cwork4b.tex 29/10/2003

MAS/202 Algorithmic Mathematics: Coursework 4

Franco Vivaldi

DEADLINE: Wednesday of week 6, at 12:00 pm.

CONTENT: Modular arithmetic

M⋆icroESSAY : Write an essay on modular arithmetic. [$\notin$, 100]

Problem 1.

(a) Write five elements of $\equiv_7$. [*Hint:* $\equiv_7$ is a *relation.*]

(b) Find all solutions to the equation $x^3 = x$ in $\mathbb{Z}/(8)$.

(c) Show that the function

$$f : \mathbb{Z}/(9) \to \mathbb{Z}/(9) \qquad\qquad f(x) = x\,[7]_9$$

is injective.

(d) Show that the function

$$f : \mathbb{Z}/(14) \to \mathbb{Z}/(14) \qquad\qquad f(x) = x\,[12]_{14}$$

is not injective.

(e) Compute the value of the expression

$$[1110]_{11}[2588]_{11} + [-1000]_{11}$$

giving your answer in the form $[k]_{11}$, with $0 \leq k < 11$.

Problem 2. Let $x \in \mathbb{Z}/(m)$. We say that x is a square if there exists $y \in \mathbb{Z}/(m)$ such that $x = y^2$.

(a) Find all squares in $\mathbb{Z}/(13)$.

(b) Write an algorithm to the following specifications

`Algorithm MSquare`
`INPUT`: $a, m \in \mathbb{Z}$, $m > 1$.
`OUTPUT`: TRUE is $[a]_m$ is a square in $\mathbb{Z}/(m)$, and FALSE otherwise.

(c) Describe the structure of the algorithm `MSquare` in fewer that 50 words, minimizing the use of symbols.

Problem 3. Let m be an integer, and $a, b \in \mathbb{Z}/(m)$.

(a) Determine all invertible elements in each of $\mathbb{Z}/(6)$, $\mathbb{Z}/(7)$, $\mathbb{Z}/(8)$.

(b) Define concisely $[\not\in]$, hence compute

$$\sum_{k=1}^{6} \frac{[1]_7}{[k]_7}.$$

(c) Prove that if a and b are invertible, then so is a^{-1} and ab.

(d) Suppose that b is invertible. Prove that $ab = [0]_m$ if and only if $a = [0]_m$.