Problem

Modular Quadratic Equations

Due: April 15, 2024

You are to write a function to solve quadratic equations modulo `n`. You can complete the square just as one does with real numbers so that the problem essentially reduces to finding square roots modulo `n`. As discussed in class, this problem reduces to finding square roots modulo the prime factors of `n` and then using Hensel's Lemma to lift them to solutions modulo prime powers. Then, the solutions can be "stitched together" using the Chinese Remainder Theorem. It is possible that some cases will have no solution. Specifically, if a given number is not a quadratic residue (i.e., a square) modulo one of the prime factors, then there will be no solution. In this case, your function should return an empty vector. Remember that you can use Euler's Criterion to determine if a number is a quadratic residue. You should probably use your previous assignment, Factor, to determine the factorization of the modulus n.

The function you write should have the following signature:

```
    vector<long> quad_solve(long n, long a, long b, long c) { }
```

where the first argument is the modulus, and the quadratic equation to be solved is `a x^2 + b x + c = 0`. The returned vector is the set of all nonnegative roots less than `n`.

Important Simplifying Assumptions: `n` is odd, and `a`, `b` and `c` are relatively prime to `n`. (This also means they are nonzero.)