Solutions to HW3

1. The integers in the interval $[10^{39}, 10^{40})$ are exactly the integers having exactly 40 digits. Let I be the set of integers in this interval. There are exactly $|I| = 10^{40} - 10^{39} = 9 \times 10^{39}$ integers in this interval. The number of primes in I is

$$|P \cap I| \;=\; \pi(10^{40}) - \pi(10^{39}) \;\approx\; \tfrac{10^{40}}{40 \ln 10} - \tfrac{10^{39}}{39 \ln 10} \;\approx\; 9.7438 \times 10^{37}$$

where $P = \{2, 3, 5, 7, 11, \ldots\}$ denotes the set of all primes.

   (a) $\frac{|P \cap I|}{|I|} \approx \frac{9.7438 \times 10^{37}}{9 \times 10^{39}} \approx 0.01083$.

   (b) The number of integers in I having last digit 1, 3, 7 or 9 is exactly $0.4|I| = 3.6 \times 10^{39}$. All primes in I (with exactly two exceptions, namely 2 and 5) have last digit 1, 3, 7 or 9, so the new probability estimate is

$$\tfrac{|P \cap I| - 2}{0.4|I|} \;\approx\; 2.5 \tfrac{|P \cap I|}{|I|} \;\approx\; 2.5 \times 0.01083 \;\approx\; 0.02707.$$

   By restricting to random integers with last digit 1, 3, 7 or 9, we have increased our probability of obtaining a prime from about 1.1% to about 2.7%.

   For (c) and (d), we replace I by the set of 40-digit integers starting with the digits 100. This is the set I' of integers in the interval $[10^{39}, 10^{39}+10^{37})$. The number of integers in this interval is $|I'| = 10^{37}$; and the number of primes in I' is

$$|P \cap I'| \;=\; \pi(10^{39}+10^{37}) - \pi(10^{39}) \;\approx\; \tfrac{10^{39}+10^{37}}{\ln(10^{39}+10^{37})} - \tfrac{10^{39}}{39 \ln 10} \;\approx\; 1.1101 \times 10^{35}.$$

   (c) $\frac{|P \cap I'|}{|I'|} \approx \frac{1.101 \times 10^{35}}{10^{37}} \approx 0.01110$.

   (d) As in (b), restricting to integers with last digit 1, 3, 7 or 9 multiplies the probability estimate by 2.5. The new estimated probability of primality is $2.5 \times 0.01110 \approx 0.02753$.

2. (a) $\left(\frac{138}{101}\right) = \left(\frac{2}{101}\right)\left(\frac{3}{101}\right)\left(\frac{23}{101}\right) = (-1)\left(\frac{101}{3}\right)\left(\frac{101}{23}\right) = -\left(\frac{2}{3}\right)\left(\frac{9}{23}\right) = (-1)(-1)(1) = 1$. (Checked using $138^{50} \equiv 1 \mod 101$.)

   (b) $\left(\frac{71}{103}\right) = -\left(\frac{103}{71}\right) = -\left(\frac{32}{71}\right) = -\left(\frac{16}{71}\right)\left(\frac{2}{71}\right) = -(1)(1) = -1$. (Checked using $71^{51} \equiv -1 \mod 103$.)

   (c) $\left(\frac{68}{107}\right) = \left(\frac{4}{107}\right)\left(\frac{17}{107}\right) = 1\left(\frac{107}{17}\right) = \left(\frac{5}{17}\right) = \left(\frac{17}{5}\right) = \left(\frac{2}{5}\right) = -1$. (Checked using $68^{53} \equiv -1 \mod 107$.)

   (d) $\left(\frac{-22}{109}\right) = \left(\frac{-1}{109}\right)\left(\frac{2}{109}\right)\left(\frac{11}{109}\right) = (1)(-1)\left(\frac{109}{11}\right) = -\left(\frac{-1}{11}\right) = 1$. (Checked using $(-22)^{54} \equiv 1 \mod 109$.)

3. (a) I checked using the command `PrimeQ[422231]` in Mathematica, which returned the answer `true`.

   (b) The smallest such positive integer is 37. I checked that $a^{(p-1)/2} \equiv 1 \mod p$ for each $a \in \{1, 2, \ldots, 36\}$, and $37^{(p-1)/2} \equiv -1 \mod p$.

4. (a) The smallest such prime is $p = 1{,}000{,}000{,}009$. (The smallest prime exceeding 10^9 is 1,000,000,007.)

   (b) I randomly chose $\eta = 33$.

   (c) I compute $c = 430{,}477{,}711$ by taking the remainder of $\eta^{(p-1)/4} \mod p$. (Half of the choices of η will yield instead $c = 569{,}522{,}298$ which is not strictly in the interval $\left[1, \frac{p-1}{2}\right]$. This might result in a slightly longer search for the answer in (d); but I don't really care which of the two square roots of -1 we choose. In hindsight, I shouldn't have required $c \leqslant \frac{p-1}{2}$.)

   (d) Using the Maple code demonstrated in class, I obtain $p = 3747^2 + 31400^2$. This is the essentially unique solution.

5. Given $\alpha \approx 1.320143884892$, I numerically obtain $\alpha \approx [1, 3, 8, 11, 149880095, 1, 5]$. This strongly suggests roundoff error, and the actual result should be obtained by replacing the term 149880095 by ∞, giving

$$\alpha = [1, 3, 8, 11] = 1 + \frac{1}{3 + \frac{1}{8 + \frac{1}{11}}} = \frac{367}{278} \approx 1.3201438848920863309.$$

   All thirteen decimal digits of the original approximation agree with these digits; so I infer that $\alpha = \frac{367}{278}$ is the correct exact value.

6. Given $\beta \approx 2.4188611699158$, I numerically obtain $\beta \approx [2, 2, 2, 1, 1, 2, 1, 1, 2, 1, 1, \ldots]$. Eventually the obvious repetition breaks down, suggesting roundoff error; and I am compelled to believe that actually

$$\beta = [2, 2, 2, 1, 1, 2, 1, 1, \ldots] = 2 + \frac{1}{2 + \frac{1}{\gamma}}, \quad \gamma = [2, 1, 1, 2, 1, 1, \ldots] = 2 + \frac{1}{1 + \frac{1}{1 + \frac{1}{\gamma}}} = \frac{5\gamma + 3}{2\gamma + 1}$$

   so that $2\gamma^2 - 4\gamma - 3 = 0$ and $\gamma = \frac{1}{2}\left(2 \pm \sqrt{10}\right)$. Since $\gamma > 0$, we must take the larger of these two roots, so $\gamma = \frac{1}{2}\left(2 + \sqrt{10}\right)$ and

$$2 + \tfrac{1}{\gamma} = 2 + \tfrac{2}{2+\sqrt{10}} \cdot \tfrac{-2+\sqrt{10}}{-2+\sqrt{10}} = 2 + \tfrac{-4+2\sqrt{10}}{6} = \tfrac{8+2\sqrt{10}}{6} = \tfrac{4+\sqrt{10}}{3};$$

$$\beta = 2 + \tfrac{1}{2+\frac{1}{\gamma}} = 2 + \tfrac{3}{4+\sqrt{10}} \cdot \tfrac{4-\sqrt{10}}{4-\sqrt{10}} = 2 + \tfrac{12-3\sqrt{10}}{6} = \tfrac{8-\sqrt{10}}{2}.$$