

We say that the ring $\mathbf{Z}/p\mathbf{Z}$ is a field. We often denote this field \mathbf{F}_p , the “field of p elements.”

Corollary 2. Suppose we want to solve a linear congruence $ax \equiv b \pmod{m}$, where without loss of generality we may assume that $0 \leq a, b < m$. First, if $\text{g.c.d.}(a, m) = 1$, then there is a solution x_0 which can be found in $O(\log^3 m)$ bit operations, and all solutions are of the form $x = x_0 + mn$ for n an integer. Next, suppose that $d = \text{g.c.d.}(a, m)$. There exists a solution if and only if $d|b$, and in that case our congruence is equivalent (in the sense of having the same solutions) to the congruence $a'x \equiv b' \pmod{m'}$, where $a' = a/d$, $b' = b/d$, $m' = m/d$.

The first corollary is just a special case of Proposition I.3.1. The second corollary is easy to prove from Proposition I.3.1 and the definitions. As in the case of the familiar linear equations with real numbers, to solve linear equations in $\mathbf{Z}/m\mathbf{Z}$ one multiplies both sides of the equation by the multiplicative inverse of the coefficient of the unknown.

In general, when working modulo m , the analogy of “nonzero” is often “prime to m .” We saw above that, like equations, congruences can be added, subtracted and multiplied (see Property 3 of congruences). They can also be divided, provided that the “denominator” is prime to m .

Corollary 3. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, and if $\text{g.c.d.}(c, m) = 1$ (in which case also $\text{g.c.d.}(d, m) = 1$), then $ac^{-1} \equiv bd^{-1} \pmod{m}$ (where c^{-1} and d^{-1} denote any integers which are inverse to c and d modulo m).

To prove Corollary 3, we have $c(ac^{-1} - bd^{-1}) \equiv (acc^{-1} - bdd^{-1}) \equiv a - b \equiv 0 \pmod{m}$, and since m has no common factor with c , it follows that m must divide $ac^{-1} - bd^{-1}$.

Proposition I.3.2 (Fermat’s Little Theorem). Let p be a prime. Any integer a satisfies $a^p \equiv a \pmod{p}$, and any integer a not divisible by p satisfies $a^{p-1} \equiv 1 \pmod{p}$.

Proof. First suppose that $p \nmid a$. We first claim that the integers $0a, 1a, 2a, 3a, \dots, (p-1)a$ are a complete set of residues modulo p . To see this, we observe that otherwise two of them, say ia and ja , would have to be in the same residue class, i.e., $ia \equiv ja \pmod{p}$. But this would mean that $p|(i-j)a$, and since a is not divisible by p , we would have $p|i-j$. Since i and j are both less than p , the only way this can happen is if $i=j$. We conclude that the integers $a, 2a, \dots, (p-1)a$ are simply a rearrangement of $1, 2, \dots, p-1$ when considered modulo p . Thus, it follows that the product of the numbers in the first sequence is congruent modulo p to the product of the numbers in the second sequence, i.e., $a^{p-1}(p-1)! \equiv (p-1)! \pmod{p}$. Thus, $p|((p-1)!(a^{p-1}-1))$. Since $(p-1)!$ is not divisible by p , we have $p|(a^{p-1}-1)$, as required. Finally, if we multiply both sides of the congruence $a^{p-1} \equiv 1 \pmod{p}$ by a , we get the first congruence in the statement of the proposition in the case when a is not divisible by p . But if a is divisible by p , then this congruence $a^p \equiv a \pmod{p}$ is trivial, since both sides are $\equiv 0 \pmod{p}$. This concludes the proof of the proposition.