MATH 467 FACTORIZATION & PRIMALITY TESTING, FALL 2023, FINAL

Return your solutions by Monday 11th December.

The task is to complete programming the quadratic sieve as described in the QS handout with the theoretical choice for B for the size of the factor base, and to apply the program to factorise the numbers n below. Printouts of your program must be included in your submissions for a grade to be assigned, but grades are dependent solely on your numerical answers.

For each number n listed below do the following.

1. List a set of exponents $e_1, e_2, \ldots, e_{K+2}$ and a set of x_j such that

$$(x_1^2 - n)^{e_1}(x_2^2 - n)^{e_2} \ldots (x_{K+2}^2 - n)^{e_{K+2}}$$

is a perfect square, y^2, and

2. such that when $x = x_1^{e_1} x_2^{e_2} \ldots x_{K+2}^{e_{K+2}}$ and y is as above $\gcd(x \pm y, n)$ gives a non-trivial factorisation of n,

3. and list the values of x, y and $\gcd(x \pm y, n)$.

$n = 3215031751$,
$n = 9912409831$,
$n = 37038381852397$,
$n = 341550071728321$,
$n = 31868712526338419047$.

It should be possible to copy these numbers from this .pdf. They can also be copied from my web site.

https://personal.science.psu.edu/rcv4/467f23/467f23.html
Because of a bug in the server you may have to click on that twice.

Note that there is a 20 digit number in addition to those from the miderm. For several of these numbers it may be necessary to increase the number of B–factorable numbers from $K+2$ to maybe $K+8$. For the last number, if you are using Pari/gp you will need to be careful about memory, the allotment of which can be increased by allocatemem, and it may be necessary to choose something a little smaller than B^2 for the initial choice of the number of x to try.