----------------------------- 31 -----------------------------

Number-Theoretic Algorithm

31.2 Greatest common divisor

31-1x

Simple methods: (1) $O(b)$ (2) $O(b^{1/2})$

Theorem 31.9: For any nonnegative integer *a* and positive integer *b*,

$a \geq 0, b > 0$

$\underline{gcd(a, b)=gcd(b, a \bmod b)}$.

$gcd(12, 9)$
$= gcd(9, 3)$
$= gcd(3, 0)$
$= 3$

Euclid's algorithm

$a \geq 0, b \geq 0$ (check outside)

EUCLID(a, b)

1 **if** $\underline{b = 0}$
2 **then return** a
3 **else return** EUCLID$(b, a \bmod b)$

* $T(a, b)=O(\log(\min\{a, b\}))$

Hint:
$gcd(a, b)$
$= gcd(b, x)$
$= gcd(x, y)$
$\Rightarrow x \leq a/2, y \leq b/2$

31.6 Powers of an element

Input: x, a
Output: x^a

A simple method: $x^1 \xrightarrow[*x]{} x^2 \xrightarrow[*x]{} x^3 \xrightarrow[*x]{} x^4 \xrightarrow[*x]{} \ldots \xrightarrow[*x]{} x$
---> $O(a)$ time

$n = \lfloor \lg a \rfloor + 1$ bits

* Let $a_{n-1}a_{n-2}\ldots a_1a_0$ be the binary representation of *a*. We have

$$x^a = \prod_{a_i=1} x^{2^i}$$

b: binary
d: decimal

Example:

$$x^{21_d} = x^{10101_b} = x^{10000_b} \times x^{00100_b} \times x^{00001_b} = x^{16_d} \times x^{4_d} \times x^{1_d}$$

16, 4, 1

31-2a

Algorithm Power(*x*, *a*) **(right-to-left)**

```
    s=1
    while a>0 do          { n = ⌊lg a⌋ + 1
                          { for i = 0 to n-1 do
    begin
                 if ai = 1 ?
      if (a mod 2)=1      (check the rightmost bit)
        then s=s*x        x, x^2, x^4, x^8, ...
      x=x*x               (repeated squaring)
      a=a div 2           (shift-right one bit)
    end
    return s
```

* $T(x, a)=O(\log a)$

Homework: Prob. 31-1.