

## CHALLENGE PROBLEM II SOLUTION

TIM McLARNAN

Challenge Problem II was to understand the function

$$Q(n) = 1 + \sum_{m=1}^{2^n} \left[ \left( \frac{n}{\sum_{j=1}^m \left\lfloor \cos^2 \left( \pi \frac{(j-1)!+1}{j} \right) \right\rfloor} \right)^{1/n} \right].$$

It turns out that  $Q(n)$  computes the  $n^{\text{th}}$  prime! This may seem surprising, since there is abroad a common belief that “There is no formula for primes.” The formula above is a constructive proof that there is indeed a formula for primes, but it also shows the weakness of such formulas. The formula is probably too complicated ever to be useful in a proof, and computing primes using  $Q$  is much slower than using the sieve of Eratosthenes.

I’m posting here both my solution and that of the winner of the cool prize, Peter McLarnan. Next week, can we try to get someone not in my family involved here?

The hints to the problem suggested that one begin by trying to understand the function

$$\chi(j) = \left\lfloor \cos^2 \left( \pi \frac{(j-1)!+1}{j} \right) \right\rfloor.$$

Experimentation should show quickly that

$$\chi(j) = \begin{cases} 1, & \text{if } j \text{ is a prime} \\ 1, & \text{if } j = 1 \\ 0, & \text{if } j \text{ is composite.} \end{cases}$$

To see that this is true, we need to remember or discover *Wilson’s Theorem*, which says that

$$(j-1)! \equiv -1 \pmod{j} \iff j \text{ is a prime or } j = 1,$$

i.e., that

$$\frac{(j-1)!+1}{j} \text{ is an integer} \iff j \text{ is a prime or } j = 1.$$

(The proof of this theorem is interesting and not hard if you approach it with the right concepts in hand; I’ll let you read about it in your favorite book on number theory.)

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

Wilson's theorem has direct bearing on the behaviour of  $\chi(x)$ . For any  $z$ ,  $0 \leq \cos^2 z \leq 1$ ; so for any  $j$ ,  $\chi(j)$  is either 0 or 1. Further,

$$\begin{aligned} \chi(j) = 1 &\iff \cos\left(\pi \frac{(j-1)! + 1}{j}\right) = \pm 1 \\ &\iff \pi \frac{(j-1)! + 1}{j} \text{ is a multiple of } \pi \\ &\iff \frac{(j-1)! + 1}{j} \text{ is an integer} \\ &\iff j \text{ is a prime or } j = 1, \end{aligned}$$

proving our claim about the nature of  $\chi(j)$ .

Once we understand  $\chi(j)$ , it is easy to see what the function

$$P(m) = \sum_{j=1}^m \left[ \cos^2\left(\pi \frac{(j-1)! + 1}{j}\right) \right]$$

does: its value is one more than the number of primes less than or equal to  $m$ . In the usual notation of number theorists,  $P(m) = 1 + \pi(m)$ .

Now we're ready to go all the way and look at what  $Q(n)$  does. The simplest way to gain insight is just to do some computations and look at what happens. For instance, to compute  $Q(3)$ , we would do this:

$$\begin{aligned} Q(3) &= 1 + \sum_{m=1}^8 \left[ \left( \frac{3}{1 + \pi(m)} \right)^{1/3} \right] \\ &= 1 + \left[ \left( \frac{3}{1} \right)^{1/3} \right] + \left[ \left( \frac{3}{2} \right)^{1/3} \right] + \left[ \left( \frac{3}{3} \right)^{1/3} \right] + \left[ \left( \frac{3}{3} \right)^{1/3} \right] \\ &\quad + \left[ \left( \frac{3}{4} \right)^{1/3} \right] + \left[ \left( \frac{3}{4} \right)^{1/3} \right] + \left[ \left( \frac{3}{5} \right)^{1/3} \right] + \left[ \left( \frac{3}{5} \right)^{1/3} \right] \\ &= 1 + 1 + 1 + 1 + 1 + 0 + 0 + 0 + 0 + 0 = 5. \end{aligned}$$

Do you see what happened here? We got a bunch of ones followed by a bunch of zeros. It's easy to see when the zeros start: they begin as soon as  $1 + \pi(m) > n$ , i.e., as soon as  $\pi(m) \geq n$ , i.e., when  $m = p_n$  is the  $n^{\text{th}}$  prime. This means that  $Q(n) = p_n$  is the  $n^{\text{th}}$  prime as long as two things happen. First, we need

$$\left[ \left( \frac{n}{1 + \pi(m)} \right)^{1/n} \right] = 1$$

whenever  $\pi(m) < n$ , and second, we need the  $n^{\text{th}}$  prime to be at most  $2^n$ .

The first of these claims is pretty easy. It's enough to show that

$$\lfloor n^{1/n} \rfloor = 1,$$

i.e., that  $n^{1/n} < 2$ , i.e., that  $n < 2^n$ , which is true for all positive integers  $n$  by any number of easy arguments.

The second claim is strongly believable, but is actually rather hard to prove. (For this reason, I nearly just set the upper limit of the sum to be  $+\infty$ . I decided not to do this in order to make clear that the sum could be evaluated in a finite computation.) It's a consequence of the following theorem from Hardy and Wright's *An Introduction to the Theory of Numbers*:

**Theorem.** (*Bertrand's Postulate*). *If  $n \geq 1$ , then there is at least one prime  $p$  such that  $n < p \leq 2n$ .*

I'll let you find and read the proof of Bertrand's Postulate yourself, or modify my formula to contain a formally infinite sum.

I had not seen this before talking to Peter, but it turns out the worst of the computational inefficiency in the formula here comes from having to run the sum up to  $2^n$ , which is normally *much* larger than  $p_n$ . By only computing terms in the sum until they became 0, Peter and I were able to reduce the time to compute  $Q(100) = 541$  from at least  $10^{40}$  times the age of the universe (estimated) to under 1 hour, which is a speed-up worth implementing. Of course, one could compute primes up this far in a fraction of a second using a sieve; so even with the improvements, our formula is not competitive

Incidentally, there are some other exotic methods available for producing primes. One based on John Conway's *Fractran*, a system for converting any algorithm into a set of calculations with rational numbers, is as follows:

Start with the following list of 14 fractions:

$$\frac{17}{91} \quad \frac{78}{85} \quad \frac{19}{51} \quad \frac{23}{38} \quad \frac{29}{33} \quad \frac{77}{29} \quad \frac{95}{23} \quad \frac{77}{19} \quad \frac{1}{17} \quad \frac{11}{13} \quad \frac{13}{11} \quad \frac{15}{14} \quad \frac{15}{2} \quad \frac{55}{1}.$$

Now begin with the number  $a = 2$ , and repeat over and over the process of replacing  $a$  by  $a$  times the first fraction in this list whose product with  $a$  is a whole number. You'll get a sequence of numbers that begins 2, 15, 825, 725, 1925, 2275, 425, 390, 330, 290, 770, 910, 170, 156, 132, 116, 308, 364, 68, 4, ... Every so often, you encounter a power of 2 on this list. The exponents of 2 will turn out to be exactly the primes in increasing order. (This process comes from John H. Conway and Richard K. Guy's *The Book of Numbers*. A proof of its validity is in Richard K. Guy, *Conway's Prime Producing Machine*, *Math. Mag.* **56**(1983) 26–33.

Another formula you might like is the simple polynomial  $x^2 - x + 41$ , whose value is prime for every  $x \in \mathbb{Z}$  with  $-40 < x < 41$ .

A fascinating collection of prime facts is also available at

<http://www.astro.virginia.edu/~eww6n/math/PrimeNumber.html>,

part of a very useful on-line mathematical encyclopedia.