1. Calculate each of the following things:

   (a) The values of $\varphi(101)$, $\varphi(40000)$, and $\varphi(6^{10})$.

   - We have $\varphi(101) = \boxed{100}$ since 101 is prime.
   - Also, $\varphi(40000) = \varphi(2^6 5^4) = (2^6 - 2^5)(5^4 - 5^3) = 32 \cdot 500 = \boxed{16000}$.
   - Likewise, $\varphi(6^{10}) = \varphi(2^{10}3^{10}) = (2^{10} - 2^9)(3^{10} - 3^9) = \boxed{2^{10}3^9}$.

   (b) The number of positive integers less than or equal to 2025 that are relatively prime to 2025.

   - This is asking for the value of $\varphi(2025) = \varphi(3^4 5^2) = (3^4 - 3^3)(5^2 - 5^1) = \boxed{1080}$.

   (c) The last two digits of 519^{242} when it is written out in base 10.

   - This is asking us to find a two-digit integer congruent to 519^{242} (mod 100).
   - By Euler's theorem, we have $519^{40} \equiv 1 \pmod{100}$.
   - So $519^{242} \equiv 519^2 \cdot (519^{40})^6 \equiv 19^2 \cdot 1^6 \equiv 361 \equiv \boxed{61} \pmod{100}$.

   (d) A unit that has order $\varphi(18)$ modulo 18.

   - Equivalently, we want a primitive root mod 18. There are 6 units mod 18: 1, 5, 7, 11, 13, 17.
   - It is easy to compute their orders as 1, 6, 3, 6, 3, 2. Thus, there are two answers: $\boxed{5}$ or $\boxed{11}$.

   (e) The order of 10 modulo 41.

   - By Fermat (or Euler), the order of 10 divides $\varphi(41) = 40$, and $10^{40} \equiv 1 \pmod{41}$.
   - Using successive squaring we can compute $10^{40/2} \equiv 10^{20} \equiv 1 \pmod{41}$ and $10^{40/5} \equiv 10^8 \equiv 16 \pmod{41}$, so the order of 10 in fact divides 20.
   - Then we can compute $10^{20/2} \equiv 10^{10} \equiv 1 \pmod{41}$ so the order divides 10, and in fact $10^{10/2} \equiv 10^5 \equiv 1 \pmod{41}$ so the order divides 5. Since the order is not 1, we conclude that 10 has $\boxed{\text{order } 5}$.

   (f) The order of 10 modulo 89.

   - By Fermat (or Euler), the order of 10 divides $\varphi(89) = 88$, and $10^{88} \equiv 1 \pmod{89}$.
   - Using successive squaring we can compute $10^{88/2} \equiv 10^{44} \equiv 1 \pmod{89}$ and $10^{88/11} \equiv 10^8 \equiv 45 \pmod{89}$. Hence the order in fact divides 44.
   - Then we can find $10^{44/2} \equiv 10^{22} \equiv -1 \pmod{89}$ and $10^{44/11} \equiv 10^4 \equiv 32 \pmod{89}$. Since neither of these is congruent to 1, we conclude that the order cannot divide 22 or 4, so 10 has $\boxed{\text{order } 44}$.

---

2. Calculate each of the following things:

   (a) The rational number with decimal expansion $0.\overline{2026}$.

   - If $x = 0.\overline{2026}$ then $10^4 x = 2026.\overline{2026}$ so $(10^4 - 1)x = 2026$ and so $x = \boxed{\dfrac{2026}{9999}}$.

   (b) The rational number with decimal expansion $0.\overline{123456789}$.

   - If $x = 0.\overline{123456789}$ then $(10^9 - 1)x = 123456789$ so $x = \boxed{\dfrac{123456789}{999999999} = \dfrac{13717421}{111111111}}$.

   (c) The rational number with decimal expansion $3.14\overline{592}$.

   - If $x = 3.14\overline{592}$ then $(10^5 - 10^2)x = 314592 - 314 = 314278$ so $x = \boxed{\dfrac{314278}{99900} = \dfrac{4247}{1350}}$.

   (d) The period of the repeating decimal 9/41 and its expansion. [Hint: See 1e.]

   - The period is the order of 10 modulo 41, which was calculated in 1e to be $\boxed{5}$.

- Then the repeating part is $\frac{9}{41}(10^5-1) = 21951$, so $\frac{9}{41} = \boxed{0.\overline{21951}}$.

(e) The period of the repeating decimal 7/89. [Hint: See 1f.]

- The period is the order of 10 modulo 89, which was calculated in 1f as $\boxed{44}$.
- Indeed, one can evaluate $7/89 = 0.\overline{4494382022471910112359550561797752808988764}$.

(f) The period of the repeating decimal 4/23.

- The period is the order of 10 modulo 23. This order divides $\varphi(23) = 22$.
- Since $10^{22/2} \equiv 10^{11} \equiv -1 \pmod{23}$ and $10^{22/11} \equiv 10^2 \equiv 8 \pmod{23}$, the order must be $\boxed{22}$.
- Indeed, one can evaluate $4/23 = 0.\overline{1739130434782608695652}$.

(g) All primes p such that $1/p$ has a repeating decimal expansion of period exactly 5.

- If $1/p$ has period 5, then p must divide $10^5 - 1 = 9 \cdot 11111 = 3^2 \cdot 41 \cdot 271$.
- Since $1/3$ has period 1, we see that $p = \boxed{41,\ 271}$. Indeed, $1/41 = 0.\overline{02439}$ and $1/271 = 0.\overline{00369}$.

(h) All primes p such that $1/p$ has a repeating decimal expansion of period exactly 6.

- If $1/p$ has period 6, then p must divide $10^6 - 1 = 3^3 \cdot 7 \cdot 11 \cdot 13 \cdot 37$.
- Since $1/3$ has period 1, $1/11 = 0.\overline{09}$ has period 2, and $1/37 = 0.\overline{027}$ has period 3, we see that $p = \boxed{7,\ 13}$. Indeed, $1/7 = 0.\overline{142857}$ and $1/13 = 0.\overline{076923}$.

---

3. Find the following things, and include relevant justification (you can just give the results of the needed modular exponentiations; you do not need to give details of the calculations):

(a) The order of 5 modulo 97.

- By Fermat (or Euler), the order of 5 divides $\varphi(97) = 96$, and $5^{96} \equiv 1 \pmod{97}$.
- Using successive squaring we can compute $5^{96/2} \equiv 5^{48} \equiv -1 \pmod{97}$ and $5^{96/3} \equiv 5^{32} \equiv 35 \pmod{97}$. Hence the order cannot divide 48 or 32, and so 5 must have $\boxed{\text{order } 96}$.

(b) The order of 5 modulo 102.

- By Euler, the order of 5 divides $\varphi(102) = \varphi(2 \cdot 3 \cdot 17) = 32$, and $5^{32} \equiv 1 \pmod{102}$.
- Then $5^2 \equiv 25$, $5^4 \equiv 13$, $5^8 \equiv 67$, $5^{16} \equiv 1 \pmod{102}$. Hence 5 has $\boxed{\text{order } 16}$.

(c) The order of 2 modulo 81.

- By Euler, the order of 2 divides $\varphi(81) = \varphi(3^4) = 3^4 - 3^3 = 54$, and $2^{54} \equiv 1 \pmod{81}$.
- Using successive squaring we can compute $2^{54/2} \equiv 2^{27} \equiv -1 \pmod{81}$ and $2^{54/3} \equiv 2^{18} \equiv 28 \pmod{81}$. Hence the order cannot divide 27 or 18, and so 2 must have $\boxed{\text{order } 54}$.

(d) The order of 5 modulo 2026.

- By Euler, the order of 5 divides $\varphi(2026) = (2-1)(1013-1) = 1012$, and $5^{1012} \equiv 1 \pmod{2026}$. Note $1012 = 2^2 \cdot 11 \cdot 23$.
- Using successive squaring we can compute $5^{1012/2} \equiv 5^{506} \equiv -1 \pmod{2026}$, $5^{1012/11} \equiv 5^{92} \equiv 1127 \pmod{2026}$, and $5^{1012/23} \equiv 5^{44} \equiv 1105 \pmod{2026}$, so the order cannot divide 1012/2, 1012/11, or 1012/23. Hence 5 has $\boxed{\text{order } 1012}$.

(e) Which of the elements from (a)-(d) are primitive roots?

- A primitive root has order $\varphi(m)$ mod m: so (a) yes, (b) no, (c) yes, (d) yes.

---

4. The message **WKHYHUBEHVWGRJVDUHVLEHULDQKXVNLHV** has been encrypted using a Caesar shift. Decode it.

- By writing down all 26 possible shifts of this message, we see there is only one that makes sense, the shift backward by 3 letters. Alternatively, one could use a frequency analysis: the letter **H** appears 6 times, more than any other letter, which suggests that it decodes to **e**.
- Either way, the decrypted message is $\boxed{\textbf{theverybestdogsaresiberianhuskies}}$, which is unarguably true.

---

5. Consider the Rabin cryptosystem with key $N = 1359692821 = 32359 \cdot 42019$.

   (a) Encode the plaintext $m = 117285016$.

   - We simply compute $m^2 \pmod{N}$, which PowerMod gives as $\boxed{654306931}$.

   (b) Find the four decodings of the ciphertext $c = 823845737$.

   - We wish to solve $m^2 \equiv c \pmod{p}$ and $m^2 \equiv c \pmod{q}$ and combine the results.
   - Since $p \equiv q \equiv 3 \pmod{4}$, we know that the solutions are $m = \pm c^{(p+1)/4} \pmod{p}$ and $m = \pm c^{(q+1)/4} \pmod{q}$.
   - We then compute $c^{(p+1)/4} \equiv 32225 \pmod{p}$ and $c^{(q+1)/4} \equiv 9955 \pmod{q}$ via PowerMod.
   - Solving the simultaneous congruences $m \equiv 32225 \pmod{32359}$, $m \equiv 9955 \pmod{42019}$ via ChineseRemainder yields $m \equiv 547643582 \pmod{N}$.
   - Solving $m \equiv 32225 \pmod{32359}$, $m \equiv -9955 \pmod{42019}$ likewise yields $m \equiv 929156192 \pmod{N}$.
   - Thus the four solutions are ± 547643582 and $\pm 929156192 \pmod{N}$.
   - Equivalently: $m = \boxed{430536629,\ 537643582,\ 812049239,\ 929156192}$.

6. Consider the RSA cryptosystem with key $N = 1085444233 = 31907 \cdot 34019$ and encryption exponent $e = 3$.

   (a) Encrypt the plaintext $m = 277891194$.

   - We simply compute $m^e \pmod{N}$ using PowerMod: we obtain $\boxed{604479369}$.

   (b) Find a decryption exponent d.

   - We need to solve $de \equiv 1 \pmod{\varphi(N)}$.
   - First we observe $\varphi(N) = 1085378308$.
   - So we want to find the inverse of 3 modulo $\varphi(N)$: this is $\boxed{723585539}$ again via PowerMod.

   (c) Decrypt the ciphertext $c = 878460400$.

   - We simply compute $m^d \pmod{N}$ using PowerMod, giving $\boxed{605435934}$.

7. Let $p = 2029$. Notice that p is prime and also that the prime factorization of $p - 1$ is $2028 = 2^2 \cdot 3 \cdot 13^2$.

   (a) Show that 2 is a primitive root modulo p. (You can just give the results of the needed modular exponentiations; you do not need to give details of the calculations.)

   - By Euler's Theorem, since $\varphi(2029) = 2^2 \cdot 3 \cdot 13^2$ and $2^{2028} \equiv 1 \pmod{2029}$, we just need to show that $2^{2028/2}$, $2^{2028/3}$, and $2^{2028/13}$ are not congruent to 1 modulo p.
   - Successive squaring yields $2^{2028/2} \equiv -1 \pmod{2029}$, $2^{2028/3} \equiv 975 \pmod{2029}$, and $2^{2028/13} \equiv 302 \pmod{2029}$. Since none of these is $1 \pmod{p}$, we see that $\boxed{\text{2 is a primitive root}}$.

   (b) Find all four solutions to the congruence $x^4 \equiv 1 \pmod{p}$.

   - We can solve the congruence by taking discrete logarithms to the base 2. This yields $4 \log_2(x) \equiv 0 \pmod{2028}$. (Remember that discrete logarithms yield congruences modulo $\varphi(p)$ in general.)
   - Since $\gcd(4, 2028) = 4$, dividing through by 4 yields $\log_2(x) \equiv 0 \pmod{507}$, which has the four solutions $\log_2 x \equiv 0,\ 507,\ 1014,\ 1521 \pmod{2028}$.
   - Then $x \equiv \boxed{2^0,\ 2^{507},\ 2^{1014},\ 2^{1521}} \pmod{p}$. Equivalently, this is $x = \boxed{1,\ 992,\ 2028,\ 1037} \pmod{p}$.

   (c) Find both solutions to the congruence $x^2 \equiv 3 \pmod{p}$, given that $3 \equiv 2^{1980} \pmod{p}$.

   - We can solve the congruence by taking discrete logarithms to the base 2.
   - From the given information we know that $x^2 \equiv 2^{1980} \pmod{2028}$, so taking logarithms yields the equality $2 \log_2(x) \equiv 1980 \pmod{2028}$.
   - Cancelling the factor of 2 yields $\log_2(x) \equiv 990 \pmod{1014}$, which has the two solutions $\log_2 x \equiv 990,\ 2004 \pmod{2028}$.
   - Then $x \equiv \boxed{2^{990},\ 2^{2004}} \pmod{p}$. Equivalently, this is $x = \boxed{1755,\ 274} \pmod{p}$.

8. Let $p > 2$ be a prime.

   (a) Show that the only solutions of the congruence $x^2 \equiv 1 \pmod{p}$ are $x \equiv 1$ and $x \equiv -1 \pmod{p}$.

   - Clearly both values are solutions. Conversely, suppose $x^2 \equiv 1 \pmod{p}$, so that $p|(x^2-1)$. Factoring yields $p|(x-1)(x+1)$.
   - Since p is prime, by the prime divisibility property we deduce that $p|(x-1)$ or $p|(x+1)$, which is to say, $x \equiv 1$ or $-1 \pmod{p}$.)

   (b) Suppose a has even order $2k$ modulo p. Prove that $a^k \equiv -1 \pmod{p}$. [Hint: Let $x = a^k$ and consider x^2 mod p.]

   - Let $x = a^k$: then $x^2 \equiv a^{2k} \equiv 1 \pmod{p}$ since a has order $2k$. So by part (a), that means $x \equiv 1$ (mod
   - We cannot have $x \equiv 1 \pmod{p}$ since $x^k \equiv 1 \pmod{p}$ would contradict the order being $2k$, so we must have $x \equiv -1 \pmod{p}$.

---

9. The goal of this problem is to show that if $N = pq$ is an Rabin/RSA modulus, then computing $\varphi(N)$ is equivalent to factoring N.

   (a) Suppose that $N = pq$ and $\varphi = (p-1)(q-1)$, where p, q are real numbers. Find a formula for p and q in terms of N and φ.

   - Since $N = pq$ we have $q = N/p$, and substituting into the equation for φ gives $\varphi = (p-1)(N/p-1)$.
   - Multiplying by p and rearranging yields the quadratic equation $p^2 - (N - \varphi + 1)p + N = 0$, whose roots are $p, q = \boxed{\dfrac{(N-\varphi+1) \pm \sqrt{(N-\varphi+1)^2 - 4N}}{2}}$ by the quadratic formula.

   (b) Deduce that if $N = pq$ is a product of two primes, then factoring N is equivalent to computing $\varphi(N)$.

   - If we know the factorization of N then we certainly can compute $\varphi(N) = (p-1)(q-1)$.
   - Conversely, by part (a), if we know N and $\varphi(N)$, then we can compute p and q.

   (c) Given the information that N is a product of two primes, where

$$\begin{aligned} N &= 22592848554175369912787642584639796662881202104422604037797641281978785567961 \\ \varphi(N) &= 22592848554175369912787642584639796662567375207606558304355492609701088213924 \end{aligned}$$

   find the prime factors of N. (You can just give the first six and last six digits of each: e.g., as $123456 \ldots 135791$.)

   - We can simply use the formula from (a), since if $N = pq$ then $\varphi(N) = (p-1)(q-1)$. This gives

$$\begin{aligned} p, q &= \frac{1}{2}[313826896816045733442148672277697354038 \pm 90088439594031908479910431243860913440] \\ &= \boxed{111869228611006912481119120516918220299,\ 201957668205038820961029551760779133739}. \end{aligned}$$
