VE475 Homework 4

Yiwen Yang

Ex.1 - Euler's Totient

1. Euler's totient function $\varphi(p^k)$ counts the invertible elements in $\mathbb{Z}/p^k\mathbb{Z}$, that is to find number of elements that are coprime with p^k. Since p is prime, then to have a common divisor with p^k is to have a factor of p. In this set, $p, 2p, \ldots, (p^{k-1}-1)p$ are not coprime with p^k, which contains $p^{k-1}-1$ elements. So $\varphi(p^k) = p^k - 1 - (p^{k-1}-1) = p^{k-1}(p-1)$.

2. Given m is coprime with n, according to Chinese Remainder Theorem, there exists a ring isomorphism between $\mathbb{Z}/mn\mathbb{Z}$ and $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$. Since there is a bijection between two sets, the invertible element count should be the same, so $\varphi(mn) = \varphi(m) varphi(n)$.

3. Factorize n and let

$$n = \prod_i p_i^{k_i}$$

Where p_i are all different primes. Then

$$\begin{aligned}
\varphi(n) &= \prod_i \varphi(p_i^{k_i}) \\
&= \prod_i p_i^{k_i - 1}(p_i - 1) \\
&= \prod_i p_i^{k_i}(1 - \frac{1}{p_i}) \\
&= n \prod_i (1 - \frac{1}{p_i})
\end{aligned}$$

4. 7 is coprime with 1000, and $\varphi(1000) = 1000 \times (1 - \frac{1}{2}) \times (1 - \frac{1}{5}) = 400$. According to Euler's Theorem, $7^{400} \equiv 1 \bmod 1000$. Then $7^{803} \equiv 7^3 \equiv 343 \bmod 1000$, so the last three digits of 7^{803} is 343.

Ex.2 - AES

1. 128 bits of 1

2. $K(5) = K(1) \oplus K(4)$

3. To `xor` a number with all ones is to bit-wise `not` the number. Since $K(0) = K(1) = K(2) = K(3) = 111\ldots1$, then

$$\begin{aligned}
K(5) &= K(1) \oplus K(4) = \overline{K(4)} \\
K(6) &= K(2) \oplus K(5) = \overline{K(5)} \\
K(7) &= K(3) \oplus K(6) = \overline{K(6)} \\
\\
K(9) &= K(5) \oplus K(8) = \overline{K(6)} \\
K(10) &= K(6) \oplus K(9) \\
&= K(6) \oplus K(5) \oplus K(8) \\
&= \overline{K(5)} \oplus K(5) \oplus K(8) \\
&= K(1) \oplus K(8) \\
&= \overline{K(8)} \\
\\
K(11) &= K(7) \oplus K(10) \\
&= \overline{K(6)} \oplus K(6) \oplus K(9) \\
&= K(1) \oplus K(9) \\
&= \overline{K(9)}
\end{aligned}$$

Ex.3 - Simple Questions

1. **ECB mode** All blocks are decrypted independently, so if one of the cipher blocks is corrupted, only the corresponding decrypted plain text block will be incorrect.
   CBC mode Each cipher block is used both in current block of decryption and also in next block of decryption as IV (xor with next deciphered block), so two output blocks will be broken if one of the cipher blocks is corrupted.

2. If IV is incremented by 1 each time, it is very likely that a list of successive plain text messages begin with the same word (e.g. "SSID = 123456", "SSID = 001122", ...). Then Eve may observe a same pattern in all first blocks, or two different messages share the same headings, which is leaking much information. If Eve can apply CPA, he may find out which part of bits changes accordingly and predict the first block of plain text when next cipher message is sent by others.

3. 29 is prime, and 28 has two prime factors 2 and 7. Test

$$\begin{aligned} 2^{28/2} = 2^{14} \equiv 12^2 \equiv 28 \neq 1 \bmod 29 \\ 2^{28/7} = 2^4 \equiv 16 \neq 1 \bmod 29 \end{aligned}$$

So 2 is a generator of $U(\mathbb{Z}/29\mathbb{Z})$.

4.

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

5. The number of solutions to the equation depends on $b^2 - 4ac$.

   (a) $b^2 - 4ac = 0$
   The equation has only one solution, and $1 + (\frac{0}{p}) = 1$.

   (b) $b^2 - 4ac > 0$
   The equation has two different solutions.

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

   So $b^2 - 4ac$ is a square mod p, $1 + (\frac{b^2-4ac}{p}) = 2$.

   (c) $b^2 - 4ac < 0$
   The equation has zero solutions, and b^2-4ac is not a square mod p, $1+(\frac{b^2-4ac}{p}) = 0$.

   Then we can conclude that number of solutions mod p is $1 + (\frac{b^2-4ac}{p})$.

6. Given p, q are primes, then

$$\begin{aligned} n^{p-1} &\equiv 1 \bmod p \\ n^{q-1} &\equiv 1 \bmod q \\ cp + dq &= 1 \end{aligned}$$

Since $q - 1 \mid p - 1$, so

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

According to Chinese Remainder Theorem, if $gcd(n, pq) = 1$, then

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

7. (a) If $(\frac{-3}{p}) = 1$, since p is prime, then $(\frac{-1}{p})(\frac{3}{p}) = (-1)^{\frac{p-1}{2}}(\frac{3}{p}) = 1$.

   When $p \equiv 1 \bmod 4$, $(\frac{-1}{p}) = 1$. Then $(\frac{3}{p}) = (\frac{p}{3}) = 1$, which implies $p \equiv 1 \bmod 3$.

   When $p \equiv 3 \bmod 4$, $(\frac{-1}{p}) = -1$. Then $(\frac{3}{p}) = -(\frac{p}{3}) = -1$, which implies $p \equiv 1 \bmod 3$.

   So $p \equiv 1 \bmod 3$.

   (b) If $p \equiv 1 \bmod 3$, then $(\frac{p}{3}) = 1$.

   When $p \equiv 1 \bmod 4$, $(\frac{3}{p}) = (\frac{p}{3}) = 1$. Then $(\frac{-3}{p}) = (\frac{-1}{p})(\frac{3}{p}) = 1$.

   When $p \equiv 3 \bmod 4$, $(\frac{3}{p}) = -(\frac{p}{3}) = -1$. Then $(\frac{-3}{p}) = (\frac{-1}{p})(\frac{3}{p}) = 1$.

   So $(\frac{-3}{p}) = 1$.

   So $(\frac{-3}{p}) = 1$ if and only if when $p \equiv 1 \bmod 3$.

8. If $(\frac{a}{p}) = 1$, then $a^{(p-1)/2} \equiv 1 \bmod p$, and 2 is a factor of $p - 1$. Then a cannot be a generator of p.

Ex.4 - Prime vs. Irreducible

1. Suppose that p is not irreducible, *i.e.*, $p = ab$ where a, b are non-zero, non-unit, non-invertible different elements. Then obviously, $ab \mid ab$, so according to (*), this implies $ab \mid a$ or $ab \mid b$. If $ab \mid a$, then $b = 1$, which contradicts. Similarly, $ab \mid b$ also not holds. So (*) indicates that p is irreducible.

2. Suppose that a is neither 1 nor p, then a is a factor of p, which means that p is irreducible, which contradicts. So irreducible indicates (**).

3. (**) indicates that if p is prime (**), then it is irreducible. Suppose $p \nmid x$ and $p \nmid y$, then $p \nmid xy$, so (*) must hold.

4. From (1) and (2) we can conclude that (*) implies (**), and from (3) (**) implies (*). So (*) and (**) are equivalent.

Ex.5 - Primitive Root Mod 65537

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

2. $(\frac{3}{65537}) = 3^{32768} \equiv -1 \not\equiv 1 \bmod 65537$

3. Since 65537 is prime, and the factor of 65536 is 2, which satisfies that $3^{(65537-1)/2} \not\equiv 1 \bmod 65537$. So 3 is a generator of 65537.