MATH 467 FACTORIZATION & PRIMALITY TESTING, FALL 2024, FINAL PROJECT

The task is to program 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 the numbers n below. The project is divided into two parts. If you submit the first half on Canvas by 2nd December I will give you feedback as to progress. **The final version of the project is due Monday 16th December.**

Part I: The sieving

For each of the numbers n below do the following.

1. List the primes in the factor base and the number K of primes in the factor base, including 2 (-1 is also in the factor base but is not prime).

2. List $K+2$ values of x for which x^2-n completely factors over the factor base (here K is the number of primes in the factor base, including 2).

3. For each x in 2. give the factorization of x^2-n. A vector of exponents suffices.

Part II: The factorisation

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 $e_1, e_2, \dots, e_{K+2}$ and a set of x_j such that

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

is a perfect square, y^2, and

2. such that when $x = x_1^{e_1}x_2^{e_2}\dots x_{K+2}^{e_{K+2}}$ 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 $\gcd(x \pm y, n)$.

$n = 3215031751$,
$n = 9912409831$,
$n = 37038381852397$,
$n = 341550071728321$,
$n = 3186871252633841 9047$.

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/rcv4/467f24/467f24.html
Because of a bug in the server you may have to click on that twice.

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.