Miniproject 2:

Number theory and applications

In this miniproject you will work with concepts and algorithms from Sections 4.3, 4.4 and 4.5 in [Rosen]. Remember that miniprojects are part of the curriculum for exam. Answers to exercises are found at the end of this document.

Exercise 1:
This exercise is done by hand. Given $a = 3$ we want to find $\bar{a}$ such that $\bar{a}a \equiv 1 \pmod 7$. Find $\bar{a}$ by trying different values. (Why do you only need to try values in $\{0, 1, 2 \dots 6\}$?).

Exercise 2:
This exercise is done by hand. Given $a = 5$, we want to find $\bar{a}$ such that $\bar{a}a \equiv 1 \pmod{19}$. You should use the Euclidean algorithm to determine $\bar{a}$ (as in Examples 1 and 2 i Section 4). When you have found the answer then test that it satisfies the required congruence.

Exercise 3:
This exercise is done with the help of Maple. The command "igcdex(a, b, s, t)" in Maple computes and returns the greatest common divisor of the integers a and b. Furthermore it saves in variables "s" and "t" values satisfying that $\gcd(a, b) = sa + tb$. You can access the value of s by writing "s" on a commandline and pressing enter. Given $a = 103$ and $m = 4627$, find $\bar{a}$ so that $\bar{a}a \equiv 1$ (mod m) (Argue that $\bar{a} = s$). Test that the computed value of $\bar{a}$ satisfies $\bar{a} \cdot 103 \equiv 1 \pmod{4627}$.

Exercise 4:
This exercise is a continuation of Exercise 2 and is done by hand. Use the method described in Example 3 in Section 4.4 to solve the congruence

$$5x \equiv 2 \pmod{19}.$$

Exercise 5:
This exercise is a continuation of Exercise 3 and is done in Maple. Use the method described in Example 3 in Section 4.4 to solve the congruence

$$103x \equiv 14 \pmod{4627}.$$

SAVE YOUR WORKSHEET BEFORE YOU DO THE NEXT EXERCISE. As part of this exercise you may experience that Maple crashes.

Read Section 4.4 in Rosen's book.

Exercise 6:
Enter in Maple the expression "3^{2005} mod 11" and press return to get the answer. Repeat with "3^{20005} mod 11", with "3^{200005} mod 11" etc. Continue until Maple can not do the computation. For example Maple can not handle "$3^{2000000000005}$ mod 11" unless you use some trick. (If necessary restart Maple.) Compute 2000000000005 mod 10 (why 10 ?) and use Fermat's Little Theorem (Theorem 3 in Section 4.4) to compute $3^{2000000000005}$ mod 11 as in Example 9 in Section 4.4.

Exercise 7:
This exercise is done by hand. Compute 3^{40} mod 13, using the method described in Example 9 in Section 4.4.

Exercise 8:

We consider a system of congruences:

$$\begin{cases} x \equiv 1 \pmod{6} \\ x \equiv 2 \pmod{7} \\ x \equiv 3 \pmod{11} \end{cases} \tag{1}$$

Let $a_1 = 1$, $a_2 = 2$, $a_3 = 3$, $m_1 = 6$, $m_2 = 7$ and $m_3 = 11$.

1. Argue that m_1, m_2, m_3 are pairwise relatively prime.
2. Determine M_1, M_2, M_3.
3. Compute the multiplicative inverse of M_1 modulo m_1 (This inverse is denoted by y_1 in the proof of Theorem 2 in Section 4.4.) Thus you should find a number y_1 satisfying that

$$y_1(M_1 \bmod m_1) \equiv 1 \pmod{m_1}$$

Find y_1 by trying different values (or by using the extended Euclidean algorithm).

4. Similarly find the multiplicative inverse y_2 of M_2 modulo m_2.

5. Also find the multiplicative inverse y_3 of M_3 modulo m_3.

6. Solve the system of congruences (1) using the following formula from the proof of Theorem 2:

$$x \equiv a_1 M_1 y_1 + a_2 M_2 y_2 + a_3 M_3 y_3 \pmod{m_1 m_2 m_3}.$$

Exercise 9:
Show that Theorem 2 on page 275 has the following form for $n = 2$: (The problem is in particular to show that the expression for x from the proof of Theorem 2 is as shown below.)
The Chinese Remainder Theorem for $n = 2$ congruences.
Let m_1 and m_2 be relatively prime integersgreater than one and let a_1 and a_2 be arbitrary integers.
The the system

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \end{cases}$$

has a unique solution modulo $m = m_1 m_2$, namely $x \equiv a_1 t m_2 + a_2 s m_1 \pmod{m}$, where $\gcd(m_1, m_2) = 1 = s m_1 + t m_2$, i.e., s og t are computed using the extended Euclidean algorithm.

Exercise 10:
Solve the following system of congruences

$$\begin{cases} x \equiv 3 \pmod{5} \\ x \equiv 2 \pmod{11} \end{cases} \tag{2}$$

Exercise 11:
Use the Method from Exercise 8 above (and Example 5 in Section 4.4) to solve this system of congruences:

$$\begin{cases} x \equiv 2 \pmod{7} \\ x \equiv 4 \pmod{9} \\ x \equiv 3 \pmod{13} \end{cases} \tag{3}$$

Read Secton 4.5 in Rosen's book.

Exercise 12:
Solve the following problems from Rosen, Section 4.5:

- Exercise 1: Which memory locations ...
- Exercise 5: What sequence of pseudorandom ...
- Exercise 11: The first nine digits of the ISBN-10 ...

Answers

- Ex. 1: 5.
- Ex. 2: 4.
- Ex. 3: 584.
- Ex. 4: The least non-negative solution is 8. The complete set of solutions is $\{8 + 19k \mid k \in \mathbb{Z}\}$.
- Ex. 5: The least non-negative solution is 3549. The complete set of solutions is $\{3548 + 4627k \mid k \in \mathbb{Z}\}$.
- Ex. 6: 1.
- Ex. 7: 3.
- 0pg. 8:
  1. $\gcd(6, 7) = \gcd(6, 11) = \gcd(7, 11) = 1$.
  2. $M_1 = 77, M_2 = 66, M_3 = 42$.
  3. $y_1 = 5$
  4. $y_2 = 5$
  5. $y_3 = 5$
  6. The least non-negative solution is 289. The complete set of solutions is $\{289 + 462k \mid k \in \mathbb{Z}\}$.
- Ex. 10: The least non-negative solution is 13. The complete set of solutions is $\{13 + 55k \mid k \in \mathbb{Z}\}$.
- Ex. 11: The least non-negative solution is 562. The complete set of solutions is $\{562 + 819k \mid k \in \mathbb{Z}\}$.
- Ex. 12: See answers in Rosen.