

Problem Set 3 Solutions

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 $95s + 52t = \gcd(95, 52)$.

Solution.

x	y	$\text{rem}(x, y)$	$= x - q \cdot y$
95	52	43	$= 95 - 1 \cdot 52$
52	43	9	$= 52 - 1 \cdot 43$ $= 52 - 1 \cdot (95 - 1 \cdot 52)$ $= -1 \cdot 95 + 2 \cdot 52$
43	9	7	$= 43 - 4 \cdot 9$ $= (95 - 1 \cdot 52) - 4 \cdot (-1 \cdot 95 + 2 \cdot 52)$ $= 5 \cdot 95 - 9 \cdot 52$
9	7	2	$= 9 - 1 \cdot 7$ $= (-1 \cdot 95 + 2 \cdot 52) - 1 \cdot (5 \cdot 95 - 9 \cdot 52)$ $= -6 \cdot 95 + 11 \cdot 52$
7	2	1	$= 7 - 3 \cdot 2$ $= (5 \cdot 95 - 9 \cdot 52) - 3 \cdot (-6 \cdot 95 + 11 \cdot 52)$ $= \boxed{23 \cdot 95 - 42 \cdot 52}$
2	1	0	

Exam tip: each time $\text{rem}(x, y)$ is calculated, substitutions are immediately made to then express it as a linear combination of 95 and 52 (using the remainders calculated on previous lines). Simplifying at each step leads to a much faster computation of s and t . ■

(b) [5 pts] Use the previous part to find the inverse of 52 modulo 95 in the range $\{1, \dots, 94\}$.

Solution. 53

From part (a), $1 = 23 \cdot 95 - 42 \cdot 52$ and so $1 \equiv -42 \cdot 52 \pmod{95}$. Therefore -42 is an inverse of 52. However, it is not the unique inverse of 52 in the range $\{1, \dots, 94\}$, which is given by $\text{rem}(-42, 95) = 53$. ■

(c) [5 pts] Use Fermat's theorem to find the inverse of 13 modulo 23 in the range $\{1, \dots, 22\}$.

Solution. 16

Since 23 is prime, Fermat's theorem implies $13^{23-2} \cdot 13 \equiv 1 \pmod{23}$ and so $\text{rem}(13^{23-2}, 23)$ is the inverse of 13 in the range $\{1, \dots, 22\}$. Using the method of repeated squaring,

$$\begin{aligned} 13^2 &= 169 \\ &= 7 \cdot 23 + 8 \\ &\equiv 8 \end{aligned}$$

$$\begin{aligned} 13^4 &\equiv 8^2 \\ &= 64 \\ &= 2 \cdot 23 + 18 \\ &\equiv 18 \end{aligned}$$

$$\begin{aligned} 13^8 &\equiv 18^2 \\ &= 324 \\ &= 14 \cdot 23 + 2 \\ &\equiv 2 \end{aligned}$$

$$\begin{aligned} 13^{16} &\equiv 2^2 \\ &= 4 \end{aligned}$$

$$\begin{aligned} 13^{21} &= 13^{16} \cdot 13^4 \cdot 13 \\ &\equiv 4 \cdot (6 \cdot 3) \cdot 13 \\ &= (4 \cdot 6) \cdot (3 \cdot 13) \\ &= 24 \cdot 39 \\ &\equiv 1 \cdot 39 \\ &\equiv \boxed{16} \end{aligned}$$

where the modulus for each of the congruences is 23. ■

(d) [5 pts] Find the remainder of $26^{1818181}$ divided by 297. (*Hint: Euler's theorem.*)

Solution. 26

Since $26 = 2 \cdot 13$ and $297 = 3^3 \cdot 11$ are relatively prime, Euler's theorem implies that $k^{\phi(297)} \equiv 1 \pmod{297}$ where

$$\begin{aligned} \phi(297) &= \phi(3^3 \cdot 11) \\ &= \phi(3^3) \cdot \phi(11) && \text{(since } \gcd(3^3, 11) = 1\text{)} \\ &= (3^3 - 3^2) \cdot (11 - 1) && \text{(since 3 and 11 are prime)} \\ &= 180. \end{aligned}$$

The trick is to notice that $1818181 = (180 \cdot 10101) + 1$, from which we can conclude

$$\begin{aligned} 26^{1818181} &= 26 \cdot 26^{180 \cdot 10101} \\ &\equiv 26 \cdot 1^{10101} \pmod{297} && \text{(by Euler's Theorem)} \\ &= 26. \end{aligned}$$

■

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

(a) [5 pts] For all $c \neq 0$, $a \mid b$ if and only if $ca \mid cb$.

Solution. The assertion $a \mid b$ holds if and only if there exists an integer k such that $ak = b$. For $c \neq 0$, this is true if and only if there exists an integer k such that $cak = cb$. And this holds if and only if $ca \mid cb$. ■

(b) [5 pts] $\gcd(a, b) = \gcd(\text{rem}(a, b), b)$ for all $b > 0$.

Solution. By the Division Algorithm, there exist unique integers q and $r = \text{rem}(a, b)$ such that $a = q \cdot b + r$ and $0 \leq r < b$. To show that $\gcd(a, b) = \gcd(r, b)$, it suffices to show that $\gcd(a, b) \mid \gcd(r, b)$ and $\gcd(r, b) \mid \gcd(a, b)$.

Since $\gcd(a, b)$ divides both a and b , it divides any linear combination of a and b , namely $a - qb = r$. Thus $\gcd(a, b)$ is a common divisor of r and b and must divide $\gcd(r, b)$.

Since $\gcd(r, b)$ divides both r and b , it divides any linear combination of r and b , namely $qb + r = a$. Thus $\gcd(r, b)$ is a common divisor of a and b and must divide $\gcd(a, b)$. ■

(c) [5 pts] If $ac \equiv bc \pmod{n}$ and $c \mid n$, then $a \equiv b \pmod{n/c}$.

Solution. If $ac \equiv bc \pmod{n}$ and $c \mid n$, then $(n/c)c \mid ac - bc$. This proves $n/c \mid a - b$, that is $a \equiv b \pmod{n/c}$. ■

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.)

Solution. By the definition of rem , there exists an integer v such that

$$x = bsm + atn + vmn \in \{0, 1, \dots, mn - 1\}.$$

Collecting multiples of m and applying $sm + tn = 1$,

$$\begin{aligned} x &= atn + (bs + vn)m \\ &\equiv atn \pmod{m} \\ &= a(1 - sm) \\ &\equiv a \pmod{m}. \end{aligned}$$

Similarly,

$$\begin{aligned} x &= bsm + (at + vm)n \\ &\equiv bsm \pmod{n} \\ &= b(1 - tn) \\ &\equiv b \pmod{n}. \end{aligned}$$

Therefore (1) is a solution to (2) and (3) in the range $\{0, 1, \dots, mn - 1\}$.

Next suppose that x, x' both satisfy congruences (2) and (3). Taking the differences we see that

$$x - x' \equiv 0 \pmod{m} \text{ and } x - x' \equiv 0 \pmod{n}.$$

So by definition, both m and n divide $x - x'$, and since m and n are relatively prime, this implies $mn \mid (x - x')$. But if x and x' are both in the range 0 to $mn - 1$, then $mn > |x - x'|$, so it must be that $x' = x$, as required. ■

(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 $(mn)^*$?

Solution. Suppose $(a, b) \in m^* \times n^*$ and let $x = \text{rem}(bsm + atn, mn)$. Then

$$\begin{aligned} 1 &= \text{gcd}(a, m) \\ &= \text{gcd}(\text{rem}(a, m), m) && \text{(by 2(b))} \\ &= \text{gcd}(\text{rem}(x, m), m) && \text{(by (2))} \\ &= \text{gcd}(x, m) && \text{(by 2(b))} \end{aligned}$$

and similarly, $\text{gcd}(x, n) = 1$ and we can conclude that $x \in (mn)^*$.

Since for every pair $(a, b) \in m^* \times n^*$ there is a unique $x \in (mn)^*$, it follows that $(mn)^*$ must have at least as many elements as $m^* \times n^*$. ■

(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

$$y \equiv bsm + atn \pmod{mn}. \quad (5)$$

(Hint: There are two steps to this proof: (i) show (4) is a solution to (5), and (ii) show that this solution is unique.)

Solution. By the definition of rem , $a = \text{rem}(y, m)$ and $b = \text{rem}(y, n)$ imply there exist integers j and k such that $a = y - jm$ and $b = y - kn$. Therefore,

$$\begin{aligned} bsm + atn &= (y - kn)sm + (y - jm)tn \\ &\equiv ysm + ytn \pmod{mn} \\ &= y(sm + tn) \\ &= y. \end{aligned}$$

Next suppose that (a, b) and (a', b') both satisfy (5). That is,

$$\begin{aligned} y &\equiv bsm + atn \pmod{mn} \\ y &\equiv b'sm + a'tn \pmod{mn}. \end{aligned}$$

Taking the difference we see that

$$0 \equiv (b - b')sm + (a - a')tn \pmod{mn},$$

implying that $(b - b')sm + (a - a')tn$ is divisible by m and by n . Therefore,

$$\begin{aligned} m \mid (a - a')tn &\Rightarrow m \mid (a - a')(1 - sm) \\ &\Rightarrow m \mid (a - a') \\ &\Rightarrow a \equiv a' \pmod{m}. \\ n \mid (b - b')sm &\Rightarrow n \mid (b - b')(1 - tn) \\ &\Rightarrow n \mid (b - b') \\ &\Rightarrow b \equiv b' \pmod{n} \end{aligned}$$

If a and a' are both in the range $\{0, \dots, m-1\}$ then they must be equal and if b and b' are both in the range $\{0, \dots, n-1\}$ then they too must be equal. ■

(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 $(mn)^*$?

Solution. Suppose $y \in (mn)^*$ and let $(a, b) = (\text{rem}(y, m), \text{rem}(y, n))$. Then since y and mn are relatively prime, y and m are relatively prime and y and n are relatively prime. Therefore,

$$\begin{aligned} 1 &= \text{gcd}(y, m) \\ &= \text{gcd}(\text{rem}(y, m), m) && \text{(by 2(b))} \\ &= \text{gcd}(a, m) \end{aligned}$$

and similarly, $\gcd(b, n) = 1$, and we can conclude that $a \in m^*$ and $b \in n^*$.

Since for every $y \in (mn)^*$ there is a unique $(a, b) \in m^* \times n^*$, it follows that $m^* \times n^*$ must have at least as many elements as $(mn)^*$. ■

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

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

where ϕ is Euler's function.

Solution. Since $\phi(mn)$ is the number of elements in $(mn)^*$ and $\phi(m)\phi(n)$ is the number of elements in $m^* \times n^*$, part (b) implies $\phi(mn) \geq \phi(m)\phi(n)$ and part (d) implies $\phi(mn) \leq \phi(m)\phi(n)$. Therefore, $\phi(mn) = \phi(m)\phi(n)$. ■

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

Solution. By definition of $\equiv \pmod{p}$, the integer k is self-inverse iff $p \mid k^2 - 1$. But $k^2 - 1 = (k - 1)(k + 1)$, and since p is a prime, we conclude that either $p \mid k - 1$ or $p \mid k + 1$. But $0 < k < p$, so $p \mid k - 1$ iff $k - 1 = 0$, and $p \mid k + 1$ iff $k + 1 = p$, so we must have $k = 1$ or $k = p - 1$.

Conversely, $1 \cdot 1 \equiv 1 \pmod{p}$ and $(p - 1) \cdot (p - 1) = p^2 - 2p + 1 \equiv 1 \pmod{p}$. ■

(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!*)

Solution. If $p = 2$, then the theorem holds, because $1 \equiv -1 \pmod{2}$. If $p > 2$, then $p - 1$ and 1 are distinct terms in the product $1 \cdot 2 \cdot \dots \cdot (p - 1)$, and these are the only self-inverses. Consequently, we can pair each of the remaining terms with its multiplicative inverse. Since the product of a number and its inverse is congruent to 1, all of these remaining terms cancel. Therefore, we have:

$$\begin{aligned} (p - 1)! &\equiv 1 \cdot (p - 1) \pmod{p} \\ &\equiv -1 \pmod{p} \end{aligned}$$

■

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:

$$\underline{2}^5 = \underline{32} \qquad \underline{79}^5 = \underline{3077056399}$$

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

Solution. Two nonnegative integers have the same last digit iff they are $\equiv \pmod{10}$. Now $\phi(10) = \phi(2)\phi(5) = 4$ and $5 \equiv 1 \pmod{4}$, so by Lemma 2,

$$k^5 \equiv k \pmod{10}. \quad \blacksquare$$

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

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

Solution. If $p \mid m$, then equation (7) holds since both sides of the congruence are $\equiv 0 \pmod{p}$.

So assume p does not divide m . Now if $a \equiv 1 \pmod{p-1}$, then $a = 1 + (p-1)k$ for some k , so

$$\begin{aligned} m^a &= m^{1+(p-1)k} \\ &= m \cdot (m^{p-1})^k \\ &\equiv m \cdot (1)^k \pmod{p} && \text{(by Fermat's Little Thm.)} \\ &\equiv m \pmod{p}. \end{aligned} \quad \blacksquare$$

(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 $a \equiv b \pmod{n}$.

Solution. By definition of congruence, $a \equiv b \pmod{k}$ iff $k \mid (a-b)$. So if $a \equiv b \pmod{p}$ for each prime factor, p , of n , then $p \mid (a-b)$ for each prime factor, p , and hence, so does their product (by the Unique Factorization Theorem). That is, $n \mid (a-b)$, which means $a \equiv b \pmod{n}$. \blacksquare

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

Solution. Suppose n is a product of distinct primes, $p_1 p_2 \cdots p_k$. Then from the formulas for the Euler function, ϕ , we have

$$\phi(n) = (p_1 - 1)(p_2 - 1) \cdots (p_k - 1).$$

Now suppose $a \equiv 1 \pmod{\phi(n)}$, that is, a is 1 plus a multiple of $\phi(n)$, so it is also 1 plus a multiple of $p_i - 1$. That is,

$$a \equiv 1 \pmod{p_i - 1}.$$

Hence, by part (b),

$$m^a \equiv m \pmod{p_i}$$

for all m . Since this holds for all factors, p_i , of n , we conclude from part (c) that

$$m^a \equiv m \pmod{n},$$

which proves Lemma 2. ■

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

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

Solution. In RSA, $n = pq$ is a product of distinct primes p and q so $\phi(n) = \phi(p)\phi(q) = (p - 1)(q - 1)$. The secret key, d , is computed such that $de \equiv 1 \pmod{\phi(n)}$. Therefore, by choosing $a = de$ the conditions required by Lemma 2 are satisfied.

From equation (6) we have

$$(m^e)^d = m^{de} \equiv m \pmod{pq}.$$

Hence,

$$\text{rem}((m^e)^d, pq) = \text{rem}(m, pq),$$

but $\text{rem}(m, pq) = m$, since $0 \leq m < pq$. ■