suppose that n is not a prime power. First, if $p|n$ with $p \equiv 3 \, mod \, 4$, then no integer raised to an even power gives $-1 \, mod \, n$ (since -1 is not a quadratic residue modulo p); hence, in this case the strong pseudoprime condition can be stated: $b^t \equiv \pm 1 \, mod \, n$. This condition obviously has the multiplicative property. Next, suppose that $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ where $p_j \equiv 1 \, mod \, 4$ for $1 \le j \le r$. Let $\pm a_j$ be the two square roots of -1 modulo $p_j^{\alpha_j}$ (a square root modulo p_j can be lifted to a square root modulo $p_j^{\alpha_j}$; see Exercise 20 of § II.2). Then any b which satisfies $b \equiv \pm a_j \, mod \, p_j^{\alpha_j}$ (for any choice of the $\pm$) is a base to which n is a strong pseudoprime, since then $b^{2t} \equiv (-1)^t \equiv -1 \, mod \, n$. Choose b_1 by taking all of the $\pm a_j$ equal to a_j, and choose b_2 by taking any of the $2^r - 2$ possible choices of sign other than all positive or all negative. Then show that for $b = b_1 b_2$ one has $b^{2t} \equiv 1 \, mod \, n$ and $b^t \equiv b \not\equiv \pm 1 \, mod \, n$.

24. (a) In that case you obtain a number c other than ± 1 whose square is 1; then $g.c.d.(c+1, n)$ is a nontrivial factor of n. (b) Choose p and q so that $p-1$ and $q-1$ do not have a large common divisor (see Exercise 5 above).

§ V.2.

1. $g.c.d.(x_5 - x_3, n) = g.c.d.(21 - 63, 91) = 7$; $91 = 7 \cdot 13$.
2. $g.c.d.(x_6 - x_3, n) = g.c.d.(2839 - 26, 8051) = 97$; $8051 = 83 \cdot 97$.
3. $g.c.d.(x_9 - x_7, n) = g.c.d.(869 - 3397, 7031) = 79$; $7031 = 79 \cdot 89$.
4. $g.c.d.(x_6 - x_3, n) = g.c.d.(630 - 112, 2701) = 37$; $2701 = 37 \cdot 73$.
5. (a) Prove by induction on k that for $1 \le k \le r$ there is a $1/r$ probability that $x_0, \ldots, x_{k-1}$ are distinct and x_k is equal to one of the earlier x_j. For $k = 1$ there is a $1/r$ probability that $f(x_0) = x_0$. The induction step is as follows. By the induction assumption, the probability that none of the earlier k's was the first for which $x_k = x_j$ for some $j < k$ is $1 - \frac{k-1}{r} = \frac{r-(k-1)}{r}$. Assuming this to be the case, there are $r - (k-1)$ possible values for $f(x_{k-1})$, since a bijection cannot take x_{k-1} to any of the $k-1$ values $f(x_j)$, $0 \le j \le k-2$. Of the $r - (k-1)$ possible values, one is x_0, and all the others are distinct from $x_0, x_1, \ldots, x_{k-1}$. Thus, there is a $1/(r - (k-1))$ chance that the value is one of the earlier x_j (namely, if this is the case, note that $j = 0$). The probability that *both* things happen — none of the earlier k's was the first for which $x_k = x_0$ but our present k has $x_k = x_0$ — is the product of the individual probabilities, i.e., $\frac{r-(k-1)}{r} \cdot \frac{1}{r-(k-1)} = \frac{1}{r}$. (b) Since all of the values from 1 to r are equally probable, the average is $\frac{1}{r}\sum_{k=1}^{r} k = \frac{1}{r}(r(r+1)/2) = (r+1)/2$.
6. Suppose that a has no common factor with n (otherwise, we would immediately find a factor of n by computing $g.c.d.(a, n)$ and we would have no need of the rho method at all). Then $f(x) = ax+b$ is a bijection of $\mathbf{Z}/r\mathbf{Z}$ to itself (for any $r|n$), and so the expected number of steps