E. Dummit's Math 3527 $\sim$ Number Theory 1, Spring 2026 $\sim$ Homework 4 Solutions

---

1. For each integer a and modulus m, determine whether the residue class $\overline{a}$ is a unit modulo m, or a zero divisor modulo m. If $\overline{a}$ is a unit then find its multiplicative inverse, while if $\overline{a}$ is a zero divisor then find a nonzero residue class $\overline{x}$ such that $\overline{x} \cdot \overline{a} = \overline{0}$.

   (a) $a = 14$, $m = 49$.

   - Since $\gcd(14, 49) = 7$, we see 14 and 49 are not relatively prime so $\boxed{\overline{14} \text{ is a zero divisor}}$.
   - Then $14 \cdot (49/7) \equiv 0 \pmod{49}$, so one possible $\overline{x}$ with $\overline{14} \cdot \overline{x} = \overline{0}$ is $\overline{x} = \boxed{\overline{7}}$.

   (b) $a = 16$, $m = 49$.

   - Since $\gcd(16, 49) = 1$, we see 16 and 49 are not relatively prime so $\boxed{\overline{16} \text{ is a unit}}$.
   - To compute the multiplicative inverse we use the Euclidean algorithm to write the gcd as a linear combination, which eventually yields $1 \cdot 49 - 3 \cdot 16 = 1$.
   - Reducing both sides modulo 49 yields $\overline{-3} \cdot \overline{16} = \overline{1}$ so the multiplicative inverse of $\overline{16}$ is $\boxed{\overline{-3} = \overline{46}}$.

   (c) $a = 125$, $m = 2026$.

   - Since $\gcd(125, 2026) = 1$, we see 125 and 2026 are relatively prime so $\boxed{\overline{125} \text{ is a unit}}$.
   - To compute the multiplicative inverse we use the Euclidean algorithm to write the gcd as a linear combination, which eventually yields $389 \cdot 125 - 24 \cdot 2026 = 1$.
   - Reducing modulo 2026 yields $\overline{389} \cdot \overline{125} = \overline{1}$ so the multiplicative inverse of $\overline{125}$ is $\boxed{\overline{389}}$.

   (d) $a = 788$, $m = 2026$.

   - Since $\gcd(788, 2026) = 2$, we see 788 and 2026 are not relatively prime so $\boxed{\overline{788} \text{ is a zero divisor}}$.
   - Then $788 \cdot (2026/2) \equiv 0 \pmod{2026}$, so one possible $\overline{x}$ with $\overline{788} \cdot \overline{x} = \overline{0}$ is $\overline{x} = \boxed{\overline{2026/2} = \overline{1013}}$.

---

2. Find the general solution to each of the given congruences, or explain why there is no solution:

   (a) $4n + 3 \equiv 2 \pmod{19}$.

   - This congruence is the same as $4n \equiv -1 \pmod{19}$.
   - Using the Euclidean algorithm, we see that $\gcd(4, 19) = 1$ and that $5 \cdot 4 - 1 \cdot 19 = 1$, so the multiplicative inverse of 4 modulo 19 is 5.
   - Thus, multiplying both sides by 5 yields $n \equiv 20n \equiv -5 \pmod{19}$, so we get $\boxed{n \equiv -5 \pmod{19}}$.

   (b) $3n \equiv 7 \pmod{21}$.

   - Notice that $\gcd(3, 21) = 3$, but 3 does not divide 7. Therefore, this congruence has $\boxed{\text{no solution}}$.

   (c) $3n \equiv 9 \pmod{21}$.

   - Notice that $\gcd(3, 21) = 3$, and 3 does divide 9, so the congruence has a solution.
   - Thus, since the congruence $ax \equiv b \pmod{m}$ is equivalent to $(a/d)x \equiv (b/d) \pmod{m/d}$ where $d = \gcd(a, m)$, by cancelling the factor 3, we see that $3n \equiv 9 \pmod{21}$ is equivalent to $\boxed{n \equiv 3 \pmod{7}}$.

   (d) $15n \equiv 4 \pmod{77}$.

   - Using the Euclidean algorithm, we can find $\gcd(15, 77) = 1$ and $36 \cdot 15 - 7 \cdot 77 = 1$.
   - Thus, multiplying both sides by 36 yields $n \equiv 36 \cdot 15n \equiv 36 \cdot 4 \equiv 108 \pmod{77}$, so the general solution is $\boxed{n \equiv 108 \equiv 31 \pmod{77}}$.

(e) $26n \equiv 130 \pmod{2026}$.

- Using the Euclidean algorithm, we can find $\gcd(26, 2026) = 2$. Since 2 also divides 130, there is a solution.
- Diving through by 2 yields the equivalent congruence $13n \equiv 65 \pmod{1013}$. The solution to this congruence is visibly $n \equiv 5 \pmod{1013}$ by dividing through by 13, so the general solution is $\boxed{n \equiv 5 \pmod{1013}}$.

---

3. Using the Chinese Remainder Theorem or otherwise, find the general solution n to each system of simultaneous congruences:

(a) $n \equiv 4 \pmod{11}$ and $n \equiv 1 \pmod{15}$.

- The solution to the second congruence is $n = 1 + 15k$ for an integer k.
- Plugging into the first congruence gives $1 + 15k \equiv 4 \pmod{11}$, whence $4k \equiv 3 \pmod{11}$.
- Since the multiplicative inverse of 4 modulo 11 is 3 (as can be found via the Euclidean algorithm), multiplying both sides by 3 yields $k \equiv 12k \equiv 9 \pmod{11}$, and so $k = 9 + 11l$.
- Setting $k = 9 + 11l$ then yields the general solution $n = 1 + 15(9 + 11l) = \boxed{136 + 165l}$ for $l \in \mathbb{Z}$. Equivalently, the solution is $\boxed{n \equiv 136 \pmod{165}}$.

(b) $n \equiv 7 \pmod{999}$ and $n \equiv 37 \pmod{1001}$.

- The solution to the second congruence is $n = 37 + 1001k$ for an integer k.
- Then the first congruence gives $37 + 1001k \equiv 7 \pmod{999}$, so $2k \equiv -30 \pmod{999}$.
- Dividing through by 2 (allowable because 2 is relatively prime to 999), or equivalently multiplying by 500, yields $k \equiv -15 \pmod{999}$, so $k = -15 + 999l$.
- Setting $k = -15 + 999l$ yields the general solution $n = 37 + 1001(-15 + 999l) = \boxed{-14978 + 999999l}$ for $l \in \mathbb{Z}$. Equivalently, the solution is $\boxed{n \equiv -14978 \pmod{999999}}$.

(c) $n \equiv 7 \pmod{84}$ and $n \equiv 21 \pmod{35}$.

- The solution to the first congruence is $n = 7 + 84k$ for an integer k.
- Then the second congruence gives $7 + 84k \equiv 21 \pmod{35}$, so $14k \equiv 14 \pmod{35}$.
- Cancelling the common factor of 14, which requires dividing the modulus by $\gcd(14, 35) = 7$, then yields $k \equiv 1 \pmod{5}$.
- Back-substituting gives $n = \boxed{91 + 420k}$ for $k \in \mathbb{Z}$. Equivalently, the solution is $\boxed{n \equiv 91 \pmod{420}}$.

(d) $n \equiv 7 \pmod{85}$ and $n \equiv 21 \pmod{34}$.

- Reduce the equations mod 17: the first gives $n \equiv 7 \pmod{17}$, while the second gives $n \equiv 4 \pmod{17}$. These are inconsistent so there is $\boxed{\text{no solution}}$.

(e) $n \equiv 2 \pmod{8}$, $n \equiv 1 \pmod{5}$, and $n \equiv 3 \pmod{9}$.

- The solution to the third congruence is $n = 3 + 9k$ for an integer k.
- Then the first congruence gives $3 + 9k \equiv 2 \pmod{8}$, so $k \equiv -1 \pmod{8}$. Setting $k = -1 + 8l$ gives $n = -6 + 72l$.
- The second congruence gives $-6 + 72l \equiv 1 \pmod{5}$, so $2l \equiv 2 \pmod{5}$, and thus $l \equiv 1 \pmod{5}$.
- Back-substituting gives $n = \boxed{66 + 360d}$ for $d \in \mathbb{Z}$. Equivalently, the solution is $\boxed{n \equiv 66 \pmod{360}}$.

(f) $n \equiv 1 \pmod{44}$, $n \equiv 81 \pmod{90}$, and $n \equiv 61 \pmod{80}$.

- The solution to the second congruence is $n = 81 + 90k$. Plugging into the third congruence yields $81 + 90k \equiv 61 \pmod{80}$, so that $10k \equiv -20 \pmod{80}$, which is equivalent to $k \equiv -2 \pmod{8}$, hence $k = -2 + 8l$ and thus $n = -99 + 720l$.
- Then the first congruence yields $-99 + 720l \equiv 1 \pmod{44}$, so that $16l \equiv 100 \pmod{44}$, which is equivalent to $4l \equiv 3 \pmod{11}$. Multiplying by 3 yields $l \equiv 12l \equiv 9 \pmod{11}$, so $l = 9 + 11d$.
- Back-substituting yields $n = \boxed{6381 + 7920d}$ for $d \in \mathbb{Z}$. Equivalently, the solution is $\boxed{n \equiv 6381 \pmod{7920}}$.

---

4. Calculate each of the following things:

   (a) The orders of each of the units modulo 9.

   - The element 1 always has $\boxed{\text{order 1}}$.
   - We have $2^1 \equiv 2$, $2^2 \equiv 4$, $2^3 \equiv 8$, $2^4 \equiv 7$, $2^5 \equiv 5$, $2^6 \equiv 1$ so 2 has $\boxed{\text{order 6}}$.
   - Also $4^1 \equiv 4$, $4^2 \equiv 7$, $4^3 \equiv 1$ so 4 has $\boxed{\text{order 3}}$.
   - Then $5^1 \equiv 5$, $5^2 \equiv 7$, $5^3 \equiv 8$, $5^4 \equiv 4$, $5^5 \equiv 2$, $5^6 \equiv 1$ so 5 has $\boxed{\text{order 6}}$.
   - Next $7^1 \equiv 7$, $7^2 \equiv 4$, $7^3 \equiv 1$ so 7 has $\boxed{\text{order 3}}$.
   - Finally $8^1 \equiv 8$ and $8^2 \equiv 1$ so 8 has $\boxed{\text{order 2}}$.

   (b) The order of 2 modulo 31.

   - Computing powers, we have $2^1 \equiv 2$, $2^2 \equiv 4$, $2^3 \equiv 8$, $2^4 \equiv 16$, and $2^5 \equiv 1 \pmod{31}$, so 2 has $\boxed{\text{order 5}}$ mod 31.

   (c) The order of 3 modulo 40.

   - Computing powers, we have $3^1 \equiv 3$, $3^2 \equiv 9$, $3^3 \equiv 27$, $3^4 \equiv 81 \equiv 1 \pmod{41}$, so 3 has $\boxed{\text{order 4}}$ mod 40.

   (d) The order of -11 modulo 17.

   - Recall that by Euler's Theorem, the order of a modulo m divides $\varphi(m)$. Since $\varphi(17) = 16$, the possible orders of any unit are 1, 2, 4, 8, and 16.
   - Since $-11 \equiv 6 \pmod{17}$, we see $(-11)^2 \equiv 36 \equiv 2 \pmod{17}$, $(-11)^4 \equiv 4 \pmod{17}$, $(-11)^8 \equiv 16 \equiv -1 \pmod{17}$, and $(-11)^{16} \equiv 1 \pmod{17}$. The only one of these that is 1 mod 17 is $(-11)^{16}$, so this element has $\boxed{\text{order 16}}$ mod 17.

   (e) The orders of 2, 4, and 8 modulo 25.

   - By Euler's Theorem, the order of 2 modulo 25 must divide $\varphi(25) = 20$.
   - We can compute $2^{20/2} \equiv -1 \pmod{25}$ and $2^{20/5} \equiv 16 \pmod{25}$, and we also know that $2^{20} \equiv 1 \pmod{25}$ by Euler's theorem.
   - Hence by our results on orders, we see that $2^{20/p} \not\equiv 1 \pmod{25}$ for any prime dividing 20, and so 2 must have $\boxed{\text{order 20}}$.
   - Then since $\gcd(2, 20) = 2$, we see that $4 = 2^2$ has order $20/2 = \boxed{10}$, and since $\gcd(3, 20) = 1$, we see that $8 = 2^3$ has order $20/1 = \boxed{20}$.

   (f) The order of 3 modulo 23.

   - By Euler's Theorem, the order of a modulo m divides $\varphi(m)$. Since $\varphi(23) = 22$, the possible orders of any unit are 1, 2, 11, and 22.
   - Since $3^1 \equiv 3$, $3^2 \equiv 9$, $3^4 \equiv 9^2 \equiv 81 \equiv 12$, $3^8 \equiv 12^2 \equiv 144 \equiv 6$, $3^{16} \equiv 6^2 \equiv 36 \equiv 13$, we have $3^1 \equiv 3$, $3^2 \equiv 9$, $3^{11} \equiv 3^8 3^2 3^1 \equiv 6 \cdot 9 \cdot 3 \equiv 1 \pmod{23}$. Hence the order must be $\boxed{11}$.

   (g) The smallest positive integer s such that $3^s \equiv 1 \pmod{11}$.

   - We can simply compute powers: $3^1 \equiv 1$, $3^2 \equiv 9$, $3^3 \equiv 2$, $3^4 \equiv 6$, $3^5 \equiv 1$. So the smallest s is $s = \boxed{5}$.

   (h) The remainder when 2^{4000} is divided by 41.

   - By Fermat (or Euler) we know that $2^{40} \equiv 1 \pmod{41}$.
   - Then $2^{4000} \equiv (2^{40})^{100} \equiv 1^{100} = 1 \pmod{41}$. Hence the remainder is $\boxed{1}$.

   (i) The remainder when 3^{65} is divided by 17.

   - By Fermat (or Euler) we know $3^{16} \equiv 1 \pmod{17}$, so $3^{65} \equiv 3 \cdot (3^{16})^4 \equiv \boxed{3} \pmod{17}$.

5. Suppose n is an integer.

(a) Show that $n^5 - n \equiv 0 \pmod{30}$. [Hint: By the Chinese Remainder Theorem, this is equivalent to showing $n^5 - n$ is divisible by 2, 3, and 5.]

- By the Chinese Remainder Theorem, we must equivalently show that 5, 2, and 3 each divide $n^5 - n$.
- By Fermat's little theorem, $n^2 \equiv n \pmod{2}$ for all n. Multiplying by n repeatedly and equating shows $n^5 \equiv n^4 \equiv n^3 \equiv n^2 \equiv n \pmod{2}$, so 2 divides $n^5 - n$.
- Similarly, we have $n^3 \equiv n \pmod{3}$. Multiplying by n^2 yields $n^5 \equiv n^3 \equiv n \pmod{3}$, so 3 divides $n^5 - n$.
- Finally, $n^5 \equiv n \pmod{5}$ by Fermat directly, so 5 divides $n^5 - n$.

(b) Show that $n^8 - n^2 \equiv 0 \pmod{84}$.

- By the Chinese Remainder Theorem, we must equivalently show that 4, 3, and 7 each divide $n^8 - n^2$.
- By Fermat, since $n^7 \equiv n \pmod{7}$, we have $n^8 \equiv n^2 \pmod{7}$.
- If n is even, then $n^8 \equiv n^2 \equiv 0 \pmod{4}$, while if n is odd, then $n^8 \equiv n^2 \equiv 1 \pmod{4}$. So 4 divides $n^8 - n^2$.
- Similarly, since $n^3 \equiv n \pmod{3}$, we see $n^8 \equiv n^6 \equiv n^4 \equiv n^2 \pmod{3}$, so 3 divides $n^8 - n^2$.

---

6. Let $m \geq 2$ be an integer. The goal of this problem is to study the value of $(m-1)!$ modulo m.

(a) If m is prime, show that $(m-1)! + 1$ is divisible by m.

- If m is prime, then by Wilson's Theorem we know that $(m-1)! \equiv -1 \pmod{m}$. Adding 1 yields $(m-1)! + 1 \equiv 0 \pmod{m}$ as required.

(b) Show that $m = 4$ is a counterexample to the statement of the proposition below, and identify the error in the proof:
Proposition: If m is composite, then $(m-1)!$ is divisible by m.
Proof: Suppose $m = ab$ where a and b are greater than 1 and less than m. Then both a and b appear as terms in the product $(m-1)! = (m-1) \cdot (m-2) \cdots 2 \cdot 1$, so $(m-1)!$ is divisible by ab.

- If $m = 4$ then $(m-1)! = 6 \equiv 2 \pmod{m}$, so m does not divide $(m-1)!$.
- The error in the proof is that if $a = b$, then both a and b appear in the product for $(m-1)!$, but as the same term.

(c) If m is composite and greater than 4, prove that $(m-1)!$ is in fact divisible by m.

- The proof in (b) is correct for $m = ab$ where $1 < a, b < m$ and $a \neq b$: then both a and b appear as distinct terms in $(m-1)!$, and so $(m-1)!$ is divisible by m.
- The only other case is when $m = a^2$ for some $a > 2$. But in that case both a and $2a$ appear as terms in $(m-1)!$, and so again $(m-1)!$ is divisible by m.

---

7. Prove that 5 has order 16 modulo 102 and order 36 modulo 111.

- For the modulus 102, we compute $5^2 \equiv 25$, $5^4 \equiv 25^2 \equiv 13$, $5^8 \equiv 13^2 \equiv 67$, $5^{16} \equiv 67^2 \equiv 1 \pmod{102}$ using successive squaring.
- Then since $5^{16} \equiv 1 \pmod{102}$ we see that the order of 5 divides 16. However since $5^8 \not\equiv 1 \pmod{102}$, the order cannot divide 8, so it must be 16.
- For the modulus 111, we compute $5^2 \equiv 25$, $5^4 \equiv 25^2 \equiv 70$, $5^8 \equiv 70^2 \equiv 16$, $5^{16} \equiv 16^2 \equiv 34$, $5^{32} \equiv 34^2 \equiv 46 \pmod{111}$ using successive squaring.
- Then $5^{36} = 5^{32} \cdot 5^4 \equiv 46 \cdot 70 \equiv 1 \pmod{111}$, so the order of 5 divides 36.
- Since the prime divisors of 36 are 2 and 3, we must also compute $5^{36/2} = 5^{18}$ and $5^{36/3} = 5^{12} \pmod{111}$.
- Since $5^{18} = 5^{16} \cdot 5^2 \equiv 34 \cdot 25 \equiv 73 \pmod{111}$, and $5^{12} = 5^8 \cdot 5^4 \equiv 16 \cdot 70 \equiv 10 \pmod{111}$, the order of 5 cannot divide 18 or 12, and therefore the order must be 36 as claimed.

---

8. The goal of this problem is to discuss elements of order 2 and order 4 modulo m.

   (a) If $p > 2$ is prime, show that there is a unique element of order 2 in $\mathbb{Z}/p\mathbb{Z}$. [Hint: If k has order 2, then p divides $k^2 - 1 = (k-1)(k+1)$.]

   - Following the hint, if k has order 2 then $k^2 \equiv 1 \pmod{p}$ so that p divides $k^2 - 1 = (k-1)(k+1)$.
   - Then since p is prime, by the prime divisibility property we see that p must divide $k-1$ so that $k \equiv 1 \pmod{p}$, or p must divide $k+1$ so that $k \equiv -1 \pmod{p}$.
   - Since $k = 1$ has order 1 modulo p, we conclude that there is a unique element of order exactly 2, namely -1.

   (b) Show using an example that if m is composite, then there may be more than one element of order exactly 2 in $\mathbb{Z}/m\mathbb{Z}$.

   - There are many examples. The smallest is $m = 8$: the elements 3, 5, and 7 all have order exactly 2 modulo 8.

   (c) Show that an element a has order 4 in $\mathbb{Z}/m\mathbb{Z}$ if and only if its square a^2 has order 2.

   - Suppose that a has order 4. Then a^2 has order $4/\gcd(2,4) = 4/2 = 2$ by properties of order.
   - Conversely, if a^2 has order 2, then $(a^2)^2 \equiv 1 \pmod{m}$ and so the order of a must divide 4. But since a^2 has order 2, it cannot be $\equiv 1 \pmod{m}$, so we see $a^2 \not\equiv 1 \pmod{m}$, so the order does not divide 2. Hence it must be 4.

   (d) Deduce that if $p > 2$ is prime, then the elements of order 4 in $\mathbb{Z}/p\mathbb{Z}$ are the elements a with $a^2 \equiv -1 \pmod{p}$.

   - This follows by combining parts (a) and (c): by (c), any such a must have a^2 be an element of order 2, but by (a), the only such element is -1.