is invertible modulo 10. Working with the first two columns modulo 3 gives A^{-1} *mod* $3 = \begin{pmatrix} 10 & 17 \\ 0 & 11 \end{pmatrix} \cdot \begin{pmatrix} 10 & 11 \\ 20 & 27 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 2 \\ 0 & 2 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 \\ 2 & 0 \end{pmatrix}^{-1}$ $= \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$. Similarly, working with the last two columns modulo 10 gives $A^{-1} \equiv \begin{pmatrix} 4 & 9 \\ 5 & 8 \end{pmatrix}$. By the Chinese Remainder Theorem there is a unique matrix A^{-1} modulo 30 that satisfies these two congruences: $A^{-1} = \begin{pmatrix} 4 & 9 \\ 25 & 28 \end{pmatrix}$. The plaintext is "GIVE THE PLANS TO KARLA."

15. Here the ciphertext is $\begin{pmatrix} 10 & 22 & 26 & 0 & 10 & 1 & 5 & 17 \\ 21 & 27 & 19 & 28 & 9 & 27 & 21 & 26 \end{pmatrix}$ and the first three columns of plaintext are $\begin{pmatrix} 2 & 8 & 0 \\ 29 & 29 & 29 \end{pmatrix}$. In attempting to use $A^{-1} = PC^{-1}$; note that the matrix formed from the first two digraphs of C has determinant whose *g.c.d.* with 30 is 6. Using the 1st and 3rd digraphs improves the situation: $det\begin{pmatrix} 10 & 26 \\ 21 & 19 \end{pmatrix} = 4$, and $g.c.d.(4, 30) = 2$. Use this matrix for C and work modulo 15 to find that $A^{-1} = \begin{pmatrix} 2 & 2 \\ 8 & 4 \end{pmatrix} + 15A_1$, where $A_1 \in M_2(\mathbf{Z}/2\mathbf{Z})$. Use the fact that $A^{-1}\begin{pmatrix} 10 & 22 & 26 \\ 21 & 27 & 19 \end{pmatrix} = \begin{pmatrix} 2 & 8 & 0 \\ 29 & 29 & 29 \end{pmatrix}$ and the fact that $det(A^{-1})$ is odd to show that either $A^{-1} = \begin{pmatrix} 17 & 2 \\ 8 & 19 \end{pmatrix}$ or $\begin{pmatrix} 17 & 2 \\ 23 & 19 \end{pmatrix}$. The first possibility gives the plaintext message "C.I.A. WILLLHTLA;" the second possibility gives "C.I.A. WILL HELP."
16. Use the Chinese Remainder Theorem.
17. $(p^2 - 1)(p^2 - p)$.
18. The determinant has no common factor with p^α if and only if it has no common factor with p; $\quad p^{4\alpha-3}(p^2 - 1)(p - 1)$.
19. $N^4 \prod_{p|N}(1 - \frac{1}{p})(1 - \frac{1}{p^2})$; 157248, 682080, 138240.
20. $N^{(k^2)} \prod_{p|N}\Big((1 - \frac{1}{p})(1 - \frac{1}{p^2}) \cdots (1 - \frac{1}{p^k})\Big)$.
21. $N^6 \prod_{p|N}(1 - \frac{1}{p})(1 - \frac{1}{p^2})$; 106,299,648; 573,629,280; 124,416,000.
22. (a) $(p^2 - 1)(p^2 - p)$; (b) $p^2 - p$.
23. (a) $A_0 = \begin{pmatrix} 21 & 27 \\ 18 & 27 \end{pmatrix}$; (b) $\begin{pmatrix} 1 \\ 1 \end{pmatrix}$; (c) six (this agrees with Exercise 22(b), where $p = 3$); they are: $A = \begin{pmatrix} a & 7 \\ c & 7 \end{pmatrix}$, where $\binom{a}{c} = \binom{21}{28}, \binom{21}{8}, \binom{1}{18}, \binom{1}{8}, \binom{11}{18}$, or $\binom{11}{28}$.
24. (a) $g.c.d.(det(A - I), N) = 1$, where $det(A - I) = (a - 1)(d - 1) - bc$ (apply the (a)$\Longleftrightarrow$(c) part of Proposition 3.2.1 with A replaced by $A - I = \begin{pmatrix} a-1 & b \\ c & d-1 \end{pmatrix}$). (b) Let $\mathbf{F}_N$ be the field $\mathbf{Z}/N\mathbf{Z}$. The digraphs are a 2-dimensional vector space, of which the fixed digraphs form a subspace. Any subspace that contains more than the zero-vector must either be 1-dimensional, in which case it has N elements, or else contain all digraphs, in which case $A = I$.
25. (a) $P = A'C + B'$, $A' = \begin{pmatrix} 14 & 781 \\ 821 & 206 \end{pmatrix}$, $B' = \begin{pmatrix} 322 \\ 202 \end{pmatrix}$; "HIT ARMY