ELEMENTARY NUMBER THEORY

HOMEWORK 6

(1) Use the Euclidean algorithm in $\mathbb{Z}[i]$ to compute $\gcd(7-6i, 3-14*i)$. (Hint: look at how we proved that $\mathbb{Z}[i]$ is Euclidean).

(2) Find the prime factorization of $-3+24i$. (Hint: first factor the norm).

(3) Solve the congruence $x^2 \equiv -1 \bmod 41$ and then compute $\gcd(x+i, 41)$ in $\mathbb{Z}[i]$. Show that this compuation gives us a presentation of 41 as a sum of two squares.

(4) Compute the Legendre symbols $(\frac{1+2i}{1+6i})$ and $(\frac{1+6i}{1+2i})$ in $\mathbb{Z}[i]$.

(5) Compute the Legendre symbols $(\frac{X+1}{X^2+1})$ and $(\frac{X^2+1}{X+1})$ in $\mathbb{F}_7[X]$. Show more generally that $(\frac{X^2+1}{X+1}) = (\frac{2}{p})$ in $\mathbb{F}_p[X]$, where the Legendre symbol on the right is the one in $\mathbb{Z}$.

(6) Let $f \in \mathbb{F}_p[X]$ be a monic polynomial. Find a necessary condition for f to be a sum of two squares ($f = g^2 + h^2$ for $g, h \in \mathbb{F}_p[X]$). Verify for some examples that this condition is also sufficient, and state a precise conjecture.