Primality Testing

May 4, 2022

Contents

Preface

This is my CATAM project, 15.1 for part II. The code for each question can be found in section 5.

1 Trial Division

1.1 Question 1

Below are the primes in the intervals $[188000, 188200]$ and $[10^9, 10^9 + 200]$.

188011
188017
188021
188029
188107
188137
188143
188147
188159
188171
188179
188189
188197

Table 1: Primes between 188000 and 188200

1000000007
1000000009
1000000021
1000000033
1000000087
1000000093
1000000097
1000000103
1000000123
1000000181

Table 2: Primes between 10^9 and $10^9 + 200$

2 The Fermat Test

2.1 Question 2

Below are tables of the pseudo primes in the intervals $[188000, 188200]$ in base 2 to base 13. We don't include a table for pseudo primes in the interval $[10^9, 10^9 + 200]$ since there are none. Note for we exclude a for which there are no pseudo primes base a in the interval.

Base								
2	3	4	5	7	8	9	10	12
188057	188191	188057	188113	188191	188057	188191	188191	188191
-	-	188191	-	-	-	-	-	-

Table 3: Pseudo primes between 188000 and 188200 in base 2 to base 13

The complexity of the algorithm is $O(n^2)$. This is because all the loops but 1 are not nested within one another so these are all $O(n)$. The only exception to this is when for each i^{th} digit of the number -1 (in binary) we're testing is 1 or 0 and then based on this decide whether or not to include $a^{2^{i-1}}$ in the final product when calculating a^{p-1}. Since we do this for each digit this has complexity $O(n^2)$ and hence the complexity of the algorithm is $O(n^2)$.

2.2 Question 3

There are 43 absolute pseudo primes and 245 pseudo primes base 2. in the interval $[2, 10^6]$. This tells us that the vast majority of composite numbers in this interval fail the Fermat test to this base. Further for the remaining composite numbers, 151 failed the Fermat test for the base 3. On average for (non absolute pseudo prime) composite numbers which passed the Fermat test base 2, it took 2.74 bases for them to fail the Fermat test and maximally took 10 bases for any such number to fail the Fermat test. In short the probability of a composite number being an absolute pseudo prime is very low in this interval, and the number of bases required to show such is also quite low.

3 The Euler Test

3.1 Question 4

There are no absolute Euler pseudo primes, this is due to the Solovay-Strassen Theorem which states for any odd $n > 2$, n is prime if and only if for all integers a s.t $(a, n) = 1$ we have

$$\left(\frac{a}{n}\right) = a^{\frac{n-1}{2}} \pmod{n}.$$

The program found no absolute Euler pseudo primes in the interval $[2, 10^6]$ and so agrees with this result.

There were 114 composite numbers in $[2, 10^6]$ which passed the Euler test for $a = 2$ and required further checking, hence the chance of a composite number passing the Euler test for $a = 2$ is lower than that of the Fermat test in this interval. Interestingly however, the average number of bases needed for a composite number to fail the Euler test, if it passed for $a = 2$ was higher than that of the Fermat test. On average such numbers needed to be checked with 3.7 different bases and maximally took 28 bases for it to fail the Euler test.

4 The Strong Test

4.1 Question 5

It is again a fact of number theory that there are no absolute strong pseudo primes. The program found no absolute strong pseudo primes in the interval $[2, 10^6]$ and so agrees with this result.

This was by far the most efficient and quickest prime tester of the three. There were only 46 composite numbers which passed the test for $a = 2$ and all of these failed the test for $a = 3$. This is much better than the previous three program.

5 Code

5.1 Question 1

```
function [outputArg1,outputArg2] = Q1(AA)
AA=N;
BBB(1)=0;
iii=1;
jjj=1;
while jjj <= size(AA,2)
    nnn=2;
    ttt=0;
    while nnn<= sqrt(AA(jjj))
        if gcd(nnn,AA(jjj))==nnn
            ttt=ttt+1;
        else
        end
        nnn=nnn+1;
    end
        if ttt==0
            BBB(iii)=AA(jjj);
```

```
            iii=iii+1;
        else
        end
 jjj=jjj+1;
    end
BBB'
end
```

5.2 Question 2

```
function [outputArg1,outputArg2] = Q2(aa,A)
rr=size(aa,2);
qq=1;
while qq<= rr
a=aa(qq);

i=1;
j=1;
B(qq,1)=0;
k=size(A,2);
while j<=k
    p=A(j);
    %Calculate a^{p-1}=t
        bin=dec2bin(p-1);
        n=numel(num2str(bin));
        f=1;
        while f<= n
            y=num2str(bin);
            d(f)=str2num(y(n-f+1));
            f=f+1;
        end
        e(1)=a;
        f=2;
        while f<= n

            edig=numel(num2str(e(f-1)));
            if edig >= 7
                esmall=mod(e(f-1),10^6);
                ebig=(e(f-1)-esmall)/10^6;



                prod1=mod(esmall*esmall,p);

                tensmall=mod(10^6,p);

                prod2a=mod(ebig*ebig,p);
                prod2b=mod(prod2a*tensmall,p);
                prod2=mod(prod2b*tensmall,p);

                prod3a=mod(ebig*esmall,p);
                prod3=mod(prod3a*tensmall,p);

                prod4a=mod(esmall*ebig,p);
                prod4=mod(prod4a*tensmall,p);

                e(f)=mod(prod1+prod2+prod3+prod4,p);
            else
                e(f)=mod(e(f-1)^2,p);
```

```
            end

            f=f+1;
        end
        h=1;
        q=1;
        D=0;
        while h<=n
            if d(h)==1
                D(q)=e(h);
                q=q+1;
            else
            end
            h=h+1;
        end
        ZZ=size(D,2);
        zz=2;
        t=D(1);
        while zz <= ZZ

            tdig=numel(num2str(t));
            Ddig=numel(num2str(D(zz)));

            if tdig+Ddig >= 14
                tsmall=mod(t,10^6);
                tbig=(t-tsmall)/10^6;
                Dsmall=mod(D(zz),10^6);
                Dbig=(D(zz)-Dsmall)/10^6;


                prod1=mod(tsmall*Dsmall,p);

                tensmall=mod(10^6,p);

                prod2a=mod(tbig*Dbig,p);
                prod2b=mod(prod2a*tensmall,p);
                prod2=mod(prod2b*tensmall,p);

                prod3a=mod(tbig*Dsmall,p);
                prod3=mod(prod3a*tensmall,p);

                prod4a=mod(tsmall*Dbig,p);
                prod4=mod(prod4a*tensmall,p);

                t=mod(prod1+prod2+prod3+prod4,p);
            else
                 t=mod(D(zz)*t,p);


            end









            zz=zz+1;
        end
    %Finished calculating a^{p-1}=t
    if t==1
```

```
        B(qq,i)=p;
        i=i+1;
    else
    end
j=j+1;
end
qq=qq+1;
end

B'
stuff=B';
maxim=size(stuff,2);
i=1;
actualprimes=[1000000007;
1000000009;
1000000021;
1000000033;
1000000087;
1000000093;
1000000097;
1000000103;
1000000123;
1000000181];
while i<= maxim
    newstuff(:,i)=setdiff(stuff(:,i),actualprimes);
    i=i+1;
end
newstuff




end
```

5.3 Question 3

```
function [outputArg1,outputArg2] = Q3(range)

rangeindex=1;
rangemax=size(range,2);
indexing=1;
otherindexing=1;
abspseudo(1,:)=[0,0];
nonprime(1,:)=[0,0];
while rangeindex <= rangemax
    p=range(rangeindex);
    p;
    a=2;
    terminatetest=0;
    while terminatetest==0 && a<= p-1
        %do fermat test
                greatestcommon = gcd(a,p);
                if greatestcommon ==1
                        bin=dec2bin(p-1);
                        n=numel(num2str(bin));
                        f=1;
                        while f<= n
                            y=num2str(bin);
```

```
        d(f)=str2num(y(n-f+1));
        f=f+1;
    end
    e(1)=a;
    f=2;
    while f<= n

        edig=numel(num2str(e(f-1)));
        if edig >= 7
            esmall=mod(e(f-1),10^6);
            ebig=(e(f-1)-esmall)/10^6;



            prod1=mod(esmall*esmall,p);

            tensmall=mod(10^6,p);

            prod2a=mod(ebig*ebig,p);
            prod2b=mod(prod2a*tensmall,p);
            prod2=mod(prod2b*tensmall,p);

            prod3a=mod(ebig*esmall,p);
            prod3=mod(prod3a*tensmall,p);

            prod4a=mod(esmall*ebig,p);
            prod4=mod(prod4a*tensmall,p);

            e(f)=mod(prod1+prod2+prod3+prod4,p);
        else
            e(f)=mod(e(f-1)^2,p);
        end

        f=f+1;
    end
    h=1;
    q=1;
    D=0;
    while h<=n
        if d(h)==1
            D(q)=e(h);
            q=q+1;
        else
        end
        h=h+1;
    end
    ZZ=size(D,2);
    zz=2;
    t=D(1);
    while zz <= ZZ

        tdig=numel(num2str(t));
        Ddig=numel(num2str(D(zz)));

        if tdig+Ddig >= 14
            tsmall=mod(t,10^6);
            tbig=(t-tsmall)/10^6;
            Dsmall=mod(D(zz),10^6);
            Dbig=(D(zz)-Dsmall)/10^6;

```

```
                                prod1=mod(tsmall*Dsmall,p);

                                tensmall=mod(10^6,p);

                                prod2a=mod(tbig*Dbig,p);
                                prod2b=mod(prod2a*tensmall,p);
                                prod2=mod(prod2b*tensmall,p);

                                prod3a=mod(tbig*Dsmall,p);
                                prod3=mod(prod3a*tensmall,p);

                                prod4a=mod(tsmall*Dbig,p);
                                prod4=mod(prod4a*tensmall,p);

                                t=mod(prod1+prod2+prod3+prod4,p);
                            else
                                 t=mod(D(zz)*t,p);


                            end









                            zz=zz+1;
                        end
                    %Finished calculating a^{p-1}=t



        %
        if t ~= 1
            nonprime(indexing,:)=[p,a-1];
            indexing=indexing+1;
            terminatetest=1;
        else


            a=a+1;
        end
                else
                    a=a+1;
                end
    end
    if ismember(p,nonprime(:,1))
    else
        abspseudo(otherindexing)=p;
        otherindexing=otherindexing+1;
    end
    rangeindex=rangeindex+1;
end

new=size(nonprime,1);
i=1;
j=1;
while i<= new
```

```
    if nonprime(i,2)>1
        care(j,:)=nonprime(i,:);
        j=j+1;
    end
    i=i+1;
end



abspseudo
care;
nonprime




end
```

5.4 Question 4

```
function [outputArg1,outputArg2] = Q4(range)
rangeindex=1;
rangemax=size(range,2);
indexing=1;
otherindexing=1;
abspseudo(1,:)=[0,0];
nonprime(1,:)=[0,0];
while rangeindex <= rangemax
    p=range(rangeindex);
    p;
    a=2;
    terminatetest=0;
    while terminatetest==0 && a<= p-1
        %do fermat test
        a;
        p;
                greatestcommon = gcd(a,p);
                N=p;
                if gcd(p,2)==2;
                    if p==2
                        a=a+1;
                        terminatetest=1;
                    else
                        nonprime(indexing,:)=[p,a-1];
                        indexing=indexing+1;
                        terminatetest=1;
                    end
                elseif greatestcommon ==1
                        bin=dec2bin((p-1)/2);
                            n=numel(num2str(bin));
                            f=1;
                            d=0;
                            while f<= n
                                y=num2str(bin);
                                d(f)=str2num(y(n-f+1));
                                f=f+1;
                            end
                            e=0;
```

```
e(1)=a;
f=2;
while f<= n

if e(f-1) >= 10^7
    esmall=mod(e(f-1),10^6);
    ebig=(e(f-1)-esmall)/10^6;



    prod1=mod(esmall*esmall,p);

    tensmall=mod(10^6,p);

    prod2a=mod(ebig*ebig,p);
    prod2b=mod(prod2a*tensmall,p);
    prod2=mod(prod2b*tensmall,p);

    prod3a=mod(ebig*esmall,p);
    prod3=mod(prod3a*tensmall,p);

    prod4a=mod(esmall*ebig,p);
    prod4=mod(prod4a*tensmall,p);

    e(f)=mod(prod1+prod2+prod3+prod4,p);
else
    e(f)=mod(e(f-1)^2,p);
end
    f=f+1;
end
h=1;
q=1;
D=0;
while h<=n
    if d(h)==1
        D(q)=e(h);
        q=q+1;
    else
    end
    h=h+1;
end
ZZ=size(D,2);
zz=2;
t=D(1);
while zz <= ZZ


        if t*D(zz) >= 10^143
            tsmall=mod(t,10^6);
            tbig=(t-tsmall)/10^6;
            Dsmall=mod(D(zz),10^6);
            Dbig=(D(zz)-Dsmall)/10^6;


            prod1=mod(tsmall*Dsmall,p);

            tensmall=mod(10^6,p);

            prod2a=mod(tbig*Dbig,p);
            prod2b=mod(prod2a*tensmall,p);
```

```
                        prod2=mod(prod2b*tensmall,p);

                        prod3a=mod(tbig*Dsmall,p);
                        prod3=mod(prod3a*tensmall,p);

                        prod4a=mod(tsmall*Dbig,p);
                        prod4=mod(prod4a*tensmall,p);

                        t=mod(prod1+prod2+prod3+prod4,p);
                    else
                         t=mod(D(zz)*t,p);


                    end
                zz=zz+1;
            end
        %Finished calculating a^{p-1}=t
        Power=t;
    %Calculated a^(N-1)/2 mod N

    %Calculate (a/N)
        d=1;
        b=N;
        J=1;
        if mod(b,2)==0
        d=2;
    end

    if gcd(a,b) ~= 1
        d=3;
    end

    if d==2
        disp(['Error'])
    elseif d==3
        Jacobi=0;
    else

            aa=a;

    while aa ~= 1
            aa=mod(aa,b);
        while mod(aa,2)==0
          J=(-1)^(((b^2)-1)/8)*J;
          aa=aa/2;
        end
        J=(-1)^(((aa-1)*(b-1))/4)*J;
        A=aa;
        aa=b;
        b=A;
        aa=mod(aa,b);

        if mod(aa+1,b)== 0
            J=(-1)^((b-1)/2)*J;
            aa=1;
        end
    end
    Jacobi=J;

    end
```

```
159
160
161                     %Test to see if Jacobi symbol is equal to power
162                     Test = mod(J-Power,N);
163
164
165
166
167                     %Finish test to see if Jacobi symbol = power
168
169
170
171
172         %
173                     if Test ~= 0
174                         nonprime(indexing,:)=[p,a-1];
175                         indexing=indexing+1;
176                         terminatetest=1;
177                     else
178
179
180                         a=a+1;
181                     end
182                 else
183                     a=a+1;
184                 end
185     end
186     if ismember(p,nonprime(:,1))
187     else
188         abspseudo(otherindexing)=p;
189         otherindexing=otherindexing+1;
190     end
191     rangeindex=rangeindex+1;
192 end
193
194 new=size(nonprime,1);
195 i=1;
196 j=1;
197
198 while i<= new
199     if nonprime(i,2)>1
200         careabout(j,:)=nonprime(i,:);
201         j=j+1;
202     end
203     i=i+1;
204 end
205
206
207
208 abspseudo
209 careabout
210 nonprime;
211 end
```

5.5 Question 5

```
1 function [outputArg1,outputArg2] = Q5(range)
2 rangeindex=1;
3 rangemax=size(range,2);
```

```
indexing=1;
otherindexing=1;
abspseudo(1,:)=[0,0];
nonprime(1,:)=[0,0];
while rangeindex <= rangemax
    p=range(rangeindex);
    p;
    a=2;
    terminatetest=0;
    while terminatetest==0 && a<= p-1
        %do fermat test
                greatestcommon = gcd(a,p);
                if greatestcommon ==1
                        %Find r and odd s with N-1=s2^r
                                        r=0;
                                        N=p;
                                        Q=p-1;
                                        while mod(Q,2)==0
                                            r=r+1;
                                            Q=Q/2;
                                        end
                                        s=(N-1)/(2^r);
                                    %Found s and r


                                    %Find Power = a^s mod N


                                        bin=dec2bin(s);
                                        n=numel(num2str(bin));
                                        f=1;
                                        while f<= n
                                            y=num2str(bin);
                                            d(f)=str2num(y(n-f+1));
                                            f=f+1;
                                        end
                                        e(1)=a;
                                        f=2;
                                        while f<= n
                                            if e(f-1) >= 10^7
                                                esmall=mod(e(f-1),10^6);
                                                ebig=(e(f-1)-esmall)/10^6;



                                                prod1=mod(esmall*esmall,p);

                                                tensmall=mod(10^6,p);

                                                prod2a=mod(ebig*ebig,p);
                                                prod2b=mod(prod2a*tensmall,p);
                                                prod2=mod(prod2b*tensmall,p);

                                                prod3a=mod(ebig*esmall,p);
                                                prod3=mod(prod3a*tensmall,p);

                                                prod4a=mod(esmall*ebig,p);
                                                prod4=mod(prod4a*tensmall,p);
```

```
                    e(f)=mod(prod1+prod2+prod3+prod4,p
                        );
                else
                    e(f)=mod(e(f-1)^2,p);
                end
                f=f+1;
            end
            h=1;
            q=1;
            D=0;
            while h<=n
                if d(h)==1
                    D(q)=e(h);
                    q=q+1;
                else
                end
                h=h+1;
            end
            ZZ=size(D,2);
            zz=2;
            t=D(1);
            while zz <= ZZ
                 if t*D(zz) >= 10^143
                        tsmall=mod(t,10^6);
                        tbig=(t-tsmall)/10^6;
                        Dsmall=mod(D(zz),10^6);
                        Dbig=(D(zz)-Dsmall)/10^6;


                        prod1=mod(tsmall*Dsmall,p);

                        tensmall=mod(10^6,p);

                        prod2a=mod(tbig*Dbig,p);
                        prod2b=mod(prod2a*tensmall,p);
                        prod2=mod(prod2b*tensmall,p);

                        prod3a=mod(tbig*Dsmall,p);
                        prod3=mod(prod3a*tensmall,p);

                        prod4a=mod(tsmall*Dbig,p);
                        prod4=mod(prod4a*tensmall,p);

                        t=mod(prod1+prod2+prod3+prod4,
                            p);
                    else
                         t=mod(D(zz)*t,p);


                    end
                zz=zz+1;
            end

           Power=t;
           if Power == p-1;
               Power= -1;
           end
       %Calculated a^s mod N


```

```
                                    %Calculate X=(a^s,...,a^2^r-1 s)

                                        i=2;
                                        X(1)=Power;
                                        while i<= r
                                            X(i)=mod((X(i-1))^2,N);
                                            if X(i)==N-1;
                                                X(i)=-1;
                                            end
                                            i=i+1;

                                        end
                                        X;
                                    %Calculated X

                                    %Carry out test
                                        if X(1)==1
                                            a=a+1;
                                        elseif all( X ~= -1)
                                            nonprime(indexing,:)=[p,a-1];
                                            indexing=indexing+1;
                                            terminatetest=1;
                                        else
                                            a=a+1;
                                        end
                                    %Carried out testr



        %

                else
                    a=a+1;
                end
    end
    if ismember(p,nonprime(:,1))
    else
        abspseudo(otherindexing)=p;
        otherindexing=otherindexing+1;
    end
    rangeindex=rangeindex+1;
end

new=size(nonprime,1);
i=1;
j=1;
while i<= new
    if nonprime(i,2)>1
        care(j,:)=nonprime(i,:);
        j=j+1;
    end
    i=i+1;
end



abspseudo
care
nonprime;
```

```
181 end
```