

Problem Set 3

Due: Tuesday, September 23

Problem 1. [20 points] Warmup Exercises

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

- (a) [5 pts] Use the Pulverizer to find integers s and t such that $95s + 52t = \gcd(95, 52)$.
- (b) [5 pts] Use the previous part to find the inverse of 52 modulo 95 in the range $\{1, \dots, 94\}$.
- (c) [5 pts] Use Fermat's theorem to find the inverse of 13 modulo 23 in the range $\{1, \dots, 22\}$.
- (d) [5 pts] Find the remainder of $26^{1818181}$ divided by 297. (*Hint: Euler's theorem.*)

Problem 2. [15 points] Prove the following assertions:

- (a) [5 pts] For all $c \neq 0$, $a \mid b$ if and only if $ca \mid cb$.
- (b) [5 pts] $\gcd(a, b) = \gcd(\text{rem}(a, b), b)$ for all $b > 0$.
- (c) [5 pts] If $ac \equiv bc \pmod{n}$ and $c \mid n$, then $a \equiv b \pmod{n/c}$.

Problem 3. [35 points] For $k > 1$, define

$$k^* = \{j \mid 1 \leq j \leq k - 1 \text{ and } \gcd(j, k) = 1\}$$

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 ,

$$x = \text{rem}(bsm + atn, mn) \tag{1}$$

is the *unique* solution in the range $\{0, 1, \dots, mn - 1\}$ to the system of equations

$$x \equiv a \pmod{m}, \tag{2}$$

$$x \equiv b \pmod{n}. \tag{3}$$

(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 $(a, b) \in m^* \times n^*$ then $\text{rem}(bsm + atn, mn) \in (mn)^*$. What does this imply about the number of elements in $m^* \times n^*$ versus the number of elements in $(mn)^*$?

(c) [10 pts] Prove that for an integer y ,

$$(a, b) = (\text{rem}(y, m), \text{rem}(y, n)) \tag{4}$$

is the *unique* solution in the range $\{0, 1, \dots, m - 1\} \times \{0, 1, \dots, n - 1\}$ satisfying

$$y \equiv bsm + atn \pmod{mn}. \tag{5}$$

(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 $y \in (mn)^*$ then $(\text{rem}(y, m), \text{rem}(y, n)) \in m^* \times n^*$. What does this imply about the number of elements in $m^* \times n^*$ versus the number of elements in $(mn)^*$?

(e) [5 pts] Conclude from the preceding parts of this problem that

$$\phi(mn) = \phi(m)\phi(n)$$

where ϕ is Euler's function.

Problem 4. [10 points] Suppose that p is a prime and $0 < k < p$.

(a) [5 pts] k is *self-inverse* if $k^2 \equiv 1 \pmod{p}$. Prove that k is self-inverse iff either $k = 1$ or $k = p - 1$.

(Hint: $k^2 - 1 = (k - 1)(k + 1)$)

(b) [5 pts] Wilson's Theorem asserts

Theorem 1 (Wilson's Theorem). *If p is a prime, then*

$$(p - 1)! \equiv -1 \pmod{p}$$

The English mathematician Edward Waring said that this theorem would probably be very difficult to prove because there was no adequate notation for primes. Gauss proved it while standing (on one foot, it is rumored). He suggested that Waring failed for lack of notions, not notations. Prove Wilson's Theorem. (Hint: While standing on one foot, think about pairing each term in $(p - 1)!$ with its multiplicative inverse!)

Problem 5. [20 points] A critical question regarding RSA encryption (see Notes for Recitation 5) is whether decrypting an encrypted message always gives back the original message! That is, whether $\text{rem}((m^d)^e, n) = m$. This will follow from something slightly more general:

Lemma 2. *Let n be a product of distinct primes and $a \equiv 1 \pmod{\phi(n)}$ for some nonnegative integer, a . Then*

$$m^a \equiv m \pmod{n}. \quad (6)$$

(a) [5 pts] Explain why Lemma 2 implies that k and k^5 have the same last digit. For example:

$$\underline{2}^5 = 3\underline{2} \qquad \underline{79}^5 = 30770563\underline{99}$$

(Hint: What is $\phi(10)$)?

(b) [5 pts] Prove that if p is prime, then for all nonnegative integers $a \equiv 1 \pmod{p - 1}$,

$$m^a \equiv m \pmod{p}. \quad (7)$$

(c) [5 pts] Prove that if n is a product of distinct primes, and $a \equiv b \pmod{p}$ for all prime factors, p , of n , then $a \equiv b \pmod{n}$.

(d) [5 pts] Combine parts (b) and (c) to complete the proof of Lemma 2.

(e) [5 pts] **EXTRA CREDIT**

Explain why Lemma 2 implies that the original message, m , equals $\text{rem}((m^e)^d, n)$.