An Eratosthenean Sieve for Prime Decades

Eric Snyder, 23 June 2021

Prime constellations of various sorts are a source of continued fascination for both professional and recreational mathematicians. Some of the problems about prime constellations, such as the Twin Prime Conjecture, are intractably difficult to solve despite being incredibly simple to state.

One type of prime constellation, the prime quadruplet, consists of four prime numbers between p and $p+8$. Other than the sequences $(3, 5, 7, 11)$ and $(5, 7, 11, 13)$, all of the quadruplets are also *prime decades*. The prime decades are sequences of four consecutive prime numbers that fall between two consecutive multiples of 10. For example, the first two prime decades are $(11, 13, 17, 19)$ and $(101, 103, 107, 109)$. All of these sequences can be expressed as $(15n-4, 15n-2, 15n+2, 15n+4)$ for some odd n. OEIS Sequence A112540[1] gives the sequence of values of n, starting with $(1, 7, 13, 55, 99, \dots)$.

The author is a recreational mathematician; no pretense is made that the notes presented here are particularly exciting or illuminating to academics. It seems all but impossible that mathematicians examining prime constellations would not use some form of sieve to find those constellations. However, while a search of the literature turned up examples of highly complex sieves[2], and sieves for large clusters[3], no sign was found of a simple sieve for the decades–one that someone with nothing more than a knowledge of modular arithmetic and basic algebra could use readily. This was surprising given the well-known Sieve of Eratosthenes for individual primes, and relatively well-known sieves for the twin primes[4][5].

The novel portion of this work, then, is the simple Eratosthenean sieve given for the prime decades. It is followed by a (longer) proof that the sieve works as described.

The Sieve

Unlike the Sieve of Eratosthenes, the sieve presented here does not sieve for the prime decades directly; instead, it removes from the number line all of the values not in the OEIS sequence given above. Once those numbers are obtained, one can readily find the four primes within the decade as well.

1. Begin with $\mathbb{N}$, the set of natural numbers or positive integers. Remove all the even numbers to give a set N_o; all the numbers in the sequence are odd.

2. Determine the value k for each prime. For each prime 7 or larger, k is the number such that, if the prime is written as $p = 15k \pm q$, then q will be between -7 and 7. In particular, q will take one of the values in $\{\pm 1, \pm 2, \pm 4, \pm 7\}$. For example, 79 is $(15)(5) + 4$, and 89 is $(15)(6) - 1$.

3. Beginning with $p = 7$ and stepping upward through the prime numbers, remove elements of N_o where $n \equiv \pm r \pmod{p}$ or $n \equiv \pm s \pmod{p}$, but $n \neq k$, as follows:

$$\begin{array}{ll}
r, s = \pm 2k, \pm 4k & \text{for } q = \pm 1 \\
r, s = \pm k, \pm 2k & \text{for } q = \pm 2 \\
r, s = \pm k, \pm(7k + 2) & \text{for } q = 4 \\
r, s = \pm k, \pm(7k - 2) & \text{for } q = -4 \\
r, s = \pm(4k + 2), \pm(8k + 4) & \text{for } q = 7 \\
r, s = \pm(4k - 2), \pm(8k - 4) & \text{for } q = -7
\end{array}$$

To demonstrate, start with the odd numbers (N_o), and strike out all those $n \equiv \pm(4k + 2) \pmod{7}$ or $n \equiv \pm(8k + 4) \pmod{7}$. $k = 0$, so this strikes out $n \equiv 2, 3, 4, 5 \pmod{7}$.

1 ~~3~~ ~~5~~ 7 ~~9~~ ~~11~~ 13 15 ~~17~~ ~~19~~ 21 ~~23~~ ~~25~~ 27 29 $\cdots$

For p = 11, $k = 1$, $q = -4$ and $r, s = \pm k, \pm(7k - 2) = \pm 1, \pm 5 \pmod{11}$. Note that $n = 1$ is *not* removed, because $n = k$.

1 7 13 15 ~~21~~ ~~27~~ ~~29~~ 35 41 ~~43~~ ~~49~~ 55 57 63 69 $\cdots$

For $p = 13$, strike $n \equiv r, s \equiv \pm 1, \pm 2 \pmod{13}$, again excepting 1:

1 7 13 ~~15~~ 35 ~~41~~ 55 57 ~~63~~ 69 73 75 ~~79~~ 81 95 $\cdots$

The integers that are not part of the sequence are slowly being removed. This process is a bit slower than the Sieve of Eratosthenes, as the number line has been compressed by a factor of around 15. The sieve using $p = 13$ really rejects the composite numbers $(15)(15)-2 = 223, (15)(41)-4 = 611, (15)(63)+4 = 949$, etc. An integer is removed (or not) from the Sieve of Eratosthenes by, at largest, a prime near $\sqrt{n}$; in this prime decade sieve, a given number must be tested with primes up to $\sqrt{15n}$. The high density of numbers removed using only 7, however, means the sieve is slightly faster than this would normally imply.

The Theorem and Proof

First, some definitions and conventions:

Herein, p always represents a prime number, and all lowercase letters represent integers. $\mathbb{P}$ is the set of all prime numbers, and $\mathbb{N}$ excludes 0, that is, $\mathbb{N} \equiv \mathbb{Z}^+$.

OEIS Sequence A112540 can be redefined as a set T with elements n_i:

$$T := \{n \in \mathbb{N} \mid \{15n-4, 15n-2, 15n+2, 15n+4\} \subset \mathbb{P}\}$$

The individual possible primes calculated from each n are represented as $t_{n,1}$, $t_{n,2}$, $t_{n,3}$, and $t_{n,4}$ respectively. For example, $t_{1,1} = (15)(1) - 4 = 11$ and $t_{5,3} = (15)(5) + 2 = 77$. These are, importantly, only *possibly* primes.

Theorem 1. Let $T := \{n \in \mathbb{N} \mid \{15n-4, 15n-2, 15n+2, 15n+4\} \in \mathbb{P}\}$. Express the primes $p \geq 7$ in a least absolute residue system as $p = 15k \pm q$, with $q \in \{1, 2, 4, 7\}$. Then:

$$\text{Given } S := \{[(n \equiv \pm r \pmod{p}) \vee (n \equiv \pm s \pmod{p})] \wedge [n \neq k]\},$$
$$\forall (p \geq 7, p = 15k \pm q)\ (\exists r \pmod{p}, s \pmod{p}) : [\forall n\ (\exists p : S) \implies n \notin T], \text{where}$$

$$r, s = \left\{ \begin{array}{lr} \pm 2k, \pm 4k & \text{for } q \equiv \pm 1, k \text{ even} \\ \pm k, \pm 2k & \text{for } q \equiv \pm 2, k \text{ odd} \\ \pm k, \pm(7k-2) & \text{for } q \equiv -4, k \text{ odd} \\ \pm k, \pm(7k+2) & \text{for } q \equiv 4, k \text{ odd} \\ \pm(4k-2), \pm(8k-4) & \text{for } q \equiv -7, k \text{ even} \\ \pm(4k+2), \pm(8k+4) & \text{for } q \equiv 7, k \text{ even} \end{array} \right\}$$

The theorem is initially expressed symbolically for clarity, as a natural-language translation is unwieldy and has fewer parentheses available. In summary: with T, p, q, and k as defined above, every prime has four residues $\pm r \pmod{p}$ and $\pm s \pmod{p}$ such that, if for *any* prime $p \geq 7$, if ($n \equiv \pm r \pmod{p}$ or $n \equiv \pm s \pmod{p}$ and $n \neq k$), then $n \notin T$.

To set up the proof, several lemmas are necessary.

Lemma 1. For a given $n \in N_o$, $n \in T$ if and only if for all i, $t_{n,i}$ is indivisible by any integer $1 < z < t_{n,i}$.

On some level this is not so much a lemma as a rearrangement of the definition of T. However, this rearrangement in terms of *divisibility* allows for easier proof.

Lemma 2. All primes $p \geq 7$ can be expressed in the form $p = 15k \pm q$ in a least absolute residue system, where $q \in \{\pm 2, \pm 4\}$ (for k odd), or $q \in \{\pm 1, \pm 7\}$ (for k even).

Proof. Consider all the integers $m = 15k \pm q$ in a least absolute residue system mod 15.

If k is odd and q is odd, then $15k \pm q$ is even and not prime. Hence, $q \not\equiv \{\pm 1, \pm 3, \pm 5, \pm 7\} \pmod{15}$. If k is odd and q is even, $15k$ and $15k \pm 6$

are divisible by 3. Only the remaining integers $15k \pm 2$ and $15k \pm 4$ can be prime.

If k is even and q is even, then $15k \pm q$ is even and not prime. If k is even and q is odd, $15k \pm 3$ and $15k \pm 5$ are divisible by 3 and 5 respectively. Only the remaining integers $15k \pm 1$ and $15k \pm 7$ can be prime. □

This lemma results in a division of the prime numbers into several classes, which are used to enumerate the values of r and s in the theorem.

Finally, a quick trick of modular arithmetic, giving a convenient method of determining divisibility (for use with Lemma 1).

Lemma 3. Choose some positive integers a, b, k, n with $(a, b) = 1, a \geq b \geq 1$, and $n \geq k$. Then:

$$(u = ak + b, v = an + b) \iff (n \equiv k \pmod{u} \implies u \mid v)$$

Proof. Since $N \pmod{u}$ is the same as $N \pmod{ak + b}$, the proof is entirely in $(\text{mod } ak + b)$. In this modulus:

$$b \equiv -ak \iff v \equiv an - ak \iff v \equiv a(n - k)$$

Additionally, $(a, b) = 1 \implies (a, ak + b) = 1$, so a is invertible mod $ak + b$. Therefore:

$$n - k \equiv 0 \implies v \equiv 0 \iff u \mid v$$
$$\therefore n \equiv k \pmod{u} \implies u \mid v$$

The reverse implication is true only if $(k, c) = 1$. However, this is not necessary for the remainder of the proof. □

Lemma 3 can be further extended to cover cases where the residues of u and v are unequal, using essentially the same algebra as in Lemma 3.

Lemma 4. Choose integers as in Lemma 3, and additionally some nonzero integers c, d with $(a, c, d) = 1$. Then:

$$(u = ak + bc, v = an + bd) \iff (cn \equiv dk \pmod{u} \implies u \mid v).$$

Proof. Working entirely in $(\text{mod } ak + bc) \equiv (\text{mod } u)$:

$$ak \equiv -bc \iff adk \equiv -bcd$$
$$v \equiv 0 \iff an \equiv -bd \iff acn \equiv -bcd \iff acn \equiv adk \iff cn \equiv dk$$
$$v \equiv 0 \iff cn \equiv dk \implies u \mid v$$
$$\therefore cn \equiv dk \pmod{u} \implies u \mid v$$

Note that if c or $d = -1$, then in many cases expressions where two signs are possible can be simplified as:

$$(u = ak \pm bc, v = an \pm bd) \iff (\pm cn \equiv \pm dk \pmod{u} \implies u \mid v)$$ □

Proof of Theorem 1. Lemmas 3 and 4 show that modular equivalences can be used to determine divisibility of two numbers originally expressed in the same modulus a. Lemma 2 shows that the primes can be expressed in several classes (mod 15), and the original set definition also looks for primes (mod 15). Lemma 1 says that showing any of the numbers $15k \pm 2, \pm 4$ are divisible by some other number implies $n \notin T$, meaning that the inclusion of a given n in T can be determined by the modular equivalences of Lemmas 3 and 4.

There are multiple cases to prove.

Case 1. $n = k$

An exception anytime $n = k$. In these instances, $p \mid t_{n,i}$ because $p = t_{n,i}$, that is, the potential prime is *also* the divisor prime. Therefore congruences in which $n = k$ do not exclude n from T as even primes are divisible by themselves.

Case 2. $p = 15k \pm 1$

Using $b = 1, c = \pm 1, d = \pm 2$, Lemma 4 gives:

$$p = 15k \pm 1, a_{n,i} = 15n \pm 2 \iff [n \equiv \pm k \pmod{p} \implies p \mid t_{n,2} \text{ or } p \mid t_{n,3}]$$

Using $b = 1, c = \pm 1, d = \pm 4$, Lemma 4 gives:

$$p = 15k \pm 1, a_{n,i} = 15n \pm 4 \iff [n \equiv \pm k \pmod{p} \implies p \mid t_{n,1} \text{ or } p \mid t_{n,4}]$$

Hence, $q = \pm 1 \implies r = \pm 2k$ and $s = \pm 4k$

Case 3. $p = 15k \pm 2$

By the method of Case 2:

$$b = 2, c = \pm 1, d = \pm 1 \implies (q = \pm 2 \implies r = \pm k)$$
$$b = 1, c = \pm 1, d = \pm 2 \implies (q = \pm 2 \implies s = \pm 2k)$$

Case 4. $p = 15k \pm 4, a_{n,i} = 15n \pm 4$

By the method of Cases 2 and 3:

$$b = 4, c = \pm 1, d = \pm 1 \implies (q = \pm 4 \implies r = \pm k)$$

Case 5. $p = 15k + 4, a_{n,i} = 15n \pm 2$

Here $b = 2, c = 2, d = \pm 1$. Lemma 4 gives a less convenient result:

$$p = 15k + 4, a_{n,i} = 15n \pm 2 \iff [2n \equiv \pm k \pmod{p} \implies p \mid t_{n,1} \text{ or } p \mid t_{n,4}]$$

However, $2n \equiv \pm k$ can be converted into an expression with only n on the left-hand side, to prevent modular inverse calculations from being necessary:
In mod $15k + 4$, taking $a_{n,2} = 15n - 2$:

$$-2n \equiv k \iff -4n \equiv 2k \iff 15kn \equiv 2k \iff$$
$$15n \equiv 2 \iff 15n \equiv 105k + 30 \iff n \equiv 7k + 2$$

In mod $15k + 4$, taking $a_{n,3} = 15n + 2$, the same algebra gives the solution $n \equiv -(7k + 2)$. Hence, $q = 4 \implies s = \pm(7k + 2)$.

Case 6. $p = 15k - 4, a_{n,i} = 15n \pm 2$

Using $b = 2, c = -2, d = \pm 1$, Lemma 4 results in $-2n \equiv \pm k \pmod{p} \implies p \mid t_{n,1}$ or $p \mid t_{n,4}$. Then, by a rearrangement similar to Case 5,

$$b = 2, c = -2, d = \pm 1 \implies (q = -4 \implies s = \pm(7k - 2))$$

Case 7. $p = 15k + 7, a_{n,i} = 15n \pm 4$

Using $b = 1, c = 7, d = \pm 4$, Lemma 4 gives:

$$p = 15k + 7, a_{n,i} = 15n \pm 4 \iff [7n \equiv \pm 4k \pmod{p} \implies p \mid t_{n,1} \text{ or } p \mid t_{n,4}]$$

Using the methods of Cases 5 and 6, in mod $15k + 7$, taking $a_{n,1} = 15n - 4$:

$$7n \equiv -4k \iff -15kn \equiv -4k \iff 15n \equiv 4 \iff$$
$$15n \equiv 120k + 60 \iff n \equiv 8k + 4$$

In mod $15k + 7$, taking $a_{n,4} = 15n + 4$, the same algebra gives the solution $n \equiv -(8k + 4)$. Hence, $q = 7 \implies r = \pm(8k + 4)$.

Case 8. $p = 15k + 7, a_{n,i} = 15n \pm 2$

Using $b = 2, c = -2, d = \pm 1$, Lemma 4 results in $-7n \equiv \pm 4k \implies p \mid t_{n,1}$ or $p \mid t_{n,4}$. Then, by a rearrangement similar to Cases 5-7, $q = 7 \implies s = \pm(4k + 2)$.

Cases 9 and 10, where $p = 15k - 7$, would proceed with the same algebra as cases 7 and 8, ending such that $q = -7$ gives $r = \pm(8k - 4)$ and $s = \pm(4k - 2)$. The algebra is omitted in the interest of brevity. □

Discussion

There are a few points of interest in the use and description of this sieve.

First, it should be noted that, if desired, the sieve using 7, 11, and 13 could be used as a low-density wheel sieve with only 189 elements (mod 2002). If one were searching for very large decades, a larger wheel sieve might be more useful, though it would take up more memory to hold the wheel. Any given programmer should, of course, consider their time/space requirements.

This sieve is connected to the sieve for the twin primes[5], as each prime decade is a "twin of twins." In other words, each decade is a pair of consecutive integers in the set $\{k \in \mathbb{N} \mid 6k - 1 \in \mathbb{P} \wedge 6k + 1 \in \mathbb{P}\}$. It seems unlikely that this is useful for computation.

The sieve as presented could also be extended to the prime *sextuplets*, i.e., $15n \pm z, z \in \{\pm 2, \pm 4, \pm 8\}$. This would add a third component to the sieve using each prime, as follows:

$\pm 8k$	for $q = \pm 1$
$\pm 4k$	for $q = \pm 2$
$\pm 2k$	for $q = \pm 4$
$\pm(k + 1)$	for $q = 7$
$\pm(k - 1)$	for $q = -7$

This implies that all of the prime sextuplets have $n \equiv 0 \pmod{7}$, other than the first case $(7, 11, 13, 17, 19, 23)$, which is a known result.

For reference, the set of elements in the wheel (mod 2002) is:

$$\{5, 13, 7, 13, 29, 35, 55, 57, 69, 85, 91, 97, 99, 113, 125, 139, 147, 161, 169, 189, 195, 211, 217, 231, 239, 251, 253, 267, 273, 279, 293, 295, 315, 321, 343, 371, 377, 385, 393, 399, 407, 421, 433, 447, 449, 455, 475, 477, 491, 497, 503, 517, 525, 539, 553, 559, 575, 581, 601, 603, 629, 631, 645, 657, 671, 673, 679, 685, 693, 707, 715, 735, 741, 757, 763, 777, 783, 785, 799, 811, 825, 827, 839, 855, 861, 867, 889, 917, 931, 939, 953, 959, 965, 979, 981, 993, 1001, 1009, 1021, 1023, 1037, 1043, 1049, 1063, 1071, 1085, 1113, 1135, 1141, 1147, 1163, 1175, 1177, 1191, 1203, 1217, 1219, 1225, 1239, 1245, 1261, 1267, 1287, 1295, 1309, 1317, 1323, 1329, 1331, 1345, 1357, 1371, 1373, 1399, 1401, 1421, 1427, 1443, 1449, 1463, 1477, 1485, 1499, 1505, 1511, 1525, 1527, 1547, 1553, 1555, 1569, 1581, 1595, 1603, 1609, 1617, 1625, 1631, 1659, 1681, 1687, 1707, 1709, 1723, 1729, 1735, 1749, 1751, 1763, 1771, 1785, 1791, 1807, 1813, 1833, 1841, 1855, 1863, 1877, 1889, 1903, 1905, 1911, 1917, 1933, 1945, 1947, 1967, 1973, 1989, 1995\}$$

Acknowledgments

The author wishes to thank the many members of the Math Stackexchange Community, who gave valuable advice on modular arithmetic, and his wife, who puts up with his mathematical mumblings and musings.

Contact

The author can be reached at esnyder2@gmail.com. He has no institutional affiliation.

References

[1] OEIS Foundation Inc. *The On-Line Encyclopedia of Integer Sequences*. 2021. URL: http://oeis.org/A112540. (accessed: 09 June 2021).

[2] Tony Forbes. "Large Prime Quadruplets". In: *The Mathematical Gazette* 84.501 (Nov. 2000), pp. 447–452. DOI: 10.2307/3620774.

[3] Thomas R. Nicely. *Dense Prime Clusters*. URL: https://faculty.lynchburg.edu/~nicely/dense/dense1.html. (accessed: 09 June 2021).

[4] H. J. Weber. *Twin Prime Sieve*. 2012. arXiv: 1203.5240v7 [math.GM].

[5] A. Dinculescu. "On Some Infinite Series Related to the Twin Primes". In: *The Open Mathematics Journal* 5.1 (May 2012), pp. 8–14. DOI: 10.2174/1874117701205010008.