1. (20 points). (i) Show that 1943 and 1234 are relatively prime (coprime) and find integers \(s\) and \(t\) so that \(1 = 1943s + 1234t\). Use the extended Euclidean algorithm (either as in the handout or as in Biggs and show your work.

(ii) Find \(x\), \(0 \leq x < 1943\), so that \(1234x \equiv 753\) (mod 1943). Do this by hand and show your work.

2. (15 points). Sometimes we write “\(a\) (mod \(m\))” (read “\(a\) modulo \(m\)”) to mean the remainder when \(a\) is divided by \(m\).

Suppose you can multiply two 20 (or less) digit numbers in one second, and divide one 40 (or less) digit number by a 20 digit number to find the remainder in one second. If you need to add or subtract, assume it takes no time at all.

Can you compute

\[12838938912892^{59283746352789949217} \pmod{76598734562319876331}\]

in less than one million years? In less than one week? How long? Explain briefly. (I don’t need an exact answer, just something ‘reasonable’.)

3. (20 points). Suppose \(a\) and \(b\) are relatively prime integers, both \(\geq 2\).

(i) Which of the nonnegative integers \(k \leq 30\) can be written as nonnegative integer linear combinations of 5 and 7? [Don’t write anything for this part. You don’t even need to do it.]

(ii) Prove that every integer \(c \geq (a - 1)(b - 1)\) can be written as a nonnegative integer linear combination of \(a\) and \(b\); that is, \(c = sa + tb\) for some nonnegative integers \(s\) and \(t\).

Suggestion: If \(c = sa + tb\) (whether \(s\) and \(t\) are nonnegative or not), then also \(c = (s - kb)a + (t + ka)b\) for any integer \(k\). By appropriate choice of \(k\) we can ensure that \(0 \leq t' = t + ka < a\). So there are integers \(s', t'\) so that \(c = s'a + t'b\) where \(0 \leq t' < a\). You do not need to explain this. But prove that if \(c \geq (a - 1)(b - 1)\), then \(s' \geq 0\).

(iii) Prove that \((a - 1)(b - 1) - 1\) cannot be written as a nonnegative linear combination of \(a\) and \(b\).

Suggestion: Suppose \((a - 1)(b - 1) - 1 = sa + tb\). Prove carefully that \(s \equiv -1\) (mod \(b\)) and \(t \equiv -1\) (mod \(a\)). Then show that \(sa + tb \geq (a - 1)(b - 1)\), which contradicts our assumption.

(iii) Explain why for any integer \(k\), the integers \(k\) and \((a - 1)(b - 1) - k - 1\) cannot both be written as nonnegative integer linear combinations of \(a\) and \(b\). [It follows that at most half of the integers \(k\) in the range \(0 \leq k < (a - 1)(b - 1)\) can be written as nonnegative integer linear combinations of \(a\) and \(b\). Further analysis shows that exactly half of the integers in that range can be so expressed.]

Do Exercises 5, 6, and 7 about Fibonacci numbers. Prove or explain your answers.