A Graph of Primes

DONALD E. G. MALM
Oakland University
Rochester, MI 48309

Some time ago a colleague asked me a question about the graph formed by associating a vertex with each prime, and placing an edge between each pair of primes whose difference in absolute value is a nonnegative power of 2. His question was whether the graph formed in this way is connected. This kind of graph, which is called a *similarity* graph, is discussed in his text [**5**, p. 540]. A similarity graph is one in which vertices connected by an edge are not too different. In this case, primes that share an edge are similar in that their expressions in binary notation are close—their difference has only one nonzero binary digit.

We readily see that 2 shares an edge with 3, and so do 5, 7, 11, 19, etc. The prime 41 chains to 2: $41 \to 37 \to 5 \to 3 \to 2$. The prime 127 chains to 2, but not mononotically: $127 \to 131 \to 3 \to 2$. It's easy to check by hand that all primes less than a few hundred chain to 2. A computer or programmable calculator check verifies without too much effort that all primes less than 3000 also chain to 2, and with a little more effort one can check that all primes less than 40,000 chain to 2.

Despite the above evidence, the answer to my colleague's question is that the graph is not connected. Fred Cohen and J. L. Selfridge [**3**], extending a technique of Erdős, exhibit a 26-digit prime that is neither a sum nor a difference of a power of two and a prime, thus proving that the graph has an isolated node. The technique is a powerful but elementary use of congruences together with some help from computers. The purpose of this paper is to show how that technique works, in the process pushing a little further to obtain the result that there are infinitely many isolated nodes in the graph.

Actually, there are two natural graphs that one can consider—the graph consisting of all positive primes (the "small graph"), and the one that includes the negative primes as well (the "total graph"). Using the total graph, one can, for example, chain $97 \to -31 \to -23 \to -7 \to -3 \to -2 \to 2$, and one can chain $3181 \to -5011 \to -2963 \to -2707 \to -659 \to -643 \to -131 \to -3 \to 5 \to 3 \to 2$. In fact, if negative primes are not allowed, it is only possible to chain 3181 to 2 by using primes of 19 digits. This is because $3181 - 2^n$ is never a positive prime, while the smallest value of n for which $3181 + 2^n$ is prime is 60. (This is easily checked using a primality test and a computer.)

In 1950 P. Erdős [**4**] proved that there is an infinite arithmetic progression of odd integers, none of which can be written in the form $p + 2^n$, with p prime. Such an arithmetic progression will contain an infinite number of primes, and each of these primes shares no edge with a smaller prime. However, such a prime may very well chain to 2 anyway, just as 127 does. To deal with the graph of primes, one must also control $p - 2^n$.

The key concept used in the proof is that of a *covering system for a set S of integers*, which is a collection of k congruences of the form $y \equiv a_i \pmod{n_i}$, with $n_1 < n_2 < \cdots < n_k$, for which every integer y in S satisfies at least one of the congruences $y \equiv a_i \pmod{n_i}$. An example of a simple covering system for the set of all integers is $x \equiv 0 \pmod 2$, $0 \pmod 3$, $1 \pmod 4$, $1 \pmod 6$, $11 \pmod{12}$. If we drop the requirement that the n_i be distinct, we will call the result a *congruence set*. Guy [**6**, p. 140–141] discusses covering systems and unsolved questions about them.

The basic idea of the proof is this. If we can find a covering system $a_i \pmod{q_i}$ for the set of numbers 2^n, $n = 0, 1, 2, \ldots$ then by the Chinese Remainder Theorem there is an arithmetic progression for which every term x satisfies all the congruences $x \equiv -a_i \pmod{q_i}$. Suppose x is a member of this arithmetic progression that is bigger than all the q_i. Then $x + 2^n$ must be composite for all $n \geqslant 0$, since for any such n, there is an a_i with $2^n \equiv a_i \pmod{q_i}$, and therefore $x + 2^n \equiv 0 \pmod{q_i}$. To find isolated vertices in either graph, we must also handle $x - 2^n$ for $n \geqslant 0$. This can be done by using a second covering system $b_i \pmod{r_i}$ for the set 2^n, $n = 0, 1, 2, \ldots$, where now we require $x \equiv b_i \pmod{r_i}$ rather than $x \equiv -b_i \pmod{r_i}$. The trouble is that these new congruences must not contradict the first ones, and we must also ensure that $x \pm 2^n$ is never equal to any of the moduli q_i or r_i, so that $x \pm 2^n \equiv 0$ implies that $x \pm 2^m$ actually is composite.

Covering systems for the set of powers of 2 can be constructed from certain congruence sets for the set of integers. The idea is illustrated by observing that if (say) $n \equiv 11 \pmod{12}$, then $n = 11 + 12m$ for some m, and $2^n = 2^{11} * 2^{12m}$. Since $2^{12} - 1$ has the prime factors 3, 5, 7, and 13, it follows that $2^{12} \equiv 1 \pmod{q}$ if q is any of the above primes, and $2^n \equiv 2^{11} \pmod{q}$. We see that we can get a covering system for the set of nonnegative powers of 2 from a congruence set for the set of all integers provided that the numbers $2^{n_i} - 1$ have sufficiently many different prime factors. In searching for such a covering system, the book [2] is invaluable, for it contains a table of the prime factors of $2^n - 1$ for positive $n < 250$. It is not necessary that the congruences for the set of all integers have distinct moduli, only that they lead to a bona fide covering system for the set of powers of 2. Table 1 lists two congruence sets for n and their corresponding covering sets for 2^n. These were found using a computer. (In this table, the number in parentheses following each residue is the corresponding modulus of the congruence.)

TABLE 1

$n \equiv$	$2^n \equiv$	$n \equiv$	$2^n \equiv$
0(2)	1(3)	1(2)	2(3)
0(3)	1(7)	0(4)	1(5)
1(8)	2(17)	0(5)	1(31)
1(9)	2(73)	0(7)	1(127)
11(12)	7(13)	2(10)	4(11)
7(18)	14(19)	2(14)	4(43)
5(24)	32(241)	1(15)	2(151)
31(36)	22(37)	2(16)	4(257)
13(36)	17(109)	14(20)	25(41)
		3(21)	8(337)
		6(28)	6(29)
		18(28)	97(113)
		8(30)	256(331)
		1(35)	2(71)
		58(60)	46(61)
		18(60)	586(1321)
		26(70)	163(281)
		206(21)	66(211)

Once the entries of the table have been found, it is simple to verify their correctness. The moduli for the first congruence set for n have l.c.m. 72, so one needs only to verify that each integer between 0 and 71 inclusive satisfies at least one of the congruences. The corresponding covering system for 2^n can be verified using the tables [2]. The second set of entries is handled in the same way. In this case the l.c.m. of the moduli for n is 1680.

Note that in each covering system for 2^n the moduli are distinct primes; also the only prime common to both systems is 3.

Now we can write down a system of congruences for which any solution will be an integer that is *not* of the form $q + 2^n$ or $q - 2^n$, with q prime. We indicate the modulus of each congruence by writing it in parentheses. The system is:

$$
\begin{array}{rrr}
x \equiv -1(3) & -1(7) & -2(17) \\
-2(73) & -7(13) & -14(19) \\
-32(241) & -22(37) & -17(109) \\
\hdashline
1(5) & 1(31) & 1(127) \\
4(11) & 4(43) & 2(151) \\
4(257) & 25(41) & 8(337) \\
6(29) & 97(113) & 256(331) \\
2(71) & 46(61) & 586(1321) \\
163(281) & 66(211) & \\
\hdashline
 & & 1000(2047)
\end{array}
\tag{1}
$$

The 27 congruences of this system (1) come from three sources:

1) The first 9, from the first covering system, guarantee that if x satisfies each, then for each n, $x + 2^n \equiv 0 \pmod{p}$ for at least one of the moduli p.

2) The next 17 are from the second covering system. Together with $x \equiv 2 \pmod 3$, which is the first congruence, they ensure that if x satisfies each of these 18 congruences, then for each n, $x - 2^n \equiv 0 \pmod{p}$ for at least one of the moduli p. It follows that if x is a solution to the first 26 congruences, then every number of the form $x \pm 2^n$ must be composite unless it *is* one of the moduli.

3) The last congruence guarantees that the numbers of the form $x \pm 2^n$ cannot be equal to any of the moduli. For, since 2047 is one less than a power of two, the set of values of $2^n \pmod{2047}$ is $\{1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1024\}$. If x satisfies all 27 congruences, then $x \pm 2^n \pmod{2047}$ must be one of the numbers $\{1001, 1002, 1004, 1008, \ldots, 1512, 2024, 999, 998, 996, 992, \ldots, 488, -24\ (\equiv 2023)\}$. However, none of the prime moduli (mod 2047) are any of these values. It follows that if x is any solution of this system of 27 congruences, then $x \pm 2^n$ must be divisible by one of the prime moduli of the first 26, but cannot be equal to any of those moduli, and so must be composite.

The Chinese Remainder Theorem guarantees that there is an infinite arithmetic progression of solutions to system (1). (Note that the moduli are relatively prime, for $2047 = 23 * 89$.) Dirichlet's theorem [7, p. 31] guarantees that this arithmetic progression contains infinitely many primes, since the first term and the common difference must be relatively prime. These primes are isolated in both the total graph and the small graph.

The solution of system (1) is the arithmetic progression $a + bm$, where m is the parameter and

$$
\begin{aligned}
a &= 16072\ 35727\ 03020\ 46589\ 74480\ 25537\ 91940\ 51479\ 85029\ 22751, \\
b &= 23526\ 41407\ 50797\ 04441\ 84622\ 22680\ 98507\ 82474\ 11014\ 41905.
\end{aligned}
$$

To exhibit a specific isolated prime as small as our covering systems allow, we omit the 27th congruence from (1), solve this smaller system, find the smallest positive prime q in the arithmetic progression of solutions, and verify directly that $q-2^n$ is never equal to any of the prime moduli in the first 26 congruences. This yields

$$q = 293\ 84382\ 54055\ 73891\ 53952\ 59805\ 37456\ 23284\ 74806\ 89009,$$

which is the smallest prime I have found that is isolated in the total graph, though the prime of Cohen and Selfridge mentioned above is smaller (their covering sets are different from ours).

One can find smaller primes that are isolated in the small graph by using only the first covering system to find an arithmetic progression of numbers x for which $x+2^n$ is never prime. Then find a positive prime q in this arithmetic progression for which $q-2^n$ is never a positive prime. This process yields $q = 5404\ 26473$, the smallest prime I found that is isolated in the graph of positive primes. This prime is not isolated in the total graph, for $q-2^{126}$ is prime.

While the original question is answered, very little else seems to be known about these two graphs. Natural questions are (we use the term degree in the usual graph-theoretic sense—the degree of a vertex is the number of edges it has):

1) Do any vertices have infinite degree?

2) In the total graph, are there any vertices of finite positive degree other than 2 and -2? In the small graph, one can find, as above, primes that don't chain upward and therefore have finite degree. I have found such vertices of degrees 0 through 6 inclusive. However, even in the small graph I do not know whether there are infinitely many vertices of finite positive degree nor whether there are vertices of arbitrarily large degree.

3) Does there exist an infinite connected component?

4) Is there a connected finite component of more than one vertex?

5) What is the smallest prime not in the component containing 2?

6) What is the smallest isolated node? Is it the same prime as in 5)?

Here, as in much of number theory, simple questions arise that seem difficult to answer.

I thank Jerrold Grossman for raising this problem, and for a careful reading of the manuscript. I also thank the referees for their helpful comments, and for bringing [3] to my attention. The numerical computations were done on Macintosh and PC computers, using my multiprecision number theory package (I distribute this package without charge via ftp, see [1] for details) and also routines distributed with the language UBASIC, most notably the Adelman-Pomerance-Rumely-Cohen-Lenstra primality test.

REFERENCES

1. Jon Barwise, Computers and Mathematics, *Notices Amer. Math. Soc.* 38 (1991), 104–110.
2. J. Brillhart, D. H. Lehmer, J. L. Selfridge, B. Tuckerman, and S. S. Wagstaff, Jr., *Factorizations of* b^n+1, $b = 2,3,5,6,7,10,11,12$ *up to High Powers*, Amer. Math. Soc., Providence, RI, 1983.
3. Fred Cohen and J. L. Selfridge, Not every number is the sum or difference of two prime powers, *Math. of Comp.* 29 (1975), 79–81.
4. P. Erdős, On integers of the form $2k+p$ and some related problems, *Summa Brasiliensis Mathematica* 2 (1950), 113–123.
5. J. Grossman, *Discrete Mathematics*, Macmillan Publishing Co., New York, 1990.
6. Richard K. Guy, *Unsolved Problems in Number Theory*, Springer-Verlag New York, Inc., New York, 1981.
7. Ivan Niven, Herbert S. Zuckerman, and Hugh L. Montgomery, *An Introduction to the Theory of Numbers*, 5th edition, John Wiley & Sons, Inc., New York, 1991.