KING SAUD UNIVERSITY
COLLEGE OF COMPUTER & INFORMATION SCIENCES
DEPT OF COMPUTER SCIENCE

CSC281 Discrete Mathematics for Computer Science Students
First Semester 1440/1441 AH
Due: TBA
Instructor: Prof. Aqil Azmi

Group Term Project

In this project you will solve a quadratic congruence equation of the form,

$$ax^2 + bx + c \equiv 0 \bmod p,$$

where $a, b, c \in \mathbb{Z}$, and p is an odd prime. Let $\mathbb{Z}_p = \{0, 1, \ldots, p-1\}$. We show how to solve this problem when $a \not\equiv 0 \bmod p$. Then,

$$\begin{aligned} ax^2 + bx + c \equiv 0 \bmod p \quad &\Leftrightarrow 4a^2x^2 + 4abx + 4ac + b^2 - b^2 \equiv 0 \bmod p, \\ &\Leftrightarrow (2ax+b)^2 \equiv b^2 - 4ac \bmod p. \end{aligned}$$

So, for the congruence to have solutions, it must be that $b^2 - 4ac = \alpha^2$ (i.e. a perfect square) for some $\alpha \in \mathbb{Z}_p$. That is, $2ax + b \equiv \pm\alpha \bmod p \Leftrightarrow x \equiv (-b \pm \alpha) / 2a \bmod p$. Which is our solution.

How to determine if $b^2 - 4ac$ has a solution and what is the value of α. Consider the problem of solving the equation $y^2 \equiv d \bmod p$ where $p \not| \, d$. This equation has either no solution or exactly two solutions. There is a theorem that says $y^2 \equiv d \bmod p$ has a solution iff $d^{(p-1)/2} \equiv 1 \bmod p$, and no solution iff $d^{(p-1)/2} \equiv p - 1 \bmod p \equiv -1 \bmod p$.

Next, to calculate the value of α, use the following simple algorithm:

$$\boxed{\begin{array}{l} k \leftarrow 0 \\ \text{while } (d + pk \text{ is NOT perfect square}) \ k \leftarrow k+1 \\ \alpha \leftarrow \sqrt{d + pk} \end{array}}$$

For example, solve $15x^2 + 19x + 6 \equiv 0 \bmod 11$. We have $(p = 11, a = 15, b = 19, c = 6)$, and $b^2 - 4ac \equiv 1^2 \bmod 11$, and so we use the above theorem to get,

$15x^2 + 19x + 6 \equiv 0 \bmod 11 \Leftrightarrow x \equiv \dfrac{-19 \pm 1}{2 \cdot 15} \bmod 11 \Leftrightarrow \dfrac{3 \pm 1}{8} \bmod 11$. We get the solutions $x \equiv \{4 \cdot \text{inverse of 8 mod 11}, 2 \cdot \text{inverse of 8 mod 11}\} \equiv \{6, 3\}$. Recall that inverse of 8 in modulo 11 is 7, which can be computed using going backward through Euclidean Algorithm.

Another example. Solve $14x^2 + 7x + 6 \equiv 0 \bmod 11$. Here we get $b^2 - 4ac \equiv 10 \bmod 11$. We do not have a solution since $10^5 \equiv -1 \bmod 11$.

Yet another example. Solve $y^2 \equiv 5 \bmod 61$. This system has a solution as $5^{30} \equiv 1 \bmod 61$. To find the solutions, we keep adding the modulus to $d = 5$ until we get a perfect square (see the algorithm),

$$y^2 \equiv 5 \equiv 5 + 61 \equiv 5 + 2 \cdot 61 \equiv 5 + 3 \cdot 61 \equiv \cdots \equiv 5 + 20 \cdot 61 = 1225 = 35^2 \bmod 61.$$

This gives the solution $y = 35$, and $y = -35 \equiv 26 \bmod 61$.

Project

Write a program that accepts four inputs: *a*, *b*, *c* and *p*. Make sure $a \not\equiv 0 \bmod p$ and *p* is odd prime. You should output the solution *x* = {*t*, *s*}, or "NO SOLUTION".

Instructions

This is a group project. Each 4-5 students will work as a team. You are free to use *any* convenient programming language. This project is worth 15 points.

What to submit

(a) Cover sheet with your names and a signed pledge.
(b) Write-up of the project (brief description of your algorithm; the data structure(s) used; sample runs and the conclusion).
(c) Hardcopy of your source code + Flash memory/CD with source and executable.