Cryptology 6

Ryan Kellar

April 2024

1 Problem 1

1.1 a)

$\gcd(51, 89) = \gcd(89, 51)$
$89x + 51y = 1$
$89 = 1 * 51 + 38$
$51 = 1 * 38 + 13$
$38 = 13 * 2 + 12$
$13 = 1 * 12 + 1$
$12 = 1 * 12 + 0$
Therefore, $\gcd(51, 89) = 1$

1.2 b)

$\gcd(102, 202) = \gcd(202, 102)$
$202x + 102y = 1$
$202 = 102 * 1 + 100$
$102 = 100 * 1 + 2$
$100 = 50 * 2 + 0$
Therefore, $\gcd(102, 202) = 2$

1.3 c)

$\gcd(666, 1414) = \gcd(1414, 666)$
$1414x + 666y = 1$
$1414 = 666 * 2 + 82$
$666 = 82 * 8 + 10$
$82 = 10 * 8 + 2$
$10 = 2 * 5 + 0$
Therefore, $\gcd(666, 1414) = 2$

2 Problem 2

2.1 a)

$1 = 13 - 12 * 1$
$= 13 - (38 - 13 * 2) * 1$
$= 13 - (38 - (51 - 38 * 1) * 2) * 1$
$= 13 - (38 - (51 - (89 - 51 * 1) * 1) * 2) * 1$

2.2 b)

$2 = 102 - 100 * 1$
$2 = 102 - (202 - 102 * 1) * 1$

2.3 c)

$2 = 82 - 10 * 8$
$2 = 82 - (666 - 82 * 8) * 8$
$2 = 82 - (666 - (1414 - 666 * 2) * 8) * 8$

3 Problem 3

$50x + 127y = 1$
$127 = 50 * 2 + 27$
$50 = 27 * 1 + 23$
$27 = 23 * 1 + 4$
$23 = 4 * 5 + 3$
$4 = 3 * 1 + 1$
$3 = 1 * 3 + 0$

Therefore, $\gcd(50, 127) = 1$ Using extended:
$1 = 4 - 3 * 1$
$= 4 - 3 * 1$
$= 4 - (23 - 4 * 5) * 1$
$= 4 * 6 - 23 * 1$
$= 27 * 6 - 23 * 7$
$27 * 6 - 7 * (50 - 27 * 1)$
$= (127 - (50 * 2)) * 13 - 50 * 7$
$= 127 * 13 - 50 * 33$
$= 94$ Using this, we can prove that the modular inverse $50 \mod 127 = 94$

4 Problem 4

To find the decoding number, D, we need to find the modular inverse of the encoding number, E mod $(p - 1)(q - 1)$.

After plugging in the values, we need to find the modular inverse of $5 \mod 192$.
$\gcd(5, 192) = 5x + 192y = 1$
$192 = 5 * 38 + 2$
$5 = 2 * 2 + 1$
$2 = 2 * 1 + 0$
Using extended euclidean algorithm, we find the modular inverse to be 77.
This means that the decoding number $D = 77$.

5 Problem 5

5.1 a)

$\gcd(9876543210, 123456789) = 9$

5.2 b)

$\gcd(11111111111, 1000000001) = 1$

5.3 c)

$\gcd(45666020043321, 73433510078091009) = 3$

6 Problem 6

6.1 a)

$\gcd(9876543210, 123456789) = 9$

6.2 b)

$\gcd(11111111111, 1000000001) = 1$

6.3 c)

$\gcd(45666020043321, 73433510078091009) = 3$

7 Problem 7

7.1 a)

Euler's theorem says that for any number $\forall a | a \in \mathbb{Z}$, $a^{\phi(m)} \equiv 1 \mod m$. In this case of this problem, that means that $2^{\phi(97)} \equiv 1 \mod 97 \implies 2^{96} \equiv 1 \mod 97$.
We can cleverly rewrite this to show that $2^{95} * 20 \equiv 1 \mod 97$, which is exactly how the modular inverse is defined.
In other words, 2^{95} is the modular inverse of 20 in $\mod 97$.

Now all we have to do is restrict 2^{95} to the domain of $\mathbb{Z}_{97}$. After this simplification, we indeed get that 34 is the modular inverse of 20 in $\mod 97$.

7.2 b)

Using Euler's theorem would require that you do likely hundreds and hundreds of coprimality calculations, depending on what your a and m values are. Each of these singular coprimality calculations require a gcd computation of their own, so it's much much more computationally expensive since it's essentially repeating a similar process to the basic/extended euclidea algorithm hundreds of times just to calculate Euler's totient function, $\phi(m)$.