Tutorial 4
GCD and Modulo Arithmetic

1 Discussion questions

Discussion questions are meant for discussion on the IVLE Forum. You may try them on your own or discuss them with your classmates. No answers will be provided by us.

D1. Recall that two integers a, b are said to be coprime iff $\gcd(a, b) = 1$. List all positive integers less than 30 that are coprime with 30.

D2. Show that if a, b, m are integers such that $m \geq 2$ and $a \equiv b \pmod{m}$, then $\gcd(a, m) = \gcd(b, m)$.

D3. Suppose that a, b are integers such that $a \equiv 4 \pmod{13}$ and $b \equiv 9 \pmod{13}$. Find the integer c with $0 \leq c \leq 12$ such that:

(a) $c \equiv 9a \pmod{13}$.

(b) $c \equiv 11b \pmod{13}$.

(c) $c \equiv a^2 + b^2 \pmod{13}$.

2 Tutorial questions

Q1. (a) Factorize 1320 and 714 into primes, and hence determine their gcd. Do this by hand.

(b) Calculate $\gcd(1320, 714)$ using Euclid's algorithm. Do this by hand, not by a program.

(c) Explicitly find $x, y \in \mathbb{Z}$ such that $\gcd(1320, 714) = 1320x + 714y$. Is (x, y) unique?

Q2. Number bases.

(a) Convert $(4103)_5$ to base 10, base 2, and base 7.

(b) Calculate by hand $(2B1)_{16} + (C3)_{16}$ in two ways: (i) directly in base 16, and (ii) converting both numbers to base 10, doing the addition, and then converting the sum back to base 16. Verify that your answers in (i) and (ii) are the same.

Q3. Well Ordering Principle.

(a) Prove by Mathematical Induction that $\forall n \in \mathbb{Z}^+,\ n < 2^n$.

(b) Using the the Well Ordering Principle 2 (Slide 10 of `Week5_NumberTheory2.pdf`), prove that every integer $n \geq 1$ can be written as $n = s2^r$, for some integer r, and some odd integer s.

Hint: Given n, let $S = \{\ k \in \mathbb{Z} \mid n = m2^k,\ \text{where } m \in \mathbb{Z}\ \}$. Apply the Well Ordering Principle 2 on the set S.

Q4. The definition of gcd can be extended to three integers as well:

> Given any $a, b, c \in \mathbb{Z}$ not all of which are zero:
>
> Define $\gcd(a, b, c)$ to be an integer d (if it exists) such that:
>
> i. $d \mid a$ and $d \mid b$ and $d \mid c$; and
>
> ii. For any $x \in \mathbb{Z}$, if $x \mid a$ and $x \mid b$ and $x \mid c$ then $x \leq d$.
>
> And we say that $\gcd(a, b, c)$ does not exist otherwise.

(a) Prove that for any $a, b, c \in \mathbb{Z}$ not all of which are zero, $\gcd(a, b, c)$ exists.

(b) Prove that for any $a, b, c \in \mathbb{Z}$ such that a, b are not both zero, $\gcd(a, b, c) = \gcd(\gcd(a, b), c)$.

(c) Write code, in a programming language of your choice, that computes the gcd of three integers.

(d) Show that your code works by computing the gcd of 2406, 1296 and 654.

Q5. Modulo arithmetic.

(a) Show that 7 divides $1^{47} + 2^{47} + 3^{47} + 4^{47} + 5^{47} + 6^{47}$, without explicitly calculating each term.

(b) Calculate 2017^{100} *mod* 50.

(c) Characterize all $k \in \mathbb{Z}$ such that $3^k \equiv 4 \pmod{11}$; that is, write the solution in the form: $k = aq + b, \forall q \in \mathbb{Z}$, where a, b are nonnegative integers that you need to determine.

Q6. Modulo inverses.

(a) Find $220^{-1} \pmod{21}$.

(b) Find the least positive solution for the congruence: $220x \equiv 6 \pmod{21}$.

(c) Solve the equation $110x + 21y = 3$ for integers x, y.

Q7. US coins come in these denominations (their nicknames are in parenthesis): 1¢ (penny), 5¢ (nickel), 10¢ (dime), 25¢ (quarter), 50¢ (half dollar), 100¢ (dollar). Aiken loathes the penny and never uses them.

Carrying some coins, Aiken enters a candy store to buy some sweets. She likes several types of sweets, each type with a different price (a positive integer in US cents) clearly labeled on each jar. Alas, Aiken discovers that if she buys 2 sweets of any type, she is a penny short. If she buys 3 sweets of any type, she will receive an unwanted penny in change. In desperation, she picks 1 sweet of every type, and is surprised to find she can pay for the sweets exactly with her coins.

Determine the types of sweets and their prices. What coins does Aiken possess? (A solution with fewer types of sweets and coins is preferred.)

Hint: Derive three simultaneous equations (congruent modulo n, for a suitable choice of n) from the problem statement. Then solve the equations.