

Homework Assignment 4

Instructions. Submit your answers as a PDF on Webcourses by **October 21 at 11:59 p.m.** I encourage you to work in groups and discuss the problems with one another. You may also use AI tools, but remember that AI will not be available during exams. Use these problems to check your own understanding of the material. Your grade is based on participation, not correctness. You must submit your answers to receive credit for this assignment.

Justify every answer. You may use results from lectures and earlier parts of this assignment. Keep computations small by reducing modulo the relevant modulus at each step. Recall that $\mathbb{Z}_N = \{0, 1, \dots, N - 1\}$.

Question 1 Remainders of squares

Throughout this question, all variables are integers.

- (a) Compute the remainders of 0^2 , 1^2 , 2^2 , and 3^2 modulo 4. Explain why these four computations show that, for *every* integer n ,

$$n^2 \equiv 0 \pmod{4} \quad \text{or} \quad n^2 \equiv 1 \pmod{4}.$$

Your explanation should also cover negative integers.

Hint. Every integer is congruent to one of 0, 1, 2, 3 modulo 4, and congruent integers have congruent squares.

- (b) Using part (a), list the possible remainders of $x^2 + y^2$ modulo 4. Prove that

$$x^2 + y^2 \neq 4k + 3$$

for all integers x, y, k . Use this result to explain why $x^2 + y^2 = 31$ has no integer solutions, without searching through possible values of x and y .

- (c) A student claims, “Every nonnegative integer whose remainder modulo 4 is 0, 1, or 2 can be written as a sum of two integer squares.” Is this true? Test the claim on 6. Explain why passing the remainder test does not by itself guarantee that a representation as a sum of two squares exists.

Hint. If $x^2 + y^2 = 6$, each square is at most 6. List the possible square values.

Question 2 Different coefficients in Bézout's identity

Since $\gcd(12, 20) = 4$, Bézout's identity guarantees integers x, y such that

$$12x + 20y = 4.$$

The integers x, y are the *Bézout coefficients*; they may be positive, negative, or zero.

- Verify that both $(x, y) = (2, -1)$ and $(x, y) = (-3, 2)$ satisfy this equation. Explain why the gcd being unique does not mean that the coefficient pair is unique.
- If x increases by 5, how must y change to keep $12x + 20y$ unchanged? Starting with $(2, -1)$, use this observation to find two more coefficient pairs.
- Set $x = 2 + 5t$ and $y = -1 - 3t$ for any integer t . Verify that $12x + 20y = 4$. Explain why this gives infinitely many distinct coefficient pairs.
- Can $12x + 20y = 4$ hold with both x and y nonnegative integers? Explain what this tells you about the signs of the coefficients in this example.

Question 3 Finding a maximum in two different ways

The algorithms below find the largest entry of a nonempty array A . Repeated values are allowed. **MaxOne** accepts any positive array length; **MaxTwo** assumes the length is a power of 2. Each use of **max** compares its two arguments once. Count only these comparisons. Subarrays are passed without copying their entries.

MaxOne(A) :

```
if len(A) == 1:
    return the only entry of A
B = A without its last entry
t = MaxOne(B)
return max(t, last entry of A)
```

MaxTwo(A) :

```
if len(A) == 1:
    return the only entry of A
split A into equal halves L, R
u = MaxTwo(L)
v = MaxTwo(R)
return max(u, v)
```

- Prove that each algorithm returns the largest entry of A . Use induction on the array length for **MaxOne**, and on k when the length is 2^k for **MaxTwo**.
- Let $C_1(n)$ and $C_2(n)$ count the comparisons performed by the two algorithms on an array of length n . Derive a recurrence and base case for each, then find exact formulas. How many comparisons does each algorithm make when $n = 8$?
- For $n = 2^k$, find the maximum recursion depth of each algorithm, counting edges from the initial call to a base call. A student claims that **MaxTwo** uses $O(\log n)$ comparisons because it halves the input on every call. Explain the mistake. Use the recursion trees to explain how different depths can lead to the same total number of comparisons.

Question 4 Solving linear recurrences

Find a closed form for each sequence using its characteristic equation. Show the roots and determine the constants from the initial values. Check each formula at $n = 2$ using the recurrence.

(a) **Two distinct roots.**

$$a_0 = 3, \quad a_1 = 8, \quad a_n = 6a_{n-1} - 8a_{n-2} \quad (n \geq 2).$$

(b) **A repeated root.**

$$b_0 = 1, \quad b_1 = 6, \quad b_n = 6b_{n-1} - 9b_{n-2} \quad (n \geq 2).$$

Question 5 Analyzing recurrences

Treat each recurrence independently. In parts (b), (c), and (e), restrict n to powers of 2: $n = 2^k$ for integers $k \geq 0$.

For parts (a)–(c), find an **exact formula** for $T_i(n)$ and state its order of growth using big- O notation. Use expansion or recursion-tree levels, as in lecture. Show where the expansion stops and how you sum the work; do not simply quote a general theorem.

(a) **Decreasing by one.**

$$T_1(1) = 0, \quad T_1(n) = T_1(n-1) + (2n-1) \quad (n \geq 2).$$

(b) **One recursive call on half the input.**

$$T_2(1) = 0, \quad T_2(n) = T_2(n/2) + n \quad (n \geq 2).$$

(c) **Two recursive calls on half the input.**

$$T_3(1) = 0, \quad T_3(n) = 2T_3(n/2) + n \quad (n \geq 2).$$

Parts (b) and (c) have the same recursion depth. Explain why their total work has different orders of growth.

For parts (d)–(e), use **guess and check**: guess a bound of the form $T_i(n) \leq Cn$ or $T_i(n) \leq Cn^2$, then prove your bound by induction. Give an explicit constant C , check the base cases, and show why the inductive step works. Use strong induction when needed. You do not need an exact formula.

(d) **Unequal recursive input sizes.** For integers $n \geq 2$,

$$\begin{aligned} T_4(0) &= T_4(1) = 0, \\ T_4(n) &= T_4(\lfloor n/3 \rfloor) + T_4(\lfloor n/2 \rfloor) + n. \end{aligned}$$

Here $\lfloor x \rfloor$ means round x down to an integer.

Hint. Compare the sum of the two recursive input sizes with n . How much of the proposed bound remains to pay for the extra n units of work?

(e) **Three recursive calls and quadratic local work.**

$$T_5(1) = 1, \quad T_5(n) = 3T_5(n/2) + n^2 \quad (n \geq 2).$$

Hint. Substitute your proposed bound into each recursive term before choosing C .

Question 6 Proving the Chinese Remainder Theorem

Example. We want a number that leaves remainder 2 when divided by 3 and remainder 1 when divided by 5. In symbols,

$$x \equiv 2 \pmod{3}, \quad x \equiv 1 \pmod{5}.$$

The number $x = 11$ works, because $11 = 3 \cdot 3 + 2$ and $11 = 5 \cdot 2 + 1$. Among the numbers $0, 1, \dots, 14$, the ones leaving remainder 2 upon division by 3 are 2, 5, 8, 11, 14; only 11 also leaves remainder 1 upon division by 5.

In the notation below, $a = 3$ and $b = 5$ are the two divisors, and $r = 2$ and $s = 1$ are the desired remainders. The set $\mathbb{Z}_{ab} = \mathbb{Z}_{15} = \{0, 1, \dots, 14\}$ specifies the allowed range for x . Other integers, such as $26 = 11 + 15$, satisfy both congruences too; uniqueness is claimed within this range.

General statement. Let $a, b \geq 2$ be coprime integers. The *Chinese Remainder Theorem* says that for any integers r, s , there is exactly one $x \in \mathbb{Z}_{ab}$ satisfying

$$x \equiv r \pmod{a}, \quad x \equiv s \pmod{b}.$$

Bézout's identity gives integers u, v with $au + bv = 1$. We give you the proposed solution:

$$x = (rbv + sau) \bmod ab.$$

Your task is to prove that this formula works and that the solution is unique. Do not assume the Chinese Remainder Theorem in your proof.

- (a) Let $x_0 = rbv + sau$. Use $au + bv = 1$ to prove $x_0 \equiv r \pmod{a}$ and $x_0 \equiv s \pmod{b}$. Explain why reducing x_0 modulo ab preserves both congruences and gives a solution in $\mathbb{Z}_{ab}$.
- (b) Suppose x and y both satisfy the two congruences. Prove that $ab \mid (x - y)$, and conclude uniqueness in $\mathbb{Z}_{ab}$.
Hint. If $a \mid t$ and $b \mid t$, multiply $au + bv = 1$ by t and explain why each term on the left is divisible by ab .
- (c) Use the given formula to find the unique $x \in \mathbb{Z}_{35}$ with $x \equiv 2 \pmod{5}$ and $x \equiv 3 \pmod{7}$. You may use $1 = 3 \cdot 5 - 2 \cdot 7$. Check both congruences.
- (d) Give a pair of congruences modulo 4 and 6 that has no solution. Explain why this shows the coprimality assumption matters.

Question 7 RSA works for every message

Let p, q be distinct odd primes and $N = pq$. Choose positive integers e, d such that

$$ed = 1 + k(p-1)(q-1)$$

for an integer $k \geq 1$. For $m \in \mathbb{Z}_N$, encryption produces $c = m^e \bmod N$, and decryption produces $c^d \bmod N$. In lecture we proved correctness when $\gcd(m, N) = 1$. Here you will remove that assumption.

You may use Fermat's little theorem: if ℓ is prime and $\ell \nmid z$, then $z^{\ell-1} \equiv 1 \pmod{\ell}$.

- (a) A student tries to repeat the lecture proof for every message by writing $m^{(p-1)(q-1)} \equiv 1 \pmod{N}$. Explain the gap. For $N = 35$ and $m = 5$, show that this congruence cannot hold without computing 5^{24} .
- (b) Prove that $m^{ed} \equiv m \pmod{p}$ for every integer m . Consider separately the cases $p \mid m$ and $p \nmid m$. In the second case, explain why $ed - 1$ is a multiple of $p - 1$.
- (c) Obtain the analogous congruence modulo q and use Question 6 to prove that $c^d \bmod N = m$ for every $m \in \mathbb{Z}_N$. Explain why congruence modulo N gives equality of the recovered message and the original message, including when $m = 0$.
- (d) Take $p = 5$, $q = 7$, and $e = d = 5$. Check the condition on ed . Encrypt $m = 10$ and decrypt the resulting ciphertext. Use small modular computations; do not expand large powers as integers. Why is this example outside the promise used in lecture?
- (e) Define $\mathcal{E} : \mathbb{Z}_N \rightarrow \mathbb{Z}_N$ by $\mathcal{E}(m) = m^e \bmod N$. Use your decryption result to prove that $\mathcal{E}$ is one-to-one. Why must it also be onto? Explain what this says about whether two different messages can have the same ciphertext.