

Primality Testing

May 4, 2022

Contents

1	Trial Division	3
1.1	Question 1	3
2	The Fermat Test	3
2.1	Question 2	3
2.2	Question 3	4
3	The Euler Test	4
3.1	Question 4	4
4	The Strong Test	4
4.1	Question 5	4
5	Code	4
5.1	Question 1	4
5.2	Question 2	5
5.3	Question 3	7
5.4	Question 4	10
5.5	Question 5	13

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

```
1 function [outputArg1,outputArg2] = Q1(AA)
2 AA=N;
3 BBB(1)=0;
4 iii=1;
5 jjj=1;
6 while jjj <= size(AA,2)
7     nnn=2;
8     ttt=0;
9     while nnn<= sqrt(AA(jjj))
10         if gcd(nnn,AA(jjj))==nnn
11             ttt=ttt+1;
12         else
13             end
14             nnn=nnn+1;
15     end
16     if ttt==0
17         BBB(iii)=AA(jjj);
```

```

18         iii=iii+1;
19     else
20     end
21     jjj=jjj+1;
22     end
23     BBB '
24 end

```

5.2 Question 2

```

1 function [outputArg1,outputArg2] = Q2(aa,A)
2 rr=size(aa,2);
3 qq=1;
4 while qq<= rr
5     a=aa(qq);
6
7     i=1;
8     j=1;
9     B(qq,1)=0;
10    k=size(A,2);
11    while j<=k
12        p=A(j);
13        %Calculate  $a^{p-1}=t$ 
14        bin=dec2bin(p-1);
15        n=numel(num2str(bin));
16        f=1;
17        while f<= n
18            y=num2str(bin);
19            d(f)=str2num(y(n-f+1));
20            f=f+1;
21        end
22        e(1)=a;
23        f=2;
24        while f<= n
25
26            edig=numel(num2str(e(f-1)));
27            if edig >= 7
28                esmall=mod(e(f-1),10^6);
29                ebig=(e(f-1)-esmall)/10^6;
30
31
32                prod1=mod(esmall*esmall,p);
33
34                tensmall=mod(10^6,p);
35
36                prod2a=mod(ebig*ebig,p);
37                prod2b=mod(prod2a*tensmall,p);
38                prod2=mod(prod2b*tensmall,p);
39
40                prod3a=mod(ebig*esmall,p);
41                prod3=mod(prod3a*tensmall,p);
42
43                prod4a=mod(esmall*ebig,p);
44                prod4=mod(prod4a*tensmall,p);
45
46                e(f)=mod(prod1+prod2+prod3+prod4,p);
47            else
48                e(f)=mod(e(f-1)^2,p);
49            end

```

```

50         end
51
52         f=f+1;
53     end
54     h=1;
55     q=1;
56     D=0;
57     while h<=n
58         if d(h)==1
59             D(q)=e(h);
60             q=q+1;
61         else
62             end
63             h=h+1;
64     end
65     ZZ=size(D,2);
66     zz=2;
67     t=D(1);
68     while zz <= ZZ
69
70         tdig=numel(num2str(t));
71         Ddig=numel(num2str(D(zz)));
72
73         if tdig+Ddig >= 14
74             tsmall=mod(t,10^6);
75             tbig=(t-tsmall)/10^6;
76             Dsmall=mod(D(zz),10^6);
77             Dbig=(D(zz)-Dsmall)/10^6;
78
79
80             prod1=mod(tsmall*Dsmall,p);
81
82             tensmall=mod(10^6,p);
83
84             prod2a=mod(tbig*Dbig,p);
85             prod2b=mod(prod2a*tensmall,p);
86             prod2=mod(prod2b*tensmall,p);
87
88             prod3a=mod(tbig*Dsmall,p);
89             prod3=mod(prod3a*tensmall,p);
90
91             prod4a=mod(tsmall*Dbig,p);
92             prod4=mod(prod4a*tensmall,p);
93
94             t=mod(prod1+prod2+prod3+prod4,p);
95         else
96             t=mod(D(zz)*t,p);
97
98
99     end
100
101
102
103
104
105
106     zz=zz+1;
107 end
108 %Finished calculating a^{p-1}=t
109 if t==1

```

```

110         B(qq,i)=p;
111         i=i+1;
112     else
113     end
114 j=j+1;
115 end
116 qq=qq+1;
117 end
118
119 B'
120 stuff=B';
121 maxim=size(stuff,2);
122 i=1;
123 actualprimes=[1000000007;
124 1000000009;
125 1000000021;
126 1000000033;
127 1000000087;
128 1000000093;
129 1000000097;
130 1000000103;
131 1000000123;
132 1000000181];
133 while i<= maxim
134     newstuff(:,i)=setdiff(stuff(:,i),actualprimes);
135     i=i+1;
136 end
137 newstuff
138
139
140
141
142
143 end

```

5.3 Question 3

```

1 function [outputArg1,outputArg2] = Q3(range)
2
3 rangeindex=1;
4 rangemax=size(range,2);
5 indexing=1;
6 otherindexing=1;
7 abspseudo(1,:)= [0,0];
8 nonprime(1,:)= [0,0];
9 while rangeindex <= rangemax
10     p=range(rangeindex);
11     p;
12     a=2;
13     terminatetest=0;
14     while terminatetest==0 && a<= p-1
15         %do fermat test
16         greatestcommon = gcd(a,p);
17         if greatestcommon ==1
18             bin=dec2bin(p-1);
19             n=numel(num2str(bin));
20             f=1;
21             while f<= n
22                 y=num2str(bin);

```

```

23         d(f)=str2num(y(n-f+1));
24         f=f+1;
25     end
26     e(1)=a;
27     f=2;
28     while f<= n
29
30         edig=numel(num2str(e(f-1)));
31         if edig >= 7
32             esmall=mod(e(f-1),10^6);
33             ebig=(e(f-1)-esmall)/10^6;
34
35
36
37             prod1=mod(esmall*esmall,p);
38
39             tensmall=mod(10^6,p);
40
41             prod2a=mod(ebig*ebig,p);
42             prod2b=mod(prod2a*tensmall,p);
43             prod2=mod(prod2b*tensmall,p);
44
45             prod3a=mod(ebig*esmall,p);
46             prod3=mod(prod3a*tensmall,p);
47
48             prod4a=mod(esmall*ebig,p);
49             prod4=mod(prod4a*tensmall,p);
50
51             e(f)=mod(prod1+prod2+prod3+prod4,p);
52         else
53             e(f)=mod(e(f-1)^2,p);
54         end
55
56         f=f+1;
57     end
58     h=1;
59     q=1;
60     D=0;
61     while h<=n
62         if d(h)==1
63             D(q)=e(h);
64             q=q+1;
65         else
66             end
67         h=h+1;
68     end
69     ZZ=size(D,2);
70     zz=2;
71     t=D(1);
72     while zz <= ZZ
73
74         tdig=numel(num2str(t));
75         Ddig=numel(num2str(D(zz)));
76
77         if tdig+Ddig >= 14
78             tsmall=mod(t,10^6);
79             tbig=(t-tsmall)/10^6;
80             Dsmall=mod(D(zz),10^6);
81             Dbig=(D(zz)-Dsmall)/10^6;
82

```



```

83
84         prod1=mod(tsmall*Dsmall,p);
85
86         tensmall=mod(10^6,p);
87
88         prod2a=mod(tbig*Dbig,p);
89         prod2b=mod(prod2a*tensmall,p);
90         prod2=mod(prod2b*tensmall,p);
91
92         prod3a=mod(tbig*Dsmall,p);
93         prod3=mod(prod3a*tensmall,p);
94
95         prod4a=mod(tsmall*Dbig,p);
96         prod4=mod(prod4a*tensmall,p);
97
98         t=mod(prod1+prod2+prod3+prod4,p);
99     else
100         t=mod(D(zz)*t,p);
101
102
103     end
104
105
106
107
108
109
110         zz=zz+1;
111     end
112     %Finished calculating a^{p-1}=t
113
114
115
116
117     %
118     if t ~= 1
119         nonprime(indexing,:)= [p,a-1];
120         indexing=indexing+1;
121         terminatetest=1;
122     else
123
124
125         a=a+1;
126     end
127         else
128             a=a+1;
129         end
130     end
131     if ismember(p,nonprime(:,1))
132     else
133         abspseudo(otherindexing)=p;
134         otherindexing=otherindexing+1;
135     end
136     rangeindex=rangeindex+1;
137 end
138
139 new=size(nonprime,1);
140 i=1;
141 j=1;
142 while i<= new

```

```

143     if nonprime(i,2)>1
144         care(j,:)=nonprime(i,:);
145         j=j+1;
146     end
147     i=i+1;
148 end
149
150
151
152 abspseudo
153 care;
154 nonprime
155
156
157
158
159
160 end

```

5.4 Question 4

```

1 function [outputArg1,outputArg2] = Q4(range)
2 rangeindex=1;
3 rangemax=size(range,2);
4 indexing=1;
5 otherindexing=1;
6 abspseudo(1,:)= [0,0];
7 nonprime(1,:)= [0,0];
8 while rangeindex <= rangemax
9     p=range(rangeindex);
10    p;
11    a=2;
12    terminatetest=0;
13    while terminatetest==0 && a<= p-1
14        %do fermat test
15        a;
16        p;
17        greatestcommon = gcd(a,p);
18        N=p;
19        if gcd(p,2)==2;
20            if p==2
21                a=a+1;
22                terminatetest=1;
23            else
24                nonprime(indexing,:)= [p,a-1];
25                indexing=indexing+1;
26                terminatetest=1;
27            end
28        elseif greatestcommon ==1
29            bin=dec2bin((p-1)/2);
30            n=numel(num2str(bin));
31            f=1;
32            d=0;
33            while f<= n
34                y=num2str(bin);
35                d(f)=str2num(y(n-f+1));
36                f=f+1;
37            end
38            e=0;

```

```

39     e(1)=a;
40     f=2;
41     while f<= n
42
43     if e(f-1) >= 10^7
44         esmall=mod(e(f-1),10^6);
45         ebig=(e(f-1)-esmall)/10^6;
46
47
48
49         prod1=mod(esmall*esmall,p);
50
51         tensmall=mod(10^6,p);
52
53         prod2a=mod(ebig*ebig,p);
54         prod2b=mod(prod2a*tensmall,p);
55         prod2=mod(prod2b*tensmall,p);
56
57         prod3a=mod(ebig*esmall,p);
58         prod3=mod(prod3a*tensmall,p);
59
60         prod4a=mod(esmall*ebig,p);
61         prod4=mod(prod4a*tensmall,p);
62
63         e(f)=mod(prod1+prod2+prod3+prod4,p);
64     else
65         e(f)=mod(e(f-1)^2,p);
66     end
67     f=f+1;
68 end
69 h=1;
70 q=1;
71 D=0;
72 while h<=n
73     if d(h)==1
74         D(q)=e(h);
75         q=q+1;
76     else
77     end
78     h=h+1;
79 end
80 ZZ=size(D,2);
81 zz=2;
82 t=D(1);
83 while zz <= ZZ
84
85
86     if t*D(zz) >= 10^143
87         tsmall=mod(t,10^6);
88         tbig=(t-tsmall)/10^6;
89         Dsmall=mod(D(zz),10^6);
90         Dbig=(D(zz)-Dsmall)/10^6;
91
92
93         prod1=mod(tsmall*Dsmall,p);
94
95         tensmall=mod(10^6,p);
96
97         prod2a=mod(tbig*Dbig,p);
98         prod2b=mod(prod2a*tensmall,p);

```

```

99         prod2=mod(prod2b*tensmall,p);
100
101         prod3a=mod(tbig*Dsmall,p);
102         prod3=mod(prod3a*tensmall,p);
103
104         prod4a=mod(tsmall*Dbig,p);
105         prod4=mod(prod4a*tensmall,p);
106
107         t=mod(prod1+prod2+prod3+prod4,p);
108     else
109         t=mod(D(zz)*t,p);
110
111
112     end
113     zz=zz+1;
114 end
115 %Finished calculating  $a^{p-1}=t$ 
116 Power=t;
117 %Calculated  $a^{(N-1)/2} \bmod N$ 
118
119 %Calculate  $(a/N)$ 
120     d=1;
121     b=N;
122     J=1;
123     if mod(b,2)==0
124         d=2;
125     end
126
127     if gcd(a,b) ~= 1
128         d=3;
129     end
130
131     if d==2
132         disp(['Error'])
133     elseif d==3
134         Jacobi=0;
135     else
136
137         aa=a;
138
139         while aa ~= 1
140             aa=mod(aa,b);
141             while mod(aa,2)==0
142                 J=(-1)^(((b^2)-1)/8)*J;
143                 aa=aa/2;
144             end
145             J=(-1)^(((aa-1)*(b-1))/4)*J;
146             A=aa;
147             aa=b;
148             b=A;
149             aa=mod(aa,b);
150
151             if mod(aa+1,b)== 0
152                 J=(-1)^((b-1)/2)*J;
153                 aa=1;
154             end
155         end
156         Jacobi=J;
157
158     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             a=a+1;
180         end
181     else
182         a=a+1;
183     end
184 end
185 if ismember(p,nonprime(:,1))
186 else
187     abspseudo(otherindexing)=p;
188     otherindexing=otherindexing+1;
189 end
190 rangeindex=rangeindex+1;
191 end
192
193 new=size(nonprime,1);
194 i=1;
195 j=1;
196
197 while i<= new
198     if nonprime(i,2)>1
199         careabout(j,:)=nonprime(i,:);
200         j=j+1;
201     end
202     i=i+1;
203 end
204
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);

```

```

4 indexing=1;
5 otherindexing=1;
6 abspseudo(1,:)= [0,0];
7 nonprime(1,:)= [0,0];
8 while rangeindex <= rangemax
9     p=range(rangeindex);
10    p;
11    a=2;
12    terminatetest=0;
13    while terminatetest==0 && a<= p-1
14        %do fermat test
15        greatestcommon = gcd(a,p);
16        if greatestcommon ==1
17            %Find r and odd s with  $N-1=s2^r$ 
18            r=0;
19            N=p;
20            Q=p-1;
21            while mod(Q,2)==0
22                r=r+1;
23                Q=Q/2;
24            end
25            s=(N-1)/(2^r);
26            %Found s and r
27
28
29            %Find Power =  $a^s \bmod N$ 
30
31
32            bin=dec2bin(s);
33            n=numel(num2str(bin));
34            f=1;
35            while f<= n
36                y=num2str(bin);
37                d(f)=str2num(y(n-f+1));
38                f=f+1;
39            end
40            e(1)=a;
41            f=2;
42            while f<= n
43                if e(f-1) >= 10^7
44                    esmall=mod(e(f-1),10^6);
45                    ebig=(e(f-1)-esmall)/10^6;
46
47
48
49                    prod1=mod(esmall*esmall,p);
50
51                    tensmall=mod(10^6,p);
52
53                    prod2a=mod(ebig*ebig,p);
54                    prod2b=mod(prod2a*tensmall,p);
55                    prod2=mod(prod2b*tensmall,p);
56
57                    prod3a=mod(ebig*esmall,p);
58                    prod3=mod(prod3a*tensmall,p);
59
60                    prod4a=mod(esmall*ebig,p);
61                    prod4=mod(prod4a*tensmall,p);
62

```

```

63         e(f)=mod(prod1+prod2+prod3+prod4,p
64         );
65     else
66         e(f)=mod(e(f-1)^2,p);
67     end
68     f=f+1;
69 end
70 h=1;
71 q=1;
72 D=0;
73 while h<=n
74     if d(h)==1
75         D(q)=e(h);
76         q=q+1;
77     else
78     end
79     h=h+1;
80 end
81 ZZ=size(D,2);
82 zz=2;
83 t=D(1);
84 while zz <= ZZ
85     if t*D(zz) >= 10^143
86         tsmall=mod(t,10^6);
87         tbig=(t-tsmall)/10^6;
88         Dsmall=mod(D(zz),10^6);
89         Dbig=(D(zz)-Dsmall)/10^6;
90
91         prod1=mod(tsmall*Dsmall,p);
92
93         tensmall=mod(10^6,p);
94
95         prod2a=mod(tbig*Dbig,p);
96         prod2b=mod(prod2a*tensmall,p);
97         prod2=mod(prod2b*tensmall,p);
98
99         prod3a=mod(tbig*Dsmall,p);
100        prod3=mod(prod3a*tensmall,p);
101
102        prod4a=mod(tsmall*Dbig,p);
103        prod4=mod(prod4a*tensmall,p);
104
105        t=mod(prod1+prod2+prod3+prod4,
106            p);
107    else
108        t=mod(D(zz)*t,p);
109
110    end
111    zz=zz+1;
112 end
113
114 Power=t;
115 if Power == p-1;
116     Power= -1;
117 end
118 %Calculated a^s mod N
119
120

```

```

121 %Calculate X=(a^s,...,a^2^r-1 s)
122
123 i=2;
124 X(1)=Power;
125 while i<= r
126     X(i)=mod((X(i-1))^2,N);
127     if X(i)==N-1;
128         X(i)=-1;
129     end
130     i=i+1;
131
132 end
133 X;
134 %Calculated X
135
136 %Carry out test
137 if X(1)==1
138     a=a+1;
139 elseif all( X ~= -1)
140     nonprime(indexing,:)= [p,a-1];
141     indexing=indexing+1;
142     terminatetest=1;
143 else
144     a=a+1;
145 end
146 %Carried out testr
147
148
149
150
151 %
152
153 else
154     a=a+1;
155 end
156
157 end
158 if ismember(p,nonprime(:,1))
159 else
160     abspseudo(otherindexing)=p;
161     otherindexing=otherindexing+1;
162 end
163 rangeindex=rangeindex+1;
164
165 end
166
167 new=size(nonprime,1);
168 i=1;
169 j=1;
170 while i<= new
171     if nonprime(i,2)>1
172         care(j,:)=nonprime(i,:);
173         j=j+1;
174     end
175     i=i+1;
176 end
177
178 abspseudo
179 care
180 nonprime;

```


