E. Dummit's Math 3527 ~ Number Theory I, Spring 2022 ~ Homework 2, due Fri Feb 4th.

Justify all responses with clear explanations and in complete sentences unless otherwise stated. Write up your solutions cleanly and neatly, and clearly identify all problem numbers. Submit scans of your responses via Canvas.

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

1. Find the following:
   (a) The gcd and lcm of 288 and 600.
   (b) The gcd and lcm of $2^8 3^{11} 5^7 7^8 11^2$ and $2^4 3^8 5^7 7^7 11^{11}$.
   (c) A positive integer n such that $n/2$ is a perfect square and $n/3$ is a perfect cube.
   (d) The values of $\overline{6}+\overline{13}$, $\overline{6}-\overline{13}$, and $\overline{6}\cdot\overline{13}$ in $\mathbb{Z}/11\mathbb{Z}$. Write your answers as $\overline{a}$ where $0 \le a \le 10$.
   (e) The addition and multiplication tables modulo 7. (For ease of writing, you may omit the bars in the residue class notation.)
   (f) All of the unit residue classes modulo 7 and their multiplicative inverses.
   (g) The multiplication table modulo 8. (Again, you may omit the bars.)
   (h) All of the unit residue classes modulo 8 and their multiplicative inverses.

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

2. 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 $x^k - 1$ is divisible by $x - 1$, for any integer x.
   (b) Show that if $a > 2$, then $N = a^k - 1$ is not prime.
   (c) Show that if k is composite, then $N = 2^k - 1$ is not prime. [Hint: If $k = rs$, show N is divisible by $2^r - 1$.]
   (d) Show that the only 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) necessarily prime?

---

3. Suppose that n is a positive integer with prime factorization $p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ for distinct primes $p_1, \dots, p_k$.
   (a) Show that the number of positive integers d dividing n is equal to $(a_1+1)(a_2+1)\cdots(a_k+1)$. [Hint: Consider the prime factorization of d.]
   (b) Prove that a positive integer n has an odd number of divisors if and only if n is a perfect square.
   (c) Show that the sum of the positive divisors of n, denoted $\sigma(n)$, is equal to $(1+p_1+\cdots+p_1^{a_1})(1+p_2+\cdots+p_2^{a_2})\cdots(1+p_k+\cdots+p_k^{a_k})$. [Hint: Try distributing out the product.]
   (d) A perfect number is a positive integer N such that $\sigma(N) = 2N$ (typically phrased as "the sum of all of the proper divisors of n equals n itself"). Show that if $2^n - 1$ is a prime number, then the number $N = 2^{n-1}(2^n - 1)$ is perfect.
   (e) Show that 28, 496, 8128 are perfect numbers.

---

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 $d \leq \sqrt{n}$. Deduce that if n is composite, then n has at least one prime divisor $p \leq \sqrt{n}$. [Hint: Note that divisors come in pairs $(a, n/a)$.]

   (b) Show that if no prime less than or equal to $\sqrt{n}$ divides n, then n is prime.

   (c) Show explicitly that the number 109 is prime by verifying that it is not divisible by any of the primes $\leq \sqrt{109}$.

---

5. Suppose a, b, c, m are integers and $m > 0$. Prove the following basic properties of modular congruences (these properties are mentioned but not proven in the notes; you are expected to give the details of the proofs):

   (a) For any a, $a \equiv a \pmod{m}$.

   (b) If $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, then $a \equiv c \pmod{m}$.

   (c) If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a + c \equiv b + d \pmod{m}$.

   (d) If $a \equiv b \pmod{m}$, then $ac \equiv bc \pmod{mc}$ for any $c > 0$.

---

6. Let R be a commutative ring with 1 and let r be an element of R.

   (a) Show that if r is a unit then $-r$ and r^{-1} are also units.

   (b) Show that if r and s are units, then rs is also a unit.
