Primes!

David Patrick
patrick@artofproblemsolving.com

October 4, 2014

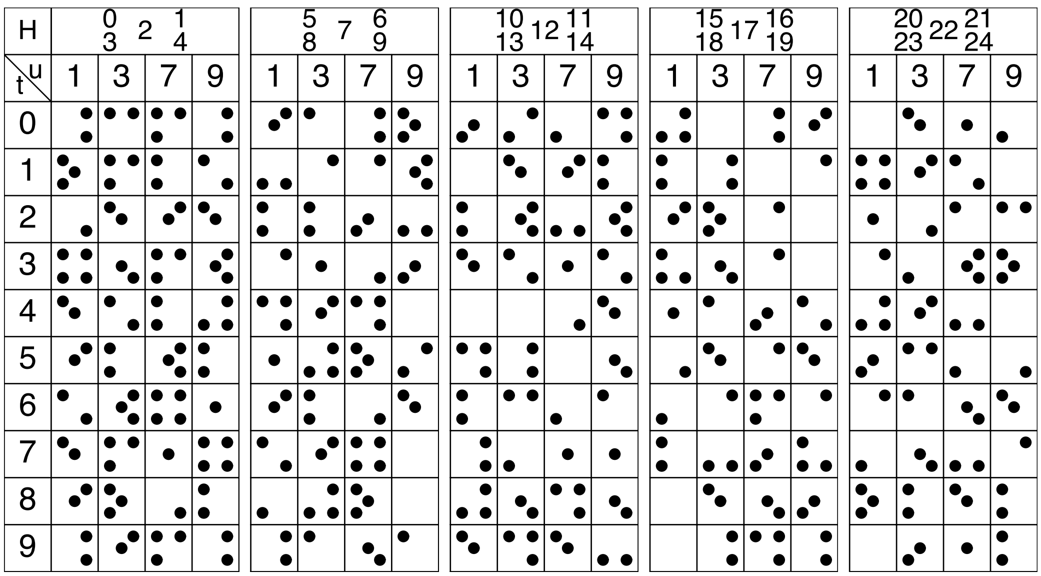
Sponsored by:

MSRI Mathematical Sciences Research Institute

A *prime number* is a positive integer with exactly two positive divisors: 1 and the number itself.

1. Here is a chart of all the prime numbers less than 2500, courtesy of Paul Zeitz:

Prime Numbers to 2500 (+2,5)



http://www.mathteacherscircle.org/assets/session-materials/primecard.pdf

   How do we read this chart? For example, can you use the chart to tell if 1651 is prime or composite? Why does it say "(+2, 5)" at the top? What patterns do you notice? Can you prove them?

2. (a) How many primes are there? Can you prove your answer?

   (b) Is there a better way to ask the question in part (a)? How "dense" are the primes?

3. Why is 1 not a prime? After all, its only positive divisors are 1 and itself: shouldn't that make it prime? What "goes wrong" if we say that 1 is a prime?

4. What's the longest group of consecutive composite numbers? To ask this another way: do the sizes of the gaps between primes have an upper bound, or do these gaps grow without bound?

5. Are there three consecutive odd numbers that are prime? How often does this occur?
   Are there two consecutive odd numbers that are prime? How often does this occur?

6. Some prime number oddities:
   (a) Examine $2^p - 1$ when p is prime.
   (b) Examine $n^2 - n + 41$ when n is a positive integer.

7. Here's a riddle that I got from Josh Zucker (who I'm sure got it from someone else):

   > A miserly old man in the desert is considering giving away all his camels. "I could divide them among my two sons, but there would be one left over. If I divided them among all my five children, but there would be two left over. Maybe I should divide them among all my seventeen children and grandchildren... but no, then there would be three left over. I suppose I might as well keep them all."

   How many camels did the old man have? Is your answer unique? If you changed the numbers of "left over" camels in the riddle, would there still be a solution?

8. If we pick two positive integers at random (what does that even mean?), what's the probability that they're relatively prime?

Primes!

David Patrick
patrick@artofproblemsolving.com

October 4, 2014

Sponsored by:

MSRI
Mathematical Sciences Research Institute

Notes

1. H stands for hundreds, t for tens, and u for units. The H boxes are the "map" for each square. A black dot indicates a prime number. For example, to locate 1651, we look for a black dot in the upper-right corner of the box in the 15–19 group of H's, in row t=5 and column u=1. Since there is no black dot, 1651 must be composite. (Indeed, $1651 = 13 \cdot 127$.)

   Note that all primes except for 2 and 5 must have units digit 1, 3, 7, or 9. (That's the reason for the "+2,5" in the title—those are the two exceptions.) There are other patterns too: for example, no box has 5 black dots, because for any n at least one of n, $n+100$, $n+200$, $n+300$, $n+400$ must be a multiple of 3. This also shows that there's only one way to have 4 black dots in a box.

2. (a) There are infinitely many primes. Here's a proof by contradiction: suppose there were finitely many, and call them $p_1, p_2, \ldots p_N$ for some N. Let $x = p_1 p_2 \cdots p_N + 1$ be the product of all the primes, plus one. But then x is not divisible by any p_i (it always leaves remainder 1), so either x is prime or all its prime factors are primes other that the p_i's, which contracts the assumption that the p_i's were all the primes. Hence, there must be infinitely many primes.

   (b) Primes get rarer as our numbers get bigger. For example, 25 out of the first 100 positive integers are prime (25%), but only 1,229 of the first 10,000 positive integers are prime (about 12%), and only 78,498 of the first 1,000,000 positive integers are prime (about 8%). The **Prime Number Theorem** states that about $N/(\ln N)$ of the first N positive integers are prime, where $\ln N$ is the natural logarithm of N. (For example, the Prime Number Theorem predicts about 72,382 primes below 1 million, which is pretty close. The estimate gets more and more accurate as N gets large.)

3. If 1 were prime, then numbers would not have unique prime factorizations. For example, $6 = 2 \cdot 3 = 1 \cdot 2 \cdot 3 = 1^{17} \cdot 2 \cdot 3 = \cdots$. So it's better to say that 1 isn't prime. 1's "prime factorization" is the empty set of primes.

4. We can have as large a gap between primes as we like. For example, if we want n consecutive composite integers, consider

   $$(n+1)!+2,\ (n+1)!+3,\ (n+1)!+4,\ \ldots,\ (n+1)!+(n+1).$$

   The first is a multiple of 2, the second is a multiple of 3, etc., and the last is a multiple of $n+1$. So all n consecutive integers in the list are composite.

5. The only three consecutive odd primes are 3, 5, and 7. To see why there aren't any others, notice that for any n, one of n, $n+2$, or $n+4$ must be a multiple of 3.

   Whether there are infinitely many pairs of consecutive odd primes is still an unsolved problem in mathematics: it is the famous **Twin Primes Conjecture**. Most mathematicians probably believe that there *are* infinitely many such pairs. The largest known pair is $3756801695685 \cdot 2^{666669} \pm 1$, discovered in 2011. In 2013, Yitang Zhang showed that there are infinitely many pairs of primes that differ by at most 70 million.

6. (a) $2^2 - 1 = 3$ is prime. $2^3 - 1 = 7$ is prime. $2^5 - 1 = 31$ is prime. $2^7 - 1 = 127$ is prime. $2^{11} - 1 = 2047$ is ... composite: $2047 = 23 \cdot 89$. A prime of the form $2^p - 1$ where p is prime is called a *Mersenne prime*.

10 of the values of p less than 100 give Mersenne primes, but then only 4 more primes less than 1000 give Mersenne primes. The largest known primes are all Mersenne primes. Also note that $2^n - 1$ is not prime if n is composite: see if you can prove this.

(b) This quadratic has the curious property that plugging in any positive integer n from 0 to 40 will give a prime number. But it doesn't work for all positive integers: for example, plugging in $n = 41$ gives $41^2 - 41 + 41 = 41^2$ which is certainly not prime. In fact there is no polynomial with integer coefficients that gives exclusively prime number outputs for all integer inputs.

7. We're looking for an integer n such that, for some integers a, b, c,

$$\begin{aligned} n &= 2a + 1, \\ n &= 5b + 2, \\ n &= 17c + 3. \end{aligned}$$

Since 2,5,17 are prime, their least common multiple is just their product, 170. We can just look at the odd numbers less than 170 that are 3 more than a multiple of 17: 3, 37, 71, 105, 139. We see that only 37 works with the middle equation, so 37 is the answer.

The **Chinese Remainder Theorem** says that if $d_1, d_2, \ldots, d_k$ are all relatively prime, and m, n are two different integers with $0 \le m, n < d_1 d_2 \cdots d_k$, then the remainders when dividing m and n by $d_1, d_2, \ldots, d_k$ must differ for at least one of the divisors. The CRT thus tells us that the solution to the camel problem is unique if we assume the man has fewer than 170 camels, and that if we changed the remainders, there would still be a unique solution. But we can add any multiple of 170 to the solution and have it still be valid, so the man might have $37, 207, 377, 547, \ldots$ camels.

8. Picking two positive integers "at random" really means specifying an upper bound N and then picking two integers from 1 to N. We can then analyze what happens when N gets really large. Running the experiment with $N = 100$ gives a proability of 60.87%.

The key fact is that two integers are relatively prime if and only if they are not the multiple of a common prime. So we look at all the primes separately.

Two integers are not both a multiple of 2 with probability $1 - \frac{1}{2} \cdot \frac{1}{2} = \frac{3}{4}$.

Two integers are not both a multiple of 3 with probaiblity $1 - \frac{1}{3} \cdot \frac{1}{3} = \frac{8}{9}$.

More generally, two integers are not both a multiple of p with probability $1 - \frac{1}{p} \cdot \frac{1}{p} = \frac{p^2-1}{p^2}$.

So the probability of two integers being relatively prime is the product of all these probabilities, or

$$\prod_{p \text{ prime}} \frac{p^2 - 1}{p^2}.$$

That is, it's the infinite product $\dfrac{3}{4} \cdot \dfrac{8}{9} \cdot \dfrac{24}{25} \cdot \dfrac{48}{49} \cdots\cdots$.

The remarkable fact is that using calculus, one can show that this is exactly equal to $\dfrac{6}{\pi^2}$, or about 61%.

This is an application of the Riemann zeta function, which is the principal object of one of the most fundamental unsolved problems in all of mathematics, the Riemann Hypothesis. But that's a story for another day.