8. $3^2 \cdot 41 \cdot 271$, $3^3 \cdot 7 \cdot 11 \cdot 13 \cdot 37$, $3^2 \cdot 11 \cdot 73 \cdot 101 \cdot 137$.
9. $7 \cdot 23 \cdot 89 \cdot 599479$; $7^2 \cdot 127 \cdot 337$ (this example shows that a prime $p|b^d - 1$ in Proposition I.4.3 may divide $b^n - 1$ to a greater power than it divides $b^d - 1$).
10. $7 \cdot 31 \cdot 151$, $3^2 \cdot 7 \cdot 11 \cdot 31 \cdot 151 \cdot 331$, $3^2 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13 \cdot 31 \cdot 41 \cdot 61 \cdot 151 \cdot 331 \cdot 1321$.
11. (a) Apply side by side the Euclidean algorithm to find $g.c.d.(a^m - 1, a^n - 1)$ and to find $g.c.d.(m, n)$. Notice that at each stage the remainder in the first Euclidean algorithm is $a^r - 1$, where r is the remainder in the second Euclidean algorithm. For example, in the first step one divides $a^m - 1$ by $a^n - 1$ to get $a^r - 1$, where r is the remainder when m is divided by n. (b) By part (a) and the Chinese Remainder Theorem, no two numbers between 0 and $\prod(2^{m_i} - 1)$ have the same set of remainders. This product is greater than $2^{r\ell/2} > 2^{2k} > ab$. For the time estimate, one has r multiplications of at most ℓ-bit integers, which take $O(r\ell^2) = O(k\ell)$ bit operations. This is better by a factor of r than the usual multiplication of a and b (which takes time $O(k^2)$).

§ II.1.

1.

prime p	2	3	5	7	11	13	17
smallest generator	1	2	2	3	2	2	3
number of generators	1	1	2	2	4	4	8

2. (a) If $g^{p-1} \equiv 1 \bmod p^2$, then replace g by $(p+1)g$ and show that then one has $g^{p-1} = 1 + g_1 p$ with g_1 prime to p. Now if $g^j \equiv 1 \bmod p^\alpha$, first show that $p-1|j$, i.e., $j = (p-1)j_1$, and so $(1+g_1p)^{j_1} \equiv 1 \bmod p^\alpha$. But show that $(1+g_1p)^{j_1} = 1 + j_1 g_1 p + higher\ powers\ of\ p$, and that then $p^{\alpha-1}$ must divide j_1. (b) For the first part, see Exercise 20 of § I.3; the proof of the second part (which reduces to showing that 5^j cannot be $\equiv 1 \bmod 2^\alpha$ unless $2^{\alpha-2}|j$) is similar to part (a).
3. 5^6.
4. 2 for $d=1$: X, $X+1$; 1 for $d=2$: X^2+X+1; 2 for $d=3$: X^3+X^2+1, X^3+X+1; 3 for $d=4$: X^4+X^3+1, X^4+X+1, $X^4+X^3+X^2+X+1$; 6 for $d=5$: X^5+X^3+1, X^5+X^2+1, $X^5+X^4+X^3+X^2+1$, $X^5+X^4+X^3+X+1$, $X^5+X^4+X^2+X+1$, $X^5+X^3+X^2+X+1$; 9 for $d=6$: X^6+X^5+1, X^6+X^3+1, X^6+X+1, $X^6+X^5+X^4+X^2+1$, $X^6+X^5+X^4+X+1$, $X^6+X^5+X^3+X^2+1$, $X^6+X^5+X^2+X+1$, $X^6+X^4+X^3+X+1$, $X^6+X^4+X^2+X+1$.
5. 3 for $d=1$: X, $X \pm 1$; 3 for $d=2$: X^2+1, $X^2 \pm X - 1$; 8 for $d=3$: $X^3+X^2 \pm (X-1)$, $X^3 - X^2 \pm (X+1)$, $X^3 \pm (X^2-1)$, $X^3 - X \pm 1$; 18 for $d=4$; 48 for $d=5$; 116 for $d=6$.
6. $(p^f - p^{f/\ell})/f$.
7. (a) $g.c.d. = 1 = X^2 g + (X+1)f$; (b) $g.c.d. = X^3+X^2+1 = f + (X^2+X)g$; (c) $g.c.d. = 1 = (X-1)f - (X^2-X+1)g$; (d) $g.c.d. = X+1 = (X-1)f - (X^3-X^2+1)g$; (e) $g.c.d. = X+78 = (50X+20)f + (51X^3+26X^2+27X+4)g$.