一个公式引发的算法学习惨案

胡船长
初航我带你，远航靠自己

引出问题

大约用时：（5 mins）

下一部分：欧几里得算法

一个令人头秃的问题

$$a^x \ mod \ b = c$$

已知 a，b 互质，给出 a、b、c 三个正整数，求 x 的最小正整数解

欧几里得算法

大约用时：（15 mins）

下一部分：扩展欧几里得算法

欧 几 里 得 算 法

整数 a, b 的最大公约数一般表示为 gcd(a, b)

终极奥义: gcd(a, b) = gcd(b, a%b)

证明1：b和a%b的最大公约数，是a和b的公约数

证明2：b和a%b的最大公约数也是a和b的最大公约数

欧几里得算法-证明1

欧几里得算法-证明2

扩展欧几里得算法

大约用时：（15 mins）

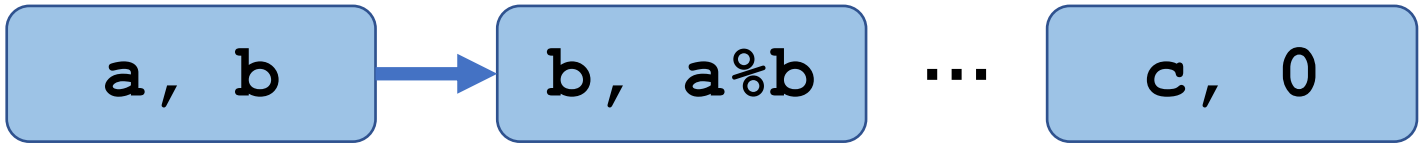
下一部分：数论中的欧拉公式

贝 祖 等 式

$$ax + by = \gcd(a, b) = c$$

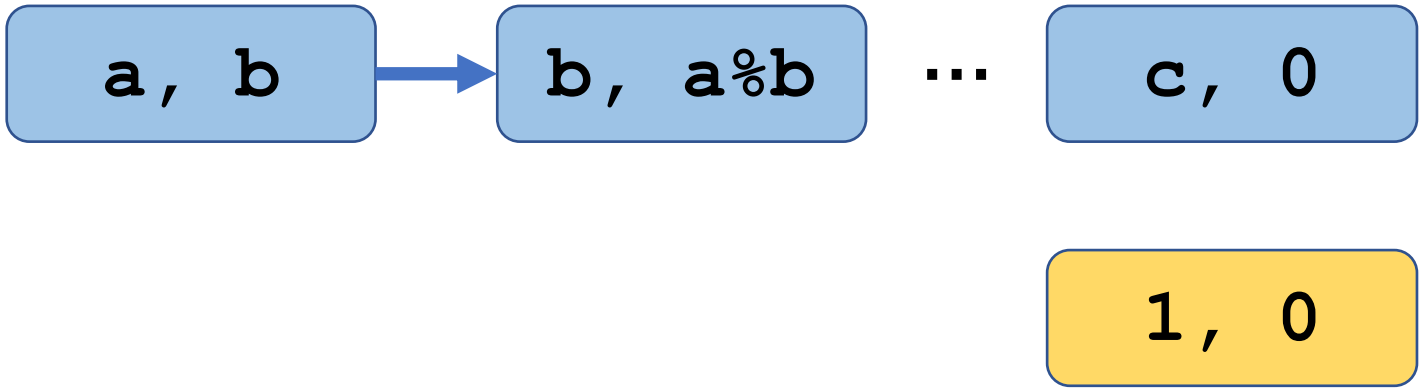
$$ax + by = \gcd(a, b) = c$$

GCD 过程



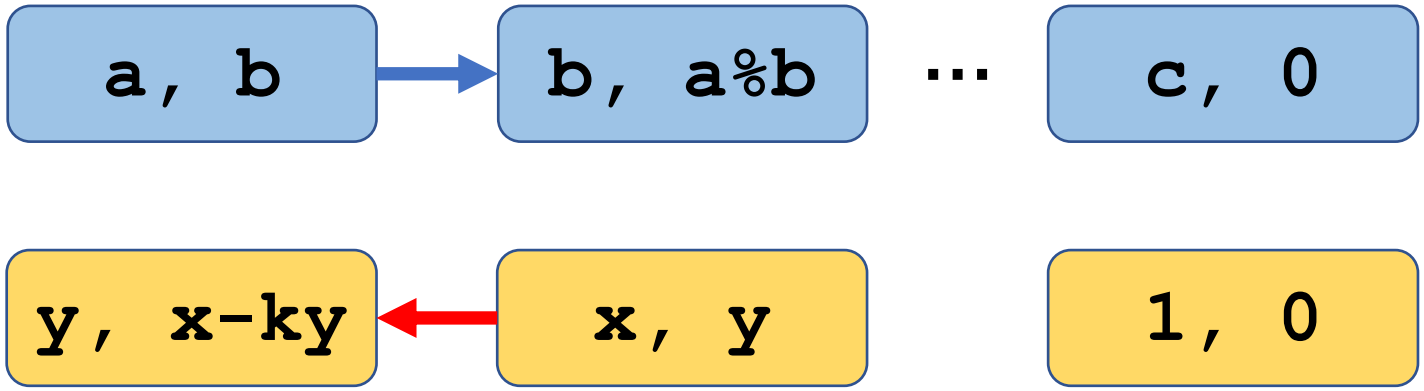
$$ax + by = \gcd(a, b) = c$$

GCD 过程



$$ax + by = \gcd(a, b) = c$$

GCD 过程



扩展欧几里得算法的用途

$$ax \,\%\, b = c$$

$$ax - kb = c$$

$$ax + by = c$$

数论中的欧拉公式

大约用时：（15 mins）

下一部分：最终问题说

欧 拉 公 式

$$a^{\varphi(n)} \ mod \ n = 1$$

最终问题说

大约用时：（15 mins）

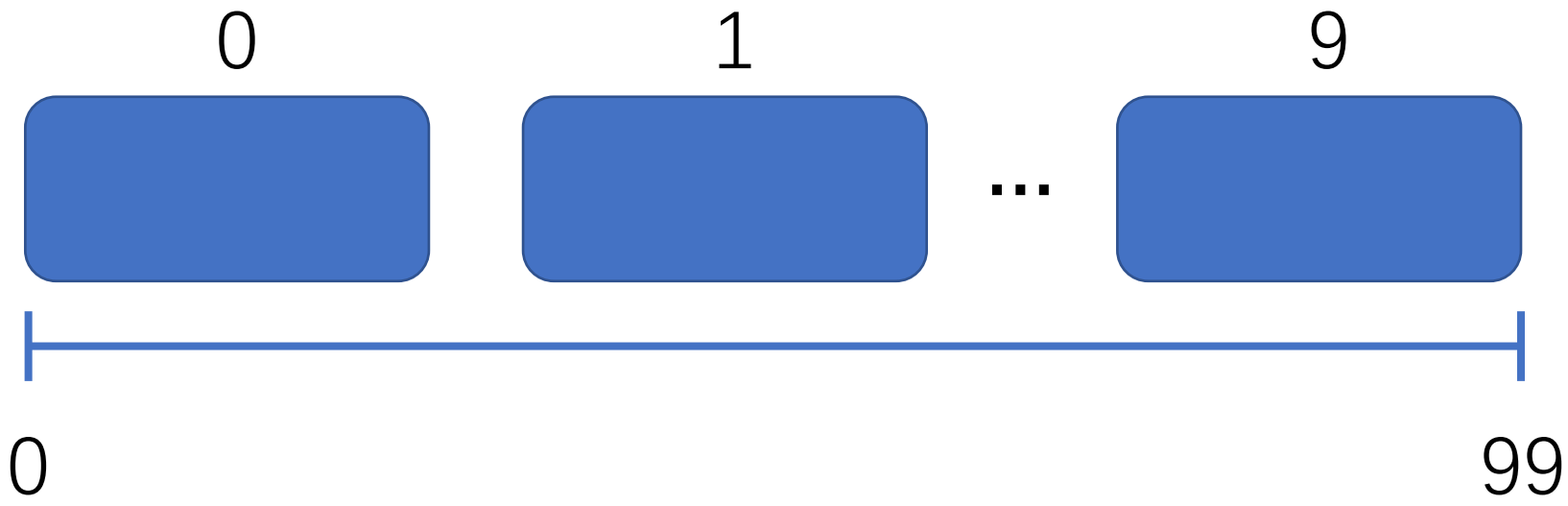
下一部分：经典面试题刷题专项环节

一个令人头秃的问题

$$a^x \ mod \ b = c$$

已知 a，b 互质，给出 a、b、c 三个正整数，求 x 的最小正整数解

分　块　算　法

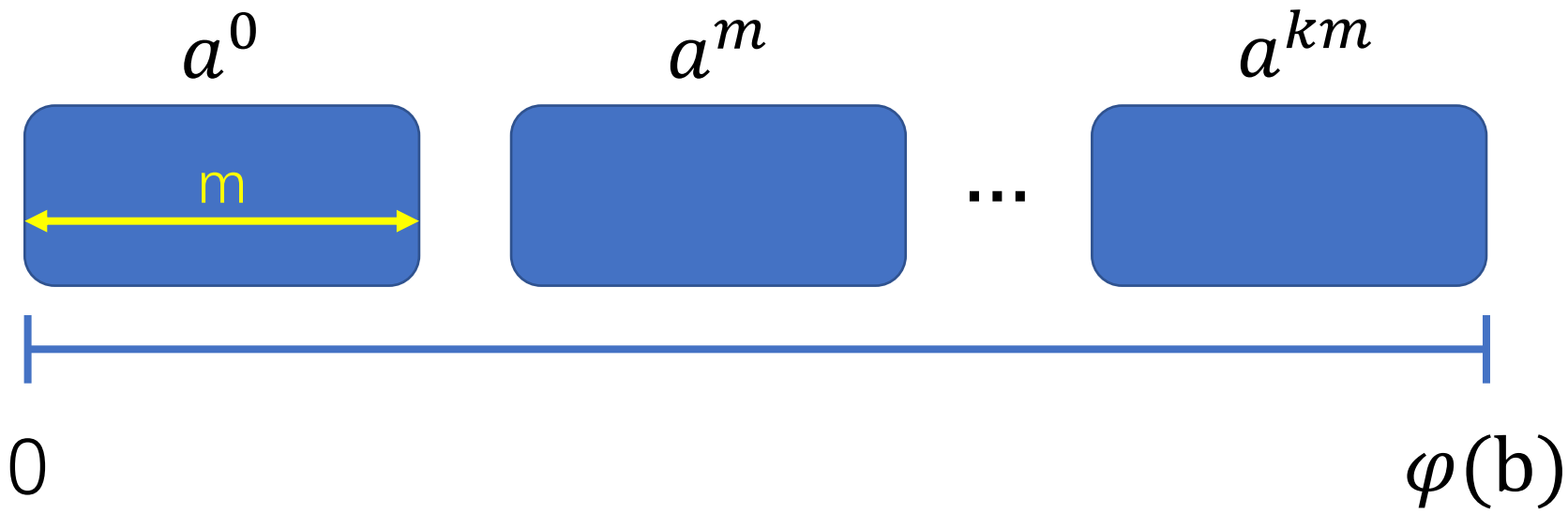


分　块　算　法

$$a^x \ mod \ b = c$$

$$a^{\varphi(b)} \ mod \ b = 1$$

$$a^{km+r} \ mod \ b = c$$



分 块 算 法

哈希表 a^0 a^m a^{2m} … a^{km}

a^0 a^1 a^2 … a^{m-1}

m

分 块 算 法

哈希表 $a^0 \quad a^m \quad a^{2m} \quad \cdots \quad a^{km}$

$$a^2 \times b \mod n = c$$

分 块 算 法

哈希表 $a^0 \quad a^m \quad a^{2m} \quad \cdots \quad a^{km}$

$a^2 \times b \mod n = c$

扩展欧几里得算法

经典面试题刷题专项环节

大约用时：（120 mins）

下一部分：大家晚安

问题板书

每天都想干翻这个世界
到头来，被世界干的服服帖帖

大家晚安
--船长