computations mod m

Ex: what is the rem of

$a = (137)^3 + 230021 \cdot 1789$ when div. by 3 ?

(so a mod 3)

$137 \equiv 17 \equiv 2$ $\quad 1789 \equiv 1$

$230021 \equiv 2$

↓

Polynomial

So $a \equiv 2^3 + 2 \cdot 1 \equiv 10 \equiv 1 \in \{0,1,2\}$. $\boxed{1}$

Ex: $(20)^{2351} \bmod 7$

$6^{2351} = ?$ But $(20)^{2351} \equiv (-1)^{2351} = -1 \equiv \boxed{6} \pmod 7$

Ex: $3^{20} \pmod 6$

$(3^2)^{10} \equiv 9^{10} \equiv 3^{10} (3^2)^5 \equiv 3^5 = 3^2 \cdot 3^2 \cdot 3 = 3 \cdot 3 \cdot 3 \equiv 3$

In fact $3^m \equiv 3$ $\forall m$ Ind. on m ...

Some Easy Congs

(1) Cong. mod 2: 0 if even
1 if odd

note: $a = d_n d_{n-1} \cdots d_1 d_0$, d_i the digits (base 10)

$= d_0 + d_1 10 + \cdots + d_n b^n \equiv d_0 \pmod 2$

($10 \equiv 0$, $b \equiv 0$)

(2) Cong mod 10: last digit

similar to above $a \equiv d_0 \pmod{10}$

↳ rem of div. by 10

(3) Cong mod 5: reduce last digit

$a \equiv d_0 \pmod 5$

(4) Cong mod 4: reduce last 2 digits

$a = d_1 d_0 + 100 \cdot d_n \cdots d_2 \equiv d_1 d_0$ Ex: ....

last 2 dig

$100 = 4 \cdot 25 \equiv 0 \pmod 4$

(5) mod 3 & 9 : reduce sum of digits (can repeat)

$$a = a_0 + a_1 \cdot 10 + a_2 10^2 + \dots + a_n 10^n \equiv a_0 + a_1 + \dots + a_n$$

$10 \equiv 1$, $10^2 \equiv 1$, $10^n \equiv 1$

Ex: $75329 \equiv 7+5+3+2+9 \equiv 17 \equiv 8 \pmod 9$

$9 \equiv 0$

$\equiv 2 \pmod 3$

note: we get div criteria, as div by m iff $\equiv 0 \pmod m$