before we get a repetition modulo r is of the order of $r/2$ (by Exercise 5(b)) rather than $\sqrt{r}$, i.e., it is much worse.

7. (a) $2^k \equiv 2^\ell \ mod\ r-1$; (b) $\ell = s$ and $k = s+m$, where m is the *order* of 2 modulo t, i.e., the smallest positive integer such that $2^m \equiv 1 \ mod\ t$. m is also the *period* of the repeating binary expansion of $1/t$, as we see by writing $2^m - 1 = ut$ and then $1/t = u\sum_{i=1}^{\infty} 2^{-mi}$. (c) k can easily have order almost as large as r, e.g., if $r-1$ is twice a prime and 2 happens to be a generator modulo that prime (in which case $s = 1$, $m = (r-3)/2$).

§ **V.3.**

1. (a) (using $t = \lceil\sqrt{n}\rceil + 1 = 93$) $89 \cdot 97$; (b) (using $t = \lceil\sqrt{n}\rceil + 4 = 903$) $823 \cdot 983$; (c) (using $t = \lceil\sqrt{n}\rceil + 6 = 9613$) $9277 \cdot 9949$; (d) (using $t = \lceil\sqrt{n}\rceil + 1 = 9390$) $9343 \cdot 9437$; (e) (using $t = \lceil\sqrt{n}\rceil + 8 = 75$) $43 \cdot 107$.
2. In the factorization $n = ab$ with $a > b$, if $a < \sqrt{n} + \sqrt[4]{n}$, then $b = n/a > n/(\sqrt{n} + \sqrt[4]{n}) > \sqrt{n} - \sqrt[4]{n}$. On the other hand, if we start with $b > \sqrt{n} - \sqrt[4]{n}$, then we must have $a < \sqrt{n} + \sqrt[4]{n} + 2$, because otherwise we would have $n = ab > (\sqrt{n} + \sqrt[4]{n} + 2)(\sqrt{n} - \sqrt[4]{n}) = n + \sqrt{n} - 2\sqrt[4]{n} > n$ (as soon as $n > 15$; we check Exercise 2 separately for the first few n). Thus, in either case $a - b < 2(\sqrt[4]{n} + 1)$. But if Fermat factorization fails to work for the first value of t, then the s and t corresponding to the factorization $n = ab$ satisfy: $t > \sqrt{n} + 1$, and so $s = \sqrt{t^2 - n} > \sqrt{(\sqrt{n}+1)^2 - n} = \sqrt{2\sqrt{n}+1} > \sqrt{2}\sqrt[4]{n}$, which contradicts the relationship $s = (a-b)/2 < \sqrt[4]{n}+1$ as soon as $n > 33$.
3. (a) We would have $t^2 - s^2 = kn \equiv 2 \ mod\ 4$; but modulo 4 the difference of two squares cannot be 2. (b) We would have $t^2 - s^2 = 4n \equiv 4 \ mod\ 8$, which can hold only if both s and t are even; but then $(t/2)^2 - n = (s/2)^2$, and so simple Fermat factorization would have worked equally well.
4. (a) (using $t = \lceil\sqrt{3n}\rceil + 1 = 455$) $149 \cdot 463$; (b) (using $t = \lceil\sqrt{3n}\rceil + 2 = 9472$) $3217 \cdot 9293$; (c) (using $t = \lceil\sqrt{5n}\rceil + 1 = 9894$) $1973 \cdot 9923$; (d) (using $t = \lceil\sqrt{5n}\rceil + 2 = 9226$) $1877 \cdot 9067$.
5. $B = \{2, 3\}$; the vectors are $\{0, 1\}$ and $\{0, 1\}$; $b = 52 \cdot 53 \ mod\ n = 55$, $c = 2 \cdot 3^2 = 18$; $g.c.d.(55 + 18, 2701) = 73$; $2701 = 37 \cdot 73$.
6. $B = \{-1, 2, 3, 61\}$; the vectors are $\{1, 0, 0, 0\}$, $\{1, 0, 0, 1\}$, and $\{0, 0, 0, 1\}$; $b = 68 \cdot 152 \cdot 153 \ mod\ n = 1555$, $c = 2 \cdot 3 \cdot 61 = 366$; $g.c.d.(1555 + 366, 4633) = 113$; $4633 = 41 \cdot 113$.
7. (a) Estimate the difference by taking the sum of the "triangular regions" between the graph of $\log x$ and the Riemann sum rectangles. (b) Compare $\int_1^n \log x\, dx$ with the sum of the areas of the trapezoids whose tops join the points $(j, \log j)$, and show that the total area between the curve and the trapezoids is bounded by a constant. (c) $lim_{y\longrightarrow\infty}(\frac{1}{y}\log y! - (\log y - 1)) = 0$, so $\log y - 1$ is the answer.
8. (a) $(1 - 2^{-n})(1 - 2^{-n+1}) \cdots (1 - 2^{-n+k-1})$; (b) 0.298.