Homework 5 (due May 06 2020)

Directions: *Write up carefully argued solutions to the following problems. Your solution should be clear enough to convince someone who does not already know the answer. You may use results from lecture and previous homeworks without proof. See the syllabus for more details and for permitted resources and collaboration.*

1. Euclidean Algorithm (10 points)

Compute each of the following using Euclid's Algorithm. Show your intermediate results, both as a sequence of recursive calls and in tableau form.

(a) [4 points] $\gcd(68, 200)$

(b) [5 points] $\gcd(441, 287)$

(c) [1 point] $\gcd(2^{64} - 1, 2^0 - 1)$

2. Extended Euclidean Algorithm and Modular Equations (22 points)

(a) [5 points] Compute the multiplicative inverse of 25 modulo 119 using the Extended Euclidean Algorithm. Your answer should be a number between 0 and 118. Show your work in tableau form (the divisions performed, the equations for the remainders, and the sequence of substitutions).

(b) [8 points] Find all integer solutions $x \in \mathbb{Z}$ to the equation

$$25x \equiv 7 \pmod{119}$$

It is not sufficient just to state the answer. You need to *prove* that your answer is correct.

(c) [6 points] Prove that there are no integer solutions to the equation

$$15x \equiv 3 \pmod{25}$$

Note: this does not follow from (just) the fact that 15 does not have a multiplicative inverse modulo 25. That argument, if true, would apply to the equation $15x \equiv 15 \pmod{25}$, which does have solutions (e.g., $x = 1$)! Hence, a different argument is required to show that this equation has no integer solutions.

(d) [3 points] Prove that all solutions to the equation in part (b) are also solutions to

$$53x + 2 \equiv 3x + 16 \pmod{119}.$$

3. Modular Exponentiation (10 points)

(a) [7 points] Compute $3^{169} \bmod 100$ using the efficient modular exponentiation algorithm. Show all intermediate results.

(b) [1 point] How many multiplications does the algorithm use for this computation?

(c) [1 point] For the multiplications performed by the algorithm, what is the maximum number of decimal digits in the result?

(d) [1 point] Suppose that we instead computed the integer 3^{169}. How many decimal digits does it have? (No need to show work. Just give the answer.)

4. Properties of GCDs (18 points)

Let m and n be positive integers.

(a) [6 points] Prove that, if $a \equiv b \pmod{m}$ and $a \equiv c \pmod{n}$, then $b \equiv c \pmod{d}$, where $d = \gcd(m, n)$.

(b) [10 points] Prove that, if $b \equiv c \pmod{d}$, with $d = \gcd(m, n)$, then there exists some $a \in \mathbb{Z}$ such that $a \equiv b \pmod{m}$ and $a \equiv c \pmod{n}$.

(c) [2 points] Explain why the pair of congruences, $a \equiv b \pmod{m}$ and $a \equiv c \pmod{n}$, has a solution if and only if $b \equiv c \pmod{d}$, where $d = \gcd(m, n)$.

5. Rationals and Primes (20 points)

Given primes p and q with $p \neq q$ prove the following statements. You may use the following definition of rationality: If z is a rational number, then there exists co-prime integers a, b such that $z = a/b$. Recall integers a and b are co-prime if and only if the only integer k which divides both a and b is 1.

(a) [10 points] $\sqrt{pq}$ is irrational.

(b) [10 points] $\sqrt{p/q}$ is irrational.

6. Alllll the Odds (20 points)

Prove that the sum of the first n positive odd numbers is a perfect square (i.e., z^2 for some integer $\mathbb{Z}$), for all $n \in \mathbb{N} \setminus \{0\}$.

Hint: You may need to use a stricter induction hypothesis.