CIS 3362 Quiz #4 (Number Theory) Solutions

Date: 11/15/2023

1) (6 pts) Determine the Prime Factorization of 121,564,800.

121564800 = 1215648 x10^2, use calculator to continue dividing out copies of 2
= 2^5 x 37989 x 2^2 x 5^2, use calculator to divide out copies of 3
= 2^7 x 3^4 x 5^2 x 469, now divide out 7 to get the final answer
= 2^7 x 3^4 x 5^2 x 7^1 x 67^1

2^7 x 3^4 x 5^2 x 7^1 x 67^1

Grading: 1 pt per term (term has to be completely correct to get the point), 1 pt bonus for getting all 5 terms.

2) (6 pts) Determine φ(121564800) **and give your answer in prime factorized form.**

$\varphi(121564800) = \varphi(2^7 \times 3^4 \times 5^2 \times 7^1 \times 67^1) =$
$= \varphi(2^7) \times \varphi(3^4) \times \varphi(5^2) \times \varphi(7^1) \times \varphi(67^1)$
$= (2^7 - 2^6)(3^4 - 3^3)(5^2 - 5^1)(7 - 1)(67 - 1)$
$= 2^6 \times 2 \times 3^3 \times 2^2 \times 5 \times 2 \times 3 \times 2 \times 3 \times 11$
$= 2^{11} \times 3^5 \times 5^1 \times 11^1$

2^{11} x 3^5 x 5^1 x 11^1

Grading: 2 pts to list each term in the product via definition of phi.
2 pts to simplify to an answer that isn't prime factorized (27371520)
2 pts to prime factorize. (Note, no need to get to intermediate answer above to get full credit.)

3) (6 pts) Determine the remainder when 11^{2187} is divided by 313. Note that 313 is prime. **For full credit use Fermat's Theorem.**

By Fermat's Theorem, $11^{312} \equiv 1 \pmod{313}$. Let's look at the given expression:

$11^{2187} = 11^{2184} \times 11^3 = (11^{312})^7 \times 11^3 \equiv 1^7 \times 1331 \equiv 79 \pmod{313}$.

It follows that the desired remainder is **<u>79.</u>**

<u>79</u>

Grading: 2 pts for stating Fermat's theorem or properly applying it.
2 pts for proper exponential breakdown to get ready to plug in Fermat's.
2 pts to reduce to final answer.

4) (6 pts) Determine the remainder when 2681^{96002} is divided by 20200. **For full credit use Euler's Theorem.**

$20200 = 100 \times 202 = 2^2 \times 5^2 \times 2 \times 101 = 2^3 \times 5^2 \times 101$

$\varphi(20200) = \varphi(2^3) \times \varphi(5^2) \times \varphi(101^1) = (2^3 - 2^2)(5^2 - 5^1)(101 - 1) = 4 \times 20 \times 100 = 8000$.

It follows by Euler's Theorem, since gcd(2681, 20200) = 1, $2681^{8000} \equiv 1 \pmod{20200}$

$2681^{96002} = 2681^{96000} \times 2681^2 = (2681^{8000})^{12} \times 2681^2 \equiv 1^{12} \times 7187761 \equiv 16761 \pmod{20200}$,
use the calculator to reduce the mod.

It follows that the desired remainder is **<u>16761.</u>**

<u>16761</u>

Grading: 1 pt prime fact, 1 pt phi, 1 pt stating Euler's, 1 pt expo breakdown, 2 pts reduce to final answer

5) (8 pts) Use the Fermat Factoring Method to factor 91787. Please fill out the table below. Note: More rows than necessary are provided.

x	x^2 - 91787	Perfect Square?
303	22	No
304	629	No
305	1238	No
306	1849 = 43 x 43	Yes

91787 = **(306+43) x (306-43) = 349 x 263**

Grading: 1 pt first row, 2 pts second row, 2 pts third row, 2 pts third row, 1 pt final answer

6) (10 pts) The multiplicative order of an integer ***a*** modulo ***n***, is the smallest positive integer ***k***, such that $a^k \equiv 1 \pmod{n}$. (Note: the term is only defined for values of a such that gcd(a, n) = 1.) Let $\mathbf{f_p(k)}$ equal the number of integers in the range [1,p-1] which have multiplicative order **k**. Determine the following values: $\mathbf{f_{101}(10)}$, $\mathbf{f_{101}(20)}$, $\mathbf{f_{101}(25)}$, $\mathbf{f_{101}(50)}$, **and** $\mathbf{f_{101}(100)}$. **(Note: full credit will only be given if students show proper justification of their answers AND use an efficient method of solution.)**

What we proved in homework 5 is that there are exactly φ(k) bases which have order k modulo a prime, p. It follows that the desired answers are:

$\varphi(10) = (2 - 1)(5 - 1) = 4$
$\varphi(20) = (2^2 - 2^1)(5 - 1) = 8$
$\varphi(25) = (5^2 - 5^1) = 20$
$\varphi(50) = (2 - 1)(5^2 - 5^1) = 20$
$\varphi(100) = (2^2 - 2^1)(5^2 - 5^1) = 40$

$\mathbf{f_{101}(10)}$ = **4** , $\mathbf{f_{101}(20)}$ = **8** , $\mathbf{f_{101}(25)}$ = **20**, $\mathbf{f_{101}(50)}$ = **20** , $\mathbf{f_{101}(100)}$ = **40**

Grading: 5 pts for stating the result from the homework,
1 pt each for properly applying the result.
If there's no work, or no proper justification 0/10

7) (7 pts) Write a function that takes in a positive integer, $\boldsymbol{n}$, and returns the sum of divisors of $\boldsymbol{n}$. If the run time of your function is O($\boldsymbol{n}$) you will get 3 points out of 7. For full credit, your run time must be $O(\sqrt{\boldsymbol{n}})$. It is guaranteed that the input value n does not exceed 10^{12}. (This restriction ensures that the result fits in a long long.)

```
long long sumDivisors(long long n) {

    long long res = 0;                          // 1 pt
    for (long long i=1; i*i<=n; i++) {          // 1 pt loop
        if (n%i == 0) {                         // 1 pts
            res += i;                           // 1 pt
            if (n/i > i)                        // 1 pt
                res += n/i;                     // 1 pt
        }
    }

    return res;                                 // 1 pt

}
```

Grading note: 3 pts out of 7 for O(n) code
Only use criteria above if code is fast enough
Give 5 out of 7 if n/i is added in all cases

8) (1 pts) What animal is used for the logo of fast food chain Panda Express?

Panda, Give to all