COT 3100 Fall 2018
Homework #4 Solution
Fnu Tulha

1) Find all integer solutions to the equation 135x + 198y = 39.

Solution:

135x + 198y = 39
9(15x + 22y) = 39

Note: if you didn't recognize that 9 divided evenly into 135 and 198, you could run the Euclidean Algorithm to obtain the greatest common divisor of these two numbers.

Since 39 isn't divisible by 9, but the left-hand side must be (since x and y are integers), it follows that there are no integer solutions to the equation.

We can use the extended Euclidean algorithm here to find all the integer solutions to the above equation.

2) (a)Find all integer solutions to the equation 255x + 104y = 1.

(b) Find all integer solutions to the equation 255x + 104y = 13.

(c) Find 104^{-1} mod 255. (Note: Answer must be in between 0 and 254, inclusive.)

Solution: (a) We will repeat the process from Q1 to find the gcd of 255 and 104 to get the following equation first, 255x + 104y = gcd(255, 104).

255 = 104*2 + 47 (1)
104 = 47*2 + 10 (2)
47 = 10*4 + 7 (3)
10 = 7*1 + 3 (4)
7 = 3*2 + 1 (5)
3 = 1*3 + 0 (6)
The gcd is 1.
Let’s use the extended Euclidean algorithm now to find solutions to 255x + 104y = 1.

Starting from ():
1 = 7 - 3*2 (5)
1 = 7 - (10 – 7*1)*2 (using (4))
1 = 7 - 10*2 + 2*7
1 = 3*7 – 10*2
1 = 3*(47 – 10*4) – 10*2 (using (3))

1 = 3*47 – 12*10 – 10*2
1 = 3*47 – 14*10
1 = 3*47 – 14(104 – 47*2) (using (4))
1 = 3*47 – 14*104 + 28*47
1 = 31*47 – 14*104
1 = 31*(255 – 104*2) – 14*104 (using (5))
1 = 31*255 – 62*104 – 14*104
1 = 31*255 – 76*104

$x_0 = 31, y_0 = -76$

However, this is only one solution. The set of all possible solutions will then be:

$x = x_0 + n\frac{b}{\gcd(a,b)}$ $and\ y = y_0 - n\frac{a}{\gcd(a,b)}$

$$where\ x_0, y_0\ is\ the\ first\ solution,$$
$$n \in \mathrm{Z},\ and\ a, b\ are\ the\ coefficients\ of\ x\ and\ y\ respectively.$$

$$\{(\boldsymbol{x}, \boldsymbol{y}) | \boldsymbol{x = 31 + 104n, y\ - 76 - 255n, n} \in \boldsymbol{Z}\}$$

(b) Using 1 = 31*255 – 76*104 from (a), we can multiply both sides by 13:

13*1 = 13*31*255 – 13*76*104
13 = 255(13*31) + 104(-13*76)
13 = 255(403) + 104(-988)

$$x_0 = 403, y_0 = -988$$

The set of all possible solutions will be:

$$x = 403 + 104n, y = -988 - 255n$$
$$where\ n \in Z$$

Since x_0, y_0 can be any solution to the given equation, we can 'simplify' our general solution by taking n = -3 to get

$$x = 403 + 104(-3), \qquad y = -988 - 255(-3)$$
$$x = 91, \qquad y = -223$$

So our new general solution will be:

$$\{(\boldsymbol{x}, \boldsymbol{y}) | \boldsymbol{x = 91 + 104n, y\ - 223 - 255n, n} \in \boldsymbol{Z}\}$$

(c) In order to find 104^{-1} mod 255, we can use the equation given in (a).

1 = 31*255 – 76*104
31*255 – 76*104 = 1

Taking mod 255 on the equation we will get:

31*255 – 76*104 ≡ 1 mod 255

0 – 76*104 = 1 mod 255
– 76*104 = 1 mod 255

It follows that $104^{-1} \equiv -76 \equiv 179 \pmod{255}$.

3) Let x and y be integers such that 13 | (6x - y). Prove that 13 | (5x + 23y).

Solution: We can express 5x + 23y as:

5x + 23y = 3*(6x - y) + 13(-x + 2y)
Since 13 | (6x - y), it will also divide 3*(6x - y), and 13*(-x + 2y) is a multiple of 13 therefore, 13 | (5x + 23).

4) On the first exam, you were asked to prove the following statement:

If n is an integer such that n ≡ 1 (mod 6), then prove that $n^2 \equiv 1 \pmod{24}$.

It turns out that this statement is a specific version of a more general statement that can be proven, which is as follows:

If n is an integer and k is a non-negative integer prove that:

$$\text{If } n \equiv 1 \pmod{4k+2}, \text{ then } n^2 \equiv 1 \pmod{(16k+8)}.$$

Solution: We know that n ≡ 1 (mod 4k+2) so there exists an integer x such that
n – 1= (4k+2)*x
n = (4k+2)*x + 1

$$n^2 = (4k+2)^2x^2 + 2\big((4k+2)x\big)(1) + 1^2$$
$$n^2 = (4k+2)\big((4k+2)x^2 + 2(x)\big) + 1$$
$$n^2 = (8k+4)x\big((2k+1)x + 1\big) + 1 \qquad (1)$$

We will now prove that $x\big((2k+1)x+1\big)$ is even. We will use proof by cases.
Case 1: x is an odd integer so x = 2y+1 where y is an integer.
=(2y+1)((2k+1)(2y+1) + 1)
=(2y+1)(4ky+2k+2y+1+1)
=2(2y+1)(2ky+k+y+1)
So when x is odd, $x\big((2k+1)x+1\big)$ is even.

Case 2: x is an even integer so x = 2y where y is an integer.
=2y((2k+1)2y + 1)
We observe that this results in an even number as well.
So when x is even, $x\big((2k+1)x+1\big)$ is even.

Therefore, $x\left((2k+1)x+1\right) = 2z$ where z is an integer as well.
Substituting this into (1), we get:
$n^2 = (8k+4)2z+1$
$n^2 = (16k+8)z+1$
$n^2 - 1 = (16k+8)z$
This implies that $16k+8$ divides $n^2 - 1$ so we conclude that $n^2 \equiv 1 \pmod{(16k+8)}$.

5) Let a = $2^3 3^4 5^2 7^9$, b = $2^2 3^9 5^4 11^8$, and c = $2^4 3^6 5^5 11^4$. Determine, in prime factorized form, both gcd(a, b, c) and lcm(a, b, c).

Solution: For gcd we will consider the minimum and for lcm the maximum exponents for each prime factor.
gcd(a, b, c) = $2^2 3^4 5^2$
lcm(a, b, c) = $2^4 3^9 5^5 7^9 11^8$

6) For the numbers a, b and c listed in problem 5, determine the number of divisors each of those numbers has.

Solution: The total divisors of a number is equal to the product of prime factors' (exponents + 1) for that number.

a = $2^3 3^4 5^2 7^9$
Total divisors = 4*5*3*10 = 600

b = $2^2 3^9 5^4 11^8$
Total divisors = 3*10*5*9 = 1350

c = $2^4 3^6 5^5 11^4$
Total divisors = 5*7*6*5 = 1050

7) Without prime factorization, calculate the least common multiple of 135 and 198.

Solution: We can evaluate the LCM of two numbers without prime factorization by the the following:

$$lcm(a,b) = \frac{ab}{\gcd(a,b)}$$

The gcd(135, 198) was evaluated in question 1 to be 9 therefore, the lcm is:

$$lcm(135, 198) = \frac{135 * 198}{9} = 2970$$

8) Give a summary of the life and mathematical contributions of Leonard Euler. 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. (Note: Euler is my favorite mathematician!)

Solution: Leonhard Euler was born on April 15, 1707, in Basel, Switzerland. Though originally slated for a career as a rural clergyman, Euler showed an early aptitude and propensity for mathematics, and thus, after studying with Johan Bernoulli, he attended the University of Basel and earned his master's during his teens. Moving to Russia in 1727, Euler served in the navy before joining the St. Petersburg Academy as a professor of physics and later heading its mathematics division. In the mid-1740s, Euler was appointed the mathematics director of the newly created Berlin Academy of Science and Beaux Arts, taking on a variety of management roles as well becoming head of the organization itself for a time starting in 1759. Not appointed president proper of the academy by King Frederick II, Euler received patronage from Catherine II and in 1766 returned to Russia to head the St. Petersburg Academy. Over his career, Euler came up with an array of principles which laid the foundation for much of modern mathematics as we know it. He was a revolutionary thinker in the fields of geometry, trigonometry, calculus, differential equations, number theory and notational systems—including the utilization of π and *f(x)*—among a legion of other accomplishments. His Euler's Identity theorem is often cited as the most delightful of equations and his work also focused on the fields of astronomy/lunar motion, acoustics, mechanics and music. Some neat results due to Euler's work are:

$$\sum_{i=1}^{\infty} \frac{1}{i^2} = \frac{\pi^2}{6}$$

For all planar graphs, $V - E + F = 2$, where V is the number of vertices, E is the number of edges and F is the number of faces.

A connected graph has an Euler Circuit if and only if the degree of each vertex in the graph is even.

For all positive integers a and n with gcd(a, n) = 1, $a^{\phi(n)} \equiv 1 \ (mod\ n)$, where $\varphi(n)$ is the Euler Phi function, equal to the number of integers from the set {1, 2, 3, …, n} that are relatively prime to n.