1. Part (a) was 4 points, part (b) was 3 points, and part (c) was 5 points.
   
   (a) We use the Euclidean algorithm:
   
   
   \[
   \begin{align*}
   488 &= 4 \cdot 212 + 40 \\
   212 &= 5 \cdot 40 + 12 \\
   40 &= 3 \cdot 12 + 4 \\
   12 &= 3 \cdot 4
   \end{align*}
   \]
   
   The last nonzero remainder is 4, so the greatest common divisor is 4.
   
   (b) Because gcd(a, b) = 4 from part (a), we can see that
   
   \[
   \frac{488}{4} \cdot 212 \equiv 0 \pmod{212}.
   \]
   
   Therefore, we can take \( s = \frac{212}{4} = 53 \) (The values 106 and 159 also work.)
   
   (c) We use the extended Euclidean algorithm to solve for the remainders one at a time. This yields
   
   \[
   \begin{align*}
   40 &= 488 - \frac{212}{4} \cdot 212 \\
   12 &= 212 - 5 \cdot 40 = -5 \cdot 488 + 21 \cdot 212 \\
   4 &= 40 - 3 \cdot 12 = 16 \cdot 488 - 67 \cdot 212
   \end{align*}
   \]
   
   Therefore, we can take \( x = 16 \) and \( y = -67 \).

2. Each part was worth 3 points.
   
   (a) The greatest common divisor is \( 2^3 \cdot 3^3 \) because those are the greatest prime powers that divide both numbers.
   
   (b) Taking the given equality modulo 1412 yields 669 \cdot 477 \equiv 1 \pmod{1412}, so the multiplicative inverse of 477 is 669.
   
   (c) We have \( \varphi(9000) = \varphi(2^3 \cdot 3^2 \cdot 5^3) = \varphi(2^3) \varphi(3^2) \varphi(5^3) = (2^3 - 2^2)(3^2 - 3)(5^3 - 5^2) = 2400 \).
   
   (d) Since 2 is a primitive root, its order is \( \varphi(2027) = 2026 \) since 2027 is prime. Then the order of \( 8 = 2^3 \) is
   
   \[ 2026 / \gcd(3, 2026) = 2026 \]
   
   by using the fact that if \( u \) has order \( n \), then \( u^k \) has order \( n / \gcd(k, n) \).
   
   (e) We need to find a prime such that 10 has order 11 modulo \( p \), which requires \( 10^{11} \equiv 1 \pmod{p} \), so that \( p \) divides \( 10^{11} - 1 \). Since 1/3 has period 1, the possibilities are \( p = 21649 \) or \( p = 513239 \) (The information about the factorization of \( 10^{10} - 1 \) was only provided to make guessing harder.)

3. Each part was worth 4 points.
   
   (a) We use the Chinese remainder theorem. If \( x \equiv 11 \pmod{12} \) then \( x = 11 + 12a \) for some \( a \in \mathbb{Z} \). Plugging into the second equation yields \( 11 + 12k \equiv 4 \pmod{11} \), which reduces to \( a \equiv 4 \pmod{11} \), meaning \( a = 4 + 11b \) for some \( b \in \mathbb{Z} \). Then \( x = 11 + 12(4+11b) = 59 + 132b \), so the solution is \( x = 59 \pmod{132} \).
   
   (b) Since 71 is prime, by Fermat’s little theorem we know that \( 2^{71} \equiv 2 \pmod{71} \). Thus, \( 2^{72} \equiv 2 \cdot 2^{71} \equiv 4 \pmod{71} \) as claimed. Alternatively, we could do successive squaring (though it would take a little while to do it by hand!)
   
   (c) Since \( \varphi(81) = \varphi(3^4) = 3^4 - 3^3 = 54 \), by Euler’s theorem we know that \( 7^{54} \equiv 1 \pmod{81} \). Then \( 7^{108} \equiv (7^{54})^2 \equiv 1 \pmod{81} \) as claimed.
   
   (d) The order of 2 divides \( \varphi(11) = 10 \). Since \( 2^{10} \equiv 1 \pmod{81} \) by Euler (or a direct check), but \( 2^5 \equiv 10 \) and \( 2^2 \equiv 4 \), we see that the order of 2 must in fact equal 10, hence it is a primitive root.
4. We use induction on $n$.

- **Base case:** $n = 1$. We see $a_1 = 1 = 3^1 - 2$ as claimed.
- **Inductive step:** suppose $a_{n-1} = 3^{n-1} - 2$ for some $n \geq 2$. Then $a_n = 3a_{n-1} + 4 = 3(3^{n-1} - 2) + 4 = 3^n - 6 + 4 = 3^n - 2$, as claimed.
- Hence by induction, the result holds for every positive integer $n$.

5. Per the hint, we show that $a^6 - a^2 \equiv 0 \mod 3$ and $\mod 4$ separately.

- One approach is just to test all possible residue classes modulo 3 and modulo 4: $0^6 - 0^2 = 0$, $1^6 - 1^2 = 0$, $2^6 - 2^2 = 60$, and $3^6 - 3^2 = 720$ are all congruent to 0 mod 3 and to 0 mod 4. Since the result holds for every residue class modulo 3 and modulo 4, we see that $a^6 - a^2$ is divisible by both 3 and 4, hence is always divisible by 12.
- Another approach is to use Fermat and Euler: we know $a^3 \equiv a \pmod{3}$ by Fermat, so $a^6 \equiv a^4 \equiv a^2 \pmod{3}$, so 3 divides $a^6 - a^2$. Likewise, if $a$ is even then $a^2 \equiv a^4 \pmod{4}$, and if $a$ is odd then $a^4 \equiv a^2 \equiv 1 \pmod{4}$ by Euler. In either case $a^4 \equiv a^2 \pmod{4}$, so then $a^6 \equiv a^4 \equiv a^2 \pmod{4}$ as claimed.
- A third approach is to factor: notice that $a^6 - a^2 = a^2(a - 1)(a + 1)(a^2 + 1)$. At least one of the terms $a - 1, a, a+1$ is always divisible by 3, and at least two of them (either $a^2$ or $(a - 1)(a + 1)$) must be even, so the product is also divisible by 4.

6. Each part was worth 3 points. Partial credit was given for technically wrong answers (e.g., “False” to a problem with a technically “True” answer) if the explanation was correct and provided relevant information.

(a) **False** the Caesar shift can be broken just by writing down all 26 possible decryptions of any given ciphertext. It is also a substitution cipher, so it is also susceptible to frequency analysis. (It is, in fact, essentially the least secure cryptosystem ever designed!)

(b) **False** although it is true that breaking Rabin encryption is equivalent to factorization, that does not mean it is secure. It is very susceptible to a chosen-ciphertext attack, as we discussed in class. Furthermore, it is still not “completely secure” because it can still be broken (namely, by factoring the modulus, which can be done given enough time!).

(c) **False** if $a^{200} \equiv 1 \pmod{m}$ then all we can say for sure is that the order of $a$ divides 200. It need not actually equal 200 (for example, $a$ could equal 1, and then its order would be 1, not 200).

(d) **True** in general, it is expected that unless Alice or Bob made some mistake with their implementation of RSA, then it would be very difficult for Eve to decode Alice’s message using only a direct attack (e.g., factoring Bob’s modulus).

(e) **True** Peggy and Victor could use a zero-knowledge proof protocol, as we discussed in class, in which Peggy can prove that she knows a secret without allowing Eve or Victor to gain any useful information about the secret itself.

(f) **False** a test like the Fermat or Miller-Rabin test can prove that a large integer is composite without finding a factorization.

(g) **False** there are numerous general-purpose factorization algorithms (Pollard $p - 1$, Pollard $\rho$, elliptic curve, quadratic sieve) that are much faster than trial division.