COT 3100 Fall 2017 Homework #4 Solutions

1) Find the greatest common divisor of each of the following pairs of integers using the Euclidean Algorithm:

Solution

a) 123 = 1 x 63 + 60
63 = 1 x 60 + 3
60 = 20 x 3, **gcd = 3**

b) 979 = 1 x 782 + 197
782 = 3 x 197 + 191
197 = 1 x 191 + 6
191 = 31 x 6 + 5
6 = 1 x 5 + 1
5 = 5 x 1, **gcd = 1**

c) 131 = 1 x 108 + 23
108 = 4 x 23 + 16
23 = 1 x 16 + 7
16 = 2 x 7 + 2
7 = 3 x 2 + 1
2 = 2 x 1, **gcd = 1**

d) 923 = 0 x 7238 + 923
7238 = 7 x 923 + 777
923 = 1 x 777 + 146
777 = 5 x 146 + 47
146 = 3 x 47 + 5
47 = 9 x 5 + 2
5 = 2 x 2 + 1
2 = 2 x 1, **gcd = 1**

e) 1111 = 10 x 111 + 1
111 = 111 x 1, **gcd = 1**

f) 555 = 1 x 330 + 225
330 = 1 x 225 + 105
225 = 2 x 105 + 15
105 = 7 x 15, **gcd = 15**

The attached program, gcdhmk.c can be used to generate questions for practice.

2) Determine 108^{-1} mod 131. (Note: You can use your work from question 1c if you'd like.)

Solution

Take the Euclidean Algorithm for these two numbers from question #1 and then run the Extended Euclidean on it:

7 - 3 x 2 = 1
7 - 3(16 - 2 x 7) = 1
7 - 3 x 16 + 6 x 7 = 1
7 x 7 - 3 x 16 = 1
7(23 - 16) - 3 x 16 = 1
7 x 23 - 7 x 16 - 3 x 16 = 1
7 x 23 - 10 x 16 = 0
7 x 23 - 10(108 - 4 x 23) = 1
7 x 23 - 10 x 108 + 40 x 23 = 1
47 x 23 - 10 x 108 = 1
47(131 - 108) - 10 x 108 = 1
47 x 131 - 47 x 108 - 10 x 108 = 1
47 x 131 - 57 x 108 = 1

Consider this equation mod 131 and we get:

47 x 131 - 57 x 108 ≡ 1 (mod 131)
47 x 0 - 57 x 108 ≡ 1 (mod 131)
-57 x 108 ≡ 1 (mod 131)

It follows that $108^{-1} \equiv -57 \equiv$ **74 (mod 131).**

3) Without the use of a calculator determine the remainder when 47^{37} is divided by 51. Please show all of your steps by hand and utilize one of the two methods shown in class.

Solution

$47^{37} \equiv (-4)^{37} \equiv -(4)^{37} \equiv -(4^2)^{18}(4) \equiv -(16)^{18}(4) \equiv -(16^2)^9(4) \equiv -(256)^9(4) \equiv -(1)^9(4) \equiv -4 \equiv$ 47 mod 51.

Thus, the remainder is 47. (Note: it's a bit of a coincidence that we got back the same answer, for any integer a that shares no common factor with 51, it will always be the case that $a^{32} \equiv 1$ mod 51, by Euler's Theorem. It turns out that for a = 47, $a^4 \equiv 1$ mod 51, so as we exponentiate 47, we "wrap around" every 4 times, meaning that we "recover" the original value if we exponentiate 5 times, or any number of times that is equivalent to 1 mod 4 for this specific set of values.)

4) Prove or disprove: if p and q are prime numbers then pq - 2 is also a prime number.

Solution

This is false. Consider p = 2, q = 5, both of which are prime, but pq - 2 = 2(5) - 2 = 8, which is NOT prime (since 2 is a proper divisor of 8). There are many other counter-examples one could find. Anything with $p = 2$ and $q > 2$ will work. Also, some odd pairs of primes work, consider p = 5 and q = 7, in this case, but pq - 2 = 5(7) - 2 = 33, which is also not prime since 3 divides evenly into 33.

5) Find the least common multiple of each pair of numbers from question 1. Use your results from question 1.

Solution

Recall that gcd(a, b) x lcm(a, b) = a x b, so that lcm (a, b) = $\frac{ab}{\gcd(a,b)}$. Using this formula and the gcd's calculated in question 1, we have the following:

a) $lcm(123, 63) = \frac{123 \times 63}{\gcd(123,63)} = \frac{123 \times 63}{3} = 123 \times 21 = 2583$

b) $lcm(979, 782) = \frac{979 \times 782}{\gcd(979,782)} = \frac{979 \times 782}{1} = 979 \times 782 = 765578$

c) $lcm(131, 108) = \frac{131 \times 108}{\gcd(131,108)} = \frac{131 \times 108}{1} = 131 \times 108 = 14148$

d) $lcm(923, 7238) = \frac{923 \times 7238}{\gcd(923,7238)} = \frac{923 \times 7238}{1} = 923 \times 7238 = 6680674$

e) $lcm(1111, 111) = \frac{1111 \times 111}{\gcd(1111,111)} = \frac{1111 \times 111}{1} = 1111 \times 111 = 123321$

f) $lcm(555, 330) = \frac{555 \times 330}{\gcd(555,330)} = \frac{555 \times 330}{15} = 555 \times 22 = 12210$

6) Determine the number of divisors that each of the following integers have:

Solution

As shown in the extra written notes added in class, given the prime factorization of an integer, we can get the number of divisors it has just by taking each exponent in the prime factorization, adding 1 to it, and multiplying all of these terms.

a) $96 = 2^5 3^1$, has (5 + 1)(1 + 1) = 12 divisors
b) $108 = 2^2 3^3$, has (2 + 1)(3 + 1) = 12 divisors
c) $267 = 3^1 89^1$ has (1 + 1)(1 + 1) = 4 divisors
d) $289 = 17^2$ has (2 + 1) = 3 divisors
e) $625040 = 2^4 5^1 13^1 601^1$, has (4 + 1)(1 + 1)(1 + 1)(1 + 1) = 40 divisors
f) $698112 = 2^8 3^3 101^1$, has (8 + 1)(3 + 1)(1 + 1) = 72 divisors

7) Give a summary of the life and mathematical contributions of Sophie Germain. Please aim for a length of roughly 200 - 400 words. ***Your summary must be typed.*** Please state the sources you used in writing your summary.

Sample Write Up

Sophie Germain, born in 1776, grew up in Paris and developed a love for mathematics by reading books in her father's library. Her parents didn't encourage her, but in spite of their initial punishments, she continued to study in secret, late at night with the aid of a candle. Upon turning 18, though she couldn't attend the Ecole Polytechnique, she was able to obtain the notes from lectures of the school and submit observations about the notes, which she did. She was afraid of being found out of being a woman, and submitted her notes under a male pseudonym. Ultimately, one of the professors, Joseph Lagrange, one of the best known mathematicians of the early 19^{th} century, wanted to meet Germain and her identity was revealed. Luckily, he had nothing against teaching and woman and worked with her individually.

Germain read both books by Lagrange and Gauss, which piqued her interest in number theory. She attempted to prove Fermat's Last Theorem for exponents of the form n = p - 1, where p is prime equivalent to 7 mod 8. Gauss never commented on her proof and she used an assumption that may not have been warranted in it. Though the two never met, Gauss was impressed with the work Germain was able to do. They stopped communicating after a couple years and thereafter, Germain turned her attention to elasticity theory. Driven by a prize from the Paris Academy of Sciences originally offered in 1809, Germain worked for many years, occasionally with Lagrange and Poisson, and on her own. She won a prize in 1816 and continued working on the problem for another ten years. Shockingly, even after she won the Academy's award, she was unable to attend its lectures as the only women allowed were wives of professors. Nonetheless, after becoming friends with Joseph Fourier, he was able to allow her to come to sessions of the academy.

Germain's biggest contributions were in the field of Number Theory. She was deeply fascinated with Fermat's Last Theorem, and resumed working on it in 1815, after finishing one of her elasticity papers. She proved Fermat's last theorem for a subset of prime numbers up to 100 that are now known as Sophie Germain primes. In particular, Sophie Germain primes are prime numbers p such that 2p + 1 is also prime. For example, 11 is a Sophie Germain prime since 2 x 11 + 1 = 23, which is also prime. Though the method ultimately used to prove Fermat's Last Theorem wasn't hers, much work in the area during her time followed her ideas. Germain was diagnosed with breast cancer in 1829 but continued work. She passed away a couple years later in 1831.

Source: https://en.wikipedia.org/wiki/Sophie_Germain