31.7-3 ★

Prove that RSA is multiplicative in the sense that

$$P_A(M_1)P_A(M_2) \equiv P_A(M_1M_2) \pmod{n} .$$

Use this fact to prove that if an adversary had a procedure that could efficiently decrypt 1 percent of messages from $\mathbb{Z}_n$ encrypted with P_A, then he could employ a probabilistic algorithm to decrypt every message encrypted with P_A with high probability.

in each iteration randomly choose a prime number m which is relatively prime to n

if we decrypt $m \cdot M$ then we can find $m^{-1}M$ because

$m^{-1} = m^{n-2}$

31.8-3

Prove that if x is a nontrivial square root of 1, modulo n, then $\gcd(x-1, n)$ and $\gcd(x+1, n)$ are both nontrivial divisors of n.

$$x^2 \equiv 1 \pmod{n}$$

$$x^2 - 1 \equiv 0 \pmod{n}$$

$$(x+1)(x-1) \equiv 0 \pmod{n}$$

if we assume $\gcd(n, x-1) = 1$ then $x+1$ is divisible by n, then $x \equiv -1 \pmod{n}$ which would make x trivial. Since it is explained to be nontrivial $\gcd(x-1, n) \neq 1$ and $\gcd(x+1, n) \neq 1$

15.2-2

Give a recursive algorithm MATRIX-CHAIN-MULTIPLY(A, s, i, j) that actually performs the optimal matrix-chain multiplication, given the sequence of matrices $\langle A_1, A_2, \ldots, A_n \rangle$, the s table computed by MATRIX-CHAIN-ORDER, and the indices i and j. (The initial call would be MATRIX-CHAIN-MULTIPLY$(A, s, 1, n)$.)

```
Matrix chain multiply(A, S, i, j)
 if(i == j)   // one arr val
      return A[i]  // return
 if(j = i + 1) // if only 1 multiplication
      return A[i] * A[j] // return after done
 else
      X1 = Matrix Chain multiply(A, S, i, S[i, j])
      X2 = Matrix chain multiply( A, S, S[i, j]+1, j)
      return X1 * X2
```

15.2-3

Use the substitution method to show that the solution to the recurrence (15.6) is $\Omega(2^n)$.

$$P(n) = \begin{cases} 1 & \text{if } n = 1\,, \\ \sum_{k=1}^{n-1} P(k)P(n-k) & \text{if } n \geq 2\,. \end{cases} \tag{15.6}$$

3

$$P_n = \begin{cases} 1 \text{ if } n=1 \\ \sum P(k)\, P(n-k) \end{cases}$$

$k = 1 .. n-1$

$P(1) * P(2-1) \geq \frac{1}{4} 2^2$

$P(1) * P(1) \geq 1$

$P(1) * P(3-1) + P(2)\, P(3-2) \geq \frac{1}{4} 2^3$

$1 \quad 1 \quad 1 \quad 1 \qquad \frac{1}{4} 8 = 2$

$4 \geq 2$

$P(1) * P(4-1) + P(2)\, P(4-2) \geq \frac{1}{4} 2^4$

$1 \quad 4 \quad 1 \quad 1 \quad 1$

$2 \quad 4 \quad 8 \quad 16$

$\frac{1}{4} 2^n == 2^{n-2}$

$P(1) * P(5-1) + P(2)\, P(5-2$

$8 + 4 + 1 + 1$

$P(n) = P(n-1) + P(n-2)$

$P(n+1) = P(n-1+1) + P(n-2+1) \ldots P(1) \geq 2^{n-2}$

$P(n+1) = P(n) + P(n-1) \ldots P(1) \geq 2^{n-1}$

$P_n = \sum_{k=1}^{n-1} P(k)\; P(n-k)$

$P(n+1) = \sum_{k=1}^{(n-1)+1} P(k)\, P((n+1)-k) \geq 2^{n-2+1}$

$P(n+1) = \sum_{k=1}^{n} P(k)\; P((n+1)-k) \geq 2^{n-1}$

$$P(n) + \sum_{k=1}^{n-1} P(k)\,P(n-k) \geq 2^{n-1}$$

$$P(n) \geq 2^{n-2} \qquad 2^{n-1} - 2^{n-2}$$

$$\sum_{k=1}^{n-1} P(k)\,P(n-k) \geq 2^{n-1} - 2^{n-2}$$

$16 - 8 = 8$

$8 - 4 = 4$

$$2^{n-1} - 2^{n-2} = 2^{n-2}$$

remove $P(n)$ and $\geq 2^{n-2}$ from both sides as they are both true

$$\sum_{k=1}^{n-1} P(k)\,P(n-k) \geq 2^{n-2}$$

$$P(n) \geq 2^{n-2} \quad \text{or} \quad P(n) \geq \frac{1}{4}2^n$$

15.2-4

Describe the subproblem graph for matrix-chain multiplication with an input chain of length n. How many vertices does it have? How many edges does it have, and which edges are they?

if $i == j$ vertex V_{ij} has no output edge

if $i < j$ for each k such that $i \le k < j$ the subproblem graph contains edges $V_{ij}\ V_{ik}$ and $(V_{ij}, V_{k+1,j})$ and these edges indicate that to solve $A_i \ldots A_j$ we need to solve $A_i \ldots A_k$, $A_{k+1} \ldots A_j$

Verticies $\frac{n(n+1)}{2} = \sum_{i=1}^{n} \sum_{j=1}^{n}$

edges $\frac{(n-1)n(n+1)}{6} = \sum_{i=1}^{n} \sum_{j=1}^{n} (j-i)$

15.2-6

Show that a full parenthesization of an n-element expression has exactly $n-1$ pairs of parentheses.

always need 1 operator and

$n-1$ things to operatr with

$(n_1 + n_2)$ first eq has 2 elements

every subsequent contains 1 element

and the original 2