Homework #5 Solutions - CIS 3362

1) Without the aid of a computer program, determine the prime factorization of 1,561,032,000. Show your work. You may do division on a calculator.

. . . . . .

We can see that 1000 divides evenly into 1561032000:
1561032000 / 1000 = 1561032000 = 1561032
1000 = 100 * 10 = 25 * 4 * 2 * 5 = 5^2 * 2^2 * 2 * 5 = $\underline{2^3 * 5^3}$

We see that 4 divides evenly into 1561032 because '32' divides evenly into 4:
1561032 / 4 = 390258
4 = $\underline{2^2}$

We see that 2 divides evenly into 390258 because it's even:
390258 / 2 = 195129
2 = $\underline{2^1}$

We see that 9 divides evenly into 195129 because adding the digits gives a number divisible by 9:
195129 / 9 = 21681
9 = $\underline{3^2}$

We see that 9 divides again into 21681 for the same reason above: 21681 / 9 = 2409
9 = $\underline{3^2}$

We see that 3 divides into 2409 because adding the digits gives a number divisible by 3:
2409 / 3 = 803
3 = $\underline{3^1}$

For 803, we have to check primes up until $\sqrt{803}$, and once we get 11 we get:
803 / 11 = 73
11 = $\underline{11^1}$

We do the same process for 73, and since $\sqrt{73} < 9$, we can check all prime numbers up until 9 and see that 73 is prime:
73 = $\underline{73^1}$

To get the prime factorization of 1561032000, we multiply together all of the prime number we divided into 1,561,032,000 and get:

Prime Factorization: $(2^6)(3^5)(5^3)(11)(73)$

---

2) What is φ(1,561,032,000)?

. . . . . .

Since $\varphi(n)$ can be calculated via the formula $n(\prod_{i=1}^{k}(1-\frac{1}{p_i}))$, where p_i is the i^{th} prime factor of n, we can use the prime factorization solved for in Question #1 to find φ as follows:

$\varphi(1561032000) = \varphi(2^6 * 3^5 * 5^3 * 11^1 * 73^1)$
$= 1561032000 * ((1-\frac{1}{2}) * (1-\frac{1}{3}) * (1-\frac{1}{5}) * (1-\frac{1}{11}) * (1-\frac{1}{73}))$
$= 1561032000 * (\frac{1}{2} * \frac{2}{3} * \frac{4}{5} * \frac{10}{11} * \frac{72}{73})$
$= 373248000$

$\varphi(1561032000) = 373248000$

---

3) Use Fermat's Theorem to calculate the remainder when 6^{5094} is divided by 1019?

. . . . . .

For Fermat's Theorem, the number which we mod by has to be prime and a quick check can conclude that 1019 is indeed prime. Knowing this, we can go forward and use Fermat's Theorem:

$a^{p-1} \equiv 1 \pmod{p}$, where p is a prime number
In our case, $a = 6$ and $p = 1019$

We can use the exponent 5094 and the value of $p - 1 = 1018$ to calculate
5094 / 1018 = 5 remainder 4. We can now write:

$6^{5094} = (6^{1018})^5 * 6^4 \equiv (1)^5 * 6^4 \equiv 1296 \equiv 277 \pmod{1019}$

Therefore, the remainder when 6^{5094} is divided by 1019 is 277.

---

4) Use Euler's Theorem to calculate the remainder when 18^{57026} is divided by 24455?

. . . . . .

Since Euler's Theorem states that $a^{\varphi(n)} \equiv 1 \pmod{n}$, we must first find $\varphi(n)$. In our case $a = 18$ and $n = 24455$:

24455 / 5 = 4891
4891 / 67 = 73 We have to check all primes before $\sqrt{4891} \approx 70$

Therefore, we know the prime factorization for 24455 = 5*67*73. With this, we can now calculate $\varphi(24455)$:

$\varphi(24455) = 24455((1 - \frac{1}{5}) * (1 - \frac{1}{67}) * (1 - \frac{1}{73}))$
$= 24455(\frac{4}{5} * \frac{66}{67} * \frac{72}{73})$
$= 19008$

We can now use the same methodology as in Question #3 to solve for our desired remainder:

$18^{19008} \equiv 1 \pmod{19008}$
57026 / 19008 = 3 R 2
$18^{57026} \equiv (18^{19008})^3 * 18^2 \equiv (1)^3 * 18^2 \equiv 324 \pmod{24455}$

Therefore, the remainder when 18^{57026} is divided by 24455 is 324.

---

5) Show the steps of running the Miller-Rabin algorithm, testing n = 561 for primality with the randomly chosen value of a = 2. Please use a calculator or computer program to calculate the modular exponents and just show the result of each squaring/mod operations.

. . . . . .

Given that we are testing $n = 561$ for primality with $a = 2$, we can begin the Miller-Rabin algorithm as follows:

$n - 1 = 560 = 2 * 2 * 2 * 2 * 35 = 2^4 * 35$
$X = 2^{35} \equiv 263 \pmod{561} \neq 1$

We now square X 4 more times (because of the 2^4), returning "Probably Prime" if X ≡ -1 (mod 561) and returning "Composite" if X ≡ 1 (mod 561):

$2^{70} \equiv 263^2 \equiv 69169 \equiv 166 \neq -1 \pmod{561}$
$2^{140} \equiv 166^2 \equiv 27556 \equiv 67 \neq -1 \pmod{561}$
$2^{280} \equiv 67^2 \equiv 4489 \equiv 1 \pmod{561} \rightarrow$ Composite

Based on the above algorithm, we can determine with certainty that 561 is composite.

---

6) Trace through the Fermat Factoring algorithm to factor 161,423 as the product of two prime numbers. You may use a calculator or computer program to execute each calculation, but print out the result of each number being tested as a perfect square.

. . . . . .

For Fermat Factoring, the general idea is to assume that the number to factor n is an odd product of 2 primes, and then try and find those 2 primes via trial-and-error. Our starting point for X will be the ceil($\sqrt{161423}$) = 402.

X	X^2 - 161423	Perfect Square?
402	181	No
403	986	No
404	1793	No
405	2602	No
406	3413	No
407	4226	No
408	5041	Yes (71^2)

Now that we have our perfect square, we can observe through algebraic manipulation that:

408^2 - 161423 = 71^2 $\leftrightarrow$ 161423 = 408^2 - 71^2 = (408+71)(408-71) = 479*337

Therefore, the prime factorization of 161423 is 479*337.

---

7) We can create a sequence from a starting integer n by repeatedly taking the previous value in the sequence and generating the next number in the sequence as φ(n) until we generate the number 1. For example, if we start with n = 11, the sequence generated would be 11, 10, 4, 2, 1. Define a function f(n) to equal the number of terms in the sequence generated above, with the first term equal to n. (For example, f(11) = 5.) Write a computer program to calculate the smallest integer n such that f(n) = 10. **(Note: This question can be solved by writing a very inefficient phi function. For a few extra credit points, write your code with an efficient phi function and find the minimal integer n such that f(n) = 20. In Python, my efficient version took 17 seconds on my laptop.)** Please attach your program separately and in your write up state the answer your program produced. In the write up, describe the algorithm you used to solve the problem.

. . . . . .
