1. You know of course that 10 is not a prime number. But pretend that you don't know that already. Use a primality test based on Fermat's Little Theorem to discover that 10 is not prime. In other words, find an integer a coprime to 10 for which

$$a^{10-1} \not\equiv 1 \bmod 10.$$

Try $a = 3$:

$3^9 \equiv 3 \cdot 3^8 \equiv 3 \cdot (3^4)^2 \equiv 3 \cdot (81)^2 \equiv 3 \cdot (1)^2 \equiv 3 \bmod 10$. Thus $3^{10-1} \not\equiv 1 \bmod 10$.

2. Let p be a prime of the form $4k + 3$ for some $k \in \mathbb{Z}$. Let a and b be two integers. Prove that if

$$a^2 + b^2 \equiv 0 \bmod p, \qquad (\star)$$

then $a \equiv 0 \bmod p$ and $b \equiv 0 \bmod p$.

Suppose (aiming for a contradiction) that $b \not\equiv 0 \bmod p$. Then b has a multiplicative inverse modulo p. Multiplying both sides of equation $(\star)$ by $(b^{-1})^2$, we get

$$(b^{-1})^2 a^2 + (b^{-1})^2 b^2 \equiv 0 \bmod p$$
$$(b^{-1}a)^2 + 1 \equiv 0 \bmod p$$

Thus we get a solution to $x^2 + 1 \equiv 0 \bmod p$. (Namely, $x = b^{-1}a$.) We saw in class that $x^2 + 1 \equiv 0 \bmod p$ has a solution for an odd prime p if and only if p is of the form $4k+1$. However we are given that $p = 4k + 3$. This is a contradiction, so the original assumption $b \not\equiv 0 \bmod p$ must be invalid.

Similarly, if we assume that $a \not\equiv 0 \bmod p$, we can multiply both sides by $(a^{-1})^2$ and get a contradiction.

3. Bob picks an secret integer M between 1 and 10. He wants to securely send this number to Alice using RSA public key cryptography. Alice picks two primes $p = 17$ and $q = 23$ and defines $a = pq = 391$ and $b = (p - 1)(q - 1) = 352$. She picks the encryption key $e = 141$, which is a valid choice because $(e, b) = (141, 352) = 1$. Alice releases the encryption tools $e = 141$ and $a = 352$ to the public.

Bob encrypts M using the encryption tools and obtains the encrypted number $N = 9$, which he sends over to Alice.

(a) Alice calculates the decryption key as $d = 5$. Verify that Alice's calculation is correct. In other words, show that $d = 5$ is indeed the decryption key associated to the encryption key $e = 141$ by confirming that $ed \equiv 1 \bmod b$.

(b) Alice uses the decryption key to decrypt $N = 9$, and she obtains M. What is the value of M?

(a) $5 \cdot 141 = 705 \equiv 1 \bmod 352$

(b) $9^5 = 59049 \equiv 8 \bmod 391$.

Therefore $M = 8$.

4. Find the prime factorization of 360. Use it to calculate:
(a) $d(360)$

(b) $\sigma(360)$
(c) $\phi(360)$.

$360 = 2^3 \cdot 3^2 \cdot 5^1$.

(a) $d(360) = d(2^3)d(3^2)d(5) = (3+1)(2+1)(1+1) = 24$.

(b) $\sigma(360) = \sigma(2^3)\sigma(3^2)\sigma(5) = \frac{2^{3+1}-1}{2-1}\frac{3^{2+1}-1}{3-1}\frac{5^{1+1}-1}{5-1} = 1170$.

(c) $\phi(360) = \phi(2^3)\phi(3^2)\phi(5) = 2^{3-1}(2-1) \cdot 3^{2-1}(3-1) \cdot (5-1) = 96$.

5. Use Euler's theorem to find the last three digits of $(13)^{802}$.

This is equivalent to finding the least residue of $(13)^{802}$ modulo 1000.

$1000 = 2^3 \cdot 5^3 \implies \phi(1000) = \phi(2^3)\phi(5^3) = 2^{3-1}(2-1)5^{3-1}(5-1) = 400$

Since $(13, 1000) = 1$, Euler's theorem implies $13^{\phi(1000)} \equiv 1 \bmod 1000$. Thus $13^{400} \equiv 1 \bmod 1000$.

So $(13)^{802} = 13^{400 \cdot 2+2} = (13^{400})^2 13^2 \equiv 1^2 13^2 \equiv 169 \bmod 1000$.

The last three digits are 169.

6. (a) Prove that if n is odd, then $\phi(2n) = \phi(n)$.

(b) Prove that if n is even, then $\phi(2n) = 2\phi(n)$.

(a) If n is odd then it is coprime with 2. Hence by the multiplicative property of the ϕ function, we get $\phi(2n) = \phi(2)\phi(n) = (2-1)\phi(n) = \phi(n)$.

(b) Write $n = 2^k m$, where $k \geq 1$ and m is odd. Then by the multiplicative property of the ϕ function, we get

$\phi(2n) = \phi(2^{k+1}m) = \phi(2^{k+1})\phi(m) = 2^{k+1-1}(2-1)\phi(m) = 2^k\phi(m) = 2 \cdot 2^{k-1}(2-1)\phi(m) = 2\phi(2^k)\phi(m) = 2\phi(2^k m) = 2\phi(n)$.