Math 261 — Fall 2007
Final exam, January 30, 2008. TIME: 2.5 hours
http://people.aub.edu.lb/~kmakdisi/

Instructions: This is a long exam; budget your time wisely. The exam is open book, and calculators are allowed. Please make sure to write your name on your exam booklet(s) and to clearly indicate which problem you are solving on any given page. **There are 110 points total on the exam.**

GOOD LUCK!

1. (5 pts) a) If p is a prime dividing a number m^4+1, show that $p=2$ or $p\equiv 1 \bmod 8$. [Hint: look at the order of m in $(\mathbf{Z}/p\mathbf{Z})^*$.]

(5 pts) b) Deduce that there are infinitely many primes congruent to 1 mod 8. [Modify Euclid's argument.]

2. (10 pts) How many primitive roots are there modulo the prime number 241?

3. (3 pts) a) State without proof the condition for a positive integer n to be a sum of two squares.

(7 pts) b) Show that the equation $x^2+y^2=3(a^2+b^2)$, with $x,y,a,b\in\mathbf{Z}$, has only the trivial solution $x=y=a=b=0$.

4. (10 pts) Find ONE solution to $x^2\equiv 148 \bmod 3^3\cdot 11$.

5. (10 pts) Given that $4+i$ and $3+2i$ are relatively prime in $\mathbf{Z}[i]$, find $\alpha,\beta\in\mathbf{Z}[i]$ such that $(4+i)\alpha+(3+2i)\beta=1$.

6. (15 pts) Let $p\geq 5$ be a prime. Determine (based on the congruence class of p mod m for a suitable m to be determined) how many solutions the following equation has in $\mathbf{Z}/p\mathbf{Z}$:

$$(x^3-1)(x^2+2)\equiv 0 \bmod p.$$

Remark: the condition $p\geq 5$ is there to ensure that the polynomial $(x^3-1)(x^2+2)$ does not have repeated roots. You may use this fact without proof.

7. (5 pts) a) Find the repeating continued fraction of $\sqrt{14}$.

(5 pts) b) List the first few convergents A_n/B_n to $\sqrt{14}$ until you reach one for which you can prove that $\left|A_n/B_n-\sqrt{14}\right|\leq 1/2000$.

(5 pts) c) Find the fundamental unit of $\mathbf{Z}[\sqrt{14}]$.

(5 pts) d) Find two distinct solutions to $x^2-14y^2=11$.

8. (5 pts) a) If p is a prime with $p\neq 2,7$, show that

$$\left(\frac{-28}{p}\right)=\left(\frac{-7}{p}\right)=\left(\frac{p}{7}\right).$$

(5 pts) b) Show that if $p\equiv 1,2,$ or $4 \bmod 7$ then there exists a quadratic form $f(x,y)=px^2+hxy+\ell y^2$ with discriminant -28.

(5 pts) c) Find all the reduced positive definite quadratic forms with discriminant -28.

(5 pts) d) Perform a reduction on the quadratic form $f=79x^2+50xy+8y^2$ (which has discriminant -28) to show that f is equivalent to the quadratic form $g=u^2+7w^2$. Do this while keeping track of the matrix M such that $f*M=g$, and use this to deduce a solution to the equation $79=u_0^2+7w_0^2$.

(5 pts) e) Show that if $p\equiv 1,2,$ or $4 \bmod 7$ then it is possible to write $p=u_0^2+7w_0^2$ for suitable $u_0,w_0\in\mathbf{Z}$. (Include a proof that the reduction of the form f from part b is indeed u^2+7w^2, and not another one of the solutions to part c.)