实验一-数论基础

【实验目的】

1、通过本次实验，熟悉编程环境，为后续实验做好铺垫。

2、回顾数论的基本算法，加深对其理解，为本学期密码学课程及实验课打好基础。

【实验内容】

1、 厄拉多塞筛法

实现厄拉多塞筛法并尝试进行优化，对于给定输入 N，请输出[2,N]之间所有素数；比较不同优化方法的时间、存储效率。

测试点：1）2；

2）103；

3）10^4；

4）10^6；

5）4275117753

2、 欧几里得算法

实现 GCD 算法和扩展 GCD 算法，对于给定输入 a 与 b，前者只需给出最大公约数(a,b)，后者需给出满足等式 ax+by=(a,b)的三个值：x,y,(a,b)；比较二者时间空间效率的不同。

测试点：1）7,5；

2）31,-13；

3）24,36；

4）

246150272351567308665870425694491242606517292557 5，

172087657754277021481119930882347652892954223171 9；

5）

137096164691449488835122291235023051763859318102840889067550902384318989727089044391788984680217107984018759866571252110844726214995953712543463907383820 42，

192350399949876251675909634808997772559337752383120440971227732556475302768063176360267276798008253704593216177248715154421474324209512570378231410696401 81；

6）

965578072786402991215194630452063779349788872980869942115905155

717173259557859237831594324363078705127423548774767900468918021530537192638456026184224746717078961368147078757933000409167572288261084994903112959425534780109130436805236126554005262552907029834903821914190670577266243488153915091613044773227 82，

1461167993057022192205401235038906667047104106008563870717762215924772567527599977981699318091564264712437997953740725104236453636805373378137742686589071309699941467834516928372227721449414349090506528257155829676849848140954610411099991614682232725348333913350366128637827407845731108240918669696559310970 32；

3、 快速幂取模

实现常规幂取模算法和快速幂模算法，实现常规幂取模算法和快速幂模算法，对于给定输入 a,b,c,要求输出为 a^b%c；比较二者时间空间效率的不同。

测试点：1）7,16,3;

2）5,1003,31

3）

1494462659429290047815067355171411187560751791530，

65537，

22688387113047243043043961195094167745977232924 74；

4）

2249081287653988504633605304004336102277206222690576441431953141675262498296718145591252615303303022298577823031407083754914306802181519791033422100433309 9，

65537，

2638103680625439121125582533003162590889548663549682017081139757611889270552615152613931291679885903024221918117851783792090402272045993185963317090572951 7；

5）

2372180752788922295351402387687622354051456455576407247442074663705448464576826633699763227989443924331042805955846358968212450487376372893618967033004547951754888617248133248674551191202846127858713043519405019307147750244177240514403375108975476612174663547008930114968923484072288061384611200649579076865 66，

65537，

3499728066887849366699657594205002874812747993283556335928400016613823405872472000557465228142759024303703309547256976487476100844

77917676220179203273361291098368287612837135979510900982047154261023406927515096043384562410643544643505195484211397819374480917731785250826080723518532061522456937734714740424476；

6）

448491664748214835887077572737743989471818983924746533195711112723370968680112145505675868905886297697651811535959153343019297445815718781370807622258565317729681110144781420923700723193680834808549790079348059612669341617763791748262779560287414722951999863579554855226385841903174595011558143906566236113746355880815410935162653615576832860612181499713446185302492149321184607038850277，

266848195381815818463717950266554236453862598799637312683425703733349860929573593996414020829279843574050749733141808826377733991992433000295290381444934817157435190251178268111713086611665708753888640498769964215272509919856595016440707694201919276657450513307401642404169770745634306482286288562684063317756864776774548994812022552274677735053131675109617882635817658233698378909301711242970820585209428037532351125028227556492657705501994644156977193457255573644987541990311834672767028439520378145222935082885623390192713665176848108677291865357438200，

264496104806945826630879147982623492753075837057692083206159998879685335475780430323991934716494671303972123381722817408983444808360534839804151416632594468843753733714512310041016226248011998384117072606363846922087540888426192580126275854056635599339955169813796313364463130201488176467179855490513011152385276774729148527427882568902594022248994534194842165583275231223417490546129679017471552761001579139105477841364398884899527245085546136326414204870392428817432327561682927099899849254369112673228859179533480646730212838229371587066786663721036270741630212605780780173040889041548591612890370709122202079469 45；

4、 中国剩余定理

实现中国剩余定理，对于式 $x\%a_i=b_i$，对于给定的 a_1， a_2， a_3 和 b_1， b_2， b_3， 求 x；

测试点：1）23,28,33;　　0,0,0;

2）23,28,33;　　5,20,34;

3）23,28,33;　　283,102,23;

4)

489808178709479466279507878773770708214878979673，
896234965496726578561614071442814700467907036641，
121382700575830560246688299217231040945605386843；

802310684485241212312289432691586430708135062249，
961714109955647014172499578071923389425123540027，
138119400608730402468355271248802259519409792870l；

5）
815796954028841163781843303955832318407477908610016550466853822192017036977491326133505960233162732113065645896298022419688053333783922605960130346477614 5，
969961604431502119495357256107650299278313062321657422042604360014234350410150883852622135904941756441580191407231578891927579250247769302285388178519811 6，
783269380225637166786651421311945219982191619366810690413581228321763773760092238170201647270885567564912127170297740821781491790856613251750370749403755 6；

133923160816514208773088752761667728086018121220523714423390788777403995692816726838202061963209550058690720028838476465265841072603554149771204532633919 47，
973446693965828282334376020659328396876590484825002158021863438386909091308634885766899927239907501628773691400085427223931576963271989696809882077456351 1，
946020035779072839886291323266403603869452185841576593106450519375520215652144615649907545003342998331712758963659113311123954882125179017169432293001192 7；

5、素性检测算法

实现 Milar-Rabin 素性检测算法，对于给定大数能够正确检测是否为素数；并分析检测次数与能够正确检测的概率之间的关系；

测试点：1）1000023；
2）1000033；
3）100160063；
4）1500450271；
5）14944626594292900478150673551714111875607517915 30；

6）

224908128765398850463360530400433610227720622269057644143195314167526249829671814559125261530330302229857782303140708375491430680218151979103342210043330997）

1731145387154422538016526365785048972358140583760120199841322804930731441408734238220669265338517685935679729860307869308653045247658739172911568203565934653959496156683117305245858627132169771180301626143311163205775331537122809971293477436230828192523540002240987023004665611577159903748518147171339859996618【实验报告】

(1) 请详细阅读附件一中有关代码和实验报告的要求部分，并将算法文件与实验报告打包为压缩文件。命名格式为：学号_姓名_实验一.rar，如 17373131_李浩民_实验一.rar。

(2) 代码应有必要的注释。实验报告应至少含有算法原理、算法流程、测试样例及运行结果，以及心得体会或感想建议。

(3) 本次课后两周内完成实验，请务必于校历第三周实验课前，将打包文件发送至指定邮箱 crypt_2020_4@163.com，逾期者酌情扣分。

【思考题】

1、 思考厄拉多塞筛法中如何减少重复比较以提高速度；

2、 考虑中国剩余定理的实现中是否有可以改进的地方。