信息安全数学基础 第四次作业

BY 18340087 李晨曦

(1)

用Euler判别法， 得到：

模13的二次剩余为：

$$\{1,3,4,9,10,12\}$$

模13的二次非剩余为：

$$\{2,5,6,7,8,11\}$$

模23的二次剩余为：

$$\{1,2,3,4,6,8,9,12,13,16,18\}$$

模23的二次非剩余为：

$$\{5,7,10,11,14,15,17,19,20,21,22\}$$

模31的二次剩余为：

$$\{1,2,4,5,7,8,9,10,14,16,18,19,20,25,28\}$$

模31的二次非剩余为：

$$\{3,6,11,12,13,15,17,21,22,23,24,26,27,29,30\}$$

模37的二次剩余为：

$$\{1,3,4,7,9,10,11,12,16,21,25,26,27,28,30,33,34,36\}$$

模37的二次非剩余为：

$$\{2,5,6,8,13,14,15,17,18,19,20,22,23,24,29,31,32,35\}$$

模47的二次剩余为：

$$\{1,2,3,4,6,7,8,9,12,14,16,17,18,21,24,25,27,28,32,34,36,37,42\}$$

模47的二次非剩余为：

$$\{5,10,11,13,15,19,20,22,23,26,29,30,31,33,35,38,39,40,41,43,44,45,46\}$$

(12)

首先分解1155为：

$$1155 = 3\times 5\times 7\times 11$$

原方程为:

$$
\begin{aligned}
x^2 &\equiv 1 \pmod{3} \quad (1)\\
x^2 &\equiv 1 \pmod{5} \quad (2)\\
x^2 &\equiv 0 \pmod{7} \quad (3)\\
x^2 &\equiv 5 \pmod{11} \quad (4)
\end{aligned}
$$

解(1)得:

$$x \equiv \pm 1 \pmod{3}$$

解(2)得:

$$x \equiv \pm 1 \pmod{5}$$

解(3)得:

$$x \equiv 0 \pmod{7}$$

解(4), 由于$11 = 4 \times 2 + 3$, 可以直接得到:

$$x \equiv \pm 5^{\frac{12}{4}} \pmod{11}$$

即:

$$x \equiv \pm 4 \pmod{11}$$

所以我们得到8组方程, 用中国剩余定理得到:

$$
\begin{aligned}
x &\equiv 224 \pmod{1155}\\
x &\equiv 994 \pmod{1155}\\
x &\equiv 686 \pmod{1155}\\
x &\equiv 301 \pmod{1155}\\
x &\equiv 854 \pmod{1155}\\
x &\equiv 469 \pmod{1155}\\
x &\equiv 161 \pmod{1155}\\
x &\equiv 931 \pmod{1155}
\end{aligned}
$$

(20)

1

$$
\begin{aligned}
\left(\frac{17}{37}\right) &= \left(\frac{37}{17}\right)\\
&= \left(\frac{3}{17}\right)\\
&= \left(\frac{2}{3}\right)\\
&= -1
\end{aligned}
$$

2

$$
\begin{aligned}
\left(\frac{151}{373}\right) &= \left(\frac{71}{151}\right) \\
&= -\left(\frac{9}{71}\right) \\
&= -\left(\frac{3}{71}\right)\left(\frac{3}{71}\right) \\
&= -1
\end{aligned}
$$

3

$$
\begin{aligned}
\left(\frac{191}{397}\right) &= \left(\frac{15}{191}\right) \\
&= \left(\frac{3}{191}\right)\left(\frac{5}{191}\right) \\
&= \left(\frac{2}{3}\right) \times -\left(\frac{1}{5}\right) \\
&= 1
\end{aligned}
$$

4

$$
\left(\frac{911}{2003}\right) = 1
$$

5

$$
\left(\frac{37}{200723}\right) = -1
$$

6

$$
\left(\frac{7}{20040803}\right) = 1
$$

(22)

1

$$
\begin{aligned}
\left(\frac{-2}{67}\right) &= \left(\frac{65}{67}\right) \\
&= \left(\frac{2}{65}\right) \\
&= 1
\end{aligned}
$$

所以， 它有两个解

2

$$
\left(\frac{2}{67}\right) = -1
$$

所以， 它无解

3

$$\begin{aligned}\left(\frac{-2}{37}\right) &= \left(\frac{35}{37}\right)\\ &= \left(\frac{5}{37}\right)\left(\frac{7}{37}\right)\\ &= \left(\frac{2}{5}\right)\left(\frac{2}{7}\right)\\ &= -1\times 1\\ &= -1\end{aligned}$$

所以， 它无解。

4

$$\left(\frac{2}{37}\right) = -1$$

所以， 它无解。

(24)

(i)

我们知道， 模p的任意二次剩余q， 都有：

$$\exists x\in A, x^2\equiv q \pmod p$$

其中A为：

$$A=\left\{-\frac{p-1}{2}, -\frac{p-2}{2}\ldots-1, 1\ldots\frac{p-1}{2}\right\}$$

对于所有的模p的二次剩余q， 任取一个对应的x， 构成集合B。显然，$B\subset A$。
对于任意的q， 如果对应的$x<0$， 我们有：

$$(-x)^2\equiv x^2 \pmod p$$

在集合B中， 用$-x$替换这个q对应的x。
这样一来， 集合B中所有的元素都是正数， 且$|B|=|\{q\}|=\frac{p-1}{2}$。
所以， 一定有：

$$B=\left\{1\ldots\frac{p-1}{2}\right\}$$

那么，

$$\prod_{i=1}^{\frac{p-1}{2}} q_i\equiv\prod_{i=1}^{\frac{p-1}{2}} x_i^2|x_i\in B\equiv\prod_{i=1}^{\frac{p-1}{2}} i^2 \pmod p\equiv\left(\left(\frac{p-1}{2}\right)!\right)^2 \pmod p$$

在第二章作业的第(26)小题中， 我们已经证明过：

$$\left(\left(\frac{p-1}{2}\right)!\right)^2\equiv(-1)^{\frac{p+1}{2}} \pmod p$$

所以，

$$\prod_{i=1}^{\frac{p-1}{2}} q_i \equiv (-1)^{\frac{p+1}{2}} \pmod p$$

(ii)

由Wilson定理， 我们知道：

$$\prod_{i=1}^{p-1} i \equiv -1 \pmod p$$

记第i个模p的二次剩余为q_i， 模p的二次非剩余为r_i， 我们有：

$$\left(\prod_{i=1}^{\frac{p-1}{2}} q_i\right)\left(\prod_{i=1}^{\frac{p-1}{2}} r_i\right) = \prod_{i=1}^{p-1} i$$

所以：

$$\begin{aligned}
\left(\prod_{i=1}^{\frac{p-1}{2}} r_i\right)(-1)^{\frac{p+1}{2}} &\equiv -1 \pmod p \\
\left(\prod_{i=1}^{\frac{p-1}{2}} r_i\right)(-1)^{p+1} &\equiv (-1)^{\frac{p+3}{2}} \pmod p \\
\left(\prod_{i=1}^{\frac{p-1}{2}} r_i\right) &\equiv (-1)^{\frac{p-1}{2}}(-1)^2 \pmod p \\
\left(\prod_{i=1}^{\frac{p-1}{2}} r_i\right) &\equiv (-1)^{\frac{p-1}{2}} \pmod p
\end{aligned}$$

证毕。

(iii)

继续利用(i)中的构造， 有：

$$\sum_{i=1}^{\frac{p-1}{2}} q_i \equiv \sum_{i=1}^{\frac{p-1}{2}} i^2 \pmod p$$

计算可知：

$$\sum_{i=1}^{\frac{p-1}{2}} i^2 = \frac{p\,(p+1)\,(p-1)}{24}$$

如果$p=3$，上式的值为1；

如果$p\neq 3$，

对于$p\equiv 1\pmod 3$，我们有：

$$(p-1)\equiv 0\pmod 3$$

对于$p\equiv 2(\bmod 3)$，我们有：

$$(p+1)\equiv 0\pmod 3$$

所以，

$$3\,|\,(p+1)\,(p-1)$$

而对于$p\equiv 1\pmod 4$，我们有：

$$\begin{array}{rcl}(p+1) & \equiv & 2\pmod 4\\ 2 & | & (p+1)\\ (p-1) & \equiv & 0\pmod 4\\ 4 & | & (p-1)\end{array}$$

同理，对于$p\equiv 3\pmod 4$，我们也有：

$$\begin{array}{rcl}4 & | & (p-1)\\ 2 & | & (p+1)\end{array}$$

所以，

$$8\,|\,(p+1)\,(p-1)$$

所以，

$$24\,|\,(p+1)\,(p-1)$$

这样一来：

$$\begin{array}{rcl}\sum_{i=1}^{\frac{p-1}{2}} i^2 & \equiv & \frac{p\,(p+1)\,(p-1)}{24}\pmod p\\ & \equiv & tp\pmod p\\ & \equiv & 0\pmod p\end{array}$$

综上所述：

$$\sum_{i=1}^{\frac{p-1}{2}} q_i\equiv\left\{\begin{array}{l}1\pmod p, p=3\\ 0\pmod p, p\neq 3\end{array}\right.$$

(iv)

由于

$$\sum_{i=1}^{p-1} i=\frac{(p-1)p}{2}$$

对于任意的奇素数p， 有：

$$2\,|\,(p-1)$$

所以，

$$\begin{aligned}\sum_{i=1}^{p-1} i &\equiv \frac{(p-1)p}{2} \pmod p \\ &\equiv tp \pmod p \\ &= 0 \pmod p\end{aligned}$$

所有的二次非剩余(r_i)之和为：

$$\begin{aligned}\sum_{i=0}^{\frac{p-1}{2}} r_i &= \sum_{i=1}^{p-1} i - \sum_{i=1}^{\frac{p-1}{2}} q_i \\ &= \begin{cases} -1 \pmod p, p=3 \\ 0 \pmod p, p\neq 3 \end{cases}\end{aligned}$$

(37)

由于$401-1=400$，$400=2^4\times 25$， 人工计算比较麻烦。我们写程序解决此问题：

```
(#%require (only racket/base random))
(#%require math/number-theory)

(define (modulo-muti a b p)
  (modulo (* a b) p))

(define fast-pow
  (lambda (a b p)
    (if (= b 0)
        1
        (let ((ret (fast-pow a (floor (/ b 2)) p)))
          (if (= (modulo b 2) 1)
              (modulo-muti (modulo-muti ret ret p) a p)
              (modulo-muti ret ret p))))))

(define Euler-pre
  (lambda (a p)
    (= 1 (fast-pow a (/ (- p 1) 2) p))))

(define (rand-choose p)
  (let ((this-time (random p)))
    (if (or
         (= (modulo this-time p) 0)
         (Euler-pre this-time p))
        (rand-choose p)
        this-time)))

(define (get-2^n p)
  (if (= (modulo p 2) 0)
      (let ((res (get-2^n (/ p 2))))
        (cons (+ (car res) 1)
```

```scheme
                (cdr res)))
        (cons 0 p)))

  (define (pow a b)
    (if (= b 0)
        1
        (* a (pow a (- b 1)))))

  (define (solve-quad-res a p)
    (define a-1 (modular-inverse a p))
    (define t (car (get-2^n (- p 1))))
    (define s (cdr (get-2^n (- p 1))))
    (define b (fast-pow 3 25 p))
    (define (solve x_t t-k)
      (if (= t-k 0)
          x_t
          (let* ((a-1x^2 (modulo-muti a-1 (modulo-muti x_t x_t p) p))
                 (y^t-k-1 (fast-pow a-1x^2 (pow 2 (- t-k 1)) p)))
            (solve
             (if (= y^t-k-1 1)
                 x_t
                 (modulo-muti x_t (fast-pow b (pow 2 (- (- t 1) t-k)) p) p))
             (- t-k 1)))))
    (solve (fast-pow a (/ (+ s 1) 2) p) (- t 1)))

  (solve-quad-res 186 401)
  (solve-quad-res 2 401)
  (solve-quad-res 3 401)
  (solve-quad-res 5 401)
  (solve-quad-res 7 401)
  (solve-quad-res 11 401)
```

得到:

i. $x \equiv \pm 348 \pmod{401}$

ii. $x \equiv \pm 280 \pmod{401}$

iii. $x \equiv \pm 178 \pmod{401}$

iv. $x \equiv \pm 85 \pmod{401}$

v. $x \equiv \pm 326 \pmod{401}$