E. Dummit's Math 3527 ~ Number Theory 1, Fall 2026 ~ Homework 2, due Fri Sep 25th.

Justify all responses with clear explanations and in complete sentences unless otherwise stated. Write up your solutions cleanly and neatly and submit via Gradescope, making sure to select page submissions for each problem. **Use of generative AI in any manner is not allowed on this or any other course assignments.**

Part I: No justifications are required for these problems. Answers will be graded on correctness.

1. For each pair of integers (a, b), use the Euclidean algorithm to calculate their greatest common divisor $d = \gcd(a, b)$ and also to find integers x and y such that $d = xa + yb$. (Make sure to show at least some steps of the Euclidean algorithm.)
   (a) $a = 44$, $b = 12$.
   (b) $a = 481$, $b = 24$.
   (c) $a = 18063$, $b = 2025$.
   (d) $a = 12445$, $b = 5567$.
   (e) $a = 18200$, $b = 3505$.
   (f) $a = 233$, $b = 144$.

---

2. Find the following:
   (a) The gcd and lcm of 288 and 600.
   (b) The prime factorizations of 2025 and 2026. (You may want to use a calculator for these!)
   (c) The prime factorizations of 2025^{2026} and 2026^{2025}.
   (d) The prime factorizations of 111, 1001, and 111111.
   (e) The gcd and lcm of $2^8 3^{11} 5^7 7^8 11^2$ and $2^4 3^8 5^7 7^7 11^{11}$.
   (f) The prime factorization of 12! and the number of positive divisors of 12!.
   (g) The number of positive divisors and the sum of positive divisors of 10000.

---

3. It is sometimes claimed (occasionally in actual textbooks) that if $p_1, p_2, \ldots, p_k$ are the first k primes, then the number $n = p_1 p_2 \cdots p_k + 1$ used in Euclid's proof is always prime for any $k \geq 1$. Find a counterexample to this statement; make sure to justify that it is actually a counterexample.

Part II: Solve the following problems. Justify all answers with rigorous, clear explanations.

4. Let n be a positive integer greater than 1.
   (a) Show that if n is composite, then n must have at least one divisor d with $1 < d \leq \sqrt{n}$. Deduce that if n is composite, then n has at least one *prime* divisor $p \leq \sqrt{n}$. [Hint: Write $n = ab$ where $1 < a \leq b < n$.]
   (b) Show that if no prime less than or equal to $\sqrt{n}$ divides n, then n is prime.
   (c) Show explicitly that $n = 109$ and $n = 251$ are prime by verifying that they are not divisible by any prime $\leq \sqrt{n}$.

---

5. Recall that the factorial of n is defined as $n! = n \cdot (n-1) \cdot \cdots \cdot 1$, so for example $4! = 4 \cdot 3 \cdot 2 \cdot 1 = 24$. (Note that 0! is defined to be 1.)
   (a) If $n \geq 3$, show that the integers $n! + 2$, $n! + 3$, ... , $n! + n$ are all composite.
   (b) Suppose we list the primes in increasing order: $p_1 < p_2 < p_3 < \cdots$, so, for instance, $p_5 = 11$. For an arbitrary positive integer n, show that there is some pair of consecutive primes p_k, p_{k+1} such that $p_{k+1} - p_k \geq n$: in other words, that there exists a "prime gap" of size at least n.

   Remark: Part (b) shows that there are arbitrarily large prime gaps. The smallest possible prime gap that could occur infinitely often is 2, and the twin prime conjecture says that there are infinitely many pairs of consecutive primes that differ by 2.

---

6. The goal of this problem is to study which numbers of the form $N = a^k - 1$ can be prime, where a and k are positive integers greater than 1.

   (a) Show that if $a > 2$, then $N = a^k - 1$ is not prime.

   (b) Show that if k is composite, then $N = 2^k - 1$ is not prime. [Hint: If $k = rs$, show N is divisible by $2^r - 1$.]

   (c) Deduce that the only possible primes of the form $N = a^k - 1$ are those of the form $2^p - 1$ where p is a prime. (Such primes are called Mersenne primes.) Are all the numbers of the form $2^p - 1$ (p prime) actually prime?

   Remark: Mersenne primes can be used to construct perfect numbers, as described in problem 8.

---

7. Suppose $a|c$ and $b|c$ where a and b are relatively prime. Show that $(ab)|c$.

   Remark: More generally, if $a|c$ and $b|c$ then c is always divisible by $\text{lcm}(a, b)$. (If you want to solve the problem using this fact, you need to prove it!)

---

8. Recall that if N is a positive integer, then $\sigma(N)$ denotes the sum of the positive divisors of N. We say that N is a perfect number when $\sigma(N) = 2N$: this is often phrased as "the sum of all of the proper divisors of N equals N itself".

   (a) Show that if $2^{n+1} - 1$ is a prime number, then the number $N = 2^n(2^{n+1} - 1)$ is perfect.

   (b) Show that 28, 496, and 8128 are perfect numbers.

   We would now like to prove a partial converse to (a): namely, that every even perfect number must be of the form given in (a). So suppose $N = 2^n c$ is a perfect number where $n \geq 1$ and c is odd, and observe that $\sigma(N) = (2^{n+1} - 1)\sigma(c)$.

   (c) Show that c must be divisible by $2^{n+1} - 1$.

   (d) Show that c must equal $2^{n+1} - 1$ and that $2^{n+1} - 1$ is prime. [Hint: Use $\sigma(c) = 2^{n+1}c/(2^{n+1} - 1)$ and the fact that c has two divisors c and $c/(2^{n+1} - 1)$ to conclude it has no other divisors.]

   (e) Deduce that the even perfect numbers are precisely the numbers of the form $N = 2^n(2^{n+1} - 1)$ where $2^{n+1} - 1$ is prime.

   Remark: Perfect numbers have been of mathematical (and numerological) interest since antiquity. Euclid established the result in (a), and roughly two millennia later, Euler proved the result in (e). It is not known whether there are infinitely many even perfect numbers, and it is also not known whether there are any odd perfect numbers.
