VE203 Assigment 4

Liu Yihao 515370910207

Exercise 4.1

i)

$$247 = 13 \times 19$$
$$3 \times 13 - 2 \times 19 = 1$$

ii)

$$10^2 \equiv 3^2 \bmod 13$$
$$10^{100} \equiv 3^{100} \bmod 13$$
$$10^{100} \equiv 3 \cdot 27^{33} \bmod 13$$
$$27^{33} \equiv 1^{33} \bmod 13$$
$$10^{100} \equiv 3 \bmod 13$$

$$10^2 \equiv 9^2 \bmod 19$$
$$10^{100} \equiv 9^{100} \bmod 19$$
$$10^{100} \equiv 9 \cdot 9^{3^{33}} \bmod 19$$
$$10^{100} \equiv 9 \cdot 7^{3^{11}} \bmod 19$$
$$343^{11} \equiv 1^{11} \bmod 19$$
$$10^{100} \equiv 9 \bmod 19$$

iii)

$$19 \times 11 \bmod 13 = 1$$
$$13 \times 3 \bmod 19 = 1$$
$$3 \times 19 \times 11 + 9 \times 13 \times 3 = 978$$
$$978 \equiv 237 \bmod 247$$

Exercise 4.2

$$4^n \equiv 7 \bmod 9$$
$$4^n \equiv 9 \bmod 11$$
$$9 \times 5 \bmod 11 = 1$$
$$11 \times 5 \bmod 9 = 1$$
$$7 \times 11 \times 5 + 9 \times 9 \times 5 = 790$$
$$790 \equiv 4^n \bmod 99$$
$$4^n = 790 + 99k \ (k \in Z, k > -8)$$
$$n = 8 \text{ is a solution to the equation.}$$

Exercise 4.3

$$45029^2 < 2027651281 < 45030^2$$
$$\sqrt{(45030 + 11)^2 - 2027651281} = 1020$$
$$2027651281 = (45041 - 1020)(45041 + 1020) = 44021 \times 46061$$

Exercise 4.4

$$5^6 \equiv 1 \bmod 7$$
$$5^{2003} \equiv 5^{6^{333}} \times 5^5 \bmod 7$$
$$5^{2003} \equiv 3 \bmod 7$$
$$5^{10} \equiv 1 \bmod 11$$
$$5^{2003} \equiv 5^{10^{200}} \times 5^3 \bmod 11$$
$$5^{2003} \equiv 4 \bmod 7$$
$$5^{12} \equiv 1 \bmod 13$$
$$5^{2003} \equiv 5^{12^{166}} \times 5^{11} \bmod 13$$
$$5^{2003} \equiv 8 \bmod 13$$
$$11 \times 13 \times 5 \bmod 7 = 1$$
$$7 \times 13 \times 4 \bmod 11 = 1$$
$$7 \times 11 \times 12 \bmod 13 = 1$$
$$3 \times 11 \times 13 \times 5 + 4 \times 7 \times 13 \times 4 + 8 \times 7 \times 11 \times 12 = 10993$$
$$10993 \equiv 983 \bmod 1001$$

Exercise 4.5

i)

$$(p-1)! \equiv -1 \text{ mod p}$$

$$(p-1)! \equiv p-1 \text{ mod p}$$

$$(p-2)! \equiv 1 \text{ mod p}$$

If p is not a prime and $p > 3$, then there must exist $k \in [2, p-2], k \in N$ and k mod $p = 0$, so $(p-2)! \equiv 0$ mod p, which reaches a contradiction.
If $p = 2$ or $p = 3$, it is obvious that $(p-1)! \equiv -1$ mod p.

ii)

$$2z = m - 1$$

$$z + 1 = m - z \equiv -z \text{ mod m}$$

$$z + k = m - z - k + 1 \equiv -z - k + 1 \text{ mod m}, \ \text{k} \in [1, \text{z}]$$

$$(z+1)(z+2)\cdots 2z \equiv (-1)^z z! \text{ mod m}$$

$$z!(z+1)(z+2)\cdots 2z \equiv (-1)^z (z!)^2 \text{ mod m}$$

$$(m-1)! \equiv (-1)^z (z!)^2 \text{ mod m}$$

iii) When $p = 4k+1, k \in N$,

$$(p-1)! \equiv (-1)^{2k}(2k!)^2 \text{ mod p}$$

p is a prime when

$$(2k!)^2 \equiv -1 \text{ mod p}$$

When $p = 4k+3, k \in N$,

$$(p-1)! \equiv (-1)^{2k+1}(2k+1!)^2 \text{ mod p}$$

p is a prime when

$$(2k+1!)^2 \equiv 1 \text{ mod p}$$

Exercise 4.6

i)

$$1^2 \equiv 1 \text{ mod } 11$$

$$2^2 \equiv 4 \text{ mod } 11$$

$$3^2 \equiv 9 \text{ mod } 11$$

$$4^2 \equiv 5 \text{ mod } 11$$

$$5^2 \equiv 3 \text{ mod } 11$$

$$6^2 \equiv 3 \text{ mod } 11$$

$$7^2 \equiv 5 \text{ mod } 11$$

$$8^2 \equiv 9 \text{ mod } 11$$

$$9^2 \equiv 4 \text{ mod } 11$$

$$10^2 \equiv 1 \text{ mod } 11$$

So $1+11k, 3+11k, 4+11k, 5+11k, 9+11k, k \in N$ are quadratic residues of 11.

ii) Suppose $p = 2k+1, k \in N$, $x = p-b, b \in [1, 2k], b \in N$

$$(p-b)^2 = (p)^2 - 2pb + b^2$$

$$(p-b)^2 \equiv b^2 \text{ mod p}$$

$$b^2 \equiv b^2 \text{ mod p}$$

Since p is an odd number, $p - b \neq b$,
so $x = b$ and $x = p - b$ are two incongruent solutions if $b^2 \equiv a$ mod p,
or there is no solution if $b^2 \not\equiv a$ mod p,

iii) According to ii), we can find that when $x = b$ or $x = p - b$, the value of a is the same.
Let $b \in [1, k]$, then $b < p - b$, and let $n \in [1, k-b], n \in N$,
then for $b \in [1, k-1]$, if for $x = b$ and $x = b + n$, suppose the value of a is the same,

$$b^2 \equiv (b+n)^2 \text{ mod p}$$

$$(2b+n)n \equiv 0 \text{ mod p}$$

$$2b + n \leqslant 2b + k - b = k + b < p$$

$$n < p$$

Since p is a prime number, $(2b+n)n \not\equiv 0$ mod p, which reaches a contradiction.
So for any two b the value of a isn't the same, there are exactly $\frac{p-1}{2}$ quadratic residues of p among the integers 1,2,...,$p-1$.

iv) Let $c \in [1, k]$, then

$$x^2 \equiv a \equiv b \equiv c^2 \text{ mod p}$$

If a is a quadratic residue of p, we can find c so that $x = c$ and $x = p - c$ are two incongruent solutions, and b is also a quadratic residue of p, then

$$\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right) = 1$$

If a isn't a quadratic residue of p, we can't find c so that $x = c$ and $x = p - c$ are two incongruent solutions, and b is also not a quadratic residue of p, then

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

v) If a is a quadratic residue of p, $(\frac{a}{p}) = 1$, then let $a = x^2 + kp, k \in Z$

$$a^{\frac{p-1}{2}} = (x^2 + kp)^{\frac{p-1}{2}} = \sum_{i=0}^{\frac{p-1}{2}} (x^2)^i + (kp)^{\frac{p-1}{2}-i} \equiv (x^2)^{\frac{p-1}{2}} \text{ mod p}$$

$$a^{\frac{p-1}{2}} \equiv x^{p-1} \text{ mod p}$$

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

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \text{ mod p}$$

If a isn't a quadratic residue of p, $(\frac{a}{p}) = -1$

$$a^{p-1} \equiv 1 \text{ mod p}$$

$$a^{\frac{p-1}{2}} \equiv \pm 1 \text{ mod p}$$

According to the above, we can easily get that if $a^{\frac{p-1}{2}} \equiv 1$ mod p, a is a quadratic residue of p, so $a^{\frac{p-1}{2}} \equiv -1$ mod p here.

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \text{ mod p}$$

vi)

$$\left(\frac{ab}{p}\right) \equiv (ab)^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} \cdot b^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \text{ mod p}$$

Since p is an odd prime ($p \geqslant 3$)
When $\left(\frac{ab}{p}\right) = 1$, $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = 1 + kp$, so

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = 1$$

When $\left(\frac{ab}{p}\right) = -1$, $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = -1 + kp$, so

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = -1$$

vii) If a is a negative integer in v), we can simply get the same conclusion

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \text{ mod p}$$

When $p = 4k + 1, k \in N$,

$$(-1)^{\frac{4k+1-1}{2}} = (-1)^{2k} = 1$$

$$\left(\frac{a}{p}\right) \equiv 1 \text{ mod p}$$

Using the method in vi), we can find $\left(\frac{a}{p}\right) = 1$, so -1 is a quadratic residue of p.
When $p = 4k + 3, k \in N$,

$$(-1)^{\frac{4k+3-1}{2}} = (-1)^{2k+1} = -1$$

$$\left(\frac{a}{p}\right) \equiv -1 \text{ mod p}$$

Using the method in vi), we can find $\left(\frac{a}{p}\right) = -1$, so -1 isn't a quadratic residue of p.

viii) Let $x^2 = 35k + 29, k \in N$

$$x^2 \equiv 4 \text{ mod } 5$$

$$x^2 \equiv 1 \text{ mod } 7$$

$$\left\{\begin{array}{ll} x \equiv & 2 \text{ mod } 5 \\ x \equiv & 1 \text{ mod } 7 \end{array}\right. \quad or \quad \left\{\begin{array}{ll} x \equiv & 2 \text{ mod } 5 \\ x \equiv & -1 \text{ mod } 7 \end{array}\right. \quad or \quad \left\{\begin{array}{ll} x \equiv & -2 \text{ mod } 5 \\ x \equiv & 1 \text{ mod } 7 \end{array}\right. \quad or \quad \left\{\begin{array}{ll} x \equiv & -2 \text{ mod } 5 \\ x \equiv & -1 \text{ mod } 7 \end{array}\right.$$

$$7 \times 3 \bmod 5 = 1$$
$$5 \times 3 \bmod 7 = 1$$
$$x_1 = [(2 \times 7 \times 3 + 1 \times 5 \times 3) \bmod 35] + 35\text{k} = 22 + 35\text{k}$$
$$x_2 = [(2 \times 7 \times 3 - 1 \times 5 \times 3) \bmod 35] + 35\text{k} = 27 + 35\text{k}$$
$$x_3 = [(-2 \times 7 \times 3 + 1 \times 5 \times 3) \bmod 35] + 35\text{k} = 8 + 35\text{k}$$
$$x_4 = [(-2 \times 7 \times 3 - 1 \times 5 \times 3) \bmod 35] + 35\text{k} = 13 + 35\text{k}$$