19. n cannot be a prime, since if it were $\varphi(n) = n - 1$. By assumption, n is not the square of a prime. If it were not a product of two distinct primes, then it would be a product of three or more primes (not necessarily distinct). Let p be the smallest. Then $p \le n^{1/3}$, and we have $\varphi(n) \le n(1 - \frac{1}{p}) \le n(1 - n^{-1/3}) = n - n^{2/3}$, a contradiction.
20. Show that the square of any odd number is $\equiv 1 \; mod \; 8$, and then use induction just as in the first paragraph of the proof of Proposition I.3.5.
21. (a) Notice that 360 is a multiple of $\varphi(p^\alpha)$ for each $p^\alpha || m$. By the remark just before Example 3 in the text, this means that $6647^{362} \equiv 6647^2 \equiv 44182609 \; mod \; m$. (Here we're also using the fact that $g.c.d.(6647, m) = 1$, which follows because $6647 = 17^2 \cdot 23$.) (b) Raise a to the 359th power modulo m by the repeated squaring method. Since $m = (101100111)_2$, we find that there are 8 squarings plus 5 multiplications (of at most 63-bit integers), in each case combined with a division (at worst of a 126-bit integer by a 63-bit integer). Thus, the number of bit operations is at most $13 \times 63 \times 63 + 13 \times 64 \times 63 = 104013$.
22. (a) Show that, if $x = j \cdot \frac{n}{d}$, then x generates S_d if and only if $g.c.d.(x, d) = 1$. Notice that j runs through $0, 1, \ldots, d-1$. (b) Partition the set $\mathbf{Z}/n\mathbf{Z}$ into subsets according to which S_d an element generates. The subset corresponding to a given S_d has $\varphi(d)$ elements, according to part (a).
23. (a) Expand each term in the product in a geometric series: $(1 + \frac{1}{p} + \frac{1}{p^2} + \frac{1}{p^3} + \cdots)$. In expanding all the parentheses, the denominators will be all possible expressions of the form $p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$. According to the Fundamental Theorem, every positive integer n occurs exactly once as such an expression. Hence, the product is equal to the harmonic series $\sum_{n=1}^{\infty} \frac{1}{n}$, which we know diverges. (b) First prove that for $x \le \frac{1}{2}$ we have $x > -\frac{1}{2} log(1 - x)$ (look at the graph of log). Apply this when $x = \frac{1}{p}$, and compare $\sum \frac{1}{p}$ with the log of the product in part (a). (c) For any sequence of prime numbers n approaching infinity we have $\frac{\varphi(n)}{n} = 1 - \frac{1}{n} \longrightarrow 1$; for any sequence of n's which are divisible by increasingly many of the successive primes (for example, take $n_j = j!$), we have $\frac{\varphi(n)}{n} = \prod_{p|n}(1 - \frac{1}{p}) \longrightarrow \prod_{\text{all } p}(1 - \frac{1}{p}) = 0$ by part (a).
24. (a) Give p_i and the residue of N modulo p_i to the i-th lieutenant general, and use the Chinese Remainder Theorem. (b) Choose each $p_i > \sqrt[k]{N}$ but much smaller than $\sqrt[k-1]{N}$.

§ **I.4.**

3. Use the same argument as in the proof of the last proposition to conclude that $b^d \equiv \pm 1 \; mod \; m$. But since $(b^d)^{a/d} \equiv -1 \; mod \; m$, it follows that $b^d \equiv -1 \; mod \; m$ and a/d is odd.
4. Use Exercise 3 with $a = n$ and $c = (p-1)/2$.
5. (a) $2^8 + 1 = 257$; (b) use Exercise 4; (c) $m = 97 \cdot 257 \cdot 673$.
6. $2 \cdot 11^2 \cdot 13 \cdot 4561$, $2^5 \cdot 5 \cdot 7 \cdot 13 \cdot 41 \cdot 73 \cdot 6481$.
7. $2^4 \cdot 3^2 \cdot 7 \cdot 13 \cdot 31 \cdot 601$.