

- ences would give $(*)$ for b_2 (since both sides are multiplicative). Next, suppose $(*)$ were false for some b . Then the set of b 's obtained by multiplying b by all the elements for which $(*)$ is true would consist of elements for which $(*)$ is false. (b) For example, take $b = 1 + n/p$, where $p^2|n$. Then $(\frac{b}{n}) = 1$, but $b^j \equiv 1$ only when $p|j$, which is not the case for $j = (n-1)/2$. (c) Show that $(\frac{b}{n}) = -1$ but that $b^{(n-1)/2} \equiv 1 \pmod{n/p}$ and hence one could not have $b^{(n-1)/2} \equiv -1 \pmod{n/p}$, let alone modulo n . Next, let a_1 be any nonresidue modulo p , and let $a_2 = 1$. Use the Chinese Remainder Theorem to find a solution b to: $x \equiv a_1 \pmod{p}$, $x \equiv a_2 \pmod{n/p}$.
22. $b^2 = (t + \alpha)^p(t + \alpha) = (t + \alpha^p)(t + \alpha) = (t - \alpha)(t + \alpha) = t^2 - \alpha^2 = a$, where the third equality comes from the fact that $\alpha = \sqrt{t^2 - a}$ has conjugate $\alpha^p = -\sqrt{t^2 - a}$; note that b must be in \mathbf{F}_p , since a has two square roots in \mathbf{F}_p by assumption, and so its square roots in \mathbf{F}_{p^2} are actually in \mathbf{F}_p .
23. Let b be the least positive residue of $n^{(p-1)/4}$ modulo p ; then b is a square root of -1 modulo p , i.e., $p|b^2 + 1$. Now compute $c + di = g.c.d.(p, b + i)$ (see Exercise 14 of § I.2).

§ III.1.

1. “We sewed a smile on a horse’s ass, and a year later it was elected President.”
2. Use the fact that “X” occurs most frequently in the ciphertext to find that $b = 19$. The message is: WEWERELUCKYBECAUSEOFTEN THEFREQUENCYMETHODNEEDSLONGERCIPHERTEXT.
3. THRPXDH.
4. SUCCESSATLAST.
5. AGENT 006 IS DEAD 007.
6. You find 9 possibilities for a' and b' : $a' = 1, 4, 7, 10, 13, 16, 19, 22, 25$, and $b' = 21, 6, 18, 3, 15, 0, 12, 24, 9$, respectively. Since you have no more information to go on, simply try all nine possibilities; it turns out that only the third one $P \equiv 7C + 18 \pmod{27}$ gives a meaningful plaintext. The plaintexts of the nine transformations are, respectively: “I DY IB RIF”, “I PS IH RIX”, “I AM IN RIO”, “I MG IT RIF”, “I YA IZ RIX”, “I JV IE RIO”, “I VP IK RIF”, “I GJ IQ RIX”, “I SD IW RIO”.
7. (a) N ; (b) $N\varphi(N) = N^2 \prod_{p|N} (1 - \frac{1}{p})$; (c) 312, 486, 812, 240.
8. (a) If $a \neq 1$, then the congruence $(a-1)P \equiv -b \pmod{N}$ has exactly one solution in the field $\mathbf{F}_N = \mathbf{Z}/N\mathbf{Z}$. (b) $P = 0$ is always fixed; for N even (so a must be odd) the congruence $(a-1)P \equiv 0 \pmod{N}$ at least has the two solutions $P = 0$ and $P = N/2$. (c) Any example with N even and b odd; more generally, any example in which b is not divisible by $g.c.d.(a-1, N)$.
9. $N^2\varphi(N^2) = N^4 \prod_{p|N} (1 - \frac{1}{p})$; 210,912; 354,294; 682,892; 216,000.