

## ASSIGNMENT 4

### SUMMARY

Write a Maple program that uses Chinese remaindering to calculate the determinant of an  $n \times n$ -integer matrix  $A$ . You may use the built-in Maple routines for integer addition, subtraction, multiplication and division but you have to supply your own implementation of the Extended Euclidean Algorithm to compute modular inverses. Verify the correctness of your programs by running the programs on various random inputs and by comparing your results with results supplied by Maple.

### DETAILED INSTRUCTIONS

- (1) Write a program that calculates an integer  $B$  such that  $\det(A) \leq B$ . You may simply let Maple calculate the determinant by performing interval arithmetic on intervals with floating point endpoints, e.g. using the command `shake(Determinant(A),10)`. Verify your program by generating random inputs using Maple's `RandomMatrix` and by invoking Maple's `Determinant`.
- (2) Write a program that generates a list of distinct prime numbers  $p$  whose product is larger than  $2B + 1$ . You may use any prime number that fits into one half of a computer word, for example any prime number  $< 2^{16}$ .
- (3) Write a program that computes modular inverses using the Extended Euclidean Algorithm. Verify your program using randomly generated inputs.
- (4) Write a program that computes  $A \bmod p$  and then  $\det(A \bmod p) \bmod p$  for each prime  $p$  on your list and that records the result. In particular, write your own modular Gaussian Elimination routine to transform  $A \bmod p$  into a matrix of upper triangular form. Then  $\det(A \bmod p) \bmod p$  is the product of the diagonal elements  $\bmod p$ . Record the value of the modular determinant. Verify your program.
- (5) Use Garner's Chinese Remainder Algorithm to obtain the integer  $\det(A)$  from the various recorded values  $\det(A) \bmod p$ . Verify your implementation of Chinese remaindering.
- (6) Verify your implementation of the complete determinant computation by computing some very small and some very large determinants.