> copyright © hexisyztem 2019.03.02

数论

> 数论算法都基于整数域进行推导

欧几里得算法

内容

欧几里得算法：$gcd(x, y)$ 返回 x, y 的最大公因数，且有 $gcd(x, y) = gcd(y\%x, x)$

证明过程

假定 d 是 x, y 的最大公因数，(假定 $x \le y$) $y = k * x + b$，因为 $d|x, d|y$， 所以 $d|(k * x + b)$， 所以 $d|b$， 所以 $gcd(x, y) = gcd(y\%x, x)$。 又因为 $y\%x < x$，所以最终 $gcd(x, y)$ 会转化成 $gcd(0, d)$ 此时，我们将 $gcd(0, d)$ 返回 d。

代码实现

```
int gcd(int x, int y){ return x == 0 ? y : gcd(y%x, x);}
```

裴蜀定理

内容

对于已知 a, b，则一定存在 x, y 使得 $a * x + b * y = gcd(a, b)$。

证明过程

设 $d = gcd(a, b)$， 则 $d|a, d|b$。 对于任意整数 x, y， 有 $d|(a * x + b * y)$。 假设有整数 x_0, y_0 使 $s = x_0 * a + y_0 * b$ 是$(a * x + b * y)$所能表示的最小的正整数， 那么 $d|s$。 令 $q = \lfloor \frac{a}{s} \rfloor, r = a\%s = a - q * s = a - q * (x_0 * a + y_0 * b) = a * (1 - q * x_0) + b * (q * y_0)$，如果 $r \neq 0$，那么因为 $r < s$，且 r 是 a, b 的线性组合，与之前的假设 s 是$(a * x + b * y)$所能表示的最小的正整数矛盾。所以 $r = 0$。所以 $s|a$，同理可证 $s|b$， 所以 $s|d$。 综上所述 $s|d$， 且 $d|s$，那么可知 $s = d$，证毕。

重要推论

已知a, b，则$a * x + b * y = 1$ 的充要条件是 $gcd(a, b) = 1$。

拓展欧几里得算法

内容

对于已知 a, b 的情况下，求 $a * x + b * y = gcd(a, b)$ 中 x, y 的一组解。

证明过程

由裴蜀定理可知解的存在性。 下面给出如何计算出一组解。

因为 $gcd(a,b)=gcd(b,a\%b)$， 由裴蜀定理可知， 存在 x_1,y_1,x_2,y_2 使得 $x_1*a+y_1*b=gcd(a,b)=gcd(b,a\%b)=x_2*b+y_2*(a\%b)$。 令 $q=\lfloor\frac{a}{b}\rfloor$，我们可将上方程写作 $x_1*a+y_1*b=x_2*b+y_2*(a-q*b)$ 那么有 $x_1*a+y_1*b=y_2*a+(x_2-q*y_2)*b$。 所以当我们已知 x_2,y_2 使 $gcd(b,a\%b)=x_2*b+y_2*(a\%b)$ 时， 我们可以反推出 $x_1=y_2,y_1=(x_2-q*y_2)$ 使 $x_1*a+y_1*b=gcd(a,b)$ 成立。 因为对 $d=gcd(a,b)=gcd(b\%a,a)......=gcd(0,d)$ 对于 $gcd(0,d)$ 一定有 $0*0+1*d=d$， 那么我们可以通过这个结果反解出 $x_1*a+y_1*b=gcd(a,b)$

代码实现

```
int extended_gcd(int a, int b, int &x, int &y){
    if(!b){
        x = 1;
        y = 0;
        return a;
    }
    int ans = extended_gcd(b, a%b, x, y);
    int tem = x;
    int q = a / b;
    x = y;
    y = tem - q * y;
    return ans;
}
```

模意义下的逆元概念

若 $a*x\equiv 1(mod \quad b)$， 则称 a 与 x 互为模 b 意义下的逆元。并且可以将 x 记做 a^{-1}。

逆元的计算: 计算 a 关于 b 的逆元

方法 1　拓展欧几里得算法

由此定义，可转化为 $a*x=1+b*y$，即 $a*x+(b*(-y))=1$。 根据裴蜀定理可得，上述方程有解，当且仅当 $gcd(a,b)=1$。 所以我们可知，a 存在关于 b 的逆元，当且仅当 $gcd(a,b)=1$。 并且可以通过拓展欧几里得算法，计算出 a 关于 b 的逆元。

方法 2　线性递推方法

首先有 $1*1=1(modb)$ 然后设 $b=k*a+r,r<a,1<a<p$， 将此式放入 $modb$ 意义下，得到: $k*a+r\equiv 0(mod \quad b)$， 等式两边同时乘上 a^{-1} 和 r^{-1}，得到 $k*r^{-1}+a^{-1}\equiv 0(mod \quad b)$ 所以，$a^{-1}\equiv -\lfloor\frac{b}{a}\rfloor*(b\%a)^{-1}(mod \quad b)$。 由此递推，每次将求 a^{-1} 转化为求 $(b\%a)^{-1}$， 由欧几里得算法可知，此过程最终求取 1^{-1}。

方法 3　费马小定理

费马小定理的内容是：若 b 为素数， a 为正整数，且 $gcd(a,b)=1$ 时， 则 $a^{b-1}\equiv 1(modb)$，$a^{-1}\equiv a^{b-2}(modb)$。

中国剩余定理

普通中国剩余定理

中国剩余定理在满足 $m_1,m_2,m_3......m_r$ 两两互质的条件下，求解关于下述方程的通解。

$$\begin{cases} x\equiv b_1(mod \quad m_1) \\ x\equiv b_2(mod \quad m_2) \\ x\equiv b_3(mod \quad m_3) \\ .... \\ x\equiv b_r(mod \quad m_r) \end{cases}$$

实现过程

记 $N=m_1*m_2*m_3....*m_r$， 因为 $gcd(\frac{M}{m_i},m_i)=1$ 所以根据拓展欧几里得算法, 有 $\frac{M}{m_i}$关于m_i的逆元y_i 使得 方程 $\frac{M}{m_i}*y_i\equiv 1(mod \quad m_i)$有解。 所以

$$\frac{M}{m_i}*y_i*b_i\equiv b_i(mod \quad m_i)$$
$$\frac{M}{m_i}*y_i*b_i\equiv 0(mod \quad m_i)$$

那么， $x=\sum_{i=1}^{r}\frac{M}{m_i}*y_i*b_i$，则 x 可以满足上述条件。

拓展中国剩余定理

普通中国剩余定理只能解决 $m_1,m_2,m_3......m_r$ 两两互质的情况。 拓展中国剩余定理则可以处理更一般的情况。

大概思路

每次将 $x\equiv B_i(mod \quad M_i),x\equiv b_{i+1}(mod \quad m_{i+1})$ 求解， 并将两个方程的通解进行求交， 得到新的方程 $x\equiv B_{i+1}(mod \quad M_{i+1})$ 来表示同时满足两个方程的通解。

具体计算

假定 t_i,k_{i+1} 使得 $t_i*M_i+B_i=x=k_{i+1}*m_{i+1}+b_{i+1}$ 成立 则有，
$t_i*M_i+B_i=k_{i+1}*m_{i+1}+b_{i+1}$， 所以可转化为 $(b_{i+1}-B_i)=t_i*M_i-k_{i+1}*m_{i+1}$。 由裴蜀定理可知，上述方程有解当且仅当 $gcd(M_i,m_{i+1})|(b_{i+1}-B_i)$。 由扩展欧几里得算法，我们可以计算出 tx,ty 使得 $gcd(M_i,m_{i+1})=tx*M_i+ty*m_{i+1}$ 成立。 所以 $t_i=tx*\frac{b_{i+1}-B_i}{gcd(M_i,m_{i+1})}$。 所以得到 x 的一组解为 $ti*M_i+B_i$。 所以得到 x 的通解为 $x=B_{i+1}(mod \quad M_{i+1})$ 其中，

$B_{i+1} = t_i * M_i + B_i$ $M_{i+1} = lcm(M_i, m_{i+1})$

待完成内容

欧拉定理

威尔逊定理

Lucas 定理

Miller-Rabin 素数测定

Polya 定理