CZ3106 Symbolic Computing, Tutorial 6

A/P Wang Jian-Sheng week 7-12 Apr 03

1. Solve the following systems of linear equations (by hand) with Chinese remainder theorem (Garner's algorithm) by solving the equations in Z_p for $p = 3, 5, 7, 11$ first, and then reconstruct the solution in Z. Of course the answer may be in Q.

$$2x + 4y - 2z = 1,$$
$$2x + y + z = 3,$$
$$5x - 3y + 7z = 0.$$

An example of similar calculation is given on page 182–183, "Algorithm for Computer Algebra", by Geddes et al.

2. Calculate the square-free factorization (Algorithm 8.1) by hand of

$$a(x) = 1 - 2x + 2x^3 - x^4 \quad \in \mathrm{Z}[x].$$

That is, do arithmetic in Z.

3. Calculate the square-free factorization (Algorithm 8.3) by hand of

$$b(x) = x^{10} + x^6 + x^5 + x^3 + x^2 + 1 \quad \in \mathrm{Z}_2[x].$$

That is, do arithmetic in Z_2.

4. (Optional) Factor the polynomials $a(x)$ and $b(x)$ in $\mathrm{Z}_2[x]$ using Berlekamp's algorithm (by hand). Note that Berlekamp's algorithm works only for square-free polynomials. So we need to do a square-free factorization first.

$$a(x) = x^{15} - 1,$$
$$b(x) = x^{10} + x^6 + x^5 + x^3 + x^2 + 1.$$