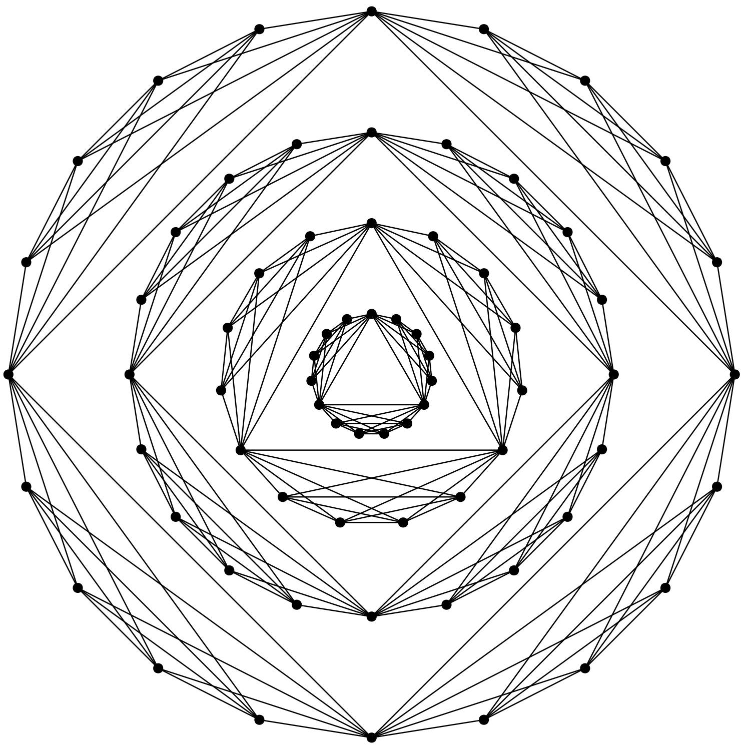
*

ISSN 1350-8539

M500 302



Trapping the primes

Martin Hansen

1. A simple beginning

An infinite arithmetic progression may be prime free,

$$\text{AP}\{4,10\}\colon 4,\ 14,\ 24,\ 34,\ 44,\ 54,\ 64,\ 74,\ 84,\ 94,\ldots,$$

or have a single prime as initial term,

$$\text{AP}\{5,10\} : \mathbf{5},\ 15,\ 25,\ 35,\ 45,\ 55,\ 65,\ 75,\ 85,\ 95,\ldots,$$

or contain many primes,

$$\text{AP}\{9,10\}\colon 9,\ \mathbf{19},\ \mathbf{29},\ 39,\ 49,\ \mathbf{59},\ 69,\ \mathbf{79},\ \mathbf{89},\ 99,\ldots.$$

These examples are amongst those depicted in the ten-wide number grid below in which only the primes within the respective sequences are shown, composite terms being indicated with a dash.

AP{1, 10}	$y = 1 + 10n$	-	11	-	31	41	-	61	71	-	-	101	...
AP{2, 10}	$y = 2 + 10n$	2	-	-	-	-	-	-	-	-	-	-	...
AP{3, 10}	$y = 3 + 10n$	3	13	23	-	43	53	-	73	83	-	103	...
AP{4, 10}	$y = 4 + 10n$	-	-	-	-	-	-	-	-	-	-	-	...
AP{5, 10}	$y = 5 + 10n$	5	-	-	-	-	-	-	-	-	-	-	...
AP{6, 10}	$y = 6 + 10n$	-	-	-	-	-	-	-	-	-	-	-	...
AP{7, 10}	$y = 7 + 10n$	7	17	-	37	47	-	67	-	-	97	107	...
AP{8, 10}	$y = 8 + 10n$	-	-	-	-	-	-	-	-	-	-	-	...
AP{9, 10}	$y = 9 + 10n$	-	19	29	-	-	59	-	79	89	-	109	...

2. No primes at all

The observation that a particular infinite arithmetic progression contains no primes at all is easily proven. For example, to prove that no number in the infinite arithmetic progression AP$\{4,10\}$ is prime I could observe that all terms in AP$\{4,10\}$ are of the form,

$$y \ = \ 4 + 10n, \qquad \text{for } n = 0,\ 1,\ 2,\ 3,\ \ldots,$$

and factorise to get

$$y \ = \ 2(2 + 5n),$$

which shows that these numbers are always divisible by 2. As the first term, 4, is also not prime, no term in AP$\{4,10\}$ is prime.

3. Where lie the primes?

The ten-wide number grid shows that, with the exception of 2 and 5, all primes must be in one of AP$\{1, 10\}$, AP$\{3, 10\}$, AP$\{7, 10\}$ or AP$\{9, 10\}$. Thus when a prime greater than 5 is divided by 10 the remainder must be one of 1, 3, 7 or 9. Furthermore, when a positive integer other than 2 and 5 is divided by 10, if the remainder is 0, 2, 4, 5, 6 or 8, then that number cannot be prime, a fact known to every school pupil in the land.

Interestingly, other than 2 and 5, of the ten available rows the primes are trapped in 4 of them. Although the rows are of infinite extent, in terms of knowing where the primes lie, there is a sense in which they are trapped in 40% of the available space as those rows head off to infinity. This argument can be made more rigorous by taking a limit as columns are added. A natural development is to wonder if we can do better than the 40% of the ten-wide number grid. We can. First, however, a small digression.

4. Can an all prime arithmetic progression exist?

At this point it's worth noticing that none of the sequences above were composed entirely of primes. It's tempting to jump to the conclusion that no sequence of the form $y = a + 10n$ can be composed entirely of primes. The conclusion would be correct, but pinning it down needs care. By way of highlighting the need for caution, consider AP$\{13, 10\}$,

$$\begin{aligned} y &= 13 + 10n \\ &= 3 + 10 + 10n \\ &= 3 + 10(n + 1) \qquad \text{for} \quad n = 0,\, 1,\, 2,\, 3,\, \ldots . \end{aligned}$$

Thus AP$\{13, 10\}$ is the sequence AP$\{3, 10\}$ with the first term removed. So, the possibility exists that by throwing away sufficient initial terms a sequence remains composed entirely of primes. The search for an all prime arithmetic progression is degenerating into a chase after the infinite; in any given infinite arithmetic progression that contains primes, every time we encounter a composite number we can throw away the sequence up to that term, and hope that what comes next is an all prime arithmetic progression.

A strategy to kill the idea of the all prime infinite arithmetic progression is to show that all infinite arithmetic progressions contain an infinite sequence of composite numbers.

Consider the generalised infinite arithmetic progression

$$y = a + dn.$$

As n increments through all non-negative integers it will take on the values given by the infinite 'kill' sequence

$$k(m) \;=\; a + m + md$$

where m is a positive integer.

The corresponding terms in the arithmetic progression are of the form

$$\begin{aligned} y &= a + d(a + m + md) \\ &= a + ad + md + md^2 \\ &= (a + md)(1 + d), \end{aligned}$$

which is composite.

5. An improved prime trap

Returning to the main thrust of the article, having dealt exhaustively with the ten-wide prime trap, now consider one that is six-wide. Shown below, it's clear that, with the exception of 2 and 3, all primes lie in AP$\{1, 6\}$ or AP$\{5, 6\}$. Two out of the six rows gives this prime trap a rating $33^1/_3\,\%$.

AP$\{1,6\}$	$y = 1 + 6n$	-	7	13	19	-	31	37	43	-	-	61	...
AP$\{2,6\}$	$y = 2 + 6n$	2	-	-	-	-	-	-	-	-	-	-	...
AP$\{3,6\}$	$y = 3 + 6n$	3	-	-	-	-	-	-	-	-	-	-	...
AP$\{4,6\}$	$y = 4 + 6n$	-	-	-	-	-	-	-	-	-	-	-	...
AP$\{5,6\}$	$y = 5 + 6n$	5	11	17	23	29	-	41	47	53	59	-	...

6. A trap of prime-width

Constructing a trap that has a width which is a prime number is a disappointing endeavour. By way of illustration, in the seven-wide trap shown, once past the number 7, only the row that contained the 7 is prime free. In general, a p-wide trap will have primes in all rows except AP$\{0, p\}$, once past p.

AP$\{1,7\}$	$y = 1 + 7n$	-	-	-	-	29	-	43	-	-	-	71	...
AP$\{2,7\}$	$y = 2 + 7n$	2	-	-	23	-	37	-	-	-	-	-	...
AP$\{3,7\}$	$y = 3 + 7n$	3	-	17	-	31	-	-	-	59	-	73	...
AP$\{4,7\}$	$y = 4 + 7n$	-	11	-	-	-	-	-	53	-	67	-	...
AP$\{5,7\}$	$y = 5 + 7n$	5	-	19	-	-	-	47	-	61	-	-	...
AP$\{6,7\}$	$y = 6 + 7n$	-	13	-	-	-	41	-	-	-	-	-	...

7. Coprime is the key

In 1837 Peter Dirichlet [1805–1859] proved that for any two positive coprime integers, a and d, there are infinitely many primes of the form $y = a + dn$. An analysis of Dirichlet's intricate proof is one of the highlights of Tom Apostol's classic book *Introduction to Analytic Number Theory* [1]. The result confirms what the ten-, six- and seven-wide traps are suggesting: the rows were the primes are trapped are those coprime to the width of the trap. To be clear, the numbers coprime to ten are 1, 3, 7 and 9 corresponding to the observation that the ten-wide trap placed the primes in AP$\{1, 10\}$, AP$\{3, 10\}$, AP$\{7, 10\}$ and AP$\{9, 10\}$.

Dirichlet's result also explains why a p-wide number grid was such a poor trap of primes. For any given prime p, all positive integers less than p are coprime to p. So the primes can and do appear in all rows except that described by AP$\{0, p\}$, which is equivalent to AP$\{p, p\}$. As no prime is coprime with itself, this is the only prime free row, once past p.

8. Euler's totient function

In the developing quest to find which width of trap is most effective in relatively restricting the primes, it is the number of coprime integers to a given width that is of interest. This is given by Euler's totient function, $\phi(n)$, also often called Euler's phi function. There is a delightfully simple formula for $\phi(n)$, when n is a prime power, p^m,

$$\phi\left(p^m\right) \;=\; p^{m-1}(p-1).$$

(For a proof see, for example, [2].)

So, when $n = 7$,

$$\phi\left(7^1\right) \;=\; 7^{1-1} \times (7-1) \;=\; 6,$$

which matches the observation that in the seven-wide number grid, the primes are to be found in six of the seven rows, bar the exception of the prime 7.

For two coprime integers, p and q, Euler's totient function is multiplicative.

$$\phi(pq) \;=\; \phi(p) \times \phi(q) \qquad \text{for coprime } p \text{ and } q.$$

(For a proof, again see, for example, [2].)

So, when $n = 10$,

$$\phi(10) \;=\; \phi(2)\phi(5) \;=\; 4,$$

which matches the observation that in the ten-wide trap, the primes are to be found in four of the ten rows.

Here is a table of values of $\phi(n)$ for $1 \le n \le 39$.

+	0	1	2	3	4	5	6	7	8	9
0	-	1	1	2	2	4	2	6	4	6
10	4	10	4	12	6	8	8	16	6	18
20	8	12	10	22	8	20	12	18	12	28
30	8	30	16	20	16	24	12	36	18	24

A much bigger table for $0 < n < 2460$ is available at [3]. A good trap will have a value of $\phi(n)$ in the table that's low in relation to those around it. The entry $\phi(6) = 2$ was good because it seems to be the last occurrence of a value of 2 in the table; a comment based on the observation that the values in the table, on average, seem to be increasing. Assuming no more occurrences of 4 or 6 are to be found in an extended table, we have the following 'best so far' results;

$$\frac{\phi(6)}{6} = \frac{\phi(12)}{12} = \frac{\phi(18)}{18} = \frac{1}{3} \qquad \left(33^1\!/_3\,\%\right).$$

Motivation to keep going is provided by the entry for $\phi(30)$,

$$\frac{\phi(30)}{30} = \frac{4}{15} \qquad \left(26^2\!/_3\,\%\right).$$

In a thirty-wide table all the primes greater than 7 will be trapped into eight of the thirty available rows. It's the best result yet but comes with a caveat; how can we be sure that there's not another n for which $\phi(n)$ takes the value of 8 further on, beyond where our table (however big) stopped?

9. Establishing boundaries

Reassurance is sought that the equation

$$n = \phi^{-1}(s) \qquad \text{when } s = 8$$

has the finite set of solutions that are visible in our table of values of $\phi(n)$. That is, n is precisely the set of solutions

$$n = \{15, 16, 20, 24, 30\}.$$

A lovely result, originally due to Gupta [4], more accessible in Coleman [5], places bounds on the value of n for a given s that's known to be in the table of values for $\phi(n)$.

Theorem 1: Given that s is an even number, and p is prime, define $A(s)$ to be

$$A(s) \;=\; s \prod_{p-1|s} \frac{p}{p-1}.$$

If $n \in \phi^{-1}(s)$, then $s < n \leq A(s)$.

Proof: If $\phi(n) = s$ then, from the definition of $\phi(n)$ being the number of positive integers less than n that are coprime to n, it's clear that $s < n$. On the other hand, if n is decomposed into its product of primes,

$$n \;=\; p_0^{k_0} p_1^{k_1} \ldots p_r^{k_r}$$

for the necessary primes, p_0, p_1, ..., p_r and positive integers, k_0, k_1, ..., k_r, then, because Euler's totient function is multiplicative,

$$\begin{aligned}
s &= \phi(n) \\
&= \phi\left(p_0^{k_0} p_1^{k_1} \ldots p_r^{k_r}\right) \\
&= \phi\left(p_0^{k_0}\right)\phi\left(p_1^{k_1}\right)\ldots\phi\left(p_r^{k_r}\right) \\
&= p_0^{k_0-1}(p_0-1)p_1^{k_1-1}(p_1-1)\ldots p_r^{k_r-1}(p_r-1) \\
&= p_0^{k_0}\left(\frac{p_0-1}{p_0}\right)p_1^{k_1}\left(\frac{p_1-1}{p_1}\right)\ldots p_r^{k_r}\left(\frac{p_r-1}{p_r}\right) \\
&= n\prod_{i=0}^{r}\frac{p_i-1}{p_i} \\
\Rightarrow\; n &= s\prod_{i=0}^{r}\frac{p_i}{p_i-1}.
\end{aligned}$$

A consequence of the formula $\phi(p^m) = p^{m-1}(p-1)$ is that if p divides n then $p-1$ must divide $\phi(n)$ and it follows that, for each p, $p_i - 1$ divides s. Hence we have $n \leq A(s)$. □

From Theorem 1, bounds of the solutions to the equation

$$n \;=\; \phi^{-1}(8)$$

are found by adding one to each of 1, 2, 4 and 8, the divisors of 8, to obtain the prime numbers 2, 3 and 5, and the composite 9 which is thrown away. Thus

$$A(8) \;=\; 8 \times \frac{2}{1} \times \frac{3}{2} \times \frac{5}{4} \;=\; 30,$$

therefore

$$8 \ < \ \phi^{-1}(8) \ \leq \ 30,$$

and the desired reassurance has been obtained.

Theorem 1 has 'holes in it' in the sense that many integers, s, are not in $\phi^{-1}(n)$. For example, a consequence of the formula $\phi\,(p^m) = p^{m-1}(p-1)$ is that if either p is odd or $p = 2$ and $m > 1$ then $p^{m-1}(p-1)$ is even. Hence, for $n \geq 3$, $\phi(n)$ cannot be odd. Some even numbers also are missing, the first example being 14 for which I'll provide a proof in Proposition 1. Other low value examples are 26, 34, 38, 50 and 62, [6].

Proposition 1: $\phi(n) = 14$ has no solutions.

Proof: If a prime p is a divisor of n then $p - 1$ is necessarily a divisor of $\phi(n)$. The primes p for which $p - 1$ is a divisor of 14 are 2 and 3.

Case 1: Suppose that $n = 2^r$; then

$$\phi\,(2^r) \ = \ 2^{r-1} \neq 14.$$

Case 2: Suppose that $n = 3^s$; then

$$\phi\,(3^s) \ = \ 3^{s-1} \times 2 \neq 14.$$

Case 3: Suppose that $n = 2^r 3^s$; then

$$\phi\,(2^r 3^s) \ = \ \phi\,(2^r) \times \phi\,(3^s) \ = \ 2^{r-1} \times 3^{s-1} \times 2 \ = \ 2^r 3^{s-1} \neq 14.$$

Thus $\phi(n) = 14$ has no solutions. There is no width of number grid that can trap the primes in 14 of the available rows. $\square$

10. How good a trap can be built?

Some stabs in the dark reveal that better traps than those for $n = 6$ and $n = 30$ exist. For example, with $n = 420$,

$$\frac{\phi(420)}{420} \times 100 \ = \ 22^{6}/_{7}\,\%.$$

The curious will wish to know how low this percentage can go. In a natural manner the requirement has arisen to understand the function

$$f(n) \ = \ \frac{\phi(n)}{n}.$$

The percentage rating of a trap is then given by simply multiplying $f(n)$ by 100. Partial illumination is provided by Theorem 2. I'll prove this carefully and in detail because it's a thought-provoking result, and interested readers may wish to revisit the steps to explore easily obtained improvements either in general, or in specific cases, such as when n is divisible by 4 or when n has some other property yet to be identified as of importance.

Theorem 2:
$$\frac{1}{2\sqrt{n}} \;\le\; \frac{\phi(n)}{n} \;\le\; 1 \qquad \text{for } n \ge 1.$$

Proof: Without loss of generality, by the fundamental theorem of arithmetic, let the positive integer n be written as a product of primes of the form
$$n \;=\; 2^{k_0} p_1^{k_1} \ldots p_r^{k_r}$$
for necessary odd primes, $p_1, \ldots, p_r$ and positive integers, $k_1, \ldots, k_r$; k_0 is a non-negative integer. That is, k_0 can be zero.

By the multiplicative property of Euler's totient function,

$$\begin{aligned} \frac{\phi(n)}{n} &= \frac{\phi\left(2^{k_0}\right)\phi\left(p_1^{k_1}\right)\phi\left(p_2^{k_2}\right)\ldots\phi\left(p_r^{k_r}\right)}{2^{k_0}p_1^{k_1}p_2^{k_2}\ldots p_r^{k_r}} \\ &= \left(\frac{2^{k_0-1}}{2^{k_0}}\right)\left(\frac{p_1^{k_1-1}(p_1-1)}{p_1^{k_1}}\right)\ldots\left(\frac{p_r^{k_r-1}(p_r-1)}{p_r^{k_r}}\right). \end{aligned} \tag{1}$$

For an upper bound we can further write (1) as

$$\begin{aligned} \frac{\phi(n)}{n} &= \left(\frac{2-1}{2}\right)\left(\frac{p_1-1}{p_1}\right)\ldots\left(\frac{p_r-1}{p_r}\right) \\ &= \left(1-\frac{1}{2}\right)\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\ldots\left(1-\frac{1}{p_r}\right) \end{aligned}$$

and use the inequality that for any prime p,

$$1-\frac{1}{p} \;\le\; 1$$

to obtain the stated upper bound, also noticing that when n is even this can effortlessly be improved to give

$$\frac{\phi(n)}{n} \;\le\; \frac{1}{2} \qquad \text{for even } n.$$

For a lower bound we can use in (1) the fact that for any odd prime, p, $p - 1 > \sqrt{p}$. Thus (1) becomes

$$\begin{aligned}\frac{\phi(n)}{n} &\geq \left(\frac{1}{2}\right)\left(\frac{p_1^{k_1-1}\sqrt{p_1}}{p_1^{k_1}}\right)\cdots\left(\frac{p_r^{k_r-1}\sqrt{p_r}}{p_r^{k_r}}\right)\\ &\geq \left(\frac{1}{2}\right)\left(\frac{p_1^{k_1-0.5}}{p_1^{k_1}}\right)\cdots\left(\frac{p_r^{k_r-0.5}}{p_r^{k_r}}\right).\end{aligned}$$

Now for $k \geq 1$, $k - 0.5 \geq 0.5k$,

$$\begin{aligned}\frac{\phi(n)}{n} &\geq \left(\frac{1}{2}\right)\left(\frac{p_1^{0.5k_1}}{p_1^{k_1}}\right)\cdots\left(\frac{p_r^{0.5k_r}}{p_r^{k_r}}\right)\\ &\geq \left(\frac{1}{2}\right)\left(\frac{2^{0.5k_0}}{2^{0.5k_0}}\right)\left(\frac{1}{p_1^{0.5k_1}}\right)\cdots\left(\frac{1}{p_r^{0.5k_r}}\right)\\ &\geq \left(\frac{1}{2}\right)\left(\frac{2^{0.5k_0}}{\sqrt{n}}\right).\end{aligned}$$

Finally, observing that for any non-negative integer value of k_0, $2^{0.5k_0} \geq 1$ yields the claimed lower bound. $\square$

The upper bound of Theorem 2 is not a surprise because of the fact established by Euclid that there are an infinite number of primes. Each time a prime is encountered $f(n)$ is almost on the upper bound. In other words,

$$f(p) = \frac{\phi(p)}{p} = \frac{p-1}{p} = 1 - \frac{1}{p} \to 1 \;\; \text{(i.e. 100\%) as } p \to \infty.$$

The lower bound of Theorem 2 is tantalising for it leaves open, but unresolved, the possibility that as n becomes larger there are widths of number grid to be found in which the primes become trapped in an ever decreasing percentage of the rows of the n-wide table. Of course, just because Theorem 2 established a lower bound, there's no guarantee that values of $\phi(n)$ come close to it. This worry is exacerbated by the fact the lower bound values seem well below the 'best in their neighbourhood' results previously obtained. That is,

$$\text{for } n = 6, \quad \frac{\phi(6)}{6} = 0.333, \quad \text{but} \quad \frac{1}{2\sqrt{6}} = 0.204;$$

$$\text{for } n = 30, \quad \frac{\phi(30)}{30} = 0.267, \quad \text{but} \quad \frac{1}{2\sqrt{30}} = 0.091.$$

As is so often experienced by those working with prime numbers, seeming progress can turn out to be an illusion.

11. Primorials

The search for a good prime trap alighted upon the fact that the number grids with widths associated with $\phi(6)$ and $\phi(30)$ were more restrictive than neighbouring values. Since 1987, when Harvey Dubner [7] invented the expression, 6 and 30 have become known as early consecutive terms of the sequence of 'primorials'. For the w^{th} prime number, $p_w\#$ is defined as the product of the first w primes.

$p_w\#$	product	value
$p_1\#$	2	2
$p_2\#$	2×3	6
$p_3\#$	$2 \times 3 \times 5$	30
$p_4\#$	$2 \times 3 \times 5 \times 7$	210
$p_5\#$	$2 \times 3 \times 5 \times 7 \times 11$	2310

What is sought is a sequence within $f(n)$ that ignores most of the terms in $f(n)$ that are displaying so much variation, and which instead steadily decreases in value towards 0 as Theorem 2 suggested is possible. Primorials are the key as Theorem 3 and its proof will show.

Theorem 3: For each primorial $p_w\#$,

$$f(p_w\#) \;=\; \frac{\phi\left(p_w\#\right)}{p_w\#}$$

is smaller than itself for any lesser primorial.

Proof: Let an arbitrary primorial $p_w\#$ with $w \geq 2$ be decomposed into its product of primes, for any $w \geq 2$, $p_w\# = p_0 p_1 \ldots p_w$. Then

$$\begin{aligned}
\frac{\phi\left(p_w\#\right)}{p_w\#} &= \frac{\phi\left(p_0 p_1 \ldots p_w\right)}{p_0 p_1 \ldots p_w} \\
&= \frac{\phi\left(p_0 p_1 \ldots p_{w-1}\right)}{p_0 p_1 \ldots p_{w-1}} \times \frac{\phi\left(p_w\right)}{p_w} \\
&= \frac{\phi\left(p_{w-1}\#\right)}{p_{w-1}} \times \frac{\left(p_w - 1\right)}{p_w} \;=\; \frac{\phi\left(p_{w-1}\#\right)}{p_{w-1}} \times \left(1 - \frac{1}{p_w}\right);
\end{aligned}$$

therefore

$$\frac{\phi\left(p_w\#\right)}{p_w\#} < \frac{\phi\left(p_{w-1}\#\right)}{p_{w-1}} \qquad \text{for any } w \geq 2. \qquad \square$$

12. Conclusion

A simple idea has been pursued a long way with a pleasingly minimalist set of tools. Success has been achieved in trapping the primes into as small a proportion of the positive integers as desired. However, some quick numerical calculations show that the widths of the number grids required rapidly become vast. For example,

$$\frac{\phi(p_{10}\#)}{p_{10}\#} = \frac{1\,021\,870\,080}{6\,469\,693\,230} = 0.158.$$

This primorial-width number grid has a lot of rows in which the primes reside, even if the percentage rating of the trap is down to 15.8%.

References

[1] T. M. Apostol, *Introduction to Analytic Number Theory*, Springer, 2000.

[2] H. Davenport, *The Higher Arithmetic*, Cambridge Univ. Press, 1999.

[3] *Tables of Euler's Totient Function*, `http://www.NumberWonder.co.uk/Pages/Page9079.html`, 2019.

[4] H. Gupta, Euler's Totient Function and its Inverse, *Indian Journal of Pure and Applied Mathematics* **12** (January 1981).

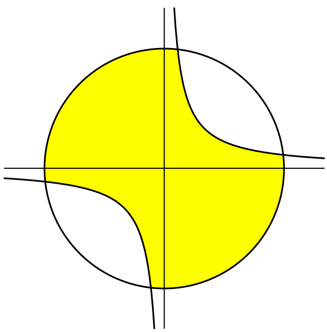
[5] R. Coleman, *Some Remarks on Euler's Totient Function*, hal-00718975, 2012.

[6] N. J. A. Sloane, *The On-Line Encyclopaedia of Integer Sequences*, A005277, `http://www.oeis.org/A005277`.

[7] H. Dubner, Factorial and Primorial Primes, *The Journal of Recreational Mathematics* **19** (1987).

Problem 302.1 – A circle and a hyperbola

The circle has radius r and the hyperbola is $y = 1/x$. What's the area of the yellow (light grey) part?



I (TF) cannot recall ever seeing this in any textbook or other publication. Yet surely it must be amongst the most natural of the various shapes that you would want to consider as soon as you have learned how to calculate areas by integrating functions. If $r \le \sqrt{2}$, the hyperbola can be ignored.