**西安电子科技大学网信院**

**信息安全基础与密码学**

**综合实验**

**实 验 报 告（二）**

**中国剩余定理**

**班级：**

**姓名：**

**学号：**

**日期：2024/10/27**

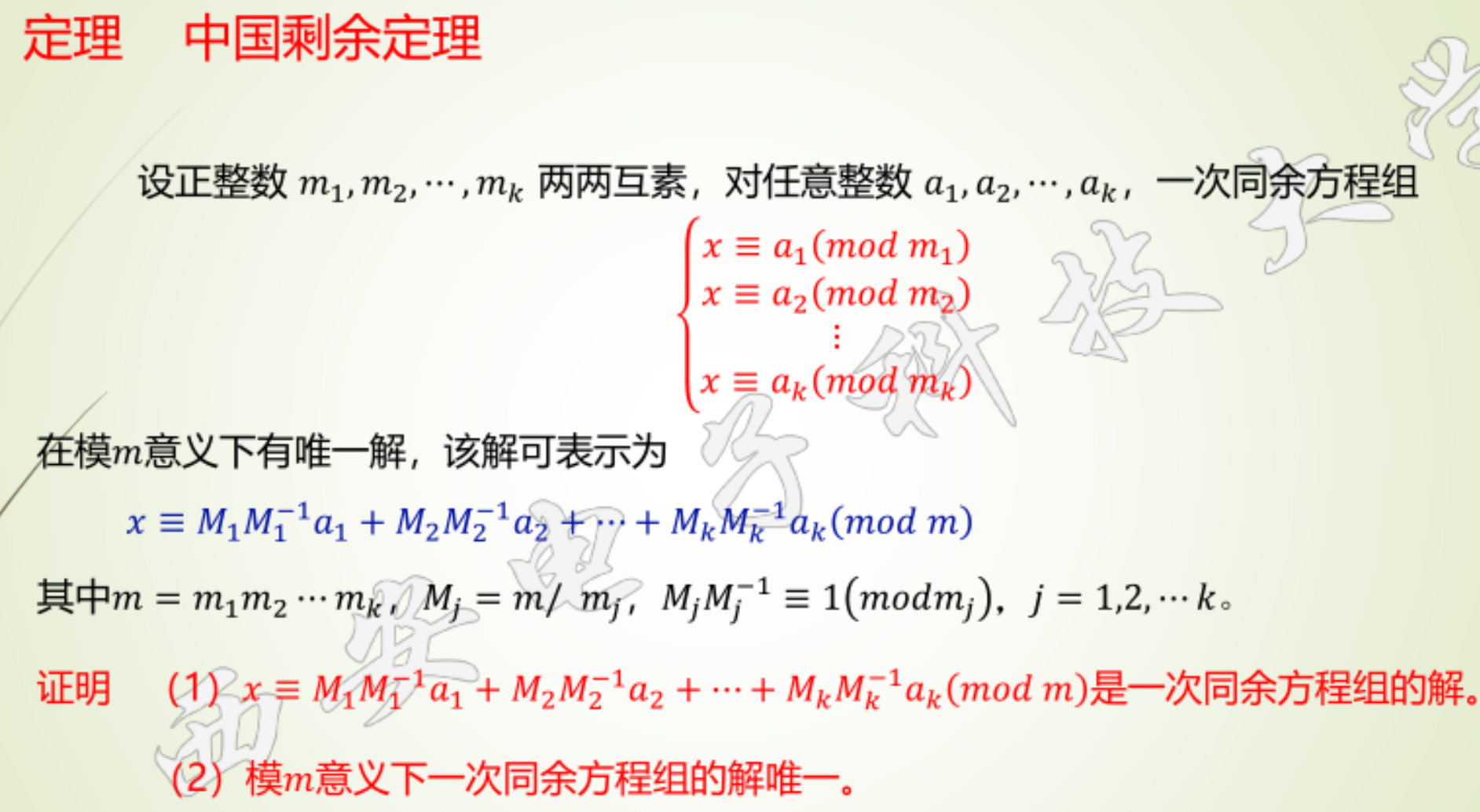
一、实验目的（包括实验环境、实现目标等等）

Python环境

实现功能：读取测试用例数据文件，根据中国剩余定理求解同余方程。若不能直接运用中国剩余定理，则抛出异常。

二、方案设计

（包括背景、原理、必要的公式、图表、算法步骤等等）



根据中国剩余定理，我们可以解出特定的同余方程组。若方程的模数两两互素，则可以直接利用中国剩余定理，反之，则需要对方程进行适当的变换。

三、方案实现

（包括算法流程图、主要函数的介绍、算法实现的主要代码等等）

**主要函数：**

read() : 读取测试用例txt文件。返回和，作为下面的Chinese\_remainder\_theorem函数的输入。

EEA(r0, r1) : 扩展的欧几里得算法EEA，既可以用来计算最大公约数gcd，判断两数是否互素，也可以用来求逆元（两数互素的情况下）。

process() :在两模数不互素的情况下，会引发Error，此时这个函数捕获Error并处理之。

举例来说，如方程组，这个函数会将其处理为。而如果发现方程组无解，如，则直接返回无解，退出整个程序。

Chinese\_remainder\_theorem(a:list, m:list) : 输入参数为两个列表a,m，表示方程组。返回方程组的求解结果

**整个程序的算法流程：**

Step 0 : 用read()函数读取文件。

Step 1 : 使用EEA算法，判断输入的是否两两互素，若不是，则抛出异常,交给process()函数处理，处理完毕后，重新进入Step 1。若是，则进入下一步。

Step 2 : 计算所有的乘积product，计个以及其对的逆元。

Step 3 : 由中国剩余定理，算出x。

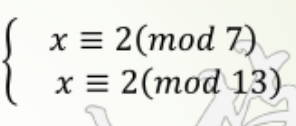
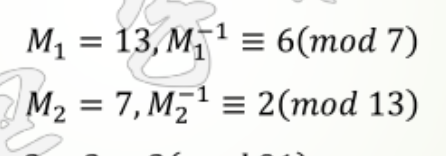
Step 4 : 把x代入每一个原始方程 ，如果发现x不符合方程，说明算法出错了，此时将抛出异常。若验证无误，进入下一步。

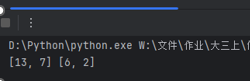
Step 5 : 返回x, product



四、数据分析(包括算法测试数据的分析，运行结果截图等等)

测试代码正确计算，的能力。输入课件中的例题。

,



我的代码正确计算并展示了，

对四个测试用例进行分析：

**测试用例1：模数不互素，此时交给process()处理，发现方程组无解。**

下面是具体信息，7为不互素的两个模数的gcd。下面的运行结果即表明了拆分出的两个方程，为，无解。

4921922096309750075533208251523367314717593943951238138265513715971801036714732566696839790240080246977741152988758234258092820455573681970491515868587779424233198757729285573790525399474751561292358503949670101971779313057008249263041379968068643559 mod 7 = 6

3840551325283606674102886622447517608826187679911017106436687357369367145645445084929833546662582898546069402730453103380742675012929023461699319099869547233097568514205177874422998622299815913136593212838213797740348979720724434773310697466616328535 mod 7 = 0

**测试用例2：模数不互素，无解。**

具体错误信息表明了程序拆分出两个方程

5564646478234054719254853557635895800739684755237704021659770004126282300536897264253153955799343011871839418345351696708344140857651062293613308591916739766144822155581219462428090037729032425995963744950022132719090576953213832964174881064568823251 mod 5 = 1

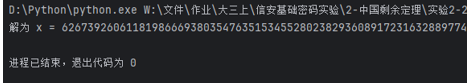
2538662590596928918650812976560631166430720191372392061450580607650881080200712115718179237788588565781836345528954308781114120890690924108478330550027320807928310868085156459127153388769582327186749348854118486996952019045410272194657704205537896945 mod 5 = 0

**测试用例3：成功运行**



解为 x = 45850971538430920039809835342035044426533971942190857312514912565486102915227406089504637818741931696932764106465317645904504603389530337155864680670919876795633911955760040080478044154170967765171716227794781985746935101945954494367888075899401250020053828724797519906076403988854722257909423631915311803168435017404946975580870213059707263130497544483848012050936544965684165927589759568960270987203441010266895562059551047160497042549580208730503986196805685742898949454146252047342004263899297290352022925068888842847365514463830992010079124868369216920001186960543284874385035998480029862150276601705976521890712672606441884107284501236336640253336010280687676722387082266736122849510381088976153557510307378833176629203010712055604988133944905160586176524594316889459005908884571099464152689527352656388293853679883196076846081112428967757311121854885585398974679164977769195152760696616838930 **mod** 102953832293616703082874624607037553231426094393000604596563545732446973727582341533346913587136260412778337180298510616242708622128935479711050576448612145240696174593019874832706301415100653058893794290959724419437953367492390340966268444747921797002666302065419051284327316436596511610022028215683792605669607405846246497742157867114795477989041761794634036907583854616979469929197455574810495931418179547756207701750504953681908376067692967274515542008467677105644775319423602660757912702485599517785360716305908479237359822322474824561080012142075430498482341564681447500226439508529311218175599586292185893671487692689314204073453837111333506885062212732994672392190791606071313185669874404097203502329489287292532064710265497653276514454976780972201788622137736651988293004202789504266484385346148359440631518283752042877070987341306359791629867004079011333875796459161265020098175460251658121

**测试用例4：成功运行**



解为 x = 6267392606118198666938035476351534552802382936089172316328897743172879764627673832131449798293751185675320730176964699395631150273511279869866962949345864622797615713555674040289129805845061504238254321801506909926464213324484282320421714571228986528089352506899736933010662849746895547877896800919085622299496414516521109484070814786174506514498019165273501727938625402571547656353590057030677574223761865456469779358997466768453711269097718055367640778587218315980747316831735149013184044851096369030486987130491601121502670977591761060152995444043920595601104637105776654836634982589836094359514364557075424100659668050103473452225458227798148841038514448303792904955511004133401282914950720654749341284341008310482855102942461387434475549098702381300184287945365098142095772121750282771162438266376091878150477584642296687481954338735808894790421992792101115025793836754451597837211648884480656 **mod** 44167277834865318505925595731740386714593071054649787728685371512227686532265418022642357197285711900295512424016844199185788883565360474703044658969981685507339838422310164225398785934740120773018715935919913595031403123730195548868895596981780364410766438153687334085748954703628390494088766685638724111099153395397990775139019064220117946529126064087603370677680157881819738461102417259553876319102288706171985087178697972986242540571926766725811581285490145946480434821092468831574238874260238224160478687257261737726163348031263191488802014458498928371530579204439498493860479203458297644637699484139562127849767251451367401649996295995201735622769926331841381668172373020987044031367797353154923281862023390934881926814699658430510263517934218266652711222603092764613010527837639734437073454613947384979607624431521137936390961606575979334870290494119935029783148127265051014571924493060770273

五、思考与总结

1. 求一次同余方程组的解，若正整数𝒎𝟏，𝒎𝟐，…，𝒎𝒌不是两两互素，是否能直接用中国剩余定理求解？例如方程组，需要如何求解？

若正整数𝒎𝟏，𝒎𝟐，…，𝒎𝒌不是两两互素，不能直接用中国剩余定理求解。需要先对方程进行变换。

由于18可以分解为18=2\*9，,可以对其进行如下改写

同理，对于第二个方程，有如下改写，这一步需要用到



综上，原方程组可以改写为：  
这样，就可以利用中国剩余定理，解得

1. 实验过程中还遇到了什么问题，如何解决的？通过该实验有何收获？

在进行试验时，模数不互素的情况很难处理。这是因为输入的数字都是大整数，如果对其进行质因数分解是困难的。因此，只能采取实验中描述的方式，在检验到不互素时，再拆分成多个方程进行处理。这一处理逻辑同样是复杂的，会出现很多bug。

通过该实验，我深入理解了中国剩余定理，加强了数论知识。通过分析和实现不同的方法，也提升了算法和编程能力。

**实验报告提交说明**：

1. 实验报告同时提交word文档与源代码（.c或者.py）。
2. 实验报告与源代码命名规则：实验2-学号-姓名，例如：实验2-20009200400-张三。
3. 请于截止日期前在西电智课平台（学在西电）提交相关文档，逾期未提交，该部分成绩记为0分，周知。