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).

We have to find $q, r \in \mathbb{Z}[i]$ with $3-14i = (7-6i)q + r$ and $Nr < N(7+6i) = 85$. To this end, write the equation in the form $\frac{3-14i}{7-6i} - q = \frac{r}{7-6i}$; now we have to find q in such a way that $N\frac{r}{7-6i} < 1$ (We can do this because the norm is multiplicative). Now $\frac{3-14i}{7-6i} = \frac{(3-14i)(7+6i)}{(7-6i)(7+6i)} = \frac{105-80i}{85} = \frac{21}{17} - \frac{16}{17}i$. The Gaussian integer nearest to this number is $1-i$, hence $r = (3-14i) - (7-6i)(1-i) = 2-i$.

The next step is $7-6i = (2-i)q + r$. Here we find $q = (5-i)$ and $r = 0$, hence $\gcd(3-14i, 7-6i) = 2-i$, the last nonzero remainder. Note that the gcd is only determined up to units, so if your calculations give $(2-i)i = 1+2i$ etc., the result is correct too.

Note that $3-14i = -(1+2i)(5+4i)$ and $7-6i = -(1+2i)(1+4i)$. Also observe that we can compute a Bezout representation of the gcd; since the Euclidean algorithm is just one line, however, this is quite trivial:

$$2-i = 3-14i - (7-6i)(1-i),$$

or, after multiplying through by i,

$$1+2i = (3-14i)i - (7+6i)(1+i).$$

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

We have $N(-3+24i) = 3^2 + 24^2 = 585 = 3^2 \cdot 5 \cdot 13$. Clearly $-3+24i = 3(-1+8i)$ with $N(-1+8i) = 65 = 5 \cdot 13$. Thus $-1+8i$ must be divisible by one of the two primes $1 \pm 2i$ with norm 5. In fact we find

$$\frac{-1+8i}{1-2i} = \frac{(-1+8i)(1+2i)}{5} = \frac{-17+6i}{5},$$
$$\frac{-1+8i}{1+2i} = \frac{(-1+8i)(1-2i)}{5} = 3+2i.$$

This shows that $-1+8i = (1+2i)(3+2i)$, hence

$$-3+24i = 3(1+2i)(3+2i).$$

(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.

We have $-1+41 = 40$ and $-1+2\cdot 41 = 81 = 9^2$, hence $9^2 \equiv -1 \bmod 41$.

Next $\frac{41}{9+i} = \frac{9}{2} - \frac{1}{2}i$, and there are several choices for "nearest Gaussian integer"; each of them will work, so let us take $q = 4 + 0i$. We find $41 -$

$(9+i)4 = 5-4i$. Next $\frac{9+i}{5-4i} = 1+i$, so $\gcd(41, 9+i) = 5-4i$, and in fact $41 = 5^2 + 4^2$.

This is (after a few modifications) one of the fastest algorithms for computing the representation of large primes $p \equiv 1 \mod 4$ as a sum of two squares.

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

Euler's criterium: $(1+6i)^{(N(1+2i)-1)/2} = (1+6i)^2 \equiv -35+12i \equiv 2i \equiv -1 \mod (1+2i)$ Here we have reduced modulo $5 = N(1+2i)$ and then modulo $1+2i$. Thus $(\frac{1+6i}{1+2i}) = -1$.

Reduction: $(\frac{1+6i}{1+2i}) = (\frac{-2}{1+2i})$ and $-2^2 \equiv 4 \equiv -1 \mod (1+2i)$ gives the same result. Here we have used that $1+6i \equiv -2 \mod (1+2i)$.

We also could use the fact that $-2 = (1+i)^2 i$ and then find $(\frac{1+6i}{1+2i}) = (\frac{-2}{1+2i}) = (\frac{i}{1+2i})$, with $i^2 \equiv -1 \mod (1+2i)$ giving us the known result.

For elements with bigger norms we could also use the reciprocity law.

(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 $\mathbb{Z}$.

Recall that the norm of a prime polynomial of degree n in $\mathbb{F}_p[X]$ is p^n. Before we can apply Euler's criterium we have to check that X^2+1 is irreducible in $\mathbb{F}_7[X]$ (in $\mathbb{F}_5[X]$, we have $X^2+1 = (X+2)(X-2)$, hence $(\frac{X+1}{X^2+1}) = (\frac{X+1}{X-2})(\frac{X+1}{X+2}) = (\frac{3}{5})(\frac{-1}{5}) = -1$ and yet $(X+1)^{12} \equiv 1 \mod X^2+1$.) Over $\mathbb{F}_7$, however, X^2+1 is irreducible because it does not have a root (-1 is a quadratic nonresidue modulo 7).

Thus $(\frac{X+1}{X^2+1}) \equiv (X+1)^{24} \equiv (X^2+2X+1)^{12} \equiv (2X)^{12} \equiv (4X^2)^6 \equiv (-4)^6 \equiv 1 \mod X^2+1$, hence $(\frac{X^2+1}{X+1}) = -1$.

On the other hand, for arbitrary odd primes p we have $(\frac{X^2+1}{X+1}) = (\frac{2}{X+1})$ since $X^2+1 \equiv 2 \mod (X+1)$. Now $(\frac{2}{X+1}) \equiv 2^{(p-1)/2} \equiv (\frac{2}{p}) \mod X+1$. This shows that the two symbols must be equal, since $X+1$ does not divide ± 2.

(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.

Note that sums of two squares in $\mathbb{F}_p[X]$ need not have even degree, as the example $(X+1)^2 + (2X)^2 = 2X+1$ in $\mathbb{F}_5[X]$ shows.

Assume that f is monic and prime. Then $f = A^2 + B^2$ for $A, B \in \mathbb{F}_p[X]$ implies $(A/B)^2 \equiv -1 \mod f$, hence $(\frac{-1}{f}) = +1$.

Is this sufficient? Let us check $\mathbb{F}_3[X]$. If f has degree 1, then $(\frac{-1}{f}) = (\frac{-1}{3}) = -1$. Next $f = X^2+2$ does not seem to be a sum of two squares; but this is because $f = (X-1)(X+1)$ is not irreducible. The irreducible polynomials of degree 2 are X^2+1 and $X^2+X+2 = (X+2)^2 + 1^2$.

In $\mathbb{F}_5[X]$ we have $(\frac{-1}{f}) = (\frac{-1}{5}) = +1$ for all linear polynomials f. In fact we find

$$\begin{aligned} X &= (X-1)^2 + (2X+2)^2, \\ X+1 &= (2X-1)^2 + X^2, \\ X+2 &= (X+1)^2 + (2X+1)^2, \\ X+3 &= (X+2)^2 + (2X-2)^2, \\ X+4 &= (X-2)^2 + (2X)^2. \end{aligned}$$

Thus it seems that f is a sum of two squares if and only if $(\frac{-1}{f}) = +1$ in $\mathbb{F}_p[x]$. I also bet that our proof for the corresponding result in $\mathbb{Z}$ carries over to the situation in $\mathbb{F}_p[x]$. I will check that after this semester.