

Solution to problem 41: Let $d = \gcd(a, N) > 1$. Thus $a \equiv 0 \pmod{d}$ and therefore $a^{N-1} \equiv 0 \not\equiv 1 \pmod{d}$. Since d is a divisor of N , we have $a^{N-1} \not\equiv 1 \pmod{N}$.

Solution to problem 42: Let us compute $2^{898} \pmod{899}$. We use the method of repeating squaring. First note that $898 = 2^9 + 2^8 + 2^7 + 2$. Now

$$2^1 \equiv 2 \pmod{899}$$

$$2^2 \equiv 4 \pmod{899}$$

$$2^{2^2} \equiv 4^2 = 16 \pmod{899}$$

$$2^{2^3} \equiv 16^2 = 256 \pmod{899}$$

$$2^{2^4} \equiv 256^2 \equiv 808 \equiv -91 \pmod{899}$$

$$2^{2^5} \equiv (-91)^2 \equiv 190 \pmod{899}$$

$$2^{2^6} \equiv 190^2 \equiv 140 \pmod{899}$$

$$2^{2^7} \equiv 140^2 \equiv 721 \equiv -178 \pmod{899}$$

$$2^{2^8} \equiv (-178)^2 \equiv 219 \pmod{899}$$

$$2^{2^9} \equiv 219^2 \equiv 314 \pmod{899}$$

Thus

$$2^{898} = 2^{2^9} \cdot 2^{2^8} \cdot 2^{2^7} \cdot 2^2 \equiv 314 \cdot 219 \cdot (-178) \cdot 4 \equiv 442 \cdot (-178) \cdot 4 \equiv 436 \cdot 4 \equiv -54 \pmod{899}$$

By Fermat's Little Theorem, 899 can not be a prime.

It is quite easy to note that $899 = 900 - 1 = 30^2 - 1 = 29 \cdot 31$, so it is not a prime. The point though is that the above method is very efficient when you deal with large numbers (compared to other methods, like checking consecutive primes for divisors). It is not that evident here, since 899 is relatively small (it would be more evident for a 20 digit number).

Solution to problem 43: Note that $15 - 1 = 2 \cdot 7$. Thus 15 is a strong pseudoprime relative to 11 iff $11^7 \equiv 1 \pmod{15}$ or $11^7 \equiv -1 \pmod{15}$. But $11^7 \equiv (-4)^7 = 16^3 \cdot (-4) \equiv -4 \pmod{15}$, so 15 is not a strong pseudoprime relative to 11.

Solution to problem 44: Note that $25-1 = 2^3 \cdot 3$. Thus 25 is a strong pseudoprime relative to 7 iff $7^3 \equiv 1 \pmod{25}$, or $7^3 \equiv -1 \pmod{25}$, or $7^{2 \cdot 3} \equiv -1 \pmod{25}$, or $7^{2^2 \cdot 3} \equiv -1 \pmod{25}$. Since $7^2 \equiv -1 \pmod{25}$, we see that $7^{2 \cdot 3} \equiv (-1)^3 = -1 \pmod{25}$ so 25 is indeed a strong pseudoprime relative to base 7.