15. In exact integer arithmetic (rather than modular arithmetic) does the repeated squaring method save time? Explain, using big-O estimates.
16. Notice that for a prime to p, a^{p-2} is an inverse of a modulo p. Suppose that p is very large. Compare using the repeated squaring method to find a^{p-2} with the Euclidean algorithm as an efficient means to find a^{-1} *mod* p when (a) a has almost as many digits as p, and (b) when a is much smaller than p.
17. Find $\varphi(n)$ for all m from 90 to 100.
18. Make a list showing all n for which $\varphi(n) \leq 12$, and prove that your list is complete.
19. Suppose that n is not a perfect square, and that $n-1 > \varphi(n) > n-n^{2/3}$. Prove that n is a product of two distinct primes.
20. If $m \geq 8$ is a power of 2, show that the exponent in Proposition I.3.5 can be replaced by $\varphi(m)/2$.
21. Let $m = 7785562197230017200 = 2^4 \cdot 3^3 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13 \cdot 19 \cdot 31 \cdot 37 \cdot 41 \cdot 61 \cdot 73 \cdot 181$.

    (a) Find the least nonnegative residue of 6647^{362} *mod* m.

    (b) Let a be a positive integer less than m which is prime to m. First, find a positive power of a less than 500 which is certain to give a^{-1} *mod* m. Next, describe an algorithm for finding this power of a working modulo m. How many multiplications and divisions are needed to carry out this algorithm? (Reducing a number modulo m counts as one division.) What is the maximum number of bits you could encounter in the integers that you work with? Finally, give a good estimate of the number of bit operations needed to find a^{-1} *mod* m by this method. (Your answer should be a specific number — do not use the big-O notation here.)
22. Give another proof of Proposition I.3.7 as follows. For each divisor d of n, let S_d denote the subset (actually a so-called "subgroup") of $\mathbf{Z}/n\mathbf{Z}$ consisting of all multiples of n/d. Thus, S_d has d elements.

    (a) Prove that S_d has $\varphi(d)$ different elements x which *generate* S_d, meaning that the multiples of x (considered modulo n) give all elements of S_d.

    (b) Prove that every element of x generates one of the S_d, and hence that the number of elements in $\mathbf{Z}/n\mathbf{Z}$ is equal to the sum (taken over divisors d) of the number of elements that generate S_d. In light of part (a), this gives Proposition I.3.7.
23. (a) Using the Fundamental Theorem of Arithmetic, prove that

$$\prod_{\text{all primes } p} \frac{1}{1-\frac{1}{p}}$$

    diverges to infinity.

    (b) Using part (a), prove that the sum of the reciprocals of the primes diverges.