How many bit operations does this take? In each step you have either 1 or 2 multiplications of numbers which are less than m^2. And there are $k-1$ steps. Since each step takes $O(log^2(m^2))= O(log^2 m)$ bit operations, we end up with the following estimate:

Proposition I.3.6. Time(b^n *mod* m) $= O((log\, n)(log^2 m))$.

Remark. If n is very large in Proposition I.3.6, you might want to use the corollary of Proposition I.3.5, replacing n by its least nonnegative residue modulo $\varphi(m)$. But this requires that you know $\varphi(m)$. If you do know $\varphi(m)$, and if $g.c.d.(b,m)=1$, so that you can replace n by its least nonnegative residue modulo $\varphi(m)$, then the estimate on the right in Proposition I.3.6 can be replaced by $O(log^3 m)$.

As a final application of the multiplicativity of the Euler φ-function, we prove a formula that will be used at the beginning of Chapter II.

Proposition I.3.7. $\sum_{d|n}\varphi(d)=n$.

Proof. Let $f(n)$ denote the left side of the equality in the proposition, i.e., $f(n)$ is the sum of $\varphi(d)$ taken over all divisors d of n (including 1 and n). We must show that $f(n)=n$. We first claim that $f(n)$ is multiplicative, i.e., that $f(mn)=f(m)f(n)$ whenever $g.c.d.(m,n)=1$. To see this, we note that any divisor $d|mn$ can be written (in one and only one way) in the form $d_1\cdot d_2$, where $d_1|m$, $d_2|n$. Since $g.c.d.(d_1,d_2)=1$, we have $\varphi(d)=\varphi(d_1)\varphi(d_2)$, because of the multiplicativity of φ. We get all possible divisors d of mn by taking all possible pairs d_1, d_2 where d_1 is a divisor of m and d_2 is a divisor of n. Thus, $f(mn)=\sum_{d_1|m}\sum_{d_2|n}\varphi(d_1)\varphi(d_2)=\left(\sum_{d_1|m}\varphi(d_1)\right)\left(\sum_{d_2|n}\varphi(d_2)\right)=f(m)f(n)$, as claimed. Now to prove the proposition suppose that $n=p_1^{\alpha_1}\cdots p_r^{\alpha_r}$ is the prime factorization of n. By the multiplicativity of f, we find that $f(n)$ is a product of terms of the form $f(p^\alpha)$. So it suffices to prove the proposition for p^α, i.e., to prove that $f(p^\alpha)=p^\alpha$. But the divisors of p^α are p^j for $0\le j\le\alpha$, and so $f(p^\alpha)=\sum_{j=0}^{\alpha}\varphi(p^j)=1+\sum_{j=1}^{\alpha}(p^j-p^{j-1})=p^\alpha$. This proves the proposition for p^α, and hence for all n.

Exercises

1. Describe all of the solutions of the following congruences:

(a) $3x\equiv 4$ *mod* 7;	(d) $27x\equiv 25$ *mod* 256;
(b) $3x\equiv 4$ *mod* 12;	(e) $27x\equiv 72$ *mod* 900;
(c) $9x\equiv 12$ *mod* 21;	(f) $103x\equiv 612$ *mod* 676.

2. What are the possibilities for the last hexadecimal digit of a perfect square? (See Exercise 7 of § I.1.)
3. What are the possibilities for the last base-12 digit of a product of two consecutive positive odd numbers?