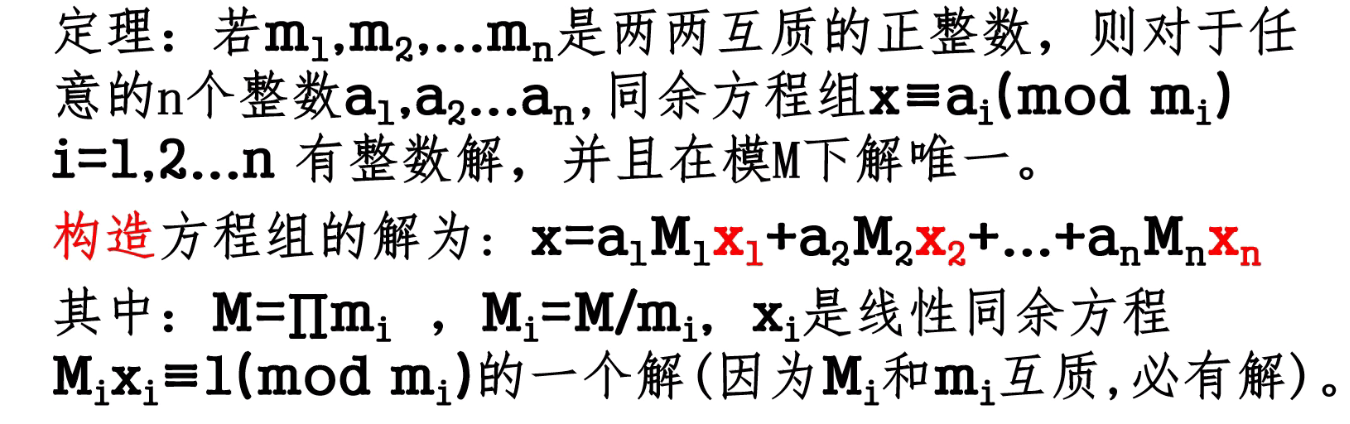
# 6.4中国剩余定理

**6.4.1 中国剩余定理**

**6.4.1.1 概述**

用于求解模数互质的线性同余方程组

**6.4.1.2 解题方法**



**6.4.1.3 代码模板**

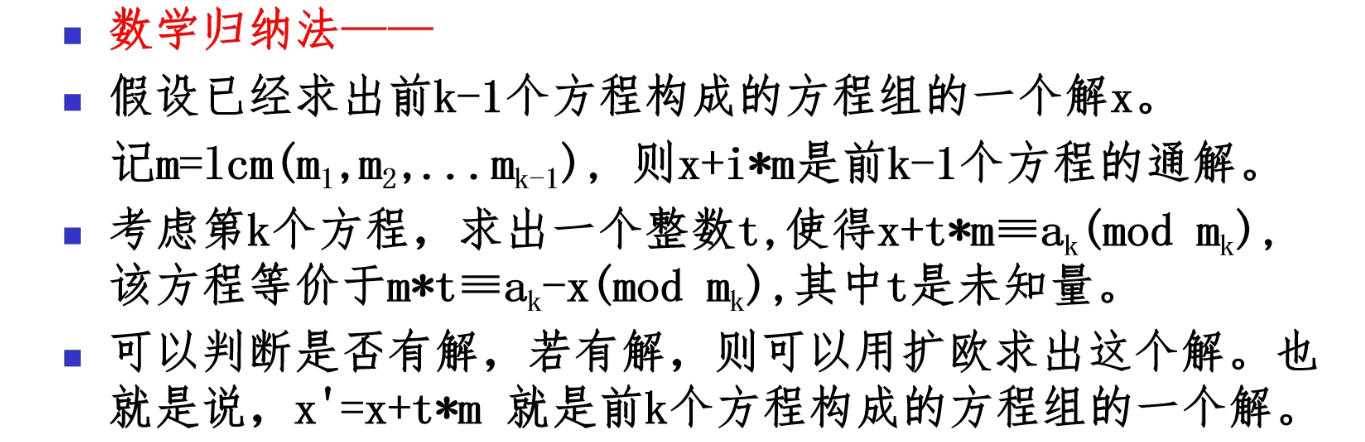
1. **int** exgcd(**int** a,**int** b,**int** &x,**int** &y)
2. {
3. **if**(b==0)
4. {
5. x=1;
6. y=0;
7. **return** a;
8. }
9. **int** ans=exgcd(b,a%b,x,y);
10. **int** tmp=x;
11. x=y;
12. y=tmp-(a/b)\*y;
13. **return** ans;
14. }
15. **int** crt(**int** n)
16. {
17. **int** ans=0;
18. **for**(**int** i=1;i<=n;i++)
19. {
20. **int** x,y;
21. exgcd(MOD/mod[i],mod[i],x,y);
22. ans=(ans+MOD/mod[i]\*x\*yu[i])%MOD;
23. }
24. **return** (ans%MOD+MOD)%MOD;
25. }

**6.4.2 扩展中国剩余定理**

**6.4.2.1 概述**

用于求解模数不互质的线性同余方程组

**6.4.2.2 解题方法**



**6.4.2.3 代码模板**

1. #include<bits/stdc++.h>
2. #define int long long
3. **using** **namespace** std;
4. **const** **int** N=1e5+5;
5. **int** x,y;
6. **int** n;
7. **int** mod[N],yu[N];
8. **int** qmul(**int** a,**int** n,**int** mod)
9. {
10. **int** res=0;
11. **while**(n)
12. {
13. **if**(n&1) res=(res+a)%mod;
14. a=(a+a)%mod;
15. n>>=1;
16. }
17. **return** res;
18. }
19. **int** exgcd(**int** a,**int** b,**int** &x,**int** &y)
20. {
21. **if**(b==0)
22. {
23. x=1;
24. y=0;
25. **return** a;
26. }
27. **int** ans=exgcd(b,a%b,x,y);
28. **int** tmp=x;
29. x=y;
30. y=tmp-(a/b)\*y;
31. **return** ans;
32. }
33. **int** ex\_crt(**int**\* mod,**int** \*yu)
34. {
35. **int** ans=yu[1];
36. **int** m=mod[1];
37. **for**(**int** i=2;i<=n;i++)
38. {
39. **int** tmp=(yu[i]%mod[i]-ans%mod[i]+mod[i])%mod[i];//yu[i]-x=t\*m(mod mod[i]) 求t
40. **int** gcd=exgcd(m,mod[i],x,y);
41. **if**(tmp%gcd) **return** -1;
42. **int** times=tmp/gcd;
43. **int** bg=mod[i]/gcd;
44. x=qmul(x,times,bg);//这里乘法可能会溢出，所以写个快速加法
45. ans=ans+m\*x;
46. m=m/gcd\*mod[i];
47. ans=(ans%m+m)%m;
48. }
49. **return** (ans%m+m)%m;
50. }
51. **signed** main()
52. {
53. cin>>n;
54. **for**(**int** i=1;i<=n;i++) cin>>mod[i]>>yu[i];
55. cout<<ex\_crt(mod,yu)<<endl;
56. **return** 0;
57. }

**6.4.4经典例题**

**6.4.4.1洛谷P1495 中国剩余定理**

**题目描述**

自从曹冲搞定了大象以后，曹操就开始捉摸让儿子干些事业，于是派他到中原养猪场养猪，可是曹冲满不高兴，于是在工作中马马虎虎，有一次曹操想知道母猪的数量，于是曹冲想狠狠耍曹操一把。举个例子，假如有 1616 头母猪，如果建了 33 个猪圈，剩下 11 头猪就没有地方安家了。如果建造了 55 个猪圈，但是仍然有 11 头猪没有地方去，然后如果建造了 77 个猪圈，还有 22 头没有地方去。你作为曹总的私人秘书理所当然要将准确的猪数报给曹总，你该怎么办？

**输入格式**

第一行包含一个整数 nn——建立猪圈的次数，接下来 n 行，每行两个整数ai，bi表示建立了ai个猪圈，有bi头猪没有去处，规定ai，aj­互质

**输出格式**

输出包含一个正整数，即为曹冲至少养母猪的数目。

**输入样例**

3

3 1

5 1

7 2

**输出样例**

16

**题解：**

1. #include<bits/stdc++.h>
2. **using** **namespace** std;
3. **typedef** **long** **long** ll;
4. ll mod[15];
5. ll yu[15];
6. ll MOD=1;
7. ll exgcd(ll a,ll b,ll &x,ll &y)
8. {
9. **if**(b==0)
10. {
11. x=1;
12. y=0;
13. **return** a;
14. }
15. ll ans=exgcd(b,a%b,x,y);
16. ll tmp=x;
17. x=y;
18. y=tmp-(a/b)\*y;
19. **return** ans;
20. }
21. ll crt(**int** n)
22. {
23. ll ans=0;
24. **for**(**int** i=1;i<=n;i++)
25. {
26. ll x,y;
27. exgcd(MOD/mod[i],mod[i],x,y);
28. ans=(ans+MOD/mod[i]\*x\*yu[i])%MOD;
29. }
30. **return** ans;
31. }
32. **int** main()
33. {
34. **int** n;
35. cin>>n;
36. **for**(**int** i=1;i<=n;i++)
37. {
38. cin>>mod[i]>>yu[i];
39. }
40. **for**(**int** i=1;i<=n;i++)  MOD\*=mod[i];
41. cout<<(crt(n)+MOD)%MOD;
42. **return** 0;
43. }

**6.4.4.2 HDU3579 Hello Kiki**

**题目背景**

One day I was shopping in the supermarket. There was a cashier counting coins seriously when a little kid running and singing "门前大桥下游过一群鸭，快来快来 数一数，二四六七八". And then the cashier put the counted coins back morosely and count again...

Hello Kiki is such a lovely girl that she loves doing counting in a different way. For example, when she is counting X coins, she count them N times. Each time she divide the coins into several same sized groups and write down the group size Mi and the number of the remaining coins Ai on her note.

One day Kiki's father found her note and he wanted to know how much coins Kiki was counting.

**输入格式**

The first line is T indicating the number of test cases.

Each case contains N on the first line, Mi(1 <= i <= N) on the second line, and corresponding Ai(1 <= i <= N) on the third line.

All numbers in the input and output are integers.

1 <= T <= 100, 1 <= N <= 6, 1 <= Mi <= 50, 0 <= Ai < Mi

**输出格式**

For each case output the least positive integer X which Kiki was counting in the sample output format. If there is no solution then output -1.

**输入样例**

2

2

14 57

5 56

5

19 54 40 24 80

11 2 36 20 76

**输出样例**

Case 1: 341

Case 2: 5996

**题解：**

1. #include<bits/stdc++.h>
2. **typedef** **long** **long** ll;
3. **using** **namespace** std;
4. ll M[10];
5. ll A[10];
6. ll ex\_gcd(ll a,ll b,ll &x,ll &y)
7. {
8. **if**(b==0)
9. {
10. x=1;
11. y=0;
12. **return** a;
13. }
14. ll ans=ex\_gcd(b,a%b,x,y);
15. ll tmp=x;
16. x=y;
17. y=tmp-(a/b)\*y;
18. **return** ans;
19. }
20. ll ex\_crt(ll\* yu,ll\* mod,ll n)
21. {
22. ll ans=yu[1];
23. ll m=mod[1];
24. ll x,y;
25. ll now;
26. **for**(ll i=2;i<=n;i++)
27. {
28. now=(yu[i]%mod[i]-ans%mod[i]+mod[i])%mod[i];//t\*m=ak-x(mod m)
29. //now=ak-x  满足 now<m
30. ll gcd=ex\_gcd(m,mod[i],x,y);//扩欧求方程的解
31. **if**(now%gcd) **return** -1;//判断t是否存在
32. ll k=now/gcd;
33. x\*=k;//求的t'为t'\*m=gcd (mod m)的解，需要乘以倍数
34. **int** s=mod[i]/gcd;
35. x=(x%s+mod[i]/gcd)%(mod[i]/gcd);//x=x+t\*m更新x
36. ans=ans+x\*m;//
37. m=m\*mod[i]/gcd;
38. }
39. **return** (ans+m)%m?(ans+m)%m:m;
40. }
41. **int** main()
42. {
43. ll t;
44. cin>>t;
45. **for**(ll i=1;i<=t;i++)
46. {
47. memset(A,0,**sizeof**(A));
48. memset(M,0,**sizeof**(M));
49. ll n;
50. cin>>n;
51. **for**(ll j=1;j<=n;j++) cin>>M[j];
52. **for**(ll j=1;j<=n;j++) cin>>A[j];
53. cout<<"Case "<<i<<": "<<ex\_crt(A,M,n)<<endl;
54. }
55. **return** 0;
56. }