拓展欧几里得算法

Qizy

2018 年 2 月 5 日

成都石室中学
yongzhengqi@gmail.com

目录

欧几里得算法

欧几里得算法

应用：求解最大公因数

在小学，我们称之为辗转相除法

相关结论

结论：$\gcd(a, b) = \gcd(b, a\%b)$

证明；https://en.wikipedia.org/wiki/Euclidean_algorithm#Proof_of_validity

代码实现：

```
int gcd(int a, int b) {
  return b? gcd(b, a%b): a;
}
```

拓展欧几里得算法

拓展欧几里得算法

求解不定方程：$ax + by = \gcd(a, b)$ 的一组整数解

使用欧几里得算法来进行迭代

数学推导

因为 $ax + by = (a\%b)x + b(y + \lfloor \frac{a}{b} \rfloor x)$

且 $gcd(a, b) = gcd(b, a\%b)$

所以
$$ax + by = \gcd(a, b)$$
$$\Leftrightarrow b(y + \lfloor \frac{a}{b} \rfloor x) + (a\%b)x = gcd(b, a\%b)$$

按照这个形式不停迭代

当 $b = 0$ 时 $a = \gcd(a, b)$，此时 $x = 1, y = 0$ 是一组解

再迭代回去

代码实现：

```
void exgcd(int a, int b, int &x, int &y) {
  if (b) {
    exgcd(b, a%b, y, x);
    y -= a / b * x;
  } else {
    x = 1;
    y = 0;
  }
}
```

一点小拓展

求解 $ax \equiv b \pmod{c}$

该方程有解，当且仅当 $\gcd(a, c) \mid b$

一点大拓展

https://oi.qizy.tech/?p=3155

https://oi.qizy.tech/?p=2959

参考资料

参考资料

[1] https://en.wikipedia.org/wiki/Extended_Euclidean_algorithm

[2] https://en.wikipedia.org/wiki/Euclidean_algorithm