

Mersenne primes are primes of
the form $2^P - 1$, where P is
a prime.

Some good proof technique here.

Claim $2^n - 1$ prime $\Rightarrow n$ prime.
 $A \Rightarrow B$

Assume $2^n - 1$ is prime

The contrapositive $\neg A \Rightarrow \neg B$
 $\neg B \Rightarrow (\neg A)$

\therefore
 \therefore

$\Rightarrow n$ is prime.

Consider contrapositive.

If n is composite then $2^n - 1$ is
composite.

n is composite $\Rightarrow 2^n - 1$ is composite.

Q8

Using modular arithmetic.

Suppose p, q are primes $p, q \geq 5$

claim $p^2 - q^2$ is divisible by 24.

i.e. we will show $\textcircled{8} \mid p^2 - q^2$

and that $\textcircled{3} \mid p^2 - q^2$

$(\gcd(a, b) = 1 \text{ then } (a|c \& b|c) \Rightarrow ab|c)$

think modulo 3

$p \equiv 1, 2 \pmod{3}, q \equiv 1, 2 \pmod{3}$

$\Rightarrow p^2 \equiv 1 \pmod{3}, q^2 \equiv 1 \pmod{3}$

$\Rightarrow p^2 - q^2 \equiv 0 \pmod{3}$

$\Rightarrow 3 \mid p^2 - q^2 \checkmark$

Think mod 8.

$$P \equiv 1, 3, 5, 7 \pmod{8}$$

and $q \equiv 1, 3, 5, 7 \pmod{8}$

(as the other values are clearly even)

$$\Rightarrow P^2 \equiv 1, q^2 \equiv 1 \pmod{8}$$

$$\Rightarrow P^2 - q^2 = 1 - 1 \equiv 0 \pmod{8}$$

$$\Rightarrow 8 \mid P^2 - q^2$$

Therefore $24 \mid P^2 - q^2$, as

$$\gcd(3, 8) = 1$$

$$a \equiv a' \pmod{m}$$

Ex 4.2 then $a^k \equiv (a')^k \pmod{m}$

Q5 What remains after
dividing 2012^{2012} by 5 }

$$2012^{2012} \equiv (2012^2)^{1006} \pmod{5}.$$

$$\equiv 2^{2012} \pmod{5}$$

since $2012 \equiv 2 \pmod{5}$

$\boxed{\text{mod } 5}$

$$2^2 \equiv 4$$

$$2^3 \equiv 3$$

0

$$\begin{matrix} 2^4 \\ 11 \\ 2 \end{matrix} \quad \text{with } 0$$

$$2 \equiv 2'$$

and $2012 \equiv 0 \pmod{4}$

so $2^{2012} \equiv (2^4)^{503} \pmod{5}$

