信息安全数学基础 第五次作业

BY 1834087 李晨曦

(2)

使用枚举法，编写程序计算：

```
(#%require math/number-theory)

(define (find-ord x p)
  (define (iter i)
    (if (= (modular-expt x i p) 1)
        i
        (iter (+ i 1))))
  (iter 1))

(find-ord 3 19)
(find-ord 7 19)
(find-ord 10 19)
```

得到结果：

$$\begin{aligned} \mathrm{ord}_{19}(3) &= 18 \\ \mathrm{ord}_{19}(7) &= 3 \\ \mathrm{ord}_{19}(10) &= 18 \end{aligned}$$

(3)

首先枚举出最小原根：

```
(define (find-smallest-root p)
  (define (iter i)
    (if (= (find-ord i p) (totient p))
        i
        (iter (+ i 1))))
  (iter 2))
```

然后用$\{s^i\}$枚举出所有的原根：

```
(define (all-root p)
  (define s (find-smallest-root p))
  (define (iter i)
    (if (> i (totient p))
        '()
        (if (coprime? i (totient p))
            (cons (modular-expt s i p) (iter (+ i 1)))
            (iter (+ i 1)))))
  (iter 1))
```

对这个问题，我们使用：

```
(all-root 81)
```

得到：

```
(2 32 47 23 11 14 56 5 20 77 65 68 29 59 74 50 38 41)
```

模81的原根即为上面列表中的数。

(6)

首先求得：

$$\varphi(59)=58$$

然后，模59的原根的个数为：

$$\varphi(\varphi(59))=28$$

用刚才的程序求得所有的原根为：

```
(2 8 32 10 40 42 50 23 33 14 56 47 11 44 55 43 54 39 38 34 18 13 52 31 6 24 37
30)
```

(8)

如果模n有原根，则存在；如果模n没有原根，则不一定存在。

证明.

首先证明如果n有原根，则存在整数a使得$\mathrm{ord}_n(a)=d$：

对于$\varphi(n)$的任意正因子d，我们取$k=\frac{\phi(n)}{d}$，

这样一来，任取一个模n的原根r，有：

$$\begin{aligned}\mathrm{ord}_n(r^k) &= \frac{\mathrm{ord}_n(r)}{(\mathrm{ord}_n(r),k)} \\ &= \frac{\varphi(n)}{(\varphi(n),k)} \\ &= \frac{\varphi(n)}{\frac{\varphi(n)}{d}} \\ &= d\end{aligned}$$

故r^k即是要找的a.

然后证明如果模n没有原根，则不一定存在整数a使得$\mathrm{ord}_n(a)=d$：

如果令$d=\phi(n)$，由于不存在原根，所以不存在这样的a；

令$d=2$，则有：$\mathrm{ord}_n(n-1)=d$.

所以，不一定存在整数a，使得$\mathrm{ord}_n(a)=d$. □

(9)

显然地，

$$a^n\equiv 1\ (\mathrm{mod}\ a^n-1) \tag{1}$$

当$k<n$时：

$$0<a^k<a^n-1$$

且

$$a^k\neq 1$$

所以

$$a^k\not\equiv 1 \pmod{a^n-1} \tag{2}$$

综合(1)(2)，我们有：

$$\mathrm{ord}_n(a)=n$$

自然地，

$$n\mid\varphi(m)$$

(17)

41是质数，它一定有原根。
找到一个原根6，我们通过枚举计算得：

$$\mathrm{ind}_6(29)=7$$

这样一来，我们得到同余方程：

$$22u=7 \pmod{40}$$

由于

$$2\nmid 7$$

这个方程是无解的，所以原方程也无解。