AM 106/206: Applied Algebra **Prof. Salil Vadhan**

Problem Set 8

Assigned: Sun. Nov. 14, 2010 Due: Fri. Nov. 19, 2010 (2:10 PM sharp)

- You may submit your problem sets in the AM106 in the Maxwell–Dworkin basement, or electronically by email to `am106-hw@seas.harvard.edu`. If you use LaTeX, please submit both the source (`.tex`) and the compiled file (`.pdf`). Name your files `PS8-yourlastname`.
- Aim for clarity and conciseness in your solutions, emphasizing the main ideas over low-level details. Justify your answers except when otherwise specified.
- Problems marked [AM106] or [AM106-X] are for AM106 students (though AM206 students should confirm that they know how to do them), and those marked [AM206-X] are for AM206 students. However, AM106 students can do a problem marked [AM206-X] instead of one marked [AM106-X] (for the same value of X) if they wish (out of interest, or for a challenge). If you wish to keep the option of staying in either AM106 or AM206 open until add/drop date, then you should do all problems marked [AM106] and all problems marked [AM206-X].

Problem 1. (Ideals and Factor Rings) For each of the following rings R and subsets $I \subseteq R$, determine whether I is a subring of R and whether I is an ideal of R. If I is an ideal, do the following:

- Find a set of generators for I of minimal size, and determine whether I is principal.
- Determine the factor ring R/I by giving an appropriate homomorphism from R to a familiar ring S.
- Determine whether I is maximal, and if not, find a maximal ideal containing I.

1. $R = \mathbb{Z} \times \mathbb{Z}$, $I = \{(a, b) : a \equiv b \pmod 6\}$.
2. $R = \mathbb{Z}[x]$, $I = \{p(x) : p(3) = 0\}$.
3. $R = \mathbb{R}[x]$, $I = \{p(x) : p(0) = 0 \text{ and } p(7) = 0\}$.
4. $R = \mathbb{R}[x]$, $I = \{p(x) : p(0) = 0 \text{ or } p(7) = 0\}$.
5. $R = \mathbb{C}$, $I = \mathbb{R}$.
6. $R = \mathbb{Q}[x]$, $I = \langle x^3 + x^2 - 2x - 2, x^2 + 2x + 1\rangle$.
7. $R = \mathbb{Z}_{96}$, $I = \{0, 32, 64\}$.

Problem 2. (Frobenius homomorphism, Gallian 15.44+) Let R be a commutative ring with unity and characteristic p, for a prime p.

1. Show that the map $\varphi : x \mapsto x^p$ is a ring homomorphism from R to itself.
2. Show that φ is an automorphism of R (i.e. an isomorphism of R with itself) in case R is a finite field. (Hint: show that in this case, it suffices to prove $\ker(\varphi) = \{0\}$.)
3. Find a ring R of characteristic p such that φ is not an automorphism of R. (Hint: look at infinite R.)

Problem 3. (Computations in $F[x]$ [AM106-A]) Note that the two parts of this problem are over different fields.

1. List all of the monic, irreducible polynomials of degree up to and including 5 over $\mathbb{Z}_2[x]$.
2. Use the polynomial analogue of the Euclidean Algorithm to find a single polynomial $h(x)$ such that the ideal $\langle h(x) \rangle$ equals the ideal $\langle x^6 + 2x^4 + 2x^3 + 2x + 1, x^5 + x^2 + 2x + 1 \rangle$ in $\mathbb{Z}_3[x]$. Show your work.

Problem 4. (Polynomial Factorization [AM206-A]) In this problem, you will see one of the main ideas that go into polynomial-time randomized algorithms for polynomial factorization. Let $\mathbb{F}$ be a finite field of odd order q, and let $p(x) = p_1(x)p_2(x)$, where $p_1(x), p_2(x) \in \mathbb{F}[x]$ are distinct irreducible polynomials of degree n.

1. Show that $\mathbb{F}[x]/\langle p(x) \rangle$ is isomorphic to $\mathbb{F}[x]/\langle p_1(x) \rangle \times \mathbb{F}[x]/\langle p_2(x) \rangle$. What theorem about the integers is this analogous to?
2. Show that if we pick a random polynomial $f(x) \in \mathbb{F}[x]$ of degree smaller than $2n$, then with probability at least $1/2$, either $\gcd(f(x), p(x)) \in \{p_1(x), p_2(x)\}$ or $\gcd(f(x)^{(q^n-1)/2} - 1, p(x)) \in \{p_1(x), p_2(x)\}$. You may use the fact that the group of units in any finite field is cyclic. (Hint: think of $f(x)$ as a random element of $\mathbb{F}[x]/\langle p(x) \rangle$.) Thus we can factor p with high probability by choosing several random f's and computing these gcd's.

Problem 5. (Multivariate polynomials) Let R be a commutative ring with unity. The ring $R[x_1, \ldots, x_n]$ of polynomials over R in indeterminates $x_1, \ldots, x_n$ consists of all expressions of the form $p(x_1, \ldots, x_n) = \sum_{i_1, \ldots, i_n \geq 0} a_{i_1, \ldots, i_n} x_1^{i_1} \cdots x_n^{i_n}$, where $a_{i_1, \ldots, i_n} \in R$, only finitely many of the $a_{i_1, \ldots, i_n}$ are nonzero, and addition and multiplication are defined as usual. The *degree* of such a polynomial p is the maximum of $i_1 + \cdots + i_n$ over all nonzero coefficients $a_{i_1, \ldots, i_n}$.

1. Exhibit a nonzero degree 2 polynomial $p(x_1, x_2) \in \mathbb{Z}[x_1, x_2]$ that has infinitely many zeroes.
2. Despite the above, it can be shown that a low-degree polynomial cannot have too many roots in any finite "cube". Specifically, show that if R is an integral domain, $S \subseteq R$ is finite, and $p(x_1, \ldots, x_n) \in R[x_1, \ldots, x_n]$ is a nonzero polynomial of degree d, then the fraction of points $\alpha = (\alpha_1, \ldots, \alpha_n) \in S^n$ on which $p(\alpha) = 0$ is at most $d/|S|$. (Hint: group terms as $p(x_1, \ldots, x_n) = \sum_i q_i(x_1, \ldots, x_{n-1}) x_n^i$, and use induction on n.) Thus we can test whether a low-degree multivariate polynomial is zero by evaluating it on random points from S^n.
3. Find an ideal in $\mathbb{Q}[x_1, x_2]$ that is not principal.