CIS 3362 Quiz #4: Number Theory Solutions

1) (6 pts) Determine the Prime Factorization of 158,059,200.

$158{,}059{,}200 = 100 \times 1580592 = 2^2 \times 5^2 \times 1580592$

Now use the calculator to continue dividing out powers of 2. When we finish, we get the following:

$2^2 \times 5^2 \times 1580592 = 2^2 \times 5^2 \times 2^4 \times 98787$

The sum of digits, $9 + 8 + 7 + 8 + 7 = 39$, so we can divide by 3:

$= 2^6 \times 3^1 \times 5^2 \times 32929$

Continuing trial division, we get the next divisors as 13 and 17:

$= \underline{\mathbf{2^6 \times 3 \times 5^2 \times 13 \times 17 \times 149}}$

Since $17^2 > 149$, we know that 149 is prime, so our prime factorization is complete!

Grading: 1 pt for each term, term has to be perfectly correct to get the answer. Exponents equal to 1 may be either omitted or written explicitly.

2) (6 pts) Determine $\varphi(158059200)$ **and give your answer in prime factorized form.**

$\varphi(158059200) = \varphi(2^6)\,\varphi(3)\varphi(5^2)\varphi(13)\,\varphi(17)\varphi(149)$

$= (2^6 - 2^5)(3 - 1)(5^2 - 5)(13 - 1)(17 - 1)(149 - 1)$
$= 32 \times 2 \times 20 \times 12 \times 16 \times 148$
$= 2^5 \times 2 \times 2^2 \times 5 \times 2^2 \times 3 \times 2^4 \times 2^2 \times 37$

$\underline{\mathbf{= 2^{16} \times 3^1 \times 5^1 \times 37^1}}$

Grading: 1 pt to write out prime factorized split of phi.
1/2 pt for each phi term (round down)
2 pts to rearrange terms into prime factorization

3) (6 pts) Determine the remainder when 73^{1388} is divided by 199. Note that 199 is prime. **For full credit use Fermat's Theorem.**

Note that via Fermat's Theorem, since 199 is prime $73^{198} \equiv 1 \pmod{199}$.

$73^{1388} = 73^{1386}73^{2} = (73^{198})^{7}73^{2} \equiv 1^{7}(5329) \equiv$ **<u>155 (mod 199).</u>**

The desired remainder is **<u>155.</u>**

Grading: 2 pts to rewrite exponent as shown above
2 pts to sub in Fermat's
2 pts to take 73^2 and properly reduce it.

4) (6 pts) Determine the remainder when 7^{7181} is divided by 2491. (Note: 2491 = 47 x 53.) **For full credit use Euler's Theorem.**

Note that $\varphi(2491) = \varphi(47)\,\varphi(53) = 46 \times 52 = 2392$.
Thus, by Euler's Theorem, $7^{2392} \equiv 1 \pmod{2491}$.

$7^{7181} = 7^{7176}7^{5} = (7^{2392})^{3}7^{5} \equiv 1^{3}7^{5} \equiv 16807 \equiv$ **<u>1861 (mod 2491).</u>**

The desired remainder is **<u>1861.</u>**

Grading: 1 pt obtain phi of 2491.
2 pts to rewrite exponent as shown above
1 pt to sub in Euler's
2 pts to take 7^5 and properly reduce it.

5) (10 pts) Use the Fermat Factoring Method to factor 44,173. Please fill out the table below. Note: More rows than necessary are provided.

x	x^2 - 44173	Perfect Square?
211	348	No
212	771	No
213	1196	No
214	1623	No
215	2052	No
216	2483	No
217	2916	Yes, 54^2

It follows that the factorization is 44173 = (217 - 54) x (217 + 54) = **163 x 271.**

Grading: 1 pt for each row on the chart, 3 pts for final factorization.

6) (8 pts) 7 is a generator/primitive root mod 17. There are a total of 8 generators mod 17. List These generators can be listed the form 7^a mod 17, 7^b mod 17, 7^c mod 17, 7^d mod 17, 7^e mod 17, 7^f mod 17, 7^g mod 17, and 7^h mod 17, where $0 < a < b < c < d < e < f < g < h < 17$. List the values of a, b, c, d, e, f, g and h in order.

As stated in class, in order for 7^x to be a generator mod 17 as well it must be the case that gcd(x, 17-1) = 1. Thus, the 8 desired values for the exponents are the eight integers from 1 to 16 that share no common factors with 16. These are:

1, 3, 5, 7, 9, 11, 13 and 15.

Grading: 1 pt for each correct answer, no exceptions.

7) (5 pts) The following attempt at fast modular exponentiation runs slowly. Why? Suggest a simple fix.

```
long long fastModExp(long long base, long long exp, long long
mod) {

    if (mod == 1) return 0;
    if (exp == 0) return 1;

    if (exp%2 == 0) {
        long long fHalf = fastModExp(base, exp/2, mod);
        long long sHalf = fastModExp(base, exp/2, mod);
        return (fHalf*sHalf)%mod;
    }

    return base*fastModExp(base, exp-1, mod);
}
```

Two recursive calls are made instead of one. So, after we go do all the work to find base to the power exp/2, we REDO all of that work. The whole savings in the first place came from doing the recursive call ONLY once and reusing its answer in the square step. So, fix the code as follows:

1) Remove the line `long long sHalf = fastModExp(base, exp/2, mod);`

2) Change the following line to: `return (fHalf*fHalf)%mod;`

Grading: 3 pts for pointing out that 2 recursive calls is the slowdown
2 pts for the fix.

8) (3 pts) The book, Euler: The Master of Us All, is about the work of which 18^{th} century mathematician?

Leonard Euler (Grading: give to all)