ELEMENTARY NUMBER THEORY

MIDTERM II

(1) Compute $\gcd(1-4\sqrt{-2}, 4+\sqrt{-2}\,)$ using the Euclidean algorithm, as well as the corresponding Bezout representation.

$$1-4\sqrt{-2} = (4+\sqrt{-2}\,)(-\sqrt{-2}\,)+1.$$

hence $\gcd(1-4\sqrt{-2}, 4+\sqrt{-2}\,) = 1$, and Bezout is trivial. I actually meant to ask $\gcd(1-4\sqrt{-2}, 4-\sqrt{-2}\,)$.

(2) (a) Show that $\alpha^2 \equiv 0,1 \bmod 2$ for every $\alpha \in \mathbb{Z}[\sqrt{-2}\,]$.

Write $\alpha = a+b\sqrt{-2}$. Then $\alpha^2 = a^2-2b^2+2ab\sqrt{-2} \equiv a^2 \equiv 0,1 \bmod 2$. Actually, the calculation shows that $\alpha^2 \equiv a^2-2b^2 \equiv 0, \pm1, 2 \bmod 2\sqrt{-2}$.

(b) Assume that $\pi \in \mathbb{Z}[\sqrt{-2}\,]$ has odd norm and can be written in the form $\pi = \alpha^2+2\beta^2$ for $\alpha, \beta \in \mathbb{Z}[\sqrt{-2}\,]$. Show that $\pi \equiv 1 \bmod 2$.

$\pi \equiv \alpha^2 \equiv 0,1 \bmod 2$, and if $\pi \equiv 0 \bmod 2$ then $N\pi$ would be even.

(c) Show that if $\pi \equiv 1 \bmod 2$, then either $\pi \equiv 1 \bmod 2\sqrt{-2}$ or $-\pi \equiv 1 \bmod 2\sqrt{-2}$.

Write $\pi = a+b\sqrt{-2}$. From $\pi \equiv 1 \bmod 2$ we deduce that a is odd and b is even, hence $\pi \equiv a \bmod 2\sqrt{-2}$. But $a \equiv \pm1 \bmod 4$, hence $\pi \equiv \pm1 \bmod 2\sqrt{-2}$.

(d) Show that every $\pi \in \mathbb{Z}[\sqrt{-2}\,]$ with $\pi \equiv 1 \bmod 2\sqrt{-2}$ can be written in the form $\pi = \alpha^2+2\beta^2$ for $\alpha, \beta \in \mathbb{Z}[\sqrt{-2}\,]$.

We have $\pi = \alpha^2+2\beta^2 = (\alpha+\beta\sqrt{-2}\,)(\alpha-\beta\sqrt{-2}\,)$. Putting $\alpha = \frac{\pi+1}{2}$ and $\beta = \frac{\pi-1}{2\sqrt{-2}}$ solves the problem.

(3) Let $\pi = a+bi$ be a prime in $\mathbb{Z}[i]$ with $N\pi = p \equiv 1 \bmod 4$. Prove that $[\frac{1+2i}{a+bi}] = (\frac{a+2b}{p})$.

We have $a \equiv -bi \bmod \pi$, hence $ai \equiv b \bmod \pi$. Moreover $[\frac{a}{\pi}] = (\frac{a}{p}) = 1$ as usual. Thus $[\frac{1+2i}{a+bi}] = [\frac{a+2ai}{a+bi}] = [\frac{a+2b}{a+bi}] = (\frac{a+2b}{p})$, where the last equality is also proved as usual.

(4) Show that, for $\alpha = a + bi \in \mathbb{Z}[i]$, we have $\alpha \equiv 1 \bmod 2 + 2i$ if and only if $2 \mid b$ and $a + b \equiv 1 \bmod 4$.

$a + bi \equiv 1 \bmod 2 + 2i$ is equivalent to $\frac{a-1+bi}{2+2i}$ being a Gaussian integer. But $\frac{a-1+bi}{2+2i} = \frac{(a-1+bi)((1-i)}{4} = \frac{a-1+b}{4} + \frac{b-a+1}{4}i$. Thus we must have $a + b - 1 \equiv -a + b + 1 \equiv 0 \bmod 4$. Adding gives $2b \equiv 0 \bmod 4$, hence $2 \mid b$.

(5) Assume that $F = A^2 + B^2$ for $A, B, F \in \mathbb{F}_p[X]$, where $p \equiv 3 \bmod 4$. Show that $\deg F$ is even.

Write $A = a_m X^m + \ldots$, $B = b_n X^n + \ldots$. If the degrees are different, say if $m > n$, then $A^2\ B^2 = a_m^2 X^{2m} + \ldots$ has even degree. If $m = n$, then $A^2 + B^2 = (a_m^2 + b_m^2)X^{2m} + \ldots$, and the coefficient $a_m^2 + b_m^2$ is nonzero because otherwise $-1 \equiv (a_m/b_m)^2 \bmod p$, which contradicts the fact that $p \equiv 3 \bmod 4$.

(6) Compute the Jacobi symbol $(\frac{X^3}{X^2+1})$ in $\mathbb{F}_3[X]$.

$(\frac{X^3}{X^2+1}) = (\frac{X}{X^2+1})^3 = (\frac{X}{X^2+1}) \equiv X^4 \equiv 1 \bmod X^2 + 1$, hence $(\frac{X^3}{X^2+1}) = 1$.

(7) Compute an approximation modulo 5^3 of the multiplicative inverse of the 5-adic number $2 + 3 \cdot 5 + 1 \cdot 5^2 + \ldots$.

$(2 + 3 \cdot 5 + 1 \cdot 5^2 + \ldots)(a + 5b + 5^2c + \ldots) = 1$ gives $a = 3$, $2 \cdot 3 + (3 \cdot 3 + 2b)5 \equiv 1 \bmod 5^2$, hence $3 \cdot 3 + 2b \equiv -1 \bmod 5$ and therefore $b = 0$; finally $(2+3\cdot5+1\cdot5^2+\ldots)(3+5^2c+\ldots) = 1$ shows $6+9\cdot5+(3+2c)\cdot5^2 \equiv 1 \bmod 5^3$, hence $3 + 2c \equiv -2 \bmod 5$ and $c = 0$.

In fact, $3(2+3\cdot5+1\cdot5^2+\ldots) = 6+9\cdot5+3\cdot5^2+\ldots = 1+10\cdot5+3\cdot5^2+\ldots = 1 + 0 \cdot 5 + 5 \cdot 5^2 + \ldots = 1 + 0 \cdot 5 + 0 \cdot 5^2 + \ldots$.

(8) Show that $\frac{1}{2} \in \mathbb{Z}_5$, and give an approximation modulo 5^3 of this 5-adic integer.

$\frac{1}{2} = \frac{2}{4} = -2\frac{1}{1-5}$, and $\frac{1}{1-5} = 1 + 5 + 5^2 + 5^3 + \ldots$, so $\frac{1}{2} \in \mathbb{Z}_5$. For the approximation, observe that $-2(1 + 5 + 5^2 + \ldots) = -2 - 2 \cdot 5 - 2 \cdot 5^2 + \ldots = 3 - 3 \cdot 5 - 2 \cdot 5^2 + \ldots = 3 + 2 \cdot 5 - 3 \cdot 5^2 + \ldots = 3 + 2 \cdot 5 + 2 \cdot 5^2 + \ldots$, hence $\frac{1}{2} \equiv 3 + 2 \cdot 5 + 2 \cdot 5^2 \bmod 5^3$.

Or: $\frac{1}{2} \equiv \frac{1}{2}(1 + 5^3) = 63 \bmod 5^3$.