E. Dummit's Math 3527 ~ Number Theory I, Spring 2020 ~ Homework 2, due Wed Jan 22nd.

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. Either staple the pages of your assignment together and write your name on the first page, or paperclip the pages and write your name on all pages.

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) The total number of positive integers that divide $2^2 3^4 5^9 7^3$. [Hint: Consider possible prime factorizations.]

   (d) A positive integer n such that $n/2$ is a perfect square and $n/3$ is a perfect cube.

   (e) A triple of positive integers (a, b, c) such that $\gcd(a, b)$, $\gcd(a, c)$, and $\gcd(b, c)$ are all greater than 1, but the only common divisors of all three of a, b, c are ± 1.

   (f) The elements $1 + 2\sqrt{5}$, $9 + 4\sqrt{5}$, $5 + \sqrt{5}$, and $2 - \sqrt{5}$ that are units in the ring $\mathbb{Z}[\sqrt{5}]$. For the elements that are units, also find their multiplicative inverses.

   (g) 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 $0 \leq a \leq 10$.

   (h) All integers n with the property that $\overline{n} + \overline{7} = \overline{1}$ modulo 23. [Hint: The answer is *not* "$n = 17$".]

---

2. If R is a commutative ring with 1, we say an element $r \in R$ is <u>irreducible</u> if r is not a unit and there exists no "factorization" $r = ab$ where neither a nor b is a unit.

   Example: In $R = \mathbb{Z}$, the irreducible elements are prime numbers (and their negatives).

   Example: In $R = \mathbb{Z}[i]$, the element $3 - i$ is not irreducible, because $3 - i = (1 + i)(2 - i)$ and neither $1 + i$ nor $2 - i$ is a unit.

   Example: In $R = \mathbb{Z}[\sqrt{2}]$, the element $\sqrt{2}$ is irreducible, because if $\sqrt{2} = ab$ then $2 = N(\sqrt{2}) = N(a)N(b)$ and then one of $N(a), N(b)$, and hence one of a, b, would have to be a unit. More generally, if an element has prime norm in $\mathbb{Z}[\sqrt{D}]$, then it is always irreducible (but note that there can also exist irreducible elements of non-prime norm).

   (a) Inside the ring $R = 2\mathbb{Z}$ of even integers, identify which of the elements 2, 4, 6, 8, 10, and 30 are irreducible.

   (b) Inside the ring $R = 2\mathbb{Z}$ of even integers, show that 60 has two different irreducible factorizations as products of positive numbers.

   (c) Inside the ring $R = \mathbb{Z}[i]$, identify which of the elements $1 + i$, $2 + i$, $3 + i$, and $4 + i$ are irreducible.

---

3. Draw the addition and multiplication tables modulo 7. (For ease of writing, you may omit the bars in the residue class notation.) Then, for each residue class, identify whether it is a unit, and if so, calculate its multiplicative inverse.

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

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 $p \leq \sqrt{n}$.

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

   (c) Use part (b) to explain why the representation $89 = 2 \cdot 5 \cdot 11 - 3 \cdot 7$ shows that 89 is prime.

---

5. Let R be a commutative ring with 1 and let r and s be elements 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.

---

6. 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 $c > 0$.

---

7. The goal of this problem is to analyze the maximum possible number of divisions that the Euclidean algorithm requires (in the parlance of computer science, this represents the worst-case time complexity). One might expect the slowest possible computation to occur when all of the quotients in the division algorithm are as small as possible, and the resulting gcd is also 1; our goal is to prove this fact.

   (a) As motivation, find a and b such that the Euclidean algorithm takes 6 divisions to compute their gcd of 1, and all of the corresponding quotients except the last are 1. In other words, find a and b such that

$$\begin{aligned} a &= q_1 b + r_1 \\ b &= q_2 r_1 + r_2 \\ r_1 &= q_3 r_2 + r_3 \\ r_2 &= q_4 r_3 + r_4 \\ r_3 &= q_5 r_4 + r_5 \\ r_4 &= q_6 r_5 \end{aligned}$$

   where $q_1 = q_2 = q_3 = q_4 = q_5 = 1$, $q_6 = 2$, and $r_5 = 1$. (Note that the last two quotients cannot be 1 if the last remainder is also 1.)

   (b) Prove that the Euclidean algorithm requires exactly n divisions to compute $\gcd(F_{n+2}, F_{n+1})$, where F_n is the nth Fibonacci number as defined on homework 1.

   (c) Suppose that $b \leq a$ and that a and b are integers for which the Euclidean algorithm requires at least $n \geq 2$ divisions to compute $\gcd(a, b)$. Prove that $b \geq F_{n+1}$ and $a \geq F_{n+2}$.

   (d) Deduce that if $b \leq a$ and a, b are the smallest integers for which the Euclidean algorithm requires exactly n divisions, then $a = F_{n+2}$ and $b = F_{n+1}$.

   - Remark: As shown on homework 1, the Fibonacci numbers grow exponentially: $F_n \approx \frac{1}{\sqrt{5}}\varphi^n$. Because $\log_\varphi(b\sqrt{5}) - 2 < 5\lceil \log_{10}(b) \rceil$, part (d) implies that the Euclidean algorithm will compute $\gcd(a, b)$ with a number of divisions that is at most 5 times the number of base-10 digits of b. Thus for example, using the Euclidean algorithm to compute the gcd of two 1000-digit numbers will only take at most 5000 steps (which is very efficient!).
