VE203
Assignment 4

Jiang Yicheng
515370910224

October 19, 2016

Exercise 4.1

i)

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

So the two primes are $p_1 = 13, p_2 = 19$, and $x = 3, y = -2$ such that $1 = p_1 \cdot x + p_2 \cdot y$.

ii)

$$10^{100} \equiv (-3)^{100} \equiv 3^{100} \equiv (27)^{33} \cdot 3 \equiv 1^{33} \cdot 3 \equiv 3 \ (mod \ \ 13)$$

$$10^{100} \equiv 100^{50} \equiv 5^{50} \equiv 25^{25} \equiv 6^{25} \equiv (-2)^{12} \cdot 6 \equiv 16^3 \cdot 6 \equiv (-3)^3 \cdot 6 \equiv 11 \cdot 6 \equiv 9 \ (mod \ \ 19)$$

So $10^{100} \equiv 3 \ (mod \ \ 13), 10^{100} \equiv 9 \ (mod \ \ 19)$

iii)

Because $11 \cdot 19 \equiv -2 \cdot 6 \equiv 1 \ (mod \ \ 13)$, $3 \cdot 13 \equiv 1 \ (mod \ \ 19)$, then according to Chinese Remainder Theorem

$$10^{100} \equiv 3 \cdot 11 \cdot 19 + 9 \cdot 3 \cdot 13 \equiv 978 \equiv 237 \ (mod \ \ 247)$$

so $r = 237$.

Exercise 4.2

We see that $2^8 = 256 = 2 \cdot 99 + 58$, so

$$4^8 \equiv 4^2 \equiv 7 \ (mod \ \ 9), 2^8 \equiv 3 \ (mod \ \ 11)$$

So $n = 8$ satisfies both $4^n \equiv 7 \ (mod \ \ 9), 2^n \equiv 3 \ (mod \ \ 11)$

Exercise 4.3

$$45029^2 < 2027651281 < 45030^2$$

We need to calculate $k^2 - 2027651281$ for

$$45029 < k < \frac{2027651281 + 1}{2} = 1013825641$$

We find:

$$45030^2 - 2027651281 = 49619, 45031^2 - 2027651281 = 139680$$

$$45032^2 - 2027651281 = 229743, 45033^2 - 2027651281 = 319808$$

$$45034^2 - 2027651281 = 409875, 45035^2 - 2027651281 = 499944$$

$$45036^2 - 2027651281 = 590015, 45037^2 - 2027651281 = 680088$$

$$45038^2 - 2027651281 = 770163, 45039^2 - 2027651281 = 860240$$

$$45040^2 - 2027651281 = 950319, 45041^2 - 2027651281 = 1040400 = 1020^2$$

So $2027651281 = 45041^2 - 1020^2 = 46061 \cdot 44021$. And we can check that both 46061 and 44021 are primes. So the factors of 2027651281 are $1, 44021, 46061, 2027651281$.

Exercise 4.4

According to Fermat's Little Theorem,

$$5^{7-1} \equiv 1 \ (mod \ \ 7), 5^{11-1} \equiv 1 \ (mod \ \ 11), 5^{13-1} \equiv 1 \ (mod \ \ 13)$$

so

$$5^{2003} \equiv 5^{333 \cdot 6+5} \equiv 1^{333} \cdot 4^2 \cdot 5 \equiv 2 \cdot 5 \equiv 3 \ (mod \ \ 7)$$
$$5^{2003} \equiv 5^{200 \cdot 10+3} \equiv 1^{200} \cdot 125 \equiv 4 \ (mod \ \ 11)$$
$$5^{2003} \equiv 5^{166 \cdot 12+11} \equiv 1^{166} \cdot (-1)^5 \cdot 5 \equiv 8 \ (mod \ \ 13)$$

Since $5 \cdot 11 \cdot 13 \equiv (-2) \cdot 4 \cdot (-1) \equiv 1 \ (mod \ \ 7)$, $4 \cdot 7 \cdot 13 \equiv 4 \cdot (-4) \cdot 2 \equiv 1 \ (mod \ \ 11)$, $12 \cdot 7 \cdot 11 \equiv (-1) \cdot 7 \cdot (-2) \equiv 1 \ (mod \ \ 13)$, then according to Chinese Remainder Theorem,

$$5^{2003} \equiv 3 \cdot 5 \cdot 11 \cdot 13 + 4 \cdot 4 \cdot 7 \cdot 13 + 8 \cdot 12 \cdot 7 \cdot 11 \equiv 10993 \equiv 983 \ (mod \ \ 1001)$$

So $5^{2003} \equiv 983 \ (mod \ \ 1001)$.

Exercise 4.5

i)

Assume that $(p-1)! \equiv -1 \ (mod \ \ p)$ while p is not a prime. Set $p = a \cdot b, a, b \in \mathbb{N}, a \leqslant b$. Then $a, b \in \mathbb{N} \cap [1, p-1]$, so $c := \dfrac{(p-1)!}{a} \in \mathbb{N}$ and

$$b \cdot (p-1)! \equiv b \cdot a \cdot \frac{(p-1)!}{a} \equiv p \cdot c \equiv 0 \ (mod \ \ p)$$

While $(p-1)! \equiv -1 \ (mod \ \ p)$, then

$$b \cdot (p-1)! \equiv -b \ (mod \ \ p)$$

So $-b \equiv 0 \ (mod \ \ p)$. Since $b \in \mathbb{N} \cap [1, p-1]$, this is impossible. So our assumption is wrong.

So p is a prime.

ii)

$\forall a \in \mathbb{N} \cap [1, m-1], a \equiv -(m-a) \ (mod \ \ m)$, so for any odd integer $m, z = \dfrac{m-1}{2}$,

$$(m-1)! \equiv \prod_{i=1}^{z} i \cdot \prod_{i=z+1}^{m-1} i \equiv \prod_{i=1}^{z} i \cdot \prod_{i=z+1}^{m-1} -(m-i) \equiv \prod_{i=1}^{z} i \cdot (-1)^z \prod_{j=1}^{z} j \equiv (-1)^z (z!)^2 \ (mod \ \ m)$$

So for any odd integer m, $(m-1)! \equiv (-1)^z (z!)^2 \ (mod \ \ m)$

iii)

To see whether an odd integer m is a prime, we can check whether $(-1)^z(z!)^2 \equiv -1 \ (mod \ \ m)$ where $z = \dfrac{m-1}{2}$.

From $i)ii)$, the method is correct. Then we need to see whether the method is practical. It seems that we haven't an easy way to calculate $z! \ \ mod \ \ m$ and therefore the method will lead to a complex calculation. However, this is a new way which can be implemented by computer. With proper programme, it can work well.

Exercise 4.6

i)

$$
\begin{gathered}
x \equiv 0 \ (mod \ \ 11) \Rightarrow x^2 \equiv 0 \ (mod \ \ 11), x \equiv 1 \ (mod \ \ 11) \Rightarrow x^2 \equiv 1 \ (mod \ \ 11) \\
x \equiv 2 \ (mod \ \ 11) \Rightarrow x^2 \equiv 4 \ (mod \ \ 11), x \equiv 3 \ (mod \ \ 11) \Rightarrow x^2 \equiv 9 \ (mod \ \ 11) \\
x \equiv 4 \ (mod \ \ 11) \Rightarrow x^2 \equiv 5 \ (mod \ \ 11), x \equiv 5 \ (mod \ \ 11) \Rightarrow x^2 \equiv 4 \ (mod \ \ 11) \\
x \equiv 6 \ (mod \ \ 11) \Rightarrow x^2 \equiv 3 \ (mod \ \ 11), x \equiv 7 \ (mod \ \ 11) \Rightarrow x^2 \equiv 5 \ (mod \ \ 11) \\
x \equiv 8 \ (mod \ \ 11) \Rightarrow x^2 \equiv 9 \ (mod \ \ 11), x \equiv 9 \ (mod \ \ 11) \Rightarrow x^2 \equiv 4 \ (mod \ \ 11) \\
x \equiv 10 \ (mod \ \ 11) \Rightarrow x^2 \equiv 1 \ (mod \ \ 11)
\end{gathered}
$$

So $x^2 \equiv a \ (mod \ 11)$ has a solution if and only if $a \equiv 0, 1, 3, 4, 5, 9 \ (mod \ 11)$. Taking $gcd(a, 11) = 1$ into account, $1 + 11t, 3 + 11t, 4 + 11t, 5 + 11t, 9 + 11t, t \in \mathbb{Z}$ are quadratic residues of 11.

ii)

For any $a \in \mathbb{Z}, p \nmid a$, then

1. $x^2 \equiv a \ (mod \ \ p)$ has no solutions modulo p
2. $x^2 \equiv a \ (mod \ \ p)$ has a solution modulo p: $x \equiv b \ (mod \ \ p), b \in \mathbb{N}$, then for some x such that $x \equiv p - b \ (mod \ \ p)$, we can see $x^2 \equiv (p-b)^2 \equiv b^2 \equiv a \ (mod \ \ p)$. If $p - b \equiv b \ (mod \ \ p)$, then $2b \equiv p \equiv 0 \ (mod \ p)$. Since p is an odd prime, $b \equiv 0 \ (mod \ p)$. So $a \equiv b^2 \equiv 0 \ (mod \ p)$ which leads to contradiction. So $x \equiv p - b \ (mod \ p)$ and $x \equiv b \ (mod \ p)$ are two incongruent solutions modulo p.

   If $x \equiv c \ (mod \ \ p)$ is another solution to $x^2 \equiv a \ (mod \ \ m)$ where $c \in \mathbb{N}, c \not\equiv b \ (mod \ \ p) \wedge c \not\equiv p - b \ (mod \ \ p)$, then $c^2 \equiv a \equiv b^2 \ (mod \ \ p)$, furthermore, $p | (c-b)(c+b)$. Since p is a prime, then $p | (c-b)$ or $p | (c+b)$. Since $c \not\equiv b \ (mod \ \ p) \wedge c \not\equiv p - b \ (mod \ \ p)$, this is contradiction.

   So if $x^2 \equiv a \ (mod \ \ p)$ has solutions, it exactly has two incongruent solutions modulo p.

To sum up, the congruence $x^2 \equiv a \ (mod \ \ p)$ has either no solutions or exactly two incongruent solutions modulo p.

iii)

From $ii)$ we know that $\forall b \in \mathbb{Z} \cap [1, \frac{p-1}{2}]$, $x \equiv b\ (mod\ \ p)$ and $x \equiv p - b\ (mod\ \ p)$ both lead to $x^2 \equiv b^2\ (mod\ \ p)$, and for different b, b^2 are incongruent modulo p. So for any odd prime, $\forall x \in \mathbb{Z}$, x^2 has $\frac{p-1}{2}$ different results modulo p (except 0). And therefore for exactly $\frac{p-1}{2}$ incongruent numbers a among $1, 2, \cdots, p-1$, $x^2 \equiv a\ (mod\ \ p)$ has solution.(These are all possible result for $x^2\ mod\ p$ except 0, so all quadratic residues modulo p are among them.) Moreover for any number a among these numbers, $gcd(a, p) = 1$.

So if p is an odd prime, then there are exactly $\frac{p-1}{2}$ quadratic residues of p among the integers $1, 2, \cdots, p-1$.

iv)

Since $a \equiv b\ (mod\ \ p)$, then $x^2 \equiv b \equiv a\ (mod\ \ p)$. So if $x^2 \equiv a\ (mod\ \ p)$ has solution and $gcd(a, p) = 1$, then $x^2 \equiv b\ (mod\ \ p)$ must have a solution and $gcd(b, p) = gcd(a + kp, p) = gcd(a, p) = 1$ where k is an integer; if $x^2 \equiv a\ (mod\ \ p)$ doesn't have a solution, neither will $x^2 \equiv b\ (mod\ \ p)$; if $gcd(a, p) \neq 1$, $gcd(b, p) = gcd(a, p) \neq 1$.

So if a is a quadratic residue, so will b; and if a isn't a quadratic residue, neither will b. So

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

v)

If a is a quadratic residue of p, then $\exists x \in \mathbb{Z} \cap [1, p-1]$ such that $x^2 \equiv a\ (mod\ \ p)$. Since p is a prime and $p \nmid x$, according to Fermat's Little Theorem,

$$x^{p-1} \equiv 1\ (mod\ \ p)$$

Since $\left(\frac{a}{p}\right) = 1$ when a is a quadratic residue of p,

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

If a is not a quadratic residue of p,

$\forall m \in \mathbb{N} \cap [1, p-1]$, $gcd(m, p) = 1$, so there exists a unique $n_0 \in \mathbb{N} \cap [1, p-1]$ such that $m \cdot n_0 \equiv 1\ (mod\ \ p)$, and therefore

$$m \cdot (a \cdot n_0) \equiv a\ (mod\ \ p)$$

If $a \cdot n_0 \equiv a \cdot n_0'\ (mod\ \ p)$, then since a is not divisible by p and p is a prime, $gcd(a, p) = 1$ and $n_0 \equiv n_0'\ (mod\ \ p)$. So $\forall m \in \mathbb{N} \cap [1, p-1]$, there exists a unique $n \in \mathbb{N} \cap [1, p-1]$ such that $m \cdot n \equiv a\ (mod\ \ p)$, and for different m, n will be different. Since a is not a quadratic residue of p, $m \neq n$. So for $1, 2, \cdots, p-1$, they can be grouped into $\frac{p-1}{2}$ pairs m, n where $m \neq n$ and $m \cdot n \equiv a\ (mod\ \ p)$, and therefore

$$2 \cdot 3 \cdot \cdots \cdot (p-1) \equiv a^{(p-1)/2}\ (mod\ \ p)$$

According to Wilson's Theorem,

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

To sum up, if p is an odd prime and a is a positive integer not divisible by p, then

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

vi)

According to v), we obtain that if p is an odd prime and a and b are integers not divisible by p,

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

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

vii)

If p is an odd prime and a is a positive integer not divisible by p, then according to Fermat's Little Theorem,

$$a^{p-1} \equiv 1 \ (mod \ \ p)$$

so $(a^{(p-1)/2} + 1)(a^{(p-1)/2} - 1) \equiv 0 \ (mod \ \ p)$. Since p is a prime,

$$a^{(p-1)/2} \equiv -1 \ (mod \ \ p) \vee a^{(p-1)/2} \equiv 1 \ (mod \ \ p)$$

then with v) we obtain that: If p is an odd prime and a is a positive integer not divisible by p, then

1. a is a quadratic residue of p if and only if $a^{(p-1)/2} \equiv 1 \ (mod \ \ p)$
2. a is not a quadratic residue of p if and only if $a^{(p-1)/2} \equiv -1 \ (mod \ \ p)$

If -1 is a quadratic residue of p ($p \nmid -1$), then

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

so $(p-1)/2 = 2k$ where $k \in \mathbb{Z}$. So $p = 4k + 1$ which implies that

$$p \equiv 1 \ (mod \ \ 4)$$

If -1 is not a quadratic residue of p ($p \nmid -1$), then

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

so $(p-1)/2 = 2k + 1$ where $k \in \mathbb{Z}$. So $p = 4k + 3$ which implies that

$$p \equiv 3 \ (mod \ \ 4)$$

To sum up, if p is an odd prime, then -1 is a quadratic residue of p if $p \equiv 1 \ (mod \ \ 4)$, and -1 is not a quadratic residue of p if $p \equiv 3 \ (mod \ \ 4)$.

viii)

$x^2 \equiv 29\ (mod\ \ 35) \Rightarrow x^2 \equiv 29 \equiv 4\ (mod\ \ 5) \wedge x^2 \equiv 29 \equiv 1\ (mod\ \ 7)$

$$x \equiv 0\ (mod\ \ 5) \Rightarrow x^2 \equiv 0\ (mod\ \ 5), x \equiv 1\ (mod\ \ 5) \Rightarrow x^2 \equiv 1\ (mod\ \ 5)$$
$$x \equiv 2\ (mod\ \ 5) \Rightarrow x^2 \equiv 4\ (mod\ \ 5), x \equiv 3\ (mod\ \ 5) \Rightarrow x^2 \equiv 4\ (mod\ \ 5)$$
$$x \equiv 4\ (mod\ \ 5) \Rightarrow x^2 \equiv 1\ (mod\ \ 5)$$

So $x^2 \equiv 4\ (mod\ \ 5) \Leftrightarrow x \equiv 2\ (mod\ \ 5) \vee x \equiv 3\ (mod\ \ 5)$.

$$x \equiv 0\ (mod\ \ 7) \Rightarrow x^2 \equiv 0\ (mod\ \ 7), x \equiv 1\ (mod\ \ 7) \Rightarrow x^2 \equiv 1\ (mod\ \ 7)$$
$$x \equiv 2\ (mod\ \ 7) \Rightarrow x^2 \equiv 4\ (mod\ \ 7), x \equiv 3\ (mod\ \ 7) \Rightarrow x^2 \equiv 2\ (mod\ \ 7)$$
$$x \equiv 4\ (mod\ \ 7) \Rightarrow x^2 \equiv 2\ (mod\ \ 7), x \equiv 5\ (mod\ \ 7) \Rightarrow x^2 \equiv 4\ (mod\ \ 7)$$
$$x \equiv 6\ (mod\ \ 7) \Rightarrow x^2 \equiv 1\ (mod\ \ 7)$$

So $x^2 \equiv 1\ (mod\ \ 7) \Leftrightarrow x \equiv 1\ (mod\ \ 7) \vee x \equiv 6\ (mod\ \ 7)$.

Because $3 \cdot 7 \equiv 1\ (mod\ \ 5)$, $3 \cdot 5 \equiv 1\ (mod\ \ 7)$, then according to Chinese Remainder Theorem

1. $x \equiv 2\ (mod\ \ 5) \wedge x \equiv 1\ (mod\ \ 7)$

   $$x \equiv 2 \cdot 3 \cdot 7 + 1 \cdot 3 \cdot 5 \equiv 57 \equiv 22\ (mod\ \ 35)$$

   so $x = 22 + 35t, t \in \mathbb{Z}$.

2. $x \equiv 2\ (mod\ \ 5) \wedge x \equiv 6\ (mod\ \ 7)$

   $$x \equiv 2 \cdot 3 \cdot 7 + 6 \cdot 3 \cdot 5 \equiv 132 \equiv 27\ (mod\ \ 35)$$

   so $x = 27 + 35t, t \in \mathbb{Z}$.

3. $x \equiv 3\ (mod\ \ 5) \wedge x \equiv 1\ (mod\ \ 7)$

   $$x \equiv 3 \cdot 3 \cdot 7 + 1 \cdot 3 \cdot 5 \equiv 78 \equiv 8\ (mod\ \ 35)$$

   so $x = 8 + 35t, t \in \mathbb{Z}$.

4. $x \equiv 3\ (mod\ \ 5) \wedge x \equiv 6\ (mod\ \ 7)$

   $$x \equiv 3 \cdot 3 \cdot 7 + 6 \cdot 3 \cdot 5 \equiv 153 \equiv 13\ (mod\ \ 35)$$

   so $x = 13 + 35t, t \in \mathbb{Z}$.

With simple check we can see that all these are solutions to the origin congruence.

So the solution set of the congruence $x^2 = 29\ (mod\ \ 35)$ is

$$\{x : x = 8 + 35t \vee x = 13 + 35t \vee x = 22 + 35t \vee x = 27 + 35t, t \in \mathbb{Z}\}$$