11. A. Divisors of Mersenne numbers

The purpose of this document is to prove a result of Fermat that is stated in the main notes for the unit.

Theorem 1. *If* $\mathbf{p}$ *is an odd prime, then every divisor of* $2^{\mathbf{p}} - 1$ *has the form* $2\,\mathbf{p}\,\mathbf{k} + 1$.

One step in the proof is the following special case.

Theorem 2. *Let* $\mathbf{p}$ *and* $\mathbf{q}$ *be odd primes. If* $\mathbf{q}$ *divides* $2^{\mathbf{p}} - 1$*, then* $\mathbf{q} \;=\; 1 \pmod{2\mathbf{p}}$.

Important note. The proof of this result will use concepts that are not covered in this course or its prerequisites but are covered in many undergraduate algebra courses. The proof will not be used subsequently in this course.

Proof that the second result implies the first. Suppose that $\mathbf{d}$ divides $2^{\mathbf{p}} - 1$, and write $\mathbf{d}$ as a product of primes $\mathbf{q}_1 \ldots \mathbf{q}_m$; since $\mathbf{d}$ divides an odd number it follows that $\mathbf{d}$ and hence each $\mathbf{q}_j$ must also be odd. Therefore by Theorem 2 we have that $\mathbf{q}_j \;=\; 1 \pmod{2\mathbf{p}}$ for all $\mathbf{j}$. Therefore it follows that

$$\mathbf{d} \;=\; \mathbf{q}_1 \ldots \mathbf{q}_m \;=\; 1 \ldots 1 \pmod{2\mathbf{p}} \;=\; 1 \pmod{2\mathbf{p}}.$$

Proof of Theorem 2. If $\mathbf{p}$ divides $2^{\mathbf{p}} - 1$, then $2^{\mathbf{p}} \;=\; 1 \pmod{\mathbf{q}}$ and the multiplicative order of $2 \pmod{\mathbf{p}}$ divides the prime $\mathbf{q}$, sand hence it must be $\mathbf{q}$. By the Little Fermat Theorem the order of 2 also divides $\mathbf{p} - 1$, and since the latter is an even number we must have $\mathbf{p} - 1 \;=\; 2\mathbf{kq}$.

Additional fact. *We also have* $\mathbf{p} \;=\; \pm 1 \pmod 8$.

Proof. The preceding discussion yields the congruences $2^{(\mathbf{p}-1)/2} \;=\; 2^{\mathbf{qk}} \;=\; 1 \pmod{\mathbf{p}}$, so 2 is a quadratic residue mod $\mathbf{p}$, and therefore by Quadratic Reciprocity it follows that $\mathbf{p} \;=\; \pm 1 \pmod 8$.

Example. If a prime number $\mathbf{p}$ divides $2^{31} - 1$, then the preceding results combine to show $\mathbf{p} = 1$ or $63 \pmod{248}$. By 1772 Euler had used this to show that

$$2^{31} - 1 \;=\; 2{,}147{,}483{,}647$$

is a (Mersenne) prime number.

Source: Most of the material above was taken from the following site:

http://www.utm.edu/research/primes/notes/proofs/MerDiv.html