(b) Using the matrix definition of f_n, prove that

$$f_n = \frac{\alpha^n - \alpha'^n}{\sqrt{5}}, \qquad \text{where} \qquad \alpha = \frac{1+\sqrt{5}}{2}, \qquad \alpha' = \frac{1-\sqrt{5}}{2}.$$

(c) Using parts (a) and (b), find an upper bound for k in terms of a. Compare with the estimate that follows from the proof of Proposition I.2.1.

11. The purpose of this problem is to find a general estimate for the time required to compute $g.c.d.(a,b)$ (where $a > b$) that is better than the estimate in Proposition I.2.1.
(a) Show that the number of bit operations required to perform a divison $a = qb + r$ is $O\big((\log b)(1 + \log q)\big)$.
(b) Applying part (a) to all of the $O(\log a)$ divisions of the form $r_{i-1} = q_{i+1}r_i + r_{i+1}$, derive the time estimate $O\big((\log b)(\log a)\big)$.

12. Consider polynomials with real coefficients. (This problem will apply as well to polynomials with coefficients in any *field*.) If f and g are two polynomials, we say that $f|g$ if there is a polynomial h such that $g = fh$. We define $g.c.d.(f,g)$ in essentially the same way as for integers, namely, as a polynomial of greatest degree which divides both f and g. The polynomial $g.c.d.(f,g)$ defined in this way is not unique, since we can get another polynomial of the same degree by multiplying by any nonzero constant. However, we can make it unique by requiring that the g.c.d. polynomial be *monic*, i.e., have leading coefficient 1. We say that f and g are relatively prime polynomials if their g.c.d. is the "constant polynomial" 1. Devise a procedure for finding g.c.d.'s of polynomials – namely, a Euclidean algorithm for polynomials — which is completely analogous to the Euclidean algorithm for integers, and use it to find (a) $g.c.d.(x^4 + x^2 + 1,\ x^2 + 1)$, and (b) $g.c.d.(x^4 - 4x^3 + 6x^2 - 4x + 1,\ x^3 - x^2 + x - 1)$. In each case find polynomials $u(x)$ and $v(x)$ such that the g.c.d. is expressed as $u(x)f(x) + v(x)g(x)$.

13. From algebra we know that a polynomial has a multiple root if and only if it has a common factor with its derivative; in that case the multiple roots of $f(x)$ are the roots of $g.c.d.(f,\ f')$. Find the multiple roots of the polynomial $x^4 - 2x^3 - x^2 + 2x + 1$.

14. (Before doing this exercise, recall how to do arithmetic with complex numbers. Remember that, since $(a+bi)(a-bi)$ is the real number a^2+b^2, one can divide by writing $(c+di)/(a+bi) = (c+di)(a-bi)/(a^2+b^2)$.) The *Gaussian integers* are the complex numbers whose real and imaginary parts are integers. In the complex plane they are the vertices of the squares that make up the grid. If α and β are two Gaussian integers, we say that $\alpha|\beta$ if there is a Guassian integer γ such that $\beta = \alpha\gamma$. We define $g.c.d.(\alpha,\beta)$ to be a Gaussian integer δ of maximum absolute value which divides both α and β (recall that the absolute value $|\delta|$ is its distance from 0, i.e., the square root of the sum of the squares of its real and imaginary parts). The g.c.d. is not unique, because we