A) Quadratic extensions

Are there infinitely many, or only finitely many such primes q? If so, what is the largest possible q?

The same problem should be asked for polynomials of first degree $f(X) = aX + b$, with $a, b \geqslant 1$. If $f(0)$ is a prime q, then $b = q$. Then $f(q) = aq + q = (a+1)q$ is composite. So, at best, $aX + q$ assumes prime values for X equal to $0, 1, \ldots, q - 1$.

Can one find such polynomials? Equivalently, can one find arithmetic progressions of q prime numbers, of which the first number is equal to q?

For small values of q this is not difficult.
If $q = 3$, take: 3, 5, 7, so $f(X) = 2X + 3$.
If $q = 5$, take: 5, 11, 17, 23, 29, so $f(X) = 6X + 5$.
If $q = 7$, take: 7, 157, 307, 457, 607, 757, 907, so $f(X) = 150X + 7$.

Quite recently, Keller communicated to me that for $q = 11, 13$ the smallest such arithmetic progressions are given by polynomials $f(X) = d_{11}X + 11$, respectively $f(X) = d_{13}X + 13$ with

$$d_{11} = 1536160080 = 2 \times 3 \times 5 \times 7 \times 7315048\,,$$

$$d_{13} = 9918821194590 = 2 \times 3 \times 5 \times 7 \times 11 \times 4293861989\,;$$

this determination required a considerable amount of computation, done by Keller & Löh.

It is not known whether for every prime q there exists an arithmetic progression of q primes of which the first number is q. Even the problem of finding arbitrarily large arithmetic progressions consisting only of prime numbers (with no restriction on the initial term or the difference) is still open. The largest known such arithmetic progression consists of 19 primes, and was found by Pritchard (1985).

The determination of all polynomials $f(X) = X^2 + X + q$ such that $f(n)$ is a prime for $n = 0, 1, \ldots, q - 2$, is intimately related with the theory of imaginary quadratic fields. In order to understand this relationship, I shall indicate now the main results which will be required.

A) Quadratic extensions

Let d be an integer which is not a square, and let $K = \mathbf{Q}(\sqrt{d})$ be the field of all elements $\alpha = a + b\sqrt{d}$, where $a, b \in \mathbf{Q}$. There is no loss of generality to assume that d is square-free, hence $d \not\equiv 0 \pmod 4$. $K \mid \mathbf{Q}$ is a quadratic extension, that is, K is a vector space of dimension 2 over $\mathbf{Q}$.

Conversely, if K is a field, which is a quadratic extension of $\mathbf{Q}$, then it is necessarily of the form $K = \mathbf{Q}(\sqrt{d})$, where d is a square-free integer.

If $d > 0$ then K is a subfield of the field $\mathbf{R}$ of real numbers: it is called a real quadratic field.

If $d < 0$ then K is not a subfield of $\mathbf{R}$, and it is called an imaginary quadratic field.

If $\alpha = a + b\sqrt{d} \in K$, with $a, b \in \mathbf{Q}$, its conjugate is $\alpha' = a - b\sqrt{d}$. Clearly, $\alpha = \alpha'$ exactly when $\alpha \in \mathbf{Q}$.

The norm of α is $N(\alpha) = \alpha\alpha' = a^2 - db^2 \in \mathbf{Q}$. It is obvious that $N(\alpha) \neq 0$ exactly when $\alpha \neq 0$. If $\alpha, \beta \in K$ then $N(\alpha\beta) = N(\alpha)\,N(\beta)$; in particular, if $\alpha \in \mathbf{Q}$ then $N(\alpha) = \alpha^2$.

The trace of α is $\mathrm{Tr}(\alpha) = \alpha + \alpha' = 2a \in \mathbf{Q}$. If $\alpha, \beta \in K$ then $\mathrm{Tr}(\alpha+\beta) = \mathrm{Tr}(\alpha) + \mathrm{Tr}(\beta)$; in particular, if $\alpha \in \mathbf{Q}$ then $\mathrm{Tr}(\alpha) = 2\alpha$.

It is clear that α, α' are the roots of the quadratic equation $X^2 - \mathrm{Tr}(\alpha)X + N(\alpha) = 0$.

B) Rings of integers

Let $K = \mathbf{Q}(\sqrt{d})$, where d is a square-free integer.

$\alpha \in K$ is an algebraic integer when there exist integers $m, n \in \mathbf{Z}$ such that $\alpha^2 + m\alpha + n = 0$.

Let A be the set of all algebraic integers of K. A is a subring of K, which is the field of fractions of A, and $A \cap \mathbf{Q} = \mathbf{Z}$. If $\alpha \in A$ then the conjugate $\alpha' \in A$. Clearly, $\alpha \in A$ if and only if both $N(\alpha)$ and $\mathrm{Tr}(\alpha)$ are in $\mathbf{Z}$.

Here is a criterion for the element $\alpha = a + b\sqrt{d}\ (a, b \in \mathbf{Q})$ to be an algebraic integer: $\alpha \in A$ if and only if

$$\begin{cases} 2a = u \in \mathbf{Z}\,, \quad 2b = v \in \mathbf{Z} \\ u^2 - d\,v^2 \equiv 0 \pmod 4\,. \end{cases}$$

Using this criterion, it may be shown:

If $d \equiv 2$ or $3 \pmod 4$ then $A = \{a + b\sqrt{d} \mid a, b \in \mathbf{Z}\}$.

If $d \equiv 1 \pmod 4$ then $A = \left\{ \dfrac{a + b\sqrt{d}}{2} \,\middle|\, a, b \in \mathbf{Z},\ a \equiv b \pmod 2 \right\}$.

If $\alpha_1, \alpha_2 \in A$ are such that every element $\alpha \in A$ is uniquely of the form $\alpha = m_1\alpha_1 + m_2\alpha_2$, with $m_1, m_2 \in \mathbf{Z}$, then $\{\alpha_1, \alpha_2\}$ is called an integral basis of A. In other words, $A = \mathbf{Z}\alpha_1 \oplus \mathbf{Z}\alpha_2$.

If $d \equiv 2$ or $3 \pmod 4$ then $\{1, \sqrt{d}\}$ is an integral basis of A.