congruence*

rspuzio†

2013-03-21 12:20:14

Let a, b be integers and m a non-zero integer. We say that a *is congruent to* b *modulo* m, if m divides $b - a$ (the word *modulo* is the dative case of the Latin noun *modulus* meaning the 'module'). We write this *number congruence* or shortly *congruence* as

$$a \equiv b \pmod{m}.$$

If a and b are congruent modulo m, it means that both numbers leave the same residue when divided by m.

Congruence with a fixed module is an equivalence relation on $\mathbb{Z}$. The set of equivalence classes, the so-called *residue classes*, is a cyclic group of order m (assuming it positive) with respect to addition and a ring if we consider also the multiplication modulo m. This ring is usually denoted as

$$\frac{\mathbb{Z}}{m\mathbb{Z}}$$

and called the *residue class ring* modulo m. This ring is also commonly denoted as $\mathbb{Z}_m$, $\mathbb{Z}/(m)$. However, when $m = p$ is a prime number, notation $\mathbb{Z}_p$ is also used to denote p-adic numbers.

Properties of congruences

1. If $a \equiv b \pmod{m}$, then $a+c \equiv b+c \pmod{m}$ and $ac \equiv bc \pmod{m}$.
2. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a \pm c \equiv b \pm d \pmod{m}$ and $ac \equiv bd \pmod{m}$.
3. If $a \equiv b \pmod{m}$ and f is a polynomial with integer coefficients, then $f(a) \equiv f(b) \pmod{m}$.
4. If $ac \equiv bc \pmod{m}$ and $\gcd(c, m) = 1$, then $a \equiv b \pmod{m}$.
5. If $ac \equiv bc \pmod{m}$, then $a \equiv b \pmod{\frac{m}{\gcd(c, m)}}$.

---

*⟨*Congruence*⟩* created: *⟨2013-03-21⟩* by: *⟨rspuzio⟩* version: *⟨30101⟩* Privacy setting: *⟨1⟩* *⟨Definition⟩* *⟨18C10⟩* *⟨11A07⟩* *⟨11A05⟩* *⟨92B20⟩* *⟨92B05⟩* *⟨55M05⟩* *⟨18E05⟩* *⟨18-00⟩*

Proof of 5. Let $\gcd(c,\, m) := d$, $c := c'd$, $m := m'd$, where $\gcd(c',\, m') = 1$. The given congruence means that $m \mid (a-b)c$, whence $m' \mid (a-b)c'$. Since c' and m' are coprime, we infer that $m' \mid a-b$, i.e. $a \equiv b \pmod{m'}$. Q.E.D.

Remark. For justifying the latter asserted congruence of 2, one forms the sum $(a-b)c + (c-d)b$ in which the both differences are supposed divisible by m. Since the sum is simply $ac - bd$ and divisible by m, one obtains the asserted congruence. By induction, it is generalised to the case with any number n of factors on both sides; hence one infers also the result $a^n \equiv b^n \pmod{m}$.