07.08.2024

- gcd
- powering.

} Cryptographic protocols.

Greatest Common Divisor

$(6, 12) \rightarrow 6$.

Euclid's algorithm

Fact: $\gcd(\overset{16}{x}, \overset{12}{y}) = \gcd(\overset{12}{y}, \overset{4}{x \bmod y})$

$x \geq y$

pmf: [sketch]

$$x = qy + r$$

any number that divides x, y, $\Leftrightarrow$ d also divides (y, r)

$\Rightarrow$

$$\gcd(x,y) \geq \gcd(y,r)$$

$$\leq$$

$\gcd(y,r)$ ↓ $x \bmod y$.

```
Procedure GCD (x, y)
// x ≥ y
 if (y = 0)  return x  else
  else  return gcd(y, x mod y)
```

Correctness ? Obvious

Time complexity ? $(x, y) \rightarrow (y, x \bmod y)$.

~~12~~ $(12, 7) \rightarrow (7, 5)$

$2n$ $\theta(n^2) = \theta(n^3)$

gcd $\rightarrow$ $O(n^3)$ time

$n \leftarrow$ # bits of x, y

Fact. If $\gcd(x,y) = d$, then $\exists$ integers a, b such that

$$ax + by = d.$$

Example:

$\gcd(25, 11)$

$\gcd(11, 3)$

$\gcd(3, 2)$

$\gcd(2, 1)$

$\gcd(1, 0) \rightarrow 1$

$1 = 1 \cdot 1 - 1 \cdot 0$

$= 1 \cdot 1 + 2 \cdot 1 - 2 \cdot 1$

$= 1 \cdot 1 + (2 - 2 \cdot 1) \cdot \#1$

$= 1 \cdot 1 + 0 \cdot \#1$

$2 = 2 \cdot 1 + 0$

$1 = 1 \cdot 1 + 0 \cdot \#1$

$$1 = 2 \cdot 1 - 1 \cdot 1$$

$$3 = 1 \cdot 2 + 1$$

$$1 = 2 \cdot 1 - (3 - 1 \cdot 2)\,1$$

$$= (2 \cdot 1 + 1 \cdot 2) - 3$$

$$= 2 \cdot 2 - 3 \quad \rightarrow (2, -1)$$

$$11 = 3.3 + 2.$$

$$1 = 2.2 + (-1).3$$

$$= (11 - 3.3).2 + (-1)3$$

$$= 11.2 + 3[(-1) + -6]$$

$$= 11.2 + 3(-7)$$

$$25 = 2.11 + 3$$

$$1 = 11.2 + 3(-7)$$

$$= 11.2 + (25 - 2.11)(-7)$$

$$1 = 11.16 - 25.7$$

$$(16, -7)$$

$$\boxed{1 = 15.25 - 39.11}$$

proof of fact :

(x, y) $\quad ax + by = d$

a ? $\quad b$?

$(y, x \bmod y) \quad a'y + b'(x \bmod y) = d.$

$x = qy + (x \bmod y)$

$a'y + b'(x - qy) = d$

$y(a' - qb') + b'x = d$ □

b $\quad a$

Exponentiation / Powering

$a, b, N \leftarrow$ n-bit numbers (+ve integers)

$(a^b \bmod N)$

$(a * a) \bmod N, \quad \cdots \quad (a^{b-1} \bmod N)$

$O(b)$ $\Theta(n^m)$ poly(n)

$(2^{2^{10}}) \bmod (2^{50})$

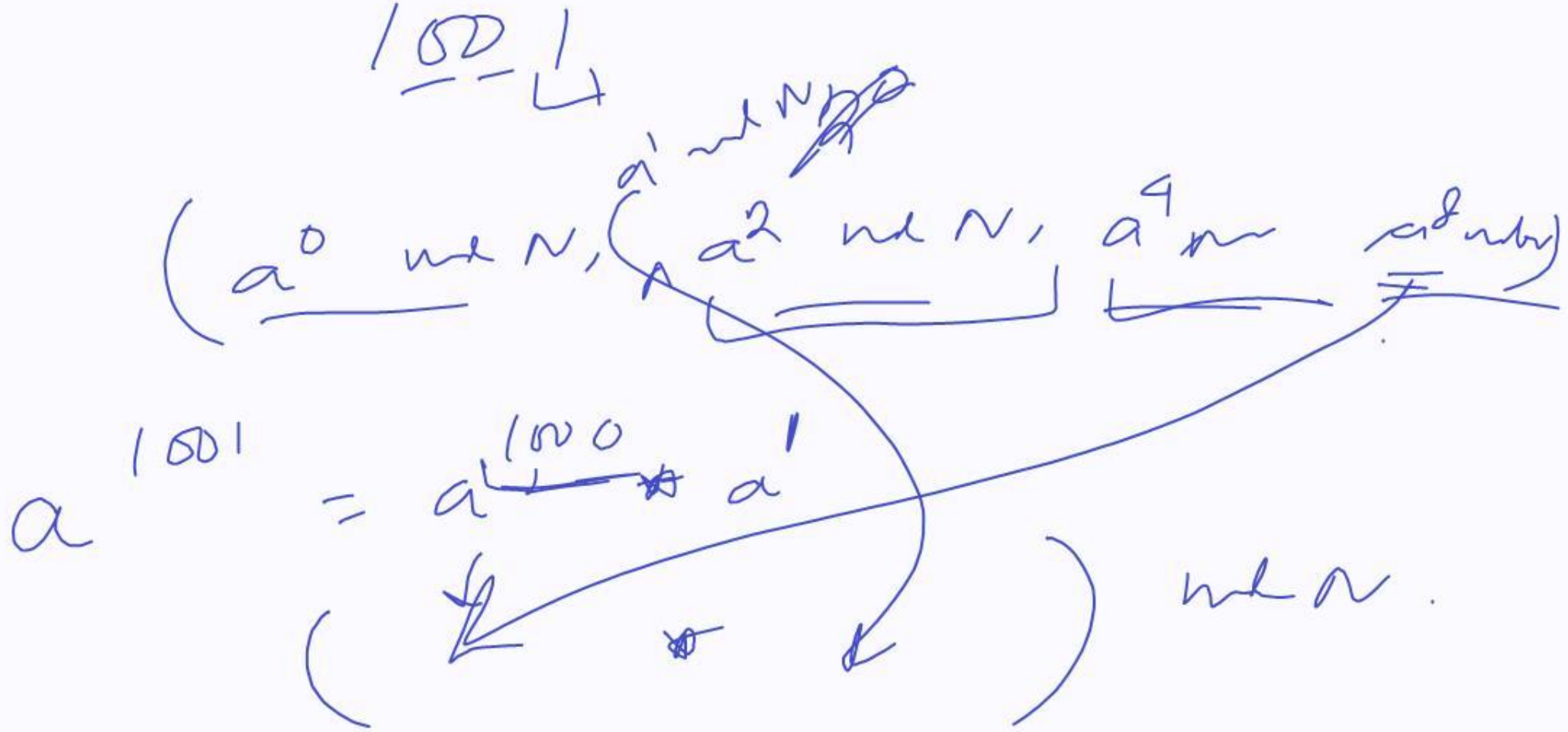
$a * a \bmod N \to a^2 \bmod N$

$(a^2 \bmod N * a^2 \bmod N) \bmod N \to a^4 \bmod N$.

$\vdots$

$(a^{2^j} \bmod N) \to j$ steps

What if b is not a perfect power of 2?



```
Procedure Power (a, b, N)
    // a, b, N are t-indexed n-bit numbers.
    result ← 1
    factor ← a
    for j = 1 to n
        if (b[j] = 0)
            factor ← (factor * factor) mod N.
            Continue
        else
            result ← (result * factor) mod
```

factor ← (factor * factor) mod N.

end if

return result

Correctness: Obvious.

time complexity ? $\Theta(n)\,\Theta(n^2) = \Theta(n^3) \rightarrow$ (or) n.

$= \Theta(6n) \equiv 2^{\omega} n$

Remarks

N, # bits $= n$

$2^{100} \to 100 \equiv n \approx \log N$.

Primality Testing.

N

$O(\sqrt{N}) = O(2^{n/2})$

$1 \times N$

$2 \times ?$

$\vdots$

$O(\log^3 n)$

poly(N)

$\downarrow$

poly($\log n$)

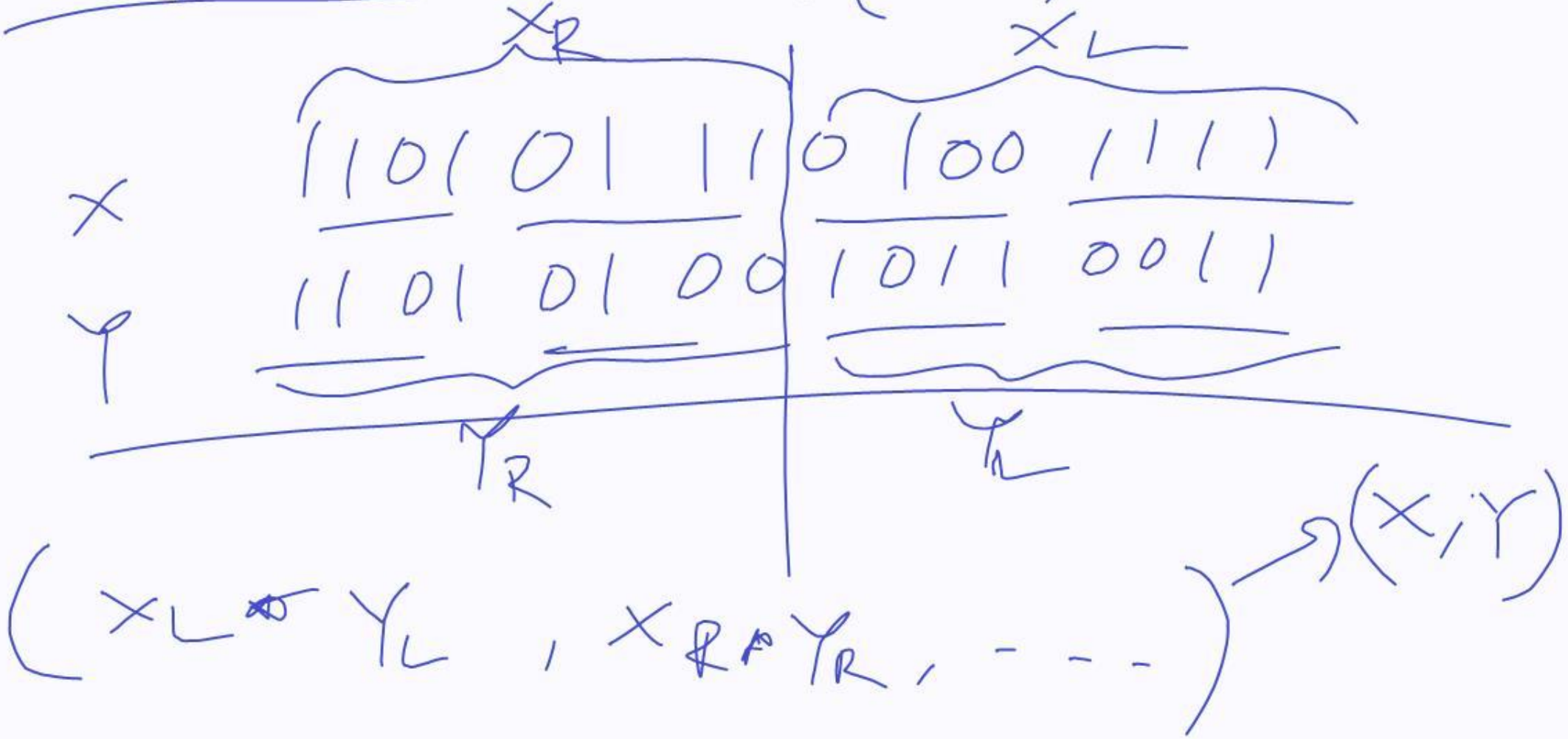
Manindra Agrawal

Nitin Saxena

Kayal

Module 3 : Divide & Conquer algorithm

Integer multiplication $O(n^{1.3})$



X : n bits, Y : n bits, n is a power of 2

$$n = 2^k.$$

$$X = X_L + X_R \cdot 2^{n/2}$$

$$Y = Y_L + Y_R \cdot 2^{n/2}$$

$$(X \cdot Y) = \underbrace{X_L Y_L}_{T(n)} + \underbrace{(X_L Y_R + X_R Y_L)}_{T(n)} 2^{n/2} + \underbrace{X_R Y_R \cdot 2^n}_{T(n)}$$