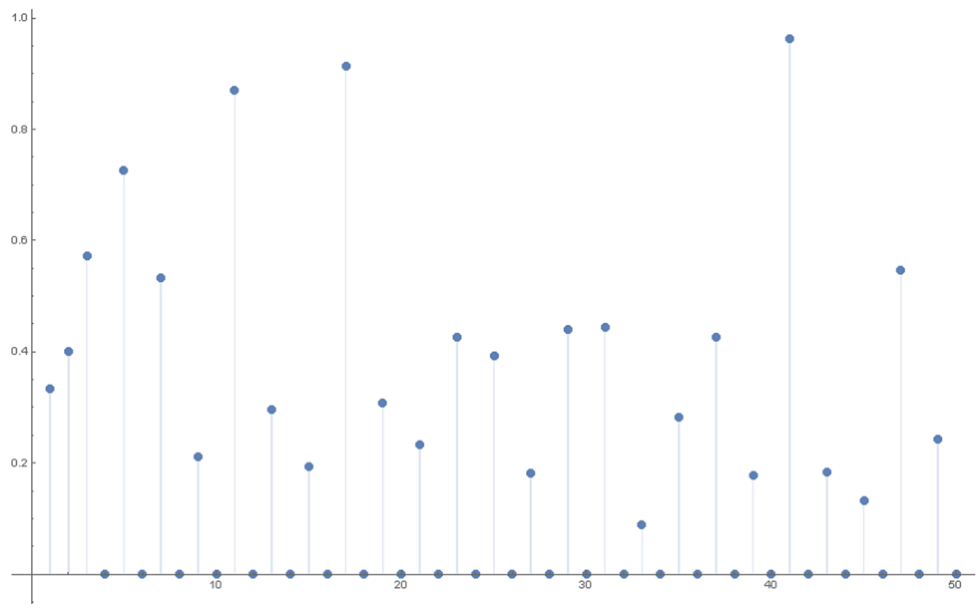
Prime Generation: Solution

Using the following two lines of input in Mathematica,

```
potential[n_]:=Sum[Boole[PrimeQ[x^2+x+n]],{x,-n,n}]/(2*n+1)

DiscretePlot[potential[n],{n,1,50}]
```

we receive the following output:



By inspection, the five highest-potential numbers are $n = 3, 5, 11, 17, 41$.

The corresponding discriminants $\Delta = 1 - 4n$ of the quadratics $x^2 + x + n$ are (minus) the largest five of the so-called **Heegner** numbers:

$$-\Delta = 1, 2, 3, 7, 11, 19, 43, 67, 163$$

These have significance in algebraic number theory.

An algebraic number is one which is the root of an integer-coefficient polynomial (in contrast to transcendental numbers), and an **algebraic integer** is one which is the root of a *monic* integer coefficient polynomial. All rational numbers are algebraic numbers, but the integers are the only rational numbers which are algebraic integers. More generally, any algebraic number is an algebraic integer divided by a whole number.

The Heegner numbers $-\Delta$ are the squarefree positive integers for which the algebraic integers generated from the imaginary surds $\sqrt{\Delta}$ enjoy **unique factorization** into irreducible elements. To illustrate, 5 is not a Heegner number because $2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$ are two inequivalent factorizations.

On April 1st, 1975, mathematical columnist Martin Gardner said $\exp(\pi\sqrt{163})$ was a whole number. In fact, it's not a whole number, but incredibly close:

$$\exp(\pi\sqrt{163}) \;\approx\; 262537412640768743.99999999999925\ldots$$

This is explained in modern number theory. More specifically, modular forms and elliptic forms. More specifically still, the j-invariant and "complex multiplication" (which is not what you think it is).

The **Bateman-Horn conjecture** predicts how often a family of polynomials $f_1(n), \cdots, f_m(n)$ are simultaneously prime. It says the number of $n \leq x$ for which each polynomials evaluate to a prime has the asymptotic estimate

$$\sim \frac{C}{D} \int_a^x \frac{\mathrm{d}t}{(\ln t)^m}$$

where a doesn't matter, $D = (\deg f_1) \cdots (\deg f_m)$, and the constant C is

$$C = \prod_p \frac{1 - N(p)/p}{(1-1/p)^m},$$

the infinite product taken over all primes p and $N(p)$ counting values mod p for which one of the values $f_1(n), \cdots, f_m(n)$ is 0 mod p.

This vastly generalizes the Twin Prime Conjecture (which says there are infinitely many pairs of primes 2 apart) and the Prime Number Theorem (which says the number of primes $\leq x$ is asymptotically $\int_0^x \mathrm{d}t/\ln t$).