$\mathbf{F}_2 = \{0, 1\}$. A polynomial in $\mathbf{F}_2[X]$ is simply a sum of powers of X. In some ways, polynomials over $\mathbf{F}_p$ are like integers expanded to the base p, where the digits are analogous to the coefficients of the polynomial. For example, in its binary expansion an integer is written as a sum of powers of 2 (with coefficients 0 or 1), just as a polynomial over $\mathbf{F}_2$ is a sum of powers of X. But the comparison is often misleading. For example, the sum of any number of polynomials of degree d is a polynomial of degree (at most) d; whereas a sum of several d-bit integers will be an integer having more than d binary digits.

Example 3. Let $f(X) = X^4 + X^3 + X^2 + 1$, $g = X^3 + 1 \in \mathbf{F}_2[X]$. Find $g.c.d.(f, g)$ using the Euclidean algorithm for polynomials, and express the g.c.d. in the form $u(X)f(X) + v(X)g(X)$.

Solution. Polynomial division gives us the sequence of equalities below, which lead to the conclusion that $g.c.d.(f, g) = X+1$, and the next sequence of equalities enables us, working backwards, to express $X + 1$ as a linear combination of f and g. (Note, by the way, that in a field of characteristic 2 adding is the same as subtracting, i.e., $a - b = a + b - 2b = a + b$.) We have:

$$\begin{aligned} f &= (X+1)g + (X^2+X) \\ g &= (X+1)(X^2+X) + (X+1) \\ X^2+X &= X(X+1) \end{aligned}$$

and then

$$\begin{aligned} X+1 &= g + (X+1)(X^2+X) \\ &= g + (X+1)(f + (X+1)g) \\ &= (X+1)f + (X^2)g. \end{aligned}$$

Exercises

1. For $p = 2, 3, 5, 7, 11, 13$ and 17, find the smallest positive integer which generates $\mathbf{F}_p^*$, and determine how many of the integers $1, 2, 3, \ldots, p-1$ are generators.
2. Let $(\mathbf{Z}/p^\alpha\mathbf{Z})^*$ denote all residues modulo p^α which are *invertible*, i.e., are not divisible by p. **Warning:** Be sure not to confuse $\mathbf{Z}/p^\alpha\mathbf{Z}$ (which has $p^\alpha - p^{\alpha-1}$ invertible elements) with $\mathbf{F}_{p^\alpha}$ (in which all elements except 0 are invertible). The two are the same only when $\alpha = 1$.
(a) Let g be an integer which generates $\mathbf{F}_p^*$, where $p > 2$. Let α be any integer greater than 1. Prove that either g or $(p+1)g$ generates $(\mathbf{Z}/p^\alpha\mathbf{Z})^*$. Thus, the latter is also a *cyclic group*.
(b) Prove that if $\alpha > 2$, then $(\mathbf{Z}/2^\alpha\mathbf{Z})^*$ is *not* cyclic, but that the number 5 generates a *subgroup* consisting of half of its elements, namely those which are $\equiv 1$ *mod* 4.
3. How many elements are in the smallest field extension of $\mathbf{F}_5$ which contains all of the roots of the polynomials X^2+X+1 and X^3+X+1?