ELEMENTARY NUMBER THEORY

MIDTERM II

NAME: ....

problem	1	2	3	4	5	6	7	8
points to earn	15	20	10	10	15	10	10	10
points earned								

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

(2) (a) Show that $\alpha^2 \equiv 0, 1 \bmod 2$ for every $\alpha \in \mathbb{Z}[\sqrt{-2}\,]$.
(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 $\pi \equiv 1 \bmod 2$.
(c) Show that if $\pi \equiv 1 \bmod 2$, then either $\pi \equiv 1 \bmod 2\sqrt{-2}$ or $-\pi \equiv 1 \bmod 2\sqrt{-2}$.
(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 $\alpha, \beta \in \mathbb{Z}[\sqrt{-2}\,]$.

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

(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 $a + b \equiv 1 \bmod 4$.

(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.

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

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

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