VE475 Homework4

Anna Li
Student ID: 518370910048

Ex. 1

1.

Since p is a prime, only when $x = np, n \in \mathbb{Z}, gcd(p^k, x) \neq 1$.
Therefore, for all $x \neq np, n \in \mathbb{Z}$, x is invertible
Hence$\phi(p^k) = p^k/p * (p-1) = p^{k-1}(p-1)$

2.

Since According to CRT, there exists a ring isomorphism. And since

$$U(\mathbb{Z}/n\mathbb{Z}) \approx U(\prod_i \mathbb{Z}/p_i^{e^i}\mathbb{Z})$$

We could conclude according to the 12page of c3 that

$$\phi(mn) = \phi(m)\phi(n)$$

3.

for every n, we could factorize it into $n = p_1^{a_1}p_2^{a_2}...p_n^{a_n}$, in which p is prime, Therefore, each $p_n^{a_n}$is coprime from each other.

$$\Rightarrow \phi(n) = \phi(p_1^{a_1})\phi(p_2^{a_2})...\phi(p_n^{a_n}) = p_1^{a_1-1}(p_1-1)p_2^{a_2-1}(p_2-1)...p_m^{a_n-1}(p_n-1)$$

$$\Rightarrow = n * (p_1-1)/p_1 * (p_2-1)/p_2 * ... * (p_n-1)/p_n = n\prod_{p|n}(1-\frac{1}{p})$$

4.

since 7 is coprime with 1000, and

$$\phi(1000) = 1000 * (1-\frac{1}{2})(1-\frac{1}{5}) = 400$$

$$7^{803} \mod 1000 = 7^{400*2+3} \mod 1000 = 7^3 \mod 1000 = 343$$

Ex.2

1.

128 bits of 1

2.

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

3.

Since X,

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

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

Therefore,

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

Ex.3

1.

This is because for ECB, one block cyphertext is only used for one block when decrypting, but for CBC, one block cyphertext will be used twice in two blocks when decrypting.

2.

If we use CBC mode with IV incremented by 1 each time, for CPA secure, the attacker could get the value of IV, then they will know all the value of plaintext in following rounds.

3.

Since 2 is coprime with 29, $\alpha \in U(\mathbb{Z}/p\mathbb{Z})$.
Moreover, since for 28, there are 2 primes, which is 2 and 7.

$$2^4 = 16 \mod 29 \qquad 2^{14} = 2^5 * 2^5 * 2^4 = 3 * 3 * 16 = 19 * 3 = -1 \mod 29$$

Therefore, 2 is a generator for 29

4.

$$\begin{array}{rcc} \left(\frac{1801}{8191}\right) & = & \left(\frac{8191}{1801}\right) \\ & = & \left(\frac{987}{1801}\right) \\ & = & \left(\frac{3}{1801}\right) * \left(\frac{329}{1801}\right) \\ & = & \left(\frac{1}{3}\right) * \left(\frac{156}{329}\right) \\ & = & \left(\frac{2^2 * 3 * 13}{329}\right) \\ & = & \left(\frac{2}{1}\right)^2 * \left(\frac{2}{3}\right) * \left(\frac{4}{13}\right) \\ & = & -1 \end{array}$$

5.

$x = -\frac{-b \pm \sqrt{b^2-4ac}}{2a} \mod p$
Therefore, if x has solutions, $b^2 - 4ac$ must be squared mod p
if this equation has no solution, $b^2 - 4ac < 0 \text{or} b^2 - 4ac$ could not be squred, which means
$\left(\frac{b^2-4ac}{p}\right) = -1 \Rightarrow \text{number of solutions} = 0 \mod p$
if this equation has one solution, $b^2 - 4ac = 0$ which means
$\left(\frac{b^2-4ac}{p}\right) = 0 \Rightarrow \text{number of solutions} = 1 \mod p$
if this equation has two solutions, $b^2 - 4ac$ is squared mod p which means
$\left(\frac{b^2-4ac}{p}\right) = 1 \Rightarrow \text{number of solutions} = 2 \mod p$

6.

$$gcd(n, pq) = 1 \Rightarrow gcd(n, p) = 1 \Rightarrow n^{p-1} \equiv 1 \mod p$$
$$\Rightarrow n^{q-1} \equiv 1 \mod q \Rightarrow n^{p-1} = n^{(q-1)*k} \equiv 1 \mod q$$
$$\Rightarrow n^{p-1} \equiv 1 \mod pq$$

7.

if $p \equiv 1 \mod 3$,

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

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

$$-3 \equiv 1 \mod 4 \Rightarrow \left(\frac{p-3}{p}\right) = \left(\frac{p}{p-3}\right) = \left(\frac{3}{p-3}\right) = \left(\frac{p-3}{3}\right)$$

if we want this equation hold, $p \equiv 1 \mod 3 \text{must exists}.$

8.

if $\left(\frac{a}{p}\right) = 1$, since p is a prime

$$1 = a^{\frac{p-1}{2}} \mod p$$

and since p is a prime, p-1 is even, therefore, for q=2, $\alpha^{(p-1)/q} \not\equiv 1 \mod p$, therefore, a is not a generator.

Ex4.

1.

Suppose there exists a prime element n is reducible, which means that n could be expressed like n = ab. a and b are intergers which are greater than 1. Therefore, there exists x,y, which $a|x, b \not| y, a \not| x, b|y$. Since this contradicts with (*). Therefore, any prime element is irreducible.

2.

for any rreducible number n, we could factorize it into n =ab, which a,b is also in integral domian and not equal to 1. Then there must exist a number greater than 1 and $a|p$. Therefore, for irreducible interger , it will not exists $a < p$ and $a|p$, which is the definition of (**)

3.

Since $p > 1\&a|p \qquad a = 1 \quad or \quad a = p$, which indicates that p is prime. Since $p \not| xandp / |y \Rightarrow p \not| xy$.Therefore, (**) implies (*)

4.

Since we have proved that (**) implies (*), we not want to prove that (*) implies (**). Since from (*), we have known that p is a prime. If there exists $a \not 1\&a \not p\&a|p$, then p will be reducible, then there will exists $a|x, p/a \not| x\&a \not| y, p/a|y\&p|(x \cdot y)$, which contradicts with (*). Therefore, (*) implies (**). Therefore, we could conclude that they are equivalent for integers.

Ex.5

1.

Since $65537 \equiv 1 \mod 4$, $\left(\frac{3}{65537}\right) = \left(\frac{65537}{3}\right) = \left(\frac{2}{3}\right) = -1$

2.

since 3 coprime with 65537, and $3^{65536} \equiv 1 \mod 65537$
Therefore, $3^{65536/2} \equiv \pm 1 \mod 65537$
Since according to 1., 3 is not a squared number for 65537, therefore,

$$3^{32768} \equiv -1 \mod 65537$$

3.

Since 65537 is a prime, and $65536 = 2^16$, and since $3^{32768} \not\equiv 1 \mod 65537$, 3 is a generator of 65537