Problem set 3

As we saw in class, the irrationality of $\zeta(3)$ is a really deep fact, which uses the Prime Number Theorem among other things. Not all irrationality proofs are hard − for instance, the one for $\sqrt{2}$ is very easy. The first 2 problems below will walk you through a somewhat more interesting (but still straightforward) method that works for $e$, $\sin(1)$, and other numbers. They don’t involve the PNT.

Problems 4-8 are based on stuff we will discuss on Monday.

1. Let $\theta$ be a real number and $a_m$ and $b_m$ two sequences of integers (with the $b_m$’s nonzero). Suppose that for every $\epsilon > 0$, there exists an $M \in \mathbb{N}$ such that

$$m \geq M \implies 0 < \left| \theta - \frac{a_m}{b_m} \right| < \frac{\epsilon}{b_m}.$$

Show that $\theta$ is irrational.

2. Suppose that $f(x)$ is a function represented by a power series (say, about 0 for simplicity) on the whole real line, and write $f(x) = P_k(x) + R_k(x)$ as a sum of the $k^{\text{th}}$ Taylor polynomial and remainder. Recall from calculus that

$$R_k(x) = \int_0^x \frac{f^{(k+1)}(t)}{k!} (x-t)^k dt.$$

Apply this formula with $f(x) := e^x$, and problem (1), to show that $e$ is irrational.

3. Explain why the PNT would lead you to expect that, on average, the gap between the prime $p$ and its successor is $\log(p)$.

4. Evaluate $\phi(m)$ for $m = 1, 2, 3, \ldots, 12$.

5. Prove that $n^{13} - n$ is divisible by 2, 3, 5, 7, and 13 for any integer $n$.

6. Let $m$ be an odd integer and let $a$ be any integer. Prove that $2m + a^2$ can never be a perfect square. [Hint: if a number is a square, what are its possible values modulo 4?]

7. Let $N$, $g$, and $A$ be positive integers. Consider the following algorithm:

1. Set $a = g$ and $b = 1$.

2. Loop while $A > 0$.

3. If $A \equiv 1 \pmod{2}$, set $b = b \cdot a \pmod{N}$.

4. Set $a = a^2 \pmod{N}$ and $A = \left\lfloor \frac{A}{2} \right\rfloor$.

5. If $A > 0$, continue with loop at Step 2.

6. Return the number $b$.

(a) Show that the output of this algorithm equals $g^A \pmod{N}$.

(b) Use it to compute $17^{183} \pmod{256}$.
(8) For each of the following primes $p$ and numbers $a$, compute $a^{-1} \mod p$ in two ways: (i) using the Euclidean algorithm; (ii) use problem (7) and Fermat’s little theorem.

(a) $p = 47$ and $a = 11$.
(b) $p = 587$ and $a = 345$. 