UC Computer Science and Software Engineering

COSC362 Data and Network Security
Semester Spring, 2021

Lab 2: Number Theory and Finite Fields (Discrete Mathematics)

Exercises from Lecture 3.

Euclidean algorithm and back substitution.

Let us start with an example. Let $a = 19$ and $b = 5$. Our goal is to find $d = \gcd(19, 5)$. (Note that 19 and 5 are prime numbers, so we can guess that $d = 1$.) We replace a, b with their assigned values in $a = bq + r$ and find q, r: $19 = 5 \times 3 + 4$. We check that $0 \leq r = 4 < 5$. Then, given $b = 5$ and $r = 4$, we use the same technique.

$$\begin{aligned} 19 &= 5 \times 3 + 4 \\ 5 &= 4 \times 1 + 1 \\ 4 &= 1 \times 4 + 0 \end{aligned}$$

The last line gives us a null remainder, hence we stop, and find the last remainder non equal to zero, here it is 1. Therefore, $d = \gcd(19, 5) = 1$.

Then, we are interested in finding x, y from $ax + by = d$. We replace using the assigned values: $19 \times x + 5 \times = 1$. We use back substitution to find x, y as follows. We first rewrite the last equality $5 = 4 \times 1 + 1$ as $1 = 5 - 4 \times 1$. We do the same with the second last one equality $19 = 5 \times 3 + 4$ as $4 = 19 - 5 \times 3$. Then, given the latter ($4 = 19 - 5 \times 3$), we replace in the former ($1 = 5 - 4 \times 1$) as follows:

$$\begin{aligned} 1 &= 5 - 4 \times 1 \\ &= 5 - (19 - 5 \times 3) \times 1 \\ &= 5 \times 1 + 19 \times (-1) + 5 \times 3 \\ &= 5 \times (1 + 3) + 19 \times (-1) \\ &= 5 \times 4 + 19 \times (-1) \\ &= 19 \times (-1) + 5 \times 4 \end{aligned}$$

And we are done: we have found $x = -1$ and $y = 4$. One can check easily that $19 \times (-1) + 5 \times 4 = -19 + 20 = 1$.

A trick to get the inverse as a positive integer.

Let $\gcd(a, n) = 1$ for two integers a and n. We are interested in finding the inverse $a^{-1} \mod n$ (slides 20-21/33 of Lecture 3). Let us suppose that we have found the values x, y such that $ax + ny = 1$. We notice that x is the inverse of a.

cont/...

However, suppose that $x < 0$ (a negative integer), and so x does not look "nice". We are now interested in finding an element $0 \leq b$ (a positive integer) such that $x \equiv b \mod n$.

Rewriting $x \equiv b \mod n$: there is an integer k such $x - b = kn$ (slides 14-15/33 of Lecture 3). Unknowns are b and k. We can also write $x = kn + b$. Since x is negative and n and b are positive integers, we can expect that k is negative too. Try $k = -1$ and see what b is. We should get b such that $0 \leq b < n$, and so we are all good.

For instance, let $n = 23$ (a prime number) and $x = -8$. Thus, we have $-8 = k \times 23 + b$. Let us see with $k = -1$:

$$\begin{aligned} -8 &= (-1) \times 23 + b \\ -8 &= -23 + b \\ -8 + 23 &= b \\ 15 &= b \end{aligned}$$

We now check that $0 \leq b < n$: indeed $0 \leq 15 < 23$. Therefore, $-8 \equiv 15 \mod 23$.

QUESTION 1

Using the Euclidean algorithm, determine:

(a) $\gcd(23, 29)$
(b) $\gcd(893, 703)$
(c) $\gcd(1045, 77)$

QUESTION 2

Use the Euclidean algorithm to find which of the following inverses exist (inverses exist when the GCD of the given number and modulus is equal to 1). For those that do exist, use back substitution to find the inverse.

(a) $3^{-1} \mod 31$
(b) $21^{-1} \mod 91$
(c) $39^{-1} \mod 195$
(d) $41^{-1} \mod 195$

QUESTION 3

Demonstrate that $\mathbb{Z}_5$ is a field by writing out the addition and multiplication tables. Tables should look like:

cont/...

$+$	0	1	2	3	4
0	....	...	....	...	...
1	....	...	....	...	...
2	....	...	....	...	...
3	....	...	....	...	...
4	....	...	....	...	...

$\cdot$	1	2	3	4
1	....	...	....	...
2	....	...	....	...
3	....	...	....	...
4	....	...	....	...

Note that the multiplication table only applies to $\mathbb{Z}_5 \setminus \{0\}$ (note that $\mathbb{Z}_5 \setminus \{0\}$ can also be denoted as $\mathbb{Z}_5^*$). You should fill "..." with values between 0 (resp. 1) and 4 (resp. 4).

What do you need to check in the tables in order to demonstrate that $\mathbb{Z}_5$ is a field?

Hint: You need to check that the tables are abelian groups in both cases (see slide 18/33 of Lecture 3), meaning that you check that the following properties hold: *Closure*, *Identity*, *Inverse*, *Associativity*, *Commutativity*, and in addition *Distributivity*.

QUESTION 4

(a) How many elements are there in $\mathbb{Z}_{11}^*$? Find a generator for this group.
Hint: Find it by trial and error.
(b) How many elements are there in $\mathbb{Z}_{12}^*$? Does this group have a generator?
Hint: Check the square of each element in $\mathbb{Z}_{12}^*$.

Example: Finding a generator of $\mathbb{Z}_p^*$.

Let $p = 7$ be a prime number. Then, $p - 1 = 6$ and its prime factors are 2 and 3. Given g in $\mathbb{Z}_p^*$, we check whether:

- $g^{6/2} = g^3 \neq 1 \mod 7$
- $g^{6/3} = g^2 \neq 1 \mod 7$

If so, then g is a generator of $\mathbb{Z}_p^*$. If not, then try with another g. You do not need to check $g = 1$ since it is equal to $1 \mod 7$.

QUESTION 5

Write the XOR operation ($\oplus$) as a Boolean truth table. Then show, using truth tables, that $z = x_1 \vee x_2$ defines the same Boolean function as $z = x_1 \oplus x_2 \oplus (x_1 \wedge x_2)$.

The Boolean truth table should look like:

x_1	x_2	$z = x_1 \vee x_2$	$a = x_1 \oplus x_2$	$b = x_1 \wedge x_2$	$z = a \oplus b$
1	1	...	...	...	...
1	0	...	...	...	...
0	1	...	...	...	...
0	0	...	...	...	...

Fill “...” with the correct bit values.