VE475 Homework 1

Liu Yihao 515370910207

Ex. 1 — Simple questions

1.

	q_i	r_i	s_i	t_i
0		17	1	0
1		101	0	1
2	$17 \div 101 = 0$	$17 - 0 \times 101 = 17$	$1 - 0 \times 0 = 1$	$0 - 0 \times 1 = 0$
3	$101 \div 17 = 5$	$101 - 5 \times 17 = 16$	$0 - 5 \times 1 = -5$	$1 - 5 \times 0 = 1$
4	$17 \div 16 = 1$	$17 - 1 \times 16 = 1$	$1 - 1 \times -5 = 6$	$0 - 1 \times 1 = -1$

$$17 \cdot 6 \equiv 1 \bmod 101$$

So the inverse of 17 modulo 101 is 6.

2.

$$12x \equiv 28 \bmod 236$$

$$3x \equiv 7 \bmod 59$$

$$3x = 59k + 7 \quad k \in Z$$

First, we can find the solutions in $[0, 58]$, try $k = 0, 1, 2$
When $k = 0$, $x = \frac{7}{3}$. When $k = 1$, $x = 22$. When $k = 1$, $x = \frac{125}{3}$.
So $x = 59k + 22$, $k \in Z$.

3.

4.

$$\sqrt{4369} < \sqrt{4883} < 70$$

Consider all of the primes in $[2, 70]$, they are 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67.
For 4883, first, try to divide 4883 by them one by one, we can find that $4883 = 19 \times 257$. Then, try to divide 257 by 2, 3, 5, 7, 11, 13, all of them have a reminder, so 257 is a prime, $4883 = 19 \times 257$.
For 4369, it's interesting because $4883 = 4369 + 2 \times 257$, so $4369 = 17 \times 257$, where 17 and 257 are primes.

5.

$$A = \begin{pmatrix} 3 & 5 \\ 7 & 3 \end{pmatrix} \bmod p$$

When $p = 2$,

$$A = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \bmod 2$$

$$\det \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} = 0$$

It is not invertible.

When $p = 3$,

$$A = \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix} \mod 3$$

$$\det \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix} = -2$$

It is invertible.

When $p = 5$,

$$A = \begin{pmatrix} 3 & 0 \\ 2 & 3 \end{pmatrix} \mod 5$$

$$\det \begin{pmatrix} 3 & 0 \\ 2 & 3 \end{pmatrix} = 9$$

It is invertible.

When $p = 7$,

$$A = \begin{pmatrix} 3 & 5 \\ 0 & 3 \end{pmatrix} \mod 7$$

$$\det \begin{pmatrix} 3 & 5 \\ 0 & 3 \end{pmatrix} = 9$$

It is invertible.

When $p > 7$,

$$A = \begin{pmatrix} 3 & 5 \\ 7 & 3 \end{pmatrix} \mod 7$$

$$\det \begin{pmatrix} 3 & 5 \\ 7 & 3 \end{pmatrix} = -26$$

It is invertible.

So when $p = 2$, it is not invertible.

6.

$$
\begin{aligned}
2^{2017} &\equiv 2 \cdot 4^{1008} \bmod 5 \\
&\equiv 2 \cdot (-1)^{1008} \bmod 5 \\
&\equiv 2 \bmod 5 \\
2^{2017} &\equiv 2 \cdot 64^{336} \bmod 13 \\
&\equiv 2 \cdot (-1)^{336} \bmod 13 \\
&\equiv 2 \bmod 13 \\
2^{2017} &\equiv 4 \cdot 32^{403} \bmod 31 \\
&\equiv 4 \cdot 1^{403} \bmod 31 \\
&\equiv 4 \bmod 31
\end{aligned}
$$

$$
\begin{aligned}
5 \cdot 13 &\equiv 3 \bmod 31 \\
65 \cdot -10 &\equiv 1 \bmod 31 \\
13 \cdot 31 &\equiv 3 \bmod 5 \\
403 \cdot 2 &\equiv 1 \bmod 5 \\
5 \cdot 31 &\equiv -1 \bmod 13 \\
155 \cdot -1 &\equiv 1 \bmod 13
\end{aligned}
$$

$$
\begin{aligned}
2^{2017} &\equiv -650 \cdot 4 + 806 \cdot 2 - 155 \cdot 2 \bmod 2015 \\
&\equiv -1298 \bmod 2015 \\
&\equiv 717 \bmod 2015
\end{aligned}
$$

7. According to Assignment 1/Ex. 1/3, let a, b and n be three positive integers such that $n \mid ab$ and $\gcd(a, n) = 1$, we can prove that $n \mid b$.
   Now let $n = p$, since p is a prime, we know $\gcd(a, p) = 1$ or $\gcd(a, p) = p$