LISTING *FUNCTION* ARITMETIKA KURVA ELLIPTIK

Nama File	Kode Program

eccfy2.m	function sqry=eccfy2(p,A,B,x)
	y1=eccfpangkat(x,3,p);
	y21=eccfkali(A,x,p);
	y2=eccfadd(y1,y21,p);
	sqry=eccfadd(y2,B,p);

eccadd.m	function R=eccadd(p,A,PP,PQ)
	if ((PP=='O') | (PP=='o'))
	  R=PQ;
	elseif ((PQ=='O') | (PQ=='o'))
	  R=PP;
	elseif ((PP(1)==PQ(1)) & (PQ(2)==mod(-PP(2),p)))
	  R='O';
	elseif ((PP(1)==PQ(1)) & (PP(2)==PQ(2)))
	  d11=eccfkali(PP(1),PP(1),p);
	  d12=eccfkali(3,d11,p);
	  d1=eccfadd(d12,A,p);
	  d2=eccfkali(2,PQ(2),p);
	  d=eccfbagi(d1,d2,p);
	  xr1=eccfkali(d,d,p);
	  xr2=mod(xr1-PP(1),p);
	  xr=mod(xr2-PQ(1),p);
	  yr1=mod(PP(1)-xr,p);
	  yr2=eccfkali(d,yr1,p);
	  yr=mod(yr2-PP(2),p);
	  R(1)=xr;
	  R(2)=yr;
	else
	  d1=mod(PQ(2)-PP(2),p);
	  d2=mod(PQ(1)-PP(1),p);
	  d=eccfbagi(d1,d2,p);
	  xr1=eccfkali(d,d,p);
	  xr2=mod(xr1-PP(1),p);
	  xr=mod(xr2-PQ(1),p);
	  yr1=mod(PP(1)-xr,p);
	  yr2=eccfkali(d,yr1,p);
	  yr=mod(yr2-PP(2),p);
	  R(1)=xr;
	  R(2)=yr;
	end

eccneg.m	function negP=eccneg(p,PP)
	if ((PP~='O') & (PP~='o'))
	  negP(1)=PP(1);

LANJUTAN LISTING *FUNCTION* ARITMETIKA KURVA ELLIPTIK

Nama File	Kode Program

eccneg.m	negP(2)=mod(-PP(2),p);
	else
	negP='O';
	end

eccsub.m	function S=eccsub(p,A,PP,PQ) negPQ=eccneg(p,PQ); S=eccadd(p,A,PP,negPQ);

eccaddsub.m	function R=eccaddsub(p,A,k,PP)
	u=eccnaf(k);
	R='O';
	for j=length(u):-1:1
	R=eccadd(p,A,R,R);
	if(u(j)==1)
	R=eccadd(p,A,R,PP);
	elseif (u(j)==-1)
	negP=eccneg(p,PP);
	R=eccadd(p,A,R,negP);
	end
	end