LISTING *FUNCTION* ARITMETIKA MODULO

Nama File	Kode Program

eccfadd.m	function addp=eccfadd(a,b,p)
	a=mod(a,p);
	b=mod(b,p);
	addp=mod(a+b,p);

eccnaf.m	function u=eccnaf(k)
	u=0;
	c=k;
	l=0;
	while(c>0)
	  if (mod(c,2)~=0)
	  u(l+1)=2-(mod(c,4));
	  c=c-u(l+1);
	  else
	  u(l+1)=0;
	  end
	  c=c/2;
	  l=l+1;
	end

eccfkali.m	function ka=eccfkali(k,a,p)
	if (k<0)
	  k=mod(k,p);
	end
	u=eccnaf(k);
	ka=0;
	for j=length(u):-1:1
	  ka=eccfadd(ka,ka,p);
	  if(u(j)==1)
	  ka=eccfadd(ka,a,p);
	  elseif (u(j)==-1)
	  nega=mod(-a,p);
	  ka=eccfadd(ka,nega,p);
	  end
	end

eccfinv.m	function invc=eccfinv(c,p)
	c=mod(c,p);
	a=[1 0 p];
	b=[0 1 c];
	ulang=1;
	while (ulang==1)
	  if (b(3)==0)
	  invc=[]; ulang=0;
	  break;
	  end

LANJUTAN LISTING *FUNCTION* ARITMETIKA MODULO

Nama File	Kode Program

eccfinv.m	if (b(3)==1)
	invc=mod(b(2),p);
	ulang=0;
	break;
	end
	if (ulang~=0)
	q=floor(a(3)/b(3));
	t=[a(1)-q*b(1) a(2)-q*b(2) a(3)-q*b(3)];
	a=b;
	b=t;
	end
	end

eccfbagi.m	function bagi=eccfbagi(a,b,p)
	invb=eccfinv(b,p);
	bagi=eccfkali(a,invb,p);

eccfpangkat.m	function ak=eccfpangkat(a,k,p)
	a=mod(a,p);
	if(k<0)
	ku=-k;
	else
	ku=k;
	end
	if(a==0)
	ak=0;
	elseif (k==0)
	ak=1;
	else
	u=eccnaf(ku);
	ak=1;
	for j=length(u):-1:1
	ak=eccfkali(ak,ak,p);
	if(u(j)==1)
	ak=eccfkali(ak,a,p);
	elseif (u(j)==-1)
	nega=eccfinv(a,p);
	ak=eccfkali(ak,nega,p);
	end
	end
	if (k<0)
	ak=eccfinv(ak,p);
	end
	end

LANJUTAN LISTING *FUNCTION* ARITMETIKA MODULO

Nama File	Kode Program

eccfakar.m	function akar=eccfakar(z,p)
	if (eccfpangkat(z,(p-1)/2,p)==1)
	  if (mod(p,4)==3)
	  y=eccfpangkat(z,(p+1)/4,p);
	  elseif (mod(p,4)==1)
	  maxs=1;
	  while (2^maxs <= p-1)
	  maxs=maxs+1;
	  end
	  for s=maxs-1:-1:2
	  for t=1:2:p-1
	  qm1=eccfpangkat(2,s,p);
	  qmin1=eccfkali(qm1,t,p);
	  if ((qmin1==p-1) & (mod(t,2)~=0))
	  break;
	  end
	  end
	  end
	  for u=1:1:p-1
	  fu=eccfpangkat(u,(p-1)/2,p);
	  if (fu==mod(-1,p))
	  break;
	  end
	  end
	  v=eccfpangkat(u,t,p);
	  soly=eccfpangkat(z,(t+1)/2,p);
	  zt=eccfpangkat(z,t,p);
	  ulang=1;
	  l=0;
	  while(ulang==1)
	  l=l+1;
	  v2l=eccfpangkat(v,2*l,p);
	  if (v2l==zt)
	  break;
	  end
	  end
	  vpl=eccfpangkat(v,l,p);
	  y=eccfbagi(soly,vpl,p);
	  end
	  akary1=y;
	  akary2=mod(-y,p);
	  akar=[akary1 akary2];
	elseif (z==0)

LANJUTAN LISTING *FUNCTION* ARITMETIKA MODULO

Nama File	Kode Program

eccfakar.m	akar=0;
	else
	akar=[];
	end