MATH135 Fall 2015 Assignment 8, Due at 8:25am on Wednesday 18, 2015

I.D. Number: 20612050 **First Name:** Nathaniel **Family Name:** Woodthorpe

List any references that you used beyond the course text and lectures (e.g. discussions, texts, or online resources). If you did not use any aids, state this is in the space provided.

I did not use any aids.

1. Solve the following simultaneous congruence. Show your work.

$$2x \equiv 18 \pmod{48}$$
$$x \equiv 11 \pmod{35}$$

First, we must simplify $25x \equiv 18 \pmod{48}$

$$25x \equiv 18 (\text{mod } 48)$$
$$50x \equiv 36 \pmod{48}$$
$$2x \equiv 36 \pmod{48}$$

$$2x = 36 + 48k, k \in \mathbb{Z}$$
$$x = 18 + 24k$$
$$x \equiv 18 \pmod{24}$$

Now we have these 2 equations:

$$x \equiv 11 \pmod{35}$$
$$x \equiv 18 \pmod{24}$$

$$x = 11 + 35l, l \in \mathbb{Z}$$
$$11 + 35l \equiv 18 \pmod{24}$$
$$35l \equiv 7 \pmod{24}$$
$$11l \equiv 7 \pmod{24}$$
$$11l - 24m = 7$$
$$11l + 24y = 7, y = -m$$

y	l	r	q
1	0	24	0
0	1	11	0
1	-2	2	2
-5	11	1	5
/	/	0	2

Therefore by EEA, $y = -5$, $l = 11$ satisfies $11l + 24y = 1$.
Therefore, $y = -35$, $l = 77$ satisfies $11l + 24y = 7$

$$l \equiv 77 \pmod{24}$$
$$l \equiv 5 \pmod{24}$$
$$l = 5 + 24n$$

$$x = 11 + 35(5 + 24n)$$
$$x = 186 + 840n$$
$$\therefore x \equiv 186 \pmod{840}$$

2. Determine the units digit (last/ones digit) of the positive integer 8^{9^7}. Justify your answer.

We must solve the following congruence:

$$\begin{aligned}
8^{9^7} &\equiv x \text{ (mod 10)} \\
8^{(9^2)^3 9} &\equiv x \text{ (mod 10)} \\
8^{(1^3)9} &\equiv x \text{ (mod 10)} \\
8^9 &\equiv x \text{ (mod 10)} \\
(8^3)^3 &\equiv x \text{ (mod(10)} \\
2^3 &\equiv x \text{ (mod 10)} \\
8 &\equiv x \text{ (mod 10)}
\end{aligned}$$

$\therefore$ the units digit of 8^{9^7} is 8.

3. Suppose $M = p_1 x p_2 x \dots x p_n$ where $p_1, \dots, p_n$ are distinct primes. Prove by induction that, for all positive integers n, if $\gcd(a, M) = 1$, then

$$a^{(p_1-1)(p_2-1)\dots(p_n-1)} \equiv 1 \pmod{M}$$

Base Case: Suppose $n = 1$. By the definition of M, $M = p_1$ where p_1 is some prime. We must prove that $a^{p_1-1} \equiv 1 \pmod{M}$. We can use $\mathrm{F}\ell\mathrm{T}$ to prove this if we can show M is prime, and $M \nmid a$.

We know M is prime because $M = p_1$, and we have already established that p_1 is a prime.

We know $M \nmid a$ because in the hypothesis we assume $\gcd(a, M) = 1$. Thus, a and M share no prime factors and cannot divide.

$\therefore a^{p_1-1} \equiv 1 \pmod{M}$

IH: Assume $a^{(p_1-1)(p_2-1)\dots(p_k-1)} \equiv 1 \pmod{M}$, where $M = p_1 p_2 \dots p_k$, for some $k \geq 1$.
Written as an equation, $a^{(p_1-1)(p_2-1)\dots(p_k-1)} = 1 + j(p_1 p_2 \dots p_k), j \in \mathbb{Z}$

IC: Lets look at $a^{(p_1-1)(p_2-1)\dots(p_k-1)(p_{k+1}-1)}$.

$$= a^{(p_1-1)(p_2-1)\dots(p_k-1)(p_{k+1}-1)}$$

$$= \left[a^{(p_1-1)(p_2-1)\dots(p_k-1)}\right]^{(p_{k+1}-1)}$$

$$= \left[1 + j(p_1)(p_2)\dots(p_k)\right]^{p_{k+1}-1} \quad \text{(By Inductive Hypothesis)}$$

(Let n = $p_{k+1} - 1$)

$$= \binom{n}{0} 1^n \left[j(p_1)(p_2)\dots(p_k)\right]^0 + \binom{n}{1} 1^{n-1} \left[j(p_1)(p_2)\dots(p_k)\right]^1 + \dots + \binom{n}{n-1} 1^1 \left[j(p_1)(p_2)\dots(p_k)\right]^{n-1} + \binom{n}{n} 1^0 \left[j(p_1)(p_2)\dots(p_k)\right]^n \quad \text{(By Binomial Theorem)}$$

$$= 1 + \binom{n}{0} \left[j(p_1)(p_2)\dots(p_k)\right]^0 + \binom{n}{1} \left[j(p_1)(p_2)\dots(p_k)\right]^1 + \dots + \binom{n}{n-1} \left[j(p_1)(p_2)\dots(p_k)\right]^{n-1} + \binom{n}{n} \left[j(p_1)(p_2)\dots(p_k)\right]^n \quad \text{(First term equals 1, multiply all the ones)}$$

$$= 1 + j\left[\binom{n}{1} \left[(p_1)(p_2)\dots(p_k)\right]^0 + \dots + \binom{n}{n-1} \left[(p_1)(p_2)\dots(p_k)\right]^{n-2} + \binom{n}{n} \left[(p_1)(p_2)\dots(p_k)\right]^{n-1}\right] ((p_1)(p_2)\dots(p_k)(p_k+1))$$

Let $j\left[\binom{n}{1}(p_1)(p_2)\dots(p_k)^0 + \dots + \binom{n}{n-1}(p_1)(p_2)\dots(p_k)^{n-2} + \binom{n}{n}(p_1)(p_2)\dots(p_k)^{n-1}\right]$ be x. We know x is an integer as the choose function strictly deals with integers, primes $p_1 \dots p_k$ are integers, and our exponents are integers.

$$a^{(p_1-1)(p_2-1)\dots(p_k-1)(p_{k+1}-1)} = 1 + j(p_1)(p_2)\dots(p_k)(p_{k+1})$$

$$a^{(p_1-1)(p_2-1)\dots(p_k-1)(p_{k+1}-1)} \equiv 1 \pmod{(p_1)(p_2)\dots(p_k)(p_{k+1})}$$

$$a^{(p_1-1)(p_2-1)\dots(p_k-1)(p_{k+1}-1)} \equiv 1 \pmod{M}$$

□

4. Suppose that in setting up RSA, Alice chooses $p = 31, q = 47$, and $e = 13$.

(a) What is Alice's public key?

The public key is (e, n) where $n = pq$.
$n = (31)(47)$
$n = 1457$
$\therefore$ Alice's public key is $(13, 1457)$

(b) What is Alice's private key?

Alice's private key is (d, n). We have already solved n.
To solve d, we must solve the following congruence:

$$\begin{aligned} ed &\equiv 1 \text{ (mod } (p-1)(q-1)) \\ 13d &\equiv 1 \text{ (mod } 1380) \end{aligned}$$

$$\begin{aligned} 13d - 1380k &= 1, k \in \mathbb{Z} \\ 13d + 1380y &= 1, y = -k \end{aligned}$$

y	d	r	q
1	0	1380	0
0	1	13	0
1	-106	2	106
-6	637	1	6
/	/	0	2

(c) Suppose Alice wishes to send Bob the message $M = 100$. Bob's public key is (11, 493) and Bob's private key is (163, 493). What is the cipher text corresponding to M? Show your work.

To find C, we must solve the following congruence:

$$\begin{aligned} M^e &\equiv C \text{ (mod } n) \\ 100^{11} &\equiv C \text{ (mod } 493) \\ (10^{11})(10^{11}) &\equiv C \text{ (mod } 493) \\ ((10^3)^3 10^2)^2 &\equiv C \text{ (mod } 493) \\ (14^3 10^2)^2 &\equiv C \text{ (mod } 493) \\ [(279)(100)^2 &\equiv C \text{ (mod } 493) \\ 292^2 &\equiv C \text{ (mod } 493) \\ 2^2 146^2 &\equiv C \text{ (mod } 493) \\ 2^2 2^2 73^2 &\equiv C \text{ (mod } 493) \\ (16)(399) &\equiv C \text{ (mod } 493) \\ 468 &\equiv C \text{ (mod } 493) \end{aligned}$$

Since C is between 0 and 493, $C = 468$.

5. Disprove the following statement:
If:

- p and q are the same prime number,
- $n = pq$
- e and d are positive integers such that $ed \equiv 1 \pmod{(p-1)(q-1)}$
- $0 \leq M < n$,
- $M^e \equiv C \pmod{n}$, and
- $C^d \equiv R \pmod{n}$ where $0 \leq R < n$

Then $R = M$.

We'll disprove this with a counter example.

Suppose p and q are 3.

$n = pq = 9$

Let $e = 5, d = 1$.

This satisfies the requirement that:

$ed \equiv 1 \pmod{(p-1)(q-1)}$
$5 \equiv 1 \pmod{4}$
$1 \equiv 1 \pmod{4}$

We have the requirement that M must be between 0 and n, or 0 and 9. Let $M = 3$

We solve for C, our ciphertext, as follows:

$M^e \equiv C \pmod{n}$
$3^5 \equiv C \pmod{n}$
$0 \equiv C \pmod{n}$

As $0 \leq C < n$, $C = 0$.

Now we can decipher this ciphertext back to the original message as follows:

$C^d \equiv R \pmod{n}$
$0^1 \equiv R \pmod{n}$
$0 \equiv R \pmod{n}$

As $0 \leq R < n$, $R = 0$.

Our message was 5, and after encrypting and decrypting, our message is now 0. $M \neq R$. This illustrates why we must use **distinct** primes when using RSA. □

6. Given prime numbers p and q where $p > q$, let $n = pq$ and $\phi(n) = (p-1)(q-1)$.

(a) Prove that $p + q = n - \phi(n) + 1$

LS: $p + q$

RS:
$$\begin{aligned} & n - \phi(n) + 1 \\ &= pq - (p-1)(q-1) + 1 \\ &= pq - (pq - p - q + 1) + 1 \\ &= p + q \end{aligned}$$

(b) Prove that $p - q = \sqrt{(p+1)^2 - 4n}$

LS: $p - q$

RS:
$$\begin{aligned} & \sqrt{(p+1)^2 - 4n} \\ &= \sqrt{p^2 + 2pq + q^2 - 4pq} \\ &= \sqrt{p^2 - 2pq + q^2} \\ &= \sqrt{(p-1)^2} \\ &= p - q \end{aligned}$$

(c) Explain why this means that $\phi(n)$ must be kept secret.

Given $\phi(n)$, an eavesdropper can easily compute (d, n), the private key. n is public, and d can be computed by solving $ed \equiv 1 \pmod{\phi(n)}$. e is in the public key, so d can easily be solved, allowing an eavesdropper to decode any messages that they like.

7. Let $z = 2 + i, u = 5 - 3i$, and $w = 2i$. Express each of the following in standard form.

(a) $2z + ui - w$

$$\begin{aligned} &= 2(2+i) + (5-3i)(i) - 2i \\ &= 4 + 2i + 5i - 3i^2 - 2i \\ &= 7 + 5i \end{aligned}$$

(b) $zu\overline{w}$

$$\begin{aligned} &= (2+i)(5-3i)(-2i) \\ &= (10 - 6i + 5i - 3i^2)(-2i) \\ &= (13 - i)(-2i) \\ &= (-26i + 2i^2) \\ &= -2 - 26i \end{aligned}$$

(c) $\dfrac{u}{z}$

$$\begin{aligned} &= \frac{5-3i}{2+i} \\ &= \frac{5-3i}{2+i}\frac{2-1}{2-1} \\ &= \frac{10 - 5i - 6i + 3i^2}{4 - i^2} \\ &= \frac{7 - 11i}{5} \\ &= \frac{7}{5} - \frac{11}{5}i \end{aligned}$$

An empty page for Crowdmark's pleasure.

An empty page for Crowdmark's pleasure.