ELEMENTARY NUMBER THEORY

(1) Assume that $p \equiv 1 \bmod 8$ is a prime, and that $p = c^2 + 2d^2$. Show that $(\frac{c}{p}) = (\frac{2}{c})$. Also show that $(\frac{d}{p}) = 1$ (note that d is even, so you cannot simply invert without thinking!)

Hint: write $d = 2^j u$ for some odd integer u and compute the factors $(2/p)^j$ and (u/p) individually.

(2) Find infinitely many solutions of the diophantine equation $x^2 + y^2 = z^3$.

Hint: find Gaussian integers $x + yi$ that are cubes.

(3) Find infinitely many solutions of the diophantine equation $x^2 + 2y^2 = z^3$.

(4) Find the prime factorizations of $X^3 + X + 1$ and $X^3 - X + 1$ in $\mathbb{F}_3[X]$. Hint: linear factors can be detected by finding roots.

(5) Compute $\gcd(-2+3\sqrt{-2}, 1+4\sqrt{-2}\,)$ using Euclid's algorithm, and compute the corresponding Bezout representation.

(6) For the following equations in $\mathbb{Z}_p$, either explain why they do not have a solution, or find approximations modulo p and p^2.

- $x^2 = 2$ in $\mathbb{Z}_5$;
- $x^2 = 2$ in $\mathbb{Z}_7$;
- $x^3 = 5$ in $\mathbb{Z}_{13}$;
- $x^2 = 2$ in $\mathbb{Z}_2$ (attention: this one has a solution modulo 2, but not modulo 4);
- $x^3 + x + 1 = 0$ in $\mathbb{Z}_5$;
- $x^3 + x + 1 = 0$ in $\mathbb{Z}_{11}$.

(7) Show that $\{0, \pm 1, \pm i\}$ is a complete system of residues modulo $1 + 2i$.

Hint: first show that every Gaussian integer is congruent modulo $1+2i$ to one of $0, 1, 2, 3, 4$. Then show that each of these is congruent to an element in $\{0, \pm 1, \pm i\}$. Finally show that no two of these elements are congruent modulo $1 + 2i$.

(8) Prove that $[\frac{i}{\pi}] = (-1)^{(p-1)/4}$ for $\pi \in \mathbb{Z}[i]$ with prime norm $N\pi = p$.

(9) Find the prime factorization of $f(X) = X^4 + 3X^2 + 1$ over $\mathbb{F}_5[X]$. Hint: check for linear factors by computing $f(a)$ for $a \in \mathbb{F}_5$; if $f(a) = 0$, then $f(X) = (X - a)g(X)$.

(10) Find the prime factorization of $f(X) = X^4 + X^2 + 1$ over $\mathbb{F}_5[X]$.

Solution: this has no linear factors since $f(a) \neq 0$ for all $a \in \mathbb{F}_5$. Now write $f(X) = (X^2+aX+b)(X^2+cX+d)$. Comparing the coefficients of X^3 shows $a+c = 0$, hence $f(X) = (X^2+aX+b)(X^2-aX+d)$. Comparing the linear terms gives $a(d-b) = 0$. If $a = 0$, then $b+d = 1$ and $bd = 1$ in $\mathbb{F}_5$; thus $1 = bd = b(1-b) = b - b^2$: but this has no solution in $\mathbb{F}_5$. Thus $a \neq 0$ and $b = d$, that is, $f(X) = (X^2+aX+b)(X^2-aX+b) = X^4+(2b-a^2)X^2+b^2$. This implies $b = 1$ and $a = \pm 1$, hence $f(X) = (X^2 + X + 1)(X^2 - X + 1)$.

This is even true over any field (not just $\mathbb{F}_5$), and could have been derived directly from the fact that f is a difference of squares: $f(X) = (X^2+1)^2 - X^2$.

(11) Factor $X^4 - X^3 - X^2 - X + 1$ over $\mathbb{F}_3[X]$.