4. For each degree $d \leq 6$, find the number of irreducible polynomials over $\mathbf{F}_2$ of degree d, and make a list of them.
5. For each degree $d \leq 6$, find the number of monic irreducible polynomials over $\mathbf{F}_3$ of degree d, and for $d \leq 3$ make a list of them.
6. Suppose that f is a power of a prime ℓ. Find a simple formula for the number of monic irreducible polynomials of degree f over $\mathbf{F}_p$.
7. Use the polynomial version of the Euclidean algorithm (see Exercise 12 of § I.2) to find $g.c.d.(f, g)$ for $f, g \in \mathbf{F}_p[X]$ in each of the following examples. In each case express the g.c.d. polynomial as a combination of f and g, i.e., in the form $d(X) = u(X)f(X) + v(X)g(X)$.
(a) $f = X^3 + X + 1$, $g = X^2 + X + 1$, $p = 2$;
(b) $f = X^6 + X^5 + X^4 + X^3 + X^2 + X + 1$, $g = X^4 + X^2 + X + 1$, $p = 2$;
(c) $f = X^3 - X + 1$, $g = X^2 + 1$, $p = 3$;
(d) $f = X^5 + X^4 + X^3 - X^2 - X + 1$, $g = X^3 + X^2 + X + 1$, $p = 3$;
(e) $f = X^5 + 88x^4 + 73X^3 + 83X^2 + 51X + 67$, $g = X^3 + 97X^2 + 40X + 38$, $p = 101$.
8. By computing $g.c.d.(f, f')$ (see Exercise 13 of § I.2), find all multiple roots of $f(X) = X^7 + X^5 + X^4 - X^3 - X^2 - X + 1 \in \mathbf{F}_3[X]$ in its splitting field.
9. Suppose that $\alpha \in \mathbf{F}_{p^2}$ satisfies the polynomial $X^2 + aX + b$, where $a, b \in \mathbf{F}_p$.
(a) Prove that α^p also satisfies this polynomial.
(b) Prove that if $\alpha \notin \mathbf{F}_p$, then $a = -\alpha - \alpha^p$ and $b = \alpha^{p+1}$.
(c) Prove that if $\alpha \notin \mathbf{F}_p$ and $c, d \in \mathbf{F}_p$, then $(c\alpha+d)^{p+1} = d^2 - acd + bc^2$ (which is $\in \mathbf{F}_p$).
(d) Let i be a square root of -1 in $\mathbf{F}_{19^2}$. Use part (c) to find $(2+3i)^{101}$ (i.e., write it in the form $a + bi$, $a, b \in \mathbf{F}_{19}$).
10. Let d be the maximum degree of two polynomials $f, g \in \mathbf{F}_p[X]$. Give an estimate in terms of d and p for the number of bit operations needed to compute $g.c.d.(f, g)$ using the Euclidean algorithm.
11. For each of the following fields $\mathbf{F}_q$, where $q = p^f$, find an irreducible polynomial with coefficients in the prime field whose root α is primitive (i.e., generates $\mathbf{F}_q^*$), and write all of the powers of α as polynomials in α of degree $< f$: (a) $\mathbf{F}_4$; (b) $\mathbf{F}_8$; (c) $\mathbf{F}_{27}$; (d) $\mathbf{F}_{25}$.
12. Let $F(X) \in \mathbf{F}_2[X]$ be a primitive irreducible polynomial of degree f. If α denotes a root of $F(X)$, this means that the powers of α exhaust all of $\mathbf{F}_{2^f}^*$. Using the big-O notation, estimate (in terms of f) the number of bit operations required to write every power of α as a polynomial in α of degree less than f.
13. (a) Under what conditions on p and f is *every* element of $\mathbf{F}_{p^f}$ besides 0, 1 a generator of $\mathbf{F}_{p^f}^*$?
(b) Under what conditions is every element $\neq 0, 1$ either a generator or the square of a generator?