Number theory-->Modular arithmetic-->modular congruence【模同余基本知识要点】

1) If **a** is congruent to **b** modulo m, then you write **a≡b**(mod **m**). that is that **a** and b leave the same remainder when they are divided by m.【**a**,b 对模 m 同余，记作 **a≡b**(mod **m**)，就是 **a**,b 被 m 除余数相同】.

2) Let m be a positive integer. If **a** and **b** are integers, then **a** is congruent to b modulo m if m|(**a**-b).【 **a** 和 **b** 是整数，**m** 是正整数，如果 m|(**a**-b)，那么，**a≡b**(mod **m**)】

3) If **a**,b∈Z, then **a** ≡ b(mod m) for some positive integer m if and only if there exists an integer k such that **a**=b+km.【**a**,b 是整数，m 是正整数，**a** ≡ **b**(mod **m**) ⟺ **a**=b+km】

4) If **a** ≡ b(mod m) and b ≡ c(mod m), then **a** ≡ c(mod m)【同余的传递性】

5) Let **a**, b, c, d, m, n∈Z and m, n>0, with **a** ≡ b(mod m) and c ≡ d(mod m). then:

a±c ≡ b±d(mod m)

ac ≡ bd(mod m)

k**a** ≡ kb(mod m)

$\mathbf{a}^n \equiv b^n \pmod m$

6) Fermat´s little theorem states that, if p is a prime number and **a** is any number not divisible by p,then $\mathbf{a}^{p-1} \equiv 1 \pmod p$ and $\mathbf{a}^p \equiv \mathbf{a} \pmod p$.【费马小理：如果 p 是质数，p∤ **a**，那么，$\mathbf{a}^{p-1} \equiv 1 \pmod p$ 和 $\mathbf{a}^p \equiv \mathbf{a} \pmod p$】

7) A multiplicative inverse of **a** modulo m is an integer p that satisfies **a**p ≡1(mod m) the multiplicative inverse exists if and only if gcd(**a**,m)=1【如果 gcd(**a**,m)=1 和 **a**p ≡1(mod m)，**p** 是 **a** 的同余乘逆】

8) If **a** and b are positive integers and p is a prime number with p∤ **a, then** $\mathbf{a}^{p-2}$ is a multiplicative inverse of **a** modulo p and the solution to the equatio **a**x ≡ b(mod p) is given by x ≡ $\mathbf{a}^{p-2}$b(mod p)【p 是质数，p∤ **a,** $\mathbf{a}^{p-2}$是 **a** 的同余乘逆，**a**x ≡ b(mod p)解是 x ≡ $\mathbf{a}^{p-2}$b(mod p)】

9) Let **a**, b, m∈Z, with m>0 and gcd(**a**,m)=d

If d∤ b then the equation **a**x ≡ b(mod p) has no solutions.

If d | b then the equation **a**x ≡ b(mod p) has d solutions in the set of least residues modulo m.【如果 d | b，则方程 **a**x ≡ b(mod p)在最小模剩余集中有 d 个解】

10) If k**a** ≡ kb(mod m) and gcd(k,m)=1 then **a** ≡ b(mod m)

If k**a** ≡ kb(mod m) and gcd(k,m)=d then **a** ≡ b(mod m/d)