§ VI.4.

1. $g.c.d.(2^k - 1, n) = n$, but $g.c.d.(3^k - 1, n) = 127$; $n = 127 \cdot 421$.
2. The probability that a random residue a in $(\mathbf{Z}/p\mathbf{Z})^*$ satisfies $p|a^k - 1$ is one out of $(p-1)/g.c.d.(k, p-1)$. Since there is little chance that $a^k - 1$ will be divisible by any other divisor of n, this is also an estimate of the probability that $g.c.d.(a^k - 1, n) = p$.
3. (a) 3 out of 41; (b) 22 out of 41; (c) 25 out of 127; (d) 68 out of 127; (e) 105 out of 399.
4. Choose $k = 2^6 \cdot 3^4 \cdot 5^2$. Here are the first value of a for which the method gives a factor, the factor it gives, and the value of k_1 for which the algorithm terminates: (a) 1, 37, 2^3; (b) 2, 71, $2^6 \cdot 3^4 \cdot 5$; (c) 1, 67, $2^6 \cdot 3^4 \cdot 5$; (d) 1, 47, $2^6 \cdot 3$; (e) 2, 79, $2^6 \cdot 3^4 \cdot 5^2$; (f) 1, 73, $2^6 \cdot 3$; (g) 5, 53, 2^2; (h) 4, 59, $2^6 \cdot 3^2$; (i) 1, 47, $2^6 \cdot 3$; (j) 3, 97, $2^6 \cdot 3$; (k) 1, 61, $2^6 \cdot 3^4 \cdot 5^2$.
5. If the latter possibility occurred, it would mean that $\ell'(k_1/\ell)P \bmod p = O \bmod p$ for some $\ell' < \ell$, while $(k_1/\ell)P \bmod p \neq O \bmod p$. But ℓ' is a product of primes $\ell^* < \ell$, and our choice of exponents in (2) ensured that for each such ℓ^* the highest power of ℓ^* that could divide the order of $P \bmod p$ in $E \bmod p$ already occurred in $(\ell^*)^{\alpha_{\ell^*}}$, i.e., in k_1/ℓ.
6. (a) If n happens to be divisible only by primes which are $\equiv 3 \bmod 4$, then there are always $p+1$ points on $E \bmod p$ for $p|n$ (see Exercise 7(a) of §1 for the case $a = -1$; but the same argument applies for any a). In that case it won't help to vary a if $p+1$ is divisible by a large prime for each $p|n$. (b) If n happens to be divisible only by primes $p \equiv 2 \bmod 3$, then there are always $p+1$ points (see Exercise 7(b) of §1), and so again it won't help to vary b if $p+1$ is divisible by a large prime for each $p|n$.
7. Generate pairs (E, P) where E has equation $y^2 = x(x-a)(x-b)$; then E has four points of order 2, including the point at infinity (see Exercise 4(a) of §VI.1). To do this, choose random a, x, y_0; set $y = x(x-a)y_0$ and then $b = x - yy_0$.