Segunda parte de la tarea Examen.

Sea Y^2 = X^3 + X + 1 (i.e. a=b=1) sobre **Z_{30677}** y observe que **P=(1090,18593)** es un punto racional. Encuentre su orden **n** (hint: n es primo) y suponiendo **d=123**, encuentre la llave publica **Q=d*P**. Siguiendo el **ECDSA**, y suponiendo que **k=555**, encontrar la **r** y la **s** de la firma del archivo "**Documento**". Tambien encontrar **w**, **u1**, **u2**, **u1*P** y **u2*Q**. Como algoritmo de digestion, para este problema, use el siguiente algoritmo chafa:

```
int SHAfa(archivo)
char *archivo;
{
	FILE *fpe;
	unsigned char text, suma[2]={0,0};

	if((fpe = fopen(archivo,"r"))==NULL) {
	   printf("Error: no puedo abrir %s\n",archivo);
	   exit(1);
	}
	while(1) {
	   if(fread(&text,1,1,fpe)!=1) break;
	   suma[0]+=text;
	   if(fread(&text,1,1,fpe)!=1) break;
	   suma[1]+=text;
	}
	fclose(fpe);
	suma[0]*=suma[1];
	suma[1]*=suma[0];
	printf("%d %d\n",suma[1],suma[0]);
	return(256*suma[1]+suma[0]);
```

```
}
```