congruence of arbitrary degree*

pahio†

2013-03-22 2:44:49

Theorem. A congruence of nth degree and modulo a prime number has at most n incongruent roots.

Proof. In the case $n = 1$, the assertion turns out from the entry linear congruence. We make the induction hypothesis, that the assertion is true for congruences of degree less than n.

We suppose now that the congruence

$$f(x) \;:=\; a_n x^n + a_{n-1}x^{n-1} + \ldots + a_0 \;\equiv\; 0 \pmod{p}, \tag{1}$$

where $p \nmid a_n$, has at least n incongruent roots $x_1, x_2, \ldots, x_n$. Form the congruence

$$f(x) \;\equiv\; a_n(x - x_1)(x - x_2)\cdots(x - x_n) \pmod{p}. \tag{2}$$

Both sides have the same term $a_n x^n$ of the highest degree, whence they may be cancelled from the congruence and the degree of (2) has a lower degree than n. Because (2), however, clearly has n incongruent roots $x_1, x_2, \ldots, x_n$, it must by the induction hypothesis be simplifiable to the form $0 \equiv 0 \pmod{p}$ and thus be an identical congruence.

Now, if the congruence (1) had an additional incongruent root x_{n+1}, i.e. $P(x_{n+1}) \equiv 0 \pmod{p}$, then the identical congruence (2) would imply

$$a_n(x_{n+1} - x_1)(x_{n+1} - x_2)\cdots(x_{n+1} - x_n) \;\equiv\; 0 \pmod{p}.$$

Yet, this is impossible, since no one of the factors of the left hand side is divisible by p. This settles the induction proof.

Cf. SpringerLink.

Example. When $f(x) := x^5 + x + 1 \equiv 0 \pmod{7}$, we have $f(0) \equiv 1 \pmod{7}$,

---

*⟨*CongruenceOfArbitraryDegree*⟩ created: ⟨2013-03-2⟩ by: ⟨pahio⟩ version: ⟨41722⟩ Privacy setting: ⟨1⟩ ⟨Theorem⟩ ⟨11A05⟩ ⟨11A07⟩

$f(1) \equiv 3 \pmod 7$,
$f(2) \equiv 32 + 2 + 1 \equiv 0 \pmod 7$,
$f(3) \equiv 27 \cdot 9 + 3 + 1 \equiv -1 \cdot 2 + 4 \equiv 2 \pmod 7$,
$f(4) \equiv (-3)^5 + 4 + 1 \equiv +2 + 5 \equiv 0 \pmod 7$,
$f(5) \equiv (-2)^5 + 5 + 1 \equiv -32 + 6 \equiv -26 \equiv 2 \pmod 7$,
$f(6) \equiv (-1)^5 + 6 + 1 \equiv 6 \pmod 7$.
Thus only the representants 2 and 4 of a complete residue system modulo 7 (see conditional congruences) are roots of the given congruense. A congruence needs not have the maximal amount of incongruent roots mentionned in the theorem.

References

[1] K. Väisälä: *Lukuteorian ja korkeamman algebran alkeet.* Tiedekirjasto No. 17. Kustannusosakeyhtiö Otava, Helsinki (1950).