

MATH 5405 - HW2

DUE 02/09/2009

- 1) Since $-1 = 2$ is not a square modulo 3, we can write \mathbb{F}_9 as $\mathbb{F}_3[i]$ where $i^2 = -1$. Write down the multiplication table for 8 non-zero elements in $\mathbb{F}_3[i]$. (For convenience write these elements as $a+bi$ where a, b are $-1, 0, 1$.)
- 2) Since the order of \mathbb{F}_9^\times is 8 and $\varphi(8) = 4$, four elements in $\mathbb{F}_3[i]^\times$ should be primitive, that is of order 8. Find them.
- 3) Complete the multiplication table for the field \mathbb{F}_8 realized as polynomials in $\mathbb{F}_2[x]$ modulo $x^3 + x + 1$.
- 4) Show that the polynomial $x^4 + x^3 + x^2 + x + 1$ cannot be factored into two degree 2 polynomials
$$x^4 + x^3 + x^2 + x + 1 = (x^2 + ax + b)(x^2 + cx + d)$$
in $\mathbb{F}_2[x]$. (This is the hardest part to show that $x^4 + x^3 + x^2 + x + 1$ is irreducible.)
- 5) Does the equation $x^2 - 6x + 11 = 0$ have a solution modulo 131? Hint: complete to a square, then use quadratic reciprocity.
- 6) Use Pepin's test to show that $F_4 = 2^{2^4} + 1$ is prime.
- 7) Let $n \geq 2$. Show that $F_n \equiv 2 \pmod{5}$. In particular, F_n is not a square modulo 5.
- 8) Let p be a prime congruent to 3 modulo 4. Then \mathbb{F}_{p^2} can be realized as the set of elements $x + yi$ where x and y are integers considered modulo p and $i^2 = -1$. Show that i is a square in $T(p)$ if and only if $p \equiv 7 \pmod{8}$.
- 9) Let ℓ be an odd prime such that $M_\ell = 2^\ell - 1$ is a Mersenne prime. Use the quadratic reciprocity to show that 5 is a square modulo M_ℓ if and only if $\ell \equiv 1 \pmod{4}$.
- 10) Let ℓ be an odd prime such that $\ell \equiv 3 \pmod{4}$. Assume that $M_\ell = 2^\ell - 1$ is a Mersenne prime. Then $\alpha = \frac{3}{2} + \frac{1}{2}\sqrt{5}$ is not a square in $T(M_\ell)$.