8. Since $g.c.d.(f, f') = X^2+1$, the multiple roots are $\pm\alpha^2$, where α is the generator of $\mathbf{F}_9^*$ in the text.
9. (a) Raising $0 = \alpha^2 + b\alpha + c$ to the p-th power and using the fact that $b^p = b$ and $c^p = c$, we obtain $0 = (\alpha^p)^2 + b\alpha^p + c$. (b) The polynomial's two distinct roots are then α and α^p. Then a is minus the sum of the roots, and b is the product of the roots. (c) $(c\alpha + d)^{p+1} = (c\alpha^p + d)(c\alpha + d)$, and then multiply out and use part (b). (d) $(2+3i)^{5(19+1)+1} = (2^2+3^2)^5(2+3i) = 14(2+3i) = 9+4i$.
10. In each division of polynomials (first f by g, then r_j by r_{j+1}), after first finding the inverse modulo p of the leading coefficient of r_{j+1} (which takes $O(log^3p)$ bit operations), one needs to perform $O(d^2)$ multiplications in the field (i.e., of integers modulo p), each taking $O(log^2p)$ bit operations. Thus, each division takes $O(log^3p+d^2log^2p)$ bit operations, and so the entire Euclidean algorithm takes $O(d)\cdot O(log^2p(log\,p+d^2)) = O(d\,log^2p(log\,p+d^2))$ operations. (This can be simplified to $O(d\,log^3p)$ if d is constrained not to grow faster than $\sqrt{log\,p}$, and to $O(d^3log^2p)$ if p is constrained not to grow faster than e^{d^2}.)
11. (a) Let α be a root of $X^2+X+1=0$; then the three successive powers of α are α, $\alpha+1$, and 1. (b) Let α be a root of $X^3+X+1=0$; then the seven successive powers of α are α, α^2, $\alpha+1$, $\alpha^2+\alpha$, $\alpha^2+\alpha+1$, α^2+1, 1. (c) Let α be a root of $X^3-X-1=0$; then the 26 successive powers of α are α, α^2, $\alpha+1$, $\alpha^2+\alpha$, $\alpha^2+\alpha+1$, $\alpha^2-\alpha+1$, $-\alpha^2-\alpha+1$, $-\alpha^2-1$, $-\alpha+1$, $-\alpha^2+\alpha$, $\alpha^2-\alpha-1$, $-\alpha^2+1$, -1, followed by the same 13 elements with all +'s and −'s reversed. (d) Let α be a root of $X^2-X+2=0$; then the 24 successive powers of α are α, $\alpha-2$, $-\alpha-2$, $2\alpha+2$, $-\alpha+1$, 2, then the same six elements multiplied by 2, then multiplied by -1, then multiplied by -2, giving all 24 powers of α.
12. $O(f2^f)$, since for each of the $O(2^f)$ powers of α one has to multiply the previous expression by α and, if α^f occurs, add the lower degree polynomial which equals α^f to the result of increasing the lower powers of α by 1 in the previous expression; all of this takes only $O(f)$ bit operations.
13. (a) $p=2$ and 2^f-1 is a "Mersenne" prime (see Example **1** and Exercise 2 of § I.4); (b) besides the cases in part (a), also when $p=3$ and $(3^f-1)/2$ is a prime (as in part (a), this requires that f itself be prime, but that is not sufficient, as the example $f=5$ shows), and when p is of the form $2p'+1$ with p' a prime and $f=1$. It is not known, incidentally, whether there are infinitely many prime fields with any of the conditions in (a)–(b) (but it is conjectured that there are). Primes p' for which $p=2p'+1$ is also prime are called "Germain primes" after Sophie Germain, who in 1823 proved that the first case of Fermat's Last Theorem holds if the exponent is such a prime.
14. Choose a sequence n_j for which $\varphi(n_j)/n_j \longrightarrow 0$ as $j \longrightarrow \infty$ (see Exercise 23 of § I.3) with none of the n_j divisible by p, and let f_j be