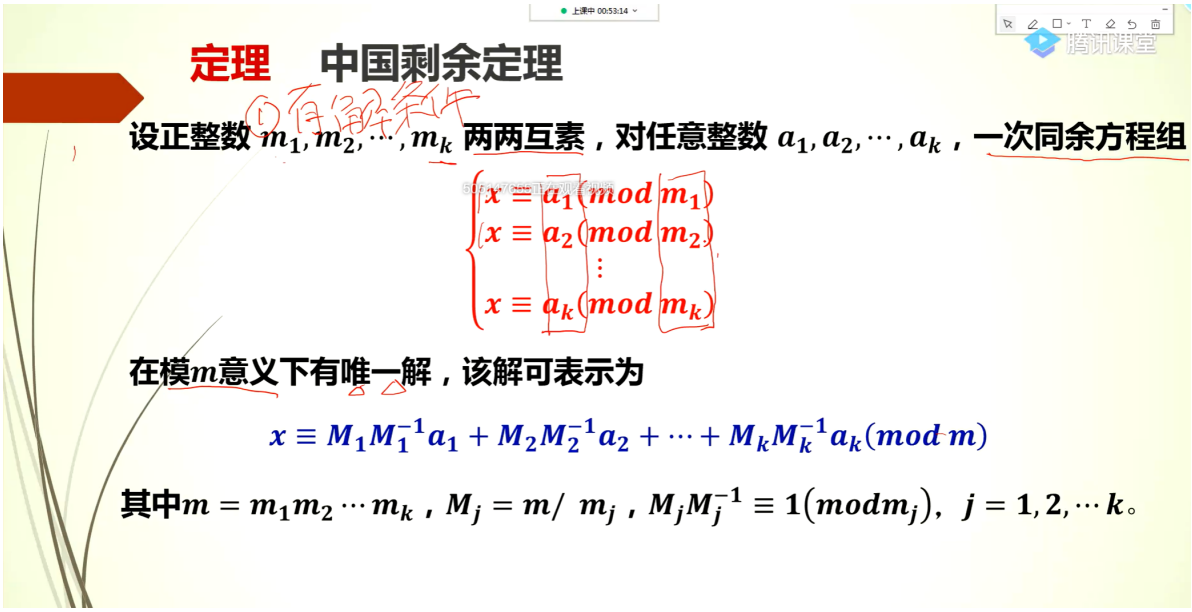
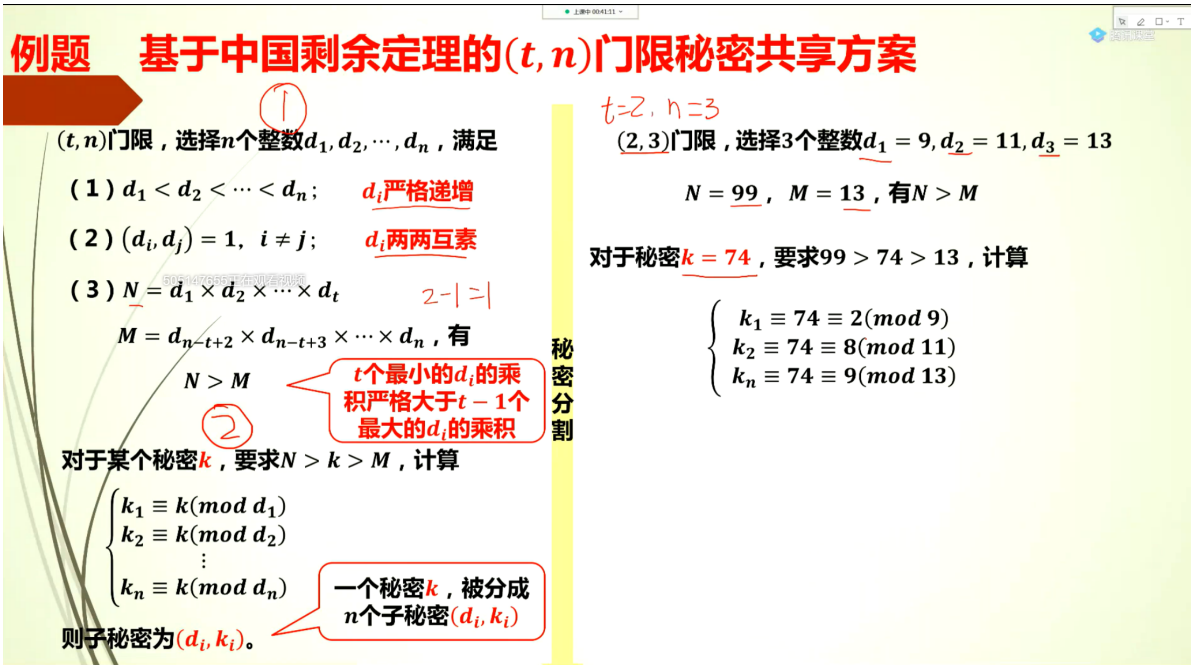
中国剩余定理：



Mignotte（t,n）门限秘密共享方案：

秘密分割：

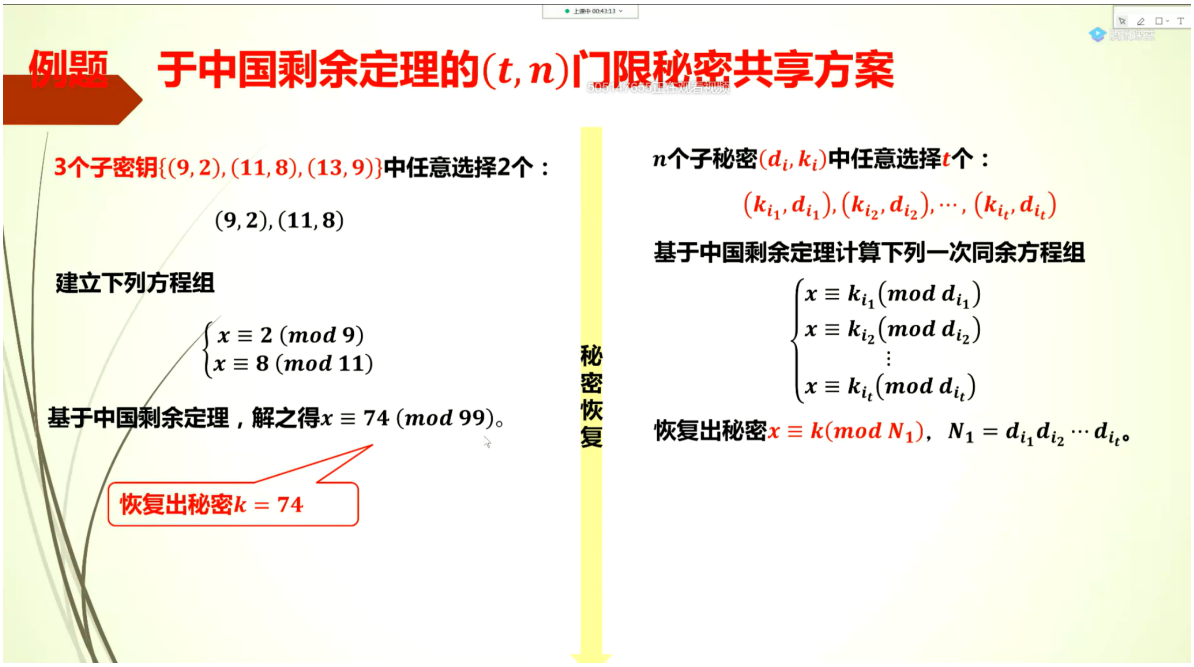


Mignotte序列/d序列的生成：
要保证任意t-1个元素的最大乘积小于k，任意t个元素的最小乘积大于k
因此我们根据k的二进制位数去生成n个大素数，其中每个大素数的二进制位长都为gen_bsize=k_bsize//(t-1)，注意gen_bsize用//向下取余

因此**M的位长一定小于k_bsize，N的位长k_bsize//(t-1)*t一定大于k_bsize**

这种方案的缺陷是秘密长度一定要足够长，否则可能生成的素数数量不能够满足n所需（gen_bsize位长的素数是有限的），所以我们还需要对t，n，k进行检查，主要是保证n要小于能够生成的所有gen_bsize位长的素数的数量

秘密恢复：



Why：任意大于等于t个**(k,d)**对可解，任意小于t个**(k,d)**对不可解