Applying the CRT to computing powers

benefits

- speed up computation of powers [if factorization of modulus is known]
- strengthen Euler's theorem

Eg $3^{29} \pmod{77}$ $\quad \phi(77) = \phi(7)\cdot\phi(11) = 60$

previously: $3^2, 3^4, 3^8, 3^{16} \pmod{77}$

$\rightsquigarrow 3^{29} = 3^{16}\cdot 3^8 \cdot 3^4 \cdot 3^1$ binary exponentiation

using CRT

$3^{29} \pmod 7$ $\quad \phi(7) = 6$

$\equiv 3^5$

$\equiv 3^4 \cdot 3^1 \equiv 4\cdot 3 \equiv -2$

$3^2 \equiv 2,\ 3^4 \equiv 2^2 \equiv 4$

$x \equiv -2 \pmod 7$

$3^{29} \pmod{11}$ $\quad \phi(11) = 10$

$\equiv 3^9$

$\equiv 3^{-1} \equiv 4$ ↑ unusual!

$x \equiv 4 \pmod{11}$

$\Rightarrow x \equiv -2\cdot 11 \cdot \underbrace{11^{-1}_{\bmod 7}}_{\equiv 4^{-1} \equiv 2} + 4\cdot 7 \cdot \underbrace{7^{-1}_{\bmod 11}}_{\equiv -3}$

$\equiv -44 - 84 \equiv \underline{\underline{26}} \pmod{77}$

Euler's thm mod 60 $\quad a^{16} \equiv 1 \pmod{60}$ for all a coprime to 60

$\phi(60) = \phi(4)\cdot\phi(3)\cdot\phi(5) = (2^2 - 2^1)\cdot 2 \cdot 4 = 16$

Eg Show that $a^4 \equiv 1 \pmod{60}$ for all a coprime to 60

$\Longleftrightarrow$ CRT

- $a^4 \equiv 1 \pmod 4$ follows from $a^2 \equiv 1 \pmod 4$ (Euler)
- $a^4 \equiv 1 \pmod 3$ follows from $a^2 \equiv 1 \pmod 3$ (Little Fermat)
- $a^4 \equiv 1 \pmod 5$ true because this is little Fermat

$\Longleftrightarrow$ a coprime to 4, 3, 5

Eg HW! $\quad a^6 \equiv 1 \pmod{42}$ for all a coprime to 42

[Euler: $a^{12} \equiv 1 \pmod{42}$]