Problem 1. Bijectons, also called “1-1 correspondences”, play a big role in mathematics. Besides introducing them in general, this problem is also number theory.

Suppose \( N \) is an odd positive integer. Establish the following bijection between the ordered pairs \((a, b)\) of integers with \( a \geq b > 0 \) and \( N = ab \), and the ordered pairs \((r, s)\) of integers with \( N \geq r > s \geq 0 \) and \( N = r^2 - s^2 \):

To get \((a, b)\) from \((r, s)\):
\[
a = r + s \quad \text{and} \quad b = r - s
\]
and

To get \((r, s)\) from \((a, b)\):
\[
r = \frac{a + b}{2} \quad \text{and} \quad s = \frac{a - b}{2}
\]

That is, you must show that (i) if \((r, s)\) has the stated properties then following the recipe for \((a, b)\) in terms of \((r, s)\) gives a pair with the properties required of \((a, b)\), (ii) similarly in the opposite direction, (iii) if you start with such a pair \((r, s)\) and use the first recipe to build a pair \((a, b)\) and then the second recipe to build a pair \((r', s')\) from \((a, b)\), then you get back where you started: \((r', s') = (r, s)\), and (iv) similarly in the opposite direction.

Once you have established a bijection then you can use it to look at a problem from a new perspective. For example, the next problem.

Problem 2. This uses the previous problem.

(a) Find a factorization of 899 as the product of two smaller positive numbers. Don’t use trial and error division. It’s easier to look instead for \( r \) and \( s \) as in the previous problem, i.e., \( 899 = r^2 - s^2 \), and then convert to a pair of factors \((a, b)\). (Hint: obviously \( r \) must be at least as big as \( \sqrt{899} \). Start looking there.)

(b) Do the same for 377.

(c) Do the same for 1,633,283. Definitely don’t try to use trial division on this one. (It is actually easier than (b), using the \( r^2 - s^2 \) method.)

Problem 3. Compute the following gcd’s. (Write out all the details of all the steps. You can check with your calculators. More practice: no. 1 in section 3.3. Do the extra practice until it becomes routine. I recommend that you use the same calculator you will use on exams.)

(a) \( \gcd(273, 91) \)

(b) \( \gcd(10001, 1001) \)

Problem 4. In this problem, give formal proofs. For part (b), you also need to write down the theorem that you are proving.

(a) If \( k \) is an integer then \( \gcd(6k + 7, 3k + 4) = 1 \).

(b) \( \gcd(n + 1, n^2 - n + 1) \) can take two possible values, when \( n \) varies over the integers. Find these values, and which \( n \)’s produce them.

Problem 5. We have seen that \( \mathbb{Z}_m \) is a lot like \( \mathbb{Z} \), but can be strange in some ways (like “even” not being meaningful when \( m \) is odd). This problem points out another difference. I assume you know the fact that a polynomial of degree \( d \) has at most \( d \) roots in the real numbers \( \mathbb{R} \). Well, the obvious analogue of this can fail in \( \mathbb{Z}_m \):

(a) The polynomial equation \( x^2 = 1 \) has more than two solutions in \( \mathbb{Z}_8 \): find them all, count them, and observe that there more of them than the degree of the polynomial. Your answer should have the form \( x \in \{\text{some set of elements of } \mathbb{Z}_8\} \), not \( x \in \{\text{some set of integers}\} \). In particular, there should be bars on elements.
(b) The same as (a) with \( \mathbb{Z}_8 \) replaced by \( \mathbb{Z}_{15} \).

(Curiously and deeply, it turns out that the fact above for polynomials \textbf{does} hold in \( \mathbb{Z}_m \) if \( m \) is a prime number. We will see more of this later in the course.)