13. last decimal digit being 1 or 9.
14. Any power of a residue is a residue, so none of the nonresidues can occur as a power, and that means a residue cannot be a generator.
15. (a) Since $p-1$ is a power of 2, the order of any element g is a power of 2. If $-1 = (\frac{g}{p}) \equiv g^{(p-1)/2}$ *mod* p, then this order cannot be less than $p-1$. (b) If $k > 1$ and $p = 2^{2^k}+1$, then $p \equiv 2$ *mod* 5 (since the exponent of 2 is a multiple of 4). Then $(\frac{5}{p}) = (\frac{p}{5}) = -1$. (c) Similar to part (b): since the exponent of 2 is not divisible by 3, it follows that the power of 2 is $\equiv 2$ or 4 modulo 7; hence $p \equiv 3$ or 5 *mod* 7, and $(\frac{7}{p}) = (\frac{p}{7}) = -1$.
16. (a) We have $(a+bi)^{p+1} = (a^p + b^p i^p)(a+bi) = (a-bi)(a+bi) = a^2+b^2$. **Claim:** If $(a+bi)^m \in \mathbf{F}_p$, then $p+1|m$. To prove the claim, let $d = g.c.d.(m, p+1)$. Using the same argument as in the proof of Proposition I.4.2, we see that $(a+bi)^d \in \mathbf{F}_p$. But since $p+1$ is a power of 2, if $d < p+1$ we find that $(a+bi)^{(p+1)/2}$ is an element of $\mathbf{F}_p$ whose square is a^2+b^2. But a^2+b^2 is not a residue (by Exercise 14). Hence, $d = p+1$ and $p+1|m$. Now that the claim has been proved, suppose that $n = n'(p+1)$ is such that $(a+bi)^n = 1$ (note that $p+1|n$ by the claim). Then $(a^2+b^2)^{n'} = 1$, and so $p-1|n'$ because a^2+b^2 is a generator of $\mathbf{F}_p^*$. (b) Show that 17 and 13 are generators of $\mathbf{F}_{31}^*$.
17. In both cases you get $O(log^3 p)$. But note that Proposition II.2.2 applies only for $(\frac{a}{n})$ when $n = p$ is prime, whereas the method in part (a) applies generally for any positive odd n. Also notice that the time for part (a) can be reduced to $O(log^2 p)$ by the method used in Exercise 11 of §I.2.
18. (a) Solve by completing the square; show that the number of solutions is the same as for the equation $x^2 \equiv D$ *mod* p. There is 1 solution if $D = 0$, none if D is a nonresidue, and 2 if D is a residue. (b) 0, 0, 2, 1, 2; (c) 2, 2, 1, 0, 0.
19. $n = 3$; $p - 1 = 2^5 \cdot 65$; $r \equiv a^{33} \equiv 203$ *mod* p (we compute 302^{33} by the repeated squaring method, successively squaring 5 times and multiplying the result by 302); also by the repeated squaring method we compute $b \equiv n^{65} \equiv 888$ *mod* p; one takes $j = 2^2$, i.e., $\sqrt{302}$ *mod* $p \equiv b^4 r \equiv 1292$ *mod* p.
20. (a) Use induction on α. To go from $\alpha - 1$ to α, suppose you have an $(\alpha-1)$-digit base-p integer $\tilde{x}$ such that $\tilde{x}^2 \equiv a \; mod\, p^{\alpha-1}$. To determine the last digit $x_{\alpha-1} \in \{0, 1, \ldots, p-1\}$ of $x = \tilde{x} + x_{\alpha-1}p^{\alpha-1}$; write $\tilde{x}^2 = a + bp^{\alpha-1}$ for some integer b, and then work modulo p^α as follows: $x^2 = (\tilde{x} + x_{\alpha-1}p^{\alpha-1})^2 \equiv \tilde{x}^2 + 2x_0 x_{\alpha-1}p^{\alpha-1} = a + p^{\alpha-1}(b + 2x_0 x_{\alpha-1})$. So it suffices to choose $x_{\alpha-1} \equiv -(2x_0)^{-1}b$ *mod* p (note that $2x_0$ is invertible because p is odd, and $a \equiv x_0^2$ *mod* p is prime to p). (b) Use the Chinese remainder theorem to find an x which is congruent modulo each p^α to the square root found in part (a).
21. (a) If $(*)$ were true for b_1 and for $b_1 b_2$, then dividing the two congru-