课程讨论

TC第31章1、2、3、4、5、8

问题1：大数相乘

- 何为大数相乘？
- 大数相乘的复杂度衡量？
  - 比特操作（bit operation）
- 两个β比特的整数相乘的代价？
  - $\Theta(\beta^2)$

问题2：Euclid算法

- Euclid算法基本思想
  - gcd(a, b) = gcd (b, a mod b)
- 算法复杂性分析
  - 构造最坏输入（adversary）
  - Fib数列

Euclid Algorithm and Fibonacci

- If $m>n\geq 1$ and the invocation Euclid(m,n) performs $k\geq 1$ recursive calls, then $m\geq F_{k+2}$ and $n\geq F_{k+1}$.
  - Proof by induction
  - Basis: $k=1$, then $n\geq 1=F_2$. Since $m>n$, $m\geq 2=F_3$.
  - For larger k, Euclid(m,n) calls Euclid(n, m mod n) which makes k-1 recursive calls. So, by inductive hypothesis, $n\geq F_{k+1}$, (m mod n)$\geq F_k$.

  Note that $m \geq n+(m-\lfloor m/n \rfloor n) = n+(m \bmod n) \geq F_{k+1}+F_k = F_{k+2}$

问题3：Extended-Euclid算法

- E-Euclid算法的作用？
  - $d = \gcd(a, b) = ax + by$
- E-Euclid算法的原理
  - $(d, x, y) = (d', y', x' - \lfloor a/b \rfloor y')$

问题4：Z_n与Z_n*

- Z_n与Z_n*的基本含义
  - Z_n：模n加法群，有限交换群
  - Z_n*：模n乘法群，群中元素是Z_n中与n互质元素。
- $Z_n = \langle a \rangle$的条件是什么？
  - a与n互质
  - 如果a不能生成Z_n，那么$\langle a \rangle$的特征是什么？
- $\Phi(n)$与$\pi(n)$的含义
  - $\Phi(n)$为Z_n*的规模。
  - $\pi(n)$为小于n的质数个数。

问题5：元素的幂

- 模取幂，即$a^b \bmod n$
  - 反复平方法

```
MODULAR-EXPONENTIATION(a, b, n)
c = 0
d = 1
let ⟨b_k, b_{k-1}, ..., b_0⟩ be the binary representation of b
for i = k downto 0
    c = 2c
    d = (d · d) mod n
    if b_i == 1
        c = c + 1
        d = (d · a) mod n
return d
```

问题6：素性判定

- 为什么要进行素性判定？
- 筛法为何不能有效用于判定素性？
- 伪素数测试过程

```
PSEUDOPRIME(n)
if MODULAR-EXPONENTIATION(2, n − 1, n) ≢ 1 (mod n)
    return COMPOSITE          // definitely
else return PRIME             // we hope!
```

- 欧拉定理与费马定理

Theorem 31.31 (Fermat's theorem)
If p is prime, then

$$a^{p-1} \equiv 1 \pmod{p} \text{ for all } a \in \mathbb{Z}_p^* .$$

问题7：Miller-Rabin算法

- M-R算法对素性判定的改进体现在？
  - 多个随机选取的a值
  - 寻找非平凡平方根

```
WITNESS(a, n)
let t and u be such that t ≥ 1, u is odd, and n − 1 = 2^t u
x_0 = MODULAR-EXPONENTIATION(a, u, n)
for i = 1 to t
    x_i = x_{i-1}^2 mod n
    if x_i == 1 and x_{i-1} ≠ 1 and x_{i-1} ≠ n − 1
        return TRUE
if x_t ≠ 1
    return TRUE
return FALSE
```

问题8：M-R算法的准确性

- M-R算法为什么出错?
  - 出错并不依赖于n，也不存在坏的输入
  - 取决于s的大小与a值选择

Theorem 31.39
For any odd integer $n > 2$ and positive integer s, the probability that MILLER-RABIN(n, s) errs is at most 2^{-s}.