COT 3100 Fall 2020 Homework #4 Solutions

1) Find all integer solutions to the equation 1326x + 348y = 18.

Solution

Start with Euclidean

1326 = 3 * 348 + 282	⇔	282 = 1326 – (3 * 348)
348 = 1 * 282 + 66	⇔	66 = 348 – (1 * 282)
282 = 4 * 66 + 18	⇔	18 = 282 – (4 * 66)
66 = 3 * 18 + 12	⇔	12 = 66 – (18 * 3)

18 = 1 * 12 + 6
12 = 2 * 6
Therefore gcd(1326, 348) = 6

Next do Extended Euclidean

6 = 18 – (1 * 12)
6 = 18 – (66 – (3 * 18)) = 4 * 18 - 66
6 = 4 (282 – (4 * 66)) – 66 = 4 * 282 – 17 * 66
6 = 4 * 282 – 17 (348 – 282) = 4 * 288 – 17 * 348 + 17 * 282 = 21 * 282 – 17 * 348
6 = 21 * (1326 – 3 * 348) – 17 * 348 = 21 * 1326 – 80 * 348
Now we need to multiply both sides of the equation by 3
63 * 1326 – 240 * 348 = 18
x = 63, y = -240 is one solution to this problem. To find all integer solutions we can divide both 1326 and 348 by our gcd (6) to get a = 221 and b = 58

Thus the set of all solutions is $\{(x, y) \mid x = 63 + 58c, y = -240 – 221c, c \in Z\}$

2) (a) Find all integer solutions to the equation 161x + 71y = 1.

Solution

Starting with Euclidean again
161 = 2 * 71 + 19
71 = 3 * 19 + 14
19 = 1 * 14 + 5
14 = 2 * 5 + 4
5 = 1 * 4 + 1

1 = 5 – 1 * 4
1 = 5 – 1 * (14 – 2 * 5) = 5 – 1 * 14 + 2 * 5 = 3 * 5 – 1 * 14
1 = 3 * (19 – 14) – 1 * 14 = 3 * 19 – 4 * 14
1 = 3 * 19 – 4 * (71 – 3 * 19) = 3 * 19 – 4 * 71 + 12 * 19 = 15 * 19 – 4 * 71
1 = 15 * (161 – 2 * 71) – 4 * 71 = 15 * 161 – 34 * 71
one solution: x = 15 y = -34

Thus the set of all solutions is $\{(x, y) \mid x = 15 + 71c, y = -34 – 161c, c \in Z\}$

(b) Find all integer solutions to the equation $161x + 71y = 15$.

To find this we must multiply the base answers (not the offset though) by 15.

Thus the set of all solutions is $\{(x, y) \mid x = 225 + 71c, y = -510 - 161c, c \in Z\}$

By plugging a number into c (e.g. -3), we can get the following equivalent solution:

$\{(x, y) \mid x = 12 + 71c\ y = -27 - 161c, c \in Z\}$

(c) Find 71^{-1} mod 161. (Note: Answer must be in between 0 and 160, inclusive.)

$15 * 161 + -34*71 = 1$ can be rewritten as
$15 * 161 - 34 * 71 \equiv 1 \pmod{161}$
$0 - 34 * 71 \equiv 1 \pmod{161}$
$71 \equiv -34 \pmod{161}$

$71^{-1} \equiv 127 \pmod{161}$

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

Solution
gcd(a, b, c) looks at the largest number of prime factors shared between all three numbers

$\gcd(a, b, c) = 2^4 3^3 5^2$

lcm(a, b, c) is looking for the minimum numbers of prime factors for all to be divisible

$\text{lcm}(a, b, c) = 2^7 3^7 5^8 7^3 11^8$

4) For the numbers a, b and c listed in problem 4, determine the number of divisors each of those numbers has.

Solution
$a = 2^5 3^6 5^2 7^3$
number of divisors = $(5+1)(6+1)(2+1)(3+1) = 6 * 7 * 3 * 4 = 504$ divisors

$b = 2^4 3^3 5^8 11^2$
number of divisors = $(4+1)(3+1)(8+1)(2+1) = 5 * 4 * 9 * 3 = 540$ divisors

$c = 2^7 3^7 5^5 11^8$
number of divisors = $(7+1)(7+1)(5+1)(8+1) = 8 * 8 * 6 * 9 = 3456$ divisors

5) How many zeroes are at the end of $\frac{2000!}{500!1500!}$?

Solution

To find this we need to keep track of how many 5s are in each factorial. Every 5 when multiplied by 2 will add an extra 0 to the end of our number.
2000 / 5 = 400
Now we check every power of 5 as well since those will account for more. e.g. $25 = 5^2$
2000/25 = 80 Since we counted the first 5 in our first division we only have to count 1 extra 5 per power of 5
2000/125 = 16
2000/625 = 3 We can ignore any decimal because only 3 will show up in the factorial
number of 5's in the prime factorization of 2000! = 499

Repeat this process for 500 and 1500
500/5 = 100
500/25 = 20
500/125 = 4
number of 5's in prime factorization of 500! = 124

1500/5 = 300
1500/25 = 60
1500/125 = 12
1500/625 = 2
number of 5's in the prime factorization of 1500! = 374

When dividing we subtract 124 and 374 from 499 and end up with 1 zero.

6) Prove for positive integers a and b with a > b, that gcd(a, b) = gcd(a-b, b). One way to prove this is to show that any common divisor of a and b is also a common divisor of a-b and b, AND to show that any common divisor of a-b and b is also a common divisor of a and b. (This proves that the two pairs of numbers have the same set of common divisors, which, in turn, proves that the greatest common divisors have to be the same.)

Solution

First, we show that for an arbitrary divisor d of a, b, that d | a-b and d | b.

Let d be a common divisor of a and b. Thus, d | a and d | b. Under this assumption, clearly d | b. Thus, it remains to be proved that d | (a - b).

Since d | a and d | b, there exist integers c and e such that
a = cd
b = ed

a – b =

cd – ed =
d(e – c), which means d | (a – b)

Thus, this shows that any common divisor of a and b, is a common divisor of a-b and b.

Now, we show the other direction:

Any common divisor of a-b and b is a common divisor of a and b.

Let d be a common divisor of a-b and b. It follows that there are integers f and g such that:

a – b = fd
b = gd

a =
(a - b) + b =
fd + gd =
d(f + g) which proves that d | a. Since we already know that d | b, it follows that d is a common divisor of a and b.

Thus, we've proven that any common divisor of a and b is also a common divisor of a-b and b, and vice versa. This means that the set of common divisors for a and b is the same set of common divisors for a-b and b. We can then conclude that the greatest common divisors for both pairs must be the same, as desired.

7) Give a summary of the academic contributions of Dr. Ron Rivest, a computer scientist. Be sure to include information about RSA encryption in your write up. 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.

Dr. Ron Rivest is a current professor at MIT, and a co-author of the book Introduction to Algorithms also referred to as CLRS(this book is used as recommended reading at UCF too!). One of Rivest's inventions is the Three Ballot voting system which is a system designed to be used for voting and use cryptographies methods without using encryption. The idea behind it is to use three votes, one verifiable and two anonymous. This wasn't a perfect system and was prone to an attack in certain instances though.

Dr Rivest also helped create the RSA(Rivest-Shamir-Adleman) algorithm where the encryption key is public but the decryption key is private. The idea behind this algorithm is to use a number with large prime factors which makes it incredibly difficult to solve. There is in fact no process to defeat it if large enough numbers are used. One of the basic principles behind the RSA algorithm is to find three very large positive integers e, d and n, such that for all integers m where $0 \leq m < n$, $(m^e)^d \equiv m \pmod{n}$. Even if you know e and n or m, it will still be very difficult to find d. The public part of the RSA key would be the integers e and n, while the private part for decryption would be d.

Sources:
https://en.wikipedia.org/wiki/RSA_(cryptosystem)
https://en.wikipedia.org/wiki/Ron_Rivest
https://en.wikipedia.org/wiki/ThreeBallot