GCD

2019年4月17日 13:08

GCD：

欧几里得算法

贝祖定理及其2个推论

基本算数定理

同余除法

素数猜想

解线性同余方程和方程组：模逆和中国剩余定理

欧拉定理和费马小定理

元根

欧几里得算法	求gcd 证明：使用因子集合完全相同来证明 扩展：形如gcd（a,b）=gcd(c,d) 可考虑如此证明
Bezout定理 gcd（a,b）=sa+tb	证明：逆用欧几里得 算法：扩展欧几里得 推论： If c|(a·b), then c|(a·gcd(b,c)). 推论证明：将贝祖等式代入gcd（b,c）即可
基本算数定理	证明唯一性： 反证 假设两个不同的分解形式，将相同部分抹去后，有pi1pi2 …piu = qj1qj2 …qjv v gcd（pi1，qik）=1，由贝祖推论，可得pi1 | qik for some k，与pi1和qik 为互异质数矛盾 证明存在性：
同余式除法	If ac ≡ bc (mod m) and gcd(c,m) = 1, then a ≡ b (mod m). 证明：应用同余式定义 和贝祖定理推论
素数猜想	Mersenne Primes 2^p-1 Goldbach’s Conjecture 哥德巴赫猜想 n>2的数都是两素数之和 孪生素数猜想 存在无穷多相差为2的素数对
解线性同余方	单个方程 gcd（a,m）=d 若d不|b 则无解

程 ax=b （mod m）	若d|b　则在模m意义下有d解 分别为x0，x0+1*(m/d).，x0+(d-1)(m/d) gcd（a,m）=1　则利用模逆求得模意义下唯一解 方程组：若m1...mn两两互质 利用中国剩余定理求解 若不互质 分别分解质因数　再利用中国剩余定理求解
欧拉定理	$\phi(p) = p - 1$ $\phi(pq) = (p-1)(q-1)$ $\phi(p^i) = p^i - p^{i-1}$ ■ **Theorem (Euler's theorem)** : Let n be a positive integer, and let x be an integer such that $\gcd(x, n) = 1$. Then $x^{\phi(n)} \equiv 1 \pmod{n}$.
费马小定理	■ **Theorem (Fermat's little theorem)** : Let p be a prime, and let x be an integer such that $x \not\equiv 0 \bmod p$. Then $x^{p-1} \equiv 1 \pmod{p}$.
元根	1.运算过程中不可重复 2. **Theorem** * There is a primitive root modulo n if and only if $n = 2, 4, p^e$ or $2p^e$, where p is an odd prime.