VE475 Homework 4

Liu Yihao 515370910207

Ex. 1 — Euler's totient

1. Suppose
$$\varphi(p^k) = p^{k-1}(p-1) = p^k - p^{k-1}$$
which means, there are p^{k-1} integers of $n \in [1, p^k]$ so that
$$\gcd(n, p^k) > 1$$
What's more, if an integer and p^k is not coprime, it can be divided by p since all of prime factors of p^k are p.

   When $k = 1$, we know $\varphi(p) = p - 1$ since p is a prime.

   When $k = i$, suppose $\varphi(p^i) = p^i - p^{i-1}$.

   When $k = i + 1$, we know that there are p^{i-1} integers in $[1, p^i]$ which are not coprime with p^i, so they are also not coprime with p^{i+1}. Then consider the integers $n \in [p^i + 1, p^{i+1}]$ which are not coprime with p^{i+1}, we know that they all have a prime factor p, and $n/p \in [p^{i-1} + 1, p^i]$, so there are $(p-1)p^{i-1}$ integers that satisfy this condition. In total, there are $p^{i-1} + (p-1)p^{i-1} = p^i$ integers which are not coprime with p^{i+1}, so $\varphi(p^{i+1}) = p^{i+1} - p^i$.

   According to the mathematical induction above, we can concluded that
$$\varphi(p^k) = p^{k-1}(p-1)$$

2. According to the Chinese Reminder Theorem, since m and n are coprime, there exists a ring isomorphism between Z/mnZ and $Z/mZ \times Z/nZ$, and here $\varphi(mn)$ is the order of Z/mnZ, $\varphi(m)$ is the order of Z/mZ and $\varphi(n)$ is the order of Z/nZ. Suppose MN is the set of counted integers in $\varphi(mn)$, M is that in $\varphi(M)$ and N is that in $\varphi(N)$, there is a bijection between MN and $M \times N$. So $\varphi(mn) = \varphi(m)\varphi(n)$.

3. Suppose
$$n = p_1^{k_1} p_2^{k_2} \cdots p_n^{k_n}$$
where $p_1, p_2, \cdots, p_n$ are primes and $k_1, k_2, \cdots, k_n \geqslant 1$, it is obvious that $p_1^{k_1}, p_2^{k_2}, \cdots, p_n^{k_n}$ are pairwise coprime, so
$$\begin{aligned}
\varphi(n) &= \varphi(p_1^{k_1})\varphi(p_n^{k_n}) \cdots \varphi(p_n^{k_n}) \\
&= p_1^{k_1-1}(p_1 - 1)p_2^{k_2-1}(p_2 - 1) \cdots p_n^{k_n-1}(p_n - 1) \\
&= p_1^{k_1}\left(1 - \frac{1}{p_1}\right) p_2^{k_2}\left(1 - \frac{1}{p_2}\right) \cdots p_n^{k_n}\left(1 - \frac{1}{p_n}\right) \\
&= n \prod_{p|n}\left(1 - \frac{1}{p}\right)
\end{aligned}$$

4. $$\varphi(1000) = 1000\left(1-\frac{1}{2}\right)\left(1-\frac{1}{5}\right) = 400$$

   According to Euler's Theorem, since 7 is coprime with 1000,

   $$7^{400} \equiv 1 \bmod 1000$$

   $$\begin{aligned} 7^{803} &\equiv 7^3 \bmod 1000 \\ &\equiv 343 \bmod 1000 \end{aligned}$$

Ex. 2 — AES

1. 128 bits of 1 is used as the key for round 1.
2. $$K(5) = K(4) \oplus K(1)$$
3. We know for a 4 bit number X,

   $$X \oplus 1111 = \overline{X}$$

   We also know

   $$K(0) = K(1) = K(2) = K(3) = 1111$$

   So it's easy to find

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

Ex. 3 — Simple Questions

1. In ECB Mode, each block is encrypted separately with a function E and a key K, so the corruption of one block won't influence other blocks, only one block will be decrypted incorrectly.

   In CBC Mode, \
2.
3. Since $p = 29$ is a prime, according to Theorem 2.17, we can test the prime factors of $p-1 = 28$, which are 2 and 7.

   First, when $q = 2$,

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

Second, when $q = 7$,
$$2^{(p-1)/q} = 2^{28/7} = 2^4 \equiv 16 \bmod 29$$
So
$$2^{(p-1)/d} \not\equiv 1 \bmod p$$
We can concluded that 2 is a generator of $U(Z/29Z)$.

4. Since 1801 and 8191 are primes, it is a Legendre Symbol, and we can only directly calculate $1801^{4095} \bmod 8191$ to solve it.

   By applying modular exponentiation, we get the following table.

i	d_i	power mod 8191
11	1	$1^2 \cdot 1801 \equiv 1801$
10	1	$1801^2 \cdot 1801 \equiv 2493$
9	1	$2493^2 \cdot 1801 \equiv 6873$
8	1	$6873^2 \cdot 1801 \equiv 7874$
7	1	$7874^2 \cdot 1801 \equiv 544$
6	1	$544^2 \cdot 1801 \equiv 557$
5	1	$557^2 \cdot 1801 \equiv 1193$
4	1	$1193^2 \cdot 1801 \equiv 4482$
3	1	$4482^2 \cdot 1801 \equiv 6085$
2	1	$6085^2 \cdot 1801 \equiv 5027$
1	1	$5027^2 \cdot 1801 \equiv 4046$
0	1	$4046^2 \cdot 1801 \equiv 8190$

$$1801^{4095} \equiv 8190 \bmod 8191$$
$$\left(\frac{1801}{8191}\right) = -1$$

5. First, if $\left(\frac{b^2-4ac}{p}\right) = 0$, then $b^2 - 4ac = 0$, so the equation only have one solution $x = -\frac{b}{2a}$, and it can always mod p, thus the number of solutions satisfies $1 + \left(\frac{b^2-4ac}{p}\right) = 1$.

   Second, if $\left(\frac{b^2-4ac}{p}\right) \neq 0$, then $b^2 - 4ac \neq 0$, the equation have two solutions $x = -\frac{b\pm\sqrt{b^2-4ac}}{2a}$, which means
$$-\frac{b \pm \sqrt{b^2 - 4ac}}{2a} \equiv x \bmod p$$
$$\sqrt{b^2 - 4ac} \equiv \pm(2ax + b) \bmod p$$
   Then the problem becomes whether $b^2 - 4ac$ is a square mod p.

   If $\left(\frac{b^2-4ac}{p}\right) = 1$, $b^2 - 4ac$ is a square mod p, and we can get 2 solutions mod p.

   Otherwise, $\left(\frac{b^2-4ac}{p}\right) = -1$, $b^2 - 4ac$ is not a square mod p, and we can get no solution mod p.

   In conclusion, 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,

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

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

Let $(p-1) = k(q-1)$,

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

Since $\gcd(n, pq) = 1$, according to Chinese Reminder Theorem, we get

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

7. If $\left(\frac{-3}{p}\right) = 1$,

$$1 \equiv (-3)^{(p-1)/2} \bmod p$$

$$1 \equiv 3k \bmod p, k \in Z$$

If $p \equiv 1 \bmod 3$, and p is an odd prime, then $p \equiv 1 \bmod 6$.

$$x \equiv (-3)^{(p-1)/2} \bmod p$$

$$x^2 \equiv 1 \bmod p$$

And we know $(-3)^{(p-1)/2} = 3k$, $k \in Z$, so

$$x \equiv 3k \bmod p$$

8.

Ex. 4 — Prime vs. irreducible

Ex. 5 — Primitive root mod 65537

1. Since 65537 is a prime, we can calculate $3^{32768} \bmod 65537$ and we can find that $3^{32768} \equiv -1 \bmod 65537$ (The calculation is shown in part 2), so

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

2. By applying modular exponentiation, we get the following table.

i	d_i	power mod 65537
15	1	$1^2 \cdot 3 \equiv 3$
14	0	$3^2 \equiv 9$
13	0	$9^2 \equiv 81$
12	0	$81^2 \equiv 6561$
11	0	$6561^2 \equiv 54449$
10	0	$54449^2 \equiv 61869$
9	0	$61869^2 \equiv 19139$
8	0	$19139^2 \equiv 15028$
7	0	$15028^2 \equiv 282$
6	0	$282^2 \equiv 13987$
5	0	$13987^2 \equiv 8224$
4	0	$8224^2 \equiv 65529$
3	0	$65529^2 \equiv 64$
2	0	$64^2 \equiv 4096$
1	0	$4096^2 \equiv 65281$
0	0	$65281^2 \equiv 65536$

So

$$3^{32768} \equiv 65536 \bmod 65537$$

$$3^{32768} \not\equiv -1 \bmod 65537$$

3. According to Theorem 2.17, we can conclude that 3 is a primitive root mod 65537 because 2 is the only prime factor of 65536 and $3^{(65537-1)/2} \not\equiv 1 \bmod 65537$.