Document: /home/jose/Criptografia/elipticas/cproyec.tex - Kile

File Edit View Build Project LaTeX Wizard Bookmarks Tools Settings Help

section | label | normalsize | left (| right)

/jose/Criptografia/elipticas/

- completos
- cproyec.tex
- curva.tex
- equiv.tex
- fschoof.tex
- grupo.tex
- id.tex
- index.tex
- kfinit.tex
- logelip.tex
- mismo.tex
- multiplos.tex
- opuesto.tex
- sistemas.tex
- suma.tex
- testprim.tex

ISO 8859-15

cproyec.tex

```
%
% CALCULOS EN COORDENADAS PROYECTIVAS
%

\subsection{C\'aculos en Coordenadas Proyectivas}\label{sec:Proyectivas}

Uno de los mayores inconvenientes que tiene la suma de puntos en curvas el\'{\i}pticas es el calculo de
inversos modulares, el cual requiere m\'as tiempo de computo que las sumas y multiplicaciones modulares.
\emph{Chudnovsky} y \emph{Chudnovsky} propusieron un m\'etodo para sumar puntos de curvas el\'{\i}pticas,
sin necesidad de realizar inversiones modulares, mediante coordenadas proyectivas.\\

Lo primero que tenemos que hacer es transformar la ecuaci\'on que define la curva el\'{\i}ptica mediante el
cambio de las coordenadas afines $(x,y)$ a las coordenadas proyectivas $(x',y',z')$ definido por:
\begin{displaymath}
(x,y) \longmapsto (x',y')=(x'/z'^2,y'/z'^3)
\end{displaymath}
con $z'\in \mathbb{F}_q$. La ecuaci\'on de la curva en coordenadas proyectivas ser\'a:
\begin{displaymath}
y'^2=x'^3+a\cdot z'^4\cdot x' +b\cdot z'^6
\end{displaymath}

Tenemos que cada punto $(x,y)$ de la curva original, en coordenadas afines, tiene m\'ultiples
representaciones en coordenadas proyectivas $(x',y',z')$ dependiendo del valor que tome $z'$. Una
representaci\'on trivial del punto $(x,y)$, en coordenadas afines, a coordenadas proyectivas es $(x,y,1)$.
Cada punto en coordenadas proyectivas s\'olo tiene una \'unica representaci\'on en coordenadas afines.\\

Sean $P_1=(x_1,y_1)$, $P_2=(x_2,y_2)$ dos puntos de la curva en coordenadas afines y sea $P_3=(x_3,y_3)$ su
suma en coordenadas afines tambi\'en. Sean $P_1'=(x_1',y_1',z_1')$ y $P_2=(x_2',y_2',z_2')$ dos de las
```

Log & Messages | Output | Konsole

Normal mode | Line: 1 Col: 1 INS NORM