Fall 2026 CIS 3362 Homework #5: Number Theory
Check WebCourses for the due date

1) (5 pts) Without the aid of a computer program, determine the prime factorization of 35,474,400. Show your work. You may do division on a calculator. State which numbers divided in evenly how many times.

Solution
$2*2*2*2*2*3*3*5*5*13*379 = 2^5 \times 3^2 \times 5^2 \times 13^1 \times 379^1$

2) (5 pts) What is φ(35,474,400)? You can use a calculator, but please show your work.

Solution
$\varphi(2^5 \times 3^2 \times 5^2 \times 13^1 \times 379^1)$
$= (2^5-2^4) * (3^2-3^1) * (5^2-5^1) *(12 – 1) * (379 – 1)$
$= 16 * 6 * 20 * 12 * 378$
$= 8{,}709{,}120$

3) (10 pts) Use Fermat's Theorem to calculate the remainder when 276^{48436} is divided by 8363?

Solution
Since GCD(276, 8363) = 1, by Fermat's Theorem, $276^{8362} = 1 \bmod 8363$.
$276^{48436} = 276^{5*8362+6626} \pmod{8363}$
$= (276^{8362})^5 * 276^{6626} \pmod{8363}$ (Note: I apologize, I must have mistyped something when I made the problem!!! I typically work these out so the leftover is very small...)
$= 1^5 * 276^{6626} \pmod{8363}$

Note: At this point, there's no reason to work this out by hand as that wasn't the intention on this question. (I had wanted the exponent to be 1, 2 or 3 that's leftover here. It's likely I meant my mod to be 8073 and mistyped it...)

$= 2560 \pmod{8363}$

4) (10 pts) Use Euler's Theorem to calculate the remainder when $629^{10483201}$ is divided by 1435109?

Solution
$1435109 = 13 * 101 * 1093$
$\phi(1435109) = (13 – 1)(101 – 1)(1093 – 1) = 12 \times 100 \times 1092 = 1310400$

Since GCD(629, 1435109) = 1, by Euler's Theorem, $629^{1310400} \equiv 1 \pmod{1435109}$.

$629^{10483201} = (629^{1435109})^8 \times 629^1$
$= 1^8 \times 629$
$= 629 \pmod{1435109}$

5) (10 pts) Use the Fermat Factoring method by hand and calculator to factor the integer 31363859. Make a table showing your work. Your table should have exactly 10 rows.

Solution

x	$x^2 - 31363859$	Perfect Square?
5601	7342	No
5602	18545	No
5603	29750	No
5604	40957	No
5605	52166	No
5606	63377	No
5607	74590	No
5608	85805	No
5609	97022	No
5610	108241	Yes, 329

x = 5610
y = 329
x+y = **5939**
x-y = **5281**

(x-y)*(x+y) = 5281 * 5939 = 31363859

6) (15 pts) For a prime number, p, under the assumption that there exists a primitive root, prove that there are exactly a total of $\phi(p-1)$ primitive roots.

Solution

We assume that at least one primitive root exists. Let's call this α. We know that of the p-1 values 1, 2, 3, …, p-1, exactly φ(p-1) of them share no common factor with p-1, based on the definition of φ.

In order to prove the assertion, we must prove that α^k is a primitive root if and only if gcd(k, p-1) = 1. If we can prove this, then from the list α, α^2, α^3, α^4 , ... , α^{p-1}, the terms that are primitive roots are precisely the terms with the exponents that don't share a common factor with p-1, of which there are exactly φ(p-1).

Let gcd(k, p – 1) = 1. We will prove that α^k is a primitive root. We prove this using proof by contradiction. Assume the opposite, that α^k is NOT a primitive root. Then, we must have that two values in the list α^k, α^{2k}, α^{3k}, …, $\alpha^{k(p-1)}$ that are equivalent mod p. Let these two values be α^{ik} and α^{jk}, where $0 < i < j < p$. Thus, we have:

$\alpha^{jk} \equiv \alpha^{ik} \bmod p$
$\alpha^{jk} - \alpha^{ik} \equiv 0 \bmod p$
$\alpha^{ik}(\alpha^{jk-ik} - 1) \equiv 0 \bmod p$

We know that p shares no common factors with α^{ik}.

It follows that $p \mid \alpha^{jk-ik} - 1$. Thus

$\alpha^{jk-ik} - 1 \equiv 0 \bmod p$
$\alpha^{(j-i)k} \equiv 1 \bmod p$

Since α is a primitive root, we know that the exponent on the left must be a multiple of p – 1:

(p – 1) | (j – i)k.

We know that gcd(p – 1, k) = 1. Thus it follows that (p – 1) | (j – i). But this contradicts the fact that 0 < i < j < p, which means that i >= 1, j <= p-1, so j – i > 0 and j – i ≤ p – 2.

This is our contradiction. It follows that our initial assumption that two values on the given list were equivalent mod p is faulty. If no two of these values are equivalent mod p, we can conclude that α^k is a primitive root.

Now, the second part of the proof is that if gcd(p – 1, k) > 1, then α^k is NOT a primitive root. Let c = gcd(p – 1, k) > 1. Now, consider the term $(\alpha^k)^{(p-1)/c}$ mod p. The exponent $\frac{p-1}{c}$ is clearly less than p – 1. Secondly, this is equivalent to $\alpha^{\frac{k}{c}(p-1)}$ mod p. Notice that c divides evenly into k because c = gcd(k, p – 1), thus c is a divisor of k. Let m = $\frac{k}{c}$, and $m \in Z$. Thus $\alpha^{\frac{k}{c}(p-1)} \equiv (\alpha^{p-1})^{\frac{k}{c}} \equiv 1^m \equiv 1 \ (mod\ p)$. This means that α^k isn't a primitive root since raising it to a power less than p – 1 yields 1.

Thus, we have shown that if AND only if gcd(p – 1, k) = 1, is α^k a primitive root of p. Thus, to count the number of primitive roots, we simply look at the list α, α^2, α^3, α^4 , ... , α^{p-1} and count the number of terms that have exponents relatively prime to p – 1. By definition of α, this number is exactly φ(p – 1). As a concrete example, if we know that 2 is a primitive root of p = 19, it follows that 2^1, 2^5, 2^7, 2^{11}, 2^{13}, and 2^{17} are all primitive roots of 19, since 1, 5, 7, 11, 13 and 17 don't share any common factors with 18, p – 1.

7) (10 pts) Pick three prime numbers in between 20 and 50 and use a program to determine each of the primitive roots of the three primes you picked. State these primitive roots and verify that the number of primitive roots you found is exactly equal to of $\phi(p-1)$ in each case. Please attach your program separately and in your written answer write down each primitive root your program found.

Solution

43 Prime
[3, 5, 12, 18, 19, 20, 26, 28, 29, 30, 33, 34] Generators
12 length of generators
φ(43 – 1) = φ(42) = φ(2 x 3 x 7) = (2 – 1)(3 – 1)(7 – 1) = 1 x 2 x 6 = 12 (works)

23 Prime
[5, 7, 10, 11, 14, 15, 17, 19, 20, 21] Generators
10 length of generators
φ(23 – 1) = φ(22) = φ(2 x 11) = (2 – 1)(11 – 1) = 1 x 10 = 10 (works)

47 Prime
[5, 10, 11, 13, 15, 19, 20, 22, 23, 26, 29, 30, 31, 33, 35, 38, 39, 40, 41, 43, 44, 45] Generators
22 length of generators
φ(47 – 1) = φ(46) = φ(2 x 23) = (2 – 1)(23 – 1) = 1 x 22 = 22 (works)

The attached code uses (ThreePrimes.py) creates a random set of 3 primes within the given range, finds their generators through brute force, prints them, and compares the length of the list of generators to phi(p-1). With a few helper functions (some were written in class), I was able to make quick work of creating the list of generators or creating a phi function.

8) (10 pts) $2^x \equiv 39\ (mod\ 59)$. In class we went over a couple of ideas to speed up the computation of the value of x beyond just multiplying 2 by itself 59 times until we find the right-hand side. Use one of these ideas, showing your work by hand/calculator to determine the smallest positive integer value of x which satisfies this equation.

Solution

We use the Giant-Step Tiny-Step method that was shown in class:

$\lceil\sqrt{59}\rceil = 8$

$2^{8i-j} = 39$

$2^{8i} = 39(2^j)$

$39 \times 2^0 \equiv 39\ (mod\ 59)$
$39 \times 2^1 \equiv 78 \equiv 19\ (mod\ 59)$
$39 \times 2^2 \equiv 156 \equiv 38\ (mod\ 59)$
$39 \times 2^3 \equiv 39 \times 2^2 \times 2 \equiv 38 \times 2 \equiv 76 \equiv 17\ (mod\ 59)$
$39 \times 2^4 \equiv 39 \times 2^3 \times 2 \equiv 17 \times 2 \equiv 34\ (mod\ 59)$
$39 \times 2^5 \equiv 39 \times 2^4 \times 2 \equiv 34 \times 2 \equiv 68 \equiv 9\ (mod\ 59)$
$39 \times 2^6 \equiv 39 \times 2^5 \times 2 \equiv 9 \times 2 \equiv 18\ (mod\ 59)$
$39 \times 2^7 \equiv 39 \times 2^6 \times 2 \equiv 18 \times 2 \equiv 36\ (mod\ 59)$

Thus our map is: 39 → 0, 19 → 1, 38 → 2, 17 → 3, 34 → 4, 9 → 5, 18 → 5, and 36 → 7.

Now, let's compute successive powers of 2^8 under mod:

$2^8 \equiv 256 \equiv 20\ (mod\ 59)$	not in map
$2^{16} \equiv (2^8)^2 \equiv 20^2 \equiv 400 \equiv 46\ (mod\ 59)$	not in map
$2^{24} \equiv (2^{16})(2^8) \equiv 46(20) \equiv 920 \equiv 35\ (mod\ 59)$	not in map
$2^{32} \equiv (2^{24})(2^8) \equiv 35(20) \equiv 700 \equiv 51\ (mod\ 59)$	not in map
$2^{40} \equiv (2^{32})(2^8) \equiv 51(20) \equiv 1020 \equiv 17\ (mod\ 59)$	map has $17 \rightarrow 3$

It follows that $2^{40} \equiv 39 \times 2^3\ (mod\ 59)$ and we can conclude that

$$2^{37} \equiv 39\ (mod\ 59)$$

Thus, the smallest positive integer that satisfies the equation is x = 39. Here we double check that this result works:

$$2^{37} = (2^{32})(2^5) \equiv (51)(32) \equiv (-8)(32) \equiv -256 \equiv 39\ (mod\ 59)$$

9) (25 pts) The prime number theorem says that the probability of an integer near the value of n being prime is roughly $\frac{1}{\ln n}$. Use the posted Miller-Rabin code and experimentally test this hypothesis. Generate random integers (say 10000 or more) in each of the following ranges:

(a) $10^{15} - 10^{16}$ (b) $10^{50} - 10^{51}$ (c) $10^{100} - 10^{101}$ (d) $10^{300} - 10^{301}$

Specifically, randomly generate 10,000 integers in this range, then use the Miller-Rabin test to see if those integers are prime or not. Compare your results to the values of $\frac{1}{\ln 10^{15}}$, $\frac{1}{\ln 10^{50}}$, $\frac{1}{\ln 10^{100}}$, and $\frac{1}{\ln 10^{300}}$. Are the results what you expected?

Solution

Results (100,000 random integers per range, 50 Miller-Rabin rounds each)

10^15 to 10^16: 2705 primes found
experimental = 0.02705
1/ln(10^15) = 0.02895

10^50 to 10^51: 897 primes found
experimental = 0.00897
1/ln(10^50) = 0.00869

10^100 to 10^101: 407 primes found
experimental = 0.00407
1/ln(10^100) = 0.00434

10^300 to 10^301: 171 primes found
experimental = 0.00171
1/ln(10^300) = 0.00145

The results are near expected. I originally tried with 10,000 random ints, and found over multiple runs that the numbers were varying a lot more than I thought they would. I swapped to 100,000 random ints per range and that kept the numbers way closer to the expected values, as would expect when making introducing a larger sample size. This also lines up with our analysis of the 10^{300} group, we find the highest relative variance in the range that has the least density of primes. I believe that with more trials it would close in further onto the expected rates.