

## A MATHEMATICAL OFFERING, PROBLEM 6 SOLUTION

TIM MCLARNAN

The final question for last semester asked,

- (a) If  $2^n - 1$  is a prime, what can you say about  $n$ ?
- (b) If  $2^n + 1$  is a prime, what can you say about  $n$ ?
- (c) What if both  $2^n - 1$  and  $2^n + 1$  are primes?

The cool prize for the best solution to this problem went to Curtis Walton, whose solution is posted beside this one. Here's my own effort, which broadly speaking resembles Curtis's.

The critical fact to remember in part (a) is that

$$x^k - y^k = (x - y)(x^{k-1} + x^{k-2}y + x^{k-3}y^2 + \cdots + y^{k-1}). \quad (1)$$

This means that if  $n = ab$  is composite (so  $1 < a, b < n$ ), then

$$2^n - 1 = 2^{ab} - 1 = (2^a - 1)(2^{a(b-1)} + 2^{a(b-2)} + 2^{a(b-3)} + \cdots + 2^a + 1)$$

is also composite. A quick answer to part (a) is therefore that if  $2^n - 1$  is prime, then  $n$  must also be prime. The converse of this claim is not true. The smallest counterexample is  $2^{11} - 1 = 23 \cdot 89$ .

Primes of the form  $2^p - 1$  are called *Mersenne primes*, after a French mathematician, Marin Mersenne, who published a somewhat flawed list of the small Mersenne primes in 1644. So far, at any given point in time, the largest known prime is always a Mersenne prime. There seems every reason to believe that there is an infinite number of these primes, but this is unproven.

Part (b) can be done in almost the same way. This time, the crucial fact is that if  $k$  is odd, then

$$x^k + y^k = (x + y)(x^{k-1} - x^{k-2}y + x^{k-3}y^2 - \cdots - xy^{k-2} + y^{k-1}). \quad (2)$$

This means that if  $n = ab$  and  $b > 1$  is odd, then

$$2^n + 1 = 2^{ab} + 1 = (2^a + 1)(2^{a(b-1)} - 2^{a(b-2)} + 2^{a(b-3)} - \cdots - 2^a + 1)$$

Typeset by  $\mathcal{A}\mathcal{M}\mathcal{S}$ -TEX

is also composite. A quick answer to part (b) is therefore that if  $2^n + 1$  is prime, then  $n$  must also be a power of 2. (Only the powers of 2 have no odd factors.) The converse of this claim is not true. The smallest counterexample is  $2^{2^5} + 1 = 642 \cdot 6700417$ .

Primes of the form  $2^{(2^n)} + 1$  are called *Fermat primes*, after a French mathematician, Pierre de Fermat, who conjectured in 1640 that  $2^{(2^n)} + 1$  was prime for every non-negative integer  $n$ . So far, at any given point in time the largest known Fermat prime is  $2^{(2^4)} + 1 = 65537$ . That is, no Fermat prime has been found for  $n > 4$ ., and there seems no compelling reason to suspect that there are any others. Again, however, this is unproven.

We can now make short work of part (c). Both  $2^n - 1$  and  $2^n + 1$  can be prime only if  $n$  is both a prime and a power of 2. This happens exactly once: when  $n = 2$ , both  $2^2 - 1 = 3$  and  $2^2 + 1 = 5$  are prime.

Pairs of primes that differ by 2, like (3 and 5) or (17 and 19) or (24107 and 24109) are called *twin primes*. It is unknown whether the number of twin primes is finite or infinite, and the question seems to be extremely difficult.

Good sources for more info on primes are Paulo Ribenboim's *The Book of Prime Number Records* and <http://www.astro.virginia.edu/~eww6n/math/PrimeNumber.html>.