1. **威尔逊定理：若p是素数，则**
2. **费马小定理**：**若p是素数，且，那么**
3. **若p是素数且a是正整数，那么**
4. **欧拉定理：设m是一正整数，a是一个整数且(a,m)=1，那么**
5. **扩展欧几里得：设a和b不全为0，则存在整数x和y，使得**

1. **素数定理：素数有无穷多个，能估计出小于一个正实数x的素数有多少个，并用π(x)表示，随着x的增长，π(x)/(x/lnx)=1**
2. **孪生素数猜想：存在无穷多的形如p和p+2的素数对。**
3. **哥德巴赫猜想：每个大于2的正偶数都可以写成两个素数的和。**
4. **猜想：存在无穷多个形如的素数。**
5. **如果n是一个合数，那么n一定有一个不超过的素因子。**
6. **的素因子分解中的素数p的幂为**
7. **毕达哥拉斯三元组： ，如果一个毕达哥拉斯三元组x,y,z满足(x,y,z)=1，那么这个毕达哥拉斯三元组是本原的。**

**(x,y,z)是一个本原的毕达哥拉斯三元组，且y是偶数，当且仅当存在互素的正整数m,n(m>n)，其中m为奇数n为偶数，或者m为偶数n为奇数。并且满足：**

1. **费马大定理：无非0整数解，其中n为整数且n>=3**
2. **形如 （d>1且d不为完全平方数）的不定方程称为佩尔方程。若佩尔方程的最小特解为(x1,y1)，那么可有迭代公式：**

1. **欧拉函数指不超过n且与n互素的正整数的个数。**
2. **原根：**在时，定义**对模的指数**为使成立的最小的正整数。由前知 一定小于等于 ，若，则称**是模的原根**。



1. **如果p有原根，则它恰有φ(φ(p))个不同的原根。**
2. **勒让德符号,**



|  |  |  |
| --- | --- | --- |
|  |  | 如果 |
| 如果，且对于某个整数 |
| 如果不存在整数，使得。 |

**勒让德原先把他的符号定义为：**



**欧拉在之前证明了这个表达式是≡ 1 (mod *p*)，如果*a*是二次剩余(mod *p*)，是≡ −1如果*a*是二次非剩余；这个结论现在称为欧拉准则。**