Problem 1

Consider a sequences of numbers $a_1, a_2, a_3, \ldots$ where $a_n = 50 + n^2$ for $n = 1, 2, 3, \ldots$. The first few values are

$$a_1 = 51, \quad a_2 = 54, \quad a_3 = 59, \quad a_4 = 66, \quad a_5 = 75, \quad \ldots$$

a. Warm-up. Compute $a_{15}, a_{16}, a_{167},$ and $a_{168}$. Check that you got the values:

$$a_{15} = 275, \quad a_{16} = 306, \quad a_{167} = 27939, \quad a_{168} = 28274$$

b. Use the Euclidean algorithm to calculate the following values, writing out every intermediate step. Providing the answer without any steps will yield no credit.

i. $\gcd(a_{15}, a_{16}) = \gcd(275, 306)$.

ii. $\gcd(a_{167}, a_{168}) = \gcd(27939, 28274)$.

c. Using part (b.i) from above, and using the extended Euclidean algorithm, solve the following congruence, writing out every intermediate step. Providing the answer without any steps will yield no credit.

$$x \text{ such that } 275 \cdot x \equiv 1 \pmod{306}.$$
d. We are interested in the value of $\gcd(a_n, a_{n+1})$ for different values of $n$. From part (b), we know that this can be different values.

Let’s compute two more examples. Use a calculator\(^1\) to compute the following:

i. $\gcd(a_{102}, a_{103}) = \gcd(50 + 102^2, 50 + 103^2)$.

ii. $\gcd(a_{368}, a_{369}) = \gcd(50 + 368^2, 50 + 369^2)$.

e. Verify that your answers from parts (b) and (d) satisfy

$$\gcd(a_n, a_{n+1}) = \gcd(n^2 - 100n, 2n + 1) = \gcd(n - 100, 201)$$

f. Using the Euclidean algorithm and algebraic manipulation, show that the property in part (e) holds true for all $n$.

g. For which $n$ is $\gcd(a_n, a_{n+1})$ the greatest, and what is the maximum value? Find and classify all $n$.

**Problem 2**

a. Prove that if an integer $n$ is odd, then either $n + 1$ or $n − 1$ is divisible by 4.

b. Prove using strong induction that for any odd integer $n \geq 3$, an $n \times n$ chessboard with the center square removed can be tiled by these 4-square L-tiles:

**Hint:** Show this for $n = 3$ and $n = 5$ first as your base cases. Then, for every other odd number $n$, can we add a 2-thick border to the tiling for $n − 4$ using our L-tiles?

**Problem 3**

Show that if $m$ is a positive integer greater than 1 and

$$ac \equiv bc \pmod{m},$$

then

$$a \equiv b \left( \mod \frac{m}{\gcd(c, m)} \right).$$

**Hint:** Use the definition $a \equiv b \pmod{m} \iff m | a − b \iff \exists k \in \mathbb{Z} \text{ s.t. } mk = a − b.$

\(^1\)You are welcome to use a site such as wolframalpha.com and simply enter a mathematical expression, such as ‘$\gcd(50 + 102^2, 50 + 103^2)$’, into the search box. You are welcome to use this to verify your solutions to part (b), but you should show your steps.
**Problem 4 (Mind Bender — Extra Credit)**

Mind Benders are extra credit problems intended to be more challenging than usual homework problems and are an exploration into a topic not covered in lecture. This week, we have an exploration into pseudoprimes and Carmichael numbers.

From Fermat’s Little Theorem, we know that for prime $p$, $a^p \equiv a \pmod{p}$ is true for $p \nmid a$. One might wonder if the converse of this is true. If $a^n \equiv a \pmod{n}$, does $n$ have to be a prime? This is unfortunately not true.

**Example**

Take $n = 341$ and $a = 2$. $2^{10} = 1024 \equiv 1 \pmod{341}$ and $2^{341} = (2^{10})^{34} \cdot 2 \equiv 2 \pmod{341}$. But $341 = 11 \cdot 31$, which is not a prime.

When this happens, we call $n$ a pseudoprime to the base $a$ if $n$ is composite but $a^n \equiv a \pmod{n}$. So, 341 is a pseudoprime to the base 2.

Are there composite numbers $n$ that are pseudoprime to all bases $a$? That is, for all $a \in \mathbb{Z}$, $a^n \equiv a \pmod{n}$ is true.

**Example**

Yes! 561 is one such number.

These numbers are called Carmichael numbers\(^2\).

a. Prove that any $n$ satisfying the following conditions is a Carmichael number\(^3\):

i. $n$ is odd.

ii. $n$ is squarefree. That is, each prime in $n$’s prime factorization appears only once; there are no powers of primes that divide $n$.

iii. For every prime $p$ dividing $n$, we have that $(p - 1) \mid (n - 1)$.

**Hint:** By the Chinese Remainder Theorem, if $a \equiv b \pmod{p_i}$ for distinct primes $p_i$, then $a \equiv b \pmod{N}$, where $N$ is the product of the $p_i$’s.

b. Prove that a Carmichael number cannot be the product of two distinct primes.

---

\(^2\)Named after Robert Daniel Carmichael.

\(^3\)This actually goes both ways. If $n$ is a Carmichael number, $n$ satisfies those conditions. We only prove the backward direction. This is called Korselt’s Criterion.