VE 203 Hw 4 周维韬 518021911039

Ex 4.1 i) $247 = 13 \times 19$

$19 = 1 \times 13 + 6$

$13 = 2 \times 6 + 1$

$6 = 6 \times 1 + 0$

$1 = 19 - 6 \times 3$

$= 19 - (19 - 13) \times 3$

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

Therefore, $x = 3$, $y = -2$

ii) $10^{100} \equiv (10^2)^{50} \equiv (9)^{50} \equiv (81)^{25} \equiv (3)^{25} \equiv (243)^5 \equiv 9^5 \equiv 59049 \equiv 3 \mod 13$

$10^{100} \equiv (10^2)^{50} \equiv 5^{50} \equiv (5^5)^{10} \equiv (9)^{10} \equiv (59049)^2 \equiv (16)^2 \equiv 256 \equiv 9 \mod 19$

iii) $m = m_1 m_2 = 247$

$M_1 = 19 \quad M_2 = 13$

$\begin{cases} 19y_1 \equiv 1 \mod 13 \\ 13y_2 \equiv 1 \mod 19 \end{cases} \Rightarrow \begin{cases} y_1 = 11 \\ y_2 = 3 \end{cases}$

$x = 11 \times 19 \times 3 + 3 \times 13 \times 9 = 978 \equiv 237 \mod 247$

Therefore, $r = 237$.

Ex 4.2 $4^n \equiv 7 \mod 9$

$4^n \equiv 9 \mod 11$

$m = 9 \times 11$

$M_1 = 11, \quad M_2 = 9$

$\begin{cases} 11y_1 = 1 \mod 9 \\ 9y_2 = 1 \mod 11 \end{cases}$

$y_1 = y_2 = 5$

$x = 5 \times 11 \times 7 + 5 \times 9 \times 9 = 790 \equiv 97 \mod 99$

$4^n = 97 + 99k$

Therefore $n = 8$

Ex 4.3 $45029^2 < 2027651281 < 45030^2$

$45030^2 - 2027651281 = 49619$

$45031^2 - 2027651281 = 139680$

$45032^2 - 2027651281 = 229743$

$45033^2 - 2027651281 = 319808$

$45034^2 - 2027651281 = 409875$

$45035^2 - 2027651281 = 499944$

$45036^2 - 2027651281 = 590015$

$45037^2 - 2027651281 = 680088$

$45038^2 - 2027651281 = 770163$

$45039^2 - 2027651281 = 860240$

$45040^2 - 2027651281 = 950319$

$45041^2 - 2027651281 = 1040044 = 1020^2$

Hence $2027651281 = (45041 + 1020)(45041 - 1020) = 46061 \cdot 44021$

Ex4.4 $5^6 \equiv 1 \mod 7$

$5^{2003} = 5^{6\times 333+5} = (5^6)^{333}\cdot 5^5$

$\equiv 5^5 \equiv 3125 \equiv 3 \mod 7$

$5^{10} \equiv 1 \mod 11$

$5^{2003} = 5^{10\times 200+3} = (5^{10})^{200}\cdot 5^3$

$\equiv 5^3 \equiv 1\times 5 \equiv 4 \mod 11$

$5^{12} \equiv 1 \mod 13$

$5^{2003} = 5^{12\times 166+11} = (5^{12})^{166}\cdot 5^{11}$

$= 5^{11} \equiv 8 \mod 13$

$M = 7\times 11\times 13 = 1001$

$m_1 = 143 \quad m_2 = 91 \quad m_3 = 77$

$$\begin{cases} 143y_1 \equiv 1 \mod 7 \\ 91y_2 \equiv 1 \mod 11 \\ 77y_3 \equiv 1 \mod 13 \end{cases} \Rightarrow \begin{cases} y_1 = 5 \\ y_2 = 4 \\ y_3 = 12 \end{cases}$$

$5^{2003} \equiv 5\times 143\times 3 + 4\times 91\times 4 + 12\times 77\times 8 \equiv 10993 \equiv 983 \mod 1001$

Ex4.5 i) If p is not prime,

we have $p = m\cdot n$, where $1 < m \le n < p$.

For $m \neq n$,

$(p-1)! = 1\times 2\times\cdots\times m\times\cdots\times n\times\cdots\times p-1$

$(p-1)! \equiv 0 \mod p$

For $m = n$, the range of m, n is $[2, \frac{p}{2}]$,

therefore, $(\frac{p}{2})^2 \le p \Rightarrow p(p-4) \le 0$.

Also p is not prime, then $p = 4$, $m = n = 2$

$3! \equiv 6 \equiv 2 \mod 4$

Therefore, both $m \neq n$ or $m = n$ contradicts with $(p-1)! \equiv -1 \mod p$.

Therefore, if $(p-1)! \equiv -1 \mod p$, then p is prime.

ii) Let $m = 2k+1$, then $z = k$.

We need to prove $(2k)! \equiv (-1)^k (k!)^2 \mod (2k+1)$

$k+n = 2k+1+n-k-1 \equiv n-k-1 \mod 2k+1$

$k+n \equiv -(k+1-n) \mod 2k+1$

$\prod_{n=1}^{k} (k+n) \equiv (-1)^k \prod_{n=1}^{k} (k+1-n) \equiv (-1)^k k! \mod 2k+1$

$k! \prod_{n=1}^{k} (k+n) \equiv (2k)! \equiv (-1)^k (k!)^2 \mod 2k+1$

Since $m = 2k+1$, $z = k$, we have

$(m-1)! \equiv (-1)^z (z!)^2 \mod m$, where $z = \frac{m-1}{2}$

iii) Let m be odd. If m is also prime.

Then $(m-1)! \equiv -1 \mod m$

$(m-1)! \equiv (-1)^z (z!)^2 \mod m$, where $z = \frac{m-1}{2}$

Therefore, if odd integer m satisfies: $(-1)^{\frac{m-1}{2}} (\frac{m-1}{2}!)^2 \equiv -1 \mod m$, then m is also prime.

Otherwise, it is not prime.

Ex4.6 i). $\gcd(a, 11)=1$

$x^2 \equiv a \mod 11$ has a solution

Due to the square of x, we can only consider non-negative x.

For $x \geq b$, we can find $x-11k$ such that $x-11k \in [-5, 5]$.

Also, due to the square, we can just consider $[0, 5]$.

0^2 doesn't satisfy.

$1^2 \equiv 1 \mod 11$

$2^2 \equiv 4 \mod 11$

$3^2 \equiv 9 \mod 11$

$4^2 \equiv 5 \mod 11$

$5^2 \equiv 3 \mod 11$

Therefore, the integers are 1, 3, 4, 5, 9

ii) $x^2 \equiv a \mod p$.

If it has no solution, we are done

If it has solution x_0, then $x_0^2 \equiv a \mod p$

$(-x_0)^2 \equiv a \mod p$.

Also $x_0 \bmod p \neq -x_0 \bmod p$

Therefore, it has either no solution or two incongruent solutions modulo p.

iii) Let $x^2 = ap+b$, then we have $x^2 \equiv b \mod p$.

For any $n \in \mathbb{Z}$, $(x+np)^2 = x^2+p^2n^2+2xnp = ap+b+n^2p^2+2xnp = (a+n^2p+2xn)p+b$

Therefore $(x+np)^2 \equiv b \mod p$.

$\Rightarrow x^2 \equiv (x+np)^2 \mod p$.

So we can just consider $[0, p-1]$.

Suppose $x_1 \neq x_2 \in [0, p-1]$ satisfying $x_1^2 \equiv x_2^2 \mod p$.

Then $x_1^2 - x_2^2 \equiv 0 \mod p$

$(x_1-x_2)(x_1+x_2) \equiv 0 \mod p$

Since x_1 and x_2 are in $[0, p-1]$ and p is odd prime, we have $p \nmid (x_1-x_2)$.

Therefore, $x_1+x_2 \equiv 0 \mod p$. Also, because of the range of x_1, x_2, we have $x_1+x_2=p$.

Hence there are $\frac{p-1}{2}$ quadratic

iv). If a is a quadratic residual of p, then $\left(\frac{a}{p}\right)=1$

Since $a \equiv b \mod p$, we have $b=a+np$.

$b^2 = a^2+n^2p^2+2anp = a^2+(n^2p+2an)p \equiv a^2 \mod p$.

Therefore, b is also quadratic. $\Rightarrow \left(\frac{b}{p}\right)=1=\left(\frac{a}{p}\right)$

If a is not a quadratic residual of p, $\left(\frac{a}{p}\right)=-1$.

Since $a \equiv b \mod p$, we have $b=a+np$.

$b^2 = a^2+n^2p^2+2anp = a^2+(n^2p+2an)p = a^2 \mod p$.

Therefore, b is also not quadratic residual $\Rightarrow \left(\frac{b}{p}\right)=-1=\left(\frac{a}{p}\right)$

v). ① If a is the quadratic residual of b.
then $\sqrt{a}$ and p are relatively prime, so $a^{\frac{p-1}{2}} \equiv 1 \equiv \left(\frac{a}{p}\right) \bmod p$.

② If a is not the quadratic residual of b.
Since p is odd prime, we can find $i, j \in [1, p-1]$ such that $ij \equiv a \bmod p$.
From 1 to $p-1$ can be divided into $\frac{p-1}{2}$ pairs, then $(p-1)! \equiv a^{\frac{p-1}{2}} \bmod p$.
We know $(p-1)! \equiv -1 \bmod p$.
Therefore $a^{\frac{p-1}{2}} \equiv -1 \equiv \left(\frac{a}{p}\right) \bmod p$.

Hence $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \bmod p$.

vi) $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = a^{\frac{p-1}{2}} \cdot b^{\frac{p-1}{2}} \bmod p$

$= (ab)^{\frac{p-1}{2}} \bmod p$

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

vii) If $p \equiv 1 \bmod 4$
$p = 4n+1$
$a = -1$
$\left(\frac{a}{p}\right) = (-1)^{\frac{4n}{2}} = 1$

Therefore, -1 is a quadratic residual of p.

If $p \equiv 3 \bmod 4$
$p = 4n+3$
$a = -1$
$\left(\frac{a}{p}\right) = (-1)^{2n+1} = -1$

Therefore, -1 is not a quadratic residual of p.

viii). $x^2 \equiv 29 \bmod 5 \Rightarrow x^2 \equiv 4 \bmod 5 \Rightarrow x = 2 \bmod 5$
$x = -2 \bmod 5$

$x^2 \equiv 29 \bmod 7 \Rightarrow x^2 \equiv 1 \bmod 7 \Rightarrow x = 1 \bmod 7$
$x = -1 \bmod 7$.

① $\begin{cases} x \equiv 2 \bmod 5 \\ x \equiv 1 \bmod 7 \end{cases}$
$M = 5 \times 7 = 35$
$m_1 = 5 \quad m_2 = 7$
$5y_1 = 1 \bmod 7$
$7y_2 = 1 \bmod 5$
$\Rightarrow y_1 = y_2 = 3$
$x = 3 \times 35 \times 1 + 3 \times 7 \times 2 = 57 \equiv 22 \bmod 35$
$x = 35k + 22$

② $\begin{cases} x \equiv 2 \bmod 5 \\ x \equiv -1 \bmod 7 \end{cases}$
Similarily $x = -1 \times 3 \times 5 + 3 \times 7 \times 2 \equiv 27 \bmod 35$
$x = 35k + 27$

③ $\begin{cases} x \equiv -2 \bmod 5 \\ x \equiv 1 \bmod 7 \end{cases}$
$x = 1 \times 3 \times 5 - 2 \times 3 \times 7 = -27 \bmod 35$
$x = 35k - 27$

④ $\begin{cases} x \equiv -2 \bmod 5 \\ x \equiv -1 \bmod 7 \end{cases}$
$x = -2 \times 3 \times 7 - 1 \times 3 \times 5 = -57 \equiv -22 \bmod 35$
$x = 35k - 22$.

$\{x \mid x = 35k \pm 22 \text{ or } x = 35k \pm 27\}$