Modular Arithmetic

George E. Collins

October 13, 1998

For any integer $m > 1$ and any integer $a >= 0$, define $\mathrm{rem}(m, a)$ to be the remainder obtained when a is divided by m. The remainder is non-negative and less than m. Let $Z_m = \{0, 1, \ldots, m-1\}$. For $a, b \in Z_m$, define $a \oplus b = \mathrm{rem}(m, a+b)$ and $a \odot b = \mathrm{rem}(m, ab)$. It is then easy to verify associativity, distributivity and commutativity of these operations, establishing that Z_m is a commutative ring when equipped with these operations. Also, 1 is a multiplicative identity for Z_m. However if m is not a prime then Z_m is not an integral domain because if a is a proper divisor of m and $b = m/a$ then $a \odot b = 0$ in Z_m. If m is a prime then Z_m is an integral domain for if $a, b \in Z_m$ then a and b are relatively prime to m and therefore ab is also relatively prime to m, so $\mathrm{rem}(m, ab) \neq 0$. In fact, if m is a prime then Z_m is a field, that is, every nonzero ellement of Z_m has a multiplicative inverse. Let $0 < a < m$. The extended Euclidean algorithm applied to m and a computes integers u and v such that $um + va = \gcd(m, a) = 1$ with $|u| \leq a/2$ and $|v| \leq m/2$. Let $w = v$ if $v > 0$ and $w = v + m$ otherwise. Then $0 < w < m$ and $\mathrm{rem}(m, wa) = 1$, so $w \odot a = 1$ in Z_m.

For the case that m is a β-digit, the arithmetic operations in Z_m are implemented in SACLIB in a straightforward way by the programs MDSUM, MDDIF, MDNEG, MDPROD, MDINV and MDQ. For the general case there are corresponding programs MISUM, MIDIF, MINEG, MIPROD, MIINV and MIQ.

For any modulus $m \geq 2$ and any integer A, define $H_m(A)$ to be the unique integer in Z_m that is congruent to A modulo m. For $A \geq 0$, $H_m(A) = \mathrm{rem}(m, A)$, but for $A < 0$, $\mathrm{rem}(m, A) \leq 0$ and if $\mathrm{rem}(m, A) < 0$ then $H_m(A) = \mathrm{rem}(m, A) + m$. H_m is a homomomorphism of Z onto Z_m. H_m is realized by the SACLIB program MDHOM for β-integers m and by MIHOM for arbitrary integers.