Modular arithmatic

A%B = remainder when A is divided by B.

1. A= q1.C+r1 .... B= q2.C+r2.
2. (a*b)modC= (q1.C+r1)(q2.C+r2)modC=(r1*r2)mod C = ((a mod C)* (b mod C))%C.
3. (a-b) mod C = (a%C – b%C)%mod C.
4. (a+b)mod C = (a%C + b%C)%mod C.
5. (a^b)mod C = (a mod C)^b mod C. (using binomial theorem).
6. If we have to calculate modulo of a negative number we have to first add it with the no given for modulo no of times so that the no becomes positive and then take modulo.
7. (a/b)%C = (a*b^-1)modC
8. ax congruent 1modC (x is modulo inverse). (3^-1 mod 5 => 3x=1 mod 5=>x= (3^-1mod5))
9. Format's little theorem (a^-1 mod P) (P is Prime), then P devides (a^p-a) ..... X= a^(P-2) mod P .
   - p/(a^p-a)
   - p/(a^(p-1)-1)a -> - p/(a^(p-1)-1)
   - a^(p-1)-1 congruent 0 mod P
   - a^(p-1) congruent 1 mod P (adding 1 both side)
   - a*a^(p-2) congruent to 1 mod P (ax congruent to 1 mod P)

   So, X= a^(P-2) mod P .
10. So (a/b) mod P = (a*(b^(P-2) mod P))mod P.