Problem Set 3

Due: Monday, September 22

Reading Assignment: Sections 4.0-4.3, 4.5-4.8

Problem 1. [16 points] Warmup Exercises

For the following parts, a correct numerical answer will only earn credit if accompanied by it's derivation. Show your work.

(a) [4 pts] Use the Pulverizer to find integers s and t such that $139s + 61t = \gcd(139, 61)$.

(b) [4 pts] Use the previous part to find the inverse of 61 modulo 139 in the range $\{1, \ldots, 138\}$.

(c) [4 pts] Use Euler's theorem to find the inverse of 19 modulo 37 in the range $\{1, \ldots, 30\}$.

(d) [4 pts] Find the remainder of 38^{82248} divided by 83. (*Hint: Euler's theorem.*)

Problem 2. [16 points]

Prove the following statements, assuming all numbers are positive integers.

(a) [4 pts] If $a \mid b$, then $\forall c$, $a \mid bc$

(b) [4 pts] If $a \mid b$ and $a \mid c$, then $a \mid sb + tc$.

(c) [4 pts] $\forall c$, $a \mid b \Leftrightarrow ca \mid cb$

(d) [4 pts] $\gcd(ka, kb) = k \gcd(a, b)$

Problem 3. [20 points] In this problem, we will investigate numbers which are squares modulo a prime number p.

(a) [5 pts] An integer n is a square modulo p if there exists another integer x such that $n \equiv x^2 \pmod{p}$. Prove that $x^2 \equiv y^2 \pmod{p}$ if and only if $x \equiv y \pmod{p}$ or $x \equiv -y \pmod{p}$. (*Hint:* $x^2 - y^2 = (x + y)(x - y)$)

(b) [5 pts] There is a simple test we can perform to see if a number n is a square modulo p. It states that

Theorem 1 (Euler's Criterion)**.** *:*

1. *If n is a square modulo p then $n^{\frac{p-1}{2}} \equiv 1 \pmod{p}$.*
2. *If n is not a square modulo p then $n^{\frac{p-1}{2}} \equiv -1 \pmod{p}$.*

Prove the first part of Euler's Criterion. (*Hint: Use Fermat's theorem.*)

(c) [10 pts] Assume that $p \equiv 3 \pmod{4}$ and $n \equiv x^2 \pmod{p}$. Fine one possible value for x, expressed as a function of n and p. (*Hint: Write p as $p = 4k + 3$ and use Euler's Criterion. You might have to multiply two sides of an equation by n at one point.*)

Problem 4. [10 points] Prove that for any prime, p, and integer, $k \geq 1$,

$$\phi(p^k) = p^k - p^{k-1},$$

where ϕ is Euler's function. (*Hint: Which numbers between 0 and $p^k - 1$* are *divisible by p? How many are there?*)

Problem 5. [10 points] Using the RSA encryption system, Pete the publisher generates a private key (d, n) and posts a public key, (e, n), which anyone can use to send encrypted messages to Pete.

RSA has the useful property that these same keys can switch roles: if Pete wants to broadcast an unforgeable "signed" message, he can encrypt his message using his private key as though it was someone's public key. That is, from a plain text $m \in [0, n)$, Pete would broadcast a signed version, $s = \text{rem}\,(m^d, n)$.

Then anyone can decrypt and read Pete's broadcast message by using Pete's public key as though it were their own private key. Readers of Pete's message can be sure the message came from Pete if they believe that the only way to generate such a message is by using the private key which Pete alone knows. (This belief is widely accepted, but not certain.)

(a) [5 pts] Explain exactly what calculation must be performed on s to recover m using the public key (e, n). Explain why the calculation yields the plain text m.

(b) [5 pts] Big Earl notices that the next problem on the 6.042 students homework seems like it could be difficult to solve without guidance (or without showing up to lecture). He decides to send the encrypted, authenticated message 1535 to the students, who can use the public key (7, 7613) to decrypt the message. Each digit of the original message corresponds

to a letter of the alphabet found in the following legend:

$$\begin{aligned}
0 &= u \\
1 &= e \\
2 &= o \\
3 &= i \\
4 &= b \\
5 &= s \\
6 &= h \\
7 &= c \\
8 &= x \\
9 &= k
\end{aligned}$$

What is the original message, and to what one-word hint does it correspond?

Problem 6. [10 points] The Lucas series is defined by:

$$\begin{aligned}
L_1 &= 2 \\
L_2 &= 1 \\
L_n &= L_{n-1} + L_{n-2} \text{ for } n \geq 3
\end{aligned}$$

Prove that L_n and L_{n+1} are relatively prime.

Problem 7. [10 points] In this problem, we will investigate systems of linear congruence equations.

(a) [5 pts] Prove that for integers a and b,

$$x = rem(bsm + atn, mn)$$

is the unique solution in the range $0, 1, \ldots, mn - 1$ to the system of equations

$$x \equiv a \pmod{m} \tag{1}$$
$$x \equiv b \pmod{n} \tag{2}$$
$$\tag{3}$$

(Hint: There are two steps to this proof: (i) show that it is a solution, (ii) show that this solution is unique.)

(b) [5 pts] Next we will investigate the general case.

Theorem 2 (Chinese Remainder Theorem)**.** *Suppose that $n_1, n_2, ..., n_k$ are coprime. Then the following system of equations*

$$x \equiv a_i \pmod{n_i}, \qquad i = 1, \cdots, k$$

has a solution x, and moreover all such solutions are congruent modulo $N = n_1 \dots n_k$

We will construct an explicit solution. For each i, the integers n_i and $\frac{N}{n_i}$ are coprime and we can use the Pulverizer to find $r_i, s_i \in \mathbb{Z}$ such that $r_i n_i - \frac{s_i N}{n_i} = 1$.

Prove that $x = \sum_{i=1}^{k} a_i \frac{s_i N}{n_i}$ is a solution.