HW3

(Due 5:00pm Friday, May 2, 2025, on WyoCourses)

Instructions: Check your answers wherever possible. Submit solutions through WyoCourses. See the syllabus and FAQ for general expectations regarding homework.

1. (*20 points*) Use the Prime Number Theorem to find *reasonable estimates* for each of the following. Explain your work.
   (a) A 40-digit positive integer n is chosen at random. Estimate the probability that n is prime.
   (b) A 40-digit positive integer n, with last digit 1, 3, 7 or 9, is chosen at random. Estimate the probability that n is prime.
   (c) A 40-digit positive integer n, with first three digits 100, is chosen at random. Estimate the probability that n is prime.
   (d) A 40-digit positive integer n, with first three digits 100, and last digit 1, 3, 7 or 9, is chosen at random. Estimate the probability that n is prime.

2. (*24 points*) In each of the following, work by hand using a calculator to evaluate the indicated Legendre symbol using the Law of Quadratic Reciprocity. Show your work. Afterwards, you should check your answers using appropriate software (typically Mathematica or SageMath) using Euler's criterion.
   (a) $\left(\frac{138}{101}\right)$ (b) $\left(\frac{71}{103}\right)$ (c) $\left(\frac{68}{107}\right)$ (d) $\left(\frac{-22}{109}\right)$

3. (*16 points*) Let $p = 422231$. Using appropriate software,
   (a) Check that p is prime.
   (b) Determine the smallest positive integer that is a nonsquare mod p.

4. (*20 points*) Using appropriate software,
   (a) Find the smallest prime $p > 10^9$ satisfying $p \equiv 1 \mod 4$.
   (b) Find a nonsquare η mod p.

(c) Find $c \in \{1, 2, \ldots, \frac{p-1}{2}\}$ satisfying $c \equiv \eta^{\frac{p-1}{4}} \mod p$ and verify that $c^2 \equiv -1 \mod p$, as required by Euler's criterion.

(d) *Use the algorithm demonstrated in class on Apr 11*, beginning with the value of c found in (c), to express p as a sum of two integer squares.

Please review the pre-recorded class of Feb 19 (slides, lecture, and Mathematica session) before answering #5,6. We will soon be discussing anther big application of continued fractions to integer factorization.

5. (*20 points*) *Using the continued fraction method demonstrated on Feb 19*, find the simplest rational number (with three-digit numerator and denominator) having decimal approximation 1.320143884892. Show your work.

6. (*20 points*) *Using the continued fraction method demonstrated on Feb 19*, find the simplest quadratic irrational number (in the form $\frac{a+b\sqrt{d}}{c}$ where a, b, c, d are small integers) having decimal approximation 2.4188611699158. Show your work.