Name: Solutions

Directions: Show all work. No credit for answers without work.

1. **[15 points]** Solve the following system of congruences.

$$x \equiv 1 \pmod{41} \qquad x \equiv 2 \pmod{25} \qquad x \equiv 3 \pmod{11}$$

41: prime, $25 = 5^2$, 11: prime.

$M = 41 \cdot 5^2 \cdot 11 = 11275$

i	m_i	M/m_i	M/m_i mod m_i	$(M/m_i)^{-1}$ mod m_i	target
1	41	275	29	17	1
2	25	451	1	1	2
3	11	1025	2	6	3
		*		*	*

$41 = (1)(29) + 12$
$29 = (2)(12) + 5$
$12 = (2)(5) + 2$
$5 = (2)(2) + 1$

$1 = 5 - (2)(2)$
$= 5 - (2)[12 - (2)(5)]$
$= (5)(5) - (2)(12)$
$= (5)[29 - (2)(12)] - (2)(12)$
$= (5)(29) - (12)(12)$
$= (5)(29) - (12)[41 - (1)(29)]$
$= (17)(29) - (12)(41)$

So $(29)^{-1} = 17 \pmod{41}$

$1^{-1} = 1 \pmod{25}$

2^{-1} mod 11:

$11 = (5)(2) + 1$
$1 = 11 - (2)(5)$
$2^{-1} = -5 = 6 \pmod{11}$

So $x = 275 \cdot 17 \cdot 1$
$+ 451 \cdot 1 \cdot 2$
$+ 1025 \cdot 6 \cdot 3$
$= 4675 + 902$
$+ 18450$
$= 24027 = \boxed{1477}$ mod M

2. **[10 points]** Let $n = 61 \cdot 67 = 4087$. Both 1 and -1 are solutions to $x^2 \equiv 1 \pmod{n}$. ~~Find a~~ (only explain) Explain how to find third, distinct solution modulo n or explain why no additional solutions exist.

$$x^2 \equiv 1 \pmod{61 \cdot 67} \iff \begin{cases} x^2 \equiv 1 \mod 61 \\ x^2 \equiv 1 \mod 67 \end{cases} \quad \text{By CRT}$$

$$\iff \begin{cases} x \equiv \pm 1 \mod 61 \\ x \equiv \pm 1 \mod 67 \end{cases}$$

Since $x^2 \equiv 1 \pmod{p}$ is equivalent to $x \equiv \pm 1$ when p is prime.

Taking $x \equiv 1$ mod 61 and $x \equiv 1$ mod 67 leads to the soln $x \equiv 1$ mod n, and taking $x \equiv -1$ mod 61 and $x \equiv -1$ mod 67 leads to the soln $x \equiv -1$ mod n. To get a third soln, we solve $x \equiv 1 \pmod{61}$ $x \equiv -1 \pmod{67}$ using the CRT.

i	m_i	M/m_i	M/m_i mod m_i	$(M/m_i)^{-1}$ mod m_i	target
1	61	67	6	-10	1
2	67	61	61	11	-1
		*		*	*

$61 = (10)(6) + 1$
$61 - (10)(6) = 1$
$6^{-1} = -10 \pmod{61}$

$67 = (1)(61) + 6$
$61 = (10)(6) + 1$
$1 = 61 - (10)(6)$
$= 61 - (10)[67 - (1)(61)]$
$= (11)(61) - (10)(67)$

So $x = (67)(-10)(1) + (61)(11)(-1) = -670 - 671 = -1341 \equiv \boxed{2746}$ mod n.

OR: $x \equiv -1 \pmod{61}$ $x \equiv 1 \pmod{67}$ gives $x \equiv -2746 \equiv \boxed{1341}$.

3. [**15 points**] Note that 149 is prime. Solve for x in $x^{39} \equiv 33 \pmod{149}$.

$N' = \phi(N) = N - 1 = 148$

Need $(39)^{-1} \bmod N'$:

$$148 = (3)(39) + 31$$
$$39 = (1)(31) + 8$$
$$31 = (3)(8) + 7$$
$$8 = (1)(7) + 1$$

$$\begin{aligned} 1 &= 8 - (1)(7) \\ &= 8 - (1)[31 - (3)(8)] \\ &= (4)(8) - (1)(31) \\ &= (4)[39 - (1)(31)] - (1)(31) \\ &= (4)(39) - (5)(31) \\ &= (4)(39) - (5)[148 - (3)(39)] \\ &= (19)(39) - (5)(148) \end{aligned}$$

So $39^{-1} = 19 \pmod{148}$.

$$x^{39} = 33 \pmod{149}$$
$$x^{39 \cdot 19} = (33)^{19} \pmod{149}$$
$$x^{1 + 5 \cdot 148} = (33)^{19} \pmod{149}$$
$$x = (33)^{19}$$

Fast power, mod 149:

$$(33)^1 = 33$$
$$(33)^2 = 1089 = 46$$
$$(33)^4 = (46)^2 = 2116 = 30$$
$$(33)^8 = (30)^2 = 900 = 6$$
$$(33)^{16} = 6^2 = 36$$

$$19 = 16 + 2 + 1$$

$$\begin{aligned} (33)^{19} &= (33)^{16} \cdot (33)^2 \cdot (33) \\ &= 36 \cdot 46 \cdot 33 \\ &= 54648 = \boxed{114} \pmod{149} \end{aligned}$$

4. [**5 points**] Alice claims she has access to the private key (N, d) associated with the RSA public key (N, e). How can Alice prove this to Eve, an untrusted third party, without compromising the security of her private key or previously encrypted messages?

Alice and Eve agree on a message like "I'm Alice 28", where the number 28 is chosen by Eve. The message is converted to a number $m \in \mathbb{Z}_N$ with the chosen encoding scheme, and Alice encerypts / signs m with her private key, generating $s = m^d \pmod N$. Alice sends s to Eve. Eve then checks if $s^e = m$. If so, Eve can be confident that Alice knows (N, d). Crucially, the message m is determined jointly and not just by one party.

5. [**5 points**] To make an RSA public/private key pair, Bob picks $p = 83$ and $q = 67$. For his public exponent, Bob wants to pick e such that $36 \le e \le 44$. Which of these values, if any, is possible, and why?

RSA requires $\gcd(e, N') = 1$, so that e has an inverse modulo N'.

Here $N' = (p-1)(q-1) = 82 \cdot 66 = 2 \cdot 41 \cdot 6 \cdot 11 = 2^2 \cdot 3 \cdot 11 \cdot 41$. So we need $2 \nmid e$, $3 \nmid e$, $11 \nmid e$, $41 \nmid e$.

So:

$$\begin{array}{ccccccccc} \cancel{36}, & 37, & \cancel{38}, & \cancel{39}, & \cancel{40}, & \cancel{41}, & \cancel{42}, & 43, & \cancel{44} \\ \uparrow & & \uparrow & \uparrow & \uparrow & \uparrow & \uparrow & & \uparrow \\ 2 & \checkmark & 2 & 3 & 2 & 41 & 2 & \checkmark & 2 \end{array}$$

So the valid choices are $e = 37$ and $e = 43$.

6. Alice generates an RSA key pair with $N = pq = 47 \cdot 41 = 1927$ and $e = 9$.

   (a) [**9 points**] What is Alice's private key? $N' = (p-1)(q-1) = 1840$

$d \cdot 9 \equiv 1 \pmod{1840}$

$1840 = (204)(9) + 4$

$9 = (2)(4) + 1$

$1 = 9 - (2)(4)$

$= 9 - (2)[1840 - (204)(9)]$

$= (409)(9) - (2)(1840).$

So $d = 409 \bmod N'$ and Alice's private key is

$(N, d) = \boxed{(1927, 409)}.$

   (b) [**8 points**] Bob wishes to encrypt and send Alice the message $m = 1718$. What should he send?

$C = m^e \pmod N$

$(1718)^2 = 1287$

$(1718)^4 = (1287)^2 = 1076$

$(1718)^8 = (1076)^2 = 1576$

$9 = 8 + 1$

$C = (1718)^9$

$= (1718)^8 \cdot 1718$

$= 1576 \cdot 1718$

$= \boxed{133}$

   (c) [**8 points**] Alice receives the ciphertext $c = 981$ from Bob. What is the corresponding plaintext? You may find the following table of powers of c modulo N useful. The first few values have been filled in.

t	1	2	4	8	16	32	64	128	256	512	1024
$c^t \pmod N$	981	788	450	165	247	1272	1231	739	780		

Need $c^d \bmod N$

$d = 409 = 256 + 128 + 16 + 8 + 1$

$c^{128} = (1231)^2 = 739$

$c^{256} = (739)^2 = 780$

$c^d = c^{256} \cdot c^{128} \cdot c^{16} \cdot c^8 \cdot c$

$= (780 \cdot 739)\, c^{16} \cdot c^8 \cdot c$

$= (247 \cdot 247) \cdot c^8 \cdot c$

$= (1272 \cdot 165) \cdot c$

$= 1764 \cdot 981$

$= \boxed{38}$

7. Let $n = 481$ and let $a = 11$.

   (a) **[10 points]** Execute a Miller–Rabin primality test on n with base a. It may be useful to know that $a^{15} \equiv 369 \pmod{n}$.

$n-1 = 480 = 2^5 \cdot 15 = 32 \cdot 15$. Modulo n.

a^{15}	$a^{2\cdot 15}$	$a^{4\cdot 15}$	$a^{8\cdot 15}$	$a^{16\cdot 15}$	$a^{32\cdot 15}$
369	38	1	1	1	1

   (b) **[5 points]** Is a a Miller–Rabin witness for n? What does this tell us about the primality of n? Explain.

$\boxed{\text{Yes}}$, a is a Miller–Rabin witness. Since $a^{15} \neq \pm 1$ and none of $a^{2^j \cdot 15}$ is -1 for $1 \le j \le 4$, we have a Miller–Rabin witness and so $\boxed{n \text{ is not prime}}$.

8. **[10 points]** Let E be the elliptic curve $y^2 = x^3 - 4x + 19$, let $P = (-3, 2)$, and let $Q = (1, 4)$. Find PQ.

$\lambda = \dfrac{y_2 - y_1}{x_2 - x_1} = \dfrac{4-2}{1-(-3)} = \dfrac{2}{4} = \dfrac{1}{2}$

$y = \lambda x + b$

$2 = \frac{1}{2}(-3) + b$

$b = 2 + \frac{3}{2} = \frac{7}{2}$

$L: \; y = \frac{1}{2}x + \frac{7}{2}$

$(\frac{1}{2}x + \frac{7}{2})^2 = x^3 - 4x + 19$

$0 = x^3 - \frac{1}{4}x^2 + \ldots$

$x_3 = \lambda^2 - x_1 - x_2 = \frac{1}{4} - (-3) - 1 = \frac{1}{4} + 2 = \frac{9}{4}$

$-y_3 = \frac{1}{2}\left(\frac{9}{4}\right) + \frac{7}{2} = \frac{9}{8} + \frac{7}{2} = \frac{9+28}{8} = \frac{37}{8}$

$\Rightarrow y_3 = -\frac{37}{8}$

So $PQ = \boxed{\left(\frac{9}{4}, -\frac{37}{8}\right)}$.