3 Congruences

Basic properties. Given three integers a, b and m, we say that "a is *congruent* to b *modulo* m" and write $a \equiv b \mod m$, if the difference $a - b$ is divisible by m. m is called the *modulus* of the congruence. The following properties are easily proved directly from the definition:

1. (i) $a \equiv a \mod m$; (ii) $a \equiv b \mod m$ if and only if $b \equiv a \mod m$; (iii) if $a \equiv b \mod m$ and $b \equiv c \mod m$, then $a \equiv c \mod m$. For fixed m, (i)–(iii) mean that congruence modulo m is an *equivalence relation.*
2. For fixed m, each *equivalence class* with respect to congruence modulo m has one and only one representative between 0 and $m - 1$. (This is just another way of saying that any integer is congruent modulo m to one and only one integer between 0 and $m - 1$.) The set of equivalence classes (called *residue classes*) will be denoted $\mathbf{Z}/m\mathbf{Z}$. Any set of representatives for the residue classes is called a *complete set of residues modulo m.*
3. If $a \equiv b \mod m$ and $c \equiv d \mod m$, then $a \pm c \equiv b \pm d \mod m$ and $ac \equiv bd \mod m$. In other words, congruences (with the same modulus) can be added, subtracted, or multiplied. One says that the set of equivalence classes $\mathbf{Z}/m\mathbf{Z}$ is a *commutative ring*, i.e., residue classes can be added, subtracted or multiplied (with the result not depending on which representatives of the equivalence classes were used), and these operations satisfy the familiar axioms (associativity, commutativity, additive inverse, etc.).
4. If $a \equiv b \mod m$, then $a \equiv b \mod d$ for any divisor $d|m$.
5. If $a \equiv b \mod m$, $a \equiv b \mod n$, and m and n are relatively prime, then $a \equiv b \mod mn$. (See Property 5 of divisibility in § I.2.)

Proposition I.3.1. *The elements of* $\mathbf{Z}/m\mathbf{Z}$ *which have multiplicative inverses are those which are relatively prime to* m*, i.e., the numbers* a *for which there exists* b *with* $ab \equiv 1 \mod m$ *are precisely those* a *for which* $g.c.d.(a, m) = 1$. *In addition, if* $g.c.d.(a, m) = 1$*, then such an inverse* b *can be found in* $O(log^3 m)$ *bit operations.*

Proof. First, if $d = g.c.d.(a, m)$ were greater than 1, we could not have $ab \equiv 1 \mod m$ for any b, because that would imply that d divides $ab - 1$ and hence divides 1. Conversely, if $g.c.d.(a, m) = 1$, then by Property 2 above we may suppose that $a < m$. Then, by Proposition I.2.2, there exist integers u and v that can be found in $O(log^3 m)$ bit operations for which $ua + vm = 1$. Choosing $b = u$, we see that $m|1 - ua = 1 - ab$, as desired.

Remark. If $g.c.d.(a, m) = 1$, then by negative powers $a^{-n} \mod m$ we mean the n-th power of the inverse residue class, i.e., it is represented by the n-th power of any integer b for which $ab \equiv 1 \mod m$.

Example 1. Find $160^{-1} \mod 841$, i.e., the inverse of 160 modulo 841.

Solution. By Exercise 6(c) of the last section, the answer is 205.

Corollary 1. *If* p *is a prime number, then every nonzero residue class has a multiplicative inverse which can be found in* $O(log^3 p)$ *bit operations.*