Topics: Structure of integers mod m, primes, RSA.

3.1. Let p be a prime number and let m be an integer such that $m \mid (p-1)$. Prove that the group $(\mathbf{Z}/p\mathbf{Z})^\times$ has an element of order m.

3.2. Prove the following formula for the Euler phi function:

$$\phi(m) = m \prod_{j=1}^{r} \left(1 - \frac{1}{p_j}\right),$$

where $p_1, \ldots, p_r$ are the distinct prime factors of m.

3.3. Prove that if $a \mid b$ then $\phi(a) \mid \phi(b)$.

3.4. Prove that $561 = 3 \cdot 11 \cdot 17$ is a Carmichael number.
[**Hint**: Show that for any a, we have $a^{561} \equiv a$ modulo 3, 11, and 17.]

3.5. Recall that we define $\mathsf{Li} : [2, \infty) \longrightarrow \mathbf{R}$ by

$$\mathsf{Li}\,(x) = \int_2^x \frac{dt}{\log(t)}.$$

(a) Use integration by parts to prove that

$$\mathsf{Li}\,(x) = \frac{x}{\log(x)} + \int_2^x \frac{dt}{(\log(t))^2} + O(1).$$

(b) Fix $x \geqslant 4$ and estimate the two integrals

$$\int_2^{\sqrt{x}} \frac{dt}{(\log(t))^2} \qquad \text{and} \qquad \int_{\sqrt{x}}^x \frac{dt}{(\log(t))^2}.$$

(c) Use part (b) to conclude that $\mathsf{Li}\,(x) \sim x/\log(x)$.

(d) Why was the splitting of the integral into two pieces necessary in part (b)?

3.6. From volume 3 of *Sun Tzu Suan Ching*: "We have a number of things, but we do not know exactly how many. If we count them by threes, we have two left over. If we count them by fives, we have three left over. If we count them by sevens, we have two left over. How many things are there?"

3.7. Show that if 35 is used as the modulus for an RSA scheme, then the encryption exponent must be the same as decryption exponent.

3.8. In the lectures, we recalled the fact that if K is a field and f is a polynomial of degree n, then f has at most n roots in K.

In particular, this says that if f is a polynomial with integer coefficients such that the leading coefficient is not divisible by p, then the congruence $f(x) \equiv 0 \pmod{p}$ has at most n solutions in $\mathbf{Z}/p\mathbf{Z}$.

(a) Give an example of a pair (p, f) showing that this can fail if p is not prime.

(b) Can you find such an example whenever p is not prime?