欧几里得算法与
扩展欧几里得算法

主讲人：邓哲也

欧几里得算法求最大公约数

利用性质：gcd(a, b) = gcd(b, a % b)

```
int gcd(int a, int b){
    if (!b) return a;
    return gcd(b, a % b);
}
```

欧几里得算法求最大公约数

求出了 gcd，就可以求出 lcm。

```
int lcm(int a, int b){
    return a / gcd(a, b) * b;
}
```

欧几里得算法求最大公约数

因为每次取模，a 至少会变成原来的二分之一。

整个算法是 O(log n) 的。

HDU 2503 a/b+c/d

给定 a, b, c, d (0 < a,b,c,d < 1000)。

求 a/b + c/d 的最简形式 e/f。

样例输入:

1 2 1 3

样例输出:

5 6

HDU 2503 a/b+c/d

先通分，求b和d的最小公倍数。

分子相加后，再约掉分子和分母的最大公约数就是答案。

扩展欧几里得算法

它能计算出满足下列条件的整系数 x 和 y：

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

扩展欧几里得算法

我们来直接推倒一下：

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

注意到由欧几里得算法得：

$$gcd(a, b) = gcd(b, a \% b)$$

扩展欧几里得算法

因此：

$$
\begin{aligned}
ax + by &= bx + (a \% b)y \\
&= bx + (a - \mathrm{int}(a / b)b)y \\
&= ay + b(x - \mathrm{int}(a / b)y)
\end{aligned}
$$

$$\gcd(a, b) = \gcd(b, a \% b)$$

$$a\textcolor{red}{x} + b\textcolor{red}{y} = a\textcolor{red}{y} + b\textcolor{red}{(x - \mathrm{int}(a / b)y)}$$

扩展欧几里得算法

例：求 $9x + 7y = 1$ 的一组整数解。

$9x + 7y = 1$

$7x + 2y = 1$

$2x + y = 1$

$x = 1$

扩展欧几里得算法

$9x + 7y$	$= 1$		➢ $x = -3,\ y = 4$
$9y + 7(x - y)$	$= 7x + 2y$	$= 1$	➢ $x = 1,\ y = -3$
$7y + 2(x - 3y)$	$= 2x + y$	$= 1$	➢ $x = 0,\ y = 1$
$2y + (x - 2y)$	$= x$	$= 1$	➢ $x = 1,\ y = 0$

扩展欧几里得算法代码实现

```
int exgcd(int a, int b, int &x, int &y){
      if (!b) {
            x = 1, y = 0;
            return a;
      }
      int d = exgcd(b, a % b, x, y);
      int t = x;
      x = y;
      y = t - a / b * y;
      return d;
}
```

扩展欧几里得算法

它能计算出满足下列条件的整系数 x 和 y：

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

更一般的，求解 $ax + by = c$

只要 $\gcd(a, b) \mid c$ 就有无数解，

否则无解。

扩展欧几里得算法的应用

求乘法逆元：

$$ax \equiv 1 \pmod m$$

$ax + my = 1$

当然如果 $\gcd(a, m) \neq 1$，就无解

注意到 x 的解是 $x_0 + km$ （k是任意整数）

我们只要求出一个 k 使得 $x_0 + km$ 是最小的正整数即可。

扩展欧几里得算法的应用

尝试一下：

（1） 求 6 在模 19 意义下的逆元。

（2） 求 13 在模 17 意义下的逆元。

下节课再见