HOMEWORK 8: §7.5, 7.8, 7.9 AND §8.1-3 DUE MARCH 23

Name: ____

- Please refer to the syllabus regarding allowed collaboration on this homework assignment.
- All answers should be fully justified.
- Your homework should be neatly written on additional paper; you may attach this cover page if you would like to keep the questions attached to the answers.

(1) Write down the last two digits of your student ID, so I don't have to look it up.

Use the RSA algorithm to encrypt the last two digits of your student ID number (or 34, if the last two digits of your ID are 01) using the public key $(N, e) = (7957, 17)$.

(2) Use the Extended Euclidean Algorithm to find a Bézout identity for the following pairs of integers (n, m). Then find the multiplicative inverse of m in $\mathbb{Z}_n$, or say that none exists.

(a) $n = 2543$, $m = 12$

(b) $n = 2544$, $m = 12$

(c) $n = 55$, $m = 34$

(3) Here you will prove that $g = \gcd(x, y)$ is the smallest positive integer expressible as a linear combination of x, y *[i.e., as $ax + by$ for integers a, b]*.

(a) First, why is g expressible this way?

(b) Next, we show that it is the smallest, by contradiction. Suppose $0 < d < g$ and that $d = ax + by$ for some integers a, b. Why is it true that $g \mid d$? (This gives our contradiction: $g \mid d$ implies that $g \leq d$ (since everything is positive), but we assumed $d < g$.)

(4) *Making change*

(a) In a certain country, there are three kinds of coins: 6¢, 22¢, and 33¢ coins. Assume that vendors and customers always have an unlimited supply of all these coins. Are there any prices that a customer cannot pay exactly if the vendor gives change? Explain.

(b) Same situation, but the government has stopped producing and reclaimed all 6¢ coins. Now are there any prices that a customer cannot pay exactly (vendors still giving change)? Explain.

(5) Find a closed form for $\displaystyle\sum_{i=2}^{n} \left(7 + 3i + 11 \cdot 2^i\right)$.

(6) A certain diner has parallel parking along the street. Being so popular with motorcyclists, the parking spots are marked to accommodate the length of a motorcycle. A car can also park there, and fits just right in two consecutive spots.

Let t_n denote the number of ways that such a parking strip with n motorcycle spaces can be filled with cars and motorcycles. For example, $t_3 = 3$: `(m|m|m)`, `(CCC|m)`, `(m|CCC)`.

Find a recurrence relation (base case(s) and recurrence) for $\{t_n\}$. *(Hint: consider the last vehicle parked in the strip.)*

Poetry is the art of giving different names to the same thing.
Mathematics is the art of giving the same name to different things.
Adapted from Poincaré