1: \( p := 329867 \) turns out to be prime.
(a) Please verify that 2 is a generator for \( \mathbb{F}_p^* \), by factoring \( p - 1 \) and checking just a few powers of 2 mod \( p \) (using the technique alluded to in Problem 4b from HW#3).
(b) Please solve for the unique \( x \in \{2, \ldots, 329866\} \) satisfying \( 2^x = 11 \mod 329867 \) via the Pohlig-Hellman Method.

2: \( p := 65537 = 2^{16} + 1 \) turns out to be prime. Using the Pohlig-Hellman Method, please solve for the unique \( x \in \{2, \ldots, 65536\} \) with \( 2^x = 3 \mod 65537 \).

3: \( p := 1009 \) turns out to be prime. Using the Shank’s Baby-Steps/Giant-Steps Method, please find the unique \( x \in \{2, \ldots, 1008\} \) with \( 11^x = 12 \mod 1009 \).

4: Suppose \( m_1, \ldots, m_k \in \mathbb{N} \) are pair-wise relatively prime, and \( a_1, \ldots, a_k \in \mathbb{Z} \). Please prove that if \( x_1, x_2 \in \mathbb{Z} \) are solutions to the simultaneous congruences \( x = a_1 \mod m_1, \ldots, x = a_k \mod m_k \), then \( x_1 = x_2 \mod \prod_{i=1}^{k} m_i \).

5: Please prove Euler’s Theorem: If \( a, n \in \mathbb{N} \) with \( \gcd(a, n) = 1 \) then \( a^{\phi(n)} = 1 \mod n \).

6: (a) Pierre Dusart’s 1998 Ph.D. thesis from the university of Limoges provides (among many other results) the following lower and upper bounds on the prime-counting function \( \pi(x) \):
\[
\frac{x}{\log x} \left( 1 + \frac{1}{\log x} \right) < \pi(x) < \frac{x}{\log x} \left( 1 + \frac{1}{\log x} + \frac{2.51}{(\log x)^2} \right), \text{ for all } x \geq 355991.
\]
Please use this estimate to find lower and upper bounds for the number of 100-digit primes.
(b) The (arguably) most important open problem in mathematics is the Riemann Hypothesis. Among many other implications, if true, it would imply the following sharper estimate for \( \pi(x) \):
\[
\text{li}(x) - \frac{\sqrt{x} \log x}{8\pi} < \pi(x) < \text{li}(x) + \frac{\sqrt{x} \log x}{8\pi}, \text{ for all } x \geq 2657,\text{ where } \text{li}(x) \text{ is a well-known integral that can be evaluated easily within Maple. In particular, the commands:}
\]
\[
\text{Digits:=100;}
\text{evalf(Li(10^{100}))};
\]
will evaluate \( \text{li}(10^{100}) \) to 100 digits of accuracy. Please use the preceding (conditional) estimate to find lower and upper bounds for the number of 100-digit primes. Are your estimates significantly sharper than those from Part (a)?

Instructor: J. Maurice Rojas