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

Problem Set 7

Assigned: Wed. Nov. 18, 2009 Due: Wed. Dec. 2, 2009 (1:10 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`.
- Aim for clarity and conciseness in your solutions, emphasizing the main ideas over low-level details.
- If you use LaTeX, please submit both the source (`.tex`) and the compiled file (`.pdf`). Name your files `PS7-yourlastname`.
- AM206 students should do the problems marked [AM206-X], and need not do the ones marked [AM106-X]. AM106 students need not do the problems marked [AM206-X], but may do so in place of the corresponding [AM106-X] problem (but not [AM106-Y] for Y $\neq X$) if desired.

Problem 1. (Factor Rings, and Maximal Ideals) For each of the following rings R and ideals I, determine the factor ring R/I by giving a homomorphism from R onto a familiar ring S with kernel I. Which of the ideals I are maximal? For those that are not maximal, find a maximal ideal containing I.

1. $R = \mathbb{Z} \times \mathbb{Z}$, $I = \{(a, b) : b \text{ even}\}$.
2. $R = \mathbb{Z}_{12}$, $I = \langle 3 \rangle$.
3. $R = \mathbb{Z}[x]$, $I = \{p(x) : p(0) \bmod 10 = 0\}$.
4. $R = \mathbb{Q}[x]$, $I = \{p(x) : p(2) = p(3) = 0\}$.

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])

1. Factor the polynomial $x^5 + 3x^4 + 2x^3 + x^2 + x \in \mathbb{Z}_3[x]$ into irreducible factors.

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 $\langle x^4 + 2x^3 + 3x^2 + 2x + 2, x^3 + x^2 + 1 \rangle$ 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. (Wilson's Theorem, Gallian 16.34)

1. Prove that if $\mathbb{F}$ is a finite field, then the product of all nonzero elements of $\mathbb{F}$ equals -1.

2. Deduce Wilson's Theorem: $(n-1)! \bmod n = n - 1$ if and only if n is prime.

Problem 6. (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.