Congruences a.k.a. modular arithmetic

Def'n $a \equiv b \pmod{n}$ iff $n \mid a-b$, i.e., $a = b + kn$, some $k \in \mathbb{Z}$.

FACT: $a \equiv b \pmod{n}$ iff a, b have the same remainder upon division by n.

pf: First, $a \equiv b \pmod{n} \Rightarrow a = b + kn$, some $k \in \mathbb{Z}$.

Also, $b = qn + r$, $0 \le r < n$ (Division Lemma)

so $a = qn + r + kn \Rightarrow a = (q+k)n + r$, $0 \le r < n$.

remainder!

Other direction: $a = q_1 n + r$, $b = q_2 n + r$ with $0 \le r < n$

$\Rightarrow a - b = (q_1 - q_2)n \Rightarrow n \mid a-b \Rightarrow$

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

$n \in \mathbb{N}$ given

FACTS

$a \equiv a \pmod n$

$a \equiv b \pmod n \implies b \equiv a \pmod n$

$a \equiv b \pmod n,\ b \equiv c \pmod n \implies a \equiv c \pmod n$

} $\equiv$ is an equivalence relation

$a \equiv b \pmod n,\ c \equiv d \pmod n \implies a+c \equiv b+d \pmod n$

and $ac \equiv bd \pmod n$

pf: $a \equiv b,\ c \equiv d \implies a = b+kn,\ c = d+qn$

$\implies a+c = b+d+(k+q)n$

$\implies a+c \equiv b+d \pmod n.$

$ac = (b+kn)(d+qn) = bd + (kd + bq + kq)n$

$\implies ac \equiv bd \pmod n.$

$a \equiv b \pmod n \implies a^k \equiv b^k \pmod n,\ k \in \mathbb{N}.$

4(a) $2^{50} \equiv ? \pmod 7$ Note: $2^{50} \approx (2^{10})^5 \approx (1{,}000)^5$

$= 10^{15}$

Soln: $2^3 \equiv 1 \pmod 7 \Longrightarrow (2^3)^{16} \equiv 1 \pmod 7$

$2^2 \equiv 4 \pmod 7$ $\quad 2^{48} \equiv 1 \pmod 7$

$2^{50} \equiv 4 \pmod 7$ remainder = 4

---

(5) $111^{333} + 333^{111}$ is divisible by 7:

$111 \equiv 6 \pmod 7$ $\quad 333 \equiv -3 \pmod 7$

i.e. $111 \equiv -1 \pmod 7$ $\quad (333)^3 \equiv -27 \equiv 1 \pmod 7$

$\Rightarrow (111)^{333} \equiv -1 \pmod 7$ $\quad \Rightarrow (333)^{111} \equiv 1 \pmod 7$,

$7 \mid 111^{333} + 333^{111}$

16 $97 \mid 2^{48}-1$ • i.e., $2^{48} \equiv 1 \pmod{97}$

$2^k \equiv 2^k \pmod{97}$ for $k = 1, 2, 3, 4, 5, 6$

$2^7 \equiv 31 \pmod{97}$

$2^8 \equiv 62 \pmod{97}$

$2^9 \equiv 124 \equiv 27 \pmod{97}$

$2^{10} \equiv 54 \pmod{97}$

$2^{11} \equiv 11 \pmod{97}$

Then

$2^{19} \equiv 62 \cdot 11 \pmod{97}$

$\equiv 682 \pmod{97}$

$2^{19} \equiv 100 \pmod{97}$

$\Rightarrow 2^{24} \equiv 3200 \pmod{97}$

$2^{24} \equiv 96 \pmod{97}$,

i.e., $2^{24} \equiv -1 \pmod{97}$

$\Rightarrow 2^{48} \equiv 1 \pmod{97}$.

FACT: $ca \equiv cb \pmod{n} \Rightarrow a \equiv b \pmod{n/d}$

where $d = \gcd(c, n)$.

Pf.: $ca - cb = kn$; $d = \gcd(c,n) \Rightarrow c = dr,\ n = ds$,

$\gcd(r, s) = 1$

Thus, $dra - drb = kds$

$\Rightarrow r(a-b) = ks$

$\Rightarrow s \mid a-b,\ s = n/d$.

∎

Corollary: $ca \equiv cb \pmod{n}$ and $\gcd(c,n) = 1$,

then $a \equiv b \pmod{n}$.