Math 467 Factorization and Primality Testing, Fall 2024, Solutions 8

1. Evaluate the following Legendre symbols (i) $\left(\dfrac{2}{127}\right)_L$, (ii) $\left(\dfrac{-1}{127}\right)_L$, (iii) $\left(\dfrac{5}{127}\right)_L$, (iv) $\left(\dfrac{11}{127}\right)_L$.

(i) $127 \equiv 7 \pmod 8$, so 2 is a QR modulo 127. (ii) $127 \equiv 3 \pmod 4$, so -1 is a QNR modulo 127. (iii) $5 \equiv 1 \pmod 4$ so, by law of QR, $\left(\frac{5}{127}\right)_L = \left(\frac{127}{5}\right)_L = \left(\frac{2}{5}\right)_L = -1$. (iv) $11 \equiv 127 \equiv 3 \pmod 4$ so, by law of QR, $\left(\frac{11}{127}\right)_L = -\left(\frac{127}{11}\right)_L = -\left(\frac{6}{11}\right)_L = 1$.

2. (i) Prove that 3 is a QR modulo p when $p \equiv \pm 1 \pmod{12}$ and is a QNR when $p \equiv \pm 5 \pmod{12}$. (ii) Prove that -3 is a QR modulo p for primes p with $p \equiv 1 \pmod 6$ and is a QNR for primes $p \equiv -1 \pmod 6$. (iii) By considering $4x^2 + 3$ show that there are infinitely many primes in the residue class $1 \pmod 6$.

(i) By law of QR, $\left(\frac{3}{p}\right)_L = (-1)^{\frac{p-1}{2}} \left(\frac{p}{3}\right)_L$. The Legendre symbol here is $\left(\frac{1}{3}\right)_L = 1$ when $p \equiv 1$ or $7 \pmod{12}$ and is -1 otherwise. The desired conclusion follows. (ii) From (i) $\left(\frac{-3}{p}\right)_L = \left(\frac{-1}{p}\right)_L \left(\frac{3}{p}\right)_L = (-1)^{\frac{p-1}{2}} \left(\frac{3}{p}\right)_L = \left(\frac{p}{3}\right)_L$ and this is 1 when $p \equiv 1 \pmod 3$ and -1 otherwise. (iii) Suppose there are only a finite number of such primes, say $p_1, \dots, p_n$ and let $x = p_1 \dots p_n$. Since $x > 0$ and $3 \nmid x$ there is a prime p such that $p | 4x^2 + 3$ and $p > 3$. Hence -3 is a QR modulo p and so by (ii) $p \equiv 1 \pmod 6$. Thus $p|x$ and $p|(4x^2 + 3) - 4x^2 = 3$ which is impossible.

3. (i) Prove that if p is an odd prime a, $b \in \mathbb{Z}$ and $(a, p) = 1$, then $\displaystyle\sum_{n=1}^{p} \left(\frac{an + b}{p}\right)_L = 0$. (ii) Prove that if p is an odd prime, then $\displaystyle\sum_{r=1}^{p-1} \left(\frac{r(r+1)}{p}\right)_L = \sum_{s=1}^{p-1} \left(\frac{1+s}{p}\right)_L = -1$. (iii) Prove that if p is an odd prime, then the number of residues r modulo p for which both r and $r+1$ are quadratic residues is $\dfrac{p - (-1)^{\frac{p-1}{2}}}{4} - 1$. Note that with our definitions 0 is neither a quadratic residue nor a quadratic non–residue.

(i) $an + b$ runs over a complete set of residues modulo p as n does. Hence one of the terms is 0, $(p-1)/2$ are $+1$ and the remainder are -1. (ii) Observe that for every reduced residue class r modulo p there is a unique reduced residue class s_r modulo p such that $rs_r \equiv 1 \pmod p$, and that for every reduced residue class s modulo p one has $s_r \equiv s \pmod p$ for some r. Then the first equality is immediate. The second follows as *per* part (i). (iii) The number in question is $\sum_{r=1}^{p-2} \frac{1}{2}\left(1 + \left(\frac{r}{p}\right)_L\right) \frac{1}{2}\left(1 + \left(\frac{r+1}{p}\right)_L\right) = \frac{p-2}{4} + \frac{1}{4}\sum_{r=1}^{p-2} \left(\frac{r}{p}\right)_L + \frac{1}{4}\sum_{r=1}^{p-2} \left(\frac{r+1}{p}\right)_L + \frac{1}{4}\sum_{r=1}^{p-2} \left(\frac{r(r+1)}{p}\right)_L$ and the result follows from parts (i) and (ii).

4. Prove that if n is odd and $p|n$, then $\displaystyle\sum_{\substack{m=1 \\ (m,n)=1}}^{n} \left(\frac{m}{p}\right)_L = 0$.

Define k and r so that $n = p^k r$ with $p \nmid r$. Then $rx + p^k y$ forms a reduced set of residues modulo n as x does modulo pk and y does modulo r. Moreover each $x = up + v$ where $0 \le u < p^{k-1}$, $1 \le v \le p-1$ and so $\left(\frac{m}{p}\right)_L = \left(\frac{rv}{p}\right)_L$. Thus the sum equals $\phi(r)p^{k-1} \left(\frac{r}{p}\right)_L \displaystyle\sum_{v=1}^{p-1} \left(\frac{v}{p}\right)_L = 0$.

5. Write computer programs to implement **LJ** and **QC**, and use them to evaluate the Legendre symbols $\left(\dfrac{a}{p}\right)_L$ when $a = 40000000003$ and $a = 400000000031$, and $p = 100000000019$ and $p = 100000000057$, and when it is 1 to solve $x^2 \equiv a \pmod p$.

$x \equiv \pm 64503358650 \pmod{100000000019}$ and $x \equiv \pm 64615316195 \pmod{100000000057}$ are the solutions.

```
lj(m,n)=
{
local(t,l);
m=m%n;
t=1;
while(m,
  while(m%2==0,
    m=m/2;
    if(((n*n-1)/8)%2,t=-t);
    );
  l=m;
  m=n;
  n=l;
  if(((m-1)*(n-1))%8,t=-t);
  m=m%n;
  );
if(n==1,return(t),return(0));
}

modexp(a,v,n)=
{
local(c,b);
c=a;
b=1;
while(v,
  if(v%2,
    b=b*c%n;
  ,);
  v=floor(v/2);
  c=c*c%n;
  );
return(b);
}
```

```
milla(n)=
{
local(a,b,c,f,g,h,m,k,t,u,v);
m=n-1;
k=min(m,floor(2*(log(n))^2));
t=0;
u=m;
while(u%2==0,
  u=u/2;
  t=t+1;
  );
o=0;
for(a=2,k,
  c=a;
  v=u;
  b=1;
  f=0;
  while(v,
    if(v%2,
      b=b*c%n;
    ,);
    v=floor(v/2);
    c=c*c%n;
    );
  if(b-1,,
    next;
    );
  for(h=0,t-1,
    if((b+1)%n,,
      f=1;
      );
    b=b*b%n
    );
  if(f,,
    print(n" is composite.");
    print(a" is a witness.");
    o=1;
    return(1);
    break(2);
  );
);
if(o,,
  print(n" is prime.");
  return(0);
  );
}

qc(a,p)=
{
local(b,c,d,f,g,m,q,r,s,t,u,v,w,y,z);
z=milla(p);
if(z,
  print(p" is not prime");
  return(0);
  break);
q=lj(a,p);
if(q==1,,
  print(a" not a QR modulo "p".");
  break;
  );
r=p%8;
w=(p+1)%4;
if(r==1,
  z=1;
  b=2;
  while(z,
    c=lj(b,p);
    if(c==-1,z=0,b=b+1);
    );
  u=(p-1)/8;
  s=3;
  v=u%2;
  while(v==0,
    s=s+1;
    u=u/2;
    v=u%2;
  );
  d=modexp(a,u,p);
  f=modexp(b,u,p);
  m=0;
  for(i=0,s-1,
    z=modexp(f,m,p);
    z=(d*z)%p;
    t=2^(s-1-i);
    g=modexp(z,t,p);
    if((g+1)==p,m=m+2^i);
    );
  v=(u+1)/2;
  y=modexp(a,v,p);
  m=m/2;
  z=modexp(f,m,p);
  x=(y*z)%p;
  ,
  if(w==0,
    x=modexp(a,(p+1)/4,p);
    ,
    y=modexp(a,(p+3)/8,p);
    b=(y*y)%p;
    c=a%p;
    if(c==b,
      x=y;
      ,
      z=modexp(2,(p-1)/4,p);
      x=(y*z)%p;
      );
    );
  );
return(x);
}
```