Math373 | **Test 3** | **Fri. Apr. 14, 2023**

Name: Solutions

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

1. **[12 points]** Solve the following system of congruences.

$7, 11, 23$: all prime. $M = 7\cdot 11\cdot 23 = 1771$

$$3x \equiv 5 \pmod 7 \qquad x \equiv 6 \pmod{11} \qquad x \equiv 10 \pmod{23}$$

$7 = (2)(3) + 1$

$1 = 7 + (-2)(3)$

$(-2)(3x) \equiv -10 \pmod 7$

$-6x \equiv 4 \mod 7$

$x \equiv 4 \pmod 7$

$11 = (1)(7) + 4$

$7 = (1)(4) + 3$

$4 = (1)(3) + 1$

$1 = 4 + (-1)(3)$

$= 4 + (-1)(7 + (-1)(4))$

$= (2)(4) + (-1)(7)$

$= (2)[11 + (-1)(7)] + (-1)(7)$

$= (2)(11) + (-3)(7)$

i	m_i	M/m_i *	$M/m_i \mod m_i$	$(M/m_i)^{-1} \mod m_i$ *	x_i *
1	7	253	1	1	4
2	11	161	7	-3	6
3	23	77	8	3	10

note $8\cdot 3 \equiv 1 \pmod{23}$

So $x = (253)(1)(4) + (161)(-3)(6) + (77)(3)(10)$

$= \boxed{424 \mod 1771}$

2. **[12 points]** Note that 73 is prime. Solve for x in $x^{49} \equiv 50 \pmod{73}$.

$EEA(49, \phi(73)) = EEA(49, 72)$.

$72 = (1)(49) + 23$

$49 = (2)(23) + 3$

$23 = (7)(3) + 2$

$3 = (1)(2) + 1$

$1 = 3 + (-1)(2)$

$= 3 + (-1)(23 + (-7)(3))$

$= (8)(3) + (-1)(23)$

$= (8)[49 + (-2)(23)] + (-1)(23)$

$= (8)(49) + (-17)(23)$

$= (8)(49) + (-17)[72 + (-1)(49)]$

$= (25)(49) + (-17)(72)$.

So 49^{-1} in $\mathbb{Z}_{72}$ is 25.

$(x^{49})^{25} \equiv (50)^{25} \pmod{73}$

$x \equiv (50)^{25} \pmod{73}$

Fast Power in $\mathbb{Z}_{73}$

$50^2 = 18$

$50^4 = (18)^2 = 32$

$50^8 = (32)^2 = 2$

$50^{16} = 2^2 = 4$

$25 = 16 + 8 + 1$

$x \equiv 50^{25} \equiv 50^{16}\cdot 50^8 \cdot 50$

$\equiv 4\cdot 2\cdot 50 \equiv 400 \equiv \boxed{35}$

3. **[6 points]** True or False: Let $a, b, m_1, m_2 \in \mathbb{Z}$. If $m_1 \neq m_2$, then the system

$$x \equiv a \pmod{m_1} \qquad x \equiv b \pmod{m_2}$$

has a unique solution modulo M, where $M = m_1 m_2$. If True, then explain why, citing a theorem from class if appropriate. If False, then give a counter-example.

This is $\boxed{\text{false.}}$ For example, $x \equiv 0 \pmod 4$ but $x \equiv 1 \pmod 2$ has no soln since x cannot be both odd and a multiple of 4.

Note: For CRT to apply, the moduli m_1, m_2 must be relatively prime.

4. **[2 parts, 15 points each]** Bob generates an RSA key pair with $N = pq = 37 \cdot 131 = 4847$ and $e = 17$.

(a) What is Bob's private key?

$N' = (p-1)(q-1) = 36 \cdot 130 = 4680$

$d = e^{-1}$ in $\mathbb{Z}_{N'}$

EEA(17, 4680):

$4680 = (275)(17) + 5$

$17 = (3)(5) + 2$

$5 = (2)(2) + 1$

$1 = 5 + (-2)(2)$

$= 5 + (-2)[17 + (-3)(5)]$

$= (7)(5) + (-2)(17)$

$= (7)[4680 + (-275)(17)] + (-2)(17)$

$= (7)(4680) + (-1927)(17)$.

So $d \equiv -1927 \equiv 2753 \mod N'$

and Bob's private key is $\boxed{(4847, 2753)}$

(b) Alice wishes to encrypt and send Bob the message $m = 90$. What should he send?

$c = m^e \pmod N$

$= (90)^{17} \mod 4847$.

$(90)^2 = 3253$

$(90)^4 = (3253)^2 = 1008$

$(90)^8 = (1008)^2 = 3041$

$(90)^{16} = (3041)^2 = 4452$

$c = (90)^{17} = 90^{16} \cdot 90 = (4452)(90)$

$= \boxed{3226}$

5. **[6 points]** What is the main advantage of the Miller–Rabin primality test over the Fermat primality test? Be specific.

The Miller-Rabin test can detect that the Carmichael numbers are composite, whereas the Fermat test will probably incorrectly say these numbers are prime.

6. **[6 points]** Suppose we try to generate a roughly 1525-bit prime by selecting random numbers from the set $\{1, \ldots, 2^{1525}\}$ until we happen to pick a prime number. On average, how many numbers will we need to pick before we find a prime?

- From prime # theorem, # primes in $\{1, \ldots, 2^{1525}\} \approx \dfrac{2^{1525}}{\ln(2^{1525})}$
- So chances of picking a prime at random $\approx \dfrac{1}{\cancel{2^{1525}}} \cdot \dfrac{\cancel{2^{1525}}}{\ln(2^{1525})} = \dfrac{1}{\ln(2^{1525})}$
  $= \dfrac{1}{(1525)(\ln 2)}$.
- So average # times is $\dfrac{1}{\frac{1}{1525 \ln(2)}} \approx (1525)(\ln 2) \approx \boxed{1057}$

7. **[6 points]** Alice claims to know the private key associated with public RSA key (N, e). To prove her claim, Alice offers to decrypt ciphertexts, so long as the corresponding plaintexts are random. So Bob may select a random $m_0 \in \mathbb{Z}_N$ and use Alice's public key to compute the corresponding ciphertext c_0, which he sends to Alice. Alice uses her private key to decrypt c_0 to recover m_0, and as long as m_0 looks random, she completes the challenge by sending m to Bob.

Explain how Eve can exploit this system to decrypt a ciphertext c that she previously intercepted.

Eve picks a random $k \in \mathbb{Z}_N^*$ and challenges Alice to decrypt ck^e.

Alice computes $(ck^e)^d = (m^e k^e)^d = (mk)^{ed} = mk$ in $\mathbb{Z}_N$.

Since mk looks random, she responds to Eve's Challenge. But now Eve can compute k^{-1} in $\mathbb{Z}_N$ and then recover m since

$(mk)k^{-1} = m$. ☑

8. Samantha uses ElGamal digital signatures, and her private signing key is given by $(p, g, a) = (269, 18, 73)$. The following powers of g in $\mathbb{Z}_p$ may be helpful.

t	1	2	4	8	16	32	64	128	256
$g^t \pmod p$	18	55	66	52	14	196	218	180	120

(a) **[7 points]** What is Samantha's public verification key?

$A = g^a = (18)^{73} = (18)^{64} \cdot (18)^8 \cdot 18 = (218) \cdot (52) \cdot 18 = 204048 = 146$

$73 = 64 + 8 + 1$

So the public verification key is $(p, g, A) = \boxed{(269, 18, 146)}$

(b) **[15 points]** Samantha wishes to sign a document $D = 134$, and she picks random element $k = 37$. What is the signature D_{sig} corresponding to D?

In $\mathbb{Z}_p$:

$S_1 = g^k \pmod p$

$= (18)^{37} \pmod{269}$

$37 = 32 + 4 + 1$

$S_1 = (18)^{37} = (196)(66)(18)$

$= 163$

In $\mathbb{Z}_{p-1}$:

$S_2 = k^{-1}(D - aS_1) \pmod{p-1}$

k^{-1} in $\mathbb{Z}_{268}$: EEA(37, 268):

$268 = (7)(37) + 9$

$37 = (4)(9) + 1$

$1 = 37 + (-4)(9)$

$= 37 + (-4)[268 + (-7)(37)]$

$= (29)(37) + (-4)(268)$

$\Rightarrow k^{-1} = 29$ in $\mathbb{Z}_{p-1}$

$S_2 = (29)(134 - 73 \cdot 163)$

$= (29)(-11765) = (29)(27) = 247$

So $D_{sig} = (S_1, S_2) = \boxed{(163, 247)}$