MATH 467 FACTORIZATION AND PRIMALITY TESTING, FALL 2025, PROBLEMS 4

Return by Monday 22nd September

Lehman's method

The object of this homework is to use Lehman's method to find factors. The first two problems could be done by hand, but it would be more convenient to use a good calculator, or Pari/gp. I do not claim that for the numbers below Lehman's method is necessarily faster than trial division, although it is a lot less tedious. More to the point, you can see the possibilities. Lehman's method runs as follows. Given $n \in \mathbb{N}$ proceed as follows.

1. Try trial division $d|n$ for $d \leq n^{1/3}$ for d in the range. It suffices to take prime values of d only and for the first number n below these are well known! If a factor is found, stop. Pari/gp has a list of primes built in.

2. For each $t \in \mathbb{N}$ with $1 \leq t \leq n^{1/3}$ and $x \in \mathbb{N}$ with $(4tn)^{1/2} \leq x \leq (4tn + n^{2/3})^{1/2}$ (for the first number below the intervals that arise contain at most one integer) compute $x^2 - 4tn$ and check to see if this is a perfect square y^2. When it is compute $(x + y, n)$ and if this gives a proper factor of n, then stop.

For full marks, in the first two cases list the remainders on division by primes $3, 7, 11, 13, 17, \ldots$ up to $n^{1/3}$ and for each t with $1 \leq t \leq n^{1/3}$ list the possible values for x, and if $x^2 - 4tn$ is a perfect square y^2, then compute $(x + y, n)$ and stop. For the third number just give a value of t, the corresponding values of x and y and the factor. Note that Pari/gp has the gcd function built in. If you use a different programming language, then you will probably need to construct the gcd algorithm from scratch. In any event, submit a copy of your code.

1. Find a non–trivial factor of 19109.

2. Find a non–trivial factor of 2048129.

3. Find a non–trivial factor of 9912409831.