CS250:	Hw5	Due as Hw5 MoodleQuiz, before 11 pm, Thu, 12/1/16

Please do these problems before looking at the Moodle Quiz. Then once you are happy with your solutions, do the quiz. I'll put the quiz up by Nov. 28. Feel free to ask questions about the meaning of any of these problems via Piazza. As always, **be careful**: if your question or its answer might give away information about a solution, then **post privately just to the instructors**. If you post privately, but I think it is a good, general interest question, then I'll make the question and answer public.

1. [50 pts.] This problem gives you practice using RSA, with tiny numbers so that you can do this easily with a calculator and see the details. Remember that in practice the primes involved would be huge: over 1000 bits each). Suppose that your two primes are 11 and 13. You publish your public modulus $n = 143$ and your public encrypting key $e = 7$. But you keep the factorizaton of n secret.

   (a) What is $\varphi(n)$?

   (b) Use Euclid's algorithm to compute your secret decryption key, d, the multiplicative inverse of e mod $\varphi(n)$.

   (c) Suppose someone wants to encrypt the message "98" to you. Showing your work, compute the encryption of 98 using your public key. (Note you should use the algorithm in Epp, Example 8.4.5.) Call this encrypted message a.

   (d) Now, showing your work, raise a to the power d mod n. The answer should be 98.

   (e) Suppose you want to sign a message, "25". Showing your work, raise 25 to the power d mod n. Call the answer c, your signed contract.

   (f) Now, showing your work, raise c to the power e mod n. This should be 25: the message you have signed, as anyone can see.

2. [50 pts.] Let p and q be distinct primes. I mentioned in L27 that $\varphi(pq) = (p-1)(q-1)$. In order to prove that, your job in this problem is to prove that if a and b are relatively prime natural numbers, then $\varphi(ab) = \varphi(a)\varphi(b)$. To prove this, you should use the Chinese Remainder Theorem. The CRT says the following:

$$\forall a, b > 1\,(\gcd(a,b) = 1 \;\rightarrow\; \forall x \in \mathbf{Z}/a\mathbf{Z}\; \forall y \in \mathbf{Z}/b\mathbf{Z}\; \exists! z \in \mathbf{Z}/ab\mathbf{Z}\; (z \equiv x \pmod{a} \;\wedge\; z \equiv y \pmod{b}))$$

Recall that $\mathbf{Z}/a\mathbf{Z} = \{0, 1, \ldots, a-1\}$ is the set of integers mod a, with operations $+$ mod a and $*$ mod a.

(a) In order to prove the CRT, let $a > 1, b > 1$ with $\gcd(a,b) = 1$. Define the function,

$$\begin{aligned} f : \mathbf{Z}/a\mathbf{Z} \;\times\; \mathbf{Z}/b\mathbf{Z} \;&\rightarrow\; \mathbf{Z}/ab\mathbf{Z} \quad \text{as follows:} \\ f(x,y) \;&\stackrel{\text{def}}{=}\; \big(x \cdot b \cdot (b^{-1}\text{mod } a) + y \cdot a \cdot (a^{-1}\text{mod } b)\big) \;\%\; (a \cdot b) \end{aligned}$$

Show that $f(x,y) \equiv x \pmod{a}$ and $f(x,y) \equiv y \pmod{b}$.

(b) Argue that it follows that f is 1:1.

Expanded Discussion: Let's consider the case where $a = 5$ and $b = 3$.

Please review L17. In particular, using Euclid's Algorithm we can compute that gcd(5,3) = 1 and that $1 = 5 \cdot 2 + 3 \cdot (-3)$, and thus 5^{-1} (mod 3) is 2 and 3^{-1} (mod 5) is (-3) % 5, thus also equal to 2. In particular, $3 \cdot 5^{-1}$ (mod 3) = 6 and $5 \cdot 3^{-1}$ (mod 5) = 10.

Now the CRT tells us that $f : \mathbf{Z}/5\mathbf{Z} \;\times\; \mathbf{Z}/3\mathbf{Z} \rightarrow \mathbf{Z}/15\mathbf{Z}$ is a 1:1 and onto function given by $f(x,y) \stackrel{\text{def}}{=} x \cdot 6 + y \cdot 10$. Take the time to compute all fifteen values of $f(x,y)$ for $0 \le x < 5$ and $0 \le y < 3$, checking by hand that f is 1:1 and onto and for each x, y, $f(x,y)\%5 = x$ and $f(x,y)\%3 = y$. **end Expanded Discussion**.

(c) What are the cardinalities of the two sets $\quad \mathbf{Z}/a\mathbf{Z} \;\times\; \mathbf{Z}/b\mathbf{Z} \quad$ and $\quad \mathbf{Z}/ab\mathbf{Z}$?

(d) Argue that it follows that f is onto.

(e) Now let $f' = f \cap (\mathbf{Z}_a^* \times \mathbf{Z}_b^*)$ be the restriction of f to $\mathbf{Z}_a^* \times \mathbf{Z}_b^*$. Argue that $f' : (\mathbf{Z}_a^* \times \mathbf{Z}_b^*) \rightarrow \mathbf{Z}_{ab}^*$ and that f' is $1:1$ and onto.

(f) It thus follows that $\varphi(ab) = \varphi(a) \cdot \varphi(b)$. Why?