ICS 505 Cryptography

Practice Assignment 2 - Mathematics Background I

Dr. Muhammad Hataba, muhammad.hataba@giu-uni.de
TA. John Ehab, john.ehab@giu-uni.de

Exercise 1–1

The Euclidean Algorithm is designed with solving the following equation in mind:

$$S * A + T * B = C$$

Where C is commonly $GCD(A, B)$. For the following values of A, B; Find C, S, and T.

(a) $A = 24, B = 15.$

(b) $A = 60, B = 25.$

(c) $A = 144, B = 100.$

(d) $A = 162, B = 225.$

(e) $A = 101, B = 103.$

(f) $A = 101, B = 107.$

(g) $A = 1776, B = 2015.$

(h) $A = 1011, B = 1101.$

(i) $A = 1000, B = 888.$

(j) $A = 332211, B = 112233$

Exercise 1–2

Given that $2391 = 23 * 100 + 91$, decide whether or not $gcd(2391, 23) = gcd(23, 91)$, and justify your answer.
(Hint: No computation is needed.)

Exercise 1–3

Find the multiplicative inverse of x in Z_m for the following:

(a) $x = 3, m = 7.$

(b) $x = 7, m = 13.$

(c) $x = 17, m = 19.$

(d) $x = 28, m = 32.$

(e) $x = 2, m = 8.$

(f) $x = 3, m = 9.$

(g) $x = 19, m = 23.$

Exercise 1–4

If possible, find integers x such that:

(a) $100|37x - 1$

(b) $601|178x - 1$

(c) $100|89x - 1$

Exercise 1–5

Given $a|b$ and $c|d$ prove that $ac|bd$.

Exercise 1–6

Given p is a prime and $p|a$ and $p|(a^2 + b^2)$ prove that $p|b$

Exercise 1–7

If $GCD(a, b) = p$, a prime, what are the possible values of:

- $GCD(a^2, b)$
- $GCD(a^3, b)$
- $GCD(a^2, b^3)$

Exercise 1–8

Solve the following:

(a) $(15 * 29) \bmod 13$

(b) $(2 * 29) \bmod 11$

(c) $(2 * 3) \bmod 19$

(d) $(-11 * 3) \bmod 7$

Exercise 1–9

Find all integers n, such that $0 < n < m$, where n and m are relatively prime. Do so for $m = 4, 5, 9, 26$

Exercise 1–10

Find $\phi(n)$ for the following values of n:

(a) $n = 2$

(b) $n = 7$

(c) $n = 15$

(d) $n = 80$

(e) $n = 100$

(f) $n = 117$

(g) $n = 10213$

Exercise 1–11

Using Euler's Theorem:

$$a^{\phi(n)} = 1 \bmod n$$

Solve the following:

(a) What is the value of $3^{330} \bmod 7$

(b) What are the last 3 digits of 2^{2020}

(c) Find the value of $(1 + 2 + 2^2 + 2^3 + \ldots\ldots + 2^{100}) \bmod 125$

(d) $3^{2012} \bmod 17$

(e) $2^{1000} \bmod 13$

(f) $5^{117} \bmod 8$

Exercise 1–12 Just for Fun

- Implement the extended Euclidean algorithm on your language of choice
- The element 0 has no multiplicative inverse, what would happen if it did?

Useful Links

http://www3.cs.stonybrook.edu/~cse371/chapter8.pdf
http://www.logicmatters.net