CIS 3362 Quiz #4: Number Theory Solutions

Date: 10/22/2025

1) (6 pts) Determine the Prime Factorization of 1,843,956,000.

Start by dividing out as many copies of 2, 3, 5, etc.

$1843956000 = 2^3 \times 5^3 \times 1843956 = 2^3 \times 5^3 \times 2^2 \times 3^2 \times 17 \times 3013$

$= 2^5 \times 3^2 \times 5^3 \times 17 \times 3013$

$= 2^5 \times 3^2 \times 5^3 \times 17 \times 23 \times 131$

Grading: 1 pt per term

2) (8 pts) Determine φ(1,843,956,000) **and give your answer in prime factorized form.**

$\varphi(1843956000) = \varphi(2^5) \times \varphi\ 3^2 \times \varphi(5^3) \times \varphi(17) \times \varphi(23) \times \varphi(131)$

$= (2^5 - 2^4)(3^2 - 3)(5^3 - 5^2)(17 - 1)(23 - 1)(131 - 1)$

$= 2^4 \times 2 \times 3 \times 5^2 \times 2^2 \times 2^4 \times 2 \times 11 \times 130$

$= 2^{12} \times 3 \times 5^2 \times 11 \times 2 \times 5 \times 13$

$= 2^{13} \times 3 \times 5^3 \times 11 \times 13$

Grading: 1 pt for breaking down by prime factor
3 pts for plugging in for each term based on each prime factor
4 pts for simplifying correctly to prime factorized form (give partial as needed)

If they answer 439296000 (answer multiplied out), award 6 of 8 points.

3) (6 pts) Determine the remainder when 47^{12208} is divided by 719. Note that 719 is prime. **For full credit use Fermat's Theorem.**

Since gcd(47, 719) = 1 and 719 is prime, $47^{718} \equiv 1 \pmod{719}$ via Fermat's Theorem.

$47^{12208} = 47^{17 \times 718 + 2} = (47^{718})^{17} \times 47^2 \equiv 1^{17} \times 2209 \equiv$ **52 (mod 719)**

Also accepted: $47^{12208} \equiv 47^{12208 \bmod 718} \equiv 47^2 \equiv 2209 \equiv$ **52 (mod 719)**, but only if they explicitly state which step (the mod in the exponent step) utilizes Fermat's Theorem.

2 pts for directly stating Fermat's Theorem or stating when it was used and using it correctly.

2 pts for reducing problem to 47^2 mod 719

2 pts for the correct answer

4) (6 pts) Determine the remainder when 48^{355743} is divided by 65219. **For full credit use Euler's Theorem.**

$65219 = 7^2 \times 1331 = 7^2 \times 11^3$

$\varphi(65219) = \varphi(7^2 \times 11^3) = \varphi(7^2) \times \varphi(11^3) = (7^2 - 7)(11^3 - 11^2) = 42 \times (1331 - 121) = 42 \times 1210$
$= 50820$

Since gcd(48, 65219) = 1, it follows that $48^{50820} \equiv 1 \pmod{65219}$ via Euler's Theorem.

$48^{355743} = 48^{50820 \times 7 + 3} = (48^{50820})^7 \times 48^3 \equiv 1^7 \times 110592 \equiv$ **45373 (mod 65219)**

Grading: 2 pts prime fact of 65219
2 pts for stating phi(65219)
2 pts to get to the correct answer
give an integer number of partial points as needed

5) (15 pts) We spend a good deal of class time on the discrete log problem. In particular, we covered an algorithm that utilizes O($\sqrt{p}$) time and memory to solve the problem, which if faster than the typical O(p) brute force solution. Utilize this technique to determine the value of x which satisfies the following equation:

$$2^x \equiv 6 \ (mod\ 101)$$

Specifically, please use increments of 11 for your stored memory. (So work out 2^{11}, 2^{22}, 2^{33}, ..., 2^{110} mod 101) and store these in the table provided below. Then, below that, show your incremental work until you get to the answer.

Exponent	2^{exp} mod 101
11	28
22	28 x 28 ≡ 77 mod 101
33	77 x 28 ≡ 35 mod 101
44	35 x 28 ≡ 71 mod 101
55	71 x 28 ≡ 69 mod 101
66	69 x 28 ≡ 13 mod 101
77	13 x 28 ≡ 61 mod 101
88	61 x 28 ≡ 92 mod 101
99	92 x 28 ≡ 51 mod 101
110	51 x 28 ≡ 14 mod 101

$2^{11} = 2048 \equiv 28 \pmod{101}$, so we can fill out the table by calculating powers of 28 mod 101.

Let x = 11y – z, in the equation above, so that we get:

$2^{11y-z} \equiv 6 \ (mod\ 101)$
$(2^z)2^{11y-z} \equiv (2^z)6 \ (mod\ 101)$
$2^{11y} \equiv (2^z)6 \ (mod\ 101)$

Thus, we must try different values of z, until we find $2^z(6)$ mod 101 in our answer column of our table. List these values in a table:

z	0	1	2	3	4	5	6	7	8	9
$2^z(6)$	6	12	24	48	96	91	81	61		

We can stop here because $2^{77} \equiv 61 \pmod{101}$

It follows that $2^{77} \equiv 2^7$ x 6 (mod 101) and
$2^{70} \equiv 6 \pmod{101}$, thus the solution for x is **x = 70.**

Grading: 10 pts for the table, 2 pts to take 6 and start multiplying it by powers of 2, 2 points to find 61 on the table, 1 pt for the final answer.

6) (8 pts) Use the Pollard-Rho Factoring Algorithm to determine the prime factorization of 13231. In the algorithm, at each iteration, values of a and b are determined, and then a gcd is computed. The first row of the table has been filled out for you. Please fill in each other row of the table. In order to help you, it is given that the algorithm succeeds on iteration #7. Use the space below the table for your scratch work and put the final prime factorization (2 primes) in the provided slots below.

Iteration	a	b	relevant gcd
1	5	26	1
2	26	8476	1
3	677	3418	1
4	8476	8581	1
5	11478	9279	1
6	3418	2439	1
7	12983	9970	131

All of this work is on the calculator. For each number in column a, do the following:

For example, when you have 8476, square it and add 1 to that to get 71842577. Then, mod this by 13231 to get 11478. (On a calculator, to do mod, first divide by 13231, then subtract out the integer portion of the result, then take that decimal and multiply by 13231.)

Here is the work for the gcd(13231, 12983 – 9970)

13231 = 3 x 3013 + 1179
3013 = 2 x 1179 + 655
1179 = 1 x 655 + 524
655 = 1 x 524 + 131
524 = 4 x 131

Thus,

13231 = 101 x 131

Grading: All entries were given in class except for the last two entries in column b. For this reason, the grading is as follows: 2 pts for 2439, 2 pts for 9970, 3 pts for the GCD, 1 pt for the final answer.

7) (1 pts) What type of tea can be purchased at Dang Boba and Musubi House?

Boba, give to all