Computer Science CSC478/2412 | Spring 1997
St. George Campus | University of Toronto

Homework Assignment #5
Due: Friday, 11 April 1997
Mark: 15%

1. Algorithm 8.7 on page 367 works over finite fields with odd (large) characteristic. Using this algorithm, factor the polynomial $f = x^{22} + x + 1$ over $\mathbb{F}_p$ for $p = 2^k - 1$ where $k = 13, 31, 61, 89, 107, 127, 521, 607, 1279$. You may prefer to implement the algorithm instead of using maple procedures for each step (of course, you cannot use the entire algorithm directly from maple). Factor over as many p as possible. [Note that isprime(p) returns true if p is a prime, so you can continue searching for other primes bigger than $2^{1279} - 1$ of the form $2^k - 1$, in case you want to search for even larger fields.]

2. Explain why for any given $0 < \varepsilon < 1$, $t = 2\lceil \log \frac{r^2}{\varepsilon} \rceil$ random choices are sufficient to obtain a complete factorization with probability at least $1 - \varepsilon$, using the equal-degree algorithm taught in the lecture.

[Hint: First compute the probability that a chosen polynomial h separates 2 fixed irreducible factors f_i and f_j. Then, deduce the probability that any pair of irreducible factors be separated in t tries. Finally, the probability of "failure" smaller than ε is equal to the probability of any two factors separated being greater than $1 - \varepsilon$. You may obtain a general result for t depending on q, or take $q = 3$ as a lower bound on q and obtain the desired bound (or a similar, but probably tighter, bound).]

3. Implement the algorithm 10.4 on page 450 to compute reduced Gröbner bases using the orders $<_L$ and $<_D$. Test your algorithm on the polynomials (a) and (b) of Problem 8 on page 467.

References

K.O. Geddes and S.R. Czapor and G. Labahn, *Algorithms for Computer Algebra*, Kluwer Academic Publishers, Boston, 1992.