

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

(a) We use the Euclidean algorithm:

$$\begin{aligned} 520 &= 5 \cdot 102 + 10 \\ 102 &= 10 \cdot 10 + 2 \\ 10 &= 10 \cdot 2 \end{aligned}$$

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

$$\begin{aligned} 10 &= 520 - 5 \cdot 102 \\ 2 &= 102 - 10 \cdot 10 = -10 \cdot 530 + 51 \cdot 102 \end{aligned}$$

Therefore, we can take $x = \boxed{-10}$ and $y = \boxed{51}$.

(c) Noting that $\overline{520} \cdot \overline{102/2} = \overline{520/2} \cdot \overline{102} = \overline{520} \cdot \overline{0} = \overline{0}$ we can take $\bar{s} = \boxed{\overline{102/2} = \overline{51}}$. (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 $\boxed{2^5 \cdot 3^3 \cdot 7^2}$ because those are the minimum powers of each prime that appear in the factorization.

(b) Taking the given equality modulo 2026 yields $-797 \cdot 877 \equiv 1 \pmod{2026}$, so the multiplicative inverse of 877 is $\boxed{-797}$.

(c) By order properties since $121 = 11^2$ and 11 has order 46, the order of 121 is $46/\gcd(2, 46) = 46/2 = \boxed{23}$.

(d) We have $\varphi(1500) = \varphi(2^2 \cdot 3 \cdot 5^3) = \varphi(2^2)\varphi(3)\varphi(5^3) = (2^2 - 2)(3 - 1)(5^3 - 5^2) = \boxed{400}$.

(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 3.5 points.

(a) Since $\gcd(6, 63) = 3$ and 30 is divisible by 3, we may divide through by 3 to obtain the equivalent congruence $2x \equiv 18 \pmod{21}$. Then since 2 is a unit, dividing by 2 yields $\boxed{x \equiv 9 \pmod{21}}$.

(b) We use the Chinese remainder theorem. If $x \equiv 6 \pmod{13}$ then $x = 6 + 13a$ for some $a \in \mathbb{Z}$. Plugging into the second equation yields $6 + 13a \equiv 1 \pmod{12}$, which reduces to $a \equiv -5 \pmod{12}$, meaning $a = -5 + 12b$ for some $b \in \mathbb{Z}$. Then $x = 6 + 13(-5 + 12b) = -59 + 156b$, so the solution is $\boxed{x \equiv -59 \equiv 97 \pmod{156}}$.

(c) Since $\varphi(100) = \varphi(2^2 \cdot 5^2) = (2^2 - 2)(5^2 - 5) = 40$, by Euler's theorem we know that $13^{40} \equiv 1 \pmod{100}$. Then $13^{2000} \equiv (13^{40})^{50} \equiv 1^{50} \equiv 1 \pmod{100}$, so the remainder is $\boxed{1}$.

(d) If $x = 0.\overline{2026}$ then $10x = 2.\overline{026}$ and $10000x = 2026.\overline{026}$ so subtracting gives $9990x = 2026 - 2 = 2024$ and so $x = \boxed{2024/9990 = 1012/4995}$.

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 5 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 71, then p is included in the product $70!$ so p divides $70!$. But then p also divides $(70!)^{70}$ so p cannot divide $n = (70!)^{70} - 1$.

(b) Solution 1: By Wilson's theorem, we know that $70! \equiv -1 \pmod{71}$, so $n \equiv (-1)^{70} - 1 \equiv 1 - 1 \equiv 0 \pmod{71}$, and thus 71 divides n . Since 71 divides n but no smaller prime does by (a), 71 is the smallest prime factor of n .

Solution 2: Since 71 doesn't divide $70!$, then $70!$ is a unit modulo 71, so by Euler's theorem $(70!)^{70} \equiv 1 \pmod{71}$. Then as in Solution 1 we conclude 71 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 $a^{60} \equiv 1$ implies that the order of a divides 60, it is not necessarily equal to 60, as it could potentially be smaller. For example, if $a = 1$ then $a^{60} \equiv 1 \pmod{m}$, but a actually has order 1.

(c) True: 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.
