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

Number-Theoretic Algorithm

31.2 Greatest common divisor

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

$$gcd(a, b)=gcd(b, a \bmod b).$$

Euclid's algorithm

```
EUCLID(a, b)
1  if b = 0
2      then return a
3      else return EUCLID(b, a mod b)
```

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

31.6 Powers of an element

Input: x, a
Output: x^a

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

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

Example:

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

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

```
s=1
while a>0 do
begin
   if (a mod 2)=1      (check the rightmost bit)
      then s=s*x
   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.