It is better to solve one problem five different ways than to solve five problems one way.
—George Polya

- *Required Reading*: Text § 9.5, 10.2, 10.3, 13.2–5
- *Optional Reading*: Handout on "Chinese Remainder Theorem", original RSA paper.

1. *RSA:* Let $m = 15943$ be an RSA modulus, with encryption exponent $e = 3$. Messages are encoded in two-letter blocks (from left to right).

   (a) Encode the message "ATTACK".

   (b) Find the decryption exponent and then decode the message assigned to your homework group below. Show your work and give the decoded message as a word in plain English. (To reduce integers in some modulus or to take powers in some modulus, use Wolfram Alpha.)

Group	Message
AAAR	$(10556, 9788)$
CCJRT	$(2938, 14425)$
AKLW	$(2938, 71)$
AKLT	$(10743, 11733)$
BBKM	$(906, 5860)$
BCKT	$(10798, 15691)$
MMMR	$(13503, 9250)$

2. *Polynomial arithmetic:* A common alternate notation for $\mathbf{Z}/p$ is $\mathbf{F}_p$ (standing for "the field with p elements"). So $\mathbf{F}_p[T]$ means $(\mathbf{Z}/p)[T]$; these are polynomial whose coefficients are integers mod p.

   (a) Use Euclid's algorithm and back-substitution to find the (monic!) gcd of $T^8 - 1$ and $T^5 + 2T^3 + 1$ in $\mathbf{F}_3[T]$. Then express the gcd as an $\mathbf{F}_3[T]$-linear combination of the two polynomials.

   (b) In $\mathbf{F}_3[T]$, express the simultaneous congruence conditions

   $$f(T) \equiv T \pmod{T^2 + T + 2} \quad \text{and} \quad f(T) \equiv T^2 + T + 1 \pmod{T^3 - T}$$

   as a single congruence condition. When you need to invert in some modulus, use Euclid's algorithm and back-substitution.

   (c) Use Euclid's algorithm to solve $(T^2 + T + 1)f(T) \equiv 1 \pmod{T^4 + T^3 + 1}$ in $\mathbf{F}_2[T]$.

   (d) Find a polynomial $f(T) \in \mathbf{F}_2[T]$ satisfying the pair of congruences

   $$f(T) \equiv T \pmod{T^2 + T + 1} \quad \text{and} \quad f(T) \equiv T^2 \pmod{T^4 + T^3 + 1}$$

3. *Arithmetic in* $\mathbf{Z}[i]$*:*

   (a) Solve $(8-i)x + (2+9i)y = 1$ in $\mathbf{Z}[i]$ by the $\mathbf{Z}[i]$-version of Euclid's algorithm and use this to find a solution to $(8-i)\alpha \equiv 3+2i \bmod 2+9i$ with $\mathrm{N}(\alpha) \leq (1/2)\,\mathrm{N}(2+9i)$. Verify your answer really works.

   (b) Adapt the method the text uses in § 13.3 to draw on graph paper a picture of the Gaussian integral multiples of $2+2i$ spread across the plane and use your picture to find a set of representatives for $\mathbf{Z}[i]/(2+2i)$. Which member of your set of representatives is congruent to $-i$? Which is congruent to 7? Use the picture to answer those questions, but then check the answers really work algebraically.

   (c) Use the table of small Gaussian primes from Exercise 5 on Set 2 (see Solution Set 2 for a correct table) to help you factor $4+7i$, $3-5i$, and $1+18i$ into primes in $\mathbf{Z}[i]$. *Show your work.*

4. *Orders of elements in* $\mathbf{Z}/m$*:*

   (a) Show that U_{2^k} has no primitive roots for $k \geq 3$. (Hint: What does HW#3, problem 1(a) tell you?)

   (b) Suppose U_m has a primitive root, and that $(a, m) = (k, \varphi(m)) = 1$. Show that the equation $x^k = a$ has a unique solution in $\mathbf{Z}/m$.

   (c) Show that if p is prime and $(k, p-1) = 1$, then the integers

   $$1^k, 2^k, \ldots (p-1)^k$$

   form a complete set of residues modulo p.

   (d) Prove that for p prime,

   $$1{\cdot}2{+}1{\cdot}3{+}\cdots{+}1{\cdot}(p{-}1){+}2{\cdot}3{+}2{\cdot}4{+}\cdots{+}2{\cdot}(p{-}1){+}\cdots{+}(p{-}2)(p{-}1) = \sum_{1\leq i<j\leq p-1} ij \equiv 0 \pmod{p}\,.$$

   Hint: Factor $x^{p-1}-1$ into linear factors in $\mathbf{F}_p[x]$, and find the above expression there. What about the (easier) sum $\sum_{i=1}^{p-1} i$?

5. *Prove or Disprove and Salvage if Possible*

   (a) For p an odd prime, If $\mathrm{ord}_p\, a = 2k$, then $a^k \equiv -1 \pmod{p}$.

   (b) For any integer $n > 1$, $n \mid \varphi(2^n - 1)$.

   (c) For p an odd prime, $ab \equiv \square \pmod{p} \iff a \equiv \square \pmod{p}$ and $b \equiv \square \pmod{p}$

   (d) For p an odd prime, if $a \equiv \square \pmod{p}$, then $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$