(b) Prove that the map in part (a) gives a 1-to-1 correspondence between the set $M_2(\mathbf{Z}/N\mathbf{Z})^*$ of invertible matrices mod N and the set $M_2(\mathbf{Z}/m\mathbf{Z})^* \times M_2(\mathbf{Z}/n\mathbf{Z})^*$.

17. For p a prime, find the number of elements in $M_2(\mathbf{Z}/p\mathbf{Z})^*$ in two ways, and check that your answers agree:
(a) Count the number of solutions in $\mathbf{F}_p$ of the equation $ad - bc = 0$, and subtract this from the number of elements in $M_2(\mathbf{Z}/p\mathbf{Z})$.
(b) Any $A \in M_2(\mathbf{Z}/p\mathbf{Z})^*$ must take $\binom{1}{0}$ and $\binom{0}{1}$ to two linearly independent vectors, i.e., the first can be any nonzero vector, and then the second can be any vector not a multiple of the first. Count the number of possibilities.
18. Prove that a matrix in $M_2(\mathbf{Z}/p^\alpha\mathbf{Z})$ is invertible if and only if its reduction mod p in $M_2(\mathbf{Z}/p\mathbf{Z})$ is invertible. Then find the number of elements in $M_2(\mathbf{Z}/p^\alpha\mathbf{Z})^*$.
19. Using Exercises 16–18, find a formula for the number of elements in $M_2(\mathbf{Z}/N\mathbf{Z})^*$. Call this number $\varphi_2(N)$. Recall the formula for the number $\varphi(N)$ of elements in $(\mathbf{Z}/N\mathbf{Z})^*$: $\varphi(N) = N\prod_{p|n}(1 - \frac{1}{p})$. Write your formula for $\varphi_2(N)$ in a similar form. How many possible 2×2 enciphering matrices A are there when $N = 26$, 29, 30?
20. Let $\varphi_k(N)$ denote the number of invertible $k \times k$–matrices with entries in $\mathbf{Z}/N\mathbf{Z}$. *Guess* a formula for $\varphi_k(N)$. This formula is not hard to prove by the method in Exercise 16(b).

Remark. The approach in Exercises 16–20 is typical of many proofs and computations modulo N. Using a multiplicativity property, one first reduces to the case of a prime power. Then, using a "lifting argument" (see Exercise 20 of § II.2 for another example of this), one reduces to the case of a prime, i.e., we can then work in a *field* $\mathbf{F}_p$. Once we are working with a field, we can more easily use our geometric intuition, as in Exercise 17(b) above. All of linear algebra that we first learn over the real numbers goes through word–for–word over any field. For example, a congruence of the form $ax + by \equiv c \bmod p$ can be depicted by a "line" in the "plane" over the field $\mathbf{F}_p$; a second such congruence will either meet the first line in a single point, be parallel to the first line, or else coincide with the first line. In the case of congruences with a composite modulus N, on the other hand, there are other possibilities, which occur when the determinant of the coefficient matrix has a nontrivial common factor with N.

21. How many possible affine enciphering transformations are there for digraphs in an N-letter alphabet? How many are there when $N = 26$, 29, 30?
22. Suppose that you want to find a deciphering matrix $A^{-1} \in M_2(\mathbf{Z}/N\mathbf{Z})^*$ from the equation $P = A^{-1}C$, where P and C are made up from two known pairs of plaintext–ciphertext digraphs. Suppose that *g.c.d.* $(det(C), N) = p$, where p is a prime dividing N only to the first power. Let $n = N/p$.
(a) Find the number of possibilities for A^{-1} you will be left with after