SOLUTIONS TO QUIZ 2 – ALGEBRA I, MATH235, FALL 2007

(1) 3^{248} is congruent modulo 7 to 2. (Use that $3^6 \equiv 1$, by Fermat, and so $3^{246} = (3^6)^{41} \equiv 1$ modulo 7, etc.)

(2) For which primes $p > 2$ does the equation $x^2 + x + 4$ have a unique solution in $\mathbb{F}_p$? The discriminant is $1 - 4 \cdot 4 = -15$. To have a unique solution the discriminant should be zero and that means that p is either 3 or 5.

(3) The gcd of the polynomials x^2+1 and x^3+2x+2 over the field $\mathbb{F}_5$ is $x+2$. (Just do the Euclidean algorithm: $x^3 + 2x + 2 = x(x^2 + 1) + x + 2, x^2 + 1 = (x - 2)(x + 2)$.)

(4) Let n be a positive integer. The number of solutions of a polynomial of the form $x^2 + ax + b$ in a ring $\mathbb{Z}/n\mathbb{Z}$ could be more than 2. (We've seen such examples when n is not prime.)

(5) Which of the following relations on $\mathbb{C}$ is an equivalence relation? (Circle all correct answers).
(a) $x \sim y$ if $|2x| \geq |y|$.
(b) $x \sim y$ if $Re(x) = Re(y)$.
(c) $x \sim y$ if $x + y = 0$.
(d) $x \sim y$ if $x = y$.
$x \sim y$ if $Re(x) = Re(y)$ and $x \sim y$ if $x = y$ are equivalence relations. For the relation $x \sim y$ if $|2x| \geq |y|$ symmetry fails: $3 \sim 1$ but not $1 \sim 3$. For the relation $x \sim y$ if $x + y = 0$ we don't have reflexive because we don't have $1 \sim 1$. (Other properties fail too in these last examples.)

(6) Which of the following sets is an ideal of the ring $\mathbb{Z}[\sqrt{2}]$? (Circle all the correct answers)
(a) $\{2a + b\sqrt{2} : a, b \in \mathbb{Z}\}$.
(b) $\{a + 2b\sqrt{2} : a, b \in \mathbb{Z}\}$.
(c) $\{5a : a \in \mathbb{Z}\}$.
(d) $\{0\}$.
The sets $\{0\}$ and $\{2a + b\sqrt{2} : a, b \in \mathbb{Z}\}$ are ideals. The other two are not closed under multiplication by $\sqrt{2}$.

(7) The *unique* factorization of $3x^3 + 5x^2 - 6x - 10$ in $\mathbb{Q}[x]$ is $3(x + 5/3)(x^2 - 2)$. (The factorization $3(x + 5/3)(x + \sqrt{2})(x - \sqrt{2})$ is not over $\mathbb{Q}$, the factorization $(3x + 5)(x^2 - 2)$ is not given using monic polynomials and the factorization $3(x - 2)(x + 5/3)(x + 1)$ cannot be correct because -1 is not a root.)

(8) How many irreducible monic quadratic polynomials are there over $\mathbb{F}_p$? The answer is $p(p - 1)/2$. The reason is that any reducible monic polynomial is the product of two linear monic polynomials that may or may not be distinct. There are $\binom{p}{2}$ choices for factorization with different linear terms $+\ p$ for factorization as a square of a linear term. Altogether there are $\binom{p}{2} + p$ reducible monic quadratic polynomials. The number of monic quadratic polynomials is p^2 and $p^2 - (\binom{p}{2} + p) = p(p - 1)/2$.

The proofs requested in Part II were all given in class.