = (00010111, 00010110, 00010110, 00010110)$$

2. According to the result we just found out, we could simply wrote out

$$K(5) = \overline{K(4)}$$

3. K(2) and K(3) are composed of all 1s, thus $x \oplus K(2) = \overline{x}$

$$\begin{aligned} K(10) &= K(6) \oplus K(9) \\ &= K(5) \oplus K(2) \oplus K(8) \oplus K(5) \\ &= K(2) \oplus K(8) \\ &= \overline{K(8)} \end{aligned}$$

$$\begin{aligned} K(11) &= K(7) \oplus K(10) \\ &= K(3) \oplus K(6) \oplus K(6) \oplus K(9) \\ &= K(3) \oplus K(9) \\ &= \overline{K(9)} \end{aligned}$$

Problem 3. Simple questions

1. For ECB, each cipher block is separate with a function E and a key K. That is to say, if one block is corrupted, only one block will be influenced and decrypted incorrectly. For CBC mode, the encrypted result will xor the next plaintext before the encryption. So if one block is corrupted (except for the last one), It will influence this corrupted block and also the next block when doing xor. For instance, if ciphertext C_{n-1} is corrupted, the only two messages being affected are m_n and m_{n-1}.

$$C_{n-1}^{-1} \oplus C_{n-2} = m_{n-1}$$

$$C_n^{-1} \oplus C_{n-1} = m_n$$

2. By applying CPA, the attacker could keep sending the same plaintext, then he could get the value of IV from ciphertext since IV keep increasing by 1. After the attacker gets IV, he could choose arbitrary plaintext and xor with IV to obtain the encrypted value, thus such kind of IV method isn't CPA secure.

3. Given $p = 29$ is a prime, we find prime factors 2, 7 of $p - 1 = 28$.

$$\alpha^{(p-1)/q} = 2^{14} \equiv 28 \bmod 29$$
$$\alpha^{(p-1)/q} = 2^{4} \equiv 16 \bmod 29$$

Since for all factors $\alpha^{(p-1)/q} \neq 1 \bmod p$, we confirm 2 is a generator of $\mathrm{U}(\mathbb{Z}/29\mathbb{Z})$.

4.

$$\begin{aligned}
\left(\frac{1801}{8191}\right) &= (\frac{8191}{1801}) = (\frac{987}{1801}) \\
&= (\frac{3}{1801})(\frac{7}{1801})(\frac{47}{1801}) = (\frac{1801}{3})(\frac{1801}{7})(\frac{1801}{47}) \\
&= (\frac{1}{3})(\frac{2}{7})(\frac{15}{47}) = (\frac{15}{47}) = (\frac{3}{47})(\frac{5}{47}) \\
&= (\frac{47}{5})(-(\frac{47}{3})) \\
&= -(\frac{2}{5})(\frac{2}{3}) \\
&= -(-1)(-1) = -1
\end{aligned}$$

5. For the given equation, we have solutions

$$-\frac{b \pm \sqrt{b^2 - 4ac}}{2a} \equiv x \bmod p$$
$$\sqrt{b^2 - 4ac} \equiv \pm(2ax + b) \bmod p$$

Then we have to find out is $b^2 - 4ac$ a square mod p, we write $\left(\frac{b^2-4ac}{p}\right)$

(a) If $p|b^2-4ac$, $\left(\frac{b^2-4ac}{p}\right) = 0$, there is only one solution and we have $1+\left(\frac{b^2-4ac}{p}\right) = 1$

(b) If $\left(\frac{b^2-4ac}{p}\right) = 1$, then $b^2 - 4ac$ is a square mod p, there are two solutions, and we have $1 + \left(\frac{b^2-4ac}{p}\right) = 1 + 1 = 2$

(c) If $\left(\frac{b^2-4ac}{p}\right) = -1$, then $b^2 - 4ac$ is not a square mod p, there are no solutions, and we have $1 + \left(\frac{b^2-4ac}{p}\right) = 1 - 1 = 0$

Hence, we conclude the number of solutions mod p to the equation $ax^2 + bx + c$ is

$$1 + \left(\frac{b^2 - 4ac}{p}\right)$$

6. According to Euler's Theorem, we have

$$n^{p-1} \equiv 1 \mod p$$

$$n^{q-1} \equiv 1 \bmod q$$

Given $p-1|q-1$, let $p-1 = k(q-1)$, then we have

$$(n^{q-1})^k = n^{p-1} \equiv 1 \bmod q$$

Since p, q are primes and $\gcd(n, pq) = 1$, Chinese Reminder Theorem gives

$$n^{p-1} \equiv 1 \bmod pq$$

7. Given $p \equiv 1 \mod 3$, and p is an odd prime, we first show the sufficiency

   (a) If $p \equiv 1 \bmod 4$, then

   $$\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = 1 \cdot \left(\frac{p}{3}\right) = 1 \cdot \frac{1}{3} = 1$$

   (b) If $p \equiv 3 \bmod 4$, then

   $$\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = (-1) \cdot \left(-\left(\frac{p}{3}\right)\right) = \frac{1}{3} = 1$$

   Next, we show the necessity. Given $\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = 1$.

   (a) If $p \equiv 1 \bmod 4$,since -1 is a square of p, $\left(\frac{3}{p}\right) = 1$. Since $p \not\equiv 3 \bmod 4$, $\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right) = 1$, we have $p \equiv 1 \bmod 3$

   (b) If $p \equiv 3 \bmod 4$, $\left(\frac{-1}{p}\right) = -1$, $\left(\frac{3}{p}\right) = -1$. Since $p \equiv 3 \bmod 4$, $\left(\frac{3}{p}\right) = -\left(\frac{p}{3}\right) = -1$. We then have $\left(\frac{p}{3}\right) = 1$ and $p \equiv 1 \bmod 3$

   In conclusion, we have proved $p \equiv 1 \bmod 3$

8. Given $\left(\frac{a}{p}\right) = 1$, we know a is a square mod p, we write it as

   $$a^{\frac{p-1}{2}} \equiv 1 \bmod p$$

   To make a a generator of $\mathbb{F}_p$, we need to satisfy for all primes q such that $q|(p-1)$, $a^{\frac{p-1}{q}} \neq 1 \bmod p$, since 2 is proven to be a factor, a cannot be a generator.

Problem 4. Prime vs. irreducible

1. For any prime element in an integral domain, let's say p, if it is reducible, let $p = ab$, where a, b are non-zero, non-invertible and not equal to the ring identity 1.
   Since we have $p \mid (xy)$. Let $x = k_1 a$, $y = k_2 b$, $k_1, k_2 \neq 0$, so $x, y \neq 0$.
   When $b \nmid k_1$ and $a \nmid k_2$, we have $ab \nmid k_1 a$ and $ab \nmid k_2 b$, which means $p \nmid x$ and $p \nmid y$.
   There exists a contradiction with (*), thus we conclude any prime element is irreducible in an integral domain.

2. Suppose there is an irreducible number p is not prime in $\mathbb{Z}$. We may find one factor $a \in \mathbb{Z}$ of p, and according to (**), since $a \mid p$, $a \neq 1, a \neq p$, it implies that there exist $p = ab$, which means p is reducible, which leads to contradiction. Therefore, any irreducible integer in $\mathbb{Z}$ is a prime.

3. Suppose (**) is true, we have $p > 1$ and $a|p$ implies $a = 1$ or $a = p$. We know p is a prime and assume there exist x, y, where $p|(x \cdot y)$ and $p \nmid x, p \nmid y$. From (**) we have $p = ab$, where $a \mid x, b \mid y$, and $a, b \neq p, a, b \neq 1$.
Therefore, we have $a \mid p$, where $a \neq 1$ and $a \neq p$, which leads to contradiction. Hence we can conclude that (**) implies (*).

4. (*) basically says all prime integers are irreducible. (**) says for all $a|p$, we have $a = 1$ or $a = p$, which is implied by (*). As we've shown that (**) also implies (*), therefore, we conclude (*) and (**) are equivalent for integers.

Problem 5. Primitive root mod 65537

1. $$\left(\frac{3}{65537}\right) = \left(\frac{65537}{3}\right) = \left(\frac{2}{3}\right) = -1$$

2. Let $3^{32768} \equiv 1 \mod 65537$, which is equivalent to $3^{2^{15}} \equiv 1 \mod 2^{16} + 1$, and then we have $k3^{2^{15}} + 1 = 2^{16} + 1$, which is $3^{(65537-1)/2} | 2^{16}$. However, this equation cannot be established since $3^{2^{15}}$ only has one prime factor 3, when 2^{16} has only one prime factor which is 2, and 3 is co-prime with 2. Therefore, the assumption is contradicted and $3^{32768} \neq 1 \mod 65537$.

3. For $65537 - 1 = 65536 = 2^{16}$, we find it has one prime factor 2. And based on the theorem of finding primitive elements, given

   $$3^{(65537-1)/2} \not\equiv 1 \mod 65537$$

   3 has satisfied the form $\alpha^{(p-1)/q} \neq 1 \mod p$ for all the prime factors q, therefore we find tha 3 is a primitive root.