

Exercise 4.1: Someone uses RSA to encode a secret message $\bar{x} \in (\mathbf{Z}/144869)^*$ by sending the coded form $\bar{y} = \bar{x}^{103} = \bar{12}$. Using a calculator or a computer, factor $N = 144869$, deduce the decryption encoding, and find the original message \bar{x} . Carefully describe the steps in your work.

Exercise 4.2: Use the lifting method discussed in class to find all solutions of the congruences:

$$x^2 + 1 \equiv 0, \quad x^3 - 3x - 11 \equiv 0, \quad x^2 - 46x + 22 \equiv 0 \pmod{13^4}.$$

Please write your answer in “base 13”, i.e., in the form $a_0 + 13a_1 + 13^2a_2 + 13^3a_3$ with each $a_i \in \{0, 1, \dots, 12\}$.

Exercise 4.3: Let p be a prime number other than 2, and let a be relatively prime to p . Show that: if given x_1 such that $x_1^2 \equiv a \pmod{p}$, then there exist x_2, x_3, \dots such that, for all k :

- (i) $x_k^2 \equiv a \pmod{p^k}$;
- (ii) $x_k \equiv x_{k-1} \pmod{p^{k-1}}$.

Show furthermore that x_k is unique mod p^k .

Hint: induction on k , as in class. This exercise shows you that to test whether a is (congruent to) a square mod p^k , it is enough to test whether it is a square mod p .

Challenge: what happens if $p = 2$?

Exercise 4.4: Consider the equation $x^2 + y^2 = 1$. Given m , define $N(m)$ to be the number of pairs (x, y) in $\mathbf{Z}/m\mathbf{Z} \times \mathbf{Z}/m\mathbf{Z}$ such that

$$x^2 + y^2 \equiv 1 \pmod{m}. \quad (*)$$

For example, $N(5) = 4$ because there are 4 solutions: $(1, 0), (4, 0), (0, 1), (0, 4)$.

a) Find $N(3)$ and $N(7)$. (If you have the time, find $N(p)$ for some more primes, perhaps using a computer, and see if you can find a pattern. Challenge: prove that your pattern always holds.)

b) [may be challenging] Show that if p is a prime other than 2, then $N(p^2) = pN(p)$, and in general $N(p^k) = pN(p^{k-1})$. Conclude that $N(p^k) = p^{k-1}N(p)$.

Hint: show that if you have a given pair (x_k, y_k) which are a solution to $(*) \pmod{p^k}$, then you can “lift” them to p possible choices of solutions $(x_{k+1}, y_{k+1}) \pmod{p^{k+1}}$, such that $x_{k+1} \equiv x_k \pmod{p^k}$, and $y_{k+1} \equiv y_k \pmod{p^k}$.

c) use parts a) and b) to find $N(15)$ and $N(1575)$.

Exercise 4.5: Fix $n > 0$.

a) If $d > 0$ and $d|n$, show that the number of elements \bar{a} in $\mathbf{Z}/n\mathbf{Z}$ such that $(a, n) = d$ is equal to $\varphi(n/d)$.

Hint: write $a = da'$. As an example of what you have to prove, the number of elements \bar{a} in $\mathbf{Z}/15\mathbf{Z}$ with $(a, 15) = 3$ is exactly $\varphi(5) = 4$: the elements in question are $\bar{3}, \bar{6}, \bar{9}, \bar{12}$.

b) Show that $n = \sum_{d|n} \varphi(n/d) = \sum_{d|n} \varphi(d)$.

Hint: separate the elements in $\mathbf{Z}/n\mathbf{Z}$ according to their GCD with n .

Exercise 4.6: (The Moebius inversion formula.) Define the Moebius μ -function $\mu : \mathbf{N} \rightarrow \mathbf{C}$ by $\mu(1) = 1$, $\mu(p_1 p_2 \cdots p_r) = (-1)^r$ if p_1, p_2, \dots, p_r are distinct primes, and $\mu(n) = 0$ otherwise (i.e., if n is not squarefree).

a) Suppose given functions $f, g : \mathbf{N} \rightarrow \mathbf{C}$ such that $g(n) = \sum_{k|n} f(k)$. Show that

$$f(n) = \sum_{k|n} \mu(k)g(n/k) = \sum_{\ell|n} \mu(n/\ell)g(\ell) = \sum_{k\ell=n} \mu(k)g(\ell).$$

Suggestion: first prove that

$$\sum_{d|m} \mu(d) = \begin{cases} 1, & \text{if } m = 1 \\ 0, & \text{if } m > 1. \end{cases}$$

b) Apply the above to $f(n) = \varphi(n)$ and $g(n) = n$ (using the result of the previous exercise) and use this to derive a different proof of the identity

$$\varphi(n) = n \prod_{p|n, p \text{ prime}} \left(1 - \frac{1}{p}\right).$$

Look at, but do not hand in: Let p be a prime.

1) Show that $1 + p$ has multiplicative order p in $(\mathbf{Z}/p^2\mathbf{Z})^*$. Conclude that for $k \geq 2$, the multiplicative order of $1 + p$ in $(\mathbf{Z}/p^k\mathbf{Z})^*$ is a multiple of p . (Challenge: prove that this order is in fact a *power* of p .)

2) Conclude that if $p^2|N$, then there exists $a \in (\mathbf{Z}/N\mathbf{Z})^*$ whose multiplicative order in $(\mathbf{Z}/N\mathbf{Z})^*$ is a multiple of p . (Caution: $1 + p$ might not be relatively prime to N . I suggest that you write $N = p^k M$, where $k \geq 2$ and $p \nmid M$, and choose a by choosing $a \bmod p^k$ and $a \bmod M$ separately and invoking the Chinese Remainder Theorem.)

3) Deduce that N is not a Carmichael number. (N.B., this shows that if N is a Carmichael number, then it is squarefree, i.e., it is the product of distinct prime numbers.)