[数学类问题总结]

[备战 NOIP]

作者：jtc172(or S.X.B)

【目录】

【1.数论问题】

【1.1 整除理论】

【1.1.1 整除】

整除的定义 设 a，b 是整数，$b \neq 0$，如果存在整数 c，使得 $a = bc$ 成立，则称 a 被 b 整除，a 是 b 的倍数，b 是 a 的约数（因数或除数），并且使用记号 $b \mid a$；如果不存在整数 c 使得 $a = bc$ 成立，则称 a 不被 b 整除。

整除的性质

1）$a \mid b \Leftrightarrow \pm a \mid \pm b$

2）$a \mid b$，$b \mid c \Rightarrow a \mid c$

3）$b \mid a \Rightarrow bc \mid ac$，此处 c 是任意的非零整数

【1.1.2 因数与倍数】

因数与倍数的定义 对于两个整数 a 和 b，若 $a \mid b$，则称 a 是 b 的因数，b 是 a 的倍数。

【1.1.3 质数与合数】

质数的定义 指在一个大于 1 的自然数集中，除了 1 和此整数自身外，不能被其他自然数整除的数。

合数的定义 指自然数中除了能被 1 和本身整除外，还能被其他的数整除的数。

【1.1.4 最大公约数与最小公倍数】

最大公约数的定义 几个自然数公有的约数叫做这几个自然数的公约数。公约数中最大的一个公约数，称为这几个自然数的最大公约数。自然数 A,B 的最大公约数用(A,B)表示。

最小公倍数的定义 几个自然数公有的倍数叫做这几个自然数的公倍数。公倍数中最小的一个公倍数，称为这几个自然数的最小公倍数。自然数 A,B 的最小公倍数用[A,B]表示。

最大公约数与最小公倍数的性质

1） $(a, 1) = 1$，$(a, 0) = a$，$(a, a) = a$

2） 若 p 是素数，a 是整数，则$(p, a) = 1$ 或 $p \mid a$

3） 若 $a = bq + r$(q、r 是自然数，同时$-1 \leq r < q$)，则$(a, b) = (b, r)$

4） 若 p 是质数，且 $a=A*p^x$(A 与 p 互质)，$b=B*p^y$(B 与 p 互质)，则$(a,b)=C*p^{\min(x, y)}$(C 与 p 互质)

5） $[a, 1] = a$，$[a, a] = a$

6） 若 $a \mid b$，则$[a, b] = b$

7） $(a, b) *[a, b] = a*b$

8） 若 p 是质数，且 $a=A*p^x$(A 与 p 互质)，$b=B*p^y$(B 与 p 互质)，则$[a,b]=C*p^{\max(x, y)}$(C 与 p 互质)

【1.1.5 算术基本定理】

算术基本定理 一个大于 1 的正整数都能分解成质因数乘积的形式，并且如果把质因数按照由小到大的顺序排列在一起，相同的质因数的积写成幂的形式，那么这种分解方法是唯一的。并且，正整数 N 最多只含一个超过根号 N 的质因子。

$$N = p_1^{k1} * p_2^{k2} * p_3^{k3} * p_4^{k4} * p_5^{k5} \cdots\cdots$$
$$N = \prod p_i^{ki}$$

唯一分解的性质

1）N 的所有约数个数为 $\prod (ki+1)$。

2）N 的所有约数之和为 $\prod \frac{1-Pi^{ki}}{1-Pi}$

【1.1.6 裴蜀定理】

裴蜀定理 若 a,b 是整数,且(a,b)=d,那么对于任意的整数 x,y,ax+by 都一定是 d 的倍数,特别地,一定存在整数 x,y,使 ax+by=d 成立。

【1.2 同余理论】

【1.2.1 同余】

同余的定义 给定正整数 m,如果整数 a 与 b 之差被 m 整除,则称 a 与 b 对于模 m 同余,或称 a 与 b 同余，模 m，记为 $a \equiv b \pmod m$，此时也称 b 是 a 对模 m 的同余。

如果整数 a 与 b 之差不能被 m 整除，则称 a 与 b 对于模 m 不同余，或称 a 与 b 不同余，模 m，记为 $a \not\equiv b \pmod m$。

同余的性质

1）$a \equiv a \pmod m$

2）$a \equiv b \pmod m \Longrightarrow b \equiv a \pmod m$

3）$a \equiv b$，$b \equiv c \pmod m \Longrightarrow a \equiv c \pmod m$

4）设 a，b，c，d 是整数，并且 $a \equiv b \pmod m$，$c \equiv d \pmod m$，则

$a+c \equiv b+d \pmod m$ ， $ac \equiv bd \pmod m$

5）$a \equiv b \pmod m$，$d \mid m$，$d > 0 \Longrightarrow a \equiv b \pmod d$

6）$a \equiv b \pmod m$，$k > 0$，$k \in \mathbf{N} \Longrightarrow ak \equiv bk \pmod{mk}$

7）$a \equiv b \pmod{m_i}$，$1 \le i \le k \Longrightarrow a \equiv b \pmod{[m_1, m_2, \cdots, m_k]}$

8） $a \equiv b \pmod m \Longrightarrow (a, m) = (b, m)$

9） $ac \equiv bc \pmod m$，$(c, m) = d \Longrightarrow a \equiv b \pmod{m/d}$

【1.2.2 欧拉定理与费马小定理】

欧拉函数 对于正整数 k，令函数$\varphi(k)$的值等于在[1,k]之中所有与 k 互质的个数，称$\varphi(k)$为 Euler 函数，或 Euler—φ函数。

$$\varphi(n)=n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_k}\right)=n\prod_{p|n}\left(1-\frac{1}{p}\right)。$$

欧拉定理 设 m 是正整数，$(a, m) = 1$，则 $a^{\varphi(m)} \equiv 1 \pmod m$

欧拉定理的简要证明 设长度为$\varphi(N)$的数列 A 中每个数代表的都是在[1,N]之中与 N 互质的数，若得出数列 B 为数列 A 中每个数乘以 a。则数列 B 中每个数对于 N 均不同余（见同余性质 9），而且数列 B 中每个数对 N 的模值均与 N 互质。则 B 中每个元素对于 N 的模值与数列 A 中的元素一一对应，所以 A 中每个数的乘积等于 B 中每个数的乘积，也就是

$$(a*A_1)*(a*A_2)*(a*A_3)*(a*A_4)\cdots\cdots\equiv A_1*A_2*A_3*A_4\cdots\cdots(\bmod N)$$
$$a^{\varphi(N)}*A_1*A_2*A_3*A_4\cdots\cdots\equiv A_1*A_2*A_3*A_4\cdots\cdots(\bmod N)$$
$$a^{\varphi(N)}\equiv 1(\bmod N)$$

费马小定理 设 p 是素数，则对于任意的整数 a，有 $a^p \equiv a \pmod p$，其实就是欧拉定理在对质数取模时的特殊情况。

【1.2.3 威尔逊定理】

威尔逊定理 当且仅当 p 为素数时：$(p-1)! \equiv -1 \pmod p$，证明参见欧拉函数。

【2.组合计数】

【2.1 排列】

排列的定义 从 n 个不同元素中取出 m（m≤n）个元素，按照一定的顺序排成一列，叫做从 n 个元素中取出 m 个元素的一个排列。

排列数公式 $A_n^m=\dfrac{N!}{M!}=A_{n-1}^m*N$

【2.1 组合】

组合的定义 从 n 个不同元素中取出 m（m≤n）个元素，构成一个集合，叫做从 n 个元素中取出 m 个元素的一个组合。

组合数公式 $C_n^m=\dfrac{N!}{M!(N-M)!}=C_n^{n-m}=C_{n-1}^{m-1}+C_{n-1}^m$

【2.3 允许取多次的组合】

允许取多次的组合个数公式（可以不取） C_{m-1}^{n-1}

允许取多次的组合个数公式（不可以不取） C_{n+m-1}^{n-1}

证明方法已讲。

【2.4 卡特兰数】

卡特兰数通项公式 $C_{2n}^{n}-C_{2n}^{n+1}$

卡特兰数递推公式 $F(n)=F(n-1)*\dfrac{4n-2}{n+1}$

卡特兰数的性质

$F(0)=1, F(1)=1, F(n)=F(0)*F(n-1)+F(1)*F(n-2)+\cdots+F(n-1)*F(0)$

【2.5 二项式定理】

二项式定理 $(x+y)^n=\sum_{k=0}^{n}\binom{n}{k}x^{n-k}y^k$，其中$\binom{n}{k}=\dfrac{n!}{k!(n-k)!}$

【2.6 容斥原理】

容斥原理 容斥原理又称排容原理，在组合数学里，其说明若$A_1, \ldots, A_n$ 为集合，则

$$\left|\bigcup_{i=1}^{n}A_i\right|=\sum_{i=1}^{n}|A_i|-\sum_{i,j:i\neq j}|A_i\cap A_j|+\sum_{i,j,k:i\neq j\neq k}|A_i\cap A_j\cap A_k|-\cdots\cdots\pm|A_1\cap\cdots\cap A_n|$$

其中$|A|$表示 A 的基数。例如在两个集的情况时，我们可以透过将$|A|$和$|B|$相加，再减去其交集的基数，而得到其并集的基数。

【2.7 斐波那契数列】

斐波那契数列 $F(1)=1, F(2)=1, F(n+2)=F(n)+F(n-1)$

斐波那契数列的性质

1） $F(1)+F(2)+\cdots+F(n)=F(n+2)-1$

2） $F^2(1)+F^2(2)+\cdots+F^2(N)=F(n)*F(n+1)$

3） $F(1)+2*F(2)+\cdots+n*F(n)=n*F(n+2)-F(n+3)+2$

4） $$\begin{aligned}&F(1)+F(3)+\cdots+F(2n-1)=F(2n)-1\\&F(2)+F(4)+\cdots+F(2n)=F(2n+1)\end{aligned}$$

【3 高效算法】

【3.1 逆元】

逆元的定义 对于两个正整数 *A,B*, 若满足 $A*B\equiv 1(\bmod P)$,则称 B 是 A 在模 P 下的逆元，对于 A 的逆元，常用 A^{-1} 表示。

逆元存在的条件 显然，当且仅当 A 与 P 互质时，A 在模 P 下存在逆元。

逆元的计算方法

1）用扩展欧几里得计算逆元

根据裴蜀定理，可得 *AB+Py=1*，那么 B 即为所求。

对于方程 *Ax+By=1* 来说，如果我们计算出了方程（*B mod A)*x+A*y=1* 的一组解 X0，Y0，可直接推导出一组 *Ax+By=1* 的解。

$$\begin{aligned}&Ax+By=(B-A*\lfloor B/A\rfloor)*x0+A*y0\\&A(x+\lfloor B/A\rfloor*x0-y0)=B*(x0-y)\\&x=y0-\lfloor B/A\rfloor*x0\\&y=x0\end{aligned}$$

2）当取模的数位质数时，线性求逆元

$$\begin{aligned}&P=P\bmod x+x*\lfloor P/x\rfloor\\&x*\lfloor P/x\rfloor\equiv -P\bmod x(\bmod P)\\&-(P\bmod x)^{-1}*x*\lfloor P/x\rfloor\equiv 1(\bmod P)\\&x^{-1}\equiv -(P\bmod x)^{-1}*\lfloor P/x\rfloor(\bmod P)\end{aligned}$$

观察上式，当我们计算 X 在模 P 下的逆元时，我们可以由(P mod X)的逆元推出。因为在 P 是质数，而且 P mod X 恒小于 X（这个是肯定的），所以就可以 O(N)地推导出 1 到 N 在模 P 下的逆元了。

【3.2 质数筛选】

方法，线性筛质数。

任何一个合数都可以表示成一个质数与另一个自然数的乘积，不妨设 F(x)是 x 的最小质因数，那么 X=K*F(x)。每当我们枚举到一个数 Y，若它未被标记，则视为质数。然后枚举质数，筛去 PrimeI*Y，直到 Y 是 PrimeI 的倍数位置，因为之后筛 Y*PrimeI+1 时，必然存在一个 Y0=Y*PrimeI+1/PrimeI 可以用更小的质因子筛去 Y*PrimeI+1.因为 1 到 N 中间所有数的最小质因子唯一，所以时间是线性的。

【3.3 组合数计算】

求完 1 到 N 的逆元之后，求出逆元数组的前缀乘积数组 Pi，同时求出数组 Si=i!对于该质数的模值，那么 $C_n^m = S(n) * P(n-m) * P(m)$。

*当取模的数是质数且相对于 N 较小时可使用 Lucas 定理。资料请上维基百科。

【4.思考数学类问题一些方法】

首先，关于数学类问题的本质是什么，傻×我是这样想的。数学类问题的本质在于模型的转化，也就是说，我们必须从一个未知的问题跳到一个已知的问题上，而在其中起到关键作用的，就是利用已学的数学知识将一个模型转变为另一个模型。

举例来说，就像第六套考试题目中的辗转相除问题，我们需要从辗转相除思考到斐波那契数列，那么我们就必须思考这个问题，为什么斐波那契数列会是辗转相乘的次数是最多的？然后进行证明。首先，我们可以发现，A 与 B 必须是互质的，因为 A,B 若不互质，那么必然存在一个更小的方案（A/(A,B)，B/(A,B))。然后，当 B>2*A 时，方法将是不优秀的，因为我们可以得到一个更小的 B0=B-A 使得他们辗转次数相同，所以最优解肯定是不断地从(A,B)推到（B-A，A)。在辗转相乘中一直满足这个条件的（A,B)，最后必然推到（1,1），那么反过来推，则 A 和 B 必然是斐波那契数，于是就完成了模型的转化。

那么，在做数学类问题的时候，我们必须具备一些起码的数学知识，在上文中已经列出来了。但是，我们不肯能总是可以想到转化，有没有别的方法呢？有！就是暴力找规律！很多同学都有点不太喜欢写暴力，这个我不推荐。暴力出一部分小数据，不仅可以得到部分分，同时还可以辅助你观察，更加有利于你接近数学类问题的本质，也就是模型。这点是十分关键的。

对于这 6 套题目，希望大家努力改对，毕竟数学类问题在某种程度上也是经验上的问题。

【参考资料】

《初等数论》
《ACM--算法数论》
《组合数学》
维基百科与百度百科

希望大家能够从参考资料中学习更多东西，不要止步于现在。

【鸣谢】

感谢博士大神的帮助，感谢宋学姐当年辛勤的教导!!! 感谢你们居然看到了这里!!!

【尾声】

Jtc172@gmail.com QQ:296491996

金天成于 2012 年 8 月 21 日 10:26:50