ELEMENTARY NUMBER THEORY

MIDTERM II

(1) Compute $\gcd(9+i, 5+3i)$ using the Euclidean algorithm, as well as the corresponding Bezout representation.

$$\begin{aligned} 9+i &= (5+3i)(1-i) + (1+3i) \\ 5+3i &= (1+3i)(1-i) + 1 + i \\ 1+3i &= (1+i)(2+i) \end{aligned}$$

Thus $\gcd(9+i, 5+3i) = 1+i$. To find the Bezout representation, we compute

$$\begin{aligned} 1+i &= 5+3i - (1+3i)(1-i) \\ &= 5+3i - (9+i-(5+3i)(1-i))(1-i) \\ &= (5+3i)(1-2i) - (9+i)(1-i). \end{aligned}$$

Thus $1+i = (5+3i)(1-2i) - (9+i)(1-i)$.

(2) (a) Show that $\{0, 1, i, 1+i\}$ is a complete system of residue classes modulo 2 in $\mathbb{Z}[i]$.

Let $\alpha = a+bi$. Reduction modulo 2 shows that $\alpha \equiv 0, 1, i, 1+i \bmod 2$. Moreover, none of these residue classes are equal since their differences 1, i, $1+i$ are not divisible by 2.

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

The squares of the residue classes $0, 1, i, 1+i \bmod 2$ are 0 or 1 mod 2. Or directly: $(a+bi)^2 = a^2 - b^2 + 2abi \equiv a^2 - b^2 \equiv 0, 1 \bmod 2$.

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

We have $\pi = \alpha^2 + \beta^2 \equiv 0, 1, 2 \bmod 4$; since $N\pi$ is odd, we must have $\pi \equiv 1 \bmod 2$.

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

We have $\pi = \alpha^2 + \beta^2 = (\alpha + i\beta)(\alpha - i\beta)$. From $\alpha + i\beta = \pi$ and $\alpha - i\beta = 1$ we get $\alpha = \frac{\pi+1}{2}$ and $\beta = \frac{\pi-1}{2i}$, and since $\pi \equiv 1 \bmod 2$ these are Gaussian integers.

(e) Write $1+4i$ as a sum of two squares in $\mathbb{Z}[i]$.

$1+4i = (1+2i)^2 + 2^2$.

(3) Compute the quadratic residue symbols $[\frac{1+i}{1+2i}]$ and $[\frac{1+i}{1+4i}]$ using Euler's criterium.

$[\frac{1+i}{1+2i}] \equiv (1+i)^2 = 2i \equiv -1 \bmod 1+2i$, hence $[\frac{1+i}{1+2i}] = -1$.
$[\frac{1+i}{1+4i}] \equiv (1+i)^8 = (2i)^4 \equiv 2^4 \equiv -1 \bmod 1+4i$, hence $[\frac{1+i}{1+4i}] = -1$.
This agrees with the next exercise: $[\frac{1+i}{1+2i}] = (\frac{2}{3}) = -1$, $[\frac{1+i}{1+4i}] = (\frac{2}{5}) = -1$.

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

Hints:

(a) Prove that $[\frac{m}{\pi}] = (\frac{m}{p})$, where $p = N\pi = a^2+b^2$ and where m is an odd integer not divisible by p. We have $[\frac{m}{\pi}] \equiv m^{(N\pi-1)/2} = m^{(p-1)/2} \bmod \pi$ and $(\frac{m}{p}) \equiv m^{(p-1)/2} \bmod p$. Since p is a multiple of π, we conclude that $[\frac{m}{\pi}] \equiv (\frac{m}{p}) \bmod \pi$. Thus π divides the difference, and this implies that the symbols are equal.

(b) Prove that $[\frac{a}{\pi}] = 1$. $[\frac{a}{\pi}] = (\frac{a}{p}) = (\frac{p}{a}) = 1$ since $p \equiv 1 \bmod 4$ and $p = a^2 + b^2 \equiv b^2 \bmod p$.

(c) Prove that $ai \equiv b \bmod \pi$. Multiply $a \equiv -bi \bmod \pi$ by i.

(d) Use b) and c) to prove that $[\frac{1+i}{a+bi}] = [\frac{a+b}{a+bi}]$. $[\frac{1+i}{a+bi}] = [\frac{a+ai}{a+bi}] = [\frac{a+b}{a+bi}]$.

(e) Complete the proof by evaluating the last symbol. $[\frac{a+b}{a+bi}] = (\frac{a+b}{p}) = (\frac{p}{a+b})$. Now $p = a^2+b^2 \equiv a^2+b^2+(a^2-b^2) = 2a^2 \bmod (a+b)$, hence $(\frac{p}{a+b}) = (\frac{2a^2}{a+b}) = (\frac{2}{a+b})$.

(5) Find all monic irreducible polynomials of the form $X^3 + aX^2 + 1$ in $\mathbb{F}_3[X]$.

We have $f(0) = 1$, $f(1) = a-1$ and $f(2) = a$ in $\mathbb{F}_3$. Now f is irreducible if and only if it does not have a root, that is, if and only if $a \neq 0$ and $a \neq 1$. Thus $X^3 + 2X^2 + 1$ is the only irreducible polynomial of the form $X^3 + aX^2 + 1$ in $\mathbb{F}_3[X]$.

(6) Find the prime factorization of $X^4 + 1$ in $\mathbb{F}_5[X]$.

$X^4 + 1 = X^4 - 4 = (X^2+2)(X^2-2)$, and both factors are irreducible since $a^2 \pm 2 \not\equiv 0 \bmod 5$.

(7) Show that $P = X^2 + 1$ and $Q = X^3 - X + 1$ are irreducible in $\mathbb{F}_3[X]$, and compute the quadratic residue symbols $(\frac{P}{Q})$ and $(\frac{Q}{P})$.

$P(0) = 1$, $P(\pm 1) = 2$, hence P is irreducible. Similarly, $Q(0) = Q(1) = Q(2) = 1$.

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

Using quadratic reciprocity, we also find $(\frac{P}{Q}) = -1$. The direct calculation goes like this: $(\frac{P}{Q}) \equiv (X^2 + 1)^{13} \bmod Q$. Now $P^3 = (X^2 + 1)^3 = X^6 + 1 \equiv (X - 1)^2 + 1 = X^2 + X - 1 \bmod Q$ since $X^3 \equiv X - 1 \bmod Q$. Next $P^6 \equiv (X^2 + X - 1)^2 = X^4 + 2X^3 - X^2 - 2X + 1 \equiv -X - 1 \bmod Q$, hence $P^{12} \equiv X^2 + 2X + 1 \bmod Q$ and $P^{13} \equiv (X^2 + 2X + 1)(X^2 + 1) \equiv -1 \bmod Q$.

(8) Show that $X^2 + X + 1 = 0$ does not have a solution in $\mathbb{Z}_5$. How many different solutions does $X^2 + X + 1 = 0$ have in $\mathbb{Z}_7$? Find the approximation modulo 7^2 to one of them.

Assume that $x \in \mathbb{Z}_5$ satisfies $x^2 + x + 1 = 0$. Then there is an integer a with $x \equiv a \bmod 5$ and $a^2 + a + 1 \equiv 0 \bmod 5$. This congruence does not have a solution, hence there is no such 5-adic number.

Playing the same game in $\mathbb{Z}_7$ we see that there should be two 7-adic numbers x with $x^2 + x + 1 = 0$, one with $x \equiv 2 \bmod 7$ and one with $x \equiv 4 \bmod 7$. Using induction it can be proved that both lift to solutions in $\mathbb{Z}_7$. For finding approximations modulo 7^2, put $z = 2 + 7y$; then $0 \equiv z^2 + z + 1 \equiv 7 + 35a \bmod 7^2$ gives $1 + 5a \equiv 0 \bmod 7$ and $a = 4$. Thus the desired approximation of z is $z \equiv 2 + 4 \cdot 7 \bmod 7^2$.