CS40 Winter 2021 Homework #5

February 7, 2021

Notes

- You may work with a partner in order to understand the problems and discuss how to approach them. If you do so, write clearly on your assignment the name of the student you collaborated with.
- Justify your answers!
- Please re-read the "Conduct" section in the class syllabus.
- No late submissions! Turn-in what you have by the deadline.

. . . . . .

1. **Integer representation**

   (a) Convert the following octal, decimal and hexadecimal numbers to binary (base 2):

   i. $(1011101011)_8$
   ii. $(121)_{10}$
   iii. $(9AB80FF)_{16}$

   (b) Write the following in 16-bit binary under two's complement:

   i. -1
   ii. -32767

   (c) What are the greatest and smallest integers representable under 16-bits with two's complement scheme?

   (d) Find $\gcd(a, b)$ and $\text{lcm}(a, b)$ if

   $$a = 2^3 5^4 7^2 11^3 19^3$$
   $$b = 2^2 3^3 5^2 7^3 11^4 19$$

   You can leave your answers in product form.

2. **Modular arithmetics**
   ϕ is Euler's totient function (defined in notes).

   (a) Find the check digit x_{10} of the ISBN-10 number $0\,0\,7\,3\,4\,0\,7\,0\,2\,x_{10}$.

   (b) Use Fermat's Little Theorem to compute $9^{2390} \bmod 13$.

   (c) Prove that for every $n \in \mathbb{Z}^+$, $11 \mid (10^{2n} - 1)$.

(d) Show that if s and t are relatively prime positive integers, then $\phi(st) = \phi(s)\phi(t)$.

[Hint: Use the Chinese Remainder Theorem to find a bijection between the set of integers less than and relatively prime to st and the set of ordered pairs (a, b) where $a < s, b < t$ and $\gcd(a, s) = 1$ and $\gcd(b, t) = 1$]

(e) Prove the following: If p, q are distinct primes, then for each integer a not divisible by p or q: $a^{(p-1)(q-1)} \equiv 1 \pmod{pq}$.

3. **Chinese Remainder Theorem**

Given the following modular equations system

$$\begin{aligned} x &\equiv 0 \pmod 3 \\ x &\equiv 0 \pmod 4 \\ x &\equiv 0 \pmod 5 \\ x &\equiv 4 \pmod{11} \end{aligned}$$

(a) Use the Chinese remainder theorem to find the unique solution in the range $0 \leq x < 660$.

(b) Use set builder notation to write down *all* integer solution to these equations.

4. **Public-key encryption (RSA)**

(a) Consider a plain RSA cryptographic system with modulus $N = 437$ and public exponent $e = 17$.

i. Encrypt $67, 83, 52, 48$.

ii. Factorize N and find out d.

iii. Decrypt the ciphertext and verify the result. Use an online ASCII table to convert the numbers to characters.

(b) The "Fermat primality test" for $n \in \mathbb{Z}^+$ chooses a random integer $1 < a < n$ and decides that n is composite if $a^{n-1} \not\equiv 1 \pmod n$. Otherwise the test concludes that n is possibly prime. Does the test always classify a composite correctly? Does it always classify a prime correctly? Prove or give a counterexample.