Math for CS 2015/2019 Problem Set 5 solutions

https://github.com/spamegg1

May 24, 2022

Contents

1 Problem 1 **1**
1.1 Background . . . 2
1.2 First attempt . . . 2
1.3 Magic trick . . . 3
1.4 Preliminary factoring . . . 3
1.5 Extended procedure . . . 3
1.6 Example of the procedure at work . . . 4
1.7 Conclusion . . . 6

2 Problem 2 **6**
2.1 (a) . . . 6
2.2 (b) . . . 7

3 Problem 3 **7**
3.1 (a) . . . 8
3.2 (b) . . . 9
3.3 (c) . . . 9
3.4 (d) . . . 10

1 Problem 1

Extend the binary gcd procedure of Problem 8.16 to obtain a new pulverizer that uses only division by 2 and subtraction in the course textbook.

Hint: After the binary gcd procedure has factored out 2's, it starts computing the $\gcd(a, b)$ for numbers a, b at least one of which is odd. It does this by successively updating a pair of numbers x, y such that $\gcd(x, y) = \gcd(a, b)$. Extend the procedure to find and update coefficients u_x, v_x, u_y, v_y such that

$$u_x a + v_x b = x \text{ and } u_y a + v_y b = y$$

To see how to update the coefficients when at least one of a and b is odd and $ua + vb$ is even, show that either u and v are both even, or else $u - b$ and $v + a$ are both even.

Proof. **1.1 Background**

This problem was extremely hard. The explanation in the Hint is very difficult to understand, the u and v mentioned in the last sentence is not even mentioned earlier in the Hint, so it looks like they copy-pasted it from somewhere else.

I had to do some research in other books to find the implementation. I found it in Chapter 14 of "Handbook of Applied Cryptography, CRC Press 1996". (Indeed there is direct reference to u and v there.)

First let's restate the Binary GCD procedure from Problem 8.16:

$$\begin{array}{rcll} \text{states} & ::= & \mathbb{N}^3 & \\ \text{start state} & ::= & (a, b, 1) & \\ \text{transitions} & ::= & \text{if } \min(x, y) > 0 \text{ then } (x, y, e) \to & \\ & & (x/2, y/2, 2e) & \text{if } 2 \mid x \text{ and } 2 \mid y \\ & & (x/2, y, e) & \text{else if } 2 \mid x \\ & & (x, y/2, e) & \text{else if } 2 \mid y \\ & & (x - y, y, e) & \text{else if } x > y \\ & & (y - x, x, e) & \text{else if } y > x \\ & & (1, 0, ex) & \text{otherwise } (x = y). \end{array}$$

1.2 First attempt

Now let's read the Hint and try to do what it says. Let us consider a case where at least one of a and b is odd. Say $a = 259$ and $b = 70$. In this case the GCD is 7: $259 = 7 \cdot 37$ and $70 = 2 \cdot 5 \cdot 7$.

At the beginning, we have $x = a$ and $y = b$, so it's natural to choose:

$$u_x = 1, v_x = 0, u_y = 0, v_y = 1$$

This way $u_x a + v_x b = 1 \cdot a + 0 \cdot b = a = x = 259$ and $u_y a + v_y b = 0 \cdot a + 1 \cdot b = b = y = 70$ hold.

At the next step we need to divide 70 by 2. So, how to update u_y and v_y?

With the current u_y and v_y we have: $u_y \cdot 259 + v_y \cdot 70 = 70$.

We want updated u_y and v_y so that: $u_y \cdot 259 + v_y \cdot 70 = \frac{70}{2}$.

We can divide the current equation by 2. We get: $\dfrac{u_y}{2} \cdot 259 + \dfrac{v_y}{2} \cdot 70 = \dfrac{70}{2}$.

But now the new coefficients $\dfrac{u_y}{2}, \dfrac{v_y}{2}$ may not be integers! (Remember $u_y = 0, v_y = 1$ in this case.)

We need to increase one of the coefficients, and decrease the other, in such a clever way, that both coefficients become integers, and the equation still remains satisfied.

1.3 Magic trick

Here is the rabbit-out-of-the-hat moment: we can increase the first coefficient by $y/2 = 70/2$, and decrease the second coefficient by $x/2 = 259/2$. So we are adding and subtracting the same number $70 \cdot 259/2$, which preserves the equality:

$$\frac{u_y}{2} \cdot 259 + \frac{70}{2} \cdot 259 + \frac{v_y}{2} \cdot 70 - \frac{259}{2} \cdot 70 = \frac{70}{2}$$

$$\frac{u_y + 70}{2} \cdot 259 + \frac{v_y - 259}{2} \cdot 70 = \frac{70}{2}$$

Now both $\frac{u_y + 70}{2}$ and $\frac{v_y - 259}{2}$ will be integers.

If both u_y and v_y were even, then we could just divide both of them by 2.

If instead x is even and y is odd, we will do a similar trick. If both x and y are odd, we will do a different trick. It would take too long to explain.

1.4 Preliminary factoring

Before describing the new procedure let's talk about a few things. In Problem 8.16 it is proved that, we reach a point, after which the rule

$$(x/2, y/2, 2e)$$

is never used again. Basically, we start with a and b, and we repeatedly use this rule to factor out the highest power of 2 that a and b have in common: $a = 2^k \cdot s$ and $b = 2^k \cdot t$ for some k. So we arrive at a situation where either s or t (or both) are odd.

1.5 Extended procedure

Let's start describing the new procedure. We are given input a, b. We want the GCD of a, b and the linear combination of a, b that gives us the GCD. For convenience, I changed the initial variables in the early part of the procedure to s, t instead.

1. Start with $s = a, t = b, e = 1$.

2. While $2 \mid s$ and $2 \mid t$, update: $s \to s/2$, $t \to t/2$, $e \to 2e$.

(At the end of this, at least one of s, t is odd.)

3. Initialize: $x = s, y = t, u_x = 1, v_x = 0, u_y = 0, v_y = 1$.

(From this point on, s and t do not change, x and y change instead.)

4. While x is even, update:

$x \to x/2$;

if both $2 \mid u_x$ and $2 \mid v_x$, then $u_x \to u_x/2$ and $v_x \to v_x/2$,

otherwise $u_x \to (u_x + t)/2$, $v_x \to (v_x - s)/2$;

5. While y is even, update:

$y \to y/2$;

if both $2 \mid u_y$ and $2 \mid v_y$, then $u_y \to u_y/2$ and $v_y \to v_y/2$,

otherwise $u_y \to (u_y + t)/2$, $v_y \to (v_y - s)/2$.

6. If $x \geq y$ then update: $x \to x - y$, $u_x \to u_x - u_y$, $v_x \to v_x - v_y$.

7. If $y > x$ then update: $y \to y - x$, $u_y \to u_y - u_x$, $v_y \to v_y - v_x$.

8. If $x = 0$ then stop. Otherwise go to Step 4.

We have: $\gcd(a, b) = e \cdot y = u_y a + v_y b$.

1.6 Example of the procedure at work

Let's go through the whole example of finding the GCD of $a = 1036$ and $b = 280$. I indicated which step of the procedure is being used as "(Step ?)".

(1.) $s = 1036, t = 280, e = 1$. (Step 1)

(2.) $s = 518, t = 140, e = 2$. (Step 2)

(3.) $s = 259, t = 70, e = 4$. (Step 2)

(4.) $x = 259, y = 70, u_x = 1, v_x = 0, u_y = 0, v_y = 1$. (Step 3)

Let's verify at each step the invariants $u_x s + v_x t = x$ and $u_y s + v_y t = y$:

$1 \cdot 259 + 0 \cdot 70 = 259 = x$✓

$0 \cdot 259 + 1 \cdot 70 = 70 = y$✓

(5.) $x = 259, y = 35, u_x = 1, v_x = 0, u_y = (0 + 70)/2 = 35, v_y = (1 - 259)/2 = -129$. (Step 5)

$1 \cdot 259 + 0 \cdot 70 = 259 = x$✓

$35 \cdot 259 + (-129) \cdot 70 = 35 = y$✓

(6.) $x = 259 - 35 = 224, y = 35, u_x = 1 - 35 = -34, v_x = 0 - (-129) = 129, u_y = 35, v_y = -129$. (Step 6)

$(-34) \cdot 259 + 129 \cdot 70 = 224 = x$✓

$35 \cdot 259 + (-129) \cdot 70 = 35 = y$✓

(7.) $x = 224/2 = 112, y = 35, u_x = (-34 + 70)/2 = 18, v_x = (129 - 259)/2 = -65, u_y = 35, v_y = -129.$ (Step 4)

$18 \cdot 259 - 65 \cdot 70 = 112 = x$✓

$35 \cdot 259 + (-129) \cdot 70 = 35 = y$✓

(8.) $x = 112/2 = 56, y = 35, u_x = (18+70)/2 = 44, v_x = (-65-259)/2 = -162, u_y = 35, v_y = -129.$ (Step 4)

$44 \cdot 259 - 162 \cdot 70 = 56 = x$✓

$35 \cdot 259 + (-129) \cdot 70 = 35 = y$✓

(9.) $x = 56/2 = 28, y = 35, u_x = 44/2 = 22, v_x = -162/2 = -81, u_y = 35, v_y = -129.$ (Step 4)

$22 \cdot 259 - 81 \cdot 70 = 28 = x$✓

$35 \cdot 259 + (-129) \cdot 70 = 35 = y$✓

(10.) $x = 28/2 = 14, y = 35, u_x = (22+70)/2 = 46, v_x = (-81-259)/2 = -170, u_y = 35, v_y = -129.$ (Step 4)

$46 \cdot 259 - 170 \cdot 70 = 14 = x$✓

$35 \cdot 259 + (-129) \cdot 70 = 35 = y$✓

(11.) $x = 14/2 = 7, y = 35, u_x = 46/2 = 23, v_x = -170/2 = -85, u_y = 35, v_y = -129.$ (Step 4)

$23 \cdot 259 - 85 \cdot 70 = 7 = x$✓

$35 \cdot 259 + (-129) \cdot 70 = 35 = y$✓

(12.) $x = 7, y = 35 - 7 = 28, u_x = 23, v_x = -85, u_y = 35 - 23 = 12, v_y = -129 - (-85) = -44.$ (Step 7)

$23 \cdot 259 - 85 \cdot 70 = 7 = x$✓

$12 \cdot 259 - 44 \cdot 70 = 28 = y$✓

(13.) $x = 7, y = 28/2 = 14, u_x = 23, v_x = -85, u_y = 12/2 = 6, v_y = -44/2 = -22.$ (Step 5)

$23 \cdot 259 - 85 \cdot 70 = 7 = x$✓

$6 \cdot 259 - 22 \cdot 70 = 14 = y$✓

(14.) $x = 7, y = 14/2 = 7, u_x = 23, v_x = -85, u_y = 6/2 = 3, v_y = -22/2 = -11.$ (Step 5)

$23 \cdot 259 - 85 \cdot 70 = 7 = x$✓

$3 \cdot 259 - 11 \cdot 70 = 7 = y$✓

(15.) $x = 7 - 7 = 0, y = 7, u_x = 23 - 3 = 20, v_x = -85 - (-11) = -74, u_y = 3, v_y = -11$. (Step 6)

$20 \cdot 259 - 74 \cdot 70 = 0 = x$✓

$3 \cdot 259 - 11 \cdot 70 = 7 = y$✓

(16.) Since $x = 0$ we stop (Step 8). So $\gcd(1036, 280) = e \cdot y = 4 \cdot 7 = 28$ and this gcd can be written as a linear combination: $3 \cdot 1036 - 11 \cdot 280 = 28$.

1.7 Conclusion

This does not really prove why the procedure is correct, I'm hoping one of you can shed light on it. I could not make heads or tails of the Hint. The updates of x, y are the same as in Problem 8.16, so that should work for the proof that the procedure produces the gcd. But I don't know how to prove that the procedure produces the correct coefficients u_y, v_y.

□

2 Problem 2

Suppose that p is a prime and $0 < k < p$.

2.1 (a)

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

Proof. Proving: if $k = 1$ or $k = p - 1$, then k is self-inverse.

1. Assume $k = 1$. Then $k^2 = 1 \equiv 1 \pmod{p}$. So k is self-inverse.

2. Assume $k = p - 1$. Then $k \equiv -1 \pmod{p}$, so $k^2 \equiv (-1)^2 = 1 \pmod{p}$. So k is self-inverse.

Proving: if k is self-inverse, then $k = 1$ or $k = p - 1$.

1. Assume k is self-inverse. So $k^2 \equiv 1 \pmod{p}$.

2. Then $k^2 - 1 \equiv 0 \pmod{p}$.

3. By (2) $k^2 - 1 = (k - 1)(k + 1) \equiv 0 \pmod{p}$.

4. Remember that if p is prime, then there are no "zero divisors" modulo p. In other words, if $xy \equiv 0 \pmod{p}$, then either $x \equiv 0 \pmod{p}$ or $y \equiv 0 \pmod{p}$ (or both). (Also remember that this is not true if p is not prime. For example $2 \cdot 3 \equiv 0 \pmod{6}$ but neither 2 nor 3 is zero.)

5. So by (3) either $k-1 \equiv 0$ or $k+1 \equiv 0 \pmod{p}$.

6. Using the fact that $0 < k < p$, (5) implies that either $k = 1$ or $k = p-1$. □

2.2 (b)

The English mathematician Edward Waring said that the following theorem would probably be very difficult to prove because there was no adequate notation for primes. Gauss then proved it (while standing on one foot, it is rumored); he suggested that Waring failed for lack of notions, not notations.

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

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

Prove Wilson's Theorem. *Hint:* While standing on one foot, think about pairing each term in $(p-1)!$ with its multiplicative inverse.

Proof. First consider the case $p = 2$. Then $(2-1)! = 1 \equiv -1 \pmod{2}$, so the Theorem is true in this case.

Now assume p is a prime greater than 2. (So p has to be odd.)

Recall that if p is prime, then all the numbers in $\{1, 2, 3, \ldots, p-1\}$ have multiplicative inverses (mod p) in $\{1, 2, 3, \ldots, p-1\}$.

The question is: which one of the numbers $\{1, 2, 3, \ldots, p-2, p-1\}$ is the inverse of which one? Some of them might be their own inverse.

Thankfully in part (a) we proved that, in $\{1, 2, 3, \ldots, p-1\}$, the only self-inverse numbers are 1 and $p-1$.

So the numbers in $\{2, 3, \ldots, p-2\}$ can be perfectly paired up with their inverses, because none of them are self-inverse, and there is an even number $(p-3)$ of them. Half of the set will be the numbers, while the other half will be the inverses of them.

This means that:

$$(p-1)! = (p-1) \cdot \Big((p-2) \cdot \ldots \cdot 3 \cdot 2\Big) \cdot 1 \equiv (p-1) \cdot \Big(1 \cdot \ldots \cdot 1\Big) \cdot 1 \pmod{p}$$

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

3 Problem 3

Suppose a, b are relatively prime integers greater than 1. In this problem you will prove that Euler's function is multiplicative, that is, that

$$\phi(ab) = \phi(a)\phi(b)$$

The proof is an easy consequence of the Chinese Remainder Theorem.

3.1 (a)

Conclude from the Chinese Remainder Theorem that the function $f : [0..ab) \to [0..a) \times [0..b)$ defined by

$$f(x) ::= (\text{rem}(x, a), \text{rem}(x, b))$$

is a bijection.

Proof. Remember the notation $[0..x)$ means the set of integers $\{0, 1, 2, \ldots, x-1\}$.

Let's remember the Chinese Remainder Theorem first: if $a, b > 1$ are relatively prime, then for all m, n there exists $x \in [0..ab)$ such that $x \equiv m \pmod{a}$ and $x \equiv n \pmod{b}$. Moreover x is unique up to (mod ab): if in addition $x' \equiv m \pmod{a}$ and $x' \equiv n \pmod{b}$ then $x \equiv x' \pmod{ab}$.

To prove that f is an injection:

1. Assume $x, x' \in [0..ab)$, and assume $f(x) = f(x')$. We want to prove $x = x'$.
2. By (1), $(\text{rem}(x, a), \text{rem}(x, b)) = (\text{rem}(x', a), \text{rem}(x', b))$.
3. By (2), $\text{rem}(x, a) = \text{rem}(x', a)$ and $\text{rem}(x, b) = \text{rem}(x', b)$.
4. Define $m = \text{rem}(x, a)$ and $n = \text{rem}(x, b)$.
5. By (3) we have $x \equiv m \pmod{a}$ and $x \equiv n \pmod{b}$.
6. Also by (3) we have $x' \equiv m \pmod{a}$ and $x' \equiv n \pmod{b}$.
7. By the uniqueness part of the Chinese Remainder Theorem, $x \equiv x' \pmod{ab}$.
8. Since both x and x' are in the interval $[0..ab)$, by (7) we get $x = x'$.

To prove that f is a surjection:

1. Assume $(y, z) \in [0..a) \times [0..b)$. We want to show there exists $x \in [0..ab)$ such that $f(x) = (y, z)$.
2. Apply the Chinese Remainder Theorem to $m = y, n = z$: there exists $x \in [0..ab)$ such that $x \equiv y \pmod{a}$ and $x \equiv z \pmod{b}$.
3. Since $y \in [0..a)$, by (2) we have $y = \text{rem}(x, a)$.
4. Similarly since $z \in [0..b)$, by (2) we have $z = \text{rem}(x, b)$.
5. Therefore by (3) and (4) we have $(y, z) = (\text{rem}(x, a), \text{rem}(x, b)) = f(x)$. □

3.2 (b)

For any positive integer, k, let $\mathbb{Z}_k^*$ be the integers in $[0..k)$ that are relatively prime to k. Prove that the function f from part (a) also defines a bijection from $\mathbb{Z}_{ab}^*$ to $\mathbb{Z}_a^* \times \mathbb{Z}_b^*$.

Proof. 1. $\mathbb{Z}_{ab}^*$ is a subset of $[0..ab)$.

2. We already know that f is injective (one-to-one). If we restrict the domain of f to a smaller subset $\mathbb{Z}_{ab}^*$ of its original domain $[0..ab)$, f will still be one-to-one.

3. So we need to prove that $f : \mathbb{Z}_{ab}^* \to \mathbb{Z}_a^* \times \mathbb{Z}_b^*$ is surjective. Assume $(y, z) \in \mathbb{Z}_a^* \times \mathbb{Z}_b^*$. We need to show there exists $x \in \mathbb{Z}_{ab}^*$ such that $f(x) = (y, z)$.

4. By the Chinese Remainder Theorem there exists $x \in [0..ab)$ such that $x \equiv y \pmod{a}$ and $x \equiv z \pmod{b}$.

5. By definition of $\mathbb{Z}_k^*$, y is relatively prime to a and z is relatively prime to b.

6. We claim that x is relatively prime to ab. Argue by contradiction and assume p is a prime that divides both x and ab.

7. Since a and b are relatively prime, either p divides a or p divides b (but not both).

8. Case 1: Assume p divides a (but not b).

9. By (4) $x \equiv y \pmod{a}$, so $x - y \equiv 0 \pmod{a}$, so a divides $x - y$.

10. Since p divides both x and a, there exist x', a' such that $x = px'$ and $a = pa'$.

11. By (9) there exists t such that $x - y = ta$.

12. By (11) and (10) we have $px' - y = tpa'$.

13. Solving for y we get $y = px' - tpa' = p(x' - ta')$.

14. So p divides y, which is a contradiction to the fact that y is relatively prime to a.

15. Case 2: Assume p divides b (but not a). Very similar to Case 1, we get a contradiction to the fact that z is relatively prime to b.

16. Therefore our assumption in (6) was false, and x is relatively prime to ab. Therefore $x \in \mathbb{Z}_{ab}^*$.

17. Now we simply need to show that $f(x) = (y, z)$. But this is obvious, since $f(x) = (\text{rem}(x, a), \text{rem}(x, b)) = (y, z)$ because $x \equiv y \pmod{a}$ and $y \in [0..a)$, and $x \equiv z \pmod{b}$ and $z \in [0..b)$. □

3.3 (c)

Conclude from the preceding parts of this problem that $\phi(ab) = \phi(a)\phi(b)$.

Proof. 1. By part (b) the size of $\mathbb{Z}_{ab}^*$ is equal to the size of $\mathbb{Z}_a^* \times \mathbb{Z}_b^*$ (because there is a bijection between them, and they are finite sets).

2. $\phi(ab)$ is defined as the number of integers relatively prime to ab, in other words, the size of $\mathbb{Z}_{ab}^*$.

3. $\phi(a)$ is defined as the number of integers relatively prime to a, in other words, the size of $\mathbb{Z}_a^*$.

4. $\phi(b)$ is defined as the number of integers relatively prime to b, in other words, the size of $\mathbb{Z}_b^*$.

5. The size of $\mathbb{Z}_a^* \times \mathbb{Z}_b^*$ is equal to the size of $\mathbb{Z}_a^*$ multiplied by the size of $\mathbb{Z}_b^*$.

5. By (1), (2), (3), (4) we have $\phi(ab) = \phi(a)\phi(b)$. □

3.4 (d)

Prove Corollary 8.10.11: for any number $n > 1$, if $p_1, p_2, \ldots, p_j$ are the (distinct) prime factors of n, then

$$\phi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_j}\right)$$

Proof. 1. We know from the lectures that for primes p we have $\phi(p) = p - 1$, and for prime powers p^k we have $\phi(p^k) = p^k - p^{k-1}$.

2. Using the Fundamental Theorem of Arithmetic, write n as

$$n = p_1^{k_1} p_2^{k_2} \ldots p_j^{k_j}$$

3. Note that each $p_i^{k_i}$ is relatively prime to every other one.

4. So, by repeatedly using part (c) and (1), we get

$$\phi(n) = \phi(p_1^{k_1} p_2^{k_2} \ldots p_j^{k_j}) = \phi(p_1^{k_1})\phi(p_2^{k_2}) \ldots \phi(p_j^{k_j}) = (p_1^{k_1} - p_1^{k_1-1}) \ldots (p_j^{k_j} - p_j^{k_j-1})$$

5. Reworking the last expression in (4) by factoring out $p_i^{k_i}$s we get

$$\phi(n) = (p_1^{k_1} - p_1^{k_1-1}) \ldots (p_j^{k_j} - p_j^{k_j-1}) = p_1^{k_1}\left(1 - \frac{1}{p_1}\right) \ldots p_j^{k_j}\left(1 - \frac{1}{p_j}\right)$$

6. Remembering that $n = p_1^{k_1} p_2^{k_2} \ldots p_j^{k_j}$, and putting it all together we get:

$$\phi(n) = p_1^{k_1}\left(1 - \frac{1}{p_1}\right) \ldots p_j^{k_j}\left(1 - \frac{1}{p_j}\right) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_j}\right)$$

□