6.885 Problem Set: Due November 14, 2005

Instructions

- If you are taking the course for credit, you must turn in this problem set.
- You should do this in pairs. If you have trouble finding a partner let me know and I'll help you find one.
- While a pair may ask around for specific questions (or consult the literature), you should try to solve the problem set on your own, to the maximum extent possible. If you do consult others, you *must* list all collaborators and/or sources.
- Coherence and clarity of the writeup are important, so please factor in at least 50% of the time to do the writing. Iterate with your partner on the writing, so that one person goes over the other's writeup and if possible improves on it.
- Answers are due before lecture on Monday, November 14.

Background: Factoring polynomials over the rationals

Recall that our goal is to verify various claims needed to assert the correctness of the following factoring algorithm for polynomials over the rationals.

Given a polynomial $f \in \mathbb{Z}[X]$ of degree at most d and coefficients bounded in magnitude by 2^n, we find a factor of f as follows:

1. Let f' denote the derivative of f. If the greatest common divisor of f and f' is nontrivial, output that factor and stop.
2. Find a prime p such that the gcd of the images of f and f' in $\mathbb{F}_p[X]$ is also trivial.
3. Factor f as $f = gh \pmod{p}$ in $\mathbb{F}_p[X]$, where g and h are monic and relatively prime and g is irreducible in $\mathbb{F}_p[X]$.
4. Use Hensel Lifting to find monic polynomials G and H such that $f = GH \pmod{p^t}$, with $G = g \pmod{p}$, and $H = h \pmod{p}$.
5. Find $\bar{g}$ and $\bar{G}$ of appropriate degree such that $\bar{g}(X) = G(X)\bar{G}(X) \pmod{p^t}$.
6. If $\bar{g}$ and f have a nontrivial gcd, output that gcd; otherwise, output "f is irreducible."

The actual problems

1. **(Resultants of integer polynomials)** Recall that for relatively prime polynomials $f, g \in \mathbb{Z}[X]$, we defined the resultant of f and g to be the smallest positive integer R such that $R = af + bg$, where $a, b \in \mathbb{Z}[X]$.

   Prove that if f and g are of degree at most d, with coefficients in the range $-C, \ldots, +C$, then their resultant is bounded by $O(dC)^{O(d)}$.

   Hint: Proceed as in the proof of the bivariate case, substituting the pigeonhole principle for one of the dimension counting arguments used in the bivariate case.

2. **(Coefficients of factors)** Prove that if $f = gh$ over $\mathbb{Z}[X]$, with the degree of f at most d and the coefficients of f are in the range $-C, \ldots, +C$, then the coefficients of g are bounded by $O(d)^{O(d)} \cdot C$.

3. **(Hensel lifting)** Let $f = g^* h^*$, with g^* being irreducible over the integers. Furthermore, let g^* factor into irreducible polynomials of the form $g(x)g_1(x)\cdots g_k(x) \pmod{p}$. Show that g^* is a candidate polynomial for the $\bar{g}$ of Step 5 of the algorithm.

4. **(Resultants and validity of the solution)** Prove that the g^* of Exercise 3 divides any $\bar{g}$ reported in Step 5 of the algorithm.

5. **(Summary)** Use the above exercise to conclude the correctness of the algorithm above. Among other things, you must bound the running time of the algorithm by some polynomial in n and d.