Bordeaux 1 University
Mathematics

MHT 933 - master 2
2009-2010

Work on machine

Choose at least one exercise in the following list. The goal of this activity is to produce programs written in Maple that allows to test the algorithms seen in course or in TD, and if possible, to compare them with naive approaches or between themselves.

Exercise 1 – [Product of polynomials (1)]

Karatsuba, Toom-Cook.

Exercise 2 – [Product (2) and division of polynomials]

FFT, Newton.

Exercise 3 – [Naive HNF, SNF]

Do not forget to do several tests leading to observe the uniqueness.

Exercise 4 – [LLL algorithm and diophantine approximation]

Use the elementary LLL seen in course.

Exercise 5 – [Sum of two squares]

Do what have been seen in TD about the decomposition into sum of 2 squares for a prime $p \equiv 1 \bmod 4$ using Euclid's algorithm in $\mathbb{Z}[i]$ or LLL.

Exercise 6 – [Sum of four squares]

Do what have been seen in TD about the decomposition into sum of 4 squares for a prime $p \equiv 3 \bmod 4$ using LLL.

Exercise 7 – [Berlekamp]

You can choose to work in $\mathbb{F}_p$ where p is a prime.

Exercise 8 – [Zassenhaus and factoring in $K[X]$]
Simple version, without LLL-improvement.

Exercise 9 – [Fermat, Lehmann, Solovay-Strassen, Rabin-Miller]
Generate a family of Carmichael numbers to compare.

Exercise 10 – [Pocklington-Lehmer, Pepin for F_n, Lehmer for M_p]
Clear.

Exercise 11 – [$(p-1)$-Pollard's method, Goldwasser-Killian, Lenstra]
Clear.

Exercise 12 – [Dixon's random squares method, Quadratic Sieve]
Clear.