# MAS/202 Algorithmic Mathematics: Coursework 7

Franco Vivaldi

*DEADLINE: Wednesday of week 9, at 12:00 pm.*

*CONTENT: Inverses, gcd*

---

**Problem 1.** Write down all the invertible elements of $\mathbb{Z}/(24)$.
[*Hint:* use theorem 21 of the web-book.]

**Problem 2.** Write an algorithm to the following specifications

`Algorithm IsInvertible`

`INPUT`: $i, m \in \mathbb{Z}$, $m > 1$.

`OUTPUT`: TRUE if $[i]_m$ is invertible in $\mathbb{Z}/(m)$, FALSE otherwise.

[*Hint:* use `GCD`, and the hint of previous problem.]

**Problem 3.** The Euler's $\phi$-function is defined on the positive integers, as follows: $\phi(1) = 1$; for $m > 1$, $\phi(m)$ is the number of invertible elements in $\mathbb{Z}/(m)$. Write the algorithm to the following specifications:

`Algorithm Phi`

`INPUT`: $m$, a positive integer.

`OUTPUT`: $\phi(m)$.

[*Hint:* use `IsInvertible`, and section 2.5.1 of the web-book.]

**Problem 4.** Write an algorithm to the following specifications.

```
Algorithm AllGCDs
```

`INPUT`: $a, b, p$, where $p$ is a prime, and $a, b \in \mathbb{Z}/(p)[x]$.

`OUTPUT`: $S$, where $S = \{f_1, f_2, \ldots\}$ is the set
of all gcds of $a$ and $b$ in $\mathbb{Z}/(p)[x]$.

[*Hint:* how do you get all gcds, if you have one of them? See end of section 5.3 of web-book, and exercise 5.11. To create the set of gcds, look at `IntegerFactorization`, for inspiration.]

**Problem 5.** Apply the algorithm `Inverse` to determine whether $[37]_{84}$ is invertible, and if so, to find its inverse.

**Problem 6.** Let $F = \mathbb{Q}, \mathbb{R}, \mathbb{C}$, or $\mathbb{Z}/(p)$, where $p$ is a prime (or indeed, $F$ can be any field). Let $f$ and $g$ be non-zero polynomials in $F[x]$. Prove that $\deg(fg) = \deg(f) + \deg(g)$.
[*Hint:* if you do not use the fact that $F$ is a field, you proof is wrong.]

**Problem 7.** Suppose that $g$ is a gcd of polynomials $a$ and $b$ in $F[x]$ ($F$ as above). Prove that if $f$ is a degree zero polynomial in $F[x]$, then $fg$ is also a gcd of $a$ and $b$.