Math 602 Problem Set #8 Due Fri., Nov. 6, 2015

1. Prove, or disprove and salvage: If K is a field, and $f(x) \in K[x]$ has no roots, then $K[x]/(f(x))$ is a field.

2. For each positive integer n, let $U_n = (\mathbb{Z}/n)^\times$, the group of units modulo n. Find a generator of U_{121}, and determine the group structure of U_{27} and U_{21} explicitly. Conjectures? Proofs?

3. a) Define the Euclidean algorithm as follows. Given non-zero integers a and b, write $a = bq_0 + r_0$ as in the division algorithm (i.e. $0 \le r_0 < |b|$); then continue: $b = r_0 q_1 + r_1$, $r_0 = r_1 q_2 + r_2$, $r_1 = r_2 q_3 + r_3$, etc. (with $0 \le r_{i+1} < |r_i|$). Show that eventually some $r_{n+1} = 0$, and that r_n is the g.c.d. of a and b.

b) Use this to find the g.c.d. of 1155 and 651.

c) Verify, in the calculations of part (b), that (in the notation of (a)),

$$\frac{1155}{651} = q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cfrac{1}{\dots + \cfrac{1}{q_{n+1}}}}}.$$

Also verify in these calculations that if we write

$$q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cfrac{1}{\dots + \cfrac{1}{q_n}}}} = \frac{x}{y}$$

in lowest terms, then x, y form a solution to the Diophantine equation $651x - 1155y = d$, where $d = \gcd(1155, 651)$. Can solutions to other equations be found in this way? Explore.

4. Do the analog of problem 3 with $\mathbb{Z}$ replaced by $k[x]$, where k is a field. In parts (b) and (c), replace 1155 and 651 with $x^3 + x^2 + x$ and $x^2 + 1$.

5. a) Show that if $m \in \mathbb{Z}$ and $x^2 - m$ has no root in $\mathbb{Z}$, then $x^2 - m$ has no root in $\mathbb{Q}$. [Hint: Generalize the proof that $\sqrt{2}$ is irrational.]

b) More generally, show that if $a_0, a_1, \dots, a_{n-1} \in \mathbb{Z}$, and if the polynomial $f(x) = x^n + a_{n-1}x^{n-1} + \cdots a_1 x + a_0$ has no root in $\mathbb{Z}$, then it has no root in $\mathbb{Q}$.

c) What if, in part (b), the polynomial $a_n x^n + a_{n-1}x^{n-1} + \cdots a_1 x + a_0$ (for some integers $a_0, a_1, \dots, a_n$) is considered instead?

6. a) Describe the maximal ideals in each of the following rings: $(\mathbb{Z}/2)[x]$, $\mathbb{C}[x, y, z, t]$, $\mathbb{R}[[x]]$, $\mathbb{Z}_{(2)}$, $\mathbb{Z}[1/15]$, $\mathbb{Z}/15$, $\mathbb{C}[x, y]/(y^2 - x^3)$, $\mathbb{R} \times \mathbb{R}$, $\mathbb{C}[x]/(x^2)$, $\mathbb{Q}[i]$, $\mathbb{Q}[\pi]$.

b) Describe all the units in these rings, and also in the rings $\mathbb{Z}[[x]]$, $\mathbb{Z}[i]$, $\mathbb{Z}[x, y]$, and $\mathbb{Z} \times \mathbb{Z}$. Which have only finitely many units?

7. Let p be a prime number and let n be a positive integer such that $p \equiv 1 \pmod{n}$.

a) Show that the map $\phi_n : (\mathbb{Z}/p)^\times \to (\mathbb{Z}/p)^\times$, given by $\phi(x) = x^n$, is exactly n-to-one.

b) Deduce that there are exactly $\frac{p-1}{n}$ elements of $(\mathbb{Z}/p)^\times$ that are nth powers.

c) What happens if instead the congruence hypothesis is dropped?

8. a) Which of the following elements of $\mathbb{Z}[i]$ can be factored non-trivially? For each one that can be, do so explicitly. $2, 3, 5, 7, 11, 13, 15, 3i, 5i, 2 + i, 3 + i$

b) Make a conjecture about which Gaussian integers can be factored non-trivially.