E. Dummit's Math 3527 ~ Number Theory I, Spring 2026 ~ Midterm 1 Solutions (Form K)

---

1. Parts (a) and (b) were worth 5 points and part (c) was worth 2 points.

   (a) We use the Euclidean algorithm:

   $$\begin{aligned} 530 &= 5 \cdot 102 + 20 \\ 102 &= 5 \cdot 20 + 2 \\ 20 &= 10 \cdot 2 \end{aligned}$$

   The last nonzero remainder is 2, so the greatest common divisor is $\boxed{2}$.

   (b) We use the extended Euclidean algorithm to solve for the remainders one at a time. This yields

   $$\begin{aligned} 20 &= 530 - 5 \cdot 102 \\ 2 &= 102 - 5 \cdot 20 = -5 \cdot 530 + 26 \cdot 102 \end{aligned}$$

   Therefore, we can take $x = \boxed{-5}$ and $y = \boxed{26}$.

   (c) Noting that $\overline{530} \cdot \overline{102/2} = \overline{530/2} \cdot \overline{102} = \overline{530} \cdot \overline{0} = \overline{0}$ we can take $\overline{s} = \boxed{\overline{102/2} = \overline{51}}$. (In fact this is the only possible nonzero residue class that works.)

---

2. Parts (a), (b), (d), (e) were worth 2.5 points, while (c) was worth 2 points.

   (a) The greatest common divisor is $\boxed{2^3 \cdot 5^5 \cdot 7^2}$ because those are the minimum powers of each prime that appear in the factorization.

   (b) Taking the given equality modulo 2026 yields $-483 \cdot 983 \equiv 1 \pmod{2026}$, so the multiplicative inverse of 983 is $\boxed{-483}$.

   (c) By properties of order, since $25 = 5^2$ and 5 has order 1012, the order of 25 is $1012/\gcd(2, 1012) = 1012/2 = \boxed{506}$.

   (d) We have $\varphi(3500) = \varphi(2^2 \cdot 5^3 \cdot 7) = \varphi(2^2)\varphi(5^3)\varphi(7) = (2^2 - 2)(5^3 - 5^2)(7 - 1) = \boxed{1200}$.

   (e) We need 10 to have order 8 modulo p which requires $10^8 \equiv 1 \pmod{p}$ but $10^4 \not\equiv 1 \pmod{p}$, so we want a prime dividing $10^8 - 1$ but not $10^4 - 1$: the two choices are $p = \boxed{73}$ or $\boxed{137}$.

---

3. Each part was worth 3 points.

   (a) Since $\gcd(6, 63) = 3$ and 30 is divisible by 3, we may divide through by 3 to obtain the equivalent congruence $2x \equiv 10 \pmod{21}$. Then since 2 is a unit, dividing by 2 yields $\boxed{x \equiv 5 \pmod{21}}$.

   (b) We use the Chinese remainder theorem. If $x \equiv 4 \pmod{12}$ then $x = 4 + 12a$ for some $a \in \mathbb{Z}$. Plugging into the second equation yields $4 + 12a \equiv 1 \pmod{11}$, which reduces to $a \equiv -3 \pmod{11}$, meaning $a = -3 + 11b$ for some $b \in \mathbb{Z}$. Then $x = 4 + 12(-3 + 11b) = -32 + 132b$, so the solution is $\boxed{x \equiv -32 \equiv 100 \pmod{132}}$.

   (c) Since $\varphi(100) = \varphi(2^2 \cdot 5^2) = (2^2 - 2)(5^2 - 5) = 40$, by Euler's theorem we know that $17^{40} \equiv 1 \pmod{100}$. Then $17^{2000} \equiv (17^{40})^{50} \equiv 1^{50} \equiv 1 \pmod{100}$, so the remainder is $\boxed{1}$.

   (d) If $x = 0.20\overline{26}$ then $100x = 20.\overline{26}$ and $10000x = 2026.\overline{26}$ so subtracting gives $9900x = 2026 - 20 = 2006$ and so $x = \boxed{2006/9900}$.

---

4. We use (strong) induction on n.

   For the base cases $n = 0$ and $n = 1$ we have $a_0 = 5 = 2^0 + 4$ and $a_1 = 6 = 2^1 + 4$ as required.
   For the inductive step suppose $n \geq 2$ and $a_{n-1} = 2^{n-1} + 4$ and $a_{n-2} = 2^{n-2} + 4$. Then by definition $a_n = 3a_{n-1} - 2a_{n-2} = 3(2^{n-1} + 4) - 2(2^{n-2} + 4) = 3 \cdot 2^{n-1} - 2^{n-1} + 4 = 2 \cdot 2^{n-1} + 4 = 2^n + 4$, as required.
   Remark: Note that two base cases are necessary here, because the argument in the inductive step needs the formula from the two previous cases.

---

5. Solution 1: Since a divides c, $c = ka$ for some k. Then $b|(ka)$ and b is relatively prime to a, so by the relatively prime divisibility property, we see $b|k$ so $k = lb$ for some l. Then $c = ka = l(ab)$ so ab divides c.
   Solution 2: Consider prime factorizations: if $a = p_1^{a_1} \cdots p_k^{a_k}$, $b = p_1^{b_1} \cdots p_k^{b_k}$, $c = p_1^{c_1} \cdots p_k^{c_k}$ for distinct primes p_i, then $a_i \leq c_i$ and $b_i \leq c_i$ for each i since a, b both divide c. But also since a, b are relatively prime, a_i or b_i is zero for each i (otherwise p_i would divide both a, b). So this means $a_i + b_i \leq c_i$ for each i, and therefore ab divides c.

---

6. The order of 11 divides $\varphi(73) = 72$ by Euler's theorem. Using the given information, we see that $11^{24} \equiv 11^{16}11^8 \equiv 4 \cdot 2 \equiv 8 \pmod{73}$ and $11^{36} \equiv 11^{32}11^4 \equiv 16 \cdot 41 \equiv 656 \equiv -1 \pmod{73}$, so we see that the order of 11 cannot divide 24 or 36. Hence the order can only be 72, meaning 11 is a primitive root.

---

7. Each part was worth 4 points.

   (a) If p is a prime less than 61, then p is included in the product 60! so p divides 60!. But then p also divides $(60!)^{60}$ so p cannot divide $n = (60!)^{60} - 1$.

   (b) Solution 1: By Wilson's theorem, we know that $60! \equiv -1 \pmod{61}$, so $n \equiv (-1)^{60} - 1 \equiv 1 - 1 \equiv 0 \pmod{61}$, and thus 61 divides n. Since 61 divides n but no smaller prime does by (a), 61 is the smallest prime factor of n.
   Solution 2: Since 61 doesn't divide 60!, then 60! is a unit modulo 61, so by Euler's theorem $(60!)^{60} \equiv 1 \pmod{61}$. Then as in Solution 1 we conclude 61 divides n but no smaller prime does by (a).

---

8. Each part was worth 3 points. A nominally incorrect answer ("false" instead of "true" or vice versa) received credit as long as the explanation was valid.

   (a) False: we can compute gcds very quickly using the Euclidean algorithm, which is extremely fast even with large numbers (it takes at most about 5 times the number of digits in the smaller number, so only 2500 steps with 500-digit numbers: that's even feasible by hand, in principle, in a day or two).

   (b) False: although $a^{90} \equiv 1$ implies that the order of a divides 90, it is not necessarily equal to 90, as it could potentially be smaller. For example, if $a = 1$ then $a^{90} \equiv 1 \pmod{m}$, but a actually has order 1.

   (c) False: the Caesar shift is very weak and can be broken by brute force or frequency analysis.

   (d) True: as discussed extensively in class, we can use number theory and modular arithmetic to implement the Rabin and RSA cryptosystems, as well as to set up zero-knowledge protocols.
