Problem Set 3

Due: Monday, September 24

Problem 1. [12 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) [3 pts] Use the Pulverizer to find integers $s$ and $t$ such that $101s + 53t = \gcd(101, 53)$.

(b) [3 pts] Use the previous part to find the inverse of 53 modulo 101 in the range \{1, \ldots, 100\}.

(c) [3 pts] Use Fermat’s theorem to find the inverse of 12 modulo 19 in the range \{1, \ldots, 18\}.

(d) [3 pts] Find the remainder of $26^{1818181}$ divided by 297. (Hint: Euler’s theorem.)

Problem 2. [12 points] Prove the following assertions:

(a) [4 pts] For all $c \neq 0$, $a \mid b$ if and only if $ca \mid cb$.

(b) [4 pts] $\gcd(ka, kb) = k \cdot \gcd(a, b)$ for all $k > 0$.

(c) [4 pts] If $ac \equiv bc \pmod{n}$ and $c \mid n$, then $a \equiv b \pmod{n/c}$.
Problem 3. [16 points] Using the RSA encryption system, Big Earl the anagramer generates a private key \((d, n)\) and posts a public key, \((e, n)\), which anyone can use to send encrypted messages to Earl. RSA has the useful property that these same keys can switch roles: if Earl wants to broadcast an unforgeable “signed” message, he can encrypt his message using his own private key. That is, from a plain text \(m \in [0, n]\), Earl would broadcast a “signed” version, \(s \equiv \text{rem}(m^d, n)\). Then anyone can decrypt and read Earl’s broadcasted public message by raising the message to the power of Earl’s public key. Readers of Earl’s message can be sure the message came from Earl if they believe that the only way to generate such a message is by using the Earl’s private key.

(a) [6 pts] Explain exactly what calculation must be performed on \(s\) to recover \(m\) using the public key \((e, n)\). Explain why this calculation yields the plain text \(m\).

(b) [10 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:

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

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

Problem 4. [15 points] Prove that the greatest common divisor of three integers \(a, b,\) and \(c\) is equal to their smallest positive linear combination; that is, the smallest positive value of \(sa + tb + uc\), where \(s, t,\) and \(u\) are integers.
Problem Set 3

Problem 5. [35 points] For \( k > 1 \), define
\[
F_k^* = \{ j \mid 1 \leq j \leq k - 1 \text{ and } \gcd(j, k) = 1 \}
\]
to be the set of integers between 1 and \( k - 1 \) that are relatively prime to \( k \). Suppose \( m, n \) are relatively prime and let \( s \) and \( t \) be integers such that \( sm + tn = 1 \).

(a) [10 pts] Prove that for integers \( a \) and \( b \),
\[
x = \text{rem}(bsm + atn, mn)
\]
is the unique solution in the range \( \{0, 1, \ldots, mn - 1\} \) to the system of equations
\[
x \equiv a \pmod{m},
\]
\[
x \equiv b \pmod{n}.
\]
(Hint: There are two steps to this proof: (i) show (1) is a solution to (2) and (3), and (ii) show that this solution is unique.)

(b) [5 pts] Prove that if \((a, b) \in F_m^* \times F_n^*\) then \( \text{rem}(bsm + atn, mn) \in F_{mn}^* \). What does this imply about the number of elements in \( F_m^* \times F_n^* \) versus the number of elements in \( F_{mn}^* \)?

(c) [10 pts] Prove that for an integer \( y \),
\[
(a, b) = (\text{rem}(y, m), \text{rem}(y, n))
\]
is the unique solution in the range \( \{0, 1, \ldots, m - 1\} \times \{0, 1, \ldots, n - 1\} \) satisfying
\[
y \equiv bsm + atn \pmod{mn}.
\]
(Hint: There are two steps to this proof: (i) show (4) is a solution to (5), and (ii) show that this solution is unique.)

(d) [5 pts] Prove that if \( y \in F_{mn}^* \) then \( (\text{rem}(y, m), \text{rem}(y, n)) \in F_m^* \times F_n^* \). What does this imply about the number of elements in \( F_m^* \times F_n^* \) versus the number of elements in \( F_{mn}^* \)?

(e) [5 pts] Conclude from the preceding parts of this problem that
\[
\phi(mn) = \phi(m)\phi(n)
\]
where \( \phi \) is Euler’s function.

Problem 6. [10 points] The Lucas series is defined by:
\[
L_1 = 2 \\
L_2 = 1 \\
L_n = L_{n-1} + L_{n-2} \text{ for } n \geq 3
\]
Show that \( \gcd(L_n, L_{n+1}) = 1 \).