Absolute pseudoprimes

review

x is a **Fermat witness** mod n if $x^{n-1} \not\equiv 1 \pmod{n}$

x is a **Fermat liar** mod n if $x^{n-1} \equiv 1 \pmod{n}$ and n is composite

n is an **absolute pseudoprime** if every $x \pmod{n}$ is either a Fermat liar or $\gcd(x,n) > 1$

1994: ∞ many
first few: 561, 1105, 1729, ...

EG 561 is an absolute pseudoprime.

needed: $x^{560} \equiv 1 \pmod{561}$ for all x with $\gcd(x, 561) = 1$

$561 = 3 \cdot 11 \cdot 17$

$\Longleftarrow$ CRT

$x^{560} \equiv 1 \pmod{3}$ follows from $x^2 \equiv 1 \pmod{3}$ (Little Fermat)

$x^{560} \equiv 1 \pmod{11}$ follows from $x^{10} \equiv 1 \pmod{11}$

$560 = 56 \cdot 10$

$x^{560} \equiv 1 \pmod{17}$ follows from $x^{16} \equiv 1 \pmod{17}$

$560 = 35 \cdot 16$

actually $x^{80} \equiv 1 \pmod{561}$ for all x with $\gcd(x, 561) = 1$

$80 = \operatorname{lcm}(2, 10, 16)$

THM Korselt's Criterion

A composite number n is an absolute pseudoprime

$\Longleftrightarrow$ n is squarefree (distinct prime factors) and $(p-1) \mid (n-1)$ for any prime divisor p of n